35495

Зарегистрировано в реестре "30" января 2018 г. № RU00000 35495

М.П. (Подпись лица уполномоченного органа) А.В.ПАРФЕНОВ (Ф.И.О.)

# НОТИФИКАЦИЯ

## о характеристиках шифровальных (криптографических) средств и товаров, их содержащих

1. Наименование товара: Автоматизированная масштабируемая ленточная медиа-библиотека Quantum Scalar серии i6000, модели "LSC6K-" и "LSNDA-", вместе с встроенным программным обеспечением управления/контроля "control/management software/firmware" (или "Quantum iLayerTM software") версии i12, а также частями и компонентами.

   Модели "LSC6K-" и "LSNDA- имеют идентичные криптографические функции, при этом отличаются операционной функциональностью. Система состоит из следующих компонентов:

   1) контрольный модуль (control module);
   2) расширительные модули (expansion modules);
   3) парковочный модуль (parking module).

   А также запасные части к продукту.

2. Назначение товара: Продукт представляет собой автоматизированную ленточную медиа-библиотеку типа SCSI, которая управляет ленточными приводами (LTO tape drives) при считывании данных с изначальных носителей. Контроль за работой ленточной библиотеки осуществляется при помощи встроенного программного обеспечения контроля/управления "control/management software/firmware" (или "Quantum iLayerTM software") версии i12, использующего интегрированные программные модули общедоступных библиотек, включая модули Linux, библиотеки C-compiler libraries, криптографические протоколы OpenSSL и Java Runtime Environment (JRE 1.6). Различие в моделях "LSC6K-" и "LSNDA-" состоит в том, что модель LSC6K- имеет опциональную функцию авто-архивирования, в модели LSNDA- такая опция отсутствует (при этом, указанное отличие не влияет на шифровальные (криптографические) функции продукта).

   Магнитно-ленточные накопители/приводы для продукта производятся компаниями International Business Machines (IBM) и Hewlett Packard (HP) и поставляются отдельно. В частности, могут использоваться ленточные приводы IBM (установленным порядком зарегистрированная нотификация № RU0000003175, срок действия до 31.12.2020, модели: 3592-EXX IBM; 3588-F4A IBM System Storage TS1040; 3588-F5A IBM System Storage TS1050).

   Криптографические функции продукта выполняются на уровне встроенного программного обеспечения управления библиотекой / "control/management software/firmware" (или "Quantum iLayerTM software") версии i12 в программных пользовательских интерфейсах libcrypt (libc), Java Runtime Environment, SNMP и SMI-S-мониторинга, реализуются в протоколах Secure Socket Layer (SSL), Transport Layer Security (TLS) and Public Key Cryptography Standards (PKCS), и используются исключительно для выполнения (а) аутентификации в виде защиты пароля и (б) использования электронной цифровой подписи (ЭЦП), а также (в) защиты каналов связи для удаленного администрирования (шифрование траффика данных, а также каких-либо иных криптографических функций продукт не выполняет).

3. Сведения об изготовителе товара: Квантум Корпорейшн, 227 Эйрпорт Паркуэй, Сьют 300, Сан Хосе, Калифорния 95110, США, номер компании (ID): 94-2665504, тел. +1 408-944-4000, электронная почта: Shawn.Hall@quantum.com, официальный сайт в Интернет: http://www.quantum.com [Quantum Corporation, 227 Airport Parkway, Suite 550, San Jose, California USA 95110. ID: 94-2665504, Shawn Hall, Vice President and General Counsel. tel. +1 408-944-4000, email: Shawn.Hall@quantum.com or Mary.Vigil@Quantum.com].

4. Используемые криптографические алгоритмы (функции) и их назначение: — № категории товара из приложения № 4

   Криптографические функции встроенного программного обеспечения управления/контроля "control/management software/firmware" (или "Quantum iLayerTM software") версии i12

4.1) Криптографические функции симметричных алгоритмов, реализуемых в протоколах SSL, TLS, PKCS (выполняемые функции: аутентификация в виде защиты пароля и ЭП/ЭЦП, а также защита технологического канала удаленного администрирования): 2.1, 2.2, 10

а. AES, максимальная длина ключа 256 бит,
б. Blowfish, максимальная длина ключа 256 бит
в. SEED, максимальная длина ключа 128 бит
г. CAMELLIA, максимальная длина ключа 256 бит
д. DES, максимальная длина ключа 56 бит
е. 3DES (Triple DES), максимальная длина ключа 168 бит
ж. RC2 и RC4, максимальная длина ключа 56 бит

4.2) Криптографические функции асимметричных алгоритмов, реализуемых в протоколах SSL, TLS, PKCS (выполняемые функции: аутентификация в виде защиты пароля и ЭП/ЭЦП, а также защита технологического канала удаленного администрирования): 2.1, 2.2, 10

а. RSA, максимальная длина ключа 4096 бит
б. DSA, максимальная длина ключа 1024 бит
в. Diffie Hellman, максимальная длина ключа 4096 бит

4.3) Хэш-функции, используемые в протоколах SSL, TLS, PKCS (выполняемые функции: аутентификация в виде защиты пароля и ЭП/ЭЦП): 2.1, 2.2

а. SHA1, длина ключа (размер хэша) 160 бит
б. SHA_256, длина ключа (размер хэша) 256 бит
в. SHA_384, длина ключа (размер хэша) 384 бит
г. SHA_512, длина ключа (размер хэша) 512 бит
д. MD2, MD5, длина ключа (размер хэша) 128 бит

5. Наличие у товара (продукции) функциональных возможностей, не описанных в предоставляемой пользователю эксплуатационной документации: нет.

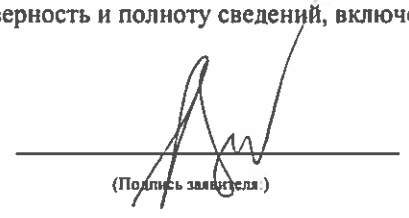
6. Срок действия нотификации: 31.12.2020.

7. Сведения о заявителе: Александр Андреевич Бычков, гражданин РФ, проживающий по адресу: гор. Москва, ул. Короленко д. 8, кв. 73, паспорт № 4513 223714 выдан 13.12.2013 Отделением УФМС России по гор. Москве, код подразделения 770-060, тел +7 (495) 787-27-00.

8. Сведения о документе изготовителя, удостоверившего полномочия лица на оформление нотификации (при необходимости): Доверенность от 30 ноября 2016 г. (без номера), выданная компанией Квантум Корпорейшн, 227 Эйрпорт Паркуэй, Сьют 300, Сан Хосе, Калифорния 95110, США, в лице ее первого вице-президента, главного юридического советника и секретаря Шона Д. Холла, гражданину РФ Александру Андреевичу Бычкову, паспорт № 4513 223714 выдан 13.12.2013 Отделением УФМС России по гор. Москве, код подразделения 770-060, тел +7 (495) 787-27-00.

9. Дата заполнения нотификации: 23.01.2018.

Достоверность и полноту сведений, включенных в нотификацию, подтверждаю:



(Подпись заявителя)

(Александр Андреевич Бычков)

(Ф.И.О.)