ISSN 1996-1588

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ


# Наукові праці Донецького національного технічного університету Серія: “Інформатика, кібернетика та обчислювальна техніка”

**№2 (23) 2016**

**Покровськ – 2016**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

# Наукові праці
Донецького національного технічного університету

# Серія: “Інформатика, кібернетика та обчислювальна техніка”

Всеукраїнський науковий збірник

Заснований у травні 1996 року

Виходить 2 рази на рік

***№2 (23)’ 2016***

**Покровськ – 2016**

**УДК 004.3+004.9+004.2+51.7+519.6+519.7**

Публікується згідно з рішенням Вченої ради ДВНЗ «Донецький національний технічний університет» (протокол № 5 від 17.11.2016).

Збірник містить наукові статті співробітників ДонНТУ та інших навчальних і наукових закладів України, які є науковими партнерами ДонНТУ. Публікації висвітлюють результати наукових досліджень і розробок в таких напрямках, як інформатика, чисельні методи, паралельні обчислення, програмування, розробка засобів обчислювальної техніки, дослідження комп'ютерних мереж, машинна графіка і обробка зображень, математичне моделювання в різних галузях. Матеріали збірника призначені для наукових співробітників, викладачів, інженерно-технічних працівників, аспірантів та студентів.

**Засновник та видавець** – Донецький національний технічний університет (ДонНТУ)

***РЕДАКЦІЙНА КОЛЕГІЯ:***

Д-р техн. наук, проф. Є.О. Башков (головний редактор); член-кореспондент НАН України, д-р техн. наук, проф. В.П. Боюн; д-р техн. наук, проф. В.А. Святний; д-р техн. наук, проф. О.А. Дмитрієва; д-р техн. наук, проф. Ю.О. Скобцов; д-р техн. наук, проф. О.О. Баркалов; д-р наук, доц. Тянев Димитр Стоянов; д-р техн. наук, проф. С.Д. Погорілий; д-р техн. наук, проф. О.Н.Романюк; д-р техн. наук, доц. Є.Є. Федоров; канд. техн. наук, доц. Н.С. Костюкова (відп. секретар випуску); канд. техн. наук, доц. С.М. Вороной; канд. техн. наук, доц. С.А. Зори.

**Адреса редакції**: 85300, м. Покровськ, пл. Шибанкова, 2, ДонНТУ.
Тел.: (06239) 2-09-38. E-mail: kostyukova_ns@mail.ru

Збірник зареєстровано в Державному комітеті інформаційної політики, телебачення та радіомовлення України. Свідоцтво: серія КВ, №7374 від 03.06.2003.

Збірник включено до переліку наукових фахових видань України, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук (наказ Міністерства освіти і науки України №261 від 6 березня 2015 р.)

© Автори статей, 2016
ISSN 1996-1588 © ДВНЗ «Донецький національний технічний університет», 2016

УДК 004.457

К.С. Гайдук, студент
О.Г. Шевченко, ст. викладач
Донецький національний технічний університет, Україна
e-mail: ukrdonntu@gmail.com

# Відновлення доступу до зашифрованих даних в ОС Windows

*У статті розглянуті проблеми втрати доступу до даних, зашифрованих файловою системою EFS ОС Windows. Проаналізовано причини відсутності можливості отримання зашифрованої інформації. Розглянуто механізми захисту звернення до таких даних. Запропоновано алгоритм, що дозволяє відновити втрачений доступ до зашифрованих даних користувача.*

***Ключові слова: шифрувальна файлова система, EFS, профіль користувача, відновлення даних, EFS Profile Recovery.***

## *Вступ*

У сучасному світі інформація, мабуть, є одним з найцінніших ресурсів. Її пошкодження або втрата може привести до величезних матеріальних і моральних збитків. При цьому, в захисті конфіденційних даних можуть мати потребу не тільки державні та військові відомства і служби, а й будь-які організації, незалежно від їх масштабу і роду діяльності. Отримання третіми особами доступу до такої інформації як перелік співробітників, їх контактні і паспортні дані, список ділових партнерів, відомості бухгалтерії та інше, може нашкодити як організації в цілому, так і її співробітникам зокрема.

