УДК 004

Б.Сільман, магістр гр. КІ-21М-1,4,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ FLASH DRIVE

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

комп'ютерна інженерія, захисту доступу, Flash Drive

Постановка проблеми. Захист конфіденційної інформації сьогодні необхідний практично будь-якому власникові Flash Drive. На сьогоднішній день під засобами захисту інформації на Flash Drive розуміють сукупність різних технічних і програмних систем і пристроїв, використовуваних для рішення різних завдань по захисту інформації, у тому числі попередження витоку, захисту даних на флешці (Flash Drive) від запису й забезпечення повного комплексу мер для безпеки информации, що захищається.

Сучасні засоби захисту інформації покликані забезпечити безпеку даних на Flash Drive, як то:

- захист файлів на флешці від запису;
- захист файлів на флешці від копіювання;
- захист файлів на флешці від видалення;
- інші несанкціоновані дії.

Всі частіше покупці прагнуть придбати не просто флеш-накопичувач, а саме захищені флеш-накопичувачі, і їх прекрасно можна зрозуміти.

Захищені Flash Drive дозволили нам вступити в зовсім нову еру не просто швидкої, але й безпечної передачі й використання інформації.

На флеш носіях, на даний час переноситься дуже багато конфіденційної інформації. І якщо при утраті флеш носія, ця інформація попаде у руки конкурентів то це приведе до значних економічних збитків, у кращому випадку.

У гіршому випадку, наслідки можуть бути катастрофічними для підприємства або якоїсь установи.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи Flash Drive.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи Flash Drive.

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

- Огляд існуючих систем Flash Drive.
- Дослідження системи Flash Drive.
- Програмна реалізація системи Flash Drive.

Об'єктом дослідження є процес Flash Drive.

Предметом дослідження є методи Flash Drive.

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

Виклад основного матеріалу.

Понад 20 років тому флеш-накопичувачі USB, також відомі як флеш-накопичувачі, вважалися проривом у технології портативного зберігання даних. Сьогодні вони розглядаються як серйозна загроза безпеці.

Експерти з кібербезпеки сходяться на думці, що шифрування USB-флешки є найкращим рішенням для захисту конфіденційних даних. Зашифровані USB-накопичувачі є дуже ефективними інструментами для усунення прогалин у ризиках і допомагають забезпечити безпеку даних, пропонуючи комплексний захист паролем (тобто найсучасніші зашифровані диски забезпечують сертифікацію FIPS, відому як FIPS 140-2 рівня 3 або шифрування військового рівня). додаткові функції включають; видалення даних у випадках, коли спроби введення пароля перевищують встановлений ліміт, технологія захисту від несанкціонованого доступу, щоб запобігти доступу хакерів до внутрішніх компонентів накопичувача (з використанням розширеного апаратного 256-бітного шифрування AES у режимі XTS і надійного захисту від несанкціонованого доступу або «On-Device Crypto chip», який забезпечує додатковий рівень укріплення), антивірусний захист і фізичний рівень захисту від несанкціонованого доступу для дисків із платами з епоксидним покриттям або металевими корпусами, наповненими епоксидною смолою, щоб захистити фізичне сховище від несанкціонованого доступу або з часом пошкодження.

Шифрування портативного флеш-накопичувача USB запобігає потраплянню конфіденційних даних у чужі руки. У цьому посібнику крок за кроком показано, як зашифрувати флеш-накопичувач USB у Windows за допомогою вбудованого засобу шифрування, відомого як BitLocker.

Хоча ОС Windows 10 може розблокувати флеш-накопичувач, зашифрований у Windows 7, і навпаки, USB-накопичувачі, зашифровані за допомогою ОС Windows, не можна відкрити в macOS.

Щодня з’являються нові загрози безпеці ваших даних із заражених апаратних носіїв; наприклад, жорсткі диски, компакт-диски чи картки пам’яті, до пошкодженого програмного забезпечення та шкідливих програм. Переважно з онлайн-джерел; веб-сайти, блоги, електронні листи. Тому дуже важливо підтвердити, що ваш захист від вірусів/шкідливих програм активний у кожній точці входу.

