УДК 004

Б.Золотухін, магістр гр. КІ-22М-1,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ СИСТЕМИ УПРАВЛІННЯ ДАНИМИ ЗОВНІШНІХ ЖОРСТКИХ ДИСКІВ З ІНТЕРФЕЙСОМ USB 3.0

У статті розроблено програмне забезпечення, яке призначено для системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0. Метою розробки є дослідження та програмна реалізація системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0. Об'єктом дослідження є процес управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0. Предметом дослідження є методи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0. Методи дослідження базуються на методах теорії архітектури персональних комп'ютерів, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Постановка проблеми. Зовнішні жорсткі диски, флеш-накопичувачі (USB) і карти пам'яті – усі ці пристрої роблять резервне копіювання та обмін даними дуже простими. Вони стають більш цінними, оскільки сучасне навчання, робота та життя переповнені даними.

Завдяки високій місткості, невеликому розміру та портативності вони є чудовими варіантами для передачі або перегляду даних з одного ПК на інший. Однак що станеться, якщо ви втратите або загубите будь-який із цих пристроїв?

У багатьох випадках це призведе до витоку даних. Цих порушень даних можна уникнути, якщо ви зашифруєте свої зовнішні жорсткі диски або USB-накопичувачі.

У разі шифрування хакерам важко отримати доступ до даних, які містять ці пристрої, якщо їх викрадуть або заблукають.

Зовнішні жорсткі диски, флеш-накопичувачі (USB) і карти пам'яті спрощують резервне копіювання та обмін даними. Однак якщо ви втратите або загубите будь-який із цих пристроїв, це може призвести до витоку даних.

Цих порушень даних можна уникнути, якщо ви зашифруєте свої зовнішні жорсткі диски або USB-накопичувачі. У разі шифрування хакерам важко отримати доступ до даних, які містять ці пристрої, якщо їх викрадуть або заблукають.

Проведені дослідження показали, що одним з найбільш перспективних напрямків управління даними з ціллю збереження конфіденційності інформації на зовнішніх носіях, зокрема на зовнішніх жорстких дисках інтерфейсу USB 3.0, є використання потокових шифрів.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-20] було виявлено певні прогалини у забезпеченні системи управління даними зовнішніх жорстких дисків з інтерфейсом usb 3.0.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.

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

– Огляд існуючих систем управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.

– Дослідження системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.

– Програмна реалізація системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.

Об'єктом дослідження є процес управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.

Предметом дослідження є методи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.

Методи дослідження базуються на методах теорії архітектури персональних комп'ютерів, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. USB-накопичувачі та ключі, маленькі, здавалося б, нешкідливі пристрої, які ми часто використовуємо для передачі файлів або зберігання даних, стали мимовільними спільниками в руках зловмисників. Потенційний вплив USB-атак тільки посилився зі збільшенням віддаленої роботи та хмарного сховища. Оскільки працівники часто підключають USB-пристрої до корпоративних мереж або персональних комп'ютерів, ризик мимовільного запровадження зловмисного програмного забезпечення чи шкідливого коду зріс.

Незважаючи на зосередженість на загрозах ШІ та фішингових атаках, USB-накопичувачі та ключі продовжують використовуватися для проникнення в системи та компрометації конфіденційних даних. У цій статті досліджується відродження USB-атак і пропонується уявлення про ефективні стратегії запобігання.

Чому USB-атаки повертаються

Зловмисники адаптують тактику, щоб обійти традиційні засоби захисту, переглядаючи атаки на основі USB через їхню ефективність і низький рівень виявлення. USB-пристрої поширені в особистих і професійних налаштуваннях і надають широкі можливості для проникнення. Використовуючи людські помилки та довіру, групи загроз використовують уразливості USB, такі як функції автоматичного запуску та легке втручання, для легкого проникнення в системи.

Недавні інциденти, висвітлені в основній презентації Майї Горовіц на CPX 2024, служать гострим нагадуванням про відновлення атак через USB. Групи загроз, такі як китайська Camaro Dragon і російська Gamaredon, продемонстрували незмінну актуальність USB-пристроїв як основних переносників інфекції. Ці інциденти підкреслюють постійну загрозу, яку становлять атаки на основі USB, і посилюють потребу організацій і окремих осіб залишатися пильними.

