УДК 004

Д.Пісаренко, магістр гр. КН-22МЗ,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ФАЙЛАМИ В ОС WINDOWS НА ОСНОВІ ТЕХНОЛОГІЇ BITLOCKER DRIVE ENCRYPTION

У статті розроблено програмне забезпечення, яке призначено для системи управління файлами в ОС Windows на основі технології BitLocker Drive Encryption. Метою розробки є дослідження та програмна реалізація системи управління файлами в ОС Windows на основі технології BitLocker Drive Encryption. Об'єктом дослідження є процес управління файлами в ОС Windows на основі технології BitLocker Drive Encryption. Предметом дослідження є методи управління файлами в ОС Windows на основі технології BitLocker Drive Encryption. Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи управління файлами в ОС Windows на основі технології BitLocker Drive Encryption. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Використовуйте шифрування, коли потрібен надійний захист даних. Щоб зашифрувати диск, на який інстальовано Windows, на комп'ютері мають бути два розділи: системний розділ (який містить файли, потрібні для запуску комп'ютера) та розділ операційної системи (на якому міститься Windows). Розділ операційної системи буде зашифровано, а системний розділ залишиться незашифрованим, отже комп'ютер можна буде запускати.

У попередніх версіях Windows можна створити ці розділи вручну. У поточних версіях Windows розділи створюються автоматично. Якщо на комп'ютері немає системного розділу, майстер BitLocker створить його, використавши 200 МБ доступного дискового простору. Системному розділу не присвоюватиметься буква диска і він не відображатиметься у папці «Комп'ютер».

За допомогою програми шифрування дисків BitLocker можна захистити файли на всьому диску. BitLocker може допомогти запобігти доступу хакерів до системних файлів, через які вони дізнаються ваші паролі, або запобігти доступу до диска шляхом його фізичного вилучення з ПК та встановлення в інший ПК. При цьому ви можете входити до системи Windows і використовувати файли, як робите це завжди.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи управління файлами в ос windows на основі технології Bitlocker Drive Encryption.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи управління файлами в ОС Windows на основі технології BitLocker Drive Encryption.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем управління файлами в ОС Windows на основі технології BitLocker Drive Encryption.

– Дослідження системи управління файлами в ОС Windows на основі технології BitLocker Drive Encryption.

– Програмна реалізація системи управління файлами в ОС Windows на основі технології BitLocker Drive Encryption.

Об'єктом дослідження є процес управління файлами в ОС Windows на основі технології BitLocker Drive Encryption.

Предметом дослідження є методи управління файлами в ОС Windows на основі технології BitLocker Drive Encryption.

Методи дослідження базуються на методах захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Шифрування дисків, файлів і баз даних – це технології, які захищають конфіденційність даних під час їх зберігання. Повне шифрування диска шифрує всі дані на диску, за винятком частини, яка містить код для розблокування решти диска, яка зазвичай не шифрується. Шифрування на основі файлів працює на рівні файлів і може здійснюватися операційною системою або програмою. Шифрування бази даних можна виконати за допомогою прозорого шифрування бази даних, шифрування на рівні стовпців або шифрування на рівні полів. Як повне шифрування диска, так і шифрування на основі файлів забезпечують хороший захист від витоку даних у разі крадіжки або втрати пристрою. Однак через свою природу вони не можуть захистити від зловмисника, який потрапив до ввімкненого пристрою, або будь-яких інших зловмисників, які можуть запускати програми на комп'ютері.

Шифрування дисків, файлів і баз даних – це технології, які використовуються для захисту конфіденційності даних під час їх зберігання. Повне шифрування диска (FDE) шифрує всі дані на диску, крім частини, яка містить код для розблокування решти диска, яка зазвичай не шифрується. Шифрування на основі файлів (FBE) працює на рівні файлів і може здійснюватися операційною системою або програмою. Ручне шифрування файлів вимагає втручання користувача та не є прозорим. Шифрування бази даних (DBE) можна виконати за допомогою прозорого DBE, шифрування на рівні стовпця або шифрування на рівні поля. Метою DBE є шифрування всієї бази даних або певних стовпців або полів, щоб гарантувати, що дані з фізичного сховища неможливо буде прочитати в разі викрадення.

