DOI 10.31891/2307-5732-2023-321-3-355-359
УДК 004.056.53

ПАВЛОВСЬКИЙ ПАВЛО
Вінницький національний технічний університет
ПРИСЯЖНИЙ ДМИТРО
Вінницький національний технічний університет
АБРАМЧУК ІГОР
abramchuk@vntu.edu.ua
Вінницький національний технічний університет
САВРАЦЬКИЙ В.В.
Вінницький національний технічний університет
БІЛОУС В.М.
Вінницький національний технічний університет

ПІДВИЩЕННЯ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ПІД ЧАС ГОЛОСУВАННЯ В ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ НА ОСНОВІ АПАРАТНОЇ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ГОЛОСУЮЧОГО

Запропоновано пристрій для забезпечення захисту від несанкціонованого доступу до інформації на основі використання автентифікації користувачів з можливістю розмежування доступу до інформаційного середовища. Пристрій дозволяє завчасно виявляти спроби несанкціонованого доступу та надавати доступ до інформаційних ресурсів санкціонованим користувачам; має підвищену довговічність і стійкість до фізичного зламу, підвищує захищеність системи захисту інформації; є простим для користувача і не вимагає спеціальних знань у сфері технічного захисту інформації; а також дозволяє завчасно виявити спроби несанкціонованого доступу, відновити основні функції пристрою в аварійних ситуаціях і має значно нижчу ціну порівняно з аналогами.

Ключові слова: несанкціонований доступ, ідентифікація користувача, біометричне сканування відбитків пальців, парольна ідентифікація.

PAVLOVSKIY PAVLO, PRUSIAZHNYI DMITRO, ABRAMCHYK IGOR, SAVRATSKIY V., BILOUS V.
Vinnytsia National Technical University

INCREASING PROTECTION AGAINST UNAUTHORIZED ACCESS DURING VOTING IN STATE AUTHORITIES BASED ON HARDWARE BIOMETRIC IDENTIFICATION OF THE VOTER

A device is proposed to provide protection against unauthorized access to information based on the use of user authentication with the possibility of delimiting access to the information environment. The device allows early detection of unauthorized access attempts and provides access to information resources to authorized users; has increased durability and resistance to physical breaking, increases the security of the information protection system; is simple for the user and does not require special knowledge in the field of technical information protection; and also allows early detection of unauthorized access attempts, recovery of basic device functions in emergency situations and has a much lower price compared to analogues.

Keywords: unauthorized access, user identification, biometric fingerprint scanning, password identification.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

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 у аспектах формування, користування інформаційними ресурсами, розроблення, виробництва та застосування інформаційних систем, технологій і засобів їхнього забезпечення здійснюється з метою попередження правопорушень, неправомірних дій, відновлення порушених прав і відшкодування заподіяної шкоди [1].

Розвиток системи голосування має визначатися прогнозованими напрямами розвитку законодавства України, визначення режиму використання її програмно-технічних засобів та інформаційних ресурсів, правового статусу документів, підготовлених з використанням системних засобів, захисту інформації в системі та цільового фінансування її розробок. Науково-методичне забезпечення створення системи голосування має базуватися на аналізі та впровадженні сучасних світових досягнень у сфері інформатизації процесів підготовки та проведення голосування, залученні вітчизняного наукового-виробничого потенціалу до розробки проектів і механізмів розвитку, а також на прогнозуванні тенденцій розвитку інформаційних технологій [2]. Матеріально-технічне забезпечення системи голосування має базуватися на сучасній комп'ютерній, телекомунікаційній техніці, системному програмному забезпеченні та оргтехніці. Інформаційно-аналітичне забезпечення системи голосування повинно базуватися на цілісності інформації у єдиному інформаційному просторі організаційної інфраструктури виборів і референдумів. До складу інформаційно-аналітичного забезпечення системи

