Kasuj do końca

OPROGRAMOWANIE | Przedstawiamy darmowe aplikacje służące do zamazywania danych. Cechą wspólną tych programów jest skuteczność na ogół wystarczająca, abyśmy mogli trwale usunąć poufne dane z naszego dysku. Podpowiadamy także, kiedy i jak możemy zrobić to „domowymi" sposobami.

Szymon Piłat, Kamil Kulesza

Usuwanie danych w tradycyjny sposób z reguły nie jest efektywne – zwyczajne kasowanie plików z dysku nie oznacza bowiem usunięcia ich zawartości. Procedura kasowania pliku polega na zapisaniu informacji o tym, że sektory, w których on się znajdował, są od tej chwili wolne i system może w tym miejscu zapisywać nowe dane. Natomiast fizycznie informacje pozostają na nośniku – tak długo aż system faktycznie nie zapisze w danym miejscu nowych danych. Wciąż mamy też dostęp do nazwy skasowanego pliku, a w najgorszym razie utracimy informację o pierwszym jej znaku.

Także formatowanie dysku nie jest skutecznym sposobem na zamazywanie danych. Operacja ta sprowadza się do utworzenia pustego systemu plików (w tym tablicy alokacji plików) oraz zapisania sektora startowego. Opcjonalnie system podczas formatowania sprawdza, czy poszczególne sektory dysku są czytelne. Same dane pozostają jednak nienaruszone.

Należy tu jeszcze wspomnieć o innym sposobie kasowania plików – funkcji „wyrzucania do kosza", dostępnej choćby w systemie Windows. Polega ona na przeniesieniu pliku do specjalnego folderu, a ujmując rzecz dokładniej, sprowadza się do zmiany wpisu w tablicy alokacji plików, natomiast sam plik pozostaje fizycznie w tym samym miejscu. Nawet „opróżnienie kosza" niczego nie załatwia, ponieważ dane fizycznie wciąż pozostają na nośniku. Podsumowując – ani wyrzucenie pliku do kosza, ani jego opróżnienie, ani formatowanie dysku nie powodują usunięcia zawartości pliku.

Niebezpieczne *slack spaces*

Jak wspomnieliśmy, plik po usunięciu pozostaje czytelny aż do zapisania w danym miejscu nowych informacji. Niestety, nawet jeśli system zapisze nowy plik w miejsce starego, poprzednik i tak może nie zniknąć. Część starego pliku nadal będzie dostępna w tzw. *slack spaces*, czyli w miejscach na dysku między końcem pliku a końcem klastra (bloku). Rozmiar klastra dla systemu NTFS wynosi domyślnie 4 kb. Jeżeli więc zapiszemy plik o wielkości 1 kb, to pozostałe 3 kb w klastrze pozostają nienaruszone. Jeśli w tym samym klastrze znajdował się wcześniej inny plik, to 3 kb tego pliku nadal można odczytać. Na dyskach z systemem FAT klaster ma rozmiar nawet 256 kb, co oznacza, że w obrębie *slack spaces* może pozostać wiele danych (mimo że już dawno je usunęliśmy i w tym samym miejscu zapisaliśmy inne pliki).

Pionier kasowania

Jak widać, opisane metody usuwania plików nie należą do skutecznych. Potrzebujemy więc programów, które potrafią efektywnie usunąć dane. Procedura działania takich aplikacji jest bardzo prosta: w miejscu, w którym znajdował się plik, są zapisywane nowe informacje (przypadkowe sekwencje bitów lub z góry ustalone wzorce). Mówimy wtedy o nadpisywaniu danych – jedno- lub wielokrotnym. I tu rodzi się pytanie: jakie dane nadpisywać na pliku, aby na pewno nie dało się go odzyskać? Okazuje się, że nie ma to znaczenia. Niemniej jednak, w ostatnich latach problem trwałego kasowania danych nabrał takiego znaczenia, że istnieje dziś co najmniej kilka standardów i zaleceń dotyczących tego, jak powinno wyglądać właściwe usuwanie plików (patrz: **ramka „Standardy kasowania danych"**).

