ЗАГАЛЬНОНАУКОВІ ПРОБЛЕМИ РОЗВИТКУ ЗБРОЙНИХ СИЛ УКРАЇНИ

DOI: https://doi.org/ 10.37129/2313-7509.2019.11.99-112
УДК 65.012.8:007

О.М. Семененко[1], д.військ.н.
Ю.Б. Добровольський[2], к.т.н., доц.
Р.В.Лукаш[3]
В.Л. Коверга[4]
О.М.Сєченєв[2]
[1]*Центральний науково-дослідний інститут Збройних Сил України, м. Київ*
[2]*Кафедра військової підготовки Національного авіаційного університету, м. Київ, Україна*
[3]*Військова академія (м. Одеса), Україна*
[4]*Національний університет оборони України, м. Київ*

АНАЛІЗ ТА ОЦІНКА МЕТОДІВ І ЗАСОБІВ ЗНИЩЕННЯ ІНФОРМАЦІЇ З МАГНІТНИХ НОСІЇВ ЯК ЕЛЕМЕНТУ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті проведено аналіз та оцінка ефективності існуючих методів і засобів знищення інформації з магнітних носіїв як важливого елементу сучасної інформаційної безпеки з метою вироблення практичних рекомендацій щодо вибору найбільш ефективних та економічно вигідних методів та засобів знищення конфіденційної інформації в сфері оборонній.

Ключові слова: *інформаційна безпека; знищення інформації; ефективність знищення інформації; магнітний носій інформації; магнітне поле; жорсткий диск; оперативна пам'ять.*

Судячи з усього, інформаційна революція на землі триває. Людство вже щорічно виробляє близько 5 екзабайт інформації (5 мільярдів Гбайт), причому, близько 80% якої зберігається і передається за безпосередньої участі накопичувачів, які використовують принципи магнітного запису [1–5]. Сьогодні в комп'ютерних інформаційних системах основні обсяги інформації зберігаються в пам'яті накопичувачів на жорстких магнітних дисках (ЖМД). "Віртуальне" програмне стирання інформації, яке забезпечується штатними засобами комп'ютера, природньо, не може задовольнити усіх користувачів, що активно стимулює пошук нових ефективних методів і засобів захисту важливої та конфіденційної інформації [1–12]. Тому сьогодні разом із розвитком засобів зберігання та перенесення інформації набувають активного розвитку методи (способи) її остаточного знищення без залишкового ефекту. Особливо цього потребують сфери бізнесу та захисту держави, які володіють значними масивами конфіденційної (таємної) інформації. У більшості випадків, після ознайомлення з цією інформацією є потреба остаточного знищення її без можливостей відновлення сучасними засобами зацікавлених сторін щодо її отримання.

Сьогодні, інформаційні системи обміну та збереження інформації в Міністерстві оборони (МО) України мають певні засоби та підходи до знищення інформації, але кожний з них має різні оцінки ефективності їх застосування, а також різну вартість їх закупівлі та використання. Тому проведення комплексного аналізу щодо оцінювання методів та засобів знищення конфіденційної інформації з метою формування практичних рекомендацій щодо вибору для МО України найбільш ефективних та економічно можливих є достатньо актуальним завданням сьогодення [1–4].

Постановка проблеми

Сьогодні розвиток і застосування нових сучасних технологій у всіх галузях виробничої діяльності нерозривно пов'язане з обміном, використанням, обробкою та зберіганням інформації. Прогрес у

розвитку технологій і обладнання для виробництва напівпровідників, матеріалів і приладів електронної техніки, що почався в кінці минулого століття, визначив широке впровадження електронно-обчислювальних машин (ЕОМ), у тому числі і персональних, у всіх сферах людської діяльності [1–3]. Об'єднання окремих ЕОМ в глобальну комп'ютерну мережу «Інтернет» дозволило органам державної влади, міністерствам, відомствам, силовим структурам, різним організаціям, фірмам і приватним особам істотно розширити доступ до інформаційних ресурсів, збільшити обмін інформаційними потоками, здійснювати їх обробку в реальному масштабі часу або в стислі часові терміни. Удосконалення різних радіоелектронних засобів, підключення їх до ЕОМ, об'єднаним в локальні мережі, призвело до виникнення складних керуючих систем і комплексів, призначених для автоматизованої обробки великих потоків інформації і видачі сигналів управління (системи управління рухом, навігаційні системи тощо).

Значне збільшення обсягу інформації, що зберігається та скорочення часових ресурсів, необхідних для її обробки, зумовило необхідність застосування поряд з паперовими носіями інформації інших носіїв, що сполучаються з ЕОМ. До таких носіїв слід віднести магнітні носії, що застосовуються в системах магнітного запису, що входять до складу персональних ЕОМ. Зараз на різних підприємствах і в організаціях, структурах, підпорядкованих військових відомств, в якості носіїв інформації, широкого поширення набули гнучкі і жорсткі магнітні диски, та флеш носії, різні типи аудіо, відео та стримерних касет, спеціальний магнітний дріт, жорсткі, переносні накопичувачі інформації [1,5,9]. Серед систем магнітного запису особливе місце займають накопичувачі на жорстких магнітних дисках (НЖМД). Вони характеризуються об'ємом записуваної інформації в десятки, сотні і, навіть, тисячі гігабайт і часом доступу порядку 0,1–1 секунди. У останні десять років поверхнева щільність запису інформації на НЖМД збільшувалася щороку в середньому на 60%. Існуюча тенденція збережеться й далі, при цьому характерні розміри носіїв значно зменшуються. Зараз ці носії займають провідні позиції серед інших видів носіїв інформації та широко застосовуються для зберігання та перенесення інформації з обмеженим доступом. На таких магнітних носіях можливе зберігання великої кількості конфіденційної інформації, тобто інформаційних ресурсів, неконтрольоване поширення яких з яких-небудь причин небажано. Сьогодні в ЗС України для захисту конфіденційної інформації, яка може зберігатися на магнітних носіях, застосовуються організаційно-режимні та організаційно-технічні заходи, що дозволяють перекрити можливі канали витоку інформації [5-8]. До організаційно-режимних заходів слід віднести обмеження кола осіб, допущених до роботи на даній ЕОМ, облік і зберігання магнітних носіїв в спеціальних місцях, що знаходяться під охороною тощо. До організаційно-технічних заходів слід віднести контроль технічних та експлуатаційних характеристик [2-4] і подальше закриття каналів витоку інформації шляхом застосування апаратури засекречування, зменшення випромінювання складових частин ЕОМ тощо. Разом з тим в комплекс заходів щодо закриття каналів витоку інформації входить не тільки охорона і приховування інформації, розміщеної на магнітних носіях, але також її надійне знищення після ознайомлення та опрацювання або в екстрених обставинах. Якщо мова йде про конфіденційну інформацію, то в цьому випадку у користувача, власника або власника цієї інформації має бути впевненість в надійності її знищення з метою забезпечення високого рівня інформаційної безпеки. Знищення інформації, що зберігається на магнітних носіях, може здійснюватися за допомогою програмного стирання заданих файлів, фізичного знищення носія інформації або зміни магнітних характеристик робочого шару [5,10]. Слід зазначити, що виконання стандартної операції для операційної системи по стиранню заданого файлу не дає необхідного позитивного ефекту, оскільки при цьому знищується не як така інформація, а тільки посилання на неї в каталозі і таблиці розміщення файлів. Сама ж інформація, як і раніше знаходиться на жорсткому диску і може бути відновлена за допомогою спеціальних пристроїв, програм (утиліт). Фізичне знищення носія вимагає або достатніх часових ресурсів, або в ряді випадків (наприклад, знищення вибухом) може становити небезпеку для персоналу, що знаходиться поблизу. Значних енергетичних і часових витрат вимагає зміна магнітних характеристик робочого шару шляхом його перегріву вище точки Кюрі.