Операційна система Windows дозволяє користувачам захищати особисті та конфіденційні дані за допомогою їх шифрування, надаючи такі криптографічні інструменти як EFS (Encrypting File System) і BitLocker.

EFS є надбудовою над файловою системою NTFS, що реалізує прозоре шифрування окремих файлів та каталогів. EFS має досить складну багаторівневу архітектуру і використовує сучасні алгоритми шифрування, що при нинішньому розвитку обчислювальної техніки робить криптоаналіз даних, зашифрованих за допомогою даної системи, практично неможливим [1]. В ОС Windows 7 архітектура EFS була розширена за рахунок включення підтримки еліптичної криптографії, завдяки чому вона стала відповідати вимогам, які пред'являються стандартом Suite B Агентства національної безпеки США, що робить допустимим використання EFS для захисту інформації в державних установах [2].

Одним з недоліків EFS є неможливість шифрування системних файлів, тому що їх розшифровка на етапі завантаження операційної системи неможлива [3]. Цього недоліку позбавлена система BitLocker, яка, на відміну від EFS, виконує шифрування не окремих об'єктів файлової системи, а логічних розділів, і працює не на рівні драйвера NTFS, а на рівні диспетчера томів, перехоплюючи всі операції введення-виведення за допомогою драйвера-фільтра FVE (Full Volume Encryption). У разі використання BitLocker, навіть наявність необмеженого доступу до фізичного накопичувача може виявитися мало корисною при криптоаналізі, якщо необхідні криптографічні ключі були збережені в енергонезалежній пам'яті криптопроцесора специфікації TPM (Trusted Platform Module) або на USB-накопичувачі [4].

Нажаль, незалежно від використовуваної системи шифрування, у ряді випадків самі легітимні користувачі можуть втратити доступ до своїх даних, що може бути викликано різними причинами, - як об'єктивними, так і суб'єктивними. Парадоксальним в подібних випадках є те, що сама інформація може бути абсолютно непошкодженою, але отримати її не представляється можливим. Тому поряд з питанням безпеки інформації необхідно вирішувати і зворотну задачу - реалізацію санкціонованого доступу до даних в нештатних ситуаціях.

## *Постановка задачі та актуальність*

Доступ до зашифрованих за допомогою EFS даних може бути втрачений з низки причин, серед яких: перевстановлення операційної системи, видалення профілю користувача, скидання пароля користувача, некоректний перенос користувача в інший домен, несправність фізичного накопичувача та ін.

Існуючі програми відновлення доступу до EFS-даних, такі як Advanced EFS Data Recovery [5], Diskinternals EFS Recovery [6], EFS Recovery [7] та EFS Key [8], дозволяють розшифрувати дані за умови, якщо необхідні файли ключів будуть знайдені на диску (також може знадобитися знання пароля користувача, який виконав шифрування файлу), з подальшим збереженням розшифрованих файлів в зазначений каталог. Перевагою вказаних програм є їх відносна універсальність (можливість застосування, незалежно від причини втрати доступу). Проте необхідність розшифровки файлів на етапі відновлення доступу може вважатися недоліком цих засобів, оскільки прихована інформація стає явною та потребує повторного шифрування.

З урахуванням вищесказаного, представляється актуальною розробка програми відновлення доступу до EFS-даних у разі видалення профілю користувача, шляхом відновлення облікового запису і відповідного каталогу профілю користувача, разом з колишніми криптографічними ключами, що позбавляє від необхідності розшифровки файлів на етапі відновлення доступу.

### *Механізм EFS*

Дані файлу шифруються за допомогою одного з симетричних алгоритмів, таких як DES, 3DES, DESX, AES. При цьому, розрізняють алгоритм, що використовується за умовчанням, а також певну кількість альтернативних доступних в системі алгоритмів. Починаючи з Windows XP SP1, алгоритмом за замовчуванням є AES . Ключ шифрування, використовуваний в даному випадку, називається File Encryption Key (FEK), і створюється за допомогою генератора випадкових чисел при шифруванні файлу. У свою чергу, FEK шифрується за допомогою одного з алгоритмів асиметричного шифрування (RSA або ECC ), після чого зберігається в атрибуті $EFS файлу, що шифрується [9,10].