Jednym z pionierów idei skutecznego kasowania danych jest Peter Gutmann. Stworzony przez niego algorytm to jedno z najgoręcej dyskutowanych rozwiązań. Praca Gutmanna (**www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html**) nie jest jednak wolna od krytyki. Najciekawszy z zarzutów mówi o tym, że zaproponowane przez naukowca 35-krotne nadpisywanie danych jest działaniem dalece na wyrost, ponieważ nawet jednokrotne nadpisanie pliku niszczy go na zawsze. Szansę na jego odzyskanie mają jedynie odpowiednio wyspecjalizowane służby, dysponujące bardzo nowoczesną technologią (*intelligence agencies*), co czyni koszt takiej operacji bardzo wysokim (takimi kwotami dysponują jedynie rządy państw). W raporcie opublikowanym w 2006 roku *Tutorial on Disk Drive Data Sanitization* Gordon Hughes z Center for Magnetic Recording Research oraz Tom Coughlin z Coughlin Associates stwierdzają, że wielokrotne nadpisywanie danych nie jest bardziej skuteczne od czynności tej wykonanej jednokrotnie. Innymi słowy, jednorazowe nadpisanie danych dowolnym ciągiem bitów jest całkowicie bezpieczne.

FOT. SZ. PIŁAT

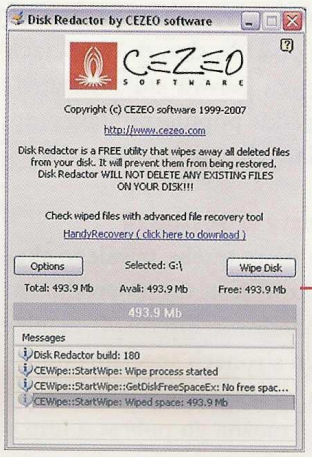
Nieosiągalne usuwanie

Biorąc pod uwagę te informacje, warto zadać pytanie, jakie są przesłanki do wielokrotnego zamazywania danych? Należy zacząć od tego, że zapis na dyskach twardych jest w istocie analogowy, patrząc więc na tę operację od strony praw fizyki, jednokrotne nadpisanie danych pozostawia wiele śladów oryginalnego pliku. Czynność ta, nawet powtórzona dwa razy, nie powinna stanowić przeszkody w odzyskaniu danych, jeśli do tego zadania użyjemy mikroskopu sił atomowych i wiedzy z zakresu analizy szeregów czasowych. Tą argumentacją posłużył się również sam Gutmann. Być może więc jego wybiegający w przyszłość postulat 35-krotnego nadpisywania danych można uznać za metodę bezpieczną. Nie zmienia to jednak faktu, że nie pozostaje ona w zasięgu przeciętnego użytkownika komputera, a co najwyżej *well funded intelligence agencies*, o której wspomniał Gutmann.

Niezależny Darik's Boot and Nuke

Wydaje się więc, że użycie ogólnodostępnych programów do kasowania może okazać się całkowicie bezpieczne i wystarczające. Spośród kilkudziesięciu narzędzi tego typu dostępnych w Sieci wybraliśmy kilka wartych polecenia – prezentujemy je w **tabeli „Programy do zamazywania danych"**.

Na szczególną uwagę zasługują programy działające niezależnie od systemu operacyjnego. Mogą być one szczególnie przydatne na przykład wtedy, gdy laptop zmienia właściciela. Przed reinstalacją systemu operacyjnego dane należy trwale usunąć. Aby zrobić to we właściwy sposób, powinniśmy wyciągnięty z laptopa dysk podłączyć do innego komputera – wtedy będziemy mogli zamazać wszystkie dane. Gdy jednak jest to kłopotliwe, pomocne są aplikacje działające niezależnie od systemu operacyjnego. Wart polecenia jest Darik's Boot and Nuke – program dostępny w postaci pliku ISO, który możemy zapisać na CD, DVD lub pamięci flash.



Disk Redactor pozwala skutecznie skasować wskazany folder. Niestety, gdy za jego pomocą zamażemy zawartość całego dysku, nazwy plików da się odzyskać.