Сьогодні для екстреного знищення конфіденційної інформації доцільним видається спосіб, заснований на розмагнічуванні або намагнічуванні магнітного шару носія. Слід очікувати, що даний спосіб дозволить здійснити операцію зі знищення інформації в порівняно невеликому часовому проміжку, однак потребує створення досить сильних магнітних полів з амплітудами, зумовленими властивостями тонкоплівкових шарів магнітних носіїв інформації.

Актуальність проблеми щодо закриття каналів витоку інформації за допомогою екстреного знищення інформації, записаної на жорсткому диску, підтверджується вимогами наказів Міністра оборони України щодо загальних, спеціальних та технічних вимог до пристроїв знищення інформації з магнітних носіїв. Ці накази формують завдання щодо необхідності створення пристроїв знищення інформації з магнітних носіїв і їх сертифікації в системі сертифікації засобів захисту інформації Міністерства оборони України. Сьогодні науково-дослідним установам Міністерства оборони України ставиться задача щодо необхідності визначення раціональних тактико-технічних характеристик для вибору із існуючих або створення нових пристроїв знищення інформації з магнітних носіїв, а органам сертифікації та випробувальним акредитованим лабораторіям в системі сертифікації засобів захисту інформації МО України необхідно буде керуватися цими вимогами безпеки інформації при проведенні їх сертифікації. Актуальне завдання знищення інформації систем магнітного запису, що входять до складу персональних ЕОМ, визначило тему цієї статті, яка повинна дати рекомендації щодо ефективного, екстреного знищення секретної інформації на електронних носіях різними методами та пристроями.

Аналіз останніх досягнень і публікацій

Проведений аналіз останніх досягнень і публікацій [1–14] з даної тематики показує, що еволюція технологій забезпечення безпеки показує, що тільки концепція комплексного підходу до захисту інформації може забезпечити сучасні вимоги інформаційної безпеки [9]. Комплексний підхід має на увазі комплексний розвиток всіх необхідних методів і засобів захисту інформації.

До основних методів і засобів забезпечення інформаційної безпеки можна віднести: управління доступом – метод захисту інформації регулюванням використання всіх ресурсів системи (елементів баз даних, програмних і технічних засобів). Управління доступом включає наступні функції захисту: ідентифікацію користувачів, персоналу і ресурсів системи (привласнення кожному об’єкту персонального ідентифікатора); впізнання (встановлення автентичності) об’єкта або суб’єкта по ідентифікатору, що був ними пред’явлений; перевірку повноважень (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту); дозвіл і створення умов роботи в межах встановленого регламенту; реєстрацію (протоколювання) звернень до ресурсів, що захищаються; реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій; перешкода – метод створення фізичної перешкоди шляху зловмиснику до інформації, що захищається (до апаратури, носіїв інформації тощо); маскування – метод захисту інформації в каналах телекомунікацій шляхом її криптографічного закриття. Цей метод захисту широко застосовується як при обробці, так і при зберіганні інформації, в тому числі на магнітних дисках. При передачі інформації по каналах телекомунікацій на велику відстань цей метод є єдиним найбільш надійним. У вітчизняних комерційних системах цей метод використовується ще досить рідко через нестачу технічних засобів криптографічного закриття і їх високу вартість в даний час; регламентація – метод захисту інформації, що створює такі умови автоматизованої обробки, зберігання та передачі інформації, що захищається, при яких можливості несанкціонованого доступу до неї зводилися б до мінімуму; примус – такий метод захисту, при якому користувачі та персонал системи змушені дотримуватися правил обробки, передачі і використання інформації, що захищається під загрозою матеріальної, адміністративної або кримінальної відповідальності; спонукання – такий метод захисту, який спонукає користувача, і персонал системи, не порушувати встановлені правила шляхом дотримання сформованих моральних і етичних норм (як регламентованих, так і "неписаних"); знищення – метод захисту інформації від витоку шляхом її знищення при спробі викрадання (захоплення).

