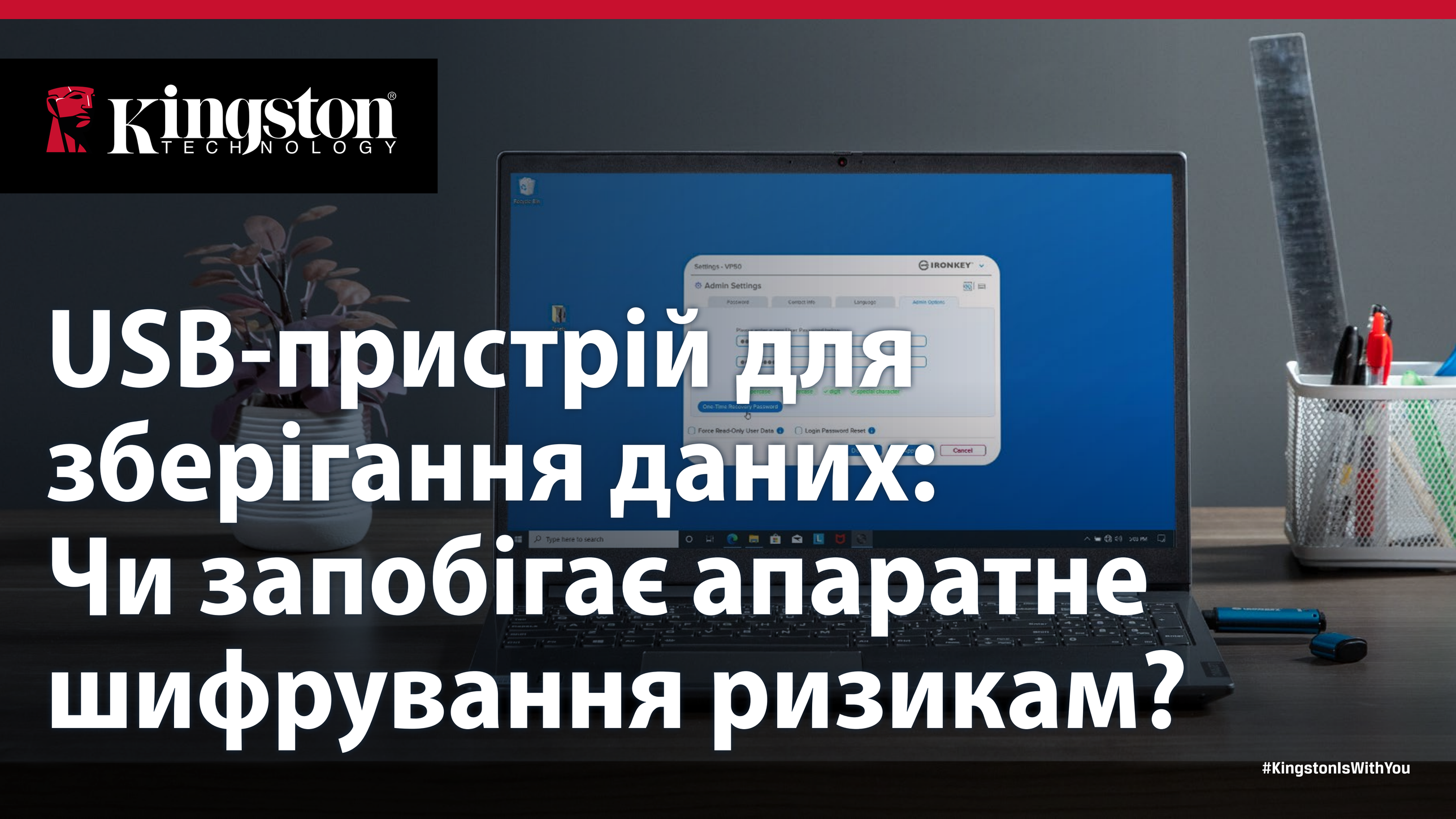



# USB-пристрій для зберігання даних: Чи запобігає апаратне шифрування ризикам?

#KingstonIsWithYou

# USB-пристрій для зберігання даних: Чи запобігає апаратне шифрування ризикам?

## Вступ і зміст

Бізнес занепокоєний питанням кібербезпеки як ніколи, але багато організацій мають недостатній рівень обізнаності та підготовки до кіберзагроз. За даними UpCity, лише 50% підприємств у США мають план кібербезпеки; із них 32% не оновлювали свої плани кібербезпеки з початку пандемії COVID-19, через що багато організацій перейшли на віддалені або гібридні моделі роботи. Частота та рівень кібератак лише зростають — у всьому світі число підприємств, що постраждали від програм-вимагачів, збільшилося з 37% у 2020 році до 66% у 2021 році[1].

Порушення захисту даних у кіберпросторі може мати руйнівні наслідки для бізнесу — окрім грошових витрат на запобігання кібератакам, втрата даних, безпекові або репутаційні ризики можуть негативно вплинути на діяльність організації як в короткостроковій, так і в довгостроковій перспективі.

Найбільшу загрозу для кібербезпеки становлять USB-накопичувачі. Багато організацій почали активно використовувати ці пристрої завдяки їх простоті — достатньо під'єднати їх до комп'ютера, і вони готові до роботи. Проте саме ця простота зробила USB-накопичувачі уразливими до атак: якщо зловмисник знайде втрачений накопичувач або вкраде його, він зможе отримати доступ до потенційно важливих даних. Саме шифрування відіграє важливу роль у захисті USB-накопичувачів, зменшуючи будь-які супутні ризики для користувача та організації. У цій електронній книзі ми постараємося знайти відповіді на такі ключові питання:

- Чому шифровані USB-накопичувачі настільки важливі для захисту від кібератак?
- Які найуразливіші місця для кібернападу в організаціях?
- Що вони можуть зробити, щоб захистити себе?



# USB-пристрій для зберігання даних: Чи запобігає апаратне шифрування ризикам?

## Автори

Ця електронна книга була створена за участі провідних фахівців у сфері IT та інноваційних технологій, а також нашого власного технічного експерта.