Щоб використовувати дані, наприклад, щоб робити з ними обчислення, дані повинні бути розшифровані для обробки, якщо не використовуються такі технології, як гомоморфне шифрування Незалежно від того, чи повинен користувач увімкненого та розблокованого пристрою надати додатковий секрет для роботи із зашифрованим файлом, диском або базою даних, ключовий матеріал, необхідний для цього, уже має бути доступним у системі. Якщо не потрібно надавати додатковий секрет, розшифровка та шифрування прозорі для користувача, а ключовий матеріал зазвичай вводиться або стає доступним під час фази запуску або розблокування пристрою. Отже, дані захищені лише тоді, коли пристрій вимкнено або заблоковано.

Повне шифрування диска (FDE)

Як випливає з назви, FDE [1] шифрує всі дані на диску, якщо тільки це не диск, з якого завантажується система. У цьому випадку частина, яка містить код для розблокування/отримання критичного матеріалу, необхідного для доступу до решти диска, не шифрується. Цей код зазвичай робить щось на зразок (1) читання зашифрованого ключа з незашифрованої частини диска, (2) введення користувачем пароля, необхідного для його розшифровки, і (3) початок завантаження операційної системи, оскільки дані на диску, що містить його, тепер можуть бути розшифровані. Після завантаження операційної системи доступ до диска здійснюється через драйвер шифрування та прозорий для користувача та будь-якої іншої особи/зловмисника, який потрапив до такої системи. Це в основному проблема під час використання FDE у середовищі сервера, оскільки важко гарантувати, що ніхто інший не матиме доступу до системи під час її роботи. Крім того, при використанні FDE в серверному середовищі слід звернути увагу на те, як пароль/секретний ключ вводиться в систему сервера [2]. Інша проблема полягає в тому, що якщо незашифрована частина диска не захищена від маніпуляцій, наприклад, за допомогою безпечних технологій

завантаження, зловмисник може ефективно виконувати атаки, такі як атака злої покоївки [3]. Окремим випадком FDE є зовнішні жорсткі диски, які містять алгоритм шифрування та PIN-код безпосередньо в корпусі. Це дозволяє легко використовувати з різними системами, оскільки вони не потребують підтримки FDE. У цьому випадку FDE є для них повністю прозорим.

Шифрування на основі файлів (FBE)

Система, яка використовує файлове шифрування, схожа на систему FDE. Однак він працює на рівні окремих файлів, а не на рівні так званих блоків. Це означає, що система FBE шифрує кожен файл окремо. Розшифровку та шифрування може здійснювати операційна система кожного разу, коли файл читається та записується, або програма, якщо вона обмежена файлами, які читає та записує ця програма. Сучасні системи FBE включають сучасні смартфони під управлінням Android або iOS, вбудовану файлову систему шифрування Windows (EFS), системи Linux із fscrypt або хмарні рішення для зберігання, як-от Proton Drive та інші. Щоб зашифрувати вміст файлів, FBE може використовувати той самий ключ шифрування для всіх файлів або різні ключі для різних файлів. Це дозволяє, наприклад, запровадити різні рівні захисту для файлів, як на пристроях Apple під керуванням iOS. Там файли, доступні в заблокованому стані, шифруються іншим ключовим матеріалом, ніж файли, доступні лише в розблокованому стані. Коли пристрій заблоковано, ключовий матеріал останнього рівня захисту більше не доступний. Його можна відновити, лише розблокувавши телефон повторно. Проте негативним моментом є те, що більшість систем FBE сьогодні залишають для зловмисника одну або кілька із наведених нижче метаданих для вивчення:

– Час доступу та розмір файлу – виявлення того, чи використовувався файл нещодавно та якого типу він може бути
– Тип запису (файл або каталог) – розкриття використовуваних програм
– Для файлів zip, захищених паролем, навіть імена файлів є відкритим текстом

Ручне шифрування файлів

На відміну від FDE та FBE, ручне шифрування файлів вимагає втручання користувача та є непрозорим. Найвідомішою системою є надання пароля для створення файлу .zip. Цей пароль зашифрує більшість, але не всі дані у файлі zip. Існують більш складні інструменти, такі як PGP, але вони створюють фундаментальну проблему керування, оскільки відправнику потрібен доступ до відкритого ключа одержувача.