Розглянуті вище методи забезпечення інформаційної безпеки реалізуються на практиці з застосуванням різних засобів захисту, таких як технічні, програмні, організаційні, законодавчі та морально-етичні. Розглянемо основні засоби, що використовуються для створення механізмів захисту. Технічні засоби реалізуються у вигляді електричних, електромеханічних і електронних пристроїв. Вся сукупність технічних засобів поділяється на апаратні і фізичні. Під апаратними технічними засобами прийнято розуміти пристрої, що вбудовуються безпосередньо в телекомунікаційну апаратуру або пристрої, які сполучаються з подібною апаратурою по стандартному інтерфейсу. З найбільш відомих апаратних засобів можна відзначити схеми контролю інформації по парності, схеми захисту полів пам'яті по ключу тощо. Фізичні засоби реалізуються у вигляді автономних пристроїв і систем. Наприклад, замки на дверях, де розміщена апаратура, решітки на вікнах, електронно-механічне обладнання охоронної сигналізації, засоби фізичного знищення інформації, її носіїв тощо. Програмні засоби являють собою програмне забезпечення, розроблене спеціально для виконання функцій захисту інформації.

Зазначені вище засоби і становили основу механізмів захисту на першій фазі розвитку технології забезпечення безпеки зв’язку в телекомунікаційних каналах [1–7], при цьому вважалося, що основними засобами захисту є програмні. Спочатку програмні механізми захисту включалися, як правило, до складу операційних систем чи систем управління базами даних. Практика показала, що надійність подібних механізмів захисту є явно недостатньою. Особливо слабкою ланкою виявився захист паролем. Тому, в подальшому механізми захисту ставали все більш складними із залученням інших засобів забезпечення безпеки.

Організаційні засоби захисту являють собою організаційно-технічні та організаційно-правові заходи, що здійснюються в процесі створення і експлуатації телекомунікаційної апаратури для забезпечення захисту інформації. Організаційні заходи охоплюють всі структурні елементи апаратури на всіх етапах їх життєвого циклу (будівництво приміщень, проектування системи, монтаж і налагодження обладнання, випробування та експлуатація). Морально-етичні засоби захисту реалізуються у вигляді всіляких норм, які склалися традиційно або складаються в міру поширення обчислювальної техніки і засобів зв’язку в даній країні або суспільстві. Ці норми здебільшого не є обов’язковими, як законодавчі заходи, проте, недотримання їх веде зазвичай до втрати авторитету і престижу людини. Найбільш показовим прикладом таких норм є Кодекс професійної поведінки членів Асоціацій користувачів ЕОМ США. Законодавчі засоби захисту визначаються законодавчими актами країни, якими регламентуються правила використання, обробки та передачі інформації обмеженого доступу і встановлюються міри відповідальності за порушення цих правил. Необхідно також відзначити, що всі розглянуті вище засоби захисту діляться на формальні (виконують захисні функції суворо за заздалегідь передбаченою процедурою без безпосередньої участі людини) і неформальні (визначаються цілеспрямованою діяльністю людини, або регламентують цю діяльність).

В силу своєї специфіки інформація про можливі канали витоку і несанкціонованого доступу тривалий час була недоступна широкому користувачеві, що, безумовно, сприяло зростанню злочинних дій. Цілком очевидно, що для успішного захисту своєї інформації користувач повинен мати абсолютно ясну картину про можливі канали витоку, щоб відповідним чином зробити контрзаходи щодо припинення несанкціонованого доступу (посилити програмний захист, використовувати антивірусні програми, змінити алгоритм закриття, посилити контроль над носіями і виробничими відходами тощо). Основними шляхами несанкціонованого отримання інформації в даний час є: перехоплення електронних випромінювань; примусове електромагнітне опромінення (підсвічування) ліній зв’язку з метою отримання паразитної модуляції несучої; застосування підслуховуючих пристроїв (закладок); дистанційне фотографування; перехоплення акустичних випромінювань і відновлення тексту принтера; зчитування даних в масивах інших користувачів; читання залишкової інформації в пам’яті системи після виконання санкціонованих запитів; копіювання носіїв інформації з подоланням заходів захисту; маскування під зареєстрованого користувача; містифікація (маскування під запити системи); використання програмних пасток; використ-

тання недоліків мов програмування і операційних систем; включення в бібліотеки програм спеціальних блоків типу "троянський кінь"; незаконне підключення до апаратури та ліній зв'язку; навмисне виведення з ладу механізмів захисту; впровадження та використання комп'ютерних вірусів; викрадання носіїв інформації і виробничих відходів; інші шляхи несанкціонованого отримання інформації.

Проблема термінового і гарантованого знищення інформації, записаної на жорстких магнітних дисках, є в даний час дуже актуальною і привертає до себе підвищену увагу [4-14].

Ще більшої актуальності сьогодні набирає проблема гарантованого знищення інформації, записаної на жорсткому диску, набуває при вирішенні таких специфічних завдань: блокування доступу до важливої інформації, що знаходиться на "вінчестерах"; стирання важливої інформації без розтину пломб для передачі комп'ютерів в ремонт; стирання інформації з несправних "вінчестерів"; технічного забезпечення кур'єрського закритого зв'язку тощо.

Сучасний ринок пристроїв знищення інформації з магнітних носіїв пропонує вироби двох основних класів: утилізатори та інформаційні сейфи. Утилізатори дозволяють швидко і гарантовано стерти інформацію на великій кількості магнітних носіїв (у тому числі несправних). Інформаційні сейфи призначені для зберігання НЖМД і стирання інформації, що зберігається на них, причому інформація може бути стерта під час експлуатації НЖМД. Інформаційні сейфи можна класифікувати за такими ознаками як кількість робочих камер, спосіб електроживлення тощо.

У всіх випадках після прийняття рішення на ліквідацію важливої інформації завдання вирішує або оператор, або автоматика відповідно до закладеної логіки, причому, до технічних засобів пред'являються досить високі сучасні вимоги, такі як швидкість, надійність, безпека, автономність тощо, при цьому якість виконання рішення буде цілком залежати від якості ліквідатора і, в першу чергу, від методу ліквідації, що використовується [5, 7-10].

Постановка задачі та її розв'язання

Тому метою статті є аналіз та оцінка ефективності існуючих методів і засобів знищення інформації з магнітних носіїв як важливого елементу сучасної інформаційної безпеки з метою вироблення практичних рекомендацій щодо вибору найбільш ефективних та економічно вигідних методів та засобів знищення конфіденційної інформації в оборонній сфері.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів

Сьогодні вибір методу ліквідації інформації на магнітних носіях не є тривіальним і представляє досить складне багатокритеріальне завдання. Для підтвердження цього в табл. 1 наведені деякі результати порівняльного аналізу існуючих сьогодні методів ліквідації інформації на магнітних носіях [2, 5, 7, 8].

