УДК 004.4'277.2.056.55

**А. О. Азарова, Н. О. Біліченко,**
**В. С. Катаєв, П. В. Павловський**
Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

# Розроблення пристрою для захисту від несанкціонованого доступу на основі трифакторної ідентифікації та аутентифікації користувачів

*Запропоновано пристрій для забезпечення захисту від несанкціонованого доступу до інформації на основі використання трифакторної ідентифікації та автентифікації користувачів з можливістю розмежування доступу до інформаційного середовища. Пристрій дозволяє: завчасно виявляти спроби несанкціонованого доступу, надавати доступ до інформаційних ресурсів санкціонованим користувачам, навіть у випадку відмови пристрою та під час виникнення аварійних ситуацій. Він має підвищену довговічність і стійкість до фізичного зламу, покращує системи захисту інформації на різних суб'єктах господарювання, є більш інформативним, простим для користувача, не вимагає спеціальних знань у сфері технічного захисту інформації, дозволяє завчасно виявити спроби несанкціонованого доступу, відновити основні функції пристрою в аварійних ситуаціях і має значно нижчу ціну.*

***Ключові слова:*** *несанкціонований доступ, трифакторна аутентифікація, ідентифікація користувача, біометричне сканування відбитків пальців, QR-ідентифікатор, парольна ідентифікація.*

## Вступ

Під захистом інформації розуміють сукупність організаційно-технічних заходів і норм, що спрямовані на запобігання заподіянню шкоди інтересам власника цієї інформації, а також осіб, які користуються нею. При цьому об'єктом захисту є не лише інформація, що обробляється, передається та зберігається у будь-якому вигляді як в автоматизованій системі, так і за допомогою інших засобів оброблення інформації, але й права власників цієї інформації і власників автоматизованої системи, а також права користувача.

Захист прав суб'єктів в аспектах формування, користування інформаційними ресурсами, розроблення, виробництва та застосування інформаційних систем, технологій і засобів їхнього забезпечення здійснюється з метою попередження пра-

вопорушень, неправомірних дій, відновлення порушених прав і відшкодування заподіяної шкоди [1].

Необхідність вирішення проблеми захисту від несанкціонованого доступу полягає в потребі:

— дотримання правил розмежовування доступу до інформації в установах, незалежно від посади та рівня доступу;

— усунення можливості несанкціонованого доступу до інформації як працівників, що не мають доступу до неї, так і третіх осіб;

— забезпечення цілісності конфіденційної інформації і дотримання необхідних умов її збереження;

— вчасного виявлення витоку інформації.

Проблематикою захисту інформації займаються провідні закордонні та вітчизняні науковці, серед яких слід відзначити О.Д. Азарова, Дж. Уілсона, О.Г. Додонова, В.В. Карпінця, Д.В. Ланде, О.О. Торокіна, О.О. Хорєва, В.О. Хорошка, М.Є. Шелеста, Ю.Є. Яремчука та ін. Останнім часом велика кількість робіт присвячена багатофакторній ідентифікації і біометричному захисту інформації, серед яких варто відзначити праці таких дослідників як Х.А. Бугаєнко, Р. Болл, О.В. Дубчак, В.П. Захаров, В.М. Лукашенко, А.О. Мороз, Ч. Стюарт та ін.

## Постановка задачі та метод дослідження

Не зважаючи на значний науковий доробок у цій царині знань, невирішеною залишається проблема несанкціонованого доступу до інформації, оскільки пристрої, створені на базі різних поодиноких підходів, мають такі недоліки:

— складність налаштування та обслуговування;

— відсутність або недостатність правил розмежування прав доступу;

— необґрунтована цінова політика;

— наявність у деяких засобах захисту механічного ключа доступу;

— відсутність у більшості модифікацій візуального інтерфейсу.

