# Програмний інтерфейс для реалізації засобу BitLocker в операційних системах сімейства Windows

УДК 004.056.5

Ірина Лозова[1], Цимбал Микита[2], Імад Ірейфідж[3]

*Національний авіаційний університет*
*[1]illozovaya@gmail.com, [2]zimbal54@gmail.com, [3]kmuinform@gmail.com*

В останні роки область застосування криптографії значно розширилася. Зокрема операційні системи сімейства Microsoft Windows надають широкі можливості для використання криптографії. BitLocker – це засіб для повного шифрування томів, що входить до версій Microsoft Windows. Він призначений для захисту даних шляхом застосування шифрування до всіх томів.

Засіб BitLocker пропонує чималу кількість налаштувань, але усі вони можуть бути застосовані лише через використання редактору групової політики (GPE) у парі з командами PowerShell. Графічний інтерфейс налаштування BitLocker у системі Windows містить лише частку налаштувань щодо вибору алгоритму та способу автентифікації, а функціонал для розгортання у рамках організацій не представлений зовсім. Часткова реалізація функціоналу для розгортання BitLocker у рамках організацій міститься у інтерфейсі MBAM, доступ до якого надається у рамках оплатної підписки MDOP для організацій. Саме тому актуальним є питання розробки програмного інтерфейсу для реалізації засобу BitLocker в операційних системах сімейства Windows.

*Метою роботи* є розробка програмного інтерфейсу для спрощення реалізації функціоналу засобу BitLocker.

За замовчуванням BitLocker використовує алгоритм шифрування AES в режимі CBC або в режимі XTS за допомогою 128-бітового або 256-бітового ключа.

Існують три механізми автентифікації, які можуть використовуватися для реалізації шифрування BitLocker: 1) Прозорий режим роботи. Цей режим використовує можливості апаратного забезпечення TPM для забезпечення прозорого користувальницького досвіду; 2) Режим автентифікації користувача. Цей режим вимагає, щоб користувач надавав певну автентифікацію до середовища перед завантаженням у вигляді PIN-коду попереднього завантаження або пароля; 3) Режим USB Key. Користувач використовує USB-пристрій, що містить ключ автозавантаження, для завантаження захищеної ОС. Ключ також може знаходитись на смарт-картці і передаватися за допомогою протоколу CCID. Використання CCID надає додаткові переваги, крім простого зберігання ключового файлу на зовнішньому USB-накопичувачі, оскільки протокол CCID приховує закритий ключ за допомогою криптографічного процесора, вбудованого в смарт-карту.

Підтримуються наведені нижче комбінації механізмів автентифікації: 1) TPM; 2) TPM + PIN; 3) TPM + PIN + USB-ключ; 4) TPM + USB-ключ; 5) USB-ключ; 6) PIN.

Ці та багато інших налаштувань доступні у повній мірі лише за умови використання командлетів PowerShell.

Для розгортання у рамках організацій BitLocker пропонує наступний сценарій для управління комп'ютерами: 1) Організації, які створюють свої власні зображення ОС за допомогою Microsoft System Center 2012 Configuration Manager SP1 (SCCM) або пізнішої, можуть використовувати існуючу послідовність завдань для попереднього налаштування шифрування BitLocker під час роботи у середовищі попередньої інсталяції Windows (WinPE) і активації за допомогою PowerShell після розгортання; 2) Організації можуть використовувати інтерфейс для адміністрування та моніторингу Microsoft BitLocker (MBAM) для управління клієнтськими комп'ютерами підключеними до домену.

На відміну від існуючих сценаріїв, розроблений інтерфейс дозволяє виконувати усі необхідні операції в єдиному середовищі і містить у собі компоненти, представлені на рисунку 1.

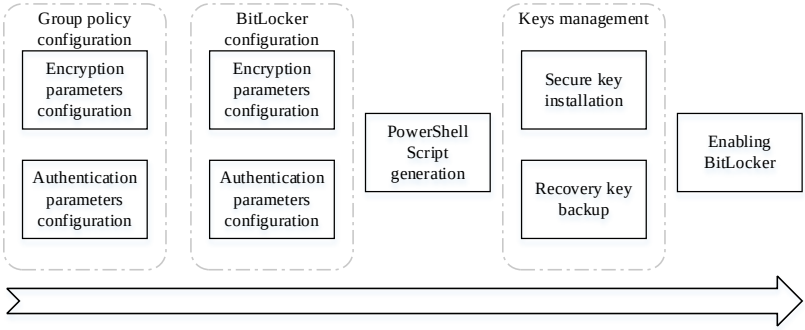


Рис. 1. Базові компоненти інтерфейсу

Конфігурація засобу BitLocker має відповідати конфігурації групової політики, тому, у першу чергу, необхідно встановити відповідність між налаштуваннями у редакторі групових політик і бажаною конфігурацією BitLocker. Відповідно до обраних налаштувань інтерфейс далі згенерує необхідну послідовність командлетів, скрипт може бути скопійовано та застосовано окремо від інтерфейсу. Після цього користувачу буде запропоновано встановити обрані секретні ключі та зберегти ключ відновлення. Останнім етапом проводиться запуск засобу BitLocker з відповідними параметрами, а прогрес шифрування відображається за допомогою запропонованого інфтерфейсу.

Отже, в роботі розроблено програмний інтерфейс для спрощення реалізації функціоналу засобу BitLocker, зокрема редагування налаштувань параметрів групових політик, налаштування параметрів самого засобу, встановлення ключів автентифікації та відновлення, зберігання ключів в на зовнішньому носії, або в системі ActiveDirectory. Зазначений інтерфейс дозволить генерувати скриптові послідовності для налаштування функцій засобу BitLocker, використовуючи графічне представлення. Дане рішення дозволить спростити та прискорити налаштування та розгортання засобу.