



Чому USB накопичувачі все ще актуальні?

#KingstonIsWithYou

Вступ та зміст

В сучасну цифрову еру, коли 60% глобальних корпоративних даних зберігаються у хмарі¹, обговорення актуальності технології зберігання даних, якій вже під тридцять років, може здаватися трохи дивним. Однак ця технологія досі продовжує еволюціонувати.

Давно пройшли ті дні, коли USB накопичувачі були всього лише стандартним засобом передачі файлів та програм. Сучасні рішення характеризуються не тільки значно вищою швидкістю передачі, але й являють собою надійні та безпечні носії інформації, що часто має критичне значення. Але як USB можуть все ще бути актуальними, якщо хмарні сховища, здавалося б, мають чимало таких самих переваг?

В цій е-Книзі ми поговоримо про місце USB накопичувачів в умовах домінування хмарних технологій. В публікації наведено думки деяких провідних експертів у цій сфері. Ми також розглянемо, як у сучасному світі організації використовують USB накопичувачі, а також поговоримо про них у контексті програмного шифрування, незалежних середовищ зберігання та наскрізної безпеки даних.

Зміст	Сторінки
Автори	3
Зростання популярності USB накопичувачів	4
Портативне сховище, що відповідає сучасним вимогам	5-6
Шифрування: Апаратне vs програмне	7-8
Зростання потреби у захисті чутливих даних	9
Захист чутливих фінансових даних	10
Захист доступу до даних пацієнтів	11
USB накопичувачі у майбутньому хмарних сховищ	12-13
Підсумки та про компанію Kingston	14



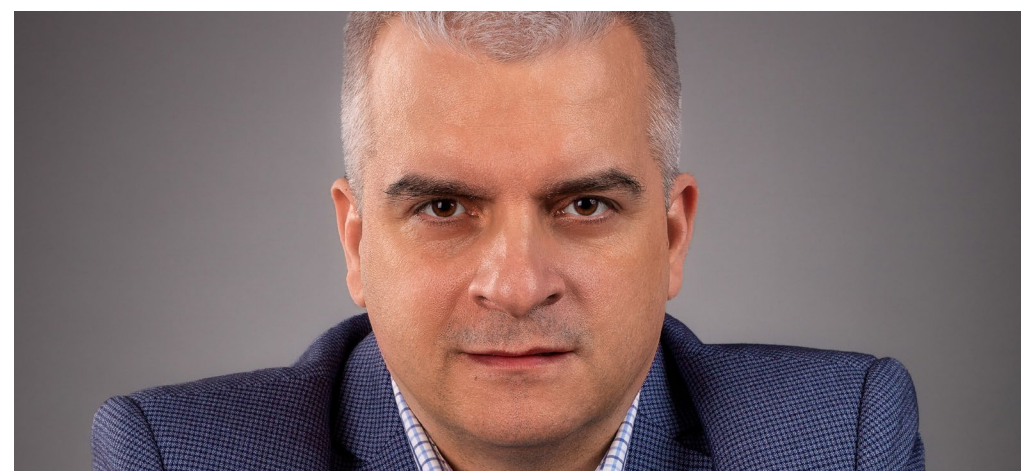
Автори

Авторами цієї е-Книги є троє провідних експертів у галузі IT та новітніх технологій.



