УДК: 400:002.1

Панченко І. В. ORCID: 0000-0001-5690-3813 (ВІТІ)
Слотвінська Л. І. ORCID: 0000-0003-2409-6206 (ВІТІ)
Ляшенко В. О. (А0515)

ВАРІАНТ СИСТЕМИ ЕЛЕКТРОННОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ НА ОСНОВІ 2D (QR) КОДУ

Завдяки розвитку цифрових технологій у сучасному світі значно підвищились вимоги до систем життєзабезпечення та діяльності суспільства, а також до документів, що беруть участь у роботі цих систем.

Прикладів таких систем безліч і майже всі вони використовують документи у вигляді пластикової картки. Оскільки це документи, то актуальними є питання захищеності систем від несанкціонованого доступу, а саме, наявність елементів захисту та надійність процесів ідентифікації та автентифікації користувачів.

В статті проаналізовано існуючі «електронні елементи захисту» й електронні елементи персоналізації сучасних документів, а саме види, характеристики, процеси функціонування.

Проведено оцінку електронних елементів захисту.

Встановлено, що на ступінь захищеності документу впливають два основні чинники, такі як контроль доступу та проведення процедури зчитування, захищеної базовим контролем доступу.

Запропоновано систему захисту на основі елементу персоналізації.

Така система може бути використана як аналог більш дорогим варіантам організації контрольно-пропускного режиму на об'єктах, завдяки своїй простоті, малоймовірності несанкціонованого доступу до алгоритмів та процесу роботи її елементів. Впровадження даної системи на контрольно-пропускних пунктах може значно покращити управління та забезпечити захищеність системи безпеки, процесу перетину контрольованої зони.

Напрямком подальших досліджень є розробка системи з переносом персоналізованої інформації з документів напряму до баз даних машинозчитуваних систем.

Однак найважливішим параметром залишиться стійкість та захищеність від несанкціонованого втручання в роботу машинозчитуваних електронних систем.

Ключові слова: *система контролю й управління доступом, машинозчитуваний проїзний документ, технологія радіочастотної ідентифікації, двовимірний штрих-код, базовий контроль доступу, автентифікація чіпа.*

I. Panchenko, L. Slotvinskaya, V. Lyashenko. Variant of electronic identification and authentification system based on 2D (QR) code.

Due to the development of digital technologies in the modern world, the requirements for life support systems and society, as well as for the documents involved in the work of these systems have increased significantly.

There are many examples of such systems and almost all of them use documents in the form of a plastic card. As these are documents, the issues of protection of systems from unauthorized access are relevant, namely, the availability of security features and the reliability of the processes of identification and authentication of users.

The article analyzes the existing "electronic elements of protection" and electronic elements of personalization of modern documents, namely the types, characteristics, processes of functioning.

The evaluation of electronic security elements was carried out.

It is established that the degree of security of the document is influenced by two main factors, such as access control and reading procedure, protected by basic access control.

A protection system based on the personalization element is proposed.

Such a system can be used as an analogue of more expensive options for the organization of access control at facilities, due to its simplicity, the likelihood of unauthorized access to algorithms and the process of its elements. The implementation of this system at checkpoints can significantly improve the management and security of the security system, the crossing process controlled area.

The direction of further research is the development of a system with the transfer of personalized information from documents directly to the databases of machine reading systems.

However, the most important parameter will remain the stability and protection against unauthorized interference in the operation of machine-readable electronic systems.

Keywords: *access control and management system, machine-readable travel document, radio frequency identification technology, two-dimensional bar code, basic access control, chip authentication.*

Постановка завдання та актуальність дослідження

Як в умовах функціонування силових структур, так і в умовах ведення гібридної війни між Україною і Росією, в тому числі на сході України та в зоні проведення Операції об'єднаних сил, дуже часто виникає потреба в мобільному та швидкому створенні пропускних пунктів, де проводиться контроль великого потоку людей з використанням різного виду документів.

Значну частину складають документи, що контролюються в автоматичному або напівавтоматичному режимах [1–7; 9].

Такі документи оснащені машинозчитуваними елементами і дістали назву машинозчитувані проїзні документи (МЗПД). Їх перевірка відбувається з використанням електронної бази даних.

Загальні вимоги до виготовлення і функціонування МЗПД викладені в стандарті «ICAO Doc 9303 Машинозчитувані проїзні документи» [12].

Згідно з нормативними документами МЗПД повинні мати поліграфічний захист від підробок, який не повинен заважати машинному зчитуванню, а також електронний елемент захисту.

Електронний елемент захисту – це електронний носій із закодованою інформацією, яка зчитується за допомогою спеціальних електронних пристроїв і програмного забезпечення.

Різноманітні електронні елементи захисту мають свої переваги і недоліки. Але, однозначно, що використання електронної бази даних, відповідних документів з машинозчитуваними елементами та програмно-апаратного комплексу може значно полегшити процедуру контролю та забезпечити безпеку роботи органів і підрозділів, які працюють з документами.