Шифрування бази даних (DBE)

DBE зазвичай виконується за допомогою одного з таких підходів: прозорий DBE, шифрування на рівні стовпця або шифрування на рівні поля. Вся база даних зашифрована тим самим симетричним ключем із прозорим DBE. Це гарантує, що дані з фізичного сховища неможливо буде прочитати в разі викрадення. Інші два підходи використовують те, як структуровані реляційні бази даних. Вони складаються з таблиць, таблиці складаються зі стовпців, а запис стовпця називається полем. За допомогою шифрування на рівні стовпців можна використовувати різні ключі шифрування для різних стовпців. Це додає, наприклад, можливість шифрувати лише частини даних і/або прив’язувати ключовий матеріал до певних ролей, що запобігає читанню даних користувачами з іншою роллю, яким вдається запитувати такий стовпець. Однак шифрування стовпців окремо може відбуватися за рахунок зниження швидкості, залежно від того, зашифровано лише один стовпець чи багато. Також можливе шифрування на рівні поля. Це дозволяє користувачам шукати в БД без розшифровки кожного поля, оскільки можна зашифрувати вміст поля (лише точні збіги), а потім шукати це значення. Однак коли шифрування рандомізовано, наприклад, шляхом додавання до вмісту випадкового значення фіксованого розміру перед його шифруванням, для однакових полів генерується інший результат. Це забезпечує більшу безпеку ціною загрози зашифрованим пошукам.

Міркування безпеки

Алгоритми шифрування

Деякі високопродуктивні пристрої шифрування існують в апаратному забезпеченні, але більшість систем засновані на програмному забезпеченні. Перевага використання програмного забезпечення полягає в тому, що систему можна легше оновлювати. Крім того, несправний апаратний компонент може унеможливити подальше використання системи, якщо заміна компонента недоступна.

Більшість систем використовують стандартні алгоритми шифрування, такі як AES або ChaCha20. Лише деякі системи створюють свої алгоритми [4]. Дивіться також [5, 6] для огляду.

AES працює як блоковий шифр, тобто може зашифрувати лише один блок даних. У випадку AES це 256 біт. Щоб зашифрувати весь диск, AES поєднується з *режимом блочного шифрування*, який дозволяє шифрувати більші блоки.

Керування ключами

Симетричний ключ, який використовується для шифрування, у найпростішому випадку отримується з пароля, наданого користувачем. Важливо, щоб пароль був достатньо довгим і мав достатню ентропію, щоб бути безпечним. Ця проста система не може відновити втрачений пароль і не може дозволити більше ніж одному користувачеві отримати доступ до тих самих даних.

Більш складні системи використовують асиметричне шифрування для захисту симетричного ключа. Цей додатковий асиметричний ключ може зберігатися в апаратному елементі, наприклад смарт-карті, модулі TPM або іншому. Ці системи також можуть включати двофакторну аутентифікацію.

У всіх системах має бути спосіб відновлення даних у надзвичайних ситуаціях. Наприклад, якщо користувачеві потрібно запам'ятати свій пароль або закритий ключ. Тим не менш, це потрібно зробити, щоб не можна було зловживати екстреним порядком. Дійсно, якщо цей надзвичайний варіант можна використовувати для доступу до несанкціонованих даних, це може стати радше проблемою, ніж рішенням. Тому необхідно знайти правильний баланс між конфіденційністю та доступністю.

Примус

Щоб отримати доступ до зашифрованих даних, будь то дані, захищені FDE, FBE або DBE, потрібен певний секретний/ключовий матеріал, наданий користувачем. Зловмисник може змусити користувача ввести пароль шляхом примусу, щоб отримати його. Це може бути насильство, загроза тюремного ув’язнення чи будь-який інший вид примусу [7]. Щоб перемогти цю атаку, деякі системи дозволяють користувачам вводити різні паролі. Залежно від пароля система відкриє один з двох контейнерів. Один пароль відкриває стандартну систему, файл або базу даних, а інший відкриває іншу, яка не містить конфіденційних даних. Для зовнішнього спостерігача майже неможливо дізнатися, на яку з двох систем він зараз дивиться. Одним із прикладів рішення, яке робить це на рівні дисків, є VeraCrypt [8].