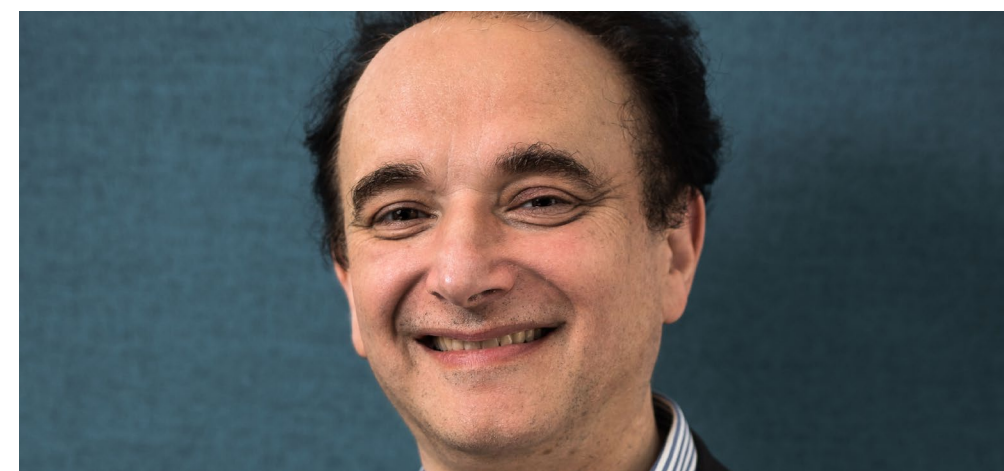
Рафаель Блум

Рафаель в основному працював на таких напрямках, як технологічна продукція, маркетингові комунікації та розвиток бізнесу. Його дорадча практика в основному стосується організаційних, продуктових та комунікаційних викликів технологічних та нормативних змін. Ця робота передбачає надання фахових консультацій щодо управління інформацією, конфіденційності даних та новітніх технологій, таких як AdTech, Mobile & 5G, штучний інтелект та машинне навчання.



Томаш Сурдик

Томаш вже 24 роки працює у сфері IT-безпеки державного сектору і є ключовою фігурою у питаннях інформаційної безпеки, персональних даних та кібербезпеки. Раніше він проводив перевірки інформаційно-телекомунікаційних систем та мереж, в яких оброблялася інформація з обмеженим доступом та персональні дані в сфері державного управління, а також має допуск до роботи з інформацією НАТО та ЄС. Протягом декількох років він був власником компанії, що спеціалізувалася на впровадженні безпечних рішень для зміцнення безпеки бізнес-інформації та персональних даних.



Девід Кларк

Девід входить у топ-десятку інфлюенсерів в рейтингу Thompson Reuter «Топ-30 найвпливовіших лідерів та мислителів у соцмережах у сфері управління ризиками, комплаєнсу та регулювання технологій у Великій Британії», а також входить до топ-50 глобальних експертів Kingston Technology. В минулому Девід неодноразово обіймав керівні посади у безпековому секторі – зокрема, очолював глобальні напрямки безпекових сервісів та безпекової інфраструктури компаній Global FTSE 100.

Із появою на ринку перших USB накопичувачів більше двадцяти років тому їхня колективна сумісність докорінно змінила ситуацію у сфері комп'ютерних технологій. Завдяки здатності забезпечити широким масам можливість роботи з декількома пристроями технологія швидко почала еволюціонувати; швидкість передачі даних значно зросла, з'явилися і нові спроможності.

З того часу відбувся значний технологічний прогрес у плані мобільних сховищ даних та безпекових потреб. Поговоримо про нинішнє покоління USB накопичувачів, які були створені відповідно до дуже конкретних потреб. У розрізі корпоративних середовищ, зростання роботи у дистанційному та змішаному режимі, використання хмарних сервісів та міркування кібербезпеки формують потребу у більш ефективних рішеннях. Окрім цього, спосіб зберігання даних також визначається нормативними вимогами. Складності ще додає існування складних розподілених систем, що можуть працювати як локально, так і в хмарі.

Ще існує питання зростання обсягів структурованих та неструктурованих даних, таких як документи, електронні листи, фотографії, відео та метадані – все це збільшує складність вимог до корпоративних сховищ.

Але якщо багато із цих питань можуть бути вирішені хмарними сховищами, чи є USB накопичувачі актуальними для сучасного бізнес-середовища?