Аналіз публікацій за темою дослідження

Для захисту документів використовують різні електронні елементи персоналізації, такі як *магнітна смуга, 1D та 2D штрих-коди, а також різновиди чипів та міток.* Дані методи полягають у захищеності електронної системи від несанкціонованого доступу до неї, сприяють запобіганню пошкодження, зміни чи викрадення інформації, яка міститься на машинозчитуваних закодованих елементах [1].

На теперішній час рівень інтеграції машинозчитуваних систем захисту й обробки персональних даних на документах перебуває на високому рівні. Створено безліч інститутів та стандартів щодо технологічних процесів виготовлення, використання та їх захисту.

Для створення ідентифікаційних та інших документів сьогодні використовують найсучасніші технології. Однак існують факти їх підробки, несанкціонованого доступу та використання. Для прикладу, отримавши банківську картку та знаючи її пароль, стає можливим проведення різного роду операцій з нею.

Попри всі методи захисту, найдостовірнішим фактором автентифікаці і отримання різного роду привілеїв залишаються біометричні дані людини. Адже саме ці дані є найунікальнішими та майже не піддаються підробці. Такі елементи захисту застосовуються в сучасних автоматичних системах, таких як FaceID, сканер сітківки ока (іридосканер), відбиток пальця та структура ДНК. Оскільки такі технології ще не зовсім досконалі та мають певні технічні недоліки, їх використання в системах, де циркулює персональна інформація, є дуже складним та проблематичним. Тому основним і кінцевим фактором обробки інформації є людина [8].

Найсучасніші досягнення в системах ідентифікації та автентифікації пластикових документів безперечно пов'язані з використанням чипів. Головним чином через те, що такий спосіб дозволяє оцифровувати персональні дані, краще захистити процес автентифікації та зробити його достатньо швидким. Використання таких технологій є досить недешевим, а процес відтворення – складним. Через що не завжди виникає доцільність їх використання в окремих видах пропускних систем, що надають доступ до тих чи інших об'єктів за посвідченнями учасників різного роду організацій.

Тому, в цьому випадку, необхідно звернути увагу на використання старих, але значно покращених машинозчитуваних елементів.

Метою статті є аналіз пластикових документів (карток) з машинозчитуваними елементами захисту, вибір відповідного елементу персоналізації і його захисту та розробка аналогу системи автентифікації користувачів.

Виклад основного матеріалу

Було проаналізовано найбільш розповсюджені електронні елементи захисту пластикових карток: види, технології виготовлення, принцип роботи.

Магнітна смуга – носій інформації з обмеженим обсягом пам'яті.

Смуга може бути виготовлена для різних напруженостей магнітного поля. Кодування магнітної смуги виконується на спеціальному пристрої (енкодері), який дозволяє записати на неї інформацію, необхідну для подальшої роботи.

Подібні пластикові картки широко використовуються в платіжних і дисконтних системах, дуже рідко – в системах доступу.

Необхідно зазначити, що за кордоном магнітні картки застосовуються в системах контролю й управління доступом значно ширше внаслідок того, що впровадження даних систем на Заході почалося набагато раніше, ніж в Україні.

Кодування Smart-чипів також здійснюється спеціалізованими енкодерами, які, як і енкодери магнітних карток, можуть бути вбудовані в деякі моделі принтерів для їх виготовлення. Існує відмінність у напруженості магнітного поля: LoCo (Low Coercitive – низькокоерцитивні = 300 ерстед) і HiCo (High Coercitive – висококоерцитивні = 2750 ерстед) магнітні смуги.

Пластикові картки з магнітною смугою HiCo надійніші і довговічніші, оскільки інформація на магнітних смугах HiCo менш схильна до розмагнічення зовнішніми магнітними полями, ніж на смугах LoCo.

Магнітна смуга HiCo використовується в тих випадках, коли потрібно захистити інформацію на магнітній карті від можливого розмагнічування, а також підвищити захищеність карток від можливої підробки. Картки з магнітною смугою HiCo коштують дорожче, ніж картки з магнітною смугою LoCo.

Штрих-коди. Всі штрих-коди поділяються на лінійні (1D) та двомірні (2D). Лінійний штрих-код читається тільки в одному напрямку (перпендикулярно чорним лініям штрих-коду), а двомірний зчитується при будь-якому положенні.

Лінійні коди – це послідовність паралельних чорних та білих смуг різної ширини. Темні смуги називаються штрихами, а світлі – пробілами. Інформацію несе суворо задана стандартизована ширина штрихів та пробілів, а також їх розташування відносно один одного. Двомірний код містить інформацію як по горизонталі, так і по вертикалі.

Серед **чипів та міток,** в основу яких покладено використання бездротових (wireless) технологій, найбільш поширені наступні.