Z tak przygotowanego bootowalnego nośnika możemy uruchomić komputer i wykonać czyszczenie całej zawartości dysku. Nie ma przy tym znaczenia, jaki system plików znajdował się na nośniku. Mamy pewność, że zostały skasowane również dane z początkowych sektorów dysku, takie jak np. MBR, tablica partycji, tablica alokacji plików (a więc usunięte zostają także informacje o nazwach plików, co nie zawsze >>

Programy do zamazywania danych

Program	Eraser 5.86a	Active@ KillDisk 5.0	Sure Delete 5.1.1	Darik's Boot and Nuke .0.7	File Shredder 2.0	Disk Redactor build 170	PC Inspector e-maxx 1.0
http://www.	heidi.ie/	killdisk.com/	wizard-industries.com/	dban.org/	fileshredder.org/	cezeo.com/	pcinspector.de/
Licencja	Freeware	Freeware	Freeware	Freeware	Freeware	Freeware	Freeware
Obsługiwane algorytmy niszczenia							
1-/2-/wielo-przebiegowy	nie/nie/nie	tak/nie/nie	nie/nie/nie	tak[3]/nie/nie	tak/tak/tak	tak/tak/nie	bd./bd./bd.
DoD/Guttman	tak/tak	nie[1]/nie[1]	tak/nie	tak/tak	tak/tak	nie/nie	bd./bd.
GOST/VISTR	nie/nie	nie[1]/nie[1]	nie/nie	nie/nie	nie/nie	nie/nie	bd./bd.
pseudolosowy/inne	nie/tak	nie/nie[1]	nie/tak[2]	nie/tak	nie/nie	nie/nie	bd./bd.
Obsługiwane systemy plików							
FAT16/FAT32	nie/tak	tak/tak	tak/tak	tak/tak	nie/tak	nie/tak	tak/tak
NTFS/inne[4]	tak/tak	tak/nie	tak/nie	tak/tak	nie/tak	nie/tak	tak/tak
Opis programu							
	Niewielki, ale za to bardzo dobry program do zamazywania danych. Ma duże możliwości konfiguracyjne.	Pozwala na niskopoziomowe kasowanie zawartości dysku. Umożliwia usunięcie danych ze *slack spaces*.	Narzędzie można uruchmić w dwóch trybach kasowania: całych dysków lub wybranych zbiorów. Niestety aplikacja jest niedopracowana.	Oprogramowanie działa niezależnie od systemu operacyjnego (uruchamia się je z płyty bootowalnej). Polecamy do kasowania dysku przed sprzedażą.	Łatwa w użyciu aplikacja o intuicyjnym interfejsie. Pozwala również na zamazanie nieużywanej części dysku.	Program pozwala skutecznie skasować wskazany folder. Niestety, gdy za jego pomocą zamażemy zawartość całego dysku, nazwy plików da się odzyskać.	Aplikacja do pobrania w postaci obrazu ISO lub „instalki", która przygotuje nam dyskietkę pozwalającą na niszczenie plików.

Legenda: bd. - brak danych; 1) – opcja dostępna wyłącznie w wersji płatnej aplikacji; 2) – algorytm o nazwie „Super Secure"; 3) – algorytm „Quick Erase"; 4) – systemy uniksowe lub płyty CD-RW/DVD-RW

>> jest oczywiste w przypadku programów działających pod Windows). W opcjach tej dostępnej za darmo aplikacji znajdują się wszystkie popularne algorytmy kasowania danych.

SDelete prosty w obsłudze

Nieobojętny na potrzebę trwałego skasowania plików jest także producent systemów Windows. Microsoft zamieścił na swoich stronach specjalny dodatek, którego zadaniem jest zamazywanie danych – można go pobrać z **http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx** (twórcą i właścicielem praw do SDelete jest Mark Russinovich). Warto mieć to narzędzie na uwadze – jest ono nadzwyczaj proste w obsłudze. Program spełnia podstawowe wymagania: kasuje pliki, nadpisując je zgodnie ze standardem DOD 5220.22-M, potrafi zamazać zawartość całego dysku lub tylko wolnej przestrzeni. Sdelete to pojedynczy plik wykonywalny, który uruchamia się z wiersza poleceń. Jak zaznacza jego twórca, SDelete kasuje jedynie zawartość plików – po jego użyciu możliwe jest nadal odtworzenie nazwy pliku. Program działa pod Windows 95, 98, NT 4.0, 2000 oraz XP.

Dysk musi działać

Specjalistyczne programy do kasowania danych są skuteczne przy spełnieniu jednego, zdawałoby się oczywistego, warunku: otóż dysk, z którego usuwamy pliki, musi być sprawny. Jeśli nie mamy pewności, że „twardziel" pracuje poprawnie, a są na nim zapisane poufne dane, to należy zastosować magnetyczne i/bądź mechaniczne usuwanie danych.

