

# Апаратні зашифровані диски Kingston IronKey – рішення у сфері безпеки

## Керуйте загрозами, які пов'язані з мобільними даними, і знижуйте ризики



Вашій компанії ризикує щоразу, коли співробітники використовують свої власні накопичувачі для перенесення даних чи роботи вдома. Захистіть конфіденційні дані, стандартизуючи на апаратно зашифрованій USB-флешці Kingston® IronKey™ або зовнішньому SSD. Серед кількох варіантів ви знайдете той, який ідеально підійде для потреб вашої компанії, незалежно від того, чи потрібно вам гарантувати безпеку мобільних даних або слідувати вимогам директив, законів, стандартів або міжнародних нормативних актів (GDPR або CCPA), які стосуються зберігання та переносу даних.

На всі накопичувачі IronKey поширюється п'ятирічна гарантія (на IronKey Keypad 200 та IronKey Vault Privacy 80 ES — трирічна гарантія), безкоштовна технічна підтримка та легендарна надійність Kingston. Усі перелічені нижче накопичувачі повністю шифровані відповідно до найстрогіших стандартів безпеки. Докладні відомості див. на сторінці [kingston.com/encryptedsecurity](http://kingston.com/encryptedsecurity)



Опис	IronKey Vault Privacy 50	IronKey Vault Privacy 80 ES	IronKey Keypad 200	DataTraveler 4000G2	IronKey D300S	IronKey S1000
Артикул	IKVP50/xxxGB USB-A IKVP50C/xxxGB USB-C <sup>1</sup>	IKVP80ES/xxGB	IKKP200/xxGB	DT4000G2DM/xxGB Optionally Managed	IKD300S/xxGB Standard IKD300SM/xxGB Managed	IKS1000B/xxGB Basic IKS1000E/xxGB Enterprise
Рівень безпеки	Основний вибір серед підприємств	Small/Medium Business Mainstream	Military Grade	Military Grade	Military Grade/Enhanced	Military Grade/Best-in-Class
Ємність <sup>2</sup>	8–256 ГБ	480–1920 ГБ	8–128 ГБ	8–128 ГБ	8–128 ГБ	4–128 ГБ
Апаратне шифрування 256-bit AES в режимі	XTS	XTS	XTS	XTS	XTS	On Device Cryptochip + XTS
Відповідність вимогам стандарту FIPS <sup>3</sup>	FIPS 197	FIPS 197	FIPS 140-3 рівень 3 (в очікуванні)	Стандарт FIPS 140-2 Level 3	Стандарт FIPS 140-2 Level 3	Стандарт FIPS 140-2 Level 3
Підтримка кількох паролів	Адміністратор / користувач / одноразовий для відновлення	Адміністратор / користувач	Адміністратор / користувач			
Режим паролльної фрази та максимальна довжина	√ До 64 символів	√ До 64 символів	√ До 15 символів			√ До 255 символів
Значок ока для відображення пароля	√	√				
Вбудоване ПЗ з цифровим підписом	√	√	√	√	√	√
Захист від шкідливого ПЗ BadUSB	√	√	√	√	√	√
Захист від зламу шляхом перебирання паролів	√	√	√	√	√	√
Відповідність вимогам ТАА	√	√	√	√	√	√
Відповідність вимогам GDPR <sup>9</sup>	√	√	√	√	√	√
Доступ лише для читання	√	√	√	√	√	√
Захист від фізичного втручання		Захищений мікропроцесор із сертифікацією CC EAL5+	√ Епоксидна смола	√ Епоксидна смола	√ Заповнено епоксидною смолою	√ Заповнено епоксидною смолою
Водонепроникність <sup>4</sup>	до 1,2 м		до 0,9 м	до 1,2 м	до 1,2 м	до 0,9 м
Можливість кастомізації <sup>5</sup>	√			√	√	
Віртуальна клавіатура	Windows® і macOS®	Сенсорний екран			Лише для Windows®	Лише для Windows®
Можливість корпоративного адміністрування	Можливість місцевого адміністрування для малого/середнього бізнесу			Можливість додаткового адміністрування (SafeConsole)	√ D300SM (SafeConsole)	√ S1000E (SafeConsole)
Користувачке значення PID – сумісність із кінцевими точками / DLP	√			√	√	
Матеріал корпусу	Анодований алюміній	Цинк і пластик	Анодований алюміній	Неіржавна сталь із титановим покриттям	Цинк	Анодований алюміній
USB-інтерфейс	USB 3.2 Gen 1	Зовнішній твердотільний накопичувач USB 3.2 Gen 1	USB 3.2 Gen 1	USB 3.1 Gen 1	USB 3.1 Gen 1	USB 3.1 Gen 1
Операційні системи, що підтримуються						
Windows® 11, 10	√	√ Незалежність від ОС	√ Незалежність від ОС	√	√	√
macOS® 10.15x - 13.x	√	√ Незалежність від ОС	√ Незалежність від ОС	√	√	√ <sup>10</sup>
Ядро Linux® версії 4.4+		√ Незалежність від ОС	√ Незалежність від ОС		√ <sup>8</sup>	√ <sup>8</sup>

1 USB Type-C® та USB-C® є зареєстрованими торговими марками USB Implementers Forum.  
 2 Частина зазначеного обсягу флешпам'яті використовується для форматування та інших функцій, і тому є недоступною для зберігання даних. Для отримання додаткової інформації дивіться посібник із використання пам'яті на сайті [kingston.com/flashguide](http://kingston.com/flashguide).  
 3 Федеральні стандарти обробки інформації (FIPS), публікація 140-2: «Вимоги безпеки для криптографічних модулів». Для отримання додаткової інформації відвідайте сайт <http://csrc.nist.gov/publications/PubsFIPS.html>.  
 4 S1000 відповідає вимогам MIL-STD-810F, IKKP200 відповідає вимогам IP57, усі інші сумісні накопичувачі відповідають вимогам IEC 60529 IPX8. Пристрій повинен використовуватись у чистому та сухому вигляді.

5 Для отримання додаткової інформації відвідайте сайт [kingston.com/encryptedsecurity](http://kingston.com/encryptedsecurity).  
 6 Команди Linux підтримують лише процесори i386/x86\_64 Intel і AMD — обмежені можливості.  
 7 IKD300S: підтримка 32-бітної та 64-бітної ОС Linux. Обмежені можливості, для отримання додаткової інформації відвідайте сайт [kingston.com/encryptedsecurity](http://kingston.com/encryptedsecurity).  
 8 IKD300SM і IKS1000B: підтримка 32-бітної та 64-бітної ОС Linux / IKS1000E: підтримка 32-бітної ОС Linux. Обмежені можливості.  
 9 Шифрування може бути частиною програми дотримання вимог GDPR, але не забезпечувати таке дотримання.  
 10 підтримка macOS® 13.x в 1Q-2023.