### Девід Кларк

Девід входить до топ-десятки інфлюенсерів за рейтингом Thompson Reuter «Топ-30 найвпливовіших лідерів і мислителів у соцмережах у сфері керування ризиками, комплаєнсу та регуляторних технологій у Великій Британії», а також до топ-50 глобальних експертів Kingston Technology.

### Пасі Сіуконен

Пасі керує експертною групою, яка займаються підтримкою таких відділів компанії Kingston, як зв'язки з громадськістю, маркетинг, місцевий збут, технічна підтримка та обслуговування клієнтів Kingston. Він спеціалізується переважно на флеш-пам'яті та твердотільних накопичувачах.

# Різниця між типовими та шифрованими накопичувачами

Хоча типові (нешифровані) накопичувачі надзвичайно прості у використанні та забезпечують швидкий доступ до даних, апаратне шифрування додає декілька рівнів безпеки (фізичних і цифрових), що робить USB-накопичувачі набагато безпечнішими. Доступність, низька вартість і портативність типових нешифрованих накопичувачів означає, що вони зручні не лише для користувачів, але й для зловмисників, які намагаються вкрасти конфіденційні дані, застосовуючи в мережі компанії зловмисні програми або програми-вимагачі. Часте використання USB-накопичувачів призводить до збільшення кількості потенційних кібератак. Із типовими накопичувачами пов'язані два основні ризики:

- **Атаки програм-вимагачів.** ці атаки, пов'язані з використанням USB-накопичувачів, передбачають проникнення зловмисної програми в мережі компаній, блокування інформації про компанію та/або комп'ютерних систем шляхом їх шифрування з метою отримання викупу. Це найвідоміший тип зловмисної програми, який використовує метод атак BadUSB.
- **Вкрадені дані.** якщо нешифрований накопичувач буде втрачено, вкрадено або залишено без нагляду, зловмисник може легко отримати доступ до будь-яких даних, що зберігаються на ньому, зокрема до інформації про клієнтів, програмного коду, важливих фінансових і виробничих даних.