Разом з тим, вирішенню питань із забезпечення високого ступеня захисту інформації відповідає лише комплексна система захисту інформації, до складу якої входять програмні, апаратно-програмні, організаційні, фізичні та технічні засоби захисту. У свою чергу, для отримання необхідного рівня захисту конфіденційної інформації необхідно поєднувати як організаційні засоби — посадові інструкції, правила розмежування доступу, так і технічні прилади для захисту інформації від витоку технічними каналами.

Аналіз недоліків і переваг різних систем захисту, що базуються на апаратно-програмних складових безпеки, дозволив обрати авторам статті найбільш ефективні методи захисту інформації на основі: біометричних особливостей людини, які є невід'ємними від неї, метода QR-ідентифікації користувача, тобто те, що він має, а також парольного захисту — те, що знає користувач.

Отже, розроблення нового функціонального пристрою з використанням методу багатофакторної (трифакторної) ідентифікації на основі поєднання біометричного сканування відбитків пальців, QR-ідентифікатора та парольної ідентифікації, що уможливлює усунення недоліків існуючих підходів та забезпечує висо-

кий рівень захисту інформації є надзвичайно актуальним у сучасних системах безпеки.

***Метою*** статті є підвищення рівня захисту від несанкціонованого доступу шляхом розроблення та застосування пристрою на основі трифакторної ідентифікації та аутентифікації користувача.

Сучасні технології захисту конфіденційної інформації реалізуються на базі наступних методів:

1) апаратних — генераторів кодів, біометричних пристроїв і пристроїв «прозорого» шифрування;

2) програмних — антивірусного ПЗ, криптографічних засобів, засобів ідентифікації санкціонованих користувачів, засобів аудиту;

3) організаційних — розроблення нормативно-правової документації, що регламентує створення, оброблення, зберігання, передавання та отримання, захист конфіденційної інформації, а також заснування відділу інформаційної безпеки, що несе відповідальність за інформаційну безпеку організації у цілому [2].

Апаратні та програмні засоби і заходи захисту засновані на використанні електронних пристроїв і спеціального ПЗ, які входять до складу автоматизованих систем і виконують функції захисту інформації самостійно або в комплексі з іншими засобами захисту інформації.

Організаційні заходи захисту інформації містять сукупність дій з підбору та перевірки персоналу, який бере участь у підготовці й експлуатації програм та інформації, чіткого регламентування процесу розроблення та функціонування інформаційної системи. Організаційні заходи захисту інформації також описані у посадових інструкціях працівників установи. Оскільки організаційний захист не виключає витік інформації у цілому, то необхідним є застосування апаратних і програмних засобів захисту разом.

Найбільш раціональним є впровадження програмних комплексів захисту інформації, оскільки вони не вимагають розроблення, закупівлі обладнання та додаткового підвищення кваліфікації працівників організації, але найбільш перспективним є захист конфіденційної інформації за допомогою криптографічних засобів та апаратно-програмних засобів захисту, наприклад, у державних установах, де витік інформації може надати шкоди державі в цілому [3].

Отже, лише комплексне використання засобів і заходів захисту інформації забезпечує надійний захист, оскільки будь-який із методів не позбавлений своїх вад.

Для створення системи захисту інформації, наперед усе, необхідно забезпечити розпізнавання санкціонованого користувача, що має назву авторизація користувачів у системі [4].

Авторизованим користувачем називається особа, яка набула визначених прав доступу для роботи з конфіденційною інформацією. У процесі авторизації для санкціонованого користувача (СК) визначаються права користувача, тобто визначаються дані, з якими йому дозволено працювати, а також операції, які йому дозволено виконувати.

Авторизація СК здійснюється за такими етапами:

1) ідентифікація користувача — присвоєння унікального ідентифікатора, який використовується для розпізнавання у системі;

2) аутентифікація користувача — підтвердження справжності особи, що виконується на основі порівняння з еталонним ідентифікатором;

3) безпосередньо авторизація користувача — встановлення прав СК у системі.

Удосконалення авторами методу трифакторної аутентифікації полягає в комплексному використанні біометричного сканування відбитків пальців, QR-ідентифікатора та парольної ідентифікації.