Багато хто сприймає USB накопичувачі як дещо старомодне – тому що раніше вони використовувалися як недорогі та не дуже захищені «штучки на раз». - **Рафаель Блум**



Портативне сховище, що відповідає сучасним вимогам

Хоча колишні підходи до використання USB накопичувачів як портативного сховища даних вже не є актуальними, зараз високотехнологічні USB скоріше грають роль локального «бекапу» із додатковим рівнем захисту та конфіденційності даних. Це може бути дуже важливим, якщо мова йде про такі чутливі дані, як документація щодо співробітників, фінансова документація, записи установ охорони здоров'я, дані щодо об'єктів інтелектуальної власності, а також інформація, що дозволяє ідентифікувати особу. Окрім цього, це покоління відрізняється швидкою передачею даних та можливостями щодо зберігання, резервного копіювання та безпеки даних, які можна використовувати для:

- ❑ Нормативної інформації, яка має бути передана вручну
- ❑ Юридичних та фінансових документів, що мають бути передані та роздруковані на місці
- ❑ У разі наявності загрози вірусів-вимагачів
- ❑ Передача на пристрої друку за відсутності мережевого доступу

Компанія Kingston Technology, провідний виробник шифрованих USB накопичувачів, швидко реагує на появу нових вимог, доказом чого є вихід таких рішень, як [Kingston IronKey™ S1000](#). Ця модель USB накопичувача, що є лідером у своєму класі, відповідає найжорсткішим вимогам; захист важливих даних забезпечується шифруванням XTS-AES 256-bit, а спеціальний крипточип забезпечує протидію зламу. Накопичувач також сертифікований за стандартом FIPS 140-2 Level 3. Це означає офіційну валідацію урядом США як ефективного криптографічного обладнання, тому він є ідеальним вибором для організацій, які не хочуть зайвого клопоту із захистом даних.

Такі накопичувачі із апаратним шифруванням мають можливість централізованого управління пристроями (в хмарі або на підприємстві). Наявність «правильного» шифрованого сховища даних, яке буде простим в експлуатації та не потребує встановлення ПЗ, також вивільняє цінний час ІТ-фахівців.



Портативне сховище, що відповідає сучасним вимогам

Резервне копіювання та архівування – це один приклад використання USB накопичувачів для захисту цифрових активів у довгостроковій перспективі та автономно від сторонніх хмарних сервісів. Дійсно, великі обсяги даних можна швидко передавати і в хмарі, однак це може бути недостатньо безпечним середовищем для чутливих даних, тому непоганою ідеєю буде зберігати на шифрованому USB, який зберігається без підключення до Інтернет.

Завжди бувають такі обставини, в яких організація потребує, щоби дані логічно та фізично перебували під її контролем, особливо при використанні шифрованих накопичувачів. А ще буває так, що сховище на HDD/SSD неможливо зашифрувати. Використання зовнішніх шифрованих USB накопичувачів, як [Kingston IronKey D300S](#), дозволяє вирішити цю проблему. Цей USB накопичувач обладнаний апаратним шифруванням XTS AES 256-bit, яке шифрує дані 128-бітними блоками. Коли виникає необхідність у шифруванні даних поза цими межами, AES вмикає режим блочного шифрування XTS, який здатний забезпечувати кращий захист даних, аніж попередні режими.



Я вважаю, що USB накопичувачі все ще є невід'ємною частиною безпеки даних. Зокрема, вони використовуються для швидкої передачі даних між пристроями, а також їх належного зберігання та захисту. - **Томаш Сурдик**

Шифрування: Апаратне vs програмне



Що стосується способу шифрування даних, то можна стверджувати, що апаратне шифрування є простішим в адмініструванні та більш безпечним. Це зумовлено тим, що процес шифрування відбувається автономно від самої системи, що значно ускладнює зовнішнє втручання. Централізоване адміністрування на рівні пристроїв забезпечує керування накопичувачем через локальну мережу та по Інтернету, і може бути прекрасним інструментом для:

- ❑ Встановлення та впровадження індивідуальних та/або групових політик використання USB
- ❑ Аудиту та відстеження переміщення даних всередині організації та поза її межами
- ❑ Дистанційного резервного копіювання критичних даних
- ❑ Дистанційного блокування пристрою у разі втрати або крадіжки накопичувача
- ❑ Дистанційне відновлення забутого паролю



Я вважаю, апаратне шифрування краще, ніж програмне. Відмінності між цими методами шифрування даних є суттєвими у розрізі вразливості перед агресивними атаками. У разі використання пристроїв з апаратним шифруванням успішне проведення атаки є малоімовірним.