NFC означає комунікацію ближнього радіусу дії, RFID – радіочастотну ідентифікацію. Обидві технології використовують радіосигнал для пошуку тегів і відстеження цілей та приходять на зміну штрих-кодуванню. NFC тільки зароджується, а RFID вже поширена в усьому світі. RFID мітки (теги) містять антену і чип, в якому зберігаються дані.

Щоб побачити дані, потрібно RFID зчитувач. RFID часто працює на великих відстанях, інакше довелося б небезпечно міняти розташування, наприклад, при парковці автомобіля, до воріт, щоб переконатися що мітку дійсно зчитано рідером.

Як приклад, RFID – це система односпрямованого зв'язку, в якій дані з мітки передаються до безконтактного зчитувача.

Технологія NFC набагато менша версії RFID. Радіус її дії становить максимум 10 см і в ній може бути встановлений як односторонній, так і двосторонній зв'язок.

Розглянемо односторонню передачу даних.

Використовуючи смартфон, можна прочитати NFC тег, який може бути вбудований в рекламні постери, політичні листівки, путівники. Розумні мітки дуже схожі на RFID теги, вони просто налаштовані на роботу з NFC зчитувачами, замість RFID. RFID однонаправлена технологія, де зчитувач читає інформацію з мітки. NFC технології більш комплексні.

Як правило, кількість витрачених ресурсів та зусиль для захисту тієї чи іншої (інформації) системи залежить від рівня важливості даної системи.

Вартість виготовлення пластикових карток може бути різною.

У таблиці 1 наведено середню кількість витрат на їх виготовлення з тим чи іншим елементом захисту, тиражем в 100 штук. Для порівняння додано поліграфічні елементи захисту – ембосування і нумерацію [18].

Таблиця 1

Витрати на виготовлення пластикових карток

Елемент захисту на картці	Середня ціна, 100 шт.
Штрих-код	480 грн
Магнітна смуга	590 грн
Безконтактний чип	1200 грн
Ембосування	510 грн
Нумерація	480 грн

З таблиці добре видно, що найдорожчим з усіх запропонованих варіантів є виготовлення пластикової картки з безконтактним чипом. А варіант з виготовлення картки з QR-кодом є найдешевшим.

Усе це можна пояснити тим, що QR-код – це лише нанесене на поверхню зображення з використанням одного з видів друку, воно не вимагає значних витрат під час виробництва та використання.

Чип, навпаки, потребує застосування спеціалізованого обладнання для монтажу, а процедура його створення сама по собі є досить складною.

Ще однією, схожою з чипом, перевагою QR-коду є швидкість процедури його зчитування, адже навіть назва дає зрозуміти, що QR-код (англ. Quick Response Code) – це код швидкого реагування.

Поряд з перевагами QR-код має ряд недоліків.

Однією з найголовніших проблем використання QR-коду, як надійного елементу в процесі ідентифікації та автентифікації, є те, що процес та алгоритми його кодування та зчитування знаходяться в публічному доступі та є відомими [11].

Наступним недоліком є обмеження в кількості кодованих символів.

З аналізу та дослідження зібраного матеріалу випливає необхідність в кодуванні тієї інформації, за допомогою якої генерується QR-код. Мета цього кодування – приховати інформацію про об'єкт від зловмисника. Для вирішення цієї задачі потрібно використати елементи криптології [13; 14].

Тому було запропоновано процес хешування. Хеш-сумою (хешем, хеш-образом, хеш-кодом) називається значення хеш-функції на якихось вхідних даних. Іноді хеш-суму також називають дайджестом повідомлення. Значення хеш-суми може використовуватися для перевірки цілісності даних, їх ідентифікації та пошуку (наприклад в p2p-мережах), а також заміняти собою дані, які небезпечно зберігати в явному вигляді.

Саме такими даними є персональні відомості про об'єкт, а в нашому випадку це дані про особу. Криптографічна хеш-функція дозволяє легко перевірити, що деякі вхідні дані зіставляються із заданим значенням хешу, але, якщо вхідні дані невідомі, то навмисно важко відновити вхідне значення (або еквівалентну альтернативу), знаючи збережене значення хеш-функції. Це використовується для забезпечення цілісності переданих даних і є будівельним блоком для хеш-кодів аутентифікації повідомлень (HMAC), які забезпечують їх автентичність.

Явне значення хеш-суми, як правило, записується в шістнадцятковому вигляді. Так, утиліта md5sum, яка обчислює значення хеш-функції MD5 від заданого файлу, видає результат у вигляді рядка з 32-х шістнадцяткових цифр – наприклад, 026f8e459c8f89ef75fa7a78265a0025.

Однак, існує проблема, якої неможливо уникнути – це алгоритми хешування. Тобто, той факт, що хеші є рядком фіксованої довжини, означає, що для кожного введення даних є інші можливі входи, які приведуть до того ж хешу. Це означає, що якщо зловмисник може створювати ситуацію, він може передавати шкідливі файли чи дані та ховатися під правильним хешем.