Тенденції

Основні функції FDE і FBE тепер легко доступні в популярних операційних системах, таких як Windows, MacOSX і Linux. Проте все ще рідко можна побачити шифрування на стороні сервера, за винятком серверів великих гравців. Наприклад, Google використовує кілька рівнів шифрування. Це також пов’язано з тим, що користувачам потрібно вплинути на те, чи зашифровані дані за хмарними службами.

Дві функції шифрування, які можуть покращити взаємодію з користувачем, можуть отримати більшу популярність до 2025 року. Обидві передбачають керування секретним ключем: делеговане (зберігаюче) керування ключами та порогове шифрування.

Делеговане (зберігальне) керування ключами означає, що ключ знаходиться на сторонньому сервері. Це дозволяє відновити ключ, якщо основний власник втратить ключ. Microsoft і Apple пропонують цю послугу під час встановлення FDE. Хоча ця система

гарантує, що ключ буде доступним навіть у разі втрати пароля, тепер ви повинні довіряти зберігачу ключа, у цьому випадку Microsoft і Apple, щоб не віддати його.

Більш безпечним методом є порогове шифрування, яке надає ключ кільком сторонам. Для відновлення ключа потрібно взяти мінімум цих сторін. Таким чином, один учасник не може витікати ключ. За цією схемою працює декілька систем.

BitLocker Drive Encryption – пропрієтарна технологія, що є частиною операційних систем Microsoft Windows 10/11 Ultimate/Enterprise, Windows 7 Ultimate/Enterprise, Windows Server 2008 R2 і Windows 8. BitLocker дозволяє захищати дані шляхом повного шифрування диска (ів) (логічних, з Windows 7 – і карт SD та USB-флешек) (у термінології Microsoft – тому(ів)).

BitLocker – це програмне рішення для шифрування, яке може шифрувати всю систему та диски з даними; Зазвичай розгортання шифрування BitLocker на пристроях займає від кількох годин до одного дня, залежно від швидкості та розміру диска.

Корпорація Майкрософт зробила кілька кроків у наданні допомоги фахівцям із IT-безпеки для пом'якшення атак і ризиків, запровадивши кілька вдосконалень у свою пропозицію шифрування дисків BitLocker.

Сьогодні приблизно 60% проданих обчислювальних пристроїв є портативними комп'ютерами. Поширеність цих пристроїв створила проблеми для фахівців з IT-безпеки, оскільки їх легше втратити або вкрасти, ніж настільні комп'ютери, які залишаються у фізичному місці.

Кінцевим користувачам також дуже легко зберігати конфіденційні дані на ноутбуці для зручності та не помічати проблем безпеки.

Для багатьох компаній ці конфіденційні дані підпадають під дію законів про дотримання нормативних вимог, які можуть передбачати суворі грошові штрафи за недотримання. У разі витоку інформації ділова репутація може бути серйозно погіршена, як нещодавно показало порушення Target.

Що таке BitLocker Drive Encryption?

Шифрування диска BitLocker вперше було представлено Microsoft у Windows Vista. Це повнофункціональний варіант шифрування диска для захисту комп'ютерів від атак, до яких система вразлива, коли зловмисник фізично володіє комп'ютером.

У Windows 7 Microsoft представила BitLocker To Go, який додав можливість шифрувати знімні диски, включаючи флеш-носії USB і зовнішні жорсткі диски, що робить це чудовим варіантом для порівняння зовнішнього жорсткого диска з хмарою для різних вимог. Процес розгортання також було вдосконалено для автоматичного використання середовища Microsoft Active Directory. BitLocker використовує алгоритм шифрування Advanced Encryption Standard (AES) із 128- або 256-бітним ключем. AES – це алгоритм шифрування, прийнятий урядом США.

Випустивши Windows Server 2012, корпорація Майкрософт внесла кілька важливих удосконалень у продукт, що спрощує розгортання та керування BitLocker фахівцям із IT-безпеки. BitLocker тепер доступний для використання з Windows 8, Windows 8 Pro та Windows 8 Enterprise разом із серверними версіями 2012.

Покращення BitLocker у Windows

Підтримка дисків із самошифруванням

У попередніх версіях BitLocker ця технологія не підтримувала використання жорсткого диска з апаратним шифруванням як завантажувального диска. Це змінилося, і тепер ви можете використовувати диски з вбудованим апаратним шифруванням (часто їх називають дисками з самошифруванням або SED).

