

№ 10203 от 13.05.2019**Руководителям организаций**

## Информационное письмо

Настоящим сообщаем, что ООО «КРИПТО-ПРО» письмом № 149/3/2/2-972 от 07.05.2019 получило выписку из заключения ФСБ России по результатам экспертизы тематических исследований СКЗИ «КриптоПро CSP» версий 5.0 КС1 исполнение 1-Base, 5.0 КС2 исполнение 2-Base, 5.0 КС3 исполнение 3-Base (далее — СКЗИ «КриптоПро CSP» версия 5.0).

В соответствии с указанной выпиской из заключения СКЗИ «КриптоПро CSP» версии 5.0 (исполнения 1-Base, 2-Base, 3-Base) в составе согласно формулярам (ЖТЯИ.00101-01 30 01, ЖТЯИ.00102-01 30 01, ЖТЯИ.00103-01 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, 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,

используемых при помощи функций, приведенных в приложении 2 Правил пользования, а также при выполнении криптографических протоколов:

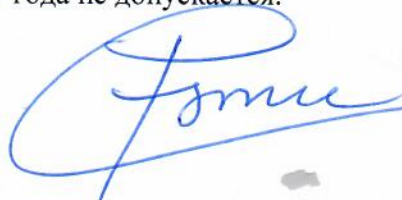
- CMS;
- EFS (только для исполнения 3-Base);
- TLS;
- IPsec;
- SESPAKE;
- PKINIT (только для исполнения 3-Base),

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 (версия 5.0 КС1 исполнение 1-Base), КС2 (версия 5.0 КС2 исполнение 2-Base) и КС3 (версия 5.0 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 (версия 5.0 КС1 исполнение 1-Base), КС2 (версия 5.0 КС2 исполнение 2-Base) и КС3 (версия 5.0 КС3 исполнение 3-Base).

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

Использование СКЗИ «КриптоПро CSP» версии 5.0 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