- Томаш Сурдик



Зростання потреби у захисті чутливих даних

« Зашифруйте всі дані якомога скоріше, зробіть їхнє резервне копіювання за допомогою методології 3-2-1 (як варіант – USB, який є під рукою) та впровадьте швидку мікросегментацію.

- Девід Кларк »

Коли заходить мова про захист чутливих даних від втрати та зламу, кожна організація має зобов'язання щодо забезпечення достатньої безпеки свого обладнання. Також варто пам'ятати, що хоча існує ціла плеяда кіберзагроз, що постійно еволюціонують, рівень цифрової зрілості та навички самих користувачів щодо поводження із даними можуть становити суттєвий фактор ризику, якщо їм не приділяти належної уваги. Загроза несанкціонованих дій користувачів – до цього відноситься втрата контролю над даними або носіями інформації, передача даних за межі безпечного середовища, використання USB накопичувачів без шифрування та передача паролів – може бути наслідком недбалої поведінки кінцевого користувача. Всього цього можна уникнути за допомогою належної підготовки, інформування та правильного вибору USB накопичувачів.

« Організація повинна мати чітку карту своїх даних, включно із рівнем важливості або чутливості всіх масивів даних, а також план дій стосовно пріоритетних даних – шляхом фізичного переривання доступу до даних або шляхом переведення джерела даних у тінь. Дуже важливо мати змогу швидко ізолювати пошкоджені системи – і, знову ж таки, мати задокументований план дій.

- Рафаель Блум »

Попереднє планування та ретельно відпрацьована структура комунікації є ключовим фактором у поводженні із потенційною загрозою. Сучасні кіберзагрози спрямовані на слабкі місця організацій.

План щодо використання USB із шифруванням краще готувати заздалегідь шляхом включення політики використання таких накопичувачів у загальну стратегію безпеки організації. Відсутність плану щодо використання шифрованих USB та відсутність нормативного регулювання – це означає незахищені тили і піддає вашу організацію ризикам на усіх рівнях, в тому числі стосовно невиконання законодавчих вимог – зокрема, Генерального регламенту ЄС про захист даних (GDPR), в статті 32 якого прямо вказано, що чутливі дані мають бути зашифровані.

« Користувачі працюють із чутливими даними. Втрата цих даних означає притягнення до відповідальності, а також може нанести серйозний удар по іміджу та безпеці компанії. Для захисту чутливих даних слід застосовувати різні серйозні рішення, в тому числі шифрування даних.

- Томаш Сурдик »

Окрім наслідків для безпеки, також існують певні стандарти, яким мають відповідати рішення для зберігання та резервного копіювання даних. Деякі із таких практик (наприклад, необхідність запроваджувати графіки оновлення даних та адмініструвати їх) є доволі поширеними по вертикальній структурі, в той час інші – наприклад, міграція корпоративних даних у хмару – викликають неоднозначні думки.

В багатьох організаціях із вертикальною структурою, наприклад, у фінансовій сфері, прийняті правила, завдяки яким належне поводження із даними стало обов'язковим. Найбільше відсутність ентузіазму щодо використання сторонніх рішень для зберігання та резервного копіювання даних демонстрували банки, і багато банків досі наполягають на тому, щоби інфраструктура даних була на 100% їхньою власністю.

Фінансові установи також повинні дотримуватися низки нормативних актів та стандартів безпеки даних (цей перелік постійно розширюється), зокрема, Закону Сарбейнса-Окслі (SOX) та Генерального регламенту ЄС про захист даних (GDPR). По мірі збільшення кількості мобільних працівників та підрядників зростає і ризик витоку даних та недотримання вимог таких нормативних документів та стандартів.

Істина полягає в тому, що всі ці зусилля можуть виявитися марними, якщо мобільні працівники не дбають про захист своїх цифрових даних, мобільних робочих місць, клієнтських даних та фінансових відомостей. Сам тому все більше організацій віддають перевагу таким мобільним безпечним рішенням, як [шифровані USB накопичувачі Kingston IronKey](#), що дозволяють захистити чутливі дані незалежно від того, де знаходиться працівник компанії.