Також важливо переконатися, що ваш антивірус оновлений. Важливо також оснастити хости кінцевих точок для будь-якого пристрою за межами брандмауера найновішим антивірусним програмним забезпеченням. Також зверніть особливу увагу на програми з розширеним захистом від шкідливих програм на USB-пристроях, коли вони використовуються на інших пристроях.

Ключовим фактором, який може поставити під загрозу рівень безпеки флеш-накопичувача, навіть незважаючи на шифрування, є якість накопичувача. Дослідження показують, що безкоштовні накопичувачі, якими користуються на конференціях, ділових зустрічах тощо, часто не можна порівняти з фактичними флеш-накопичувачами найвищої якості, які можуть коштувати вам трохи.

Переваги/відмінності використання цих якісних флеш-накопичувачів USB, на відміну від дешевих роздаткових матеріалів, можна побачити в їх продуктивності та довговічності з часом. Отже, важливо знати різні типи та якості флеш-накопичувачів USB і гарантувати, що ви сплачуєте витрати на безпеку своїх даних.

Окрім фізичного захисту файлів, настійно рекомендується також захистити важливі дані на онлайн-серверах, які називаються «хмарою». До таких серверів належать Dropbox, Google Drive або iCloud. Ці інструменти дозволяють легко зберігати та отримувати файли з будь-якої точки світу.

Зашифрований хмарний сервіс усуває ризик втрати даних через неправильне розташування флешки. Усе, що вам знадобиться, це підключення до Інтернету та ваш

пароль. Важливо також зазначити, що не всі хмарні служби зберігання повністю захищають вашу конфіденційність. Більшість хмарних служб можуть допомогти зашифрувати ваші файли, але збережуть ваші ключі шифрування; тобто вони можуть мати доступ до ваших файлів у будь-який час. Це робить ці служби більш вразливими до витоку даних у разі злому системи.

Ви можете обійти це, використовуючи лише хмарні служби з наскрізним шифруванням; це означає, що ваші дані спочатку шифруються перед надсиланням на їхні сервери, і, таким чином, навіть якщо їхні сервери якимось чином незаконно отримали доступ, лише ви зможете розшифрувати їх, щоб отримати доступ до даних у цих файлах.

Якщо вам потрібно використовувати флеш-накопичувач USB для зберігання даних, є способи покращити захист ваших даних. Читайте далі, щоб дізнатися, як захистити флешку.

Перш ніж зберігати їх на флеш-накопичувачі, важливо спочатку визначити, що вважати конфіденційними даними, а також ширші вимоги щодо безпеки. Конфіденційні дані – це будь-яка конфіденційна інформація, для доступу до якої потрібен дозвіл.

Конфіденційні дані включають таку конфіденційну інформацію – оригінальну або скопійовану:

– Захищена медична інформація (PHI).
– Інформація, що дозволяє ідентифікувати особу (PII).
– Записи про освіту.
– Інформація споживача.
– Дані власника картки.
– Конфіденційна інформація про персонал.
– Конфіденційні дані.

Організації повинні мати суворі методи захисту даних та інформаційної безпеки, щоб гарантувати, що ці дані не будуть скомпрометовані через несанкціонований доступ. Вони також повинні дотримуватися відповідного законодавства про персональні дані, наприклад Загального регламенту захисту даних (GDPR).

Деякі організації можуть запровадити заходи безпеки конфіденційних даних, зокрема:

1. Управління даними.
2. Безпечне керування привілейованим доступом.
3. Шифрування.
4. Програми навчання персоналу.
5. Тестування безпеки даних.
6. Класифікація даних.
7. Плани реагування на інциденти.
8. Регулярне резервне копіювання даних систем зберігання.
9. Безпечні процеси видалення.
10. Моніторинг сторонніх і четвертих постачальників.

Як безпечно зберігати дані на флеш-накопичувачі USB.

Настійно рекомендуємо не зберігати конфіденційні дані на флеш-накопичувачі USB, а натомість вибрати безпечніші пристрої для збереження даних. Їх невеликий розмір дозволяє легко транспортувати, але також легко втратити або вкрасти. Це падіння збільшує ризик втрати даних, витоків і порушень даних, що коштує значних витрат для організацій.

Якщо ви все ж використовуєте флеш-накопичувач, дотримуйтеся цих 7 порад, щоб захистити свої дані.

