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

№ 11750 от 11.01.2021

Руководителям организаций

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 КС1 исполнение 1-Base, 5.0 R2 КС2 исполнение 2-Base, 5.0 R2 КС3 исполнение 3-Base (далее — СКЗИ «КриптоПро CSP» версия 5.0 R2).

Ключевыми особенностями новой версии «КриптоПро CSP» являются поддержка российских криптографических стандартов 2015 года (ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015) и современных версий протоколов TLS и CMS, возможность эксплуатировать СКЗИ без проведения исследований по оценке влияния с веб-серверами Apache и nginx, а также с браузером Chromium ГОСТ (в ОС Astra Linux), поддержка операционной системы Astra Linux по классу КС3, расширение перечней поддерживаемых программно-аппаратных платформ, ключевых носителей и СЗИ, развитие приложения для создания TLS-туннеля в виде утилиты stunnel_mssp, а также расширение перечня вызовов, использование которых при разработке систем на основе СКЗИ возможно без дополнительных тематических исследований, – в него теперь входят и функции установки клиентских TLS-соединений (с односторонней и двусторонней аутентификацией).

В соответствии с указанной выпиской из заключения СКЗИ «КриптоПро CSP» версии 5.0 R2 (исполнения 1-Base, 2-Base, 3-Base) в составе согласно формулярам (ЖТЯИ.00101-02 30 01, ЖТЯИ.00102-02 30 01, ЖТЯИ.00103-02 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,

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

- CMS;
- TLS;
- IPsec;
- SESPAKE,

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 класса КС1 (версия 5.0 R2 КС1 исполнение 1-Base), КС2 (версия 5.0 R2 КС2 исполнение 2-Base) и КС3 (версия 5.0 R2 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» и «Требованиям по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» для СКЗИ по уровню $КС_Б$ и «Требованиям к средствам электронной подписи», утверждённым приказом ФСБ России от 27.12.2011 г. №796, для средств ЭП классов КС1 (версия 5.0 R2 КС1 исполнение 1-Base), КС2 (версия 5.0 R2 КС2 исполнение 2-Base) и КС3 (версия 5.0 R2 КС3 исполнение 3-Base).

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

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

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