Пара ключів (публічний та приватний), що використовується асиметричним алгоритмом шифрування для захисту FEK, генерується при виконанні користувачем першої операції шифрування, або при виклику вбудованої утиліти cipher.exe з параметром /K [11]. Публічний ключ користувача зберігається в незашифрованому вигляді у файлі сертифіката (С). Приватний ключ (ПК) захищається шляхом шифрування за допомогою майстер-ключа (МК) користувача, сформованого на основі паролю користувача, після чого зберігається в файлі приватного ключа. Майстер-ключ захищається шляхом шифрування за допомогою сесійного ключа, що генерується вбудованою утилітою syskey.exe, після чого зберігається у файлі майстер-ключа. Варто відзначити, що, в дійсності, у файлах приватного ключа і майстер-ключа, зберігаються не самі зашифровані ключі, а лише окремі байтові масиви, необхідні для формування ключів [12,13]. Розташування файлів ключів у каталозі профілю користувача наведено в табл. 1. Абревіатурою SID (Security Identifier) в таблиці позначено ідентифікатор безпеки користувача, який умовно можна поділити на дві частини: номер машини (перша частина ідентифікатора – однозначно визначає локальний комп'ютер) та відносний ідентифікатор користувача (RID, Relative Identifier), що визначає користувача у межах хосту [9,14].

Якщо після шифрування файлу, доступ до нього необхідно надати іншому користувачеві, то FEK також шифрується за допомогою відкритого ключа відповідного користувача. В результаті, формується множина зашифрованих примірників FEK (за кількістю користувачів, що мають доступ до файлу, включаючи користувача, який виконав шифрування), що утворює поле розшифровки даних - Data Decrypt Field (DDF).

У тому випадку, якщо в системі призначені агенти відновлення (користувачі, уповноважені виконувати розшифровку файлів, зашифрованих іншими користувачами), FEK також шифрується за допомогою публічного ключа кожного агента відновлення, в результаті чого формується поле відновлення даних - Data Recovery Field (DRF) [9].

DDF і DRF складаються з так званих елементів ключів. Кожен елемент ключа, в числі іншого, містить наступну інформацію про користувача: ім'я, SID, відбиток сертифіката (хеш сертифіката, що співпадає з ім'ям файлу сертифіката), ім'я контейнера (ідентифікатор приватного ключа). SID вказується тільки для користувача, який виконав шифрування файлу - тобто, для користувача, зазначеного в першому елементі поля DDF.

Якщо профіль користувача був видалений, а потім заново створений (нехай навіть з колишнім ім'ям користувача і паролем), всі ключі системою будуть згенеровані заново, і RID користувача буде також іншим. Як наслідок, заново створений користувач не матиме доступу до своїх раніше зашифрованих файлів. Якщо перед видаленням профілю не був виконаний експорт сертифіката користувача, не було призначено агента відновлення, або не була створена контрольна точка відновлення системи, то відновити доступ до зашифрованих файлів без допомоги стороннього програмного забезпечення неможливо.

Таблиця 1 - Розташування файлів ключів у каталозі профілю користувача.

| Тип файлу ключа | Шлях |
|---|---|
| Файл сертифіката | %USERPROFILE%\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates |
| Файл приватного ключа | %USERPROFILE%\AppData\Roaming\Microsoft\Crypto\RSA\<SID> |
| Файл майстер-ключа | %USERPROFILE%\AppData\Roaming\Microsoft\Protect\<SID> |

### *Алгоритм програми EFS Profile Recovery*

Алгоритм програми EFS Profile Recovery складається з двох етапів, кожний з яких, в свою чергу, складається з декількох кроків (рис. 1).

На першому кроці першого етапу виконується сканування системного логічного диску з метою пошуку видалених файлів ключів та їх подальшого відновлення. Пошук необхідних файлів здійснюється на підставі наступних критеріїв:

– наявність у файлу атрибута "системний";

– довжина імені файлу;

– відповідність імені файлу заданому шаблону;

– стан кластерів тіла атрибута $DATA (виділені / не виділені);

– наявність в тілі файлу певних байтових послідовностей, прийнятих за сигнатури.