голосування можуть входити сегменти баз даних, довідники та кодифікатори, що створюються та підтримуються іншими установами. Склад та функціональне призначення інформаційно-аналітичного забезпечення визначаються переліком завдань, що покладаються на систему голосування. Системне програмно-технічне забезпечення (операційні системи, системи телекомунікаційного зв'язку, системи приймання-передавання інформації, системи управління базами даних, системи захисту інформації) у системі голосування спрямоване на організацію функціонування корпоративної інформаційної комп'ютерної мережі, управління її компонентами і рівнями, а також організацію інформаційних потоків та інформаційної безпеки. Системне програмно-технічне забезпечення базується на принципах єдиної платформи та сумісності, забезпечує передачу даних, контроль за їх цілісністю, моніторинг передачі даних, а також моніторинг функціонування системи голосування, контроль повноважень і прав доступу користувачів. Системне програмно-технічне забезпечення на кожному рівні системи голосування має відповідати функціональному навантаженню рівня та його місцю у системі. Система голосування має будуватись за принципом відкритих систем, що надає можливості використання розподілених баз даних та обчислень, масштабованості та можливості перенесення на інші платформи у процесі розвитку, забезпечення сумісності та інтеграції з іншими системами. Система голосування розширюється за модульним принципом організації та поетапним нарощуванням функціональних можливостей, що дозволяє розвивати складові, не порушуючи функціонування системи у цілому. Прикладне програмне забезпечення системи голосування повинно базуватися на сучасних засобах управління базами даних та забезпечувати формування, обробку, накопичення та підготовку інформації для передавання за узгодженими форматами. Прикладне програмне забезпечення повинно виконувати максимально можливий перелік функцій для інформаційної підтримки діяльності системи голосування. Прикладне програмне забезпечення системи голосування має підтримувати усі види формування і обробки інформації, автоматизацію виборчих процедур на усіх етапах підготовки та проведення голосування. Інформаційна безпека системи забезпечується нормативно-організаційними, стандартними програмно-технічними та спеціалізованими засобами захисту інформації. Стійкість системи у цілому не повинна залежати від працездатності будь-якої складової єдиного програмно-інформаційного простору системи. Створювані програмні засоби повинні забезпечувати запобігання втратам інформації та несанкціонованого втручання, знищення, спотворення, підробки, копіювання інформації. Система голосування повинна забезпечити контроль за інформаційними потоками, шифрування трафіка, ідентифікацію як суб'єкта програмно-інформаційного простору [3].

Аналіз існуючих систем голосування показав, що основним недоліком біометричної ідентифікації є вартість устаткування, адже для кожного пульта для голосування, що входять до системи голосування, необхідно придбати власний сканер. Варто також відзначити, що подібні дешеві сканери недовговічні. Крім того, у них досить високий відсоток помилок другого роду (відмова у доступі зареєстрованому користувачеві), а також недостатній рівень захищеності під час ідентифікації користувачів. Виходячи з цього актуальним для систем голосування є таке.

Постановка задачі та метод дослідження. Розроблення нового функціонального пристрою з використанням підсистеми апаратної біометричної ідентифікації голосуючого та парольної ідентифікації, що уможливлює усунення недоліків існуючих підходів та забезпечує високий рівень захисту інформації.

Формулювання цілі статті. Метою статті є підвищення рівня захисту від несанкціонованого доступу шляхом розроблення та застосування пристрою підсистеми апаратної біометричної ідентифікації голосуючого.

Моделювання пристрою трифакторної ідентифікації

Пропонується пристрій, що використовує біометричну ідентифікацію у вигляді сканера відбитків пальців (дактилоскопічний сканер), який буде встановлено на кожний із пультів для голосування і буде забезпечувати захист результатів голосування та зберігати їхню достовірність.

У даному пристрої буде використано сканер відбитку пальця FPM10A, що базується на оптичному методі. Даний сканер є найбільш мініатюрним, стійким до муляжів та має помірну цінову категорію [3].

Оптичні датчики відбитків пальців FPM10A зазвичай використовуються у системах безпеки, ці сенсори включають у себе чіп, який обробляє зображення, робить необхідні розрахунки для виявлення відповідності між записаними і поточними даними. З використанням відповідного програмного забезпечення можна навіть відобразити фотографію відбитка на дисплеї (рис. 1).

