



Прайс-лист на ключи безопасности YubiKey 5, YubiKey FIPS и YubiHSM2 от 11 Сентября 2019г.

	YubiKey 5 NFC	YubiKey 5 Nano	YubiKey 5C	YubiKey 5C Nano	YubiKey 5 Ci	Security Key	Security Key NFC
<b>Без упаковки</b>							
<b>Цена</b>	₽ 5 299,00	₽ 5 799,00	₽ 5 799,00	₽ 6 799,00	₽ 8 199,00	₽ 2 499,00	₽ 3 099,00
<b>Индивидуальная упаковка</b>							
<b>Цена</b>	₽ 5 399,00	₽ 5 899,00	₽ 5 899,00	₽ 6 899,00	₽ 8 299,00	₽ 2 599,00	₽ 3 199,00
<b>Описание</b>	USB-ключ аутентификации, криптостойкий, поддерживает стандарты FIDO2 и U2F, беспарольный вход, одноразовые пароли OTP, статические пароли, режим смарт-карты PIV, OATH-HOTP, OATH-TOTP, Challenge-Response, OpenPGP.  Поддержка NFC у модели YubiKey 5 NFC.					USB-Ключ аутентификации, который работает с любым онлайн-сервисом с поддержкой FIDO2 или U2F.	USB/NFC-ключ аутентификации, который работает с любым онлайн-сервисом с поддержкой FIDO2 или U2F.
<b>Размер и вес</b>	18 x 45 x 3.3мм, 3г.	12 x 13 x 3.1мм, 1г.	12.5 x 29.5 x 5мм, 2г.	12 x 10.1 x 7, 1г.	12 x 40.3 x 5мм, 2.9г.	18 x 45 x 3.3мм, 3г.	18 x 45 x 3.3мм, 3г.
<b>Сертификация</b>							
Сертификация FIDO Certification™	Y	Y	Y	Y	Y	Y	Y
Сертификация FIPS 140							
<b>Поддерживаемые подключения</b>							
USB-A 	Y	Y				Y	Y
USB-C 			Y	Y	Y		
Lightning 					Y		
NFC (Связь на малых расстояниях)	Y						Y
<b>Тип устройства</b>							
Клавиатура HID	Y	Y	Y	Y	Y		
Смарт-карта CCID	Y	Y	Y	Y	Y		
Устройство FIDO HID	Y	Y	Y	Y	Y	Y	Y
<b>Спецификации криптографии</b>							
RSA 2048	Y	Y	Y	Y	Y		
RSA 4096 (PGP)	Y	Y	Y	Y	Y		
ECC p256	**	**	**	**	**	**	**
ECC p384	***	***	***	***	***		







\*\* ECC применяется только к апплету смарт карты; не применяется к апплету OpenPGP. Типом ключа, генерируемого для ключевой пары U2F, является ECC p256.

\*\*\* ECC применяется только к апплету смарт карты; не применяется к апплету OpenPGP.

OATH-TOTP требует дополнительное приложение — [Yubico Authenticator](#); Для ключей типа YubiKey 5 NFC, сертификация FIDO применяется для обоих видов подключения — USB и NFC.



## Прайс-лист на сертифицированные ключи безопасности YubiKey FIPS от 01 Января 2019г.

	YubiKey FIPS	YubiKey Nano FIPS	YubiKey C FIPS	YubiKey C Nano FIPS
<b>Модели</b>				
<b>Цена</b>	₽ 5 599,00	₽ 6 899.00	₽ 6 899.00	₽ 8 299.00
<b>Описание</b>	FIPS 140-2 сертифицированный USB-ключ аутентификации, криптостойкий, поддерживает стандарты FIDO2 и U2F, беспарольный вход, одноразовые пароли OTP, статические пароли, режим смарт-карты PIV, OATH-HOTP, OATH-TOTP, Challenge-Response, OpenPGP.			
<b>Размер и вес</b>	18 x 45 x 3.3мм, 3г	12 x 13 x 3.1мм, 1г	12.5 x 29.5 x 5мм, 2г	12 x 10.1 x 7, 1г
<b>Сертификация</b>				
Сертификация FIDO Certification™	Y	Y	Y	Y
Сертификация FIPS 140	Y	Y	Y	Y
<b>Поддерживаемые подключения</b>				
USB-A 	Y	Y		
USB-C 			Y	Y
NFC (Связь на малых расстояниях)				
<b>Тип устройства</b>				
Клавиатура HID	Y	Y	Y	Y
Смарт-карта CCID	Y	Y	Y	Y
Устройство FIDO HID	Y	Y	Y	Y
<b>Спецификации криптографии</b>				
RSA 2048	Y	Y	Y	Y
RSA 4096 (PGP)	Y	Y	Y	Y
ECC p256	**	**	**	**
ECC p384	***	***	***	***

\*\* ECC применяется только к апплету смарт карты; не применяется к апплету OpenPGP. Типом ключа, генерируемого для ключевой пары U2F, является ECC p256.