Розуміння методів атак USB

USB-атаки можуть приймати різні форми, від використання людської цікавості до розповсюдження заражених дисків у громадських місцях. Основні методи атаки включають атаки натисканням клавіші, перепрограмування мікропрограми та атаки з відкиданням USB, кожна з яких призначена для компрометації систем і викрадення конфіденційних даних.

Ін'єкція натискання клавіші

Цей тип атаки маніпулює функціями USB-пристроїв, щоб імітувати натискання клавіш у цільовій системі. Це часто досягається за допомогою спеціально створених USB-пристроїв, таких як емулятори HID (Human Interface Device) або гумові пристрої. Зловмисники попередньо завантажують на ці пристрої шкідливі сценарії або корисні навантаження, які імітують введення користувача, наприклад введення команд або виконання макросів. При підключенні до комп'ютера жертви USB-пристрій емулює введення з клавіатури, минаючи традиційні заходи безпеки та потенційно виконуючи зловмисні команди або запускаючи зловмисне програмне забезпечення.

Перепрограмування прошивки

Перепрограмування мікропрограми передбачає зміну мікропрограми USB-пристрою з метою введення шкідливого коду або зміни його функціональності. Зловмисники можуть

використовувати уразливості в мікропрограмі USB-пристроїв, щоб отримати несанкціонований доступ або контроль над пристроєм. Перепрограмувавши прошивку, зловмисники можуть імплантувати бекдори, руткіти або інші форми зловмисного програмного забезпечення на USB-пристрій, дозволяючи їм постійно заражати системи під час підключення.

USB Drop Attacks

USB-атаки передбачають стратегічне розміщення заражених USB-накопичувачів або пристроїв у громадських місцях, де нічого не підозрюють особи можуть знайти та підключити їх до своїх комп'ютерів. Зловмисники можуть маскувати ці пристрої як загублені або покинуті, використовуючи людську цікавість і вроджене бажання досліджувати та потенційно використовувати знайдені об'єкти. Після підключення до комп'ютера жертви заражений USB-пристрій може виконувати зловмисний код, використовувати вразливості або запускати атаки соціальної інженерії для отримання несанкціонованого доступу до системи.

Останні загрози USB-накопичувача для 2024 року

Варті уваги загрози, такі як зараження зловмисним програмним забезпеченням SOGU, зараження зловмисним програмним забезпеченням SNOWYDRIVE і зараження WispRider, підкреслюють еволюцію загроз на основі USB. Ці шкідливі кампанії спрямовані на різні галузі промисловості та використовують складні методи проникнення в мережі та компрометації систем.

Шкідливе зараження SOGU

Варіант зловмисного програмного забезпечення SOGU розроблено для того, щоб залишатися непомітним і уникати виявлення традиційним антивірусним програмним забезпеченням. Коли USB-накопичувач, заражений шкідливим програмним забезпеченням SOGU, підключений до системи, він може виконувати шкідливий код, викрадати конфіденційну інформацію або встановлювати канали несанкціонованого доступу.

SNOWYDRIVE Зараження шкідливим програмним забезпеченням

Цей складний варіант зловмисного програмного забезпечення здатний поширюватися через USB-накопичувачі та використовувати вразливі місця в цільових системах. SNOWYDRIVE може використовувати різні методи, такі як безфайлове виконання або поліморфний код, щоб уникнути виявлення та компрометації систем. Після активації SNOWYDRIVE може викрадати дані, встановлювати бекдори або сприяти віддаленому доступу, створюючи значний ризик для безпеки та цілісності уражених мереж.

Інфекція WispRider

Зловмисне програмне забезпечення WispRider вправно обходить традиційні заходи безпеки та використовує USB-пристрої як засіб проникнення. WispRider може використовувати передові методи обфускації або використовувати вразливості нульового дня, щоб непомітно зламати системи. Це створює серйозну загрозу для конфіденційності, цілісності та доступності цільових систем і даних.

Найкращі методи запобігання атак через USB

Для подолання атак через USB потрібен багаторівневий підхід, який поєднує технологічні рішення з обізнаністю користувачів і проактивними заходами безпеки. Нижче наведено кілька практичних порад щодо запобігання атакам через USB:

Впроваджуйте рішення безпеки кінцевих точок

Використовуйте антивірусне програмне забезпечення та системи EDR для виявлення та блокування зловмисної активності, що походить від пристроїв USB.