Коли ми дивимось на загальний зсув тенденцій в бік більш розподіленого ІТ та чистого масштабування хмарної інфраструктури, стає очевидно, що у більшості сфер діяльності (і дуже багато представників малого та середнього бізнесу) вже мало хто заморочується власними охолодженими серверними приміщеннями.

- Рафаель Блум



Охорона здоров'я є ще однією сферою, де безпека даних є надзвичайно важливою. Ризик крадіжки є навіть вищим для даних пацієнтів – лише у 2021 році через злами відбувся витік 45,67 млн. записів пацієнтів, що є найвищим річним показником з 2015 р.² Що стосується зберігання та резервного копіювання, то можна сказати, що дані пацієнтів мають критичне значення, оскільки така інформація допомагає працівникам сфери охорони здоров'я у належний спосіб їх лікувати.

До них може відноситися будь-що від електронних карток пацієнтів із історією хвороби, результатами аналізів, фотографіями, радіографічними зображеннями, і до адміністративних файлів із зарплатними відомостями, даними щодо страхування пацієнтів та бухгалтерськими документами. В умовах зростання відсотку мобільних працівників та значної трансформації глобального ринку охорони здоров'я не дивно, що постачальники послуг в цій сфері занепокоєні безпекою даних.

Нездатність прорахувати ризики та забезпечити дотримання жорстких вимог таких нормативних актів, як Закон про уніфікацію даних та підзвітність у сфері страхування здоров'я (HIPAA) або Закон про інформаційні технології у економічній сфері та сфері охорони здоров'я (HITECH) може призвести до дуже дорогих наслідків витоку даних та втрати довіри пацієнтів, партнерів та регуляторних органів.

Завдяки таким рішенням, як лінійка шифрованих USB накопичувачів Kingston IronKey, організації, що працюють у сфері охорони здоров'я, можуть встановлювати паролі, визначати порядок використання програм, відновлення даних тощо – як для декількох одиниць накопичувачів, так і для декількох тисяч, і все з однієї консолі. Маючи зручні у використанні рішення, які ліквідують потребу встановлювати драйвери чи інші програми для безпечного доступу до даних, мобільні бригади можуть охопити більшу кількість пацієнтів. При цьому користувачі та адміністратори можуть легко та швидко блокувати дані незалежно від місцезнаходження.



Програми-вимагачі набувають особливо широкого вжитку, тому будь-яка організація, що має справу із чутливими даними, повинна продумати план дій на випадок позаштатних ситуацій. - **Рафаель Блум**



USB накопичувачі у майбутньому хмарних сховищ



Хмарні сховища даних – це сучасне та майбутнє. Я все ще стверджую, що фізичний захист даних, зокрема, за допомогою шифрованих USB, є найбільш надійним. Користувачі не мають контролю над тим, що відбувається у хмарі. Але ми можемо контролювати дані на шифрованих USB накопичувачах, які ми убезпечуємо та зберігаємо самі. До вмісту цього носія маємо доступ лише ми.

- Томаш Сурдик



Отже, з перевагами USB накопичувачів розібралися, так в чому ж власне полягає їхня роль у майбутньому хмарних сховищ?

З десять років тому на «флешки» був величезний попит як на зручний засіб зберігання та передачі даних. Однак завдяки появі нових моделей гібридної роботи та все більш розгалуженій роботі груп хмарні середовища швидко та просто забезпечують доступ до збереженої інформації з багатьох пристроїв. Популярність «флешок» пояснюється їхньою зручністю для передачі файлів. Сучасні хмарні сервіси є навіть більш зручними.

При цьому хмарні сховища мають і свої обмеження. Необхідно мати підключення до мережі, що не лише визначає порядок та час резервного копіювання або передачі файлів, але й додає безпекових складнощів. Коли компанія приймає рішення про організацію роботи в хмарі, вона не завжди здатна контролювати, звідки відбувається доступ до даних. Тому просте підключення до VPN з використанням персонального або публічного Wi-Fi з'єднання створює ризик зламу. Хмарні сервіси також дуже приваблюють зловмисників, і наразі більша частина (61%) шкідливого програмного забезпечення передається через хмарні застосунки³.