Підтримується широкий вибір типів накопичувачів, включаючи IDE, ATA, SATA, eSATA, SAS і SCSI, а також IEEE 1394 і USB. Windows Server 2012 робить крок вперед і підтримує BitLocker на дисках Fibre Channel і iSCSI. Ви також можете використовувати BitLocker з апаратними масивами RAID (але не з програмним RAID).

Розблокування мережі

Іншою функцією BitLocker для Windows 8 і Server 2012 є розблокування мережі.

Функція розблокування мережі призначена для корпоративних середовищ, зокрема для систем, які належать до домену Windows. Це автоматично розблокує диски, захищені BitLocker, коли комп'ютер перезавантажується, якщо комп'ютер під'єднано до корпоративної мережі через дротове з'єднання (не відбувається з Wi-Fi або віддаленими з'єднаннями).

Це дозволяє уникнути проблеми, коли користувачі забувають свої PIN-коди або USB-ключі, коли вони підключені до довіреної мережі (припускається, що якщо вони фізично знаходяться в приміщенні з підключеним Ethernet, вони, ймовірно, є авторизованими користувачами). Це також полегшує розгортання виправлень та інших оновлень на робочих столах без нагляду, захищених BitLocker. Звичайно, це необов'язкова конфігурація. Для кращої безпеки організації все ще можуть вимагати введення PIN-коду (та/або вставлення USB-ключа) для доступу до захищених дисків навіть у корпоративній мережі.

Попередня підготовка BitLocker

Ще одна особливість, призначена для підприємств, – це можливість попереднього налаштування BitLocker або його надання перед встановленням операційної системи. У Windows 7 уже була можливість підготувати розділи диска для BitLocker під час інсталяції, а Windows 8/Server 2012 дозволяє піти ще далі. Використовуючи Active Directory, фахівці з IT-безпеки можуть налаштувати середовище для розгортання систем із готовим BitLocker.

Захист цілісності процесу завантаження

На додаток до переваг, згаданих вище, ще однією вагомою причиною для впровадження BitLocker є те, що він може захистити цілісність процесу завантаження. Якщо в комп'ютер втручаються без відома користувача, наприклад, шляхом несанкціонованого встановлення трояна чи іншого шкідливого програмного забезпечення, комп'ютер увійде в середовище відновлення BitLocker.

BitLocker і BitLocker to Go є чудовими рішеннями для запобігання неавторизованим третім сторонам від відновлення даних, що зберігаються на втрачених або викрадених портативних комп'ютерах або USB-накопичувачах. З огляду на те, що відбулася низка відомих порушень, і, на жаль, експерти погоджуються, що вони відбуватимуться й надалі, використання BitLocker і BitLocker to Go для захисту конфіденційних даних – це те, що вам і вашій організації слід серйозно розглянути.

З моменту випуску BitLocker зазнав низки оновлень, щоб підвищити ефективність захисту даних і полегшити використання для користувачів. Поточна версія BitLocker дозволяє адміністраторам Windows 11 і Windows 10 УВІМКНУТИ BitLocker безпосередньо в середовищі попередньої інсталяції Windows.

Якщо ви не знайомі з BitLocker, для користувачів доступні два методи шифрування:

1. Метод апаратного шифрування, для якого потрібен чіп безпеки Trusted Platform Module (TPM).
2. Програмний метод шифрування, який можна активувати за допомогою пароля або за допомогою USB-накопичувача.

Адміністрування та моніторинг Microsoft BitLocker

За допомогою Microsoft Desktop Optimization Pack (MBAM) користувачі можуть без особливих зусиль керувати BitLocker і BitLocker To Go і надавати необхідну підтримку. Остання версія MBAM 2.5 постачається з пакетом оновлень 1, який містить низку функцій:

– Забезпечує сумісність із Windows 10 і дозволяє легко налаштовувати процес відновлення.

– Включає Microsoft Endpoint Configuration Manage, який є централізованим оператором, який використовується для створення звітів і керування обсягами даних.

– Користувачі можуть використовувати Портал самообслуговування для відновлення зашифрованих пристроїв.

– Дозволяє системним адміністраторам шифрувати великі обсяги даних, створених підприємствами-клієнтами, шляхом ефективної автоматизації процесу шифрування.