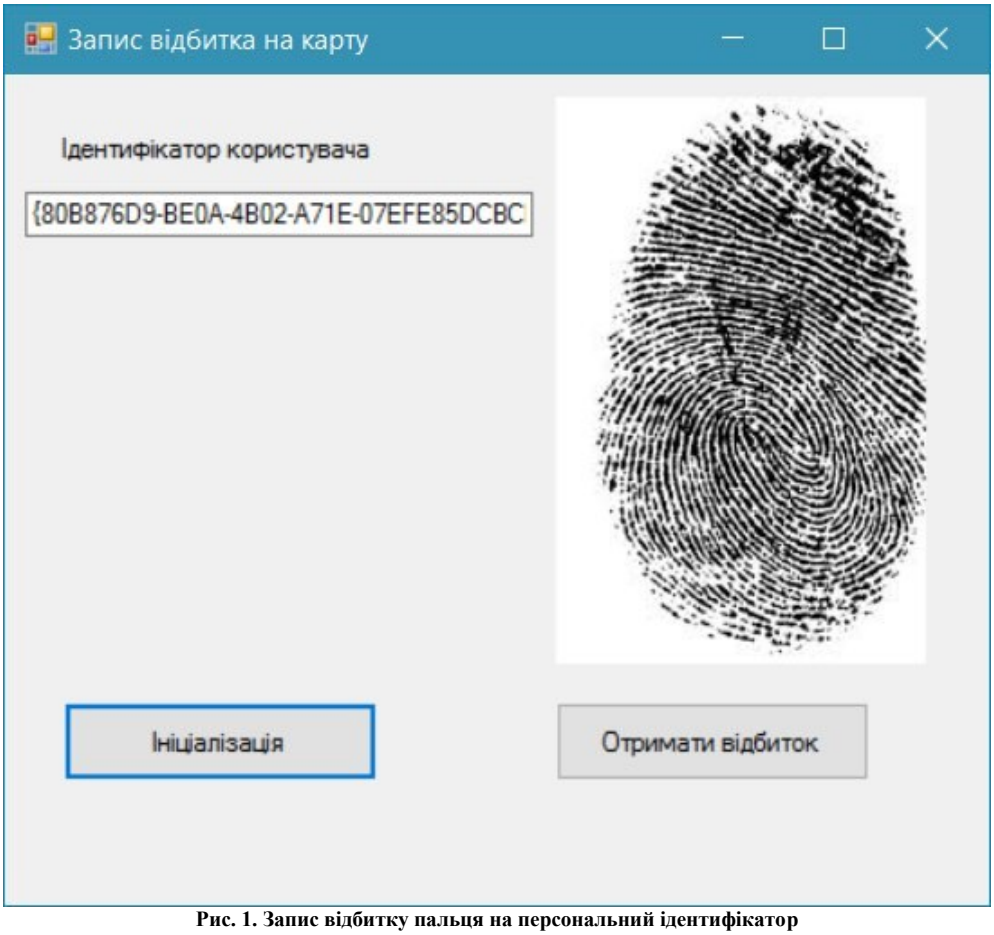

Рис. 1. Запис відбитку пальця на персональний ідентифікатор

При використанні датчика відбитку пальців є два основних етапи. Спочатку треба записати дані у пам’ять сенсора, тобто привласнити свій унікальний ідентифікатор кожного відбитка, який буде використовуватись для порівняння у подальшому. Після запису даних, здійснюється перехід до пошуку, порівнюючи поточне зображення відбитка з тими, які записані у пам'яті датчика. Для запису відбитків пальців можна використовувати запропоноване програмне забезпечення або скетч для Arduino (рис. 2) (у залежності від платформи, під яку встановлюється сканер). Найпростіший шлях запису нових даних у пам'ять оптичного датчика відбитків пальців – програма для Windows. Нажаль, для інших операційних систем програмне забезпечення не передбачено. Спочатку треба підключити сенсор до комп’ютера, після чого записати скеч на Arduino. Провідники на датчику даної модифікації FPM10A скріплені для більш зручного підключення, але за необхідності їх можна розділити. Так як провідники на датчику тонкі і короткі, можна припаяти їх до окремих рейок контактів, або просто нанести на кінці припою для надійного контакту з роз’ємами мікроконтролера. Після підключення живлення буде блимати червоний світлодіод, позначаючи, що сенсор працює [4].

Кожен голосуючий має свою персональну картку, яка містить персональні дані та біометричний відбиток пальця.

Для того, щоб голосування було достовірним, використаємо програму, яка буде звіряти відбиток пальця голосуючого з відбитком, що збережений у персональній картці.

Запис відбитку пальця на картку проводиться адміністратором за допомогою програмного засобу біометричної ідентифікації.