Одним із найбільш перспективним в сучасному світі є метод впливу магнітним полем. Цей метод дозволяє ліквідовувати пристрої з конфіденційною інформацією навіть на відстані, що є важливим фактором подальшого розвитку нових пристроїв, засобів та систем, які дозволяють це робити. Розмагнітити феромагнетик можна й іншим способом – помістити його в змінне магнітне поле, що повільно зменшується. Однак з НЖМД виникають труднощі, пов'язані з великою коерцитивною силою (залишкової намагніченістю) феромагнітного покриття диска. Отримання сильних стаціонарних полів в зазорах електромагнітів вимагає складних технічних рішень і великих енерговитрат [7, 13, 15]. Більш продуктивним є підхід, пов'язаний з намагнічуванням робочих поверхонь носія до максимально можливих значень (насичення) носія. Спосіб заснований на тому, що зовнішнє магнітне поле розглядається як аналог поля, створюваного магнітними головками НЖМД під час запису. Якщо характеристики зовнішнього поля будуть перевищувати напруженість поля, що створюється головками на таку величину, при якій відбудеться магнітне насичення матеріалу поверхні диска, то всі магнітні домени будуть переорієнтовані у напрямку цього зовнішнього поля, і вся інформація на жорсткому диску буде знищена.

Таблиця 1

Основні особливості сучасних методів ліквідації інформації на магнітних носіях

Методи ліквідації інформації	Принцип дії	Основні особливості	Примітки
Фізичні (впливу магнітним полем)	Неруйнівного перебудова структури намагніченості матеріалу робочої поверхні носія шляхом його розмагнічування або намагнічування до стану магнітного насичення	Використовується магнітне поле: постійне; змінне; імпульсне	Носій інформації не руйнується. Є можливість термінового і гарантованого знищення інформації
Програмні (типу BCWipe, Wipe info, Data Eraser, Acronis Proof Eraser, Sanitizer)	Реалізуються штатними засобами стирання запису в пристрої запису/відтворення інформації. Як правило, ліквідація інформації - "віртуальна"	Метод простий, але вимагає значного часу, надійність знищення невелика, спецзасоби відновлюють багаторазовий перезапис (до 5 шарів). Низька ціна і вартість експлуатації	Носій інформації не руйнується. Метод не забезпечує термінового і гарантованого знищення інформації. Метод безпечний для оператора
Механічні	Подрібнення носія, його руйнування механічною дією	Використовуються засоби: фізичного впливу; піротехнічні; вибухові речовини (ВР)	Носій інформації руйнується. Можливо гарантоване знищення. Є проблеми із забезпеченням безпеки оператора при використанні ВР. Висока вартість ТО
Термічні	Нагрівання носія до температури руйнування його основи	Використовуються засоби: електродугові; електроіндукційні; безкисневого горіння	Носій інформації руйнується. Гарантія знищення є. Перспективний метод безкисневого горіння
Хімічні	Руйнування робочого шару або основи носія хімічно агресивними середовищами	Наявність агресивних середовищ вимагає складних засобів контролю і забезпечення безпеки оператора	Носій інформації руйнується разом з інформацією. Складно забезпечити безпеку
Радіаційні	Руйнування носія іонізуючими випромінюваннями	Розрахунки показують необхідність використання високих рівнів іонізації	Носій інформації руйнується. Через великі дози опромінення ймовірність застосування малоймовірна
Інші методи, в тому числі, комбіновані	Знаходяться в процесі розробки, випробувань і впровадження	Дуже перспективні комбіновані методи, наприклад, термічні і впливу магнітним полем	Забезпечують як руйнування, так і збереження носіїв

Найбільшого поширення набули імпульсні намагнічуючі установки. Вони використовуються в більшості апаратних систем знищення інформації, що серійно випускаються і забезпечують: можливість створення сильних полів намагнічування з малими енергетичними витратами; короткочасність впливу імпульсного поля на зразок; можливість завантаження НЖМД цілком в камеру намагнічування; можливість застосування простих індукторних систем розімкнутого типу без магнітопровідника; формування магнітного поля необхідної спрямованості [1, 4, 7]. Сьогодні найбільшими можливостями реалізувати запропоновані вимоги до ліквідаторів інформації на

магнітних носіях мають методи фізичного впливу магнітним полем. У залежності від завдань, які вирішуються і конструктивних особливостей пристроїв екстреної ліквідації інформації з магнітних носіїв можуть бути стаціонарними, мобільними і портативними.

У табл. 2 наведені основні особливості подібних пристроїв ліквідації магнітних записів, що реалізують зазначені методи, а в табл. 3 наведені існуючі сьогодні на ринку засоби екстреного знищення інформації на електронних носіях.

Таблиця 2

Основні особливості сучасних пристроїв ліквідації магнітних записів

Тип пристроїв	Принцип дії	Особливості пристроїв	Примітка
SR 1, INCAS	Ручна протяжка магнітної мікрокасети між полюсами потужного постійного магніту	Для отримання стану магнітного насичення використовується сильне постійне магнітне поле. Пристрої мають просту конструкцію, не вимагають електроживлення, мають постійну готовність до роботи, малі габарити і вартість, однак, не забезпечують гарантованої якості стирання	Для габаритних носіїв високі рівні магнітного поля потребують вирішення завдань персонального та екологічного захисту. У цих пристроях можна зберігати носії, вони не забезпечують високої якості стирання інформації
РУ-2	Напівавтоматичний пристрій розмагнічування зі змінним магнітним полем, що плавно зменшується великої напруженості	Необхідна якість забезпечується високим енергоспоживанням, габаритами і вагою	Конструктивне виконання: стаціонарний пристрій з живленням від мережі 220 В
РУТЛ1	Як джерело магнітного поля використовується соленоїд, на який розряджається неполярний конденсатор	Під час стирання утворюються затухаючі коливання, істотно знижує залишкову намагніченість носія	Використання не полярних конденсаторів великої ємності не дозволяє істотно покращити масогабаритні характеристики
Garner HD-1 Professional Degausser	Магнітне поле, що періодично змінюється від позитивного до негативного значення, робить носій нейтральним, незалежно від характеру попереднього запису	Цей пристрій підтримує: швидке стирання (5с); збільшення відношення сигнал/шум; знищення всіх комп'ютерних вірусів на магнітних носіях	Виробник - Garner Products є світовим лідером в області ліквідації інформації з магнітних носіїв
“Стек”	Швидке знищення інформації з магнітних носіїв за рахунок їх намагнічування імпульсним магнітним полем певної величини і орієнтації	Метод реалізує максимальну з можливих енергетичну ефективність стирання з магнітних носіїв (можливість автономного електроживлення, компактність і т.п.)	Конструктивне виконання: в стаціонарному, мобільному і портативному варіантах, з живленням як від мережі, так і з автономним живленням

