DOI: 10.32347/2412-9933.2024.59.131-137
УДК 004.93

Шабала Євгенія Євгенівна
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії,
https://orcid.org/0000-0002-0428-9273
Київський національний університет будівництва і архітектури, Київ
Корнійчук Борис Валерійович
Кандидат технічних наук, доцент, доцент кафедри професійної освіти, *https://orcid.org/0000-0003-3881-1581*
Київський національний університет будівництва і архітектури, Київ
Гуменний Дмитро Олександрович
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії,
https://orcid.org/0000-0001-6736-0543
Київський національний університет будівництва і архітектури, Київ

НЕДОЛІКИ ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ІДЕНТИФІКАТОРІВ У СИСТЕМАХ ОБМЕЖЕННЯ ДОСТУПУ

Анотація. *Біометричні системи здійснюють ідентифікацію особи на основі її унікальних фізичних характеристик, таких як відбитки пальців, розпізнавання обличчя, ірису, голосу тощо. Ці системи набули широкого застосування в різних сферах, зокрема у безпеці, управлінні доступом, банківському секторі та охороні здоров'я. Однак вони також стикаються з низкою технічних, етичних і правових викликів, які необхідно вирішувати для забезпечення їх ефективного впровадження та використання. Переваги біометричних систем включають високу точність і надійність ідентифікації, що забезпечується унікальністю біометричних даних кожної особи. Це робить їх ефективними у забезпеченні безпеки об'єктів та інформації, контролі доступу і автоматизації різноманітних процесів. Біометричні системи також відомі своєю зручністю для користувачів, які можуть уникнути потреби запам'ятовування складних паролів або носіння ключів. Проте існують і серйозні обмеження. Одним із найбільших є питання приватності і безпеки даних. Біометричні дані, які разом із тим є незмінними, можуть стати об'єктом крадіжок або зловживань. Це може призвести до серйозних наслідків для користувачів, включаючи ідентифікаційне шахрайство і злочини. Крім того, важливо враховувати, що не всі люди можуть комфортно використовувати біометричні системи через фізичні або медичні обмеження. Другим ключовим аспектом є технічні проблеми, такі як недостатня точність систем, вразливість до фальсифікації і нестабільність у різних умовах експлуатації. Наприклад, системи розпізнавання обличчя можуть недостатньо точно працювати при зміні емоцій або освітлення. Для вирішення цих проблем необхідно розробляти комплексні підходи, які включають у себе не лише технічні, але й етичні та правові механізми захисту даних. Також важливо забезпечити високий рівень освіти користувачів щодо безпеки і приватності використання біометричних систем. Отже, біометричні системи являють собою потужний інструмент для забезпечення безпеки й ідентифікації в різних сферах, однак їх ефективне впровадження потребує уваги до технічних, етичних і правових аспектів.*

Ключові слова: біометричні системи; ідентифікація особи; безпека даних; точність розпізнавання; ідентифікатор

Постановка проблеми

Біометричні системи відіграють важливу роль у сучасному світі, пронизуючи різні сфери нашого життя. Вони забезпечують унікальні можливості ідентифікації особи на основі її фізичних характеристик, таких як відбитки пальців, розпізнавання обличчя, зіниць ока, голосу та інших біометричних параметрів. Отже, біометричні системи являють собою потужний інструмент для забезпечення безпеки, ефективності та зручності в різних сферах нашого життя. Їх важливість продовжує зростати в умовах зростаючих вимог до безпеки та швидкості опрацювання інформації.