Формат імені кожного типу файлів ключів фіксований, що робить можливим їх пошук на підставі знання довжини та шаблону імені файлу (табл. 2).

Якщо файл видалений, проте кластери, що відповідають тілу атрибута $DATA, позначені як виділені, це свідчить про те, що дані видаленого файлу вже перезаписані, і не підлягають відновленню.

В якості сигнатури в тілі файлу майстер-ключа було прийнято ім'я файлу майстер-ключа, розмір і зміщення якого відносно початку файлу наведені в табл. 3 [15]. В якості сигнатур файлів сертифікатів і приватних ключів були прийняті символьні послідовності, вказані в табл. 3.

Всі знайдені файли ключів відновлюються в окремий каталог програми.

Таблиця 2 – Формати імен файлів ключів.

| Тип файлу ключа | Довжина імені в символах | Шаблон (регулярний вираз) |
|---|---|---|
| МК | 36 | [0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12} |
| С | 40 | [0-9A-F]{40} |
| ПК | 69 | [0-9a-f]{32}_[0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12} |

На другому кроці першого етапу виконується пошук зашифрованих файлів у вказаному користувачем каталозі. Результатом виконання кроку є формування двох списків: списку зашифрованих файлів і списку облікових даних, добутих з атрибутів $EFS (рис. 2). Під обліковими даними мається на увазі множина, що включає в себе ім'я користувача, який виконав шифрування файлу, його SID, відбиток сертифіката, а також ім'я контейнера.

На рис. 2 показано, що кілька файлів можуть бути зашифровані одним користувачем (User1@PC1), але з використанням різних сертифікатів (відбиток 1.1, відбиток 2.1). Також показано, що збіг локальних імен користувачів ще не гарантує того, що файли зашифровані одним і тим же користувачем - файл міг бути зашифрований віддаленим користувачем: імена локального і віддаленого користувачів можуть збігатися, однак хости і SID будуть відмінними (на рисунку - користувачі User1@PC1 і User1@PC2). Варто відзначити, що ім'я користувача та ім'я хоста можуть змінюватися, в той час як SID користувача змінюватися не може - таким чином, User1@PC1 і User2@PC1.1 - це один і той же користувач. Якщо ім'я хосту було змінено, то при шифруванні файлів в атрибуті $EFS буде вказуватися нове ім'я хосту. Однак, якщо було змінено ім'я користувача, то при шифруванні буде використовуватися перше ім'я користувача – з яким створювався профіль (навіть за умови генерації нового сертифікату та / або майстер-ключа).

Таблиця 3 – Сигнатури файлів ключів.

| Тип файлу ключа | Довжина сигнатури в байтах | Зсув | Сигнатура |
|---|---|---|---|
| МК | 72 | 0x000c | Ім'я файлу МК |
| С | 92 | 0x0098 | "Microsoft Enhanced Cryptographic Provider v1.0" |
| ПК | 18 | 0x01c9 | "CryptoAPI" |

В кінці другого кроку першого етапу, виконується попередня фільтрація раніше отриманих списків за номером машини (частина SID, однакова для всіх локальних користувачів), що дозволяє усунути зі списку файли, зашифровані віддаленими користувачами, а також усунути зі списку облікових даних віддалених користувачів.

На третьому кроці першого етапу виконується фільтрація списку зашифрованих даних і списку облікових даних на підставі імені користувача, профіль якого необхідно відновити. Якщо користувач із вказаним ім'ям вже існує, відновлення профілю неможливе.

Фільтрований вказаним чином список зашифрованих файлів зберігається у файлі, з якого він потім зчитується під час виконання кроку перевірки наявності доступу (вказаний крок виконується після перезавантаження комп'ютера).

На наступному кроці виконується формування наборів файлів ключів. Імена необхідних файлів сертифікатів збігаються зі значеннями відбитків сертифікатів. Пошук необхідних файлів приватних ключів (між файлом приватного ключа і файлом сертифікату існує взаємно однозначна відповідність, що показано на рис. 3 двонаправленими стрілками) здійснюється на підставі імені контейнера, що зберігається в тілі файлу приватного ключа за зсувом 0x28 і має розмір 40 байт. Файл майстер-ключа, за допомогою якого був зашифрований приватний ключ, зберігається в тілі файлу приватного ключа за зсувом 0x195 і має розмір 16 байт.