Таблиця 3

Засоби екстреного знищення інформації на електронних носіях

Флеш-накопичувач "EPOS eFlash-X" з можливістю знищення даних	
	Спеціалізований флеш-накопичувач EPOS eFlash-X забезпечує можливість екстреного знищення даних у разі загрози несанкціонованого доступу або фізичного захоплення накопичувача, для чого передбачений вбудований акумулятор.
Флеш-накопичувач "EPOS eFlash" з функцією знищення даних	
	Спеціалізований флеш-накопичувач EPOS eFlash з функцією гарантованого знищення даних призначений для забезпечення безпечного зберігання та транспортування конфіденційної інформації.
Пристрій миттєвого гарантованого знищення інформації на флеш-накопичувачах "Магма - 4"	
	Корпоративний утилізатор інформації «Магма-4» призначений для гарантованого знищення інформації на флеш-накопичувачах будь-якого обсягу, і забезпечує фізичне знищення елемента пам’яті і збереженої на ньому інформації.
Пристрій миттєвого гарантованого знищення інформації на картах пам’яті MicroSD "Магма-8"	
	Призначений для зчитування і екстреного знищення інформації на картах пам’яті MicroSD. Дані, які зберігалися в накопичувачі, відновленню не підлягають. Карта пам’яті непридатна для подальшої експлуатації.
Пристрій знищення інформації на FLASH- накопичувачах "Магма-4"	
	Пристрій "Магма-4" призначено для гарантованого знищення інформації на флеш-накопичувачах будь-якого обсягу, і забезпечує фізичне знищення елементу пам’яті і збереженої на ньому інформації. Дані, які зберігалися в накопичувачі, відновленню не підлягають. Підключення спеціалізованого flash-накопичувача до виробу "Магма-4" здійснюється способом підключення його до виділеного USB-2.0-порту.
Флеш носій "АБС EF V 2.0"	
	АБС EF є високошвидкісний USB пристрій для зберігання будь-якого типу інформації з можливістю миттєвого фізичного знищення носія разом з наявною на ньому інформацією. Дані, що містилися на носії, відновленню не підлягають.

Проведений методом експертного опитування порівняльний аналіз даних, наведених в табл. 1 - табл. 3 дозволив сформувати загальні оцінки пріоритетності використання в ЗС України різних методів та пристроїв знищення інформації на магнітних носіях станом на сьогодні та на перспективу (5-10 років). На рис. 1 проілюстровані кінцеві результати експертного опитування. Загальна оцінка формувалася за оцінками експертів за критеріями: простота реалізації; надійність знищення інформації; економічність засобів знищення інформації; часовий інтервал процесу знищення інформації; кількість людського ресурсу залученого до знищення інформації та обслуговування та контроль працездатності цих систем і засобів.

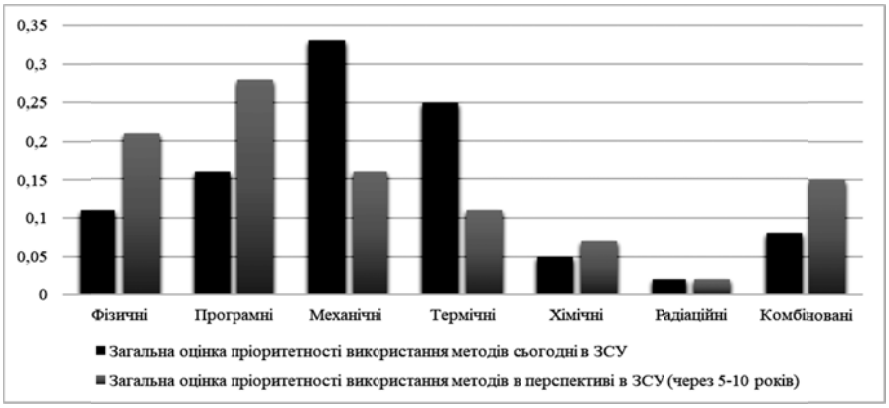

Рис. 1. Загальна оцінка пріоритетності використання методів в ЗС України

Результати аналізу показують, що для практичної реалізації пристроїв екстреної ліквідації інформації, записаної на жорстких магнітних дисках, в сучасних умовах розвитку ЗС України найчастіше сьогодні використовуються методи механічного та термічного знищення. На середньо-строкову перспективу вектор використання методів ліквідації носіїв інформації зміниться в бік методів фізичного впливу імпульсним магнітним полем та програмних методів. Необхідно відзначити, що незважаючи на зазначену вище актуальність цієї проблеми, сьогодні відповідний сектор ринку засобів забезпечення безпеки досить вузький, що пояснюється суперечливими вимогами, що пред'являються до подібних засобів. Основні вимоги, що пред'являються до сучасних пристроїв ліквідації магнітних записів, приведені в табл. 4.