\*\*\* ECC применяется только к апплету смарт карты; не применяется к апплету OpenPGP.



NIST | Национальный Институт Стандартов и Технологий (США)  
Сертификация криптографических модулей YubiKey



## Аппаратный модуль безопасности YubiHSM 2 для защиты криптографических ключей на серверах

YubiHSM 2	
Модель	
Цена	₽ 74 999.00
Размер и вес	12 мм x 13 мм x 3.1 мм, 1 грамм
Поддержка ОС	
Версия	<b>Linux</b> CentOS 6, CentOS 7, Debian 8, Debian 9, Fedora 25, Ubuntu 1404, Ubuntu 1604
	<b>MS Windows</b> Windows 10, Windows Server 2012, Windows Server 2016
	<b>Mac OS</b> 10.12 Sierra, 10.13 High Sierra
Архитектура	amd64
Криптографические возможности	
Хеширование	Применяется с HMAC и асимметричными подписями <ul style="list-style-type: none"> <li>SHA-1, SHA-256, SHA-384, SHA-512</li> </ul>
RSA	<ul style="list-style-type: none"> <li>2048, 3072, и 4096-битные ключи</li> <li>Подпись с помощью PKCS#1v1.5 и PSS</li> <li>Дешифрация PKCS#1v1.5 и OAEP</li> </ul>
Эллиптическая криптография (ECC)	<ul style="list-style-type: none"> <li>Кривые: secp224r1, secp256r1, secp256k1, secp384r1, secp521r1, bp256r1, bp384r1, bp512r1, curve25519</li> <li>Подпись: ECDSA (все кроме curve25519), EdDSA (только curve25519)</li> <li>Дешифрация: ECDH (все кроме curve25519)</li> </ul>
Упаковка ключей	Импорт и экспорт при помощи NIST AES-CCM Wrap при 128, 196, и 256 битах
Случайные числа	Встроенный в чип генератор реальных случайных чисел (TRNG) с зерном NIST SP 800-90 AES 256 CTR_DRBG
Аттестация	Сгенерированные на устройстве асимметричные ключевые пары могут проходить проверку при помощи заводского сертифицированного ключа аттестации и сертификата, или при помощи Вашего личного ключа, импортированного в модуль безопасности
Быстродействие	Быстродействие зависит от целевого применения. В примере приведена метрика YubiHSM2, незадействованного в других процессах: <ul style="list-style-type: none"> <li>RSA-2048-PKCS1-SHA256: ~139ms сред.</li> <li>RSA-3072-PKCS1-SHA384: ~504ms сред.</li> <li>RSA-4096-PKCS1-SHA512: ~852ms сред.</li> <li>ECDSA-P256-SHA256: ~73ms сред.</li> <li>ECDSA-P384-SHA384: ~120ms сред.</li> <li>ECDSA-P521-SHA512: ~210ms сред.</li> <li>EdDSA-25519-32 Байт: ~105ms сред.</li> <li>EdDSA-25519-64 Байт: ~121ms сред.</li> <li>EdDSA-25519-128 Байт: ~137ms сред.</li> <li>EdDSA-25519-256 Байт: ~168ms сред.</li> <li>EdDSA-25519-512 Байт: ~229ms сред.</li> <li>EdDSA-25519-1024 Байт: ~353ms сред.</li> <li>AES-(128 192 256)-CCM-Wrap: ~10ms сред.</li> <li>HMAC-SHA-(1 256): ~4ms сред.</li> <li>HMAC-SHA-(384 512): ~243ms сред.</li> </ul>
Хост-интерфейс	(USB) 1.x Full Speed (12Mbit/s) периферийный интерфейс.
Физические характеристики	<ul style="list-style-type: none"> <li>Форм-фактор: 'nano', разработанный для малогабаритных мест установки, таких как внутренние USB порты серверов</li> <li>Потребление тока 20 мА сред., 30 мА макс.</li> <li>USB-A штекер</li> </ul>
Обеспечение соблюдения экологических норм	<ul style="list-style-type: none"> <li>FCC</li> <li>CE</li> <li>WEEE</li> <li>ROHS</li> </ul>