Отже, у статті розглядається процес розроблення пристрою захисту інформації на основі поєднання трьох методів захисту з урахуванням найменших витрат, можливості обслуговування пристрою без залучення фахівціві спеціального обладнання. Такий пристрій можна використовувати за призначенням у будь-якій галузі.

Таким чином, першим етапом роботи пристрою є визначення належності користувача до системи безпеки. На цьому етапі також відбувається розмежування прав доступу до інформаційного середовища. Користувач класифікується за одним із трьох рівнів, наприклад, рівень 3 — «Бухгалтер», рівень 2 — «Заступник по замовленням», рівень 1 — «Головний фінансовий аналітик». Кожен рівень має інформацію різного ступеня важливості, потрапляння якої до третіх осіб може серйозно нашкодити підприємству чи установі. Звідси виникає необхідність розмежування прав доступу, яка реалізується поєднанням методів аутентифікації, а саме: для рівня 3 — зчитування QR-коду, рівня 2 — зчитування QR-ідентифікатора та підтвердження особи зчитуванням відбитку пальця, для рівня 1 — зчитування ідентифікатора користувача, підтвердження біометричними ознаками особи, а також запит унікального паролю для доступу до рівня системи.

У випадку підтвердження усіх етапів користувачеві надається доступ до інформаційного середовища. Якщо користувач на першому етапі не підтверджує належності до інформаційної бази даних, пристрій надає другу спробу для зчитування ідентифікатора. На другому та третьому етапах також надається повторна аутентифікація користувача для зменшення ймовірності помилок другого роду в системі, прикладом якої може бути ненадання доступу санкціонованому користувачеві.

У випадку, коли засіб захисту виявляє несанкціонованого користувача, записується час, дата та кількість невдалих спроб на добу до електронного журналу системи захисту, що дає змогу аналітикам безпеки підприємства або установи зчитувати відомості про загальну ситуацію у системі безпеки інформаційного середовища, а також сповіщати про несанкціонований доступ до системи охорони.

## Моделювання пристрою трифакторної ідентифікації

Моделювання пристрою трифакторної ідентифікації за відбитками пальців користувача проводилося у середовищі Proteus Design Suite — пакет програм для автоматизованого проектування електричних схем, що являє собою систему схемотехнічного моделювання, яке базується на основі моделей електричних компонентів [5]. Вибір цього середовища пояснюється: можливістю моделювання роботи пристроїв, які програмуються: мікроконтролерів, мікропроцесорів і т.п.; наявними (у бібліотеках електричних компонентів) відомостями про їхній склад, роботу та призначення; реалізованою концепцією проектування у реальному часі.

Для моделювання пристрою трифакторної ідентифікації користувача було використано такі елементи та компоненти середовища проектування:

— модель мікроконтролера Arduino UNO R3 [6];

— Arduino sensor shield, що збільшує кількість контактних логічних та аналогових пінів мікроконтролера для підключення електричних компонентів і периферійних пристроїв. Через відсутність даного елемента у середовищі розроблення Proteus Design Suite було замінено його на додаткові конектори шини I2C;

— логічні елементи нуль та одиниця, що підключені через Switch_1, для моделювання роботи пристрою сканера QR-коду, де нуль — відсутність коду або його невідповідність еталону, який знаходиться в базі записаних у пам'яті мікроконтролера, а одиниця — відповідність мітки зареєстрованому шаблону [7];

— логічні елементи нуль та одиниця, що підключені через Switch_2, для моделювання роботи пристрою біометричного сканера відбитків пальців, де нуль — відсутність відбитку пальця користувача на сканері або його невідповідність еталону, який знаходиться у базі відбитків записаних у пам'яті мікроконтролера, а одиниця — відповідність відбитка пальця зареєстрованому шаблону;

— мембранну цифро-символьну клавіатуру Arduino keypad 4×4;

