УДК 004.056.53(043.2)

Кульбачинський О.І.
Національний авіаційний університет, Київ

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ОСОБИСТИХ ДАНИХ КОРИСТУВАЧА ШЛЯХОМ НАДІЙНОГО ВИДАЛЕННЯ ЗАЛИШКОВОЇ ІНФОРМАЦІЇ

При роботі за комп'ютером засоби операційної системи та прикладних програм фіксують дії користувача та зберігають їх, як тимчасову інформацію. Так браузери зберігають історію відвідувань сайтів, cookie, тимчасові файли в кеші, паролі для доступу до веб-сайтам. У системному реєстрі Windows зберігаються списки додатків, що запускались, результати пошуку, інформація про підключені мережеві диски і зовнішні пристрої, відомості про роботу різноманітних встановлених програм. Операційна система веде масу журналів (лог-файлів): журнали Windows Update, подій Windows, брандмауера Windows, журнали WMI, діагностики та Центру безпеки. Різноманітна персональна і навіть конфіденційна інформація запросто може потрапити в dat-файли, що містять інформацію про аварійне завершення Windows, в файли підкачки, в файл гібернації та в буфер обміну. Коли жорсткій диск потрапляє до чужих рук, ця, так звана залишкова інформація, може стати відомою будь кому. Тому важливим є захист особистої інформації користувача шляхом видалення та приховання залишкових даних.

Коли йдеться про видалення зрозуміло мається на увазі не звичайне передбачене в Windows видалення файлів і папок, а знищення інформації за допомогою спеціальних програмних або апаратних засобів. Справа в тому, що видалення файлу засобами операційної системи не забезпечує його реального знищення. Видаляється не тіло файлу, а тільки його заголовок; кластери, в яких він був записаний, позначаються як порожні, і можуть бути прочитані до тих пір, поки не будуть перезаписані. Більше того, можливо, що і після перезапису кластерів в частині з них збережуться дані з видаленого раніше файлу.

Тому надійне знищення інформації на носії ведеться зазвичай або шляхом багаторазового перезапису інформації, або шляхом знищення носія інформації. Для програмного знищення інформації пропонується величезна кількість програм-шредерів, що використовують різні алгоритми стирання даних і характеризуються різними надійністю і швидкодією. Проведений порівняльний аналіз цих програм показує, що рівень секретності, що забезпечується шредером, визначається вибраним алгоритмом і числом проходів – при збільшенні кількості проходів ступінь надійності видалення інформації підвищується і одночасно збільшуються часові витрати. При цьому аналізувалися алгоритми, як визначені державними стандартами, так і від незалежних експертів у галузі інформаційної безпеки.

Для захисту особистих даних користувача потрібно слідкувати за залишковою інформацією, що зберігається на носію, забезпечувати надійне їх знищення, здійснювати перезапис вільних кластерів для гарантування безповоротного знищення всіх даних, що раніше містилися в них. Тоді при можливості зловмисником спроби несанкціонованого доступу чи заволодінні носієм, ризик порушення конфіденційності персональних даних користувача значно знизиться.

Науковий керівник – В.Г.Павлов, к.т.н., доц.