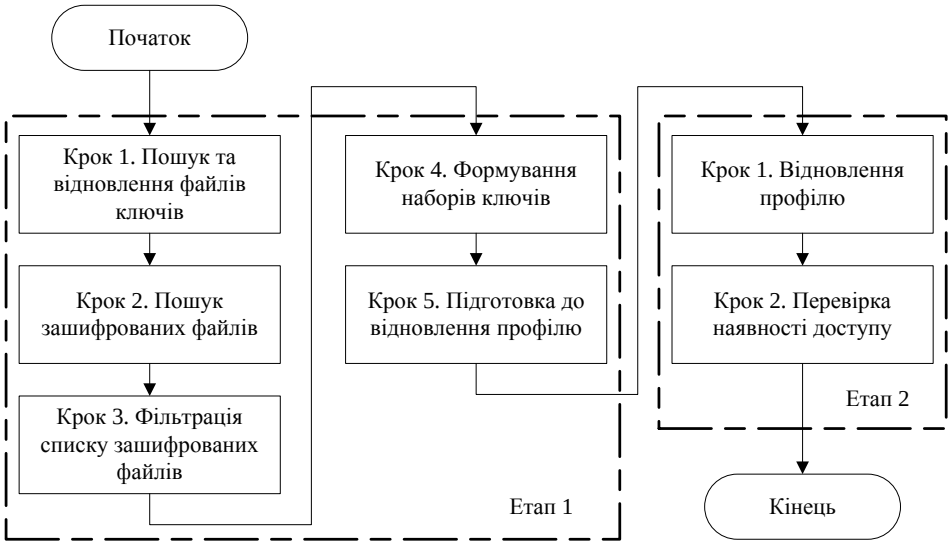


Рисунок 1 – Блок-схема узагальненого алгоритму програми EFS Profile Recovery.

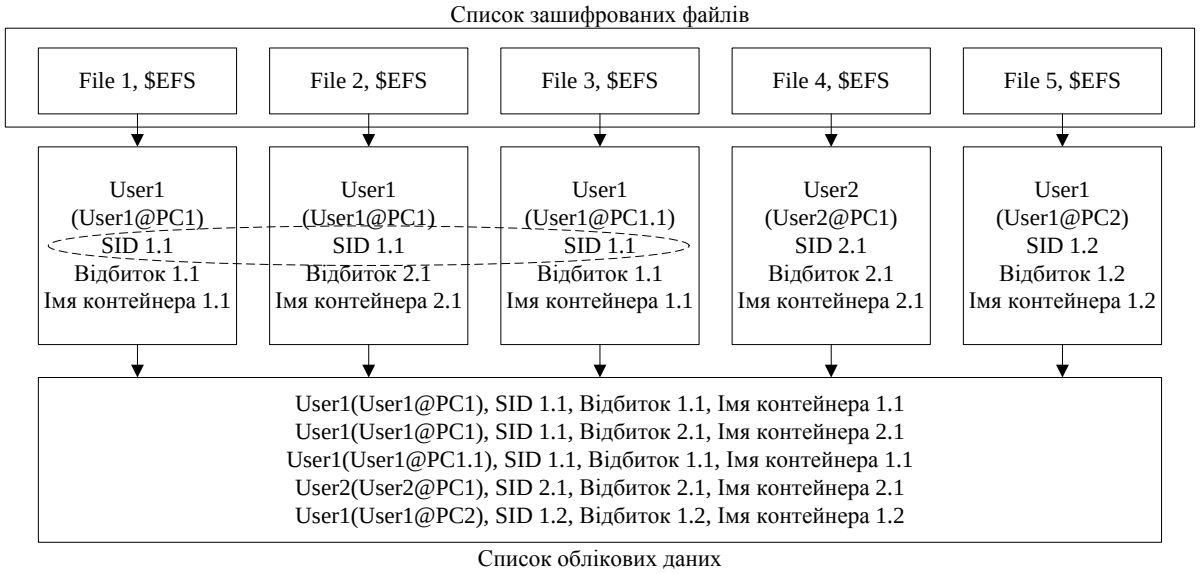


Рисунок 2 – Формування списку облікових даних.