BadUSB — це атака, яка може використовувати вразливість USB-накопичувачів із незахищеною прошивкою для подальшого перепрограмування зловмисною програмою. Подібні зловмисні інструменти найчастіше використовуються кіберзлочинцями, проте обізнаність про ці інструменти залишається на низькому рівні, через що вони легко підміняють прошивку типового накопичувача, маскуючи USB-накопичувач під клавіатуру та запускаючи сценарії для здійснення атак на брандмауер. Оскільки більшість кібератак здійснюється штатними співробітниками свідомо або без злого наміру, вкрай важливо, щоб підприємства використовували шифровані накопичувачі, оснащені прошивкою з цифровим підписом, для ефективної протидії таким атакам кіберзлочинців.

> **Вартість робіт з відновлення інфраструктури й можливі витрати, пов'язані з викупом або здирством, набагато перевищують вартість USB-накопичувачів.**
> **- Девід Кларк**

# Навіщо використовувати USB-накопичувачі?

Шифровані накопичувачі спеціально розроблено для захисту даних, які зберігаються на них, а також будь-яких пристроїв, до яких вони приєднуються, що робить їх безцінним інструментом в арсеналі IT-фахівця будь-якої організації. Загрози в кіберпросторі стають дедалі досконалішими, проте шифровані накопичувачі також вдосконалюються, випереджаючи кіберзлочинців на крок у боротьбі за безпеку даних. Наприклад, лінійка пристроїв Kingston IronKey™ з апаратним шифруванням використовує шифрування AES 256-bit у найнадійнішому режимі XTS, міцний корпус із захистом від несанкціонованого доступу, прошивку з цифровим підписом, віртуальні клавіатури, режими «Складний пароль» і «Парольна фраза» та багато інших функцій, які розроблялись і додавались протягом багатьох років, гарантуючи користувачеві справжній захист від будь-яких видів атак.

Оскільки загрозам в кіберпросторі не завжди приділяється достатньо уваги, багато підприємств вибирають типові накопичувачі, незважаючи на різні вразливості, які вони несуть у собі. На перший план виходить доступність, низька вартість і зручність використання програмного шифрування, а також відсутність процесу корпоративного допуску флеш-накопичувачів. Зазвичай в компаніях відсутні передові політики або процедури дотримання різних стандартів у сфері інформаційної та кібербезпеки, як-от ISO27001, GDPR, SOC2 та найкращі урядові практики WISP. Це означає, що ризики нерідко оцінюються на основі думок, а не доказів, що робить організації вразливішими до атак.

Хоча деякі організації використовують типові накопичувачі з програмними засобами шифрування, така економія може виявитися вкрай неефективною, оскільки багато накопичувачів із програмним шифруванням можна легко зламати за допомогою безкоштовних або платних інструментів, якими переповнений Інтернет. Крім того, користувач може видалити програмне шифрування простим переформатуванням накопичувача заради зручності або для використання накопичувачів на непідтримуваних платформах. Хоча USB-накопичувачі з апаратним шифруванням мають завжди ввімкнене шифрування, яке неможливо видалити, вони підходять під встановлені цілі; вони захищені від несанкціонованого доступу й проникнення, а також використовують прошивку з цифровим підписом, що гарантує автентичність і цілісність накопичувача. Обмеження кількості спроб введення пароля (захист від атак прямим добором) і використання віртуальних клавіатур (захист від клавіатурних і екранних шпигунів) — дві додаткові функції шифрованих накопичувачів, зокрема IronKey VP50, які означають, що пристрої відповідають найкращим практикам захисту даних від зловмисників, які намагаються вкрасти паролі у користувачів.