— RGB LED-діод, червоний колір якого інформує про невідповідність введених даних користувачем, а також систему безпеки про несанкціонований доступ, тобто, після двох невдалих спроб авторизації пристрій надсилає сигнал небезпеки до системи охорони, звідки приймається рішення про надання доступу шляхом натискання на кнопку «Надати доступ». Зелений колір інформує щодо збігу введених даних і надання доступу користувачеві;

— LED-діод D1 синього кольору, який моделює роботу соленоїдного електромагнітного замка, тобто активність індикатора свідчить про відкриття замка, відповідно, жовтий колір RGB-діода свідчить про те, що замок закритий. Використання LED-діодів зумовлене відсутністю елементів пристрою у середовищі розроблення Proteus Design Suite, тому було замінено ці елементи світловими індикаторами, що також інформують про стан змодельованого компонента [8];

— фізичну кнопку «Надати доступ», що належить системі охорони для надання доступу користувачеві, відбитки пальців якого не знаходяться в базі зареєстрованих шаблонів, створену для випадків збоїв роботи пристрою захисту, а також для ситуацій, що є винятковими;

— два елементи живлення напругою дев'ять вольт для живлення мікроконтролера Arduino UNO R3, а також LED-діода D1, що слугує соленоїдним електромагнітним замком;

— дисплей OLED SSD1306 для відображення стану роботи пристрою, а також візуальної взаємодії з користувачем [9];

— транзистор TIP122, який контролює відкриття соленоїдного електромагнітного замка у момент надходження до нього сигналу;

Також для використання мікроконтролера необхідно до середовища розроблення Proteus Design Suite додати бібліотеку Arduino, що містить схематичну модель Arduino UNO R3 та дозволяє завантажувати файл прошивки для симуляції роботи мікроконтролера у середовищі розробки [10]. Такий підхід до розроблення пристрою надав можливість створити пристрій у симуляторі та спостерігати за коректністю його роботи.

Під час налагодження роботи пристрою було перевірено виконання усіх умов коректності його роботи, що забезпечило його практичне застосування.

Схематичну модель пристрою біометричної ідентифікації відбитків пальців зображено на рис. 1.