Мета хорошої хеш-функції полягає в тому, щоб зробити надзвичайно складними для зловмисників способи генерації вхідних даних, які хешуються з однаковим значенням. Обчислення хеша не повинно бути занадто простим, так як це полегшує зловмисникам штучне обчислення.

Алгоритми хешування повинні бути стійкі до «атак знаходження прообразу». Тобто, щоб отримуючи хеш, було б надзвичайно складно обчислити зворотні детерміновані кроки, зроблені для відтворення значення, яке створило хеш.

З аналізу та дослідження опрацьованого матеріалу було визначено, що процес автентифікації має певні вимоги згідно з низкою керівних документів. Головним чином вимоги, що забезпечують автентичність документа, – це контроль доступу до системи (мережі) та створення процедури пасивної активної автентифікації.

Першочерговими та вже добре відомими способами захисту інформації у корпоративній мережі є встановлення надійних паролів, наявність резервних копій, безпечне використання додатків, оновлення системи та зміна налаштувань за замовчуванням.

Поряд з цим, особливу увагу під час забезпечення безпеки корпоративної мережі слід приділити захисту баз даних. Оскільки інформація, яку вони містять, особливо цінна для організацій та приваблива для зловмисників. Бази даних потребують особливої уваги та додаткового захисту [15].

Було опрацьовано питання щодо захисту баз даних. Проаналізовано інформацію компанії ESET – міжнародного розробника антивірусного програмного забезпечення та рішень в області комп'ютерної безпеки.

Спеціалісти ESET надають декілька основних порад щодо захисту баз даних підприємств і організацій.

1. *Контроль доступу до бази даних*. Запобігти атакам кіберзлочинців допоможуть обмеження дозволів та привілеїв. Крім базових системних дозволів слід застосувати:

Обмеження доступу до конфіденційних даних для певних користувачів і процедур, які можуть робити запити, пов'язані з конфіденційною інформацією.

Обмеження використання основних процедур тільки певними користувачами.

Уникнення використання і доступу до баз даних в неробочий час.

2. *Визначення критично важливих даних.* Першим кроком має стати аналіз важливості захисту для конкретної інформації. Для полегшення визначення місця та способу збереження конфіденційних даних слід зрозуміти логіку й архітектуру бази даних. Не всі дані є критично важливими чи потребують захисту, тому на них немає сенсу витрачати час і ресурси.

3. *Шифрування інформації*. Після ідентифікації критично важливих даних потрібно застосувати надійні алгоритми шифрування конфіденційної інформації.

У разі використання уразливості або отримання доступу до сервера або системи, зловмисники в першу чергу спробують викрасти бази даних, які, зазвичай, містять багато цінної інформації. Кращий спосіб захистити базу даних – зашифрувати її для осіб, які намагаються отримати доступ без авторизації.

4. *Реалізація анонімності непродуктивних баз даних*. Багато компаній інвестують час та ресурси у захист своїх продуктивних баз даних, але при розробці проєкту або створення тестового середовища вони просто роблять копію вихідної бази даних і починають використовувати її в середовищах з менш жорстким контролем, тим самим розкриваючи всю конфіденційну інформацію.

Тобто за допомогою маскування та анонімізації можна створити аналогічну версію з тією ж структурою, що й оригінал, але зі зміненими конфіденційними даними для їх захисту. За допомогою цієї технології значення змінюються за умови збереження формату.

Дані можуть бути змінені шляхом змішування, шифрування, переставляння символів або заміни слів. Конкретний метод, правила і формати залежать від вибору адміністратора, але незалежно від вибору метод повинен забезпечити неможливість отримати вихідні дані за допомогою зворотної інженерії.

Цей метод рекомендовано використовувати для баз даних, які є частиною середовища тестування і розробки, оскільки він дозволяє зберегти логічну структуру даних, забезпечуючи відсутність доступу до конфіденційної інформації поза виробничим середовищем.

5. *Моніторинг активності баз даних*. Аудит і відстеження дій всередині бази даних передбачає знання про те, яка інформація була оброблена, коли, як і ким.

Взявши до уваги цю інформацію, для ідентифікації було запропоновано використання алгоритму SHA3 для створення персонального QR-коду на основі текстових або інших, наприклад, біометричних, даних людини.

Даний QR буде унікальним посиланням на комірку пам'яті в системі та виконуватиме роль об'єкта безпеки системи. Головне завдання цього QR-коду – передати унікальність об'єкта (людини) для машинозчитувальних систем.

Створення хеш-суми відбувається за допомогою спеціального додатку divHasher. Це невелика програма, що працює під Windows, призначена для зручного і надзвичайно швидкого обчислення хешів (або контрольних сум) для будь-яких файлів або тексту. Утиліта вміє підраховувати контрольні суми практично за всіма поширеними алгоритмами: MD2, MD4, MD5, SHA1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD-128, RIPEMD-160, RIPEMD-256, WHIRLPOOL, Tiger , Adler32, CRC32 і Panama.