Варто продумати порядок дій на випадок недоступності хмари в тих сценаріях, коли дані мають бути доступні на 100%, і де довготривале зберігання може призвести до вразливості.

- Девід Кларк





З іншого боку, USB-шифрування може здійснюватися як апаратними, так і програмними засобами. Апаратне шифрування є найбільш ефективним способом захисту від кібератак. Це чудове і просте рішення забезпечує захист від зламу даних, дотримання жорстких стандартів та надзвичайний рівень безпеки даних, що дозволяє організаціям із впевненістю протидіяти загрозам та ризикам.

USB із апаратним шифруванням є самодостатніми та не вимагають програмного елементу на комп'ютері. Відсутність програмної вразливості також означає відсутність можливостей здійснення атак «в лоб», шпигунів тощо. USB накопичувачі із програмним шифруванням також несуть ризик того, що будь-який користувач може відключити шифрування шляхом форматування накопичувача на будь-якому комп'ютері і зберігати чутливі дані без належного захисту.

USB накопичувачі з апаратним шифруванням також мають прекрасні фізичні засоби захисту даних. Вони передбачають можливість встановлення критеріїв доступу до інформації користувачем або адміністратором, та можуть інтегруватися із наявними місцевими наскрізними рішеннями. Завдяки цьому вони є зручним та бюджетним рішенням для багатьох сценаріїв, в яких з якихось причин хмарне сховище не

підходить або буде не настільки ефективним. Наприклад, коли дані мають зберігатися на пристроях, які не підключені по мережі, або мають бути приватними, або вимагають доступу у режимі офлайн.



Якщо ми розглядаємо дані як «гарячі» або «холодні» залежно від частоти використання у поточній роботі організації, то має сенс розташувати «холодні» дані в хмарі, а «гарячі» – на локалізованих USB сховищах, якщо операційна безперервність та висока продуктивність є пріоритетом для організації або для конкретної критичної функції або процесу. - **Рафаель Блум**



Хоча неможливо спрогнозувати появу наступних інновацій, ми пропонуємо лінійку USB накопичувачів преміум-сегменту, які містять динамічний спектр шифрованих рішень на будь-які потреби щодо захисту мобільних даних. Від буквенно-цифрової клавіатури для зручного захисту PIN-кодом; сертифікації за стандартом FIPS 140-2 Level 3, що засвідчує найвищий рівень шифрування та захист від зламу; до технології SuperSpeed USB 3.1, в якій швидкість не зменшує безпеку; лінійка USB накопичувачів IronKey від Kingston достойно подолає будь-які виклики та забезпечить ефективне перенесення та зберігання мобільних даних.

Наша команда експертів готова супроводжувати вас на кожному кроці під час вибору сховища даних під конкретні потреби.

У нас є навички та технічні спроможності для того, щоби допомогти вам убезпечити конфіденційну інформацію та виконати нові нормативні вимоги – підбираєте ви найкращі моделі USB накопичувачів для свого бізнесу або встановлюєте та впроваджуєте політику безпеки. Ми пропонуємо персоналізований сервіс і дбаємо про те, щоби наша продукція сприяла досягненню ваших пріоритетів щодо зберігання даних та допомагала тримати той безпрецедентний темп, з яким змінюється світ бізнесу.

Про компанію Kingston

Компанія Kingston має 35 років досвіду та готова допомогти вам у подоланні будь-яких викликів стосовно мобільних даних, щоби ваші працівники могли працювати безпечно та не піддавати ризикам вашу організацію.

1. Statista - <https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data>
2. SC Magazine - <https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015>
3. Infosecurity Magazine - <https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers>

ЦЕЙ ДОКУМЕНТ МОЖЕ БУТИ ЗМІНЕНО БЕЗ ПОПЕРЕДЖЕННЯ.

©2022 Kingston Technology Corporation 17600 Newhope Street, Fountain Valley, CA 92708 USA.

Усі торгові марки та зареєстровані торгові марки є власністю їх відповідних власників.

#KingstonIsWithYou