http://www.moderntechno.de/index.php/meit/article/view/meit41-01-049
DOI: 10.30890/2567-5273.2025-41-01-049

УДК 004.056.53(043.2)

PREVENTION OF RESIDUAL INFORMATION LEAKAGE FROM PHYSICAL MEDIA

ЗАПОБІГАННЯ ВИТОКУ ЗАЛИШКОВОЇ ІНФОРМАЦІЇ З ФІЗИЧНИХ НОСІЇВ

Kindrat P.V. / Кіндрат П.В.
k.l.s. associate professor / к.ю.н, доцент
ORCID: 0000-0003-0351-3349
National university of water and environmental engineering,
Rivne, Soborna 11, 33000
Національний університет водного господарства та природокористування,
м. Рівне, вул. Соборна 11, 33000

Анотація: *У статті розглянуто проблему захисту від витоку залишкової інформації з фізичних носіїв, яка становить серйозну загрозу для інформаційної безпеки, особливо в умовах недотримання відповідних стандартів. Було висвітлено різницю між логічним видаленням та фізичним стиранням даних, акцентуючи увагу на небезпеці відновлення інформації зі списаних або викинутих носіїв. Проаналізовано основні методи санітаризації даних – логічне очищення, обнулення та фізичне знищення носіїв, а також їхні переваги та обмеження. Окрему увагу приділено криптографічному стиранню як сучасному ефективному методу захисту, зокрема шляхом використання носіїв з апаратним самошифруванням. Окреслено принцип роботи таких накопичувачів, їх переваги та відомі вразливості. Зроблено висновок щодо сфери використання криптографічного стирання як засобу захисту залишкової інформації від витоку.*

Ключові слова: *витік інформації, залишкова інформація, технічний захист інформації, криптографічне стирання, само шифрування.*

Вступ.

В сучасному світі розвиток кіберзагроз досяг такого рівня що протидія їм стає частиною повсякденного життя не лише спеціалістів з інформаційної безпеки, а й звичайних громадян. У зв’язку з чим особливо актуальними є як розробка інструментів захисту від різних видів загроз, так і проведення інформаційно-просвітницької роботи серед користувачів цифрових пристроїв для мінімізації ризиків з ними пов’язаних.

В межах такої діяльності проблематика технічного захисту інформації знаходиться в медійній «тіні». А її обговорення рідко виходить за межі професійних кіл. Водночас окремі її аспекти мають особливе значення саме для побутових користувачів та невеликих організацій. Оскільки такі користувачі здебільшого не дотримуються вимог міжнародних стандартів (наприклад ISO/IEC 27040), або ж не володіють достатніми ресурсами для їх застосування

на практиці. До таких аспектів відноситься запобігання витоку інформації через матеріально-технічні канали, шляхом збору і відновлення інформації на списаних (викинутих) фізичних носіях.

Метою статті є розкрити проблематику витоку залишкової інформації з фізичних носіїв та запропонувати напрямки розв'язання цієї проблеми.

Основний текст

Витік залишкової інформації є серйозною загрозою, оскільки він дозволяє несанкціоновано відновити конфіденційні дані навіть після того, як користувач чи система нібито їх видалили. Ця загроза виникає через фундаментальну різницю між логічним видаленням та фізичним стиранням даних на носії, яка не завжди зрозуміла користувачам. У них часто виникає ілюзія видалення інформації, коли вони видаляють файли у звичайній операційній системі. Проте операційна система не стирає фізичні біти даних по замовчуванню. Натомість вона лише видаляє посилання на цей файл у таблиці файлової системи втрачаючи зв'язність інформації не знищуючи безпосередньо дані.

Попри те що витокам даних через хакерські атаки приділяється багато медійної уваги, все ж найчастіше витік відбувається не через них, а через невірне поводження з обладнанням, яке виводиться з експлуатації. [1] Так комп'ютери, сервери, мобільні телефони чи принтери з жорсткими дисками можуть продаватись на вторинному ринку чи передаватись іншим підрозділам організації, або ж викидатись на смітник без належної санітаризації носіїв інформації. Таким чином будь-яка особа, яка отримає доступ до старого носія, може відновити критичну залишкову інформацію застосовуючи широкий спектр спеціалізованого програмного та апаратного забезпечення та завдати шкоди її власнику.

Залишкова інформація – це дані, які фізично зберігаються на носії (жорсткому диску, SSD, флеш-пам'яті тощо) після того, як їх було логічно видалено за допомогою стандартних дій операційної системи: форматування або перезапису. Її наявність на носії після завершення строку його експлуатації є прямою загрозою безпеці, оскільки дозволяє легко відновити конфіденційні дані.