1. Придбайте зашифрований USB

Шифрування захищає конфіденційну інформацію, роблячи її доступною лише для тих, хто має ключ дешифрування. Купуючи флеш-накопичувач, вам слід вибрати флеш-накопичувач військового класу з 256-бітним апаратним шифруванням AES – найнадійнішим алгоритмом шифрування.

Серед інших функцій зашифрованого USB-накопичувача:

– Захист від злому.

– Антивірусне сканування.
– Захист від грубої сили.
– Захист паролем.
– Відповідність TAA.
– Можливості віддаленого керування.
– Сертифікація FIPS 140-2 (рівень 3).
– Відповідність галузевим стандартам безпеки, таким як HIPAA, SOX і GLBA.

2. Використовуйте програмне забезпечення для шифрування USB

В якості альтернативи придбанню зашифрованого флеш-накопичувача користувачі операційної системи Microsoft Windows можуть використовувати BitLocker для шифрування своїх флеш-накопичувачів. Зауважте, що апаратне забезпечення шифрування забезпечує кращий захист, ніж програмне забезпечення.

Інструкції Microsoft щодо ввімкнення BitLocker доступні нижче:

– Перегляньте інструкції щодо ввімкнення BitLocker у Windows 10.
– Перегляньте інструкції щодо ввімкнення BitLocker у Windows 11.

3. Майте резервну копію

У разі втрати, викрадення чи пошкодження флеш-пам’яті ви можете ніколи не відновити дані, що зберігаються на ній. Навіть якщо втрачену або вкрадену флеш-накопичувач повернули, не слід використовувати його знову, оскільки на ньому потенційно може бути встановлено програмне забезпечення-вимагач або інший тип шкідливого програмного забезпечення. Найкраща гарантія відновлення даних на вашому флеш-пам’яті – це резервна копія всіх файлів, збережена в іншому окремому місці зберігання, наприклад у хмарному сховищі.

4. Видалити дані після використання

Після того, як ви зберегли, відредагували та передали свої дані з USB-накопичувача, найбезпечніше негайно повністю видалити їх. Потім вам слід вийняти флеш-накопичувач із USB-порту та зберігати його в надійному місці, щоб уникнути втрати або крадіжки.

5. Встановіть антивірусний захист

З огляду на те, що різні типи зловмисного програмного забезпечення з’являються щодня, підтримувати ваше програмне забезпечення в актуальному стані є надзвичайно важливим. Використовуйте антивірусне програмне забезпечення, яке забезпечує захист від зловмисного програмного забезпечення на всіх кінцевих точках, включаючи жорсткі диски, USB-пристрої та SD-карти – можна заразити всіх.

6. Оновлюйте програмне забезпечення

Експлойти нульового дня використовують невиправлені вразливості програмного забезпечення – поширений вектор атак, який може мати руйнівні наслідки. Кіберзлочинці можуть легко отримувати доступ, редагувати та викрадати дані з уразливих систем і пристроїв, включаючи USB-накопичувачі.

Якнайшвидше встановлення оновлень програмного забезпечення не дозволить кіберзлочинцям скористатися цими вразливими місцями. Більшість операційних систем, включаючи Microsoft Windows, Mac OS/Apple iOS і Linux, пропонують автоматичні оновлення, щоб забезпечити ваш захист.

7. Використовуйте альтернативні методи зберігання

Зрештою, флеш-накопичувачі не є відповіддю, якщо ви хочете серйозно поставитися до безпеки своїх даних. Навіть найбезпечніші USB-накопичувачі не підходять для сучасних методів зберігання даних, як-от хмарне сховище. Хмарні служби пропонують багато інноваційних функцій безпеки, наприклад Secure Access Service Edge (SASE).

SASE – це хмарна модель безпеки, яка використовує брандмауери, брокери послуг хмарного доступу (CASB), захищений веб-шлюз (SWG) і доступ до мережі без довіри (ZTNA). Інші механізми безпеки хмари включають Cloud Security Posture Management і Cloud Infrastructure Entitlement Management (CIEM).