Таблиця 4

Основні вимоги до сучасних пристроїв знищення інформації з магнітних носіїв

Основні вимоги до сучасних пристроїв знищення інформації з магнітних носіїв		
Експлуатаційні	**Спеціальні**	**Економічні**
час стирання габарити і маса пристрою тип енергоживлення споживана потужність безпека час напрацювання на відмову	неможливість визначення слідів інформативного сигналу неможливість гарантованого визначення ознак інформативного сигналу (для секретної інформації) неможливість визначення змісту повідомлення інші	ціна пристрою вартість технічного обслуговування можливість повторного використання носія можливість утилізації

Одним із найбільш розповсюджених методів та найбільш економічно вигідним є метод термічної дії на носії інформації. Термічний метод ґрунтується на одному з важливих ефектів магнетизму: при нагріванні феромагнетика до температури, що перевищує точку Кюрі, інтенсивність теплового руху атомів стає достатньою для руйнування його спонтанної намагніченості. Матеріал стає парамагнетиком [8, 13, 14]. При цій температурі феромагнітний матеріал робочого шару втрачає свою залишкову намагніченість, і всі сліди раніше записаної інформації знищуються. Температура, що відповідає точці Кюрі, для більшості феромагнітних матеріалів робочого шару носіїв інформації становить величину порядку декількох сотень градусів. При цьому треба враховувати, що кожен виробник НЖМД тримає в секреті шари основи і склад феромагнітного покриття. Найімовірніше, найбільш уразливими для температурних впливів компонентами робочого шару та основи НЖМД виявляться сполучні матеріали органічної природи. В цьому випадку при нагріванні до високих температур НЖМД вийде з ладу через плавлення елементів конструкції, що мають температуру плавлення або деформації менше точки Кюрі для даного магнітного носія.

Значним потенціалом щодо подальшого розвитку володіють програмні методи. Сьогодні вони активно використовуються та постійно розвиваються. Головною метою їх розвитку є знищення інформації на відстані. Усі програмні методи знищення інформації можна за ступенем надійності розділити на 3 рівні [1-14]:

Перший – найбільший простий та найчастіше застосовується для знищення інформації на НЖМД. Замість повного перезапису жорсткого диска в завантажувальний сектор, основну і резервну таблиці розділів записується послідовність нулів. Тим самим ускладнюється доступ до даних, що зберігаються на диску. Самі дані не знищуються. Повний доступ до інформації на НЖМД легко відновлюється за допомогою посекторного читання. Цей рівень забезпечує найбільшу швидкість, але не може використовуватися під час обробки інформації, витік якої небажаний.

Другий – запис послідовності нулів або одиниць в сектори, що містять інформація, яка знищується. Програмний доступ до перезапису даними неможливий. Однак існує можливість відновлення інформації після перезапису. В її основі лежить наявність залишкової намагніченості крайових областей дискових доріжок, що несе інформацію при попередніх записах. Для відновлення інформації, вилученої цим методом, можуть бути застосовані технології типу магнітної силової мікроскопії. Швидкість знищення інформації значно нижче, ніж в попередньому рівні, і визначається швидкістю роботи (а саме – швидкістю запису) НЖМД.

Третій – це використання декількох циклів перезапису інформації. Зі збільшенням числа циклів перезапису ускладнюється завдання відновлення видалених даних. Це обумовлюється природним дрейфом голівки запису НЖМД кожного наступного циклу. Імовірність перезапису крайових областей доріжок зростає. Отже, різко підвищується складність процесу відновлення знищених даних [9-14]. Повної гарантії незворотного руйнування інформації немає і в цьому випадку, оскільки програмно неможливо управляти траєкторією руху блоку головок НЖМД і процесом перемагнічування бітових інтервалів. Також знищення інформації ускладнено із-за складності оцінки факторів, що впливають на точність позиціонування голівок. Недоліком методів цього рівня є низька швидкість знищення інформації.

Сьогодні розроблено велику кількість рекомендацій, що визначають склад маскування послідовностей, що записуються в сектори даних при використанні методів різного рівня. В ідеальному випадку маскування послідовності повинно підбиратися таким чином, щоб перемагнітився кожен бітовий інтервал в запису максимальне число раз. Вибір методу знищення залежить від методу кодування інформації, що використовується на цільовому носії [5-7]. Вибір конкретного методу також залежить від рівня секретності інформації, що підлягає знищенню. У багатьох країнах існують державні стандарти, які регламентують склад і кількість проходів при знищенні інформації з НЖМД. Великою популярністю користується метод, визначений Міністерством оборони США. Відповідно до цього методу повинний бути виконаний триразовий перезапис інформації: запис в кожен байт перезаписуваної області випадково обраного байта; запис в кожен байт перезаписуваної області доповнення до нього; запис в перезаписуваної області послідовності випадково вибраних байт. Цей метод носить довільний характер і не враховує особливостей роботи конкретних НЖМД. Міністерство оборони США визнає цей факт і при знищенні інформації вищої категорії секретності забороняє використання програмних методів [1, 5]. В Україні на сучасному етапі не існує сертифікованого державними органами методу програмного знищення інформації з магнітних носіїв, що дозволяє знизити рівень конфіденційності носія. Мінімальні рекомендації щодо вибору методу наводяться в документах, які регламентують ці процеси в МО України сьогодні.

Крім методів, визначених державними стандартами, існує цілий ряд методів, запропонованих незалежними експертами в області інформаційної безпеки. Найбільш поширеними з них є два методи – Б. Шнайдера і П. Гутмана [1-7].

Шнайдер запропонував метод знищення інформації, що складається з семи проходів: перші два – запис одиниць і нулів відповідно, і останні п'ять – запис випадкових даних. Однак ні кількість проходів, ні вибір маскування послідовностей необґрунтовані. Замість цього Шнайдер залишає наступне

повідомлення: "Останні дослідження Національного інституту стандартів і технологій, виконані за допомогою електронних тунельних мікроскопів, показали, що навіть цього може бути недостатньо. Тобто, якщо ваші дані досить цінні, можна вважати, що їх повне видалення з магнітного носія неможливо. Спаліть носій або зітріть його в порошок. Дешевше купити новий носій, ніж втратити ваші секрети" [1-7].