– Користувачі Windows Enterprise можуть бути впевнені, що їхні корпоративні дані в безпеці незалежно від того, де вони працюють.

– Дозволяє співробітникам служби безпеки контролювати індивідуальні чи клієнтські комп'ютери та миттєво перевіряти стан їх відповідності. Вони також мають доступ до аудиту, який є необхідною умовою для отримання та відновлення конфіденційної інформації.

– Забезпечує ефективне виконання будь-яких політик щодо шифрування BitLocker, які ви налаштували для підприємств.

– Значно зменшує навантаження на службу підтримки, надаючи підтримку за допомогою запитів на відновлення BitLocker.

– Дозволяє користувачам легко інтегруватися з Microsoft Endpoint Configuration Manager та іншими корисними інструментами для автоматизації керування.

Шифрування пристрою BitLocker у Microsoft увімкнено за допомогою 128-бітного методу шифрування XTS-AES. Якщо ви хочете застосувати інший метод шифрування або налаштувати надійність шифру, вам потрібно буде розшифрувати зашифрований пристрій і за потреби застосувати нові налаштування.

Шифрування пристрою BitLocker: що вам слід знати

Перш ніж розпочати роботу з шифруванням BitLocker, ось кілька ключових деталей, про які вам слід знати:

– Шифрування диска BitLocker підтримується Windows 10 Pro і Enterprise. Версія BitLocker сумісна з Windows 10 (у версії Home є своя версія BitLocker, але лише для вибраних пристроїв).

– Для шифрування диска BitLocker потрібен модуль довіреної платформи (TPM), щоб активувати розширені функції безпеки на вашому пристрої.

– Якщо ви вирішите ввімкнути BitLocker за допомогою програмного шифрування, вам потрібно буде надати додаткову автентифікацію (пароль або флеш-USB).

– Переконайтеся, що вбудоване програмне забезпечення вашого комп'ютера підтримує TPM або USB. Немає функції? Зверніться до виробника та подайте запит на оновлення базової системи введення-виведення (BIOS) або уніфікованого розширюваного інтерфейсу мікропрограми (UEFI).

– Ваш пристрій має містити два розділи – один для файлів на жорсткому диску та інший для початку процесу інсталяції. Переконайтеся, що на вашому розділі жорсткого диска відформатована файлова система NTFS.

– Залежно від обсягу та типу даних процес шифрування може тривати деякий час.

– Ваш комп'ютер має мати джерело безперебійного живлення (UPS), поки увімкнено шифрування BitLocker.

– Хоча це нечасто, переконайтеся, що ви створили повну резервну копію вашої системи, якщо пізніше ви зіткнетеся з ризиками безпеки.

Розробка структурної схеми

Структурна схема системи зображена на рисунку 1. Робота системи відбувається наступним чином. BitLocker Drive Encryption працює, управляючи кожним файлом з метою збереження конфіденційності, за допомогою алгоритму симетричного управління файлами з метою збереження конфіденційності, що залежить від версії операційної системи й настроювань