У ході даного дослідження було розроблено дослідний зразок пульта голосуючого, схема електрична-принципова пристрою наведена на рисунку 3. Основою пристрою є мікроконтролерна платформа сімейства Arduino, версії Nano, яка займається обробкою результатів голосування та біометричної ідентифікації. На входи D2, D3 плати підключено біометричний датчик зчитування відбитків, моделі FPM10A, даний датчик є функціонально завершеним модулем і для його роботи достатньо пройти процедуру ініціалізації відповідного протоколу роботи у програмному коді пристрою, обмін даними між датчиком і мікроконтролером відбувається у послідовному коді через зазначені входи. До входів D4 – D6 підключені кнопки для голосування, при натисканні яких зараховуються відповідні голоси «За», «Проти», «Утримався». До входу D7 підключена кнопка, натискання якої імітує сигнал запуску голосування з головного пульта системи. На вхід D12 підключено активний бузер для звукової сигналізації етапів роботи пристрою, а на входи A0 – A4 підключені світлодіоди для світлової індикації відповідних етапів та результатів голосування.

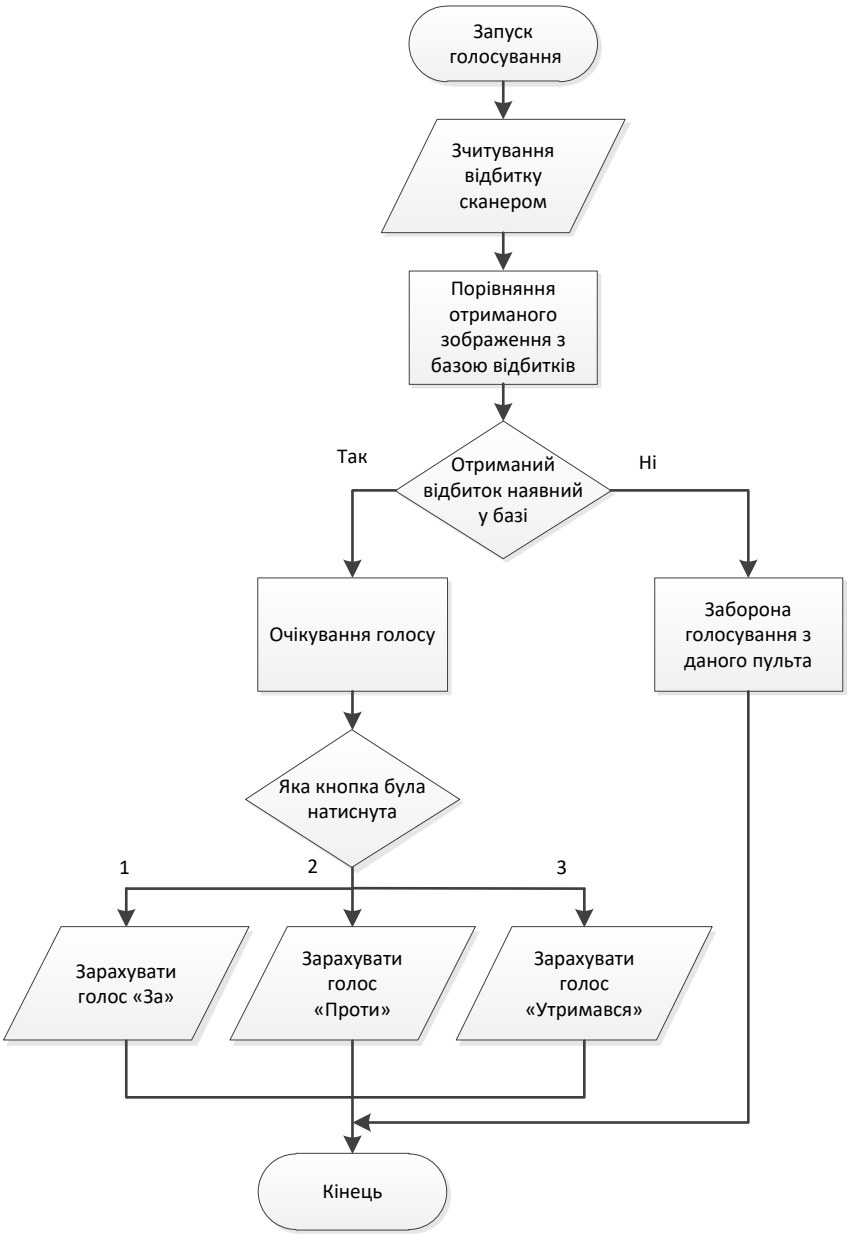

Рис. 2. Алгоритм роботи програми

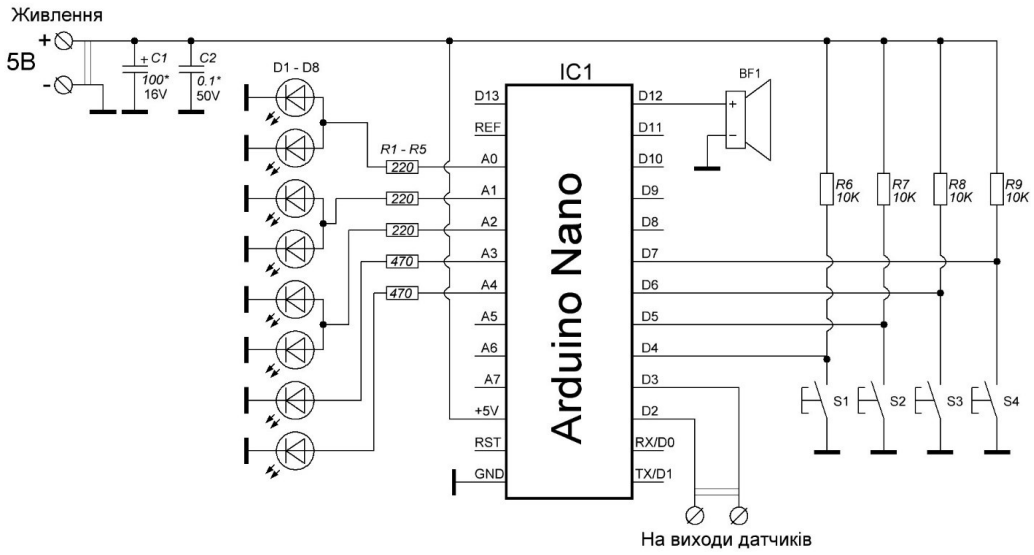

Рис. 3. Принципова схема підсистеми апаратної біометричної ідентифікації голосуючого

Аналіз роботи та можливостей запропонованого пристрою показав, що він за рахунок трифакторної біометричної ідентифікації підвищує захищеність системи захисту інформації, є більш інформативним і простим для користувача; не вимагає спеціальних знань у сфері технічного захисту інформації; дозволяє завчасно виявити спроби несанкціонованого доступу, відновити основні функції пристрою у аварійних ситуаціях; має значно нижчу ціну, що прискорює його впровадження у системах безпеки.