УДК 004.67

Студ. К. О. Синяк
Науч. рук. ст. преп. Ю. О. Герман
(кафедра информационных систем и технологий, БГТУ)

ПРОГРАММНО-АППАРАТНОЕ СРЕДСТВО АУНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

Основанием для разработки программного изделия является мероприятие 12 «Создание Белорусской интегрированной сервисно-расчетной системы» подпрограммы 2 «Инфраструктура информатизации» Государственной программы развития цифровой экономики и информационного общества на 2016–2020 г.г., утвержденной постановлением Совета Министров Республики Беларусь от 23 марта 2016 г. № 235. Наименование темы: «Разработка программного обеспечения криптографического токена аутентификации единой системы идентификации физических и юридических лиц» [1–3].

Полное наименование – программный комплекс «Криптографический токен аутентификации». Условное наименование – КТА.

Областью применения КТА является обеспечение поддержки сервисов идентификации и аутентификации пользователей, зарегистрированных в единой системе идентификации физичесских и юридических лиц, и авторизации прикладной системы на доступ к ресурсам пользователя.

Пользователь, регистрируясь в единой системе идентификации физических и юридических лиц, соглашается с размещением его данных на сервере ресурсов. Ресурсы пользователя включают его идентификационные данные: полное имя, адрес, дату рождения, номер телефона и др. Кроме этого, в состав ресурсов могут входить настройки личного кабинета, история транзакций, личные файлы-документы.

В ходе регистрации пользователь и сервер идентификации согласуют перечень токенов аутентификации, сервер идентификации формирует и сохраняет у себя аттестат, касающийся согласованных токенов аутентификации.

Пользователь взаимодействует с прикладной системой и сервером идентификации с помощью клиентской программы, которая, как правило, выполняется на персональном компьютере или мобильном телефоне пользователя. В качестве клиентской программы может быть браузер, отдельное приложение или связка браузера с приложением.

В ходе взаимодействия токена аутентификации и сервера идентификации выполняется аутентификация пользователя. При аутенти-

фикации клиентской программы используется токен аутентификации пользователя, а сервер идентификации — его аттестат.

Одним из видов токенов аутентификации является КТА, который обеспечивает максимальный уровень гарантий аутентификации.

Если пользователь использует КТА для аутентификации перед сервером, то его ресурсы могут размещаться на КТА. При этом сервер идентификации выступает в роли виртуального сервера ресурсов, который логически хранит часть ресурсов пользователей на их же токенах.

В КТА реализованы следующие основные задачи:

1) аутентификация владельца на доступ к ресурсам и сервисам токена (активация токена);

2) управление объектами, размещенными в пределах криптографической границы токена;

3) аутентификация сервера идентификации и аутентификация перед ним;

4) установка защищенного соединения с сервером идентификации;

5) проверка полномочий сервера идентификации и передача ему ресурсов владельца;

6) выработка и проверка электронной цифровой подписи.

ЛИТЕРАТУРА

1. СТБ 34.101.19 Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых. – Минск, Госстандарт, 2013. – 42 с.

2. СТБ 34.101.27 Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации. – Минск, Госстандарт, 2011. – 33 с.

3. СТБ 34.101.31 Информационные технологии и безопасность. Защита информации. Криптографические алгоритмы шифрования и контроля целостности. – Минск, Госстандарт, 2011. – 32 с.