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

№ 13892 от 18.09.2023

Руководителям организаций

Информационное письмо

Настоящим сообщаем, что ООО «КРИПТО-ПРО» письмом № 149/3/2/1-2506 от 06.09.2023 получило выписку из заключения ФСБ России по результатам экспертизы тематических исследований СКЗИ «КриптоПро CSP» версий 5.0 R3 КС1 исполнение 1-Base, 5.0 R3 КС2 исполнение 2-Base, 5.0 R3 КС3 исполнение 3-Base (далее — СКЗИ «КриптоПро CSP» версия 5.0 R3).

Ключевыми особенностями указанных исполнений новой версии СКЗИ «КриптоПро CSP» являются:

- поддержка протокола TLS версии 1.3 с использованием российских криптографических алгоритмов;
- возможность эксплуатировать СКЗИ без проведения исследований по оценке влияния с веб-серверами Apache Tomcat и Bellsoft Libercat, сервером терминалов и клиентом RDP, с браузерами Chromium ГОСТ (в ОС Windows, Linux и macOS) и Яндекс.Браузер (в ОС Linux и macOS);
- включение в состав СКЗИ инструментария разработчика КриптоПро PKI SDK (КриптоПро TSP SDK, КриптоПро OCSP SDK, КриптоПро ЭЦП SDK и КриптоПро ЭЦП Browser Plug-in);
- возможность использования СКЗИ в качестве клиентского компонента ПАКМ «КриптоПро HSM» версии 2.0 R3;
- расширение перечня вызовов, использование которых при разработке систем на основе СКЗИ возможно без дополнительных тематических исследований, – в него теперь входят функции интерфейса КриптоПро PKI SDK, значительное количество новых функций КриптоПро JavaTLS (в т.ч. дополнительных функций языка Java для установки клиентских TLS-соединений с односторонней и двусторонней аутентификацией), новые флаги для функций CryptoAPI, а также функции интерфейса CryptoAPI и модуля cpcurl для использования в ОС Android;
- реализация требований по криптографической защите информации по классу КС3 под управлением ОС Astra Linux SE версий 1.6 и 1.7, сертифицированных ФСБ России и ФСТЭК России, ОС Альт 8 СП, а также под управлением Windows 11 и Windows Server 2022;
- расширение списка поддерживаемых виртуальных сред (включая QEMU/KVM), Java-машин, операционных систем (включая ОС Аврора 4.0/4.1), платформ и ключевых носителей, аппаратно-программных модулей доверенной загрузки;
- возможность эксплуатировать СКЗИ по классу КС1 в среде под управлением средства контейнеризации Docker Engine и средств оркестрации контейнеров Kubernetes и OpenShift Container Platform.

В соответствии с указанной выпиской из заключения СКЗИ «КриптоПро CSP» версии 5.0 R3 (исполнения 1-Base, 2-Base, 3-Base) в составе согласно формулярам (ЖТЯИ.00101-03 30 01, ЖТЯИ.00102-03 30 01, ЖТЯИ.00103-03 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;
- EFS (только для версии 5.0 R3 КС3 (исполнение 3-Base))
- TLS;
- IPsec;
- SESPAKE;
- PKINIT,

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 R3 КС1 (исполнение 1-Base)), СКЗИ класса КС2 (версия 5.0 R3 КС2 (исполнение 2-Base)) и СКЗИ класса КС3 (версия 5.0 R3 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. СТ-Р» и «Требованиям по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» для СКЗИ по уровню $КС_Б$, а также «Требованиям к средствам электронной подписи», утверждённым приказом ФСБ России от 27.12.2011 г. №796, для средств ЭП классов КС1 (версия 5.0 R3 КС1 (исполнение 1-Base)), КС2 (версия 5.0 R3 КС2 (исполнение 2-Base)) и КС3 (версия 5.0 R3 КС3 (исполнение 3-Base)).

СКЗИ «КриптоПро CSP» версии 5.0 R3 разрешается эксплуатировать до 01 мая 2024 года.

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

Исп. Князева Е.Р. (495) 995-48-20, доб. 318