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Запропоновано пристрій, який на основі біометричної ідентифікації дозволяє завчасно виявляти спроби несанкціонованого доступу, надавати доступ до інформаційних ресурсів санкціонованим користувачам, навіть у випадку відмови пристрою та під час виникнення аварійних ситуацій; має підвищену довговічність і стійкість до фізичного зламу.

Поєднання біометричного сканування відбитків пальців та парольної ідентифікації дозволили значно підвищити захищеність систем голосування від несанкціонованого доступу та безпеку інформаційних ресурсів у цілому.

Література

1. Закон України «Про захист інформації в автоматизованих системах».
2. Концепція технічного захисту інформації в Україні, затверджена постановою КМУ від 08.10.97 р., №1126
3. Азаров О.Д., Хорошко В.О., Шєлєст М.Є., Яремчук Ю.Є. Основи комп’ютерної стеганографії: навч. посіб. — Вінниця: ВДТУ, 2003. 143 с
4. Кулішов В.В. Мікро-макроекономіка : підручник / В.В. Кулішов. – Львів: Магнолія, 2008. – 468 с.
5. Системи охорони периметра [Електронний ресурс] – Режим доступу: http://guard-lviv.com.ua/oxrana-perimetra/index.html

References

1. Law of Ukraine "On Information Protection in Automated Systems".
2. The concept of technical protection of information in Ukraine, approved by the resolution of the CMU of October 8, 1997, No. 1126.
3. Azarov O.D., Khoroshko V.O., Shelest M.E., Yaremchuk Yu.E. Basics of computer steganography: training manual, Vinnytsia: VDTU, 2003. 143 p.
4. Kulishov V.V. Micro-macroeconomics: a textbook, Lviv: Magnolia, 2008, 468 p.
5. Perimeter protection systems [Electronic resource] - Access mode: http://guard-lviv.com.ua/oxrana-perimetra/index.html