

## Информационное письмо

Настоящим сообщаем, что ООО «КРИПТО-ПРО» письмом № 149/3/2/1-2506 от 06.09.2023 получило выписку из заключения ФСБ России по результатам экспертизы тематических исследований СКЗИ «КриптоПро CSP» версий 5.0 R3 KC1 (исполнение 1-КриптоАРМ ГОСТ 3) и 5.0 R3 KC2 (исполнение 2-КриптоАРМ ГОСТ 3).

Исполнения 1-КриптоАРМ ГОСТ 3 и 2-КриптоАРМ ГОСТ 3 СКЗИ «КриптоПро CSP» версии 5.0 R3 (в состав данных исполнений входит приложение КриптоАРМ ГОСТ, производитель ООО «Цифровые технологии») являются развитием исполнений 1-КриптоАРМ и 2-КриптоАРМ, входящих в состав СКЗИ «КриптоПро CSP» версии 5.0 R2. В указанные исполнения в новой версии СКЗИ «КриптоПро CSP» был добавлен почтовый клиент, поддерживающий алгоритмы ГОСТ при подключении по протоколу TLS к почтовым серверам и при обработке почтовых сообщений S/MIME (шифровании, подписи), модули поддержки алгоритмов ГОСТ для криптографической защиты сообщений форматов XML и PDF, а также добавлена поддержка работы под управлением ОС «Аврора».

В соответствии с указанной выпиской из заключения СКЗИ «КриптоПро CSP» версии 5.0 R3 KC1 (исполнение 1-КриптоАРМ ГОСТ 3) и 5.0 R3 KC2 (исполнение 2-КриптоАРМ ГОСТ 3) в составе согласно формулярам (ЖТЯИ.00101-13 30 01 и ЖТЯИ.00102-13 30 01 соответственно) при выполнении операций:

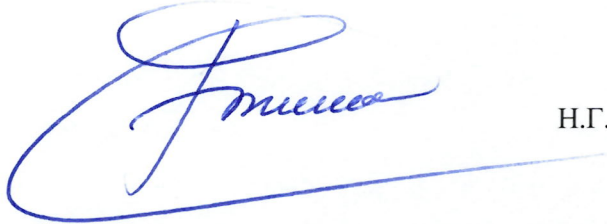
- зашифрование/расшифрование, вычисление имитовставки (в соответствии с ГОСТ 28147-89, ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018));
- создание ЭП (в соответствии с ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018));
- проверка ЭП (в соответствии с ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018));
- выработка значения хэш-функции (в соответствии с ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018));
- создание ключа ЭП/ключа проверки ЭП,

удовлетворяет «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» для СКЗИ класса KC1 (версия 5.0 R3 KC1 (исполнение 1-КриптоАРМ ГОСТ 3)) и KC2 (версия 5.0 R3 KC2 (исполнение 2-КриптоАРМ ГОСТ 3)), «Специальным требованиям к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации. СТ-Р» и «Требованиям по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» для СКЗИ по уровню КС<sup>Б</sup>, а также «Требованиям к средствам электронной подписи», утверждённым приказом ФСБ России от 27.12.2011 г. №796, для средств ЭП

классов КС1 (версия 5.0 R3 КС1 (исполнение 1-КриптоАРМ ГОСТ 3)) и КС2 (версия 5.0 R3 КС2 (исполнение 2-КриптоАРМ ГОСТ 3)).

СКЗИ «КриптоПро CSP» версии 5.0 R3 разрешается эксплуатировать до 01 мая 2024 года.

Генеральный директор  
ООО «КРИПТО-ПРО»

A handwritten signature in blue ink, appearing to read 'Н.Г. Чернова', with a long horizontal flourish extending to the right.

Н.Г. Чернова