З рис. 3 видно, що один і той же файл майстер-ключа може входити відразу до декількох наборів. Якщо жодного набору не сформовано, то відновлення профілю неможливе. Інформація про сформовані набори файлів ключів зберігається у реєстрі, і використовується під час відновлення профілю користувача на другому етапі роботи програми.

Останнім кроком першого етапу є підготовка до відновлення профілю користувача, в ході якої виконується зміна RID наступного створюваного в системі користувача на RID користувача, профіль якого відновлюється. Даний параметр зберігається в бінарному параметрі реєстру HKLM\SAM\SAM\Domains\Account\F за зміщенням 0x48 (подвійне слово) [14].

Після виконання перезавантаження комп'ютера, необхідного для набрання чинності внесених в реєстрі змін, починається перший крок другого етапу роботи програми, в ході якого виконується створення облікового запису з необхідними значеннями імені користувача, пароля і SID, а також створення відповідного профілю. Після створення профілю, в ньому створюється необхідна структура підкаталогів, в які копіюються раніше сформовані набори ключів.

Щоб в подальшому (після відновлення профілю) в системі не виникло конфлікту відносних ідентифікаторів при створенні нового користувача, значення RID наступного створюваного в системі користувача перед зміною зберігається (5-й крок 1-го етапу), і відновлюється

на 1-му кроці 2-го етапу - після відновлення профілю користувача.

На останньому кроці роботи програми виконується перевірка наявності доступу до зашифрованих файлів зі списку, отриманого на першому етапі.

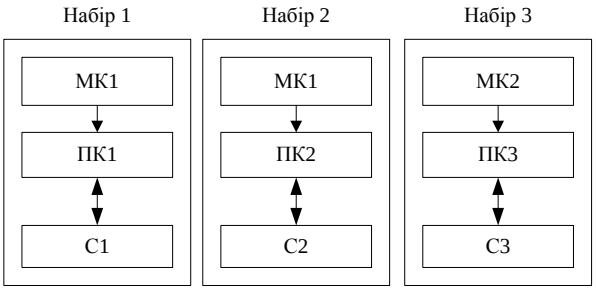


Рисунок 3 – Приклад формування наборів файлів ключів.

## *Висновки*

Було розроблено алгоритм відновлення доступу до зашифрованих за допомогою EFS даних у разі видалення профілю користувача, а також виконана його програмна реалізація у вигляді програми EFS Profile Recovery [17]. Тестування програми проводилося в наступних версіях і редакціях ОС Windows: Windows 7 Ultimate, Windows 8 Pro, Windows 8.1 Pro, Windows 10 Pro.

Після відновлення профілю, користувач отримує доступ до всіх або до частини раніше зашифрованих ним файлів, а також файлів, до яких він раніше мав доступ (але не шифрував їх). Відновлення доступу можливе лише в разі успішного відновлення одного або всіх наборів ключів, асоційованих з користувачем.