Аналіз останніх досліджень і публікацій

Є два основних чинники, які ускладнюють практичне впровадження біометричних методів. Альтернативний підхід, який не має значущих

недоліків, полягає у використанні моделей ідентифікації осіб на підставі їхньої ходи [1]. Суттєвою складністю впровадження біометричної системи є розробка її архітектури. У роботі «Автоматизовані системи керування доступом» [2] описана класифікація та вимоги до всіх сучасних систем керування доступом:

– забезпечувати контроль доступу на всіх типах КПП;

– виключати можливість пронесення/провезення заборонених предметів і препаратів;

– затримувати потенційних порушників як внутрішнього трудового розпорядку, так і зовнішніх відвідувачів, які намагаються проникнути на об'єкти, які перебувають під охороною;

– мати можливість використовувати різні способи ідентифікації особистості;

– мати відкриту програмно-апаратну платформу, яку в подальшому можна буде інтегрувати з будь-якими іншими системами безпеки;

– забезпечувати автоматизацію процесів управління та координацію діяльності об'єкта;

– системно функціонувати в разі виходу з ладу окремих компонентів та в інших надзвичайних ситуація.

Мета статті

Метою статті є огляд біометричних ідентифікаторів як ефективного інструменту для забезпечення безпеки й ідентифікації в різних сферах життя, з особливим акцентом на їхні переваги та недоліки. Розглянуто технічні, приватнісні та соціальні виклики, які стоїть перед впровадженням таких систем. Біометричні ідентифікатори, такі як відбитки пальців, розпізнавання обличчя, голосові та інші параметри, стають все більш популярними завдяки їх високій точності та надійності порівняно з традиційними методами ідентифікації, такими як паролі чи ключі. Однак вони також стикаються із серйозними викликами, включаючи приватнісні питання, технічні обмеження та потребу у високих витратах на впровадження та підтримку, що потребує розроблення методів підвищення безпеки та зниження чинників, які впливають на поширеність використання біометричних ідентифікаторів у системах обмеження доступу.

Виклад основного матеріалу

Біометричні ідентифікатори відіграють ключову роль у біометричних системах обмеження доступу. Ці системи використовують фізичні характеристики людини, такі як відбитки пальців, розпізнавання обличчя, розпізнавання ірису, голосові реєстри, для автентифікації особи.

Одним з основних переваг біометричних ідентифікаторів є їхня висока точність і надійність, оскільки біометричні дані унікальні для кожної людини. Однак у цьому є і обмеження.

По-перше, можливі проблеми з приватністю, оскільки біометричні дані можуть бути викрадені або скомпрометовані. Це може породжувати серйозні збої в системі безпеки, оскільки біометричні дані неможливо змінити, як пароль чи PIN-код.

По-друге, важливо враховувати, що не всі люди можуть бути зручні з використанням біометричних систем. Деякі можуть мати фізичні або медичні обмеження, які роблять біометричну аутентифікацію важкою або неможливою.

Крім того, впровадження біометричних систем може бути дорогим і складним процесом. Потрібна велика кількість технічних знань і ресурсів для розгортання та підтримки таких систем.

Незважаючи на ці обмеження, біометричні ідентифікатори продовжують набувати широкого застосування у сфері забезпечення безпеки та доступу, завдяки своїй унікальності і надійності.

Наведемо деякі недоліки біометричних ідентифікаторів у біометричних системах, які слід врахувати.

Приватність і безпека даних. Одним з найбільших недоліків є ризик порушення приватності та безпеки даних. Хоча біометричні дані унікальні для кожної людини, вони можуть бути вкрадені або підроблені. Якщо таке станеться, користувач може стати жертвою ідентифікаційного шахрайства або зловживання.

Проблемою надійності є питання безпеки зібраної біометричної інформації. Більшість біометричних систем уразливі для зламу за допомогою перехоплення, збереження та подальшого відтворення даних. Наскільки це можливо, залежить від методу передавання біометричної інформації по мережі. Найгірше те, що будь-який біокод, на відміну від безособового коду-паролю, практично завжди несе в собі набагато більше інформації, ніж це потрібно для перевірки доступу. Навіть малюнок райдужної оболонки ока, не кажучи вже про ДНК код, може повідомити фахівцю важливу інформацію про стан індивідуума, його вроджені або набуті властивості, у т. ч. хвороби. А ця інформація, очевидно, є надто інтимною, щоб давати доступ до неї не тільки своєму лікарю. Можливі зловживання очевидні кожному – від дискримінації прийому на роботу до прямого шантажу [3].