**Якщо накопичувач IronKey виявить спробу внесення будь-яких змін у прошивку, він заблокує всі дані та не завантажиться, що підвищить рівень безпеки у кіберпросторі. - Пасі Сіуконен**

# Хто перебуває в зоні ризику?

Будь-які компанії, які не можуть контролювати доступ до своїх USB-накопичувачів, перебувають в зоні ризику. Дуже часто вони навіть не знають, у чому саме полягає цей ризик. Проте існують чинники, які здатні зробити деякі компанії привабливішою мішенню для зловмисників або уразливішими до кібератак.

Дані організацій, які працюють у сфері охорони здоров'я і надання фінансових послуг, не лише приваблюють кіберзлочинців, але й суттєво впливають як на самі організації, так і на їхніх клієнтів. У Великий Британії кібератака, спрямована на державну систему охорони здоров'я (NHS) у 2017 році, призвела до скасування більш ніж 19 000 направлень, через що на відновлення даних і систем було витрачено 92 млн фунтів стерлінгів. Це не тільки завадило пацієнтам отримати медичну допомогу, але й наразило NHS на нищівну критику за недостатньо швидке та ефективне реагування на попередні повідомлення про зростання кіберзагроз. Хоча всі організації мають володіти актуальною та повною інформацією про кіберзагрози, підприємства, які працюють з конфіденційною інформацією — особливо зі спеціальними категоріями даних — повинні проявляти особливу пильність щодо питань безпеки в кіберпросторі.

Із збільшенням обороту компанії збільшується винагорода для зловмисників, що неминуче призводить до зростання кількості кібератак на цю компанію. Проте це не означає, що малі компанії не повинні турбуватись про кібербезпеку; хоча підприємства більше приваблюють зловмисників, вони також мають відповідні ресурси та спеціалізований персонал для боротьби з відповідними кіберзагрозами. З іншого боку, багато малих компаній не мають своїх відділів кібербезпеки та роблять виключення для вищого керівництва, щоб не контролювати їхні USB-накопичувачі. Такі дії підвищують уразливість компаній до кібератак і призводять до катастрофічних наслідків. Деякі дослідження показують, що малий і середній бізнес частіше стає мішенню для кібератак.

У зоні підвищеного ризику перебувають працівники, які обіймають керівні посади; керівників легко відстежити, і вони часто мають привілеї у своїх організаціях, а це означає, що кіберконтроль (наприклад, керування USB-накопичувачами) до них не застосовується, що робить їх дуже зручною мішенню для кіберзлочинців. Саме тому накопичувачі з завжди ввімкненим апаратним шифруванням, повна інформаційна обізнаність про кібербезпеку та дотримання найкращих практик і процедур можуть значно зменшити ризик і захистити від атак.

