

Информационное письмо

Настоящим сообщаем, что ФСБ России письмом с номером № 149/3/2/1-1403 от 05.05.2026 г. согласовано техническое задание на опытно-конструкторскую работу «Разработка и проведение тематических исследований средства криптографической защиты информации «КриптоПро CSP» версии 6.0».

СКЗИ «КриптоПро CSP» версии 6.0 является развитием СКЗИ «КриптоПро CSP» версии 5.0, а также должно реализовывать следующие операции:

- шифрование/расшифрование, вычисление имитовставки (в соответствии с ГОСТ 28147-89, ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018));
- выработка значения хэш-функции (в соответствии с ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018));
- создание электронной подписи (ЭП) (в соответствии с ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018));
- проверка ЭП (в соответствии с ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018));
- создание ключа ЭП/ключа проверки ЭП;
- поддержка протоколов: TLS, IPsec, SESPake, PKINIT, EFS;
- поддержка форматов криптографических сообщений: CMS, *AdES.

Ключевой особенностью СКЗИ «КриптоПро CSP» версии 6.0 является реализация преобразований, рассматриваемых в качестве постквантовых: алгоритм ЭП и механизм инкапсуляции ключа, а также реализация протокола защиты канала на основе TLS с использованием механизма инкапсуляции ключа.

В соответствии с техническим заданием в состав СКЗИ «КриптоПро CSP» версии 6.0 должно быть включено приложение «КриптоПро-Браузер» – веб-браузер с поддержкой совместной работы с ППО «КриптоПро Browser plug-in» и возможностью установки TLS-соединений с использованием российских криптографических алгоритмов.

Помимо этого, в СКЗИ «КриптоПро CSP» версии 6.0 должны быть включены и другие улучшения, в том числе связанные с актуализацией и расширением перечня сред функционирования, оптимизацией работы провайдера.

В соответствии с ТЗ СКЗИ «КриптоПро CSP» версии 6.0 должно удовлетворять установленным ФСБ России требованиям по классам КС1, КС2 и КС3.

Генеральный директор
ООО «КРИПТО-ПРО»

С.В. Смышляев