Неможливість скасування. На відміну від паролів чи ключів доступу, які можна легко змінити в разі компрометації, біометричні дані неможливо змінити. Це означає, що якщо біометричні дані скомпрометовані, користувачу може бути складно або навіть неможливо знову забезпечити безпеку своїх даних.

Приватність і безпека даних біометричних ідентифікаторів викликають серйозні занепокоєння і потребують ретельної уваги. Наведемо кілька ключових аспектів, які слід врахувати.

– *Ризик викрадення даних*. Біометричні дані, такі як відбитки пальців чи розпізнавання обличчя, є унікальними і невідновлюваними. Це означає, що якщо ці дані потраплять у ненадійні руки, їх можна використати для викрадення ідентичності або для здійснення ідентифікаційного шахрайства.

– *Потенційні атаки на системи зберігання даних.* Біометричні дані зазвичай зберігаються в базах даних або на пристроях для зчитування. Ці системи можуть бути піддані кібератакам або фізичним вторгненням, що може призвести до компрометації даних.

– *Можливість фальсифікації*. Незважаючи на те, що біометричні дані унікальні, їх можна використовувати для створення фальшивих біометричних ідентифікаторів. Наприклад, ірис може бути відтворений за допомогою контактних об'єктивів або образів.

– *Законодавчі аспекти*. Збирання і зберігання біометричних даних можуть підпадати під законодавчі обмеження, які регулюються стосовно захисту особистих даних і приватності користувачів.

– *Анонімізація та шифрування*. Важливо застосовувати ефективні методи анонімізації та шифрування для захисту біометричних даних від несанкціонованого доступу.

– *Контроль доступу і аудит*. Системи біометричної ідентифікації повинні мати механізми контролю доступу й аудиту, щоб відслідковувати та контролювати доступ до біометричних даних.

У багатьох розвинених країнах світу практично половина дорослого населення перебуває у базах даних. Цей тренд є серйозною загрозою для особистої приватності, за словами правозахисних організацій. Агентство національної безпеки США збирає такі фотографії протягом багатьох років. Урядові органи в Україні дуже цікавляться технологіями розпізнавання облич з міркувань безпеки й застосування права. Нещодавно з'явилася інформація, що міські ради обласних центрів планують установити камери на всіх мостах і тунелях, щоб розпізнавати тих, хто ними користується. У ЄС такі технології мають відповідати Директиві ЄС про захист даних та Генеральному регламенту про захист даних. Але права людини в різних країнах ЄС досі відрізняються. Автоматична ж перевірка, що виконується на основі розпізнавання облич, є дуже сумнівною з погляду збереження права людини на приватність [4].

Загальною практикою є впровадження комплексних заходів захисту даних, включаючи технологічні, організаційні та правові заходи, щоб забезпечити високий рівень приватності та безпеки даних біометричних ідентифікаторів.

Технічні недоліки. Біометричні системи можуть мати технічні недоліки, такі як недостатня точність або вразливість до фальсифікації. Наприклад, система розпізнавання обличчя може бути помилкова при розпізнаванні осіб з різними емоціями або зміненими фізичними параметрами.

Технічні недоліки біометричних ідентифікаторів можуть включати різні аспекти, які слід врахувати.

– *Недостатня точність.* Деякі системи біометричної ідентифікації можуть мати недостатню точність у розпізнаванні осіб. Це може призводити до помилок в ідентифікації та автентифікації користувачів, що своєю чергою може призвести до відмов у доступі або неправомірного доступу.

– *Вразливість до фальсифікації.* Деякі біометричні системи можуть бути вразливі до методів фальсифікації. Наприклад, відбитки пальців можуть бути відтворені за допомогою макетів, а розпізнавання обличчя може бути обмануте за допомогою обличчя-маски або фотографії.

– *Чутливість до змін.* Деякі біометричні характеристики можуть бути чутливими до змін у фізичних параметрах особи, таких як вага, зачіска, вік тощо. Це може призводити до помилок у розпізнаванні в разі змін у зовнішності користувача.

