

БЕЗОПАСНОСТЬ ПРИ АУТЕНТИФИКАЦИИ ФИЗИЧЕСКИХ ЛИЦ ПОСРЕДСТВОМ ЕДИНОЙ СИСТЕМЫ ИДЕНТИФИКАЦИИ ФИЗИЧЕСКИХ И ЮРИДИЧЕСКИХ ЛИЦ

Д.И. Шуманский

Единая система идентификации физических и юридических лиц (ЕС ИФЮЛ) является компонентом Белорусской интегрированной сервисно-расчетной системы (БИСРС) и предназначена для предоставления гражданам Республики Беларусь сервисов строгой цифровой аутентификации для получения электронных услуг в информационных системах электронного правительства. Взаимодействие ЕС ИФЮЛ с внешними информационными системами построено на базе спецификации Open ID connect, расширенной криптографическими алгоритмами, стандартизированными в Республике Беларусь.

Защита данных, передаваемых от ЕСИФЮЛ до внешней информационной системы достигается использованием средств выработки ЭЦП и средств предварительного шифрования, сертифицированных на соответствие требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ). Защита данных, передаваемых от идентификационной карты до ЕС ИФЮЛ, достигается передачей информации в зашифрованном виде на общем ключе, сформированном в результате выполнения протокола VAUTH (п. 8.4 СТБ 34.101.78). Защита данных, передаваемых от клиентской программы до ЕС ИФЮЛ, достигается путем применения алгоритма предварительного шифрования BELT-CFB256 (п. 6.4 СТБ 34.101.31). Защита данных, передаваемых от клиентской программы до информационной системы, достигается путем применения протокола защиты транспортного уровня TLS (СТБ 34.101.65).

Идентификационная карта гражданина Республики Беларусь содержит два криптографических приложения eID и eSign. Приложение eID предназначено для хранения и предоставления персональных данных. Приложение eSign содержит личный ключ ЭЦП и предназначено для выработки электронной цифровой подписи. Идентификационная карта является пропуском гражданина в мир электронного правительства Республики Беларусь.