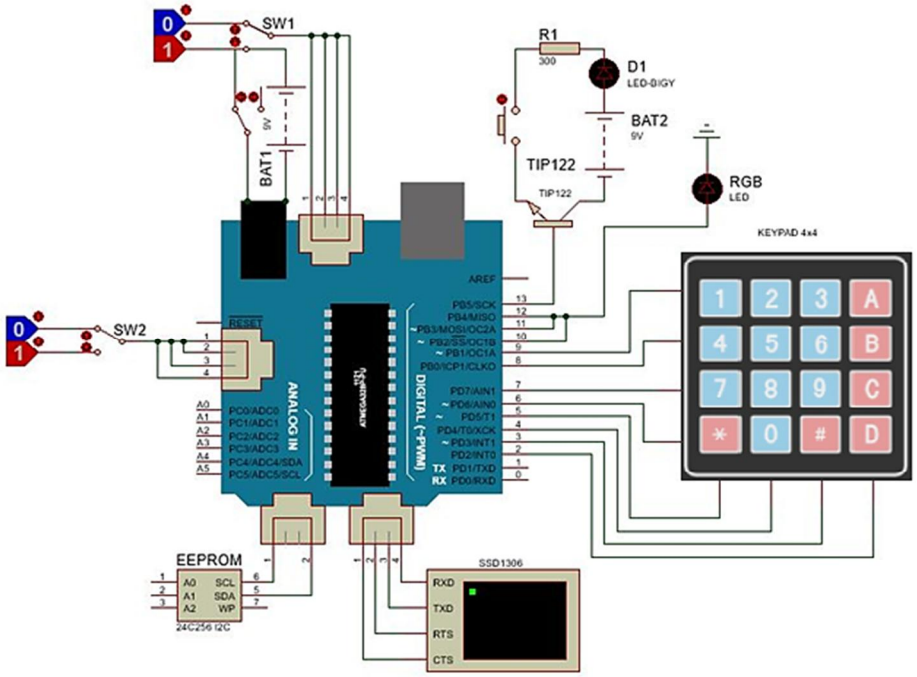


Рис. 1. Схематична модель пристрою біометричної ідентифікації відбитків пальців

## Побудова програмної складової пристрою

Розроблення програмної частини виконувалося у середовищі Arduino IDE, що дозволяє працювати з відкритим кодом будь-якої складності. Цей додаток було обрано, оскільки він застосовується на платформі різних ОС: Windows, Linux та MacOS, а також підтримує мови програмування C і C++ за умови дотримання спеціальних правил структурування коду, наявності бібліотек програмного забезпечення Wiring, що вимагає від користувача введення кількох основних функцій для запуску ескізів та основних циклів коду розробника, які компілюються до виконуваної програми з інструментом GNU та записуються в постійну пам'ять мікроконтролера.

Алгоритм роботи починається з введення номера ідентифікатора та сканування пред'явленого QR-кода користувача. Залежно від рівня доступу особи до інформаційного середовища, ідентифікатор (QR-код) визначає ступінь доступу до інформації. Наприклад, якщо особа має доступ рівня 3, тобто найменший, їй необхідно представити тільки ідентифікатор QR-коду. У випадку доступу другого рівня також потрібно представити QR-ідентифікатор і підтвердити особу шляхом сканування відбитку пальця. Якщо користувач має доступ третього рівня йому необхідно виконати описані процедури та додатково ввести унікальний пароль доступу до інформаційного середовища, обов'язковими умовами якого є великі та малі літери, цифри та спеціальні символи, загальна кількість яких повинна скла-

дати не менше восьми. Якщо представляється ідентифікатор, що не є зареєстрованим в інформаційному середовищі, пристрій проінформує про несанкціонований доступ до конфіденційних даних. Якщо не відбувається підтвердження особи або вводиться хибний унікальний пароль користувача на другому та третьому рівнях доступу користувачеві надається друга спроба. У випадку повторного введення хибних даних пристрій проінформує систему безпеки про несанкціонований доступ, а інформаційне середовище залишиться заблокованим.

Блок-схему алгоритму програмної складової пристрою наведено на рис. 2.

