

Информационное письмо

Настоящим сообщаем, что ООО «КРИПТО-ПРО» письмом № 149/3/2/2-3069 от 30.12.2020 получило выписку из заключения ФСБ России по результатам экспертизы тематических исследований СКЗИ «КриптоПро CSP» версий 5.0 R2 KC1 исполнение 1-КриптоАРМ и 5.0 R2 KC2 исполнение 2-КриптоАРМ.

Исполнения 1-КриптоАРМ и 2-КриптоАРМ СКЗИ «КриптоПро CSP» версии 5.0 R2 (в состав данных исполнений входит приложение КриптоАРМ ГОСТ, производитель ООО «Цифровые технологии») предоставляют графический интерфейс для создания/проверки ЭП (в формате CMS) файлов, шифрования/расшифрования данных (в формате CMS) в файлах, создания и управления ключевой информацией, работы с объектами инфраструктуры PKI, а также позволяют установить защищенное соединение по протоколу TLS.

В соответствии с указанной выпиской из заключения СКЗИ «КриптоПро CSP» версии 5.0 R2 KC1 исполнение 1-КриптоАРМ и СКЗИ «КриптоПро CSP» версии 5.0 R2 KC2 исполнение 2-КриптоАРМ в составе согласно формулярам (ЖТЯИ.00101-12 30 01 и ЖТЯИ.00102-12 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 34.11-2012 (ГОСТ 34.11-2018));
- создание ключа ЭП/ключа проверки ЭП,

удовлетворяют «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» для СКЗИ класса KC1 (версия 5.0 R2 KC1 исполнение 1-КриптоАРМ) и KC2 (версия 5.0 R2 KC2 исполнение 2-КриптоАРМ), «Специальным требованиям к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации» и «Требованиям по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» для СКЗИ по уровню КСБ и «Требованиям к средствам электронной подписи», утверждённым приказом ФСБ России от 27.12.2011 г. №796, для средств ЭП классов KC1 (версия 5.0 R2 KC1 исполнение 1-КриптоАРМ) и KC2 (версия 5.0 R2 KC2 исполнение 2-КриптоАРМ).

СКЗИ «КриптоПро CSP» версии 5.0 R2 разрешается эксплуатировать до 01.05.2024.

Генеральный директор
ООО «КРИПТО-ПРО»



Н.Г. Чернова