Nie tylko Windows

Do kasowania danych dla systemów Unix i Linux służą programy Wipe (**http://wipe.sourceforge.net/**) oraz srm (**http://srm.sourceforge.net/**). Obecnie w prawie każdej dystrybucji Linuksa znajduje się także polecenie *shred*, za pomocą którego można trwale zamazać dane. *Shred* (podobnie jak Wipe i srm) działa z linii komend i domyślnie 25-krotnie nadpisuje plik (można tę liczbę redefiniować).

W przypadku systemów uniksowych należy jednak pamiętać o dodatkowych ograniczeniach (w mniejszym stopniu ma je również Windows). Wspomniane narzędzia działają przy założeniu, że system nadpisuje plik tam, gdzie pierwotnie był on fizycznie zapisany. Oznacza to, że zamazywanie plików może nie być skuteczne, jeśli na dysku znajduje się system plików z księgowaniem (*journaling*), np. XFS, etx3, ReiserFS (do wersji 10.2 był to domyślny system plików w systemach Novella: SUSE Linux i OpenSUSE). Usuwanie plików nie będzie trwałe w systemach, które zapisują dane w tymczasowych lokalizacjach (np. NFS w wersji 3). Oczywiście – i to dotyczy wszystkich systemów operacyjnych – należy pamiętać, że zamazywanie danych nie jest efektywne tam, gdzie mamy do czynienia ze sprzętową redundancją, np. w dyskach macierzy RAID. Dzięki redundancji – sprzętowej czy na poziomie systemu plików – możliwe jest odzyskanie skasowanych danych.

Jak odzyskać dane

Odzyskiwanie danych jest działaniem przeciwstawnym do ich kasowania. Jest to zadanie nieporównywalnie bardziej skomplikowane, nawet, gdy poprzestaniemy na wykorzystaniu ogólnodostępnych programów do odzyskiwania danych przeznaczonych do użytku w warunkach domowych czy stosowanych w dziale informatycznym urzędu lub firmy.

Uszkodzenia fizyczne a logiczne

Większość z takich aplikacji ma szansę skutecznie działać tylko wtedy, gdy dysk nie jest fizycznie uszkodzony. „Twardziele" z niesprawną elektroniką czy uszkodzoną głowicą odczytu/zapisu wymagają operacji, które z reguły są poza zasięgiem przeciętnego użytkownika. Innym rodzajem uszkodzeń fizycznych są *bad sectors*, czyli nieczytelne obszary dysku. Odzyskanie zawartych tam danych jest trudne, ale bardzo często możliwe.

Uszkodzenia logiczne polegają na nieprawidłowym zapisaniu informacji o plikach. Przykładem może być sytuacja, w której informacje o położeniach dwóch różnych plików wskazują na te same sektory dysku. Uszkodzenia logiczne wynikają z nieprawidłowego działania systemu operacyjnego, działalności wirusów itd. – jednak sam dysk pozostaje sprawny. Z tego punktu widzenia przypadkowe skasowanie pliku lub sformatowanie „twardziela" możemy traktować jako logiczną utratę danych – fizycznie informacje prawdopodobnie nadal istnieją. W takich sytuacjach możemy skorzystać z programów do odzyskiwania danych.

Dwa sposoby

Ważne jest, aby dysk, z którego odzyskujemy dane był podłączony do innego komputera niż ten, w którym pracował jako dysk systemowy. Na „twardzielu", z którego odzyskujemy dane, nie można zapisywać żadnych plików – każda operacja zapisu zmniejsza nasze szanse na przywrócenie ważnych informacji. Po podłączeniu dysku do komputera można albo od razu rozpocząć odzyskiwanie danych, albo najpierw wykonać obraz dysku i z niego przywracać dane.

Obraz dysku

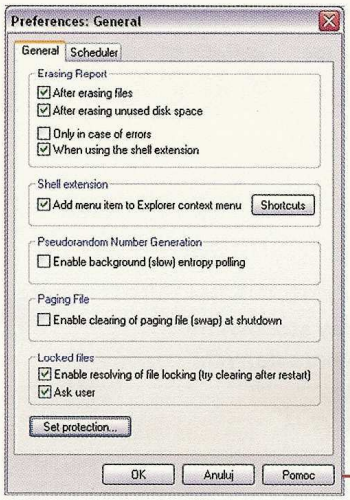
Sposób drugi – czyli odzyskiwanie danych z wykonanego obrazu – jest lepszy i to z kilku powodów. Po pierwsze – nie ryzykujemy, że jakiś program (lub omyłkowo my sami) zapisze dane na dysku, z którego odzyskujemy dane, i przez to zmniejszą się szanse na przywrócenie plików. Po drugie – czasem kłopoty z dyskiem oznaczają, że jest on uszkodzony i być może zdoła popracować jeszcze tylko kilka godzin. Jeżeli nie wykonamy obrazu i zaczniemy odzyskiwać dane bezpośrednio z dysku, możemy się liczyć z tym, że nośnik nagle przestanie działać i wtedy pozostanie nam już tylko zgłoszenie się do firmy profesjonalnie zajmującej się odzyskiwaniem danych.