Розповідайте користувачам про ризики

Розкажіть співробітникам про ризики підключення невідомих USB-пристроїв і заохочуйте їх повідомляти про підозрілу діяльність персоналу служби безпеки IT.

Вимкніть функцію автозапуску

Запобігайте автоматичному виконанню програм, вимкнувши функцію автозапуску в операційних системах Windows, зменшуючи ризик розповсюдження шкідливих програм через USB-накопичувачі.

Регулярно оновлюйте системи

Переконайтеся, що операційні системи, додатки та програмне забезпечення безпеки регулярно оновлюються, щоб усунути прогалини в безпеці та зменшити ризик використання USB.

Використовуйте інструменти безпеки USB

Розгортайте рішення для моніторингу USB кінцевої точки та програмне забезпечення для керування пристроями, щоб застосовувати політики, відстежувати активність USB і блокувати неавторизовані пристрої або файли.

Роль зашифрованих USB-пристроїв

Зашифровані USB-пристрої, такі як ті, що пропонує DataLocker, відіграють вирішальну роль у зменшенні ризиків атак USB. Забезпечуючи сумісне з FIPS 140-2 шифрування та постійну безпеку, зашифровані USB-пристрої DataLocker гарантують захист конфіденційних даних навіть у разі атаки через USB.

Відповідність стандарту FIPS 140-2

Зашифровані USB-пристрої від DataLocker відповідають Федеральним стандартам обробки інформації (FIPS) 140-2, широко визнаному стандарту для криптографічних модулів. Ця відповідність гарантує, що алгоритми шифрування та механізми безпеки, які використовуються пристроями DataLocker, відповідають суворим вимогам безпеки, встановленим урядовими установами та органами галузевих стандартів.

Постійна безпека

Зашифровані USB-пристрої DataLocker забезпечують постійні функції безпеки, які допомагають запобігти несанкціонованому доступу до конфіденційних даних. Ці функції можуть включати апаратне шифрування, автентифікацію пароля та можливості віддаленого керування.

Керування пристроєм USB

DataLocker пропонує SafeConsole, комплексне програмне забезпечення для керування пристроями для централізованого керування та моніторингу зашифрованих USB-пристроїв, розгорнутих в організації. SafeConsole дозволяє адміністраторам застосовувати політики безпеки, віддалено налаштовувати параметри пристрою та відстежувати використання та активність пристрою.

Зменште ризики USB і загрози безпеці шляхом впровадження зашифрованих USB-пристроїв

Оскільки USB-атаки продовжують створювати значні ризики для окремих осіб і організацій, впровадження надійних заходів запобігання є першорядним. Використовуючи зашифровані USB-пристрої та приймаючи постійну безпеку, компанії можуть ефективно зменшити ризики атак USB і захистити конфіденційні дані.

У роботі пропонується використання жорсткого диску Verbatim Store n Go.

Портативний жорсткий диск Verbatim Store n Go оснащений високопродуктивним накопичувачем за допомогою інтерфейсу USB 3.0 «Super Speed». USB 3.0 забезпечує до 10 разів більшу швидкість передачі даних, ніж USB 2.0 (на основі швидкості шини USB), забезпечуючи надшвидку передачу даних у дорозі.

Зберігайте та переносьте свої цифрові та повсякденні файли на цьому справді мобільному накопичувачі. Його стильний дизайн акуратно розміщується на сучасному столі як ідеальне доповнення до вашого ноутбука.

Портативний жорсткий диск Store n Go живиться від шини USB 3.0 (1 x інтерфейс USB 3.0), але зворотно сумісний з будь-якими портами USB 2.0 на вашому ПК чи ноутбуці. Привід не вимагає зовнішнього живлення для роботи; просто plug n play.

Диски ємністю 2 ТБ або менше відформатовані у FAT32, що дозволяє їм негайно працювати в Windows і Mac OSx. Диски об'ємом понад 2 ТБ відформатовано у NTFS, яка сумісна з системами Windows, але від користувачів Mac потрібно переформатувати диск у HFS+, щоб зробити їх повністю сумісними з операційними системами Mac OSx. Форматування HFS+ можна застосувати за допомогою Verbatim VHD Formatter, який є на диску.

