



## Прайс-лист на стандартные ключи безопасности YubiKey 5, YubiKey FIPS и YubiHSM2 от Сентября 2020г.

	YubiKey 5 NFC	YubiKey 5C NFC	YubiKey 5 Nano	YubiKey 5C	YubiKey 5C Nano	YubiKey 5 CI	Security Key	Security Key NFC
В оптовой упаковке (по 50шт)								
Индивидуальная упаковка								
Цена	грн 1800,00	грн 2100,00	грн 1950,00	грн 1950,00	грн 2300,00	грн 2700,00	грн 1000,00	грн 1200,00
Описание	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, 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.
Размер и вес	18 x 45 x 3.3мм, 3г.	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.
Сертификация								
Сертификация FIDO certification™	Y	Y	Y	Y	Y	Y	Y	Y
Сертификация FIPS 140								
Поддерживаемые подключения								
USB-A	Y		Y				Y	Y
USB-C		Y		Y	Y	Y		
Lightning						Y		
NFC (Связь на малых расстояниях)	Y	Y						Y
Тип устройства								
Клавиатура HID	Y	Y	Y	Y	Y	Y		
Смарт-карта CCID	Y	Y	Y	Y	Y	Y		
Устройство FIDO HID	Y	Y	Y	Y	Y	Y	Y	Y
Спецификации криптографии								
RSA 2048	Y	Y	Y	Y	Y	Y		
RSA 4096 (PGP)	Y	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 Сентября 2020г.

	YubiKey FIPS	YubiKey Nano FIPS	YubiKey C FIPS	YubiKey C Nano FIPS
Модели				
Цена	грн 1900,00	грн 2200,00	грн 2200,00	грн 2650,00
Описание	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.			
Размер и вес	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
Сертификация				
Сертификация FIDO Certification™	Y	Y	Y	Y
Сертификация FIPS 140	Y	Y	Y	Y
Поддерживаемые подключения				
USB-A 	Y	Y		
USB-C 			Y	Y
NFC (Связь на малых расстояниях)				
Тип устройства				
Клавиатура HID	Y	Y	Y	Y
Смарт-карта CCID	Y	Y	Y	Y
Устройство FIDO HID	Y	Y	Y	Y
Спецификации криптографии				
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	грн 25000.00
Размер и вес	12 мм x 13 мм x 3.1 мм, 1 грамм
Поддержка ОС	
Версия	Linux CentOS 6, CentOS 7, Debian 8, Debian 9, Fedora 25, Ubuntu 1404, Ubuntu 1604 MS Windows Windows 10, Windows Server 2012, Windows Server 2016 Mac OS 10.12 Sierra, 10.13 High Sierra
Архитектура	amd64
Криптографические возможности	
Хеширование	Применяется с HMAC и асимметричными подписями <input type="checkbox"/> SHA-1, SHA-256, SHA-384, SHA-512
RSA	<input type="checkbox"/> 2048, 3072, и 4096-битные ключи <input type="checkbox"/> Подпись с помощью PKCS#1v1.5 и PSS <input type="checkbox"/> Дешифрация PKCS#1v1.5 и OAEP
Эллиптическая криптография (ECC)	<input type="checkbox"/> Кривые: secp224r1, secp256r1, secp256k1, secp384r1, secp521r, bp256r1, bp384r1, bp512r1, curve25519 <input type="checkbox"/> Подпись: ECDSA (все кроме curve25519), EdDSA (только curve25519) <input type="checkbox"/> Дешифрация: ECDH (все кроме curve25519)
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 асимметрические 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: <input type="checkbox"/> RSA-2048-PKCS1-SHA256: ~139ms сред. <input type="checkbox"/> RSA-3072-PKCS1-SHA384: ~504ms сред. <input type="checkbox"/> RSA-4096-PKCS1-SHA512: ~852ms сред. <input type="checkbox"/> ECDSA-P256-SHA256: ~73ms сред. <input type="checkbox"/> ECDSA-P384-SHA384: ~120ms сред. <input type="checkbox"/> ECDSA-P521-SHA512: ~210ms сред. <input type="checkbox"/> EdDSA-25519-32 Байт: ~105ms сред. <input type="checkbox"/> EdDSA-25519-64 Байт: ~121ms сред. <input type="checkbox"/> EdDSA-25519-128 Байт: ~137ms сред. <input type="checkbox"/> EdDSA-25519-256 Байт: ~168ms сред. <input type="checkbox"/> EdDSA-25519-512 Байт: ~229ms сред. <input type="checkbox"/> EdDSA-25519-1024 Байт: ~353ms сред. <input type="checkbox"/> AES-(128 192 256)-CCM-Wrap: ~10ms сред. <input type="checkbox"/> HMAC-SHA-(1 256): ~4ms сред. <input type="checkbox"/> HMAC-SHA-(384 512): ~243ms сред.
Хост-интерфейс	(USB) 1.x Full Speed (12Mbit/s) периферийный интерфейс.
Физические характеристики	<input type="checkbox"/> Форм-фактор: 'nano', разработанный для малогабаритных мест установки, таких как внутренние USB порты серверов <input type="checkbox"/> Потребление тока 20 мА сред., 30 мА макс. <input type="checkbox"/> USB-A штекер
Обеспечение соблюдения экологических норм	<input type="checkbox"/> FCC <input type="checkbox"/> CE <input type="checkbox"/> WEEE <input type="checkbox"/> ROHS