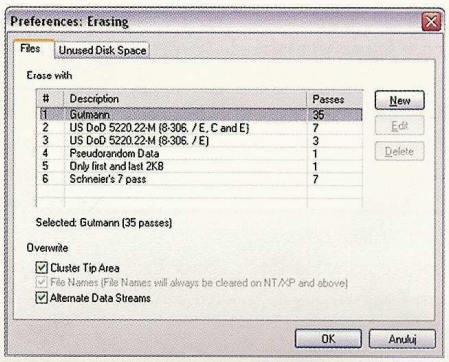
Obraz dysku możemy wykonać za pomocą powszechnie dostępnych narzędzi. Najłatwiej mają użytkownicy systemów

Zrób to sam

Może się zdarzyć, że musimy trwale usunąć dane, a nie mamy pod ręką odpowiedniego programu. Najprostszym „domowym" sposobem na skuteczne zamazanie informacji jest wypełnienie dysku innymi danymi, np. dużymi plikami AVI. Wprawdzie jesteśmy wtedy narażeni na to, że dane pozostaną w *slack spaces*, ale biorąc pod uwagę wielkość plików AVI (kilkaset MB) i maksymalną wielkość pojedynczej *slack space*, jest to ryzyko niezwykle małe. Trzeba jednak zaznaczyć, że tą „domową" metodą w wielu przypadkach możemy nie skasować informacji o nazwach plików.

Zamazywanie danych jest proste, jeśli pracujemy w systemie uniksowym. Wtedy kasowanie możemy przeprowadzić za pomocą polecenia *dd*, np. wpisując (jako administrator): *dd if=/dev/random of=/dev/hda*. W ten sposób możemy trwale usunąć całą zawartość dysku twardego lub innego nośnika. Co więcej, odpowiednia składnia tego polecenia pozwala nam na usunięcie danych zgodnie z algorytmem Gutmanna, Scheninera, GOST, NAVSO lub VSITR. Ponadto wykorzystanie polecenia *dd* z jakiejkolwiek dystrybucji Linuksa w wersji *live* pozwala nam na kasowanie informacji w podobny sposób, jak czyni to program Darik's Boot and Nuke, tj. niezależnie od tego, jaki system operacyjny (i czy w ogóle) jest zainstalowany w komputerze.





Eraser kryje w sobie duży potencjał. Pozwala skorzystać ze **zdefiniowanych i tworzyć własne algorytmy kasowania**.

Jednak formatowanie

Wspomnieliśmy, że formatowanie dysku nie narusza zapisanych na nim danych. Jednak w piątej wersji systemu MS-DOS 5.0 w poleceniu *format* pojawiła się nieudokumentowana opcja */U*, która sprawia, że system zamazuje cały obszar danych zerami. A więc formatowanie z opcją */U* skutecznie usuwa dane z dysku. Funkcja ta dostępna jest we wszystkich wersjach systemu operacyjnego Windows łącznie z Windows Vista. W najnowszej wersji Windows pojawiła się udokumentowana opcja pozwalająca na zamazanie danych *–/P*. Umożliwia >>

uniksowych, którzy wykonają obraz dysku za pomocą polecenia *dd*. Narzędzie to ma swoje ograniczenia, ale jest to funkcja darmowa i znajduje się standardowo w każdej dystrybucji. Nieco większe możliwości daje użycie polecenia *ddrescue*.

Obraz dysku pracującego pod systemem Windows możemy wykonać, korzystając z takich aplikacji jak WinDD (odpowiednik linuksowego *dd*), SelfImage, Dubaron DiskImage (darmowa, ale tylko do użytku osobistego) lub pakietu Forensic Acquisition Utilities (darmowy, do użytku osobistego i komercyjnego na zasadach *Open Licence*). Jest też wiele płatnych narzędzi – niestety często ich cena jest bardzo wysoka – od kilkudziesięciu do kilkuset dolarów.