Для додаткової безпеки надається програмне забезпечення Nero Backup, яке допоможе створити резервну копію жорсткого диска вашого ноутбука чи ПК. Резервне копіювання надає програму для резервного копіювання всіх ваших файлів, папок і дисків у будь-який час або за плануванням автоматичного резервного копіювання на встановлений час для додаткової безпеки.

Програма Nero Backup Software сумісна з Windows XP, Vista, Windows 7, Windows 8 і Windows 10 (не сумісна з Mac OS).

Портативні жорсткі диски Verbatim Store 'n' Go також постачаються з програмним забезпеченням для збереження енергії Green Button. Програмне забезпечення Green Button призупиняє обертання жорсткого диска, коли він не використовується, підвищуючи ефективність і заощаджуючи енергію.

Є 3 варіанти «Налаштування сну». Встановіть режим призупинення на ввімкнення через 10 хвилин використання або з кроком від 10 хвилин до 120 хвилин. Налаштуйте диск на негайне призупинення, двічі клацнувши піктограму зеленої кнопки на робочому столі, або ви можете встановити диск у режим «Ніколи не призупиняти диск».

Деталі продукту:

– Ємність: 1 ТБ.
– Інтерфейс: USB 3.0.
– Розміри: 119 мм x 81 мм x 14,5 мм.
– Вага продукту: 158 г.
– Висока швидкість, велика ємність зберігання. Швидке та безпечне рішення для розширення пам'яті або резервного копіювання файлів.
– USB 3.0 SuperSpeed - для надшвидкої передачі даних.
– USB plug 'n' play (додаткове живлення не потрібне).
– Програма резервного копіювання Nero.
– Програмне забезпечення для енергозбереження
– USB REC & PLAY* - підтримує запис/відтворення USB

*може бути недоступним у деяких країнах.

Потокові шифри засновані на РЗЛЗЗ. Ускладнення

На жаль, вихідна послідовність РЗЛЗЗ легко передбачувана. Так, знаючи 2L знаків вихідної послідовності, легко знайти вихідне заповнення регістра, вирішивши систему лінійних рівнянь.

Уважається, що для криптографічного використання вихідна послідовність РЗЛЗЗ повинна мати наступні властивості:

– великий період;
– високу лінійну складність;
– гарні статистичні властивості.

Існує кілька методів проектування генераторів ключового потоку, які руйнують лінійні властивості РЗЛЗЗ і тим самим роблять такі системи криптографічнобільше стійкими:

– використання нелінійної функції, що поєднує виходи декількох РЗЛЗЗ;
– використання нелінійної фільтруючої функції для вмісту кожного осередку єдиного РЗЛЗЗ;
– використання виходу одного РЗЛЗЗ для керування синхросигналом одного (або декількох) РЗЛЗЗ.

Нелінійна комбінація генераторів

Відомо, що кожна булева функція:

$$f(x_1, x_2, \ldots, x_n),$$

може бути записана як сума за модулем 2 добутків порядків m незалежних змінних:

$$0 \leqslant m \leqslant n.$$

Це вираження називається алгебраїчною нормальною формою функції f. Нелінійним порядком функції f називається максимальний порядок членів у записі її алгебраїчної нормальної форми.

Генератор Геффа

У цьому генераторі використовуються три РЗЛЗЗ, об'єднані нелінійним образом. Довжини цих регістрів:

$$L_1, L_2, L_3,$$

попарно прості числа.

Нелінійну функцію для даного генератора можна записати в такий спосіб:

$$f(x_1, x_2, x_3) = x_1x_2 \oplus (1 + x_2)x_3 = x_1x_2 \oplus x_2x_3 \oplus x_3.$$

Довжина періоду:

$$(2^{L_1} - 1) \cdot (2^{L_2} - 1) \cdot (2^{L_3} - 1).$$

Лінійна складність:

$$L = L_1 \cdot L_2 + L_2 \cdot L_3 + L_3.$$

Генератор Геффа криптографічнослабшав, тому що інформація про стани генераторів РЗЛЗЗ 1 і РЗЛЗЗ 3 утримується в його вихідній послідовності.