Обґрунтування вибору маскування послідовностей методом Гутмана показує, що метод складається з 27 проходів, орієнтованих на знищення записів, закодованих методами MFM і різними поширеними модифікаціями RLL [1-4]. Маскування послідовностей підібрано таким чином, щоб забезпечити максимально можливе число перемикань знаку намагніченості кожного бітового інтервалу. Це значно ускладнює відновлення перезаписаних даних, оскільки робить нетривіальним роздільне зчитування накладених один на одного записів. У різних накопичувачах можуть застосовуватися різні методи кодування (наприклад, в сучасних жорстких дисках MFM- і RLL-кодування в чистому вигляді не використовується). Детальні специфікації методів, які застосовуються для конкретних видів накопичувачів, в загальному випадку недоступні. Тому до складу методу додані 8 проходів з випадковою послідовністю (4 на початку і 4 в кінці). Метод Гутмана не має великих практичних переваг перед методами, описаними раніше. Практично, будь-який НЖМД, вироблений після 1997 року, використовує різні модифікації PRML, специфікації яких тримаються виробником в секреті [14].

Однією із незахищених видів інформації є інформація, яка зберігається в оперативній пам'яті. Всупереч традиційної, «очевидної» думки, дані, які зберігаються в момент відключення живлення комп'ютера, в схемах оперативної пам'яті (RAM) не зникають зовсім, а деяким чином зберігаються, як мінімум до наступного включення живлення. Такого ефекту мають схеми обох відомих типів, як статичні (SRAM), так і динамічні (DRAM), але, звичайно, статичні схеми набагато більш показові в цьому відношенні. Ранні чіпи типу SRAM могли зберігати образи даних в осередках протягом декількох днів. Взагалі, можливе створення схем пам'яті, які можуть тримати інформацію як завгодно довго, і навіть після включення живлення з функцією подальшого перезапису всього поля. Щось на кшталт «перезаписуваної ROM». Ця ідея могла б привести до створення комп'ютера, який зовсім не потребував би завантаження при включенні: просто миттєво відновлювалася б конфігурація системи, що була при останньому відключенні живлення, як ніби вмикається освітлення. Сьогодні надійних рішень такого роду для масових застосувань поки не впроваджено, є часткові випадки реалізації, але серійного виробництва немає. Якщо додатково з'являються вимоги щодо очищення оперативної пам'яті – це передбачає дворазовий запис довільних даних в звільнену область пам'яті, раніше використану для зберігання даних, що захищаються. Таким чином, досягається неможливість читання збережених раніше в області оперативної пам'яті даних при виділенні її іншому користувачеві або програмі (процесу).

Схеми типу DRAM теж можуть зберігати образи минулих діянь, але інакше у порівнянні зі схемами SRAM. Це зовсім не заряди, які зберігаються в осередках схеми, а деякі електронні образи, закарбовані в оксидних (окислових) шарах мікросхем під впливом електричних полів, доданих до активних елементів. Цікаво те, що ефект запам'ятовування значною мірою залежить від тривалості часу стану. Тобто якщо перед вимиканням комп'ютер перебуватиме тривалий час без дії, то ймовірність тривалого збереження інформації в RAM буде істотна. В принципі, ефекти залишкового збереження інформації тестуються будь-яким з виробників схем пам'яті, але для масового користувача дані тестів не публікуються. Більш того, в звичайній комп'ютерній системі просто неможливо активувати спеціальні режими, що забезпечують тестування мікросхем на цей ефект і зчитування залишкових даних. Проте, це цілком можливо і в потрібних випадках застосовується. Найпростішим, але досить небезпечним методом повного руйнування даних в схемах оперативної пам'яті є їх легке нагрівання. Підвищення температури мікросхеми на 140°С в порівнянні з температурою навколишнього середовища – повністю знищує будь-які залишки відображеної інформації. Для гарантій результату цього акту його тривалість має становити кілька годин. І навпаки, якщо хочеться зберегти дані в мікросхемах, їх потрібно помістити в термостат, встановивши температуру

не вище, ніж 60°С. Це дозволить зберігати залишкові дані в мікросхемах не те що дні або години, але *(навіть)* тижні. Простий повторний перезапис даних в схемах пам'яті RAM не має такої ефективності, яка можлива при знищенні даних на магнітних носіях. Справа в тому, що накладання електричних полів до оксидів не позбавляє їх пам'яті попередніх станів. Власне, мова йде про те, що з плином часу зі зростаючою безліччю минулих станів зменшується ймовірність збереження колишніх станів. Зрозуміло, що в звичайному режимі напруга, що йде до мікросхеми однакова. А тому вплив напруги для створення протилежного значення осередку протягом, наприклад, кількох мікросекунд не викличе істотних змін в стані оксидів активного елементу. Таким чином, для того щоб повністю стерти залишкові дані в мікросхемі, її слід піддавати термічній дії при максимально можливій температурі. Але це веде до різкого зниження надійності її функціонування та скорочення терміну загальної працездатності.

Багато програмних засобів з ліквідації інформації в оперативній пам'яті, засновані на методі багаторазового перезапису даних, що зачищає сектори оперативної пам'яті. Це процес, як згадувалося раніше, не дозволяє здійснити повне знищення інформації, але дозволяє зробити її недоступною при виділенні місця роботи іншому користувачеві або програмі (процесу). Деякі програми передбачають аналіз очищеної області оперативної пам'яті на можливість відновити з неї знищені дані. Висновок, який випливає з вищевикладеного, парадоксальний: для того щоб більш надійно знищити дані в пам'яті RAM, їх потрібно міняти якомога рідше, а для того щоб їх надійно і безпечно зберігати, потрібно їх оновлювати якомога частіше. Згідно з експериментальними даними, зберігання даних в осередку протягом однієї секунди практично не виявляє ефекту залишкового зберігання, одна хвилина дає достатню ймовірність визначення, а 10 хвилин майже повну ймовірність визначення даних. Таким чином, ефективним рішенням для не відновлення даних з мікросхем є постійна зміна станів осередків для того щоб образи не зберігались в оксидах. Цей метод, непридатний в загальному вигляді, може застосовуватися до деяких зон оперативної пам'яті, в яких зберігаються особливо чутливі дані, наприклад, ключі шифрування [11, 14].

