Островський О. О., студент групи КБ-2,
Щур Н. О., старший викладач кафедри КІтаКБ
Державний університет «Житомирська політехніка»

ПОВНЕ ШИФРУВАННЯ ДАНИХ НА ЕЛЕКТРОННИХ НОСІЯХ ЯК МЕТОД ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Щодня ми користуємося ґаджетами для комунікацій, роботи, зберігаємо конфіденційну інформацію. Компанії впроваджують політику BYOD (Bring Your Own Device) – «принеси свій пристрій», завдяки чому спостерігалось підвищення рівня задоволеності та продуктивності серед співробітників та зниження витрат на IT-відділ [1]. Проте, у цього є й інша сторона. При втраті пристрою можливий доступ до комерційної чи іншої таємниці неавторизованим користувачам. Тому надзвичайно важливо захистити дані від третіх осіб, які можуть заволодіти нею. Інструмент захисту інформації має поєднувати у собі декілька факторів:

– Швидкість. Не має бути помітно істотних змін у швидкості роботи пристрою, щоб не зменшувалась продуктивність.
– Зручність. Легкість в використанні для користувачів різного рівня володіння комп'ютером.
– Надійність. Недопущення доступу нелегітимних користувачів до будь-якої інформації на носії або пристрої.

Найкращим варіантом для задоволення усіх трьох пунктів буде повне шифрування диску (FDE). FDE (Full Disk Encryption) – це найбільш надійний метод шифрування розділів диска, бо використовує шифрування на рівні блоків. Тобто, забезпечується шифрування навіть таких даних як кількість файлів або їх розмір, що є безумовною перевагою перед шифруванням на рівні файлів, де ці дані залишаються відкритими. При цьому, втрати швидкості при виконанні читання (запису) диску є незначними.

Повне шифрування диску призначене для захисту від офлайнових атак, коли доступ до носія здійснюється при завантаженні з іншої операційної системи або ж носій взагалі фізично підключається до чужого комп'ютера. Така ситуація виникає, коли зловмисник отримує фізичний доступ до вимкненого пристрою, наприклад, при його крадіжці або втраті. Це найбільш суттєво в організаціях або компаніях, де захист даних повинен забезпечуватися тоді, коли неможливо уникнути людських помилок.

Шифрування для системних дисків вимагає проходження попередньої аутентифікації (Pre-Boot Authentication, PBA) для отримання від користувача інформації (пароля, ключового файлу), що дозволяє розблокувати носій даних, тобто отримати доступ до ключів шифрування даних, що зберігаються у зашифрованому вигляді.

Корпорація Microsoft постачає у своїх операційних системах сімейства Windows утиліту BitLocker, що є найвідомішою програмою для шифрування томів дисків та переносних пристроїв. Однією з переваг є сумісність з TPM (Trusted Platform Module) – криптографічний модуль, вбудований у материнську плату, що дозволяє зберігати ключі та виконувати процеси шифрування (дешифрування) «на льоту». Також завдяки йому можлива перевірка цілісності даних при старті системи, чого не дозволяє робити базовий FDE. BitLocker використовує симетричний алгоритм шифрування AES (у режимах CBC та XTS) з 128-бітним ключем, але, для більшої надійності, доступний 256-бітний ключ [2]. Цю утиліту легко використовувати завдяки максимальній автоматизації усіх дій, тому з нею можуть впоратись навіть користувачі із базовим рівнем володіння комп'ютером.

Принцип шифрування програмою Bitlocker наступний:

1. При ввімкнені створюється ключ шифрування тому FVEK (Full Volume Encryption Key) за допомогою генератора псевдовипадкових чисел. Ним буде зашифровано кожен сектор.
2. FVEK шифрується за допомогою ключа VMK (Volume Master Key) та зберігається в метаданих тому.
3. Якщо наявний модуль TPM, ключ VMK зашифровується ключем SRK (Storage Root Key), який і міститься у цьому модулі. За його відсутності, замість SRK користувач може вибрати зручний для нього спосіб шифрування: пін-код або флеш-накопичувач з записаною на ньому ключовою інформацією.
4. Додатково можна захистити ключ VMK паролем.

Отже, варто пам'ятати, що у деяких випадках персональні або корпоративні дані можуть бути важливіші та цінніші, ніж обладнання, на якому вони зберігаються. На сьогодні FDE є досить надійним методом захисту конфіденційних даних від несанкціонований доступу, оскільки при правильному шифруванні та зберіганні ключа зламати зашифрований диск практично неможливо.

Список використаних джерел

1. Avantika Monnappa. What is BYOD (Bring Your Own Device) and Why Is It Important?, 2016. URL: https://www.simplilearn.com/what-is-byod-and-why-it-is-important-article.
2. The specifications of the AES-CBC + diffuser algorithm used in BitLocker Drive Encryption. URL: http://www.microsoft.com/en-us/download/details.aspx?id=13866.