Генератор на нелінійному фільтрі

Вихід кожного осередку подається на вхід деякої нелінійної булевої фільтруючої функції f. Припустимо, що фільтруюча функція порядку m, тоді лінійна складність потоку ключів не більше:

$$L_m = \sum^{m} \left(.$$

Генератори засновані на керуванні синхросигналом

У нелінійних комбінаціях генераторів і генераторах на нелінійних фільтрах переміщення даних у всіх РЗЛЗЗ контролюється одним синхросигналом.

Основна ідея функціонування розглянутого типу генераторів – внести нелінійність у роботу генераторів потоку ключів, заснованих на РЗЛЗЗ, шляхом керування синхросигналом одного регістра вихідною послідовністю іншого.

Є 2 типи генераторів заснованих на керуванні синхросигналом:

– генератор змінного кроку;
– стискаючий генератор.

Генератор змінного кроку

РЗЛЗЗ 1 використовується для керування пересуванням бітів двох інших РЗЛЗЗ 2 і 3.

Алгоритм роботи:

1. Регістр РЗЛЗЗ 1 синхронізований зовнішнім синхросигналом.

2. Якщо на виході регістра РЗЛЗЗ 1 одиниця, то на регістр РЗЛЗЗ 2 подається синхросигнал, а РЗЛЗЗ 3 повторює свій попередній вихідний біт (для початкового моменту часу попередній вихідний біт РЗЛЗЗ 3 приймається рівним 0).

3. Якщо на виході регістра РЗЛЗЗ 1 нуль, то на регістр РЗЛЗЗ 3 подається синхросигнал, а РЗЛЗЗ 2 повторює свій попередній вихідний біт (для початкового моменту часу попередній вихідний біт РЗЛЗЗ 2 також приймається рівним 0).

4. Вихідна послідовність бітів генератора зі змінним кроком є результатом застосування операції побітового АБО, що виключає, до вихідних послідовностей регістрів РЗЛЗЗ 2 і РЗЛЗЗ 3.

Збільшення безпеки генераторів зі змінним кроком:

– довжини регістрів РЗЛЗЗ 1, РЗЛЗЗ 2, РЗЛЗЗ 3 повинні бути обрані попарно простими числами;

– довжини цих регістрів повинні бути близькими числами.

Стискаючий генератор

Контролюючий регістр РЗЛЗЗ 1 використовується для керування виходом РЗЛЗЗ 2.

Алгоритм:

– Регістри РЗЛЗЗ 1 і РЗЛЗЗ 2 синхронізовані загальним синхросигналом.

– Якщо вихідний біт РЗЛЗЗ 1 дорівнює 1, вихід генератора формується вихідним бітом регістра РЗЛЗЗ 2.

– Якщо вихідний біт РЗЛЗЗ 1 дорівнює 0, вихідний біт регістра РЗЛЗЗ 2 відкидається.

Стискаючий генератор простий, масштабуємий й має гарні захисні властивості. Його недолік полягає в тому, що швидкість генерації ключа не буде постійної, якщо не прийняти деяких обережностей.

Для збільшення безпеки стискаючого генератора:

– довжини регістрів РЗЛЗЗ 1 і РЗЛЗЗ 2 повинні бути взаємно простими числами;

– бажано використовувати сховане з'єднання між регістрами РЗЛЗЗ 1 і РЗЛЗЗ 2.