## *Список літератури*

1. Сравнительный анализ некоторых блочных алгоритмов шифрования. / А.В. Кутузов, А.А. Парнакян, П.А. Поспелов // Электронный научно-практический журнал "Современная техника и технологии". / Електронний ресурс. Режим доступу: http://technology.snauka.ru/2016/01/9292
2. Изменения в шифрованной файловой системе (EFS). / Електронний ресурс. Режим доступу: https://technet.microsoft.com/ru-ru/library/dd630631(v=ws.10).aspx
3. Набор средств шифрования данных для мобильных ПК — анализ безопасности. / Електронний ресурс. Режим доступу: https://technet.microsoft.com/ru-ru/library/cc162818.aspx
4. Внутреннее устройство ядра Windows Vista: Часть 3 / М. Руссинович / Електронний ресурс. Режим доступу: https://technet.microsoft.com/ru-ru/magazine/2007.04.vistakernel.aspx
5. Advanced EFS Data Recovery. / Електронний ресурс. Режим доступу: http://www.elcomsoft.ru/aefsdr.html
6. Efs Data Recovery for Encrypted Files and Folders. / Електронний ресурс. Режим доступу: http://www.diskinternals.com/efs-recovery/
7. EFS Recovery. / Електронний ресурс. Режим доступу: http://softambulance.com/efs_recovery
8. EFS Recovery Key. / Електронний ресурс. Режим доступу: http://www.lostpassword.com/efs.htm
9. Руссинович М. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. / М. Руссинович, Д. Соломон. – СПб.: Питер, 2008. – 992 стр.
10. Encrypting File System. / Електронний ресурс. Режим доступу: https://en.wikipedia.org/wiki/Encrypting_File_System
11. Cipher. / Електронний ресурс. Режим доступу: https://technet.microsoft.com/ru-ru/library/cc771346(v=ws.10).aspx
12. Функциональное описание FES. / Т.С. Сургученко / Електронний ресурс. Режим доступу: http://re.mipt.ru/infsec/2004/essay/2004_File_Encryption_System_Functional_Description__Surguchenko.htm
13. Security Analysis of Microsoft Encrypting File System (EFS). / А. Малышев / Електронний ресурс. Режим доступу: http://www.blackhat.com/presentations/bh-europe-03/bh-europe-03-malyshev.pdf
14. Encrypted file system recovery. / Електронний ресурс. Режим доступу: http://www.beginningtoseethelight.org/efsrecovery/index.htm
15. Секреты DPAPI. / Електронний ресурс. Режим доступу: http://www.passcape.com/index.php?setLang=6&section=docsys&cmd=details&id=25
16. Где Windows NT хранит пароли. / М. Эдвардс, Д. Лебланк / Електронний ресурс. Режим доступу: http://www.diwaxx.ru/hak/pass-nt.php
17. EFS Profile Recovery. / Електронний ресурс. Режим доступу: https://github.com/ks-gayduk/efspr

*Надійшла до редакції 11.09.2016*

**К.С. ГАЙДУК, О.Г. ШЕВЧЕНКО**
Донецкий национальный технический университет, г. Покровск, Украина

**ВОССТАНОВЛЕНИЕ ДОСТУПА К ЗАШИФРОВАННЫМ ДАННЫМ В ОС WINDOWS**

В статье рассмотрены проблемы потери доступа к данным, зашифрованным файловой системой EFS ОС Windows. Проанализированы причины отсутствия возможности получения зашифрованной информации. Рассмотрены механизмы защиты обращения к таким данным. Предложен алгоритм, позволяющий восстановить утраченный доступ к зашифрованным данным пользователя.

***Ключевые слова: шифровальная файловая система, EFS, профиль пользователя, восстановление данных, EFS Profile Recovery.***

**K. GAYDUK, O. SHEVCHENKO**
Donetsk National Technical University, Pokrovsk, Ukraine

**RECOVERY ACCESS TO ENCRYPTED DATA IN WINDOWS OS**

The article deals with the problem of the loss of the access to data, with are by EFS-encrypted Windows OS file system. The analysis of standard tools, which is provided the by Windows in order to protect sensitive data, such as EFS and BitLocker was done. The attention is focused on the fact that the data may not be damaged, but the operation with it is not possible due to the loss of the access. The reasons for the lack of the possibility of obtaining encrypted data are the following: reinstallation the operating system; deleting the user profile; deleting the user's password; incorrect way of moving user to a different domain; physical defect of the data storage media, etc. The analysis of functionality of popular software products for restoration of the lost access to the encrypted data was done.

The urgency of developing your own program of recovery of the access to the encrypted data was justified. A detailed description of the functioning of the algorithm developed by EFS Profile Recovery program was presented. The algorithm is based on the search for deleted key files for the purpose of further recovery, and on the search of the encrypted data and accounts. The examples of the formation of the list of accounts in accordance with the list of encrypted files were given. The developed program enables full or partial restoration the lost access.

EFS Profile Recovery was tested in these versions of Windows: Windows 7 Ultimate, Windows 8 Pro, Windows 8.1 Pro and Windows 10 Pro.

***Keywords: encrypted file system, EFS, user profile, data recovery, EFS Profile Recovery.***