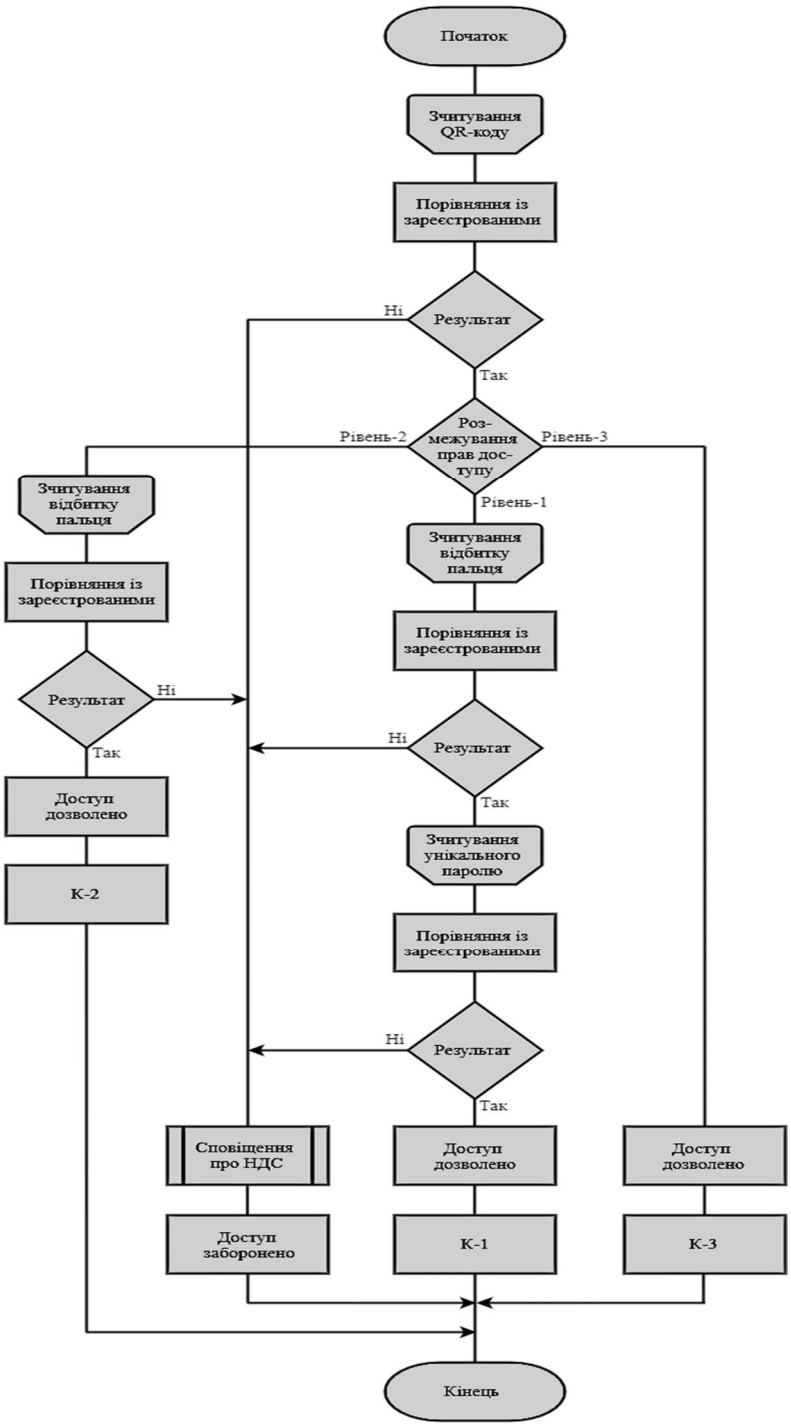

Рис. 2. Структурна схема засобу біометричної ідентифікації

## Застосування та тестування пристрою біометричної аутентифікації

Перш за все необхідно встановити пристрій так:

1) сканери QR-коду та відбитків пальців, мембранну клавіатуру та дисплей візуальної взаємодії з користувачем вивести на передню частину дверей і встановити у зручному для користування місці з урахуванням послідовності дій під час ідентифікації;

2) керуючі компоненти пристрою встановити у недоступному для звичайного користувача місці;

3) електрозамок установити на місце звичайного механічного замка та під'єднати до контролера;

4) сигнал сповіщення про несанкціонований доступ під'єднати до системи безпеки організації і встановити для служби охорони фізичну кнопку «Надати доступ»;

5) виконати налаштування пристрою:

— під'єднати контролер до ПК і виконати реєстрацію користувачів у базі даних шаблонів;

— перевірити коректність роботи пристрою;

— установити елементи автономного живлення пристрою.

Розроблений пристрій трифакторної ідентифікації користувачів задовольняє усім вимогам своєчасного виявлення спроб несанкціонованого доступу та усуває недоліки існуючих аналогів [11]. Це реалізується шляхом надсилання сигналу тривоги до служби охорони установи після двох невдалих спроб аутентифікації за відбитками пальців. Система охорони виконує відповідні дії щодо користувача.

У тому випадку, коли СК не має можливості здійснити вдалу авторизацію, система охорони надає доступ шляхом натискання на кнопку «Дозволити доступ». Після цього користувач може увійти.

У випадку відмови пристрою СК може отримувати доступ від системи охорони установи, що є перевагою розробленого пристрою. Така функція є недоступною в існуючих аналогах, створених за принципами багатофакторної аутентифікації.

Під час тестування розробленого пристрою було з'ясовано, що санкціонованому користувачеві надавався доступ у 97 % випадків, у 2 % випадків користувачеві необхідно було дочекатися завершення попередньої аутентифікації. Лише в 1 % пристрій не надавав доступу санкціонованому користувачеві.

Довговічність розробленого пристрою визначається лише ємністю блока живлення, а також п'ятьма тисячами авторизацій.