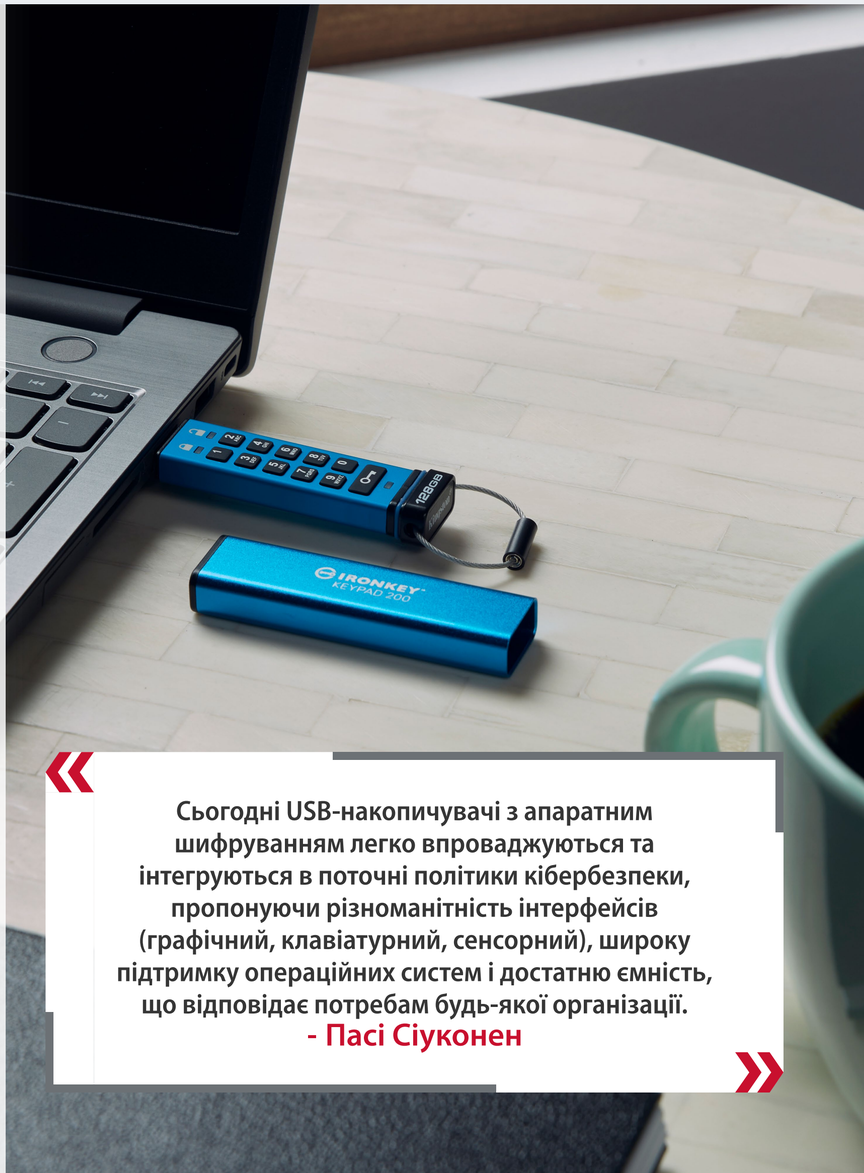
**Останнім часом багато порушень було здійснено зловмисниками, що спеціалізуються на використанні допомоги штатних співробітників, які діють свідомо або несвідомо. - Девід Кларк**

# Хто перебуває в зоні ризику?

> **Організації докладають недостатньо зусиль для протидії загрозам у кіберпросторі. - Девід Кларк**

Ланцюг постачання — ще одне потенційно вразливе місце для організацій, тому атаки на ланцюги постачання є доволі поширеним явищем. У 2013 році в американській роздрібній мережі Target стався один із найбільших в історії роздрібної торгівлі витік даних, унаслідок якого зловмисники отримали доступ до інформації про дебетові та кредитні картки понад 40 мільйонів покупців. Хоча сама компанія Target дуже серйозно ставилася до питання кібербезпеки, встановивши за 6 місяців до атаки масштабну систему кібербезпеки, зловмисники проникли до одного зі сторонніх постачальників Target і через нього отримали доступ до основної мережі даних Target. Загалом проти Target було подано 90 судових позовів, і компанія втратила 61 мільйон доларів США, реагуючи на цю ситуацію; можливо, компанія не несе прямої відповідальності за атаку, але цей недолік системи кібербезпеки в ланцюзі постачання завдав як фінансового, так і репутаційного збитку.

Обхідні шляхи, якими користуються співробітники, також можуть призвести до порушення безпеки даних. Незважаючи на те, що ці обхідні шляхи можуть підвищити ефективність повсякденної роботи співробітників, їх використання дуже часто порушує базові процедури або практики захисту даних, такі, як керування паролями. Хоча Національний центр кібербезпеки (NCSC) або Агентство з кібербезпеки та безпеки інфраструктури (CISA) надають досить прості рекомендації, їх зазвичай складно реалізувати на практиці, особливо тим учасникам команд, які не знайомі з IT-системами та кібербезпекою. Створення спеціальної команди з кібербезпеки, безумовно, може допомогти, але надання співробітникам належних інструментів, зокрема накопичувачів з апаратним шифруванням, може значно зменшити ризики, пов’язані з використанням співробітниками обхідних шляхів.