Висновки

Проведений у статті аналіз та оцінка ефективності існуючих методів і засобів знищення інформації з магнітних носіїв як важливого елементу сучасної інформаційної безпеки дозволяє спеціалістам з визначеної галузі досліджень виробити ряд практичних рекомендацій щодо вибору найбільш ефективних та економічно вигідних методів та засобів знищення конфіденційної інформації. Також викладений матеріал дозволяє сформувати погляди спеціалістів в сфері оборони щодо прийняття рішень: по вибору найбільш перспективних методів знищення конфіденційної інформації; зберігання такого роду інформації; вибору засобів її знищення та захисту; формування вимог до надійності знищення інформації; розроблення переліку документів, які повинні регламентувати ці питання в сфері оборони тощо.

Перспективи подальших досліджень

Перспективи подальшого розвитку способів (методів) та пристроїв знищення інформації з магнітних носіїв цілком визначаються перспективами використання на практиці цих носіїв. Відомо, що в процесі розвитку суспільства змінилося вже досить велика кількість видів носіїв інформації (пергамент, папір, дріт, стрічки, диски, карти тощо). Крім того, один і той же конструктив може використовуватися різними технологіями запису, наприклад, диски можуть бути магнітними, перфорованими, лазерними тощо. У серйозній конкурентній боротьбі різні види носіїв здобувають перемогу і стають своєрідним стандартом. Зараз технічні засоби інформаційної безпеки, зокрема, засоби ліквідації інформації з магнітних носіїв, постійно удосконалюються, вбираючи в себе останні досягнення сучасних технологій безпеки. Розширюється їх модельний ряд, що враховує різноманітність вимог Замовника, таких як тип енергоживлення, рівень мобільності, надійності і умов експлуатації. Усе це зумовлює актуальність тематики досліджень за цим напрямком в майбутньому.

Список використаних джерел

1. Hansen F. and Oleshchuk V.: Conformance Checking of RBAC Policy and its Implementation, The First Information Security Practice and Experience Conference, – ISPEC2005, Singapore, LNCS, Volume 3439, 2005. 144-155 p. DOI: https://doi.org/10.1007/978-3-540-31979-5_13.

2. Mueller S. Upgrading and Repairing PCs, 13th Edition. Indianapolis: Que. 2002.

3. Industrial Security Manual for Safeguarding Classified Information. Department of Defense Manual, DoD 5220.22. M. 1987.

4. Levy S.V., Ostrovski A.S., Agalidi Ju.S. Magnetic field topographical survey by magnetooptical spatial-time light modulators. SPIE Proceedings, 1993. 142–146 p.

5. Menezes A.J., Oorschot P.C., Vanstone S.A. Handbook of applied cryptography. N.Y.: CRC Press, 1996. 780p.

6. Mueller S. Upgrading and Repairing PCs, 13th Edition. Indianapolis: Que, 2002. 1556 p.

7. Антология: Информационная безопасность офиса. Технические средства защиты информации. Вып.1. Киев: ТИД «ДС». 2003.

8. Барсуков В.С. Чтобы сохранить информацию, ее необходимо уничтожить! Специальная техника. 2001. № 6.

9. Беседин Д.И., Боборыкин С.Н., Рыжиков С.С. Предотвращение утечки информации, хранящейся в накопителях на жестких магнитных дисках. Специальная техника. 2001. № 1.

10. Рохманюк В.М., Фокин Е.М. Аппаратура экстренного уничтожения записей на магнитных носителях. БДИ. 2009. № 5.

11. Рохманюк В.М., Фокин Е.М. Шредер для винчестера. PCWEEK/RE. 2000. № 39.

12. Барсуков В.С. Современные технологии безопасности. М.: Нолидж, 2000.

13. Боборыкин С.Н. Оценка эффективности средств уничтожения информации, хранящейся в накопителях на жестких магнитных дисках. Спец. техника. 2001. № 3.

14. Гордиенко И. Уничтожение данных. Практический подход.: https://www.ferra.ru/review/computers/s25303.htm.

АНАЛИЗ И ОЦЕНКА МЕТОДОВ И СРЕДСТВ УНИЧТОЖЕНИЯ ИНФОРМАЦИИ С МАГНИТНЫХ НОСИТЕЛЕЙ КАК ЭЛЕМЕНТА СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

О.М. Семененко, Ю.Б. Добровольский, Р.В.Лукаш, В.Л. Коверга,О.М. Сеченев

В статье проведен анализ и оценка эффективности существующих методов и средств уничтожения информации с магнитных носителей как важного элемента современной информационной безопасности с целью выработки практических рекомендаций по выбору наиболее эффективных и экономически выгодных методов и средств уничтожения конфиденциальной информации в оборонной сфере.

Ключевые слова: *информационная безопасность; уничтожение информации; эффективность уничтожения информации; магнитный носитель информации; магнитное поле; жесткий диск; оперативная память.*

ANALYSIS AND ASSESSMENT OF METHODS AND MEANS OF DESTRUCTING INFORMATION FROM MAGNETIC MEDIA AS AN ELEMENT OF MODERN INFORMATION SECURITY

O. Semenenko, Y. Dobrovolsky, V. Koverga, O. Sechenev

Evolution of security technologies shows that only the concept of an integrated approach to information security can provide modern information security requirements. A comprehensive approach means the complex development of all the necessary methods and means of information protection.

Today, the information exchange and information systems in the Ministry of Defense of Ukraine have certain means and approaches to the destruction of information, but each of them has different estimates of the effectiveness of their use, as well as different cost of their purchase and use. Therefore, the main purpose of the article is to carry out a comprehensive analysis of means of destroying confidential information of methods of its destruction in order to formulate practical recommendations for choosing the most effective and economically feasible for the Ministry of Defense of Ukraine.

The perfection of methods and means of destroying information from magnetic media is an important element of modern information security. The results of the analysis carried out in the article are the disclosure of the main features of modern devices for the elimination of magnetic records, as well as the ability to formulate a list of basic requirements for modern devices for the destruction of information from magnetic media.

Today, technical means of information security, in particular, the elimination of information on magnetic media, are constantly being improved, absorbing the latest advances in modern security technologies. Their model range, which takes into account the diversity of customer requirements, such as the type of energy supply, the level of mobility, reliability and operating conditions, expands. All this determines the relevance of research topics in this direction in the future.

Key words: *information security; destruction of information; the effectiveness of the destruction of information; magnetic storage media; a magnetic field; HDD; RAM.*