ООО «КРИПТО-ПРО»
Адрес офиса: 127018, г. Москва,
Сущёвский вал, д. 18, эт.17
Почтовый адрес: 127018, г. Москва,
а/я «КРИПТО-ПРО» (б/н)
Тел./факс: (495) 995-48-20

№ 9301 от 30.07.2018

Руководителям организаций

Информационное письмо

Настоящим сообщаем, что ООО «КРИПТО-ПРО» получило выписку из заключения ФСБ России (№ 149/3/2/2-1788 от 27.07.2018) по результатам экспертизы тематических исследований ПАКМ «КриптоПро HSM» версия 2.0 (Комплектация 3).

В Комплектацию 3 входят следующие исполнения: «DSS+myDSS» (iOS, Android), «DSS+AirKey Lite» (iOS, Android), «DSS+SIM (QES)» (уровень защиты КС1), а также «DSS+CSP 3.9 (исп. 1, 2, 3)» и «DSS+CSP 4.0 (1-Base, 2-Base, 3-Base)» (уровни защиты КС1, КС2, КС3); перечень доступных с устанавливаемых на стационарное рабочее место клиентских компонент DSS интерфейсов включает функционал Cloud CSP.

В соответствии с указанной выпиской из заключения, ПАКМ «КриптоПро HSM» версия 2.0 (Комплектация 3) в составе согласно формуляру ЖТЯИ.00096-02 30 01 при выполнении операций:

- создание и управление ключевой информацией;
- 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;
- идентификации, аутентификации, шифрования и имитозащиты TLS-соединений;
- криптографической аутентификации абонентов при установлении соединения,

реализуемых при помощи функций, приведенных в Приложениях 1 и 2 документа ЖТЯИ.0096-02 95 01, удовлетворяет (за исключением реализации иностранных алгоритмов) Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, для СКЗИ классов КС1/КС2/КС3, 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/КС2/КС3.

При использовании функций, не указанных в Приложениях 1 и 2 документа ЖТЯИ.00096-02 95 01, использование ПАКМ «КриптоПро HSM» версия 2.0 (Комплектация 3) допускается только для построения на его основе криптосредств, с проведением установленным порядком его тематических исследований.

ПАКМ «КриптоПро HSM» версия 2.0 (Комплектация 3) разрешается эксплуатировать до 01 февраля 2023 года.

Генеральный директор
ООО «КРИПТО-ПРО» Н.Г. Чернова

Исп. Мошнина Д.А. (495) 995-48-20, доб. 208