Візуальна взаємодія з користувачем у вигляді OLED-дисплея спрощує роботу з пристроєм, оскільки на ньому відображується кожен крок, необхідний для успішної аутентифікації.

Вмонтоване виконання пристрою багатофакторної аутентифікації унеможливлює несанкціонований доступ до інформаційних ресурсів шляхом фізичного зламу, оскільки перед користувачем наявні тільки пристрої зчитування та OLED-дисплей. Усі інші компоненти доступні лише за умови успішної аутентифікації,

але щоб отримати доступ до них необхідно здійснити розбирання основного пристрою, що є вмонтованим, і в якому містяться керуючі елементи і блок живлення.

## Висновки

Запропоновано пристрій, який на основі багатофакторної аутентифікації дозволяє: завчасно виявляти спроби несанкціонованого доступу, надавати доступ до інформаційних ресурсів санкціонованим користувачам, навіть у випадку відмови пристрою та під час виникнення аварійних ситуацій.

Він має підвищену довговічність і стійкість до фізичного зламу.

Наукова новизна роботи полягає в удосконаленні системи захисту інформації від несанкціонованого доступу, що, на відміну від існуючих підходів, шляхом застосування методу трифакторної аутентифікації: на основі поєднання біометричного сканування відбитків пальців, QR-ідентифікатора та парольної ідентифікації, дозволяє значно підвищити безпеку інформаційних ресурсів.

Практична цінність. Розроблений пристрій уможливлює покращення системи захисту інформації на різних суб'єктах господарювання, є більш інформативним, простим для користувача, не вимагає спеціальних знань у сфері технічного захисту інформації, дозволяє завчасно виявити спроби несанкціонованого доступу, відновити основні функції пристрою в аварійних ситуаціях, має значно нижчу ціну, що прискорює його впровадження у системах безпеки.

1. Азаров О.Д., Хорошко В.О., Шєлєст М.Є., Яремчук Ю.Є. Основи комп`ютерної стеганографії: навч. посіб. — Вінниця: ВДТУ, 2003. 143 с.

2. Лівак Е.Н. Методы защиты компьютерной информации. URL: http://mf.grsu.by/UchProc/livak/discipline_zachi-ta.htm (Дата звернення: 24.05.21).

3. Захист інформації в інформаційних системах. URL: https://pidruchniki.com/13670622/informatika/zahist_informatsiyi_informatsiynih_sistemah (Дата звернення: 24.05.21).

4. Сінько Ю.І. Загрози безпеці інформації обмеженого доступу. *Проблеми інформатизації та управління.* 2017. № 4 (60). С.64–70.

5. Середовище розробки Протеус. URL: https://ru.wikipedia.org/wi-ki/Proteus (Дата звернення: 24.05.21).

6. Середовище розробки Ардуіно. URL: http://arduino.ru/Arduino_environment (Дата звернення: 24.05.21).

7. Офіційний сайт компанії Лабцентр електронікс. URL: https://www.labcenter.com/ (Дата звернення: 24.05.21).

8. Логічні елементи в електричних схемах. URL: http://elec-tricalschool.info/main/electroshemy/1613-logicheskie-jelementy-v.html (Дата звернення: 24.05.21).

9. Контролер/драйвер SSD1306 для дисплеїв OLED/PLED. URL: http://microsin.net/adminstuff/hardware/ssd1306-oled-controller.html (Дата звернення: 24.05.21).

10. Додаткові бібліотеки Ардуіно. URL: https://doc.arduino.ua/ru/-guide/Libraries (Дата звернення: 24.05.21).

11. Азарова А.О., Гудзь В.О., Блонський В.О. Управління інформаційною безпекою в державних установах на основі біометричної аутентифікації відбитків пальців для захисту інформації від несанкціонованого доступу. Тези XLVIII науково-технічної конференції ВНТУ. 2019. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm2019/paper/view/7429 (Дата звернення: 24.05.21).

Надійшла до редакції 05.06.2021