УДК 004.457
Поволоцький В. – ст. гр. СНм-51
Тернопільський національний технічний університет імені Івана Пулюя

СИСТЕМА ШИФРУВАННЯ BITLOCKER

Науковий керівник: асистент Маєвський О.В.

Втрата конфіденційних даних часто відбувається після того, як зловмисник отримав доступ до інформації на жорсткому диску. Для недопущення подібного, присутній інструмент BitLocker, який дозволяє шифрувати весь диск. Цей інструмент реалізований тільки у версіях Microsoft Windows Vista Ultimate, Windows Vista Enterprise, Windows 7 Ultimate, Windows 7 Enterprise та Windows Server 2008.

Технологія шифрування даних BitLocker застосовується до будь-яких файлів системного диска.

BitLocker використовує багаторівневе шифрування – одночасне задіювання декількох видів захисту, включаючи апаратний і програмний метод. Комбінації способів захисту даних дозволяють отримати декілька різних режимів роботи системи шифрування BitLocker. Кожен з них має свої переваги, а також забезпечує свій рівень безпеки:

- режим з використанням довіреного платформеного модуля;
- режим з використанням довіреного платформеного модуля і USB-пристрою;
- режим з використанням довіреного платформеного модуля і персонального ідентифікаційного номера (ПІН-коду);
- режим з використанням USB-пристрою, що містить ключ.

Довірений платформений модуль - це спеціальний криптографічний чіп, який дозволяє виконувати ідентифікацію. Така мікросхема може бути інтегрована, наприклад, в деяких моделях ноутбуків, настільних ПК, різних мобільних пристроях та ін.

Технологія BitLocker дає можливість застосовувати алгоритм шифрування до дисків з даними, на яких використовуються файлові системи exFAT, FAT16, FAT32 або NTFS. Метод шифрування, який використовує технологія BitLocker, заснований на стійкому алгоритмі AES із 128-бітовим ключем.

Існує три механізми перевірки достовірності, які можна використовувати для реалізації Bitlocker шифрування:

- *Прозорий режим роботи:* Цей режим використовує можливості апаратного забезпечення Trusted Platform Module (TPM) для надання прозорої роботи користувачів. Користувачі включають і входять на комп'ютер з операційною системою Windows, як завжди. Ключ, використовуваний для шифрування диска закодований в чіп TPM і він може бути виданий тільки в коді завантажувача. Цей режим вразливий для нападу при холодному завантаженні.
- *Режим перевірки достовірності користувача:* Цей режим припускає, що користувач пройшов деяку аутентифікацію в пред-завантажувальному середовищі у вигляді попереднього вводу PIN-коду. Цей режим уразливий при використанні буткіт-атак.
- *Режим USB-ключа:* Користувач повинен вставити пристрій USB в комп'ютер, який містить ключ запуску, щоб мати можливість завантаження в захищену операційну систему. Цей режим також вразливий до буткіт-атак.