Для використання програми необхідно вибрати файл або вставити в спеціальне віконце текст, контрольні суми яких потрібно розрахувати.

Далі вибирають алгоритми і натискають кнопку «Обчислити». Після підрахунку можна скопіювати будь-які дані в буфер обміну прямо з програми. Приклад обчислення даних наведено на рис. 1.

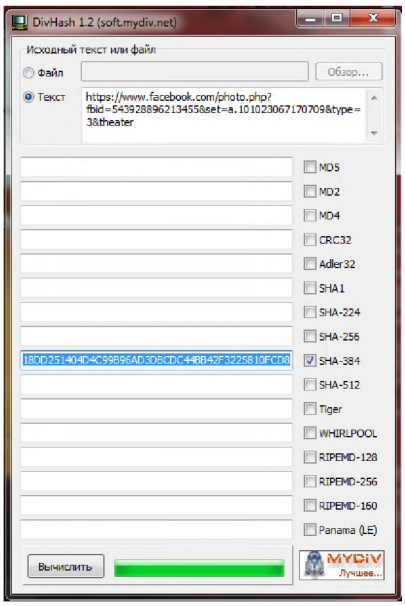

Рис. 1. Приклад отримання хеш-суми завдяки алгоритму SHA3

У запропонованому прикладі хешуються персональні дані, такі як ПІБ, дата та місце народження, місце навчання (роботи, служби), ідентифікаційний номер. Додатково можна використовувати відповіді на запитання.

Далі генеруємо QR-код за допомогою спеціального додатку QR-Code Studio. QR-Code Studio – Дизайнер QR-Code – безкоштовна програма для швидкого та легкого створення QR-кодів. Програма дуже проста у використанні і не вимагає ніяких спеціальних знань. Помічник введення даних спрощує створення штрих-кодів QR-Code для мобільного маркування та маркетингу: всього за кілька секунд можна створити штрих-коди QR-Code для вебсайтів, скачування файлів, для посилань на додатки, Facebook, Twitter і LinkedIn сторінки, SEPA-платежі, відправки SMS.

Створені QR-Code штрих-коди можуть бути збережені у форматі растрової графіки (BMP, GIF, JPG, TIF, PNG) або скопійовані в буфер обміну.

Отримані зображення поширюються за ліцензією Royalty Free і можуть бути використані або оброблені для цілей приватного чи некомерційного використання.

Крім цього, підтримується створення електронних бізнес-карток в форматах vCard або meCard. Приклад генерації наведено на рис. 2.

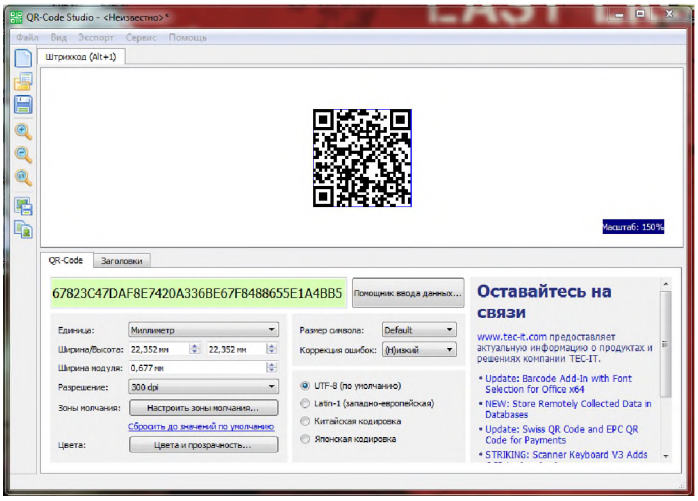

Рис. 2. Генерування QR-коду з даних у вигляді хеш суми

В подальшому даний QR-код можна застосовувати на пластиковому документі, комбінуючи його з іншими елементами захисту. Однак це не обов'язково, адже в процесі автентифікації буде представлено всі дані про об'єкт, якому належить цей код.

Практична реалізація процедури автентифікації

Контроль доступу в запропонованому алгоритмі реалізується шляхом захищеності процедури доступу до всіх груп даних, що містяться в системі. Приклад структури бази даних зображено в таблиці 2. Застосування об'єкта системи та захищеність її бази даних від несанкціонованого доступу відіграє роль активної та пасивної автентифікації в даному алгоритмі. Далі, після зчитування QR-коду, персональні дані графічно виводяться на пристрій. Це надає змогу вповноваженій особі чи системі отримати та порівняти потрібну персоналізовану інформацію про людину, щоб підтвердити її статус.

Таблиця 2

Структура бази даних

Хеш-сума	Об'єкт системи
026f8e459c8f89ef75fa7a78265a0025	file 1425.jpg
ef75fa7a78265a0025026f8e459c8f89	file 2467.jpg

Дану систему можна реалізувати на апаратній частині у вигляді спеціалізованого ліцензійного додатку для різних операційних систем (android, IOS, Windows, Linux та ін.). А також є варіант створення спеціального вебсервера баз даних.