– *Вартість інфраструктури.* Впровадження та підтримка біометричних систем може бути витратним завданням. Це включає в себе вартість обладнання для збору та аналізу біометричних даних, програмне забезпечення для обробки даних, а також витрати на навчання персоналу та підтримку системи.

– *Неоднорідність біометричних даних.* Біометричні дані можуть відрізнятися у кожної людини через такі фактори, як умови освітлення, кути зйомки, якість обладнання тощо. Це може ускладнювати процес розпізнавання ідентичності.

– *Проблеми з використанням.* Деякі люди можуть мати проблеми з використанням біометричних систем через фізичні або медичні обмеження, наприклад, люди з ушкодженими пальцями не можуть використовувати системи розпізнавання відбитків пальців.

Медичні або фізичні обмеження. Деякі люди можуть мати медичні або фізичні особливості, які ускладнюють або навіть унеможливлюють використання біометричних ідентифікаторів. Наприклад, люди з певними захворюваннями або травмами можуть мати проблеми з розпізнаванням відбитків пальців або інших біометричних характеристик. Перешкодою до точної ідентифікації може стати накладання гриму або суттєва зміна частини обличчя (пластична хірургія) [5].

Медичні або фізичні обмеження можуть ускладнювати використання біометричних ідентифікаторів для деяких користувачів.

– *Ушкодження відбитків пальців.* Люди з ушкодженими відбитками пальців, такими як рубці, опіки або інші пошкодження шкіри, можуть мати проблеми з розпізнаванням відбитків пальців системами біометричної ідентифікації.

– *Особливості обличчя*. Деякі люди можуть мати особливості обличчя, такі як великі окуляри або бороду, які можуть ускладнювати розпізнавання обличчя системами біометричної ідентифікації.

– *Ірисові аномалії.* Ірис очей кожної людини унікальні, але деякі медичні стани, такі як катаракта чи глаукома, можуть впливати на форму та текстуру ірису, що може ускладнювати розпізнавання системами біометричної ідентифікації.

– *Проблеми з акустикою голосу*. Деякі люди можуть мати проблеми з голосом через захворювання або травми, що може ускладнювати розпізнавання голосових біометричних ідентифікаторів.

– *Фізичні обмеження.* Інколи люди можуть мати фізичні обмеження, які ускладнюють використання біометричних систем. Наприклад, люди з обмеженими рухами можуть мати проблеми зі збереженням статичного положення для сканування відбитків пальців або обличчя.

– *Анатомічні відмінності.* Інколи анатомічні відмінності між особами можуть призвести до того, що певні біометричні характеристики, такі як відбитки пальців чи ірис очей, будуть менш надійними для ідентифікації.

У зв'язку з цим важливо розглядати альтернативні методи ідентифікації або використовувати комплексні системи, які поєднують декілька методів біометричної ідентифікації, для забезпечення надійності і доступності для всіх користувачів.

Вартість і складність реалізації. Впровадження біометричних систем може бути витратним і технічно складним процесом. Потрібна велика кількість ресурсів для розроблення, налаштування та підтримки таких систем.

Незважаючи на ці недоліки, біометричні ідентифікатори залишаються ефективним інструментом для забезпечення безпеки та ідентифікації в різних сферах, включаючи в'їзд на територію, банківські операції та ідентифікацію працівників.

Вартість реалізації біометричних систем може значно відрізнятися залежно від різних факторів, таких як масштаб проєкту, вибір технологій, потреби в налаштуванні та інтеграції, а також вартість обслуговування та підтримки. Наведемо деякі ключові аспекти, які впливають на вартість:

– *Обладнання.* Вартість обладнання для збору біометричних даних, такого як сканери відбитків пальців, камери для розпізнавання обличчя або сканери ірисів очей, може бути значною, особливо якщо потрібна велика кількість пристроїв для широкомасштабного застосування.

– *Програмне забезпечення.* Вартість програмного забезпечення для обробки та аналізу біометричних даних також може бути значною. Це включає в себе розроблення або придбання програмного