Незважаючи на потужні можливості безпеки, хмарні служби, як і всі сторонні

постачальники, несуть ризики для третіх сторін та інші ризики, пов'язані з їх функціональністю. Організації та окремі особи повинні проводити належну перевірку, щоб переконатися, що їхні хмарні постачальники дотримуються відповідних вимог безпеки даних.

Найкращі методи безпечного зберігання конфіденційних даних на флеш-накопичувачах USB діляться на дві категорії: профілактичні та реактивні. Профілактичні заходи вимагають глибокого розуміння того, де і коли USB-накопичувачі використовуються у вашій організації, а також їх потенційної можливості бути каналом для кібератак. Реактивні стратегії охоплюють інший кінець спектру та включають методи відновлення даних. Застосуйте обидві стратегії, щоб забезпечити безпечне використання USB-накопичувачів у вашій організації.

6 найкращих методів безпеки для USB-накопичувачів

Застосуйте політику використання USB-накопичувача для всієї організації

Розробіть і запровадьте детальну політику використання USB-накопичувачів, яка описує належне використання, обмеження та вказівки щодо реагування на інциденти.

Проведення аудитів управління активами

Керуйте інвентаризацією флеш-накопичувачів USB, які використовуються у вашій організації. Періодично перевіряйте інвентаризацію, щоб переконатися, що користувачі дотримуються політики використання USB-накопичувача вашої організації.

Використовуйте шифрування для захисту конфіденційних даних

Шифруйте конфіденційну інформацію, що зберігається на USB-накопичувачах. У разі несанкціонованого використання або втрати цих дисків зашифровані файли будуть марними для зловмисників.

Слідкуйте за діями копіювання та передачі файлів

Виявляйте та блокуйте неавторизовану передачу даних і вимагайте автентифікації, коли користувачі копіюють або передають важливі файли на USB.

Резервне копіювання даних із виведених з експлуатації USB-накопичувачів

Якщо USB-накопичувач виведено з експлуатації, створіть резервні копії необхідних файлів і папок, щоб захистити їх розташування, і зітріть усі дані з диска, щоб запобігти витоку даних.

Розгорніть повний антивірусний захист

Періодично перевіряйте кінцеві точки та флеш-накопичувачі USB кожного разу, коли вони використовуються, щоб уникнути зараження зловмисним програмним забезпеченням, яке виникло за межами вашої організації.

USB-накопичувач і безпека - Як захистити вміст USB-накопичувача

USB-накопичувач (USB-накопичувач) дуже корисний, коли дані потрібно транспортувати з одного місця в інше. USB-накопичувач легкий і невеликий за розміром, його можна, наприклад, зберігати в кишені або гаманці. Ви також можете зберігати великі обсяги даних на флеш-накопичувачах USB, на деяких флешках до 64 ГБ, тому, якщо вам потрібно перенести багато даних, використання USB-накопичувачів може бути дуже зручним.

Ризики безпеці

USB-флеш-накопичувачі корисні, але під час носіння USB-флеш-пам'яті слід враховувати певні ризики для безпеки – його можна загубити або вкрасти. Це справді викликає серйозне занепокоєння, якщо накопичувач містить конфіденційну інформацію, наприклад фінансову інформацію, бізнес-плани, вихідний код програмного забезпечення, дані про співробітників, технічні креслення тощо. Щоб запобігти потраплянню інформації в чужі руки, існують флеш-накопичувачі USB які можуть захистити дані, що зберігаються на диску. Дані зберігатимуться в зашифрованому вигляді, і ніхто не зможе отримати до них доступ без правильного пароля, пін-коду, відбитка пальця чи іншої інформації для автентифікації.

Приклади флеш-накопичувачів USB (USB-накопичувачів), які можуть захищати дані

Нижче ми наведемо кілька прикладів флеш-накопичувачів USB, безпека яких була в центрі уваги під час їх створення. Вони використовують всю апаратну систему для захисту вмісту накопичувача.

Sandisk Cruzer Professional – USB-накопичувач Sandisk Cruzer Professional використовує апаратну систему шифрування для шифрування даних, а конфіденційна інформація зберігається в спеціальному захищеному паролем розділі на USB-накопичувачі. Менш конфіденційну інформацію можна зберігати у загальнодоступному місці для легкого доступу та спільного використання. Для захисту даних використовується надійне 256-бітне шифрування AES. На USB-накопичувачі можна зберігати до 8 ГБ.