Analiza odczytanych danych

Po wykonaniu obrazu przystępujemy do odzyskiwania danych. Podstawową metodą służącą do tego celu jest skanowanie danych na dysku (skanowanie obrazu dysku) w poszukiwaniu informacji charakterystycznych dla określonego rodzaju pliku np. nagłówków, a następnie wyodrębnieniu ich spośród innych. Właśnie w ten sposób działa większość programów. Jednak dostępne aplikacje często nie radzą sobie z tym zadaniem, jeśli plik jest położony w różnych miejscach na dysku (jest pofragmentowany). Należy dodać, że odzyskiwanie danych jest operacją bardzo czasochłonną i znacznie obciąża system.

Do koloru, do wyboru

Najskuteczniejsze i jednocześnie najprostsze w obsłudze programy służące do odzyskiwania danych działające pod systemem Windows to: EasyRecovery, R-Studio, PC Inspector File Recovery, Recover My Files. Większość z nich jest płatna. Spośród darmowych narzędzi warto polecić R-Linuksa, który odzyskuje dane z dysków linuksowych (niestety, jedynie z systemów ext2). Także użytkownicy Uniksa i Linuksa mają w czym wybierać. Skuteczne i dostępne za darmo są m.in. Foremost, pakiet The Coroner's Toolkit (licencja IBM Public License) czy pakiet The Sleuth Kit. Możliwości analizy danych dwóch ostatnich pakietów wykraczają znacznie poza same odzyskiwanie. Dostępne są również programy wyspecjalizowane w przywracaniu określonych rodzajów plików, takich jak na przykład PhotoRec (dla plików graficznych, klipów wideo i innych dokumentów).

Każdy z programów cechuje się inną skutecznością, w zależności od rodzaju plików, które odzyskujemy. Efektywność działania tych narzędzi zależna jest także od systemu plików, jaki jest lub był na dysku. Tak więc, kiedy naszym zadaniem jest przywrócenie danych na skalę masową, warto przeprowadzić własne testy dostępnego oprogramowania i wybrać aplikacje, najlepiej odpowiadające warunkom, w których działamy. Czas poświęcony na właściwe przygotowanie warsztatu pracy i przetestowanie narzędzi na pewno nie jest stracony, o czym mieliśmy okazję przekonać się osobiście, prowadząc badania nad masowym odzyskiwaniem danych z używanych dysków (patrz: artykuł na str. 17). •

Standardy kasowania danych

Programy kasują dane na trzech poziomach – określonych zgodnie z normami dotyczącymi bezpowrotnego usuwania danych. Profesjonalne aplikacje spełniają uwarunkowania zdefiniowane w Instrukcji o ochronie informacji Departamentu Obrony Stanów Zjednoczonych, jednym z najbardziej restrykcyjnych dokumentów tego typu.

Poziom początkowy (poziom 0)
Najprostsza, najszybsza i często stosowana forma usuwania danych polegająca na niszczeniu części informacji poprzez formatowanie lub kasowanie, ewentualnie usunięcie danych o partycjach. Na tym poziomie dane na dysku nie są niszczone – natomiast dostęp do nich jest utrudniony. Można go jednak odzyskać za pomocą specjalnego oprogramowania przeprowadzającego analizę sektorów dysku (Norton DiskEdit, WinHex).

Poziom 1
Na dysku dokonywany jest zapis ciągu zer albo jedynek do sektorów danych, który niszczy nie tylko obszar ładowania, ale również i informacje. Wykorzystanie tej metody uniemożliwia odzyskanie danych poza profesjonalnym laboratorium. Teoretycznie odtworzenie plików jest jednak nadal możliwe.

Poziom 1+
Poziom ten wymusza wykorzystanie kilku cykli zapisu ponownego. Użycie tej metody praktycznie eliminuje możliwość odzyskania danych.

Algorytmy stosowane w kasowaniu danych:

DoD 5220.22-M
Jeden z najpopularniejszych standardów usuwania plików opracowany w 1995 roku przez Departament Obrony Stanów Zjednoczonych. Polega na nadpisaniu danych dowolnym ciągiem danych, następnie jego odwrotnością i ponownie dowolnym ciągiem. Jest to więc proces trójprzebiegowy. Niekiedy w ustawieniach programów do kasowania plików można znaleźć nowszą, siedmioprzebiegową wersję tego algorytmu.