Сервер баз даних виконує обслуговування та управління базою даних та відповідає за цілісність та збереження даних, а також забезпечує операції введення-виведення при доступі клієнта до інформації. Архітектура клієнт – сервер складається з клієнтів та серверів. Основна ідея полягає в тому, щоб розміщувати сервери на потужних машинах, а додаткам, що використовують мовні компоненти системи контролю і управління доступом, забезпечити доступ до них з менш потужних машин-клієнтів за допомогою зовнішніх інтерфейсів.

Дана система дозволяє відмовитись від елементів персоналізації на самій картці, адже всі персоналізовані дані тепер зберігаються в захищеній базі даних системи. Це дозволить значно здешевити процес створення ідентифікаційного документу. Однак необхідне чітке розмежування в доступі різних класів користувачів. Наприклад, супер-користувач – співробітник організації (установи), який наділений правами щодо втручання та допуску до бази даних може додавати та видаляти учасників системи. Адміністратор – співробітник, який використовує базу даних для службових цілей, але не має можливості зміни або втручання в роботу бази даних. Та учасник системи – фізична особа, яка лише користується системою для отримання допуску до об'єкта або привілеїв, пов'язаних з цим об'єктом.

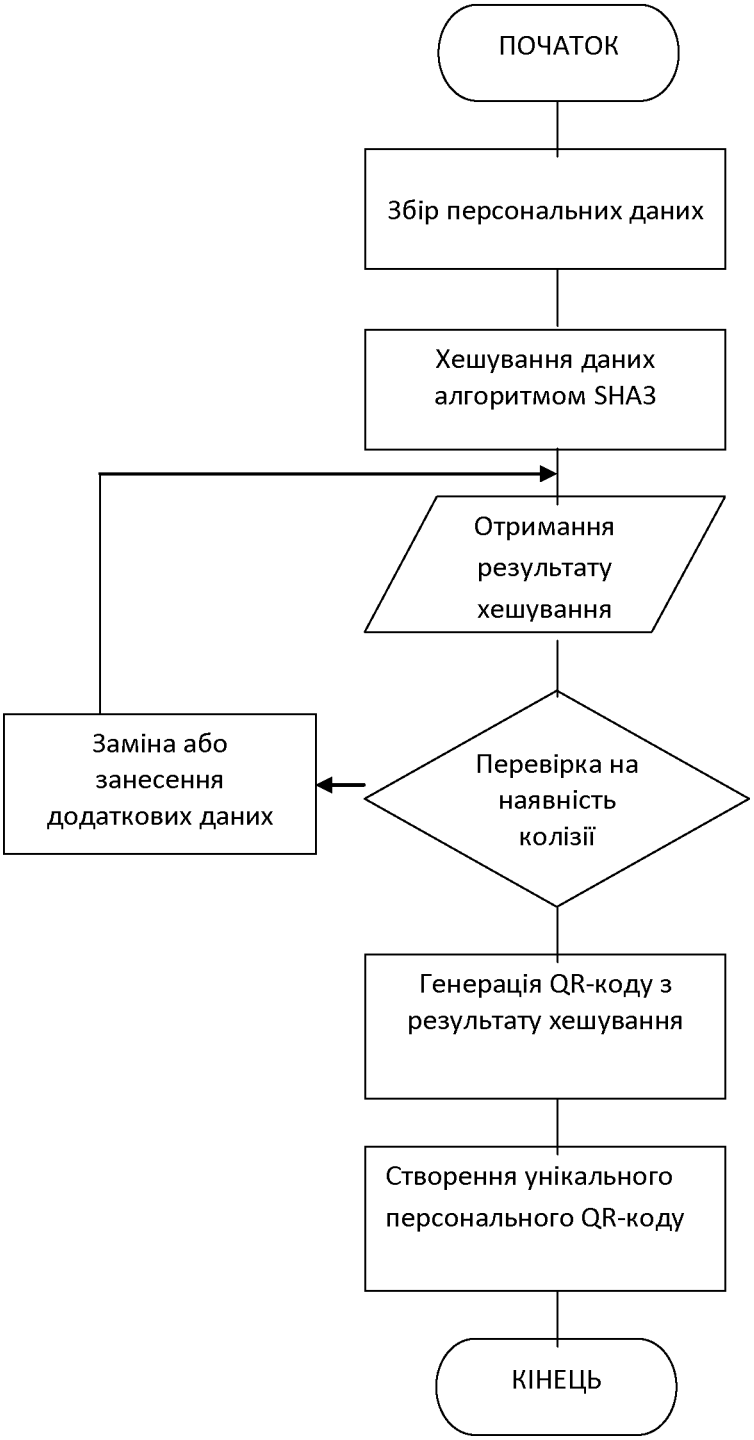

Рис. 3. Блок-схема алгоритму ідентифікації та створення персонального QR-коду

Практичне застосування

Використовуючи алгоритм ідентифікації, хешуємо дані у вигляді вебпосилання (URL), як приклад використовується персональна сторінка з соцмережі facebook (рис. 1). Також необхідно перевірити, чи не відбулась невідповідність в процесі хешування інформації. Відомості чи сукупність відомостей про фізичну особу, в тому числі фото, статус, рід занять, дозволять здійснити перевірку дійсності документа та відповідність його власнику. В подальшому є можливість створити спеціальний захищений вебсервер для обробки, зберігання та використання персональної інформації членів установи або організації.