Corsair Flash Padlock 2 – флеш-накопичувач USB Corsair Flash Padlock 2 використовує вбудоване 256-бітне апаратне шифрування AES для захисту даних, а для доступу до даних необхідно ввести PIN-код із 4–10 цифр (безпосередньо на USB-накопичувачі).. Міцна гумова кришка захищає USB-накопичувач від випадкового фізичного пошкодження. На USB-накопичувачі можна зберігати до 16 ГБ.

Kingston DataTraveler 5000 – флеш-накопичувач USB Kingston DataTraveler 5000 – це флеш-накопичувач USB із сертифікатом FIPS 140-2 рівня 2, який використовує апаратне 256-бітне шифрування AES (у режимі XTS) для захисту даних, що забезпечує дуже високий рівень безпеки. Функції шифрування в DataTraveler були розроблені компанією Spyrus, яка також виготовляє безпечні флеш-накопичувачі USB. Одним із замовників Spyrus є армія США, яка має дуже високі вимоги до безпеки. Ви можете прочитати більше про співпрацю Kingston і Spyrus тут. На цьому USB-накопичувачі можна зберігати до 16 ГБ.

IronKey Enterprise S200 – флеш-накопичувач USB IronKey Enterprise S200 – це флеш-накопичувач USB із сертифікатом FIPS 140-2 рівня 3, який забезпечить дуже високий рівень безпеки. IronKey Enterprise захищає дані за допомогою надійного 256-бітного апаратного шифрування AES, а хмарна система під назвою IronKey Enterprise Management Service дає адміністраторам повний контроль над розгорнутими флеш-накопичувачами USB через Інтернет. Адміністратор може віддалено вимкнути пристрої та стерти дані, якщо це необхідно. IronKey Enterprise також має вбудований активний захист від шкідливих програм. На цьому USB-накопичувачі можна зберігати до 16 ГБ. На ринку доступні інші флеш-накопичувачі USB, які можуть захистити дані. Наприклад, Kingston також має USB-накопичувач (Kingston DataTraveler 6000), який має сертифікат FIPS 140-2 рівня 3. Існують також USB-накопичувачі з меншим рівнем безпеки, які замість цього використовують програмне забезпечення для захисту даних, наприклад SanDisk Cruzer Switch.

Стандарт FIPS 140-2

FIPS 140-2, згаданий у тексті вище, є стандартом комп’ютерної безпеки, який використовується для акредитації криптографічних модулів. Стандарт FIPS 140-2 був створений NIST (Національний інститут стандартизації технологій) і визначає 4 різні рівні безпеки:

– Рівень безпеки 1. Це найнижчий рівень безпеки. Необхідно використовувати принаймні один схвалений алгоритм або схвалену функцію безпеки, але не вимагається жодного фізичного механізму безпеки, окрім основної вимоги для компонентів виробничого класу.

– Рівень безпеки 2. Це другий найнижчий рівень, і він вимагає, щоб було неможливо відкрити або втручатися в фізичний пристрій, не залишивши слідів.

– Рівень безпеки 3. Рівень безпеки 3 вимагає, щоб пристрій виявляв, коли хтось намагається його відкрити, і намагався захистити інформацію різними способами.

– Рівень безпеки 4. Це найвищий рівень безпеки, який вимагає, щоб уся конфіденційна інформація (наприклад, криптографічні ключі та дані автентифікації) була негайно знищена, якщо зловмисник намагається відкрити пристрій або намагається отримати до нього доступ іншим способом.

Захист програмного забезпечення та шифрування

Існують системи безпеки програмного забезпечення, які можуть захищати інформацію незалежно від апаратного забезпечення чи від конкретного виробника USB-накопичувача. Програмні рішення в деяких випадках менш безпечні, ніж апаратні рішення, але в основному рівень безпеки, який вони забезпечують, є достатнім для загального використання. Однією з найбільших переваг використання програмного рішення є те, що воно набагато дешевше. Захищені апаратні рішення часто коштують досить дорого, тому, якщо вам потрібно придбати велику кількість USB-накопичувачів, ви виберете USB-накопичувачі з апаратним захистом, що коштуватиме багато.