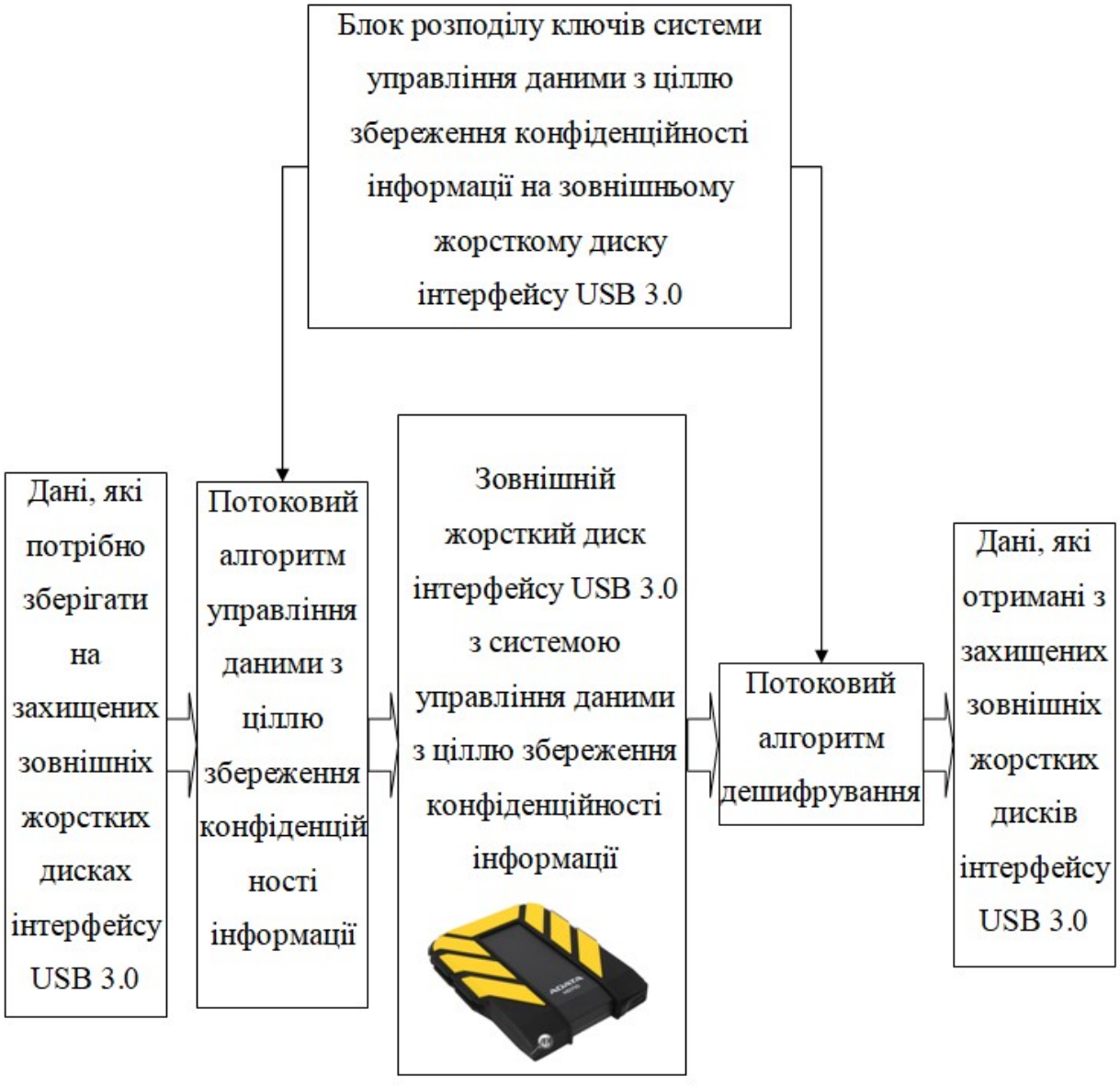

Рисунок 1 – Структурна схема системи

Структурна схема зображена на рисунку 1. У процесі управління даними з ціллю збереження конфіденційності інформації використовується певний алгоритм управління даними з ціллю збереження конфіденційності інформації, на вхід якому подаються вихідні незашифровані дані, називані також plaintext, і ключ. Виходом алгоритму є зашифровані дані, називані також ciphertext. Ключ є значенням, що не залежить від шифруємих даних. Зміна ключа повинна приводити до зміни зашифрованого повідомлення.

Зашифровані дані зберігаються на зовнішньому жорсткому диску інтерфейсу USB 3.0 й передаються одержувачеві, при читанні даних з зовнішнього жорсткого диску інтерфейсу USB 3.0. Одержувач перетворить зашифровані дані у вихідні незашифровані дані за допомогою алгоритму дешифрування даних з ціллю збереження конфіденційності інформації й того ж самого ключа, що використовувався при шифруванні, або ключа, легко одержуваного із ключа управління даними з ціллю збереження конфіденційності інформації.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.

– Досліджена система управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.

– На основі отриманих результатів досліджень створена програмна реалізація системи управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання управління даними зовнішніх жорстких дисків з інтерфейсом USB 3.0.

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.