> **Сьогодні USB-накопичувачі з апаратним шифруванням легко впроваджуються та інтегруються в поточні політики кібербезпеки, пропонуючи різноманітність інтерфейсів (графічний, клавіатурний, сенсорний), широку підтримку операційних систем і достатню ємність, що відповідає потребам будь-якої організації. - Пасі Сіуконен**

# Як організації можуть зменшити ризик кібератак?

З погляду організації, є ряд речей, які можна зробити для захисту кінцевих точок та даних. Без системи GRC (керування, ризик-менеджмент, відповідність вимогам) кібербезпека приречена на провал, тому підприємства обов'язково повинні ознайомитися з процедурами та дотримуватись їх, щоб захистити себе. Наявність надійного програмного забезпечення для захисту кінцевих точок може нейтралізувати низку кіберзагроз, а також миттєво усунути будь-які вразливості в системі безпеки.

> **Приймати чи не приймати примусові політики шифрування — одне з головних питань у сфері керування ризиками, яке може бути важливішим навіть за резервне копіювання даних. - Пасі Сіуконен**

Проте на індивідуальному рівні шифрований пристрій може суттєво зменшити вразливість до загроз у кіберпросторі. Через зростання та поширення віддаленої або гібридної моделі роботи, а також збільшення кількості кібератак за останній рік, украй важливо забезпечити максимальний захист під час обробки, передачі або зчитування корпоративних даних співробітниками на кожному рівні організації.

Скориставшись пристроями з апаратним шифруванням, користувачі можуть відчути всі переваги портативних і зручних флеш-накопичувачів, а також значно зменшити пов'язані з ними ризики; якщо втрачений або вкрадений типовий накопичувач може призвести до втрати даних, грошей або репутації, то накопичувачі з апаратним шифруванням здатні захистити конфіденційні дані від широкого спектру атак. А оскільки кіберзлочинці вигадують нові способи атак, шифровані накопичувачі продовжуватимуть вдосконалюватись, щоб протистояти новим викликам.

Загалом, витрати на боротьбу з кібератаками можуть бути величезними. І дійсно, незважаючи на те, що впровадження й використання шифрованих накопичувачів на кожному рівні організації може потребувати їх ретельнішого затвердження та налаштування, в довгостроковій перспективі це може допомогти компанії заощадити багато грошей, чи то йдеться про витрати, пов'язані зі здирством, чи то про доходи, втрачені через зіпсовану репутацію. Лише одні судові витрати можуть перевищувати вартість USB-накопичувача з апаратним шифруванням.


> **Займаючись вже багато років розробкою високоякісних шифрованих USB-пристроїв, компанія Kingston може запропонувати рішення, які задовольнятимуть вимоги будь-якої організації у сфері кібербезпеки. Це може бути примусове апаратне шифрування, що відповідає галузевим стандартам, дизайн, сумісний із політикою кінцевих точок, а також різноманітні можливості керування пристроями. - Пасі Сіуконен**

# Підсумки

Компанія Kingston постійно відстежую будь-які зміни у сфері кібербезпеки. Наші шифровані накопичувачі IronKey відповідають усім останнім вимогам і задовольняють потреби великих і малих організацій. Оскільки кібербезпека викликає все більше занепокоєння всього світу, ми впевнені, що, маючи у своєму розпорядженні відповідні інструменти та знання, організації зможуть гідно впоратися з цими викликами, захистивши себе, своїх співробітників і клієнтів.

## Про компанію Kingston

Маючи більш ніж 35-річний досвід роботи, компанія Kingston готова допомогти вам у вирішенні будь-яких питань, пов'язаних із передачею мобільних даних, щоб гарантувати безпечні умови роботи для ваших співробітників і захистити вашу компанію від загроз.

**#KingstonIsWithYou**

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021