Одним із прикладів програмного рішення є інструмент SamLogic CD-Menu Creator, який, незважаючи на свою назву, також можна використовувати з флеш-накопичувачами USB і для захисту даних на диску. Інструмент має вбудовані функції для шифрування та обробки паролів, і ці функції можна використовувати для захисту документів, зображень, малюнків, відео тощо. Функції безпеки в CD-Menu Creator можуть запобігти несанкціонованому доступу до файлів, якщо, наприклад, USB палицю втрачено або вкрадено. Усі конфіденційні файли зберігаються на флеш-накопичувачі USB у зашифрованому вигляді. BitLocker To Go у Windows 10/11 також може захистити флеш-накопичувач USB BitLocker To Go – це нова функція в Windows 10/11, яку можна використовувати для шифрування даних на флеш-накопичувачі USB. Коли ви підключаєте USB-накопичувач до комп'ютера з інстальованою Windows 10/11, вам буде запропоновано ввести пароль, і ви повинні ввести правильний пароль, щоб розблокувати диск і отримати доступ до вмісту. Також можна отримати доступ до вмісту з Windows Vista та Windows XP, якщо запустити спеціальну програму під назвою BitLocker To Go Reader, яка поширюється разом із флеш-накопичувачем (вона автоматично встановлюється на диск Windows 10/11). Але одна відмінність порівняно з Windows 10/11 полягає в тому, що ви можете лише переглядати файли та копіювати їх, але ви не можете записати назад будь-який вміст. USB-накопичувач буде лише для читання.

Розробка структурної схеми

Структурна схема наведена на рисунку 1. З неї ми бачимо, що розроблена система складається з наступних структурних блоків.

1. Дані, які записуються на флешку.
2. Блок шифрування за допомогою алгоритму AES.
3. Блок розшифрування за допомогою алгоритму AES.
4. Флешка на яку записані зашифровані дані.

Основним блок системи є блок шифрування AES. Розглянемо його більш детальніше.

Алгоритм шифрування AES працює наступним чином:

1. Дані для шифрування input, розбивається на блоки та копіюються до установочного масиву State, згідно визначеного правилу.

2. Формується сеансовий ключ Round Key з ключа шифрування Cipher Key, за допомогою функції KeyExpansion().

3. Визначається число раундів в залежності від довжини ключа 10, 12, або 14 разів.

4. Виконання операції шифрування, тобто виконання раундів шифрування визначену в пункті 3 кількість раз:

– застосування SubBytes();
– застосування ShiftRows();
– застосування MixColumns();
– застосування AddRoundKey().

5. Формування блоку зашифрованих даних, для цього після завершення останнього раунду трансформації, State копіюється в output за визначеним правилом.

Алгоритм розшифрування AES працює наступним чином:

1. Дані для розшифрування input, розбивається на блоки та копіюються до установочного масиву State, згідно визначеного правилу.

2. Формується сеансовий ключ Round Key з ключа шифрування Cipher Key, за допомогою функції KeyExpansion().

3. Визначається число раундів в залежності від довжини ключа 10, 12, або 14 разів.

4. Виконання операції розшифрування, тобто виконання раундів шифрування визначену в пункті 3 кількість раз:

– застосування InvShiftRows(), яке призначене для трансформації при розшифруванні яка є зворотною стосовно ShiftRows();

– застосування InvSubBytes();

– застосування InvAddRoundKey().

– застосування InvMixColumns().

5. Формування блоку роз зашифрованих даних, для цього після завершення останнього раунду трансформації, State копіюється в output за визначеним правилом.