Далі генеруємо QR-код з хеш-суми (URL). Таким чином інформація про дані у вигляді вебпосилання приховується, а залишається лише набір символів. Для реалізації процедури

автентифікації розроблено спеціальний додаток faceScanQr для смартфонів з операційною системою Android. Цей додаток має вбудовану базу даних з можливістю запису та видалення з неї інформації. Також в програму вбудовано елемент, який зчитує 2D (QR) коди. Інформація подається у вигляді ключа та вебпосилання (URL), далі вони заносяться в базу даних інстальованого додатку (рис. 4).

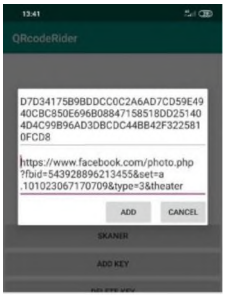

Рис. 4. Занесення інформації в базу даних

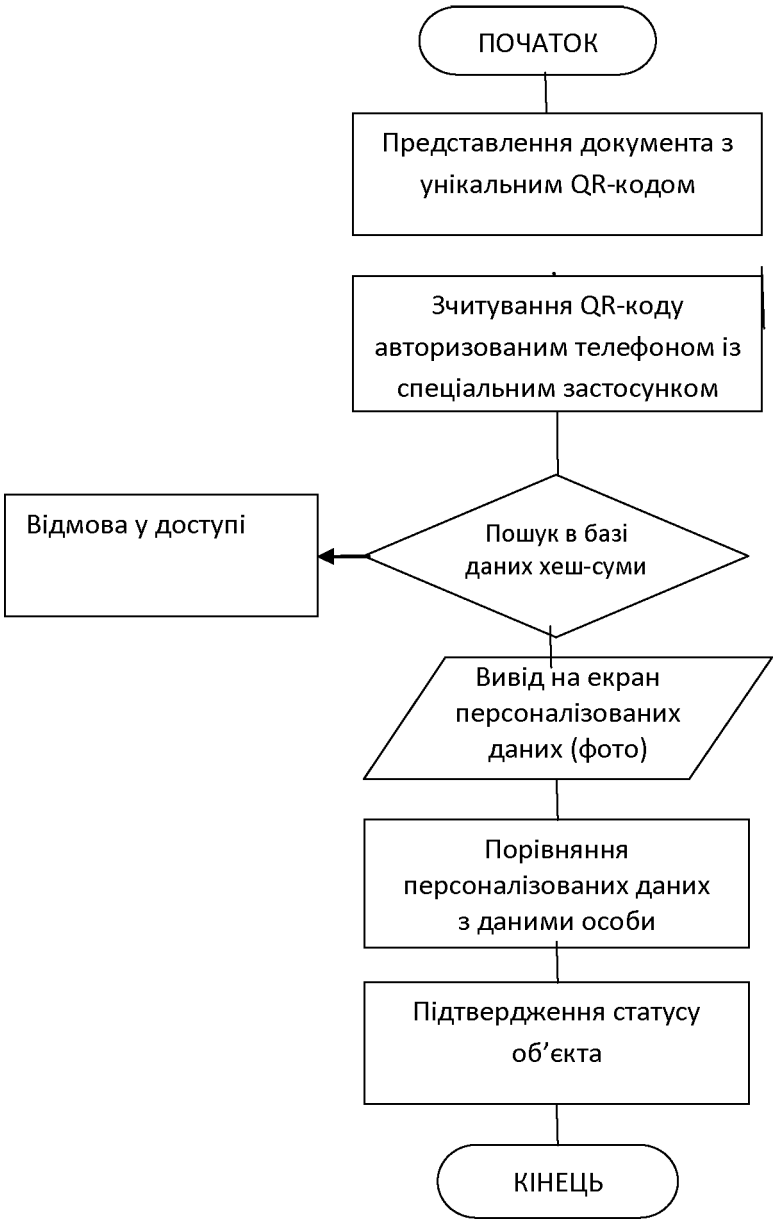

Рис. 5. Блок-схема алгоритму автентифікації та підтвердження статусу

Процес роботи можна описати, використовуючи змінні Н, у, та х. Де Н – це об'єкт бази даних (рядок в таблиці), х – це ключ (код), у – посилання, де х=у. При зчитуванні сканером ключа на екран виводиться лише у. Тобто реалізується система, де наявні публічні та приватні дані (рис. 6).

