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

№ 11713 от 30.12.2020

Руководителям организаций

Информационное письмо

Настоящим сообщаем, что ООО «КРИПТО-ПРО» получило выписку из положительного заключения ФСБ России (№ 149/3/2/3-2981 от 23.12.2020) по итогам экспертизы результатов тематических исследований средства криптографической защиты информации «КриптоПро JCP» версии 2.0 R4 (исполнения 1, 2).

Ключевыми особенностями новой версии «КриптоПро JCP» являются поддержка работы под управлением виртуальных Java-машин Oracle «Java(TM) Runtime Environment, Standard Edition», «OpenJDK» и «Liberica» версий 12, 13 и 14 (в том числе поддержка работы в ОС семейства Windows для Java-машин «Liberica» и «OpenJDK»), расширение перечня вызовов, использование которых при разработке систем на основе «КриптоПро JCP» версия 2.0 R4 возможно без дополнительных тематических исследований, предоставляющее возможность установки TLS-соединения с односторонней аутентификацией, поддержка формата подписи CAdES-A, а также возможность эксплуатировать СКЗИ с веб-сервером в составе ПО Apache Tomcat версий 7.0, 8.5 и 9.0 без проведения исследований по оценке влияния (при соблюдении требований документации на СКЗИ).

В соответствии с указанной выпиской из заключения СКЗИ «КриптоПро JCP» версии 2.0 R4 (исполнения 1, 2) в составе согласно формуляру ЖТЯИ.00091-04 30 01 при выполнении операций:

- зашифрование/расшифрование, вычисление имитовставки (в соответствии с ГОСТ 28147-89) (только исполнение 2);
- создание/проверка ЭП (в соответствии с ГОСТ Р 34.10-2012);
- выработка значения хэш-функции (в соответствии с ГОСТ Р 34.11-2012);
- создание ключа ЭП/ключа проверки ЭП;
- идентификация, аутентификация, шифрование и имитозащита TLS-соединений (только исполнение 2),

реализуемых при помощи функций, приведенных в Приложении 2 документа «ЖТЯИ.00091-04 92 01. Правила пользования», удовлетворяет «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» для СКЗИ класса КС1, «Специальным требованиям к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации» для СКЗИ по уровню $КС_Б$ и «Требованиям к средствам электронной подписи», утверждённым приказом ФСБ России, для средств ЭП класса КС1.

СКЗИ «КриптоПро JCP» версия 2.0 R4 (исполнения 1, 2) разрешается эксплуатировать до 05 октября 2021 года.

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

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