Окремою проблемою знищення залишкової інформації є також фізичні властивості носіїв інформації, які уможливлюють її відтворення навіть після перезапису. Так в жорстких дисках магнітна поверхня може зберігати дані до 8 перезаписів, а сучасні твердотільні накопичувачі використовують технологію вирівнювання зносу (Wear Leveling), що ще більше ускладнює надійне стирання.

Для запобігання витоку залишкової інформації здебільшого використовують методи санітаризації носіїв. До них відносять:

1. очищення – коли здійснюється логічний перезапис даних на носії за допомогою програмного забезпечення (наприклад, перезапис нулями або випадковими послідовностями). Воно захищає від простих програмних атак, але може бути недостатньо надійним для високочутливих даних, оскільки не гарантує очищення всіх прихованих областей (наприклад, Reallocated Sectors).

2. обнулення – більш глибокий метод, що забезпечує незворотність видалення навіть для складних носіїв. Проте він все ж не гарантує повну неможливість відновлення даних на фізичному рівні.

3. фізичне знищення – метод який передбачає фізичне пошкодження носія до стану, коли його відновлення стане статистично неможливим. Для цього застосовуються:

- шредерування – фізичне подрібнення диска на дрібні частинки (розмір частинок має відповідати вимогам безпеки);
- розмагнічування – застосування потужного магнітного поля для обнулення магнітних доменів (працює лише для HDD);
- спалювання або плавлення – високотемпературна обробка матеріалу носія до незворотної зміни його фізичних властивостей.

Проте зазначені методи можуть бути ефективними лише за умови наявності чіткого організаційного та функціонального управління інформаційною безпекою пристроїв, а також при наявності відповідного апаратного забезпечення. Для використання в побутових умовах, або ж умовах невеликих організацій застосування таких методів може нівелюватись людським фактором, браком ресурсів, або ж простою недбалістю.

Для мінімізації зазначених ризиків доцільно використовувати системи які здійснюють наскрізне шифрування усіх даних що зберігаються на диску. Це дозволить гарантувати, що навіть за умови зчитування зловмисником даних на фізичному носії, без ключа шифрування він не зможе відновити інформацію яка була там записана.

Такий підхід має назву «криптографічне стирання». Це метод санітаризації носія, який полягає не у знищенні самих даних, а у знищенні криптографічного ключа, який використовувався для їх шифрування. Досягнення цієї мети може бути здійснено як програмними так і апаратними методами або ж їх комбінацією.

Для програмних методів наскрізного шифрування є притаманним використання або вбудованого рішення операційної системи (BitLocker, FileVault, LUKS тощо), або стороннього рішення (VeraCrypt, VeraCrypt тощо), або вбудованих протоколів мови розробки програмного продукту. Їх перевагою є простота налаштування і експлуатації, а також можливість копіювання шифрованих даних між носіями без необхідності їх попереднього дешифрування. Проте до недоліків слід віднести те, що вони не забезпечують повного шифрування усіх даних в системі. Так власне сама операційна система та її системні файли будуть залишатись не зашифрованими і вразливими для відновлення після видалення. Тип шифрування AES

Наскрізне апаратне шифрування – це концепція, яка поєднує принципи наскрізного програмного шифрування і використання спеціалізованого апаратного забезпечення для виконання всіх криптографічних операцій. Воно забезпечує високий рівень безпеки, оскільки ключі шифрування ніколи не покидають захищене апаратне середовище. Воно також усуває ризики, пов'язані з програмним забезпеченням, такі як атака побічними каналами. А за рахунок того що ключі шифрування зберігаються в апаратній пам'яті, то це не дозволяє шкідливому програмному забезпеченню чи операційній системі отримати до них доступ.

Останнє водночас є і недоліком, оскільки для доступу до інформації що зберігається на змінних носіях необхідно завжди мати фізичний токен з ключами

доступу. А втрата ключа доступу унеможливить відновлення зашифрованих даних.

Та найкращих результатів можна досягти на пристроях які успішно комбінують ці два методи. На сьогоднішній день існує лінійка накопичувачів які підтримують апаратне самошифрування (Self-Encrypting Drives, SED). Ключової їх особливістю є використання швидких алгоритмів шифрування на низовому рівні, що дозволяє зберігати дані на носії у зашифрованому вигляді, водночас обробка інформації системою після її зчитування відбувається у дешифрованому вигляді, що, в свою чергу, не потребує змін у роботі операційних систем та прикладного програмного забезпечення.