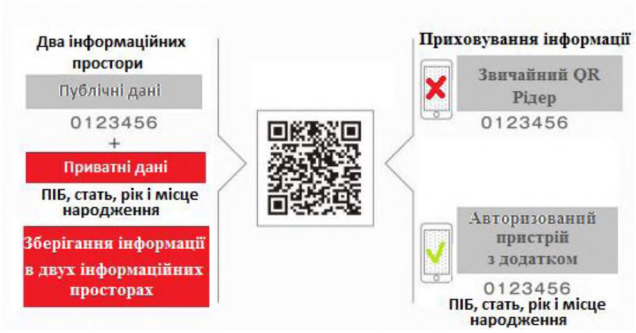

Рис. 6. Принцип дії системи

Рис. 7. Блок-схема алгоритму роботи додатку faceScanQr

Висновки. Аналіз сучасних пластикових документів, ступенів їх захисту, елементів ідентифікації та автентифікації показав, що найголовнішим методом забезпечення процесу ідентифікації та автентифікації пластикових документів виступає реалізація в процесі

створення систем на основі машинозчитуваних елементів. Кожен вид машинозчитуваного елементу має власну технологію створення і відповідні властивості. Залежно від цих властивостей підбирається варіант застосування елементу в пластикових документах різного рівня важливості.

Встановлено, що на ступінь захищеності документа впливають два основні чинники, такі як контроль доступу та проведення кінцевих пасивної або активної автентифікацій.

Розроблено власний варіант системи ідентифікації та автентифікації пластикових документів на основі 2D (QR) коду.

Запропонована система може бути використана як аналог більш дорогим варіантам організації контрольно-пропускного режиму на об'єктах завдяки своїй простоті, малоймовірності несанкціонованого доступу до алгоритмів і процесу роботи її елементів.

Використання даної системи на контрольно-пропускних пунктах може значно покращити управління та забезпечити захищеність системи безпеки, процесу перетину контрольованої зони. Підсумовуючи результати, можна стверджувати: щоб якісно та надійно захистити документ від підробки, забезпечити його автентичність – необхідно надалі покращувати процеси кодування, ідентифікації та автентифікації персоналізованої інформації. Напрямком подальших досліджень може бути розробка системи з переносом персоналізованої інформації з документів напряму до баз даних машинозчитуваних систем. Адже, по-перше, це захистить персональну інформацію особи від дій зловмисника. По-друге, це полегшить сам процес створення документів і значно здешевить його. Однак найважливішим параметром залишиться стійкість та захищеність від несанкціонованого втручання в роботу машинозчитуваних електронних систем.

ЛІТЕРАТУРА

1. Вольфган Р., Вольфганг Е. Довідник зі смарт-карток. *Довідник* / John Wiley & Sons. 4 листопада 2010 р. Технологія та інженерія. 1088 с.

2. ДСТУ ISO–7810. ID-картки – фізичні характеристики.

3. ДСТУ ISO 7811. ID-картки – методи запису.

4. ДСТУ ISO–7812. ID-картки – система нумерації і процедура реєстрації ідентифікаторів емітентів (5 частин).

5. ДСТУ ISO–7813. ID-картки – картки для фінансових транзакцій.

6. ДСТУ ISO–7816. ID-картки – картки з мікросхемою і контактами (6 частин).

7. Абакумов В. Г. Методи захисту пластикових карт / В. Г. Абакумов, Л. В. Ратомська // Друга конференція молодих вчених «Електроніка – 2009»: збірник статей. Київ, 2009. Ч. 2. С. 61–68.

8. Пиріг С. О. Платіжні системи: навч. посіб. Київ: Центр учбової літератури, 2008. 240 с.

9. Бугаєв Леонід. Мобільний маркетинг. Як зарядити свій бізнес в мобільному світі. Москва: Паблішер, 2012. 214 с. ISBN 978-5-9614-2222.

10. ДСТУ ISO / IEC 18004-2015. Інформаційні технології. Технології автоматичної ідентифікації та збору даних. Специфікація символіки штрихового коду QR Code.

11. Проведення судово-технічної експертизи документів, оснащених машинозчитуваними елементами захисту: метод. рек. / Мін'юст України; за ред. Л. М. Головченко. Київ: КНДІСЕ, 2012. 95 с.

12. Шнайер Брюс. Прикладна криптографія. Протоколи, алгоритми, вихідні тексти на мові Сі. Москва: Тріумф, 2002. ISBN 5-89392-055-4.

13. Дональд Кнут. Мистецтво програмування. (The Art of Computer Programming). 2-ге вид. Москва: Вільямс, 2007. Том 3. Сортування і пошук (Vol. 3. Sorting and Searching). 824 с. ISBN 0-201-89685-0.

14. Вірт Ніклаус. Алгоритми і структури даних. Москва: Мир, 1989. ISBN 5- 03-001045-9.

15. Киричок П. О. Захист цінних паперів та документів суворого обліку. Київ: НТУУ «КПІ», 2008. 368 с.