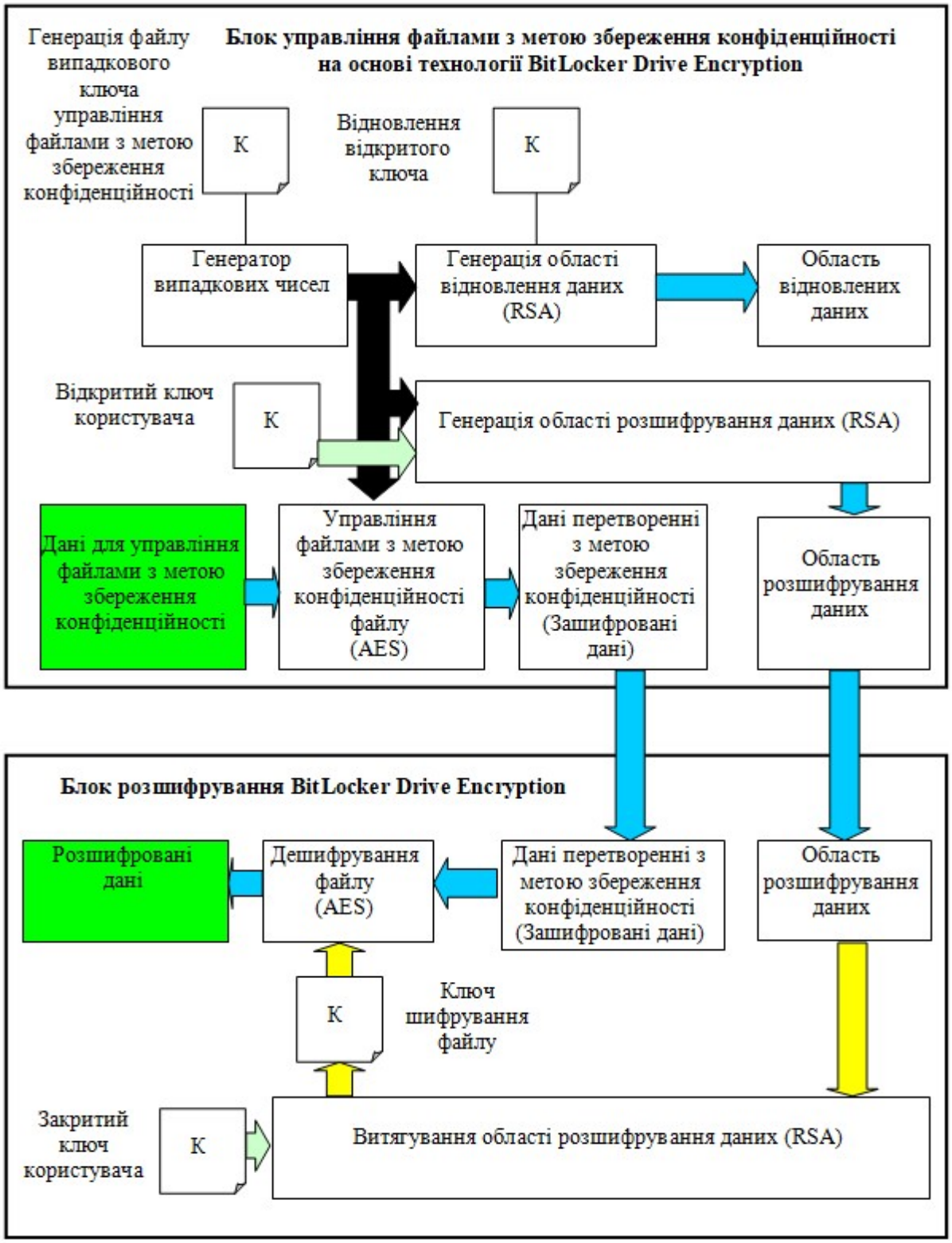

Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління файлами в ОС Windows на основі технології BitLocker Drive Encryption. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем управління файлами в ОС Windows на основі технології BitLocker Drive Encryption; Досліджена система управління файлами в ОС Windows на основі технології BitLocker Drive Encryption; На основі отриманих результатів досліджень створена програмна реалізація системи управління файлами в ОС Windows на основі технології

BitLocker Drive Encryption. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання управління файлами в ОС Windows на основі технології BitLocker Drive Encryption. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Frontoni, E., Kandiy, S., Smirnova, T., Prokopov, S., Bilanovych, A. «New Cost Function for S-boxes Generation by Simulated Annealing Algorithm». Lecture Notes on Data Engineering and Communications Technologies, 2023. vol 180. pp. 310-320. Springer, Cham.
2. Kuznetsov, O., Frontoni, E., Kandiy, S., Smirnov, O., Ulianovska, Y., Kobylianska, O. «Heuristic Search for Nonlinear Substitutions for Cryptographic Applications». Lecture Notes on Data Engineering and Communications Technologies, 2023. vol 180. Springer, Cham. pp. 288-298.
3. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». CEUR Workshop Proceedings, 2023, 3628, pp. 93-105.
4. Kuznetsov O., Frontoni E., Kuznetsova Ye., Smirnov O., Chevardin V. «Achieving Enhanced Security in Biometric Authentication: A Rigorous Analysis of Code-Based Fuzzy Extractor». CEUR Workshop Proceedings, Volume 3624, 2023, pp. 330-339.
5. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
6. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
7. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
8. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
9. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
10. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
11. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
12. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.
13. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58.
14. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
15. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
16. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
17. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131.
18. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
19. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84.

20. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
21. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I.,Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 166-171.
22. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
23. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.