

## **Система зберігання даних з обмеженим доступом на основі флеш-пам'яті**

**Стан проблеми.** Програми для зберігання даних на флеш-пам'яті широко використовуються в різних сферах, від особистих пристроїв до корпоративних систем. Важливою характеристикою цих засобів є здатність захищати інформацію, зберігати її у зашифрованому вигляді та забезпечувати доступ лише до авторизованих комп'ютерів. Нині існує ряд підходів до забезпечення безпеки даних, проте не всі вони враховують специфіку флеш-пам'яті. Методи генерації HWID використовують різні параметри апаратного забезпечення, що дає можливість створювати унікальні ідентифікатори [1]. Аналіз методів і технологій, що використовуються для ідентифікації пристроїв, свідчить про необхідність удосконалення існуючих алгоритмів [2], тому розроблення системи, яка забезпечить не лише захищене зберігання даних на основі флеш-пам'яті, але й ініціалізацію пристрою, налаштування захисту, верифікацію HWID є актуальним завданням.

**Розв'язання задачі.** Для досягнення поставленого завдання розроблено пристрій та програмне забезпечення, які організують захищене зберігання даних на основі флеш-пам'яті з використанням механізмів шифрування та унікальних апаратних ідентифікаторів (HWID). Розроблений пристрій передбачає перевірку HWID під час підключення до комп'ютера, що забезпечує доступ до даних лише авторизованим користувачам. Цей підхід гарантує високий рівень безпеки даних і є ефективним рішенням для захисту інформації. Алгоритм роботи системи передбачає, що при підключенні пристрою до ПК відбувається перевірка HWID, і лише за умови його відповідності - надається доступ до даних на флеш-пам'яті [3].

Для реалізації захищеного пристрою зберігання даних на основі флеш-пам'яті, використано плату Arduino та модуль з SD-картою. Модуль з SD-картою дає можливість зберігати великі обсяги інформації у компактному форматі і підтримує різні формати файлів.

Структура програмної системи захищеного зберігання даних наведена на рисунку 1. Система містить такі модулі:

- модуль ініціалізації, що виконує налаштування після підключення пристрою;

- модуль визначення - перевіряє чи пристрій є захищеним і визначає, чи буде надано доступ до даних;
- модуль роботи з флеш-пам'яттю - реалізує операції зберігання та зчитування даних;
- модуль налаштування захисту пристрою - дає можливість користувачу адаптувати параметри безпеки згідно з його вимогами.

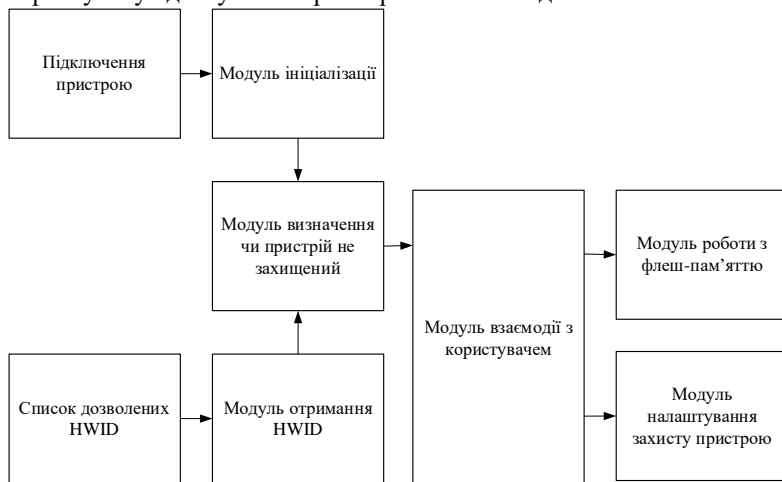


Рисунок 1. Структурна схема роботи програмної системи захищеного зберігання даних на основі флеш-пам'яті.

**Висновки.** У роботі розглянуто проблему захисту пристроїв за допомогою унікальних ідентифікаторів HWID та розроблено систему, що забезпечує перевірку захисту пристроїв. Розроблена система також забезпечує комплексний підхід до захищеного зберігання даних та контролю доступу на основі HWID і зручний та безпечний процес роботи з інформацією.

#### Література.

- [1] Khan, A., & Ali, M. Data Protection and Device Security: An Overview. *Advances in Computer Science and Engineering*, 11(5), 2021, pp. 12-24.
- [2] Smith, R. Understanding HWID: A Key to Device Security. *Security Magazine* [електронний ресурс]. – Режим доступу: [https:// www.securitymagazine.com](https://www.securitymagazine.com)
- [3] Feng, H., & Liu, Y. Innovative Techniques for HWID Generation. *Journal of Information Technology and Security*, 14(1), 2023, pp 55-65.