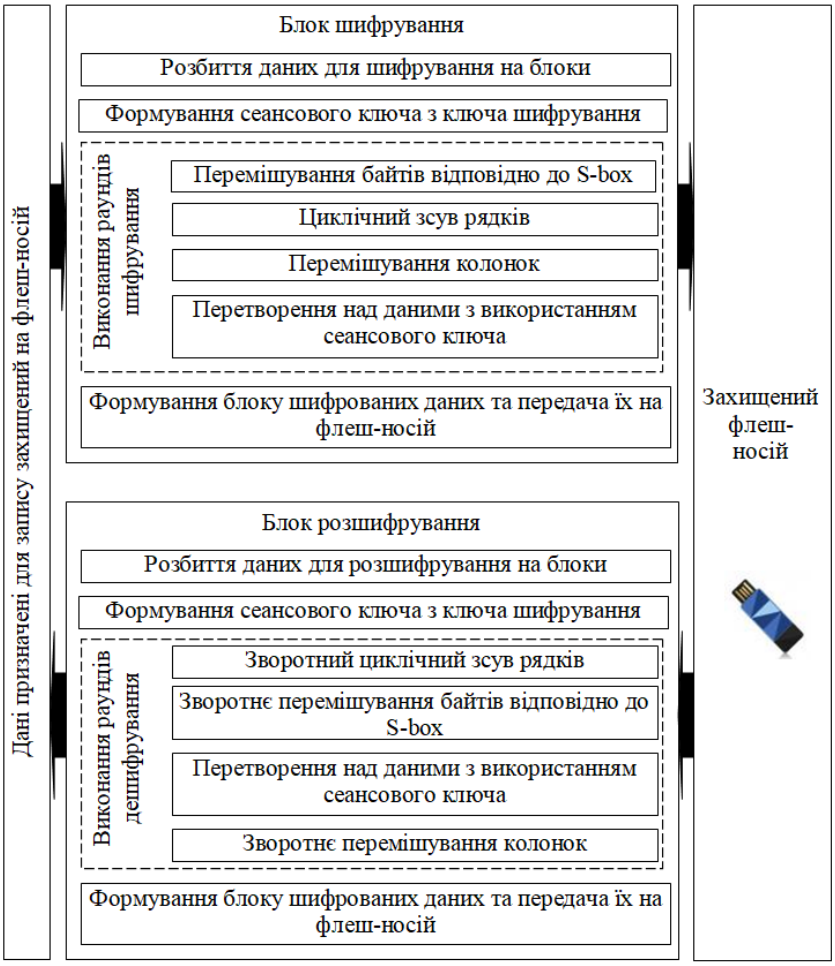

Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів Flash Drive. Рішення даного завдання полягало у вирішенні наступних задач: Був проведений огляд існуючих систем Flash Drive. Досліджена система Flash Drive. На основі отриманих результатів досліджень створена програмна реалізація системи Flash Drive. Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання Flash Drive. 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. 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. (Scopus).
2. 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. (Scopus).
3. Smirnov O., Kuznetsov A., Kryvinska N., Kiian A., Kuznetsova K. «Full Non-Binary Constant-Weight Codes». SN Computer Science, Vol 2, 337, 2021. https://doi.org/10.1007/s42979-021-00739-w (Scopus).
4. Smirnov O., Kovalenko O., Kovalenko A., Kavun S. «Quantitative Risk Assessment Method Development in the Context of the SDLC-model». 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2021, pp. 203-208, doi: 10.1109/PICST54195.2021.9772143 (Scopus).
5. Smirnov O., Neskorodieva T., Fedorov E., Rymar P. «Neural Network Modeling Method of Transformations Data of Audit Production with Returnable Waste». CEUR Workshop Proceedings Volume 3101, 2021, Pages 192-207. (Scopus).
6. 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. (Scopus).
7. 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. (Scopus).
8. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114. (Scopus).
9. Smirnov O.A., 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. (Scopus).
10. 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. (Scopus).
11. 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. (Scopus).
12. 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. (Scopus).
13. 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. (Scopus).
14. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136. (Scopus).
15. Smirnov, O., Drieieva, H., Drieiev, O., Polishchuk, Y., Brzhanov, R., Aleksander, M. «Method of fractal traffic generation by a model of generator on the graph». CEUR Workshop Proceedings Volume 2616, 2020, Pages 366-379. (Scopus).
16. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43. (Scopus).
17. Smirnov, O., Drieieva, H., Drieiev, O., Simakhin, V., Bondar, S., Odarchenko, R. «Managing multifractal properties of the binary sequence generated with the Markov chains», CEUR Workshop Proceedings Volume 2608, 2020, Pages 633-645. (Scopus).
18. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660., (Scopus).
19. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407. (Scopus).
20. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019. (Scopus).