

## Ile razy nadpisywać dysk?

<http://ipsec.pl/kryptografia/2009/ile-razy-nadpisywac-dysk.html>

Programowe metody nadpisywania nośników danych są najbardziej rozpowszechnioną metodą stosowaną do niszczenia informacji zapisanej na dyskach twardych, pamięciach USB i innych popularnych nośnikach.

W popularnych narzędziach takich jak <http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx> czy <http://www.truecrypt.org/> zaimplementowane jest to przy pomocy wielokrotnego nadpisywania nośnika zmiennymi sekwencjami. Liczba przebiegów nadpisywania wynosi od jednego aż do trzydziestu paru. Ta ostatnia wartość została podana w 1996 roku przez nowozelandzkiego kryptologa Petera Gutmanna jako jedyna w pełni gwarantująca trwałe usunięcie danych.

Tymczasem Craig Wright z SANS w artykule <http://sansforensics.wordpress.com/2009/01/15/overwriting-hard-drive-data/> przekonuje, że w przypadku współczesnych dysków twardych w zupełności wystarczy jednokrotne nadpisanie nośnika aby odzyskanie informacji było w praktyce całkowicie niemożliwe.

Wright argumentuje, że techniki odzyskiwania danych takie jak mikroskopia sił magnetycznych (MFM) opisywane np. przez Gutmanna mogły mieć zastosowanie do informacji zapisanej na nośnikach niskiej gęstości - na przykład na dyskietkach. W przypadku współczesnych dysków twardych gęstość zapisu i probabilistyczne techniki konwersji gęsto upakowanych wartości analogowych na dane cyfrowe powodują, że prawdopodobieństwo odtworzenia porcji danych większych niż jeden bit szybko maleje z każdym kolejnym bitem długości (prawdopodobieństwo poprawnego odtworzenia pojedynczego bajtu wynosi około 1

Całkowicie błędne jest przekonanie - twierdzi Wright - że przy pomocy mikroskopu elektronowego można odczytać gigabajty danych z dysku, w którym dane zostały nadpisane choćby raz, czy to celowo czy przez zajęcie miejsca po skasowanych plikach.