Принцип роботи роботи такої системи має вигляд:

1. початкове шифрування: накопичувач з SED має вбудований контролер, який постійно шифрує всі дані, що записуються на диск, використовуючи унікальний Ключ шифрування даних (Data Encryption Key, DEK).

2. захист ключа: цей DEK, у свою чергу, зашифрований Ключем авторизації (Authorization Key), який надається користувачем (або системою).

3. процес стирання (CE): Коли запускається команда криптографічного стирання, контролер диска не перезаписує мільярди комірок пам'яті. Замість цього він робить одну з двох речей:

– знищує DEK (ключ шифрування даних), або

– генерує новий DEK та шифрує ним диск.

4. Результат: Оскільки старий DEK знищено (або він став недоступним), всі дані на диску залишаються зашифрованими старим ключем, але їх неможливо розшифрувати, оскільки ключ безповоротно втрачено. Для будь-кого, хто спробує відновити дані, вони будуть виглядати як випадковий, нечитабельний набір біт.

До ключових недоліків такого рішення є чутливість до апаратного забезпечення: старі чи дешеві накопичувачі можуть не мати функції SED, а також потреба у встановленні спеціалізованого програмного забезпечення або BIOS/UEFI.

Також слід відмітити низку досліджень надійності накопичувачів з апаратним самошифруванням які у 2019 році показали наявність апаратної вразливостей в багатьох популярних накопичувачах з функцією SED [2]. Вразливість виражалась в реалізації алгоритму AES та управлінні ключами на рівні прошивки диску. Зокрема окремі моделі не прив'язували ключ шифрування диску до пароля користувача, що дозволяло обійти цей рівень захисту. В той час як інші виробники залишали простий майстер-ключ до криптоалгоритму, що дозволяло його ігнорувати.

Виявлені проблеми похитнули довіру користувачів до SED систем, та спонукали доповнювати вбудоване апаратне шифрування програмним, в якому також з часом було знайдено вразливості

Та попри наявні обмеження та вразливості (які не дозволяють гарантувати високий рівень криптографічного захисту інформації на диску), використання криптографічного стирання є пріоритетним вибором для швидкої та надійної санітаризації сучасних SSD-накопичувачів.

Висновки

Запобігання витоку залишкової інформації є важливим елементом забезпечення технічного захисту інформації. Воно вимагає комплексного підходу та узгодження організаційних і технічних рішень. І оскільки фізичне знищення носія є економічно та ресурсозатратним, а організаційні заходи можуть бути неефективними через людський фактор то для запобігання витоку інформації доцільно скористатись спеціалізованим програмно-апаратними засобами які дозволяють здійснювати криптографічне стирання.

Застосування носіїв з апаратним самошифруванням дозволяє:

- ✓ здійснювати обхід прихованих областей які виникають в SSD під час переміщення даних контролером диску.
- ✓ прискорити процес очищення диску, оскільки він не потребує перезапису всіх комірок диску, а лише комірок в яких зберігається ключ шифрування.

Література:

1. Полотай О.І. Аналіз засобів запобігання витоку конфіденційної інформації на підприємствах на прикладі системи DLP / О. І. Полотай, А. О. Пузир // Львів: Вісник ЛДУБЖД, 2024. – №30. – С. 134-144 DOI: 10.32447/20784643.30.2024.13

2. Meijer C. Self-Encrypting Deception: Weaknesses in the Encryption of Solid State Drives / C. Meijer B. van Gastel // San Francisco: IEEE Symposium on Security and Privacy (SP), 2019. P. 72-87. DOI: 10.1109/SP.2019.00088

Abstract. *The article examines the problem of protection against residual information leakage from physical media, which poses a serious threat to information security, especially in conditions where relevant standards are not fully adhered to. The paper highlights the difference between logical deletion and physical data erasure, emphasizing the danger of data recovery from decommissioned or discarded storage devices.*

The core data sanitization methods – logical clearing, purging (zeroing), and physical destruction of media – are analyzed, along with their advantages and limitations. Special attention is paid to cryptographic erase as a modern, effective protection method, particularly through the use of self-encrypting drives. The paper outlines the operating principle of such drives, their benefits, and known vulnerabilities. A conclusion is drawn regarding the scope of using cryptographic erasure as a means of protecting residual information from leakage.

Key words: *data leakage, residual information, technical information security, cryptographic erase, self-encryption.*

Статтю надіслано: 20.10.2025 р.