УДК 004.56.5

Ю. Купчак, В. Муж
Тернопільський національний технічний університет імені Івана Пулюя

МЕТОДИКА БЕЗПЕЧНОГО ЗБЕРІГАННЯ ІНФОРМАЦІЇ НА ЦИФРОВИХ НОСІЯХ

UDC 004.56.5

Y. Kupchak, V. Muzh
(Ternopil Ivan Pului National Technical University, Ukraine)

METHOD OF SECURITY STORAGE OF INFORMATION ON DIGITAL MEDIA

На сучасному етапі розвитку людства, неабияким питанням є реалізація можливості безпечного зберігання інформації будь-якої важливості, без великих затрат коштів та часу. Питання захисту інформації з використанням цифрових носіїв визначається поширенням видів контролю доступу, інформаційних, ідентифікаційних, біометричних та інших систем, а також окремих прикладних програм, які використовують цифрові носії як засіб зберігання і обробки персональних даних користувачів комп'ютерних систем.

Виходячи з вищесказаного, для усіх сфер діяльності людини, методика безпечного зберігання та використання інформації, що належить до державних інформацій ресурсів чи інформації з обмеженим доступом, на цифрових носіях є актуальним питання, вирішення якої дозволить підвищити безпеку інформації від несанкціонованого доступу та дій, що можуть призвести до її випадкової або умисної модифікації чи знищення, унеможливити передачу та/або розголошення конфіденційної інформації шляхом неконтрольованого ознайомлення чи копіювання. В той же час, забезпечити безвідмовний доступ до інформації особам, які мають на це право[1].

З цього приводу варто звернути увагу на способи безпечного зберігання інформації на цифрових носіях та впровадження методики безпечного зберігання критичної інформації на цифрових носіях, а саме на флеш-накопичувачах (типу USB, SD, SSD та ін.). За результатами неодноразових експерементальних досліджень виявлено актуальність використання програмних засобів шифрування, а саме: «TrueCrypt», «VeraCrypt» та «BitLocker», які можуть працювати спільно з 32-х і 64-х розрядною операційною системою із закритим вихідним кодом - Microsoft Windows[3].

Шифрування може здійснюватися за такими алгоритмами як: AES, Serpent, Twofish, Camellia, а також комбінацією даних алгоритмів. Використовуються криптографічні гешфункції «RIPEMD-160», «SHA-256», «SHA-512» та «Whirlpool». Можливості даних програм дозволяють легко працювати із зашифрованими віртуальними дисками, видаляти, створювати, записувати дані, а також створювати окремі розділи, що сприяє безпечній роботі з інформацією [2].

Запропонована методика зберігання та використання критичної інформації на носіях інформації, за допомогою шифрування програмним засобом, дозволить:

1 забезпечити цілісність, доступність та конфіденційність інформації;
2 унеможливити (значно ускладнити) несанкціонований доступ до критичної інформації;
3 зменшити економічні та часові витрати.

Висновком даної роботи є те, що на сьогоднішній день є доволі значна кількість програмних засобів, які дозволяють забезпечити конфіденційність, цілісність та доступність інформації, однак залишаються проблеми ліцензування, експертизи та сертифікації таких програмних засобів в Україні.

Література

1. https://zakon.rada.gov.ua
2. https://habr.com/en/