ООО "КРИПТО-ПРО"
127018, Москва, ул. Сущёвский Вал, 18
Телефон: (495) 995-48-20
https://www.cryptopro.ru
e-mail: info@cryptopro.ru

№ 15587 от 09.04.2025

Руководителям организаций

Информационное письмо

Настоящим сообщаем, что ООО «КРИПТО-ПРО» получило выписку из заключения ФСБ России (№ 149/3/2/1-992 от 02.04.2025) по результатам экспертизы тематических исследований СКЗИ «КриптоПро CSP» версий 5.0 R3 КС1 (исполнение 1-Base), 5.0 R3 КС2 (исполнение 2-Base), 5.0 R3 КС3 (исполнение 3-Base), доработанных в соответствии с извещениями об изменениях (ЖТЯИ.00101-03.2-2024, ЖТЯИ.00102-03.2-2024, ЖТЯИ.00103-03.2-2024 соответственно). Рабочее название изделия: СКЗИ «КриптоПро CSP» версия 5.0 R3+ (сборка № 5.0.13003).

Ключевыми особенностями обновленной версии СКЗИ «КриптоПро CSP» являются:

- поддержка индивидуальных ключевых носителей «РусТокен-Lite-A» и «РусТокен-Lite-AC» при работе СКЗИ под управлением ОС семейств Windows, Linux и FreeBSD;
- поддержка версий мобильных ОС — Android 15 и iOS (включая iPadOS) 18;
- повышение производительности выполнения криптографических операций при взаимодействии СКЗИ «КриптоПро CSP» с ПАКМ «КриптоПро HSM».

В соответствии с указанной выпиской из заключения СКЗИ «КриптоПро CSP» версии 5.0 R3+ (исполнения 1-Base, 2-Base, 3-Base) в составе согласно Формулярам (ЖТЯИ.00101-03 30 01, ЖТЯИ.00102-03 30 01, ЖТЯИ.00103-03 30 01 соответственно), доработанные в соответствии с указанными выше извещениями об изменениях при выполнении алгоритмов и 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 34.11-2012 (ГОСТ 34.11-2018));
- создание ключа ЭП/ключа проверки ЭП,

используемых при помощи функций, приведенных в Приложениях 2 Правил пользования (ЖТЯИ.00101-03 95 01, ЖТЯИ.00102-03 95 01, ЖТЯИ.00103-03 95 01 соответственно), а также при выполнении криптографических протоколов:

- CMS;
- EFS (только исполнение 3-Base)
- TLS;
- IPsec;
- SESPAKE;
- PKINIT,

реализованных с использованием перечисленных выше алгоритмов, удовлетворяют «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» для СКЗИ класса КС1 (исполнение 1-Base), класса КС2 (исполнение 2-Base) и класса КС3 (исполнение 3-Base), «Требованиям к средствам электронной подписи», утверждённым приказом ФСБ России от 27 декабря 2011 г. №796, для средств ЭП класса КС1 (исполнение 1-Base), класса КС2 (исполнение 2-Base) и класса КС3 (исполнение 3-Base), «Специальным требованиям к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации (СТ-Р)» для СКЗИ по уровню $КС_Б$, а также «Требованиям по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» по уровню защищенности $КС_Б$.

СКЗИ «КриптоПро CSP» версии 5.0 R3+ разрешается эксплуатировать до 01 мая 2029 года.

Генеральный директор
ООО «КРИПТО-ПРО» С.В. Смышляев