

№ 9740 от 04.12.2018

Руководителям организаций

Информационное письмо

Настоящим сообщаем, что ООО «КРИПТО-ПРО» письмом № 149/3/2/2-2977 от 04.12.2018 получило выписку из заключения ФСБ России по результатам экспертизы тематических исследований СКЗИ «КриптоПро CSP» версии 4.0 R4 (исполнения 1-Base, 2-Base, 3-Base, 1-Lic, 2-Lic).

В соответствии с указанной выпиской из заключения СКЗИ «КриптоПро CSP» версии 4.0 R4 (исполнения 1-Base, 2-Base, 3-Base, 1-Lic, 2-Lic), доработанное в соответствии с извещениями об изменениях (ЖТЯИ.00087-03.1-2018, ЖТЯИ.00088-03.1-201, ЖТЯИ.00089-03.1-2018, ЖТЯИ.00087-04.1-2018, ЖТЯИ.00088-04.1-2018 соответственно), в составе согласно формулярам (ЖТЯИ.00087-03 30 01, ЖТЯИ.00088-03 30 01, ЖТЯИ.00089-03 30 01, ЖТЯИ.00087-04 30 01, ЖТЯИ.00088-04 30 01 соответственно) при выполнении операций:

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

реализуемых при помощи функций, приведенных в Приложении 2 Правил пользования, а также при выполнении криптографических протоколов:

- EFS (только для исполнения 3-Base);
- TLS;
- PKINIT (только для исполнения 3-Base),

реализованных с использованием перечисленных выше алгоритмов, удовлетворяет Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, для СКЗИ классов КС1 (исполнения 1-Base, 1-Lic), КС2 (исполнения 2-Base, 2-Lic) и КС3 (исполнение 3-Base), Специальным требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации, по уровню КС и Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27.12.2011 г. №796, для средств ЭП классов КС1 (исполнения 1-Base, 1-Lic), КС2 (исполнения 2-Base, 2-Lic), и КС3 (исполнение 3-Base).

СКЗИ «КриптоПро CSP» версии 4.0 R4 (исполнения 1-Base, 2-Base, 1-Lic, 2-Lic) разрешается эксплуатировать до 15 января 2021 года.

СКЗИ «КриптоПро CSP» версии 4.0 R4 (исполнение 3-Base) разрешается эксплуатировать до 20 ноября 2022 года.

Использование СКЗИ «КриптоПро CSP» версии 4.0 R4 для формирования электронной подписи по ГОСТ Р 34.10-2001 после 31 декабря 2019 года не допускается.

Генеральный директор  
ООО «КРИПТО-ПРО»



Н.Г. Чернова