Algorytm Gutmanna
Opracowany w 1996 roku przez Petera Gutmanna, naukowca pracującego wówczas w Department of Computer Science na University of Auckland. Algorytm ten został opublikowany w pracy, w której Gutmann opisuje fizyczne podstawy zapisu danych na nośnikach magnetycznych. Zaproponowana przez naukowca metoda skutecznego usuwania informacji polega na 35-krotnym ich nadpisaniu odpowiednio przygotowanymi sekwencjami bitów (w tym w ośmiu przypadkach powinny być to wartości losowe)

Algorytm Schneinera
Jego autorem jest Bruce Schneiner – amerykański kryptograf i specjalista od bezpieczeństwa informacji. Algorytm jest dużo mniej popularny niż ten opracowany przez Gutmanna. Z siedmiu przebiegów w tym algorytmie jeden zawiera same jedynki, drugi – same zera, a pięć pozostałych to dane losowe.

GOST P50739–95
Rosyjski algorytm napisany w 1995 roku polegający na dwóch przebiegach nadpisywania: najpierw zapisuje się tylko zera, następnie dane losowe.

NAVSO P-5239–26
Algorytm amerykański występujący w dwóch odmianach w zależności od kodowania bitów na dysku twardym (RLL lub MFM). NAVSO P-5239–26 jest trójprzebiegowy.

VISR
Niemiecki algorytm z 1999 roku przewiduje trzy cykle nadpisywania: zerami, jedynkami, a następnie naprzemiennie zerami i jedynkami.

>> ona także zdefiniowanie, ile razy dane mają być nadpisane. Pod Vistą działa również opcja */U*.

Złe sektory

Jak widać, mamy do dyspozycji całą gamę środków pozwalających skutecznie skasować pliki. Wiemy też, że aby tego dokonać, najczęściej wystarczy już jednokrotne nadpisanie danych.

Trzeba jednak podkreślić pomimo tych optymistycznych wniosków, że zawsze może istnieć ryzyko pozostawienia danych na dysku. Nawet użycie kilku z przedstawionych programów może w pewnych okolicznościach nie wystarczyć. Przykładem może być tu choćby sytuacja, gdy na dysku znajdują się uszkodzone sektory (*bad sectors*), które podczas zamazywania danych zostaną pominięte bez informowania o tym użytkownika. Kilka lub kilkanaście megabajtów „złych" sektorów na naszym „twardzielu" może zawierać dużą ilość poufnych danych. A odczytanie informacji z uszkodzonych sektorów wcale nie jest trudne.

Możliwe jest też celowe zaznaczanie pewnych sektorów jako nieczytelnych, tak aby system operacyjny nie próbował na nich niczego zapisywać. W konsekwencji znajdujące się tam dane wciąż pozostają nieusunięte. A jest to tylko jeden z wielu możliwych scenariuszy.

Czy oznacza to, że jedynym sposobem na skasowanie poufnych danych jest wrzucenie dysku do pieca hutniczego? Teoretycznie tak. Wszystko jednak zależy od tego, co chcemy ukryć przed światem, a także – jaką siłą i środkami dysponuje nasz potencjalny wróg. Chodzi o znalezienie rozwiązania kompromisowego, odpowiedniego dla naszej sytuacji. Na ogół wystarczy po prostu skorzystać z dostępnych programów do kasowania danych. Koszt odzyskania nawet jednokrotnie nadpisanych danych jest bardzo wysoki, więc musiałyby być one naprawdę niezwykle cenne, aby użycie aplikacji do usuwania plików okazało się niewystarczającym środkiem ochronnym.

Szymon Piłat jest studentem Wydziału Fizyki Uniwersytetu Warszawskiego. Od kilku lat zajmuje się m.in. analizą sygnałów oraz problematyką bezpieczeństwa i odzyskiwania danych. W opisywanym w artykule projekcie pełnił funkcję lidera grupy.

Kamil Kulesza jest adiunktem w Instytucie Badań Systemowych PAN oraz pracownikiem naukowym University of Cambridge. W swojej pracy badawczej zajmuje się zagadnieniami związanymi z informatyką i zastosowaniami matematyki, ze szczególnym uwzględnieniem bezpieczeństwa informacji. Jest też zaangażowany w Letnie Praktyki Badawcze PAN od momentu ich powstania.