

# YubiKey 5 NFC

## Технічні характеристики

### 5-те покоління ключів безпеки для надійної автентифікації

YubiKey 5 — це серія компактних USB ключів безпеки для мультифакторної автентифікації. Відтепер з підтримкою FIDO2 безпарольної автентифікації та USB + NFC моделлю — YubiKey 5 NFC. Мультифакторна автентифікація в поєднанні з апаратними рішеннями дозволяє підвищити захист облікових записів до найвищого рівня. Відомо, що одноразові СМС паролі вразливі до зламу та не в змозі забезпечити належний рівень захищеності. Уникнути неприємнощів, пов'язаних з хакерськими атаками та клонуванням SIM карт, можна використовуючи апаратний ключ безпеки, для захисту доступу до облікових записів додатків та онлайн сервісів. Ці USB ключі готові до роботи з ОС Windows, Linux та macOS, а також з популярними браузерями, додатками та вебсайтами. П'яте покоління YubiKey поєднує у собі підтримку багатьох алгоритмів шифрування з простотою використання — безпечний вхід до облікових записів лиш одним дотиком до кнопки.



# Технічні характеристики

## Інтерфейс

<b>USB</b>	USB 2.0 типу А (Сумісний з USB 3.0)
<b>NFC</b>	Дальність дії не більш ніж 10 см. Зворотна сумісність з MIFARE

## Режими роботи

<b>FIDO2</b>	<p>Режим FIDO2 дозволяє зберігати облікові дані для подальшого безпарольного входу до облікових записів на сайтах та пристроях.</p> <p>Режим USB: FIDO</p>
<b>Одноразовий пароль OTP</b>	<p>OTP аплет містить два програмованих слоти, кожен може вміщувати один з наступних типів облікових даних:</p> <ul style="list-style-type: none"><li>• Одноразовий пароль Yubico</li><li>• HMAC-SHA1 Виклик-Відповідь</li><li>• Статичний пароль</li><li>• OATH-HOTP</li></ul> <p>Режим USB: OTP</p>
<b>Універсальна двофакторна автентифікація U2F</b>	<p>Режим U2F дозволяє зберігати необмежену кількість облікових даних та є FIDO-сертифікованим.</p> <p>Режим USB: FIDO</p>
<b>OATH</b>	<p>Цей режим дозволяє зберігати до 32-х записів облікових даних OATH і підтримує як OATH-TOTP (фактор часу), так і OATH-HOTP (фактор лічильника). Для доступу до даного аплету потрібен Yubico Authenticator.</p> <p>Режим USB: CCID</p>
<b>PIV-сумісна смарт-карта</b>	<p>Режим смарт-карти PIV (посвідчення особистості). Значення за замовчуванням:</p> <ul style="list-style-type: none"><li>• PIN: 123456</li><li>• PUK: 12345678</li><li>• Ключ керування: 10203040506070801020304050607080102030405060708</li></ul> <p>Підтримувані алгоритми:</p> <ul style="list-style-type: none"><li>• RSA 1024</li><li>• RSA 2048</li><li>• ECC P256</li><li>• ECC P384</li></ul> <p>Слоти інформації:</p> <ul style="list-style-type: none"><li>• Slot 9a: Автентифікація</li><li>• Slot 9b: Ключ керування</li><li>• Slot 9c: Цифровий підпис</li><li>• Slot 9d: Керування ключами</li><li>• Slot 9e: Автентифікація карти</li><li>• Slot f9: Атестація</li><li>• Слоти 82-95: Керування незадіяними ключами</li></ul> <p>Режим USB: CCID</p>

<b>OpenPGP</b>	<p>Цей режим відповідає специфікаціям смарт-карт OpenPGP версії 2.0, яка може застосовуватись з GnuPG. Для ключів довжиною більш ніж 2048 біт потрібно GnuPG версії 2.0 або вище.</p> <p>Підтримувані алгоритми:</p> <ul style="list-style-type: none"> <li>• RSA 1024</li> <li>• RSA 2048</li> <li>• RSA 3072</li> <li>• RSA 4096</li> </ul> <p>Режим USB: CCID</p>
----------------	--

#### Загальні характеристики

Інтерфейс	USB-A
Габаритні розміри (Ш*Д*В)	18мм x 45мм x 3.3мм
Вага	3 г

#### Температурні характеристики

Робочий режим	Від 0 °С до 40 °С
Зберігання	Від -20 °С до 85 °С

#### Криптографічні характеристики (протоколи та алгоритми)

RSA 1024	Макс. довжина ключа: 1024 біт
RSA 2048	Макс. довжина ключа: 2048 біт
RSA 3072	Макс. довжина ключа: 3072 біт
RSA 4096	Макс. довжина ключа: 4096 біт
ECC p256	Макс. довжина ключа: 256 біт
ECC p384	Макс. довжина ключа: 384 біт
SHA1	Макс. довжина ключа: 160 біт

## Виникли питання?

### Об'єднані Арабські Емірати – Головний офіс

Dubai Airport Free Zone 6EA, #209. Dubai – UAE

Tel. +971 (04) 7017 260

Email: [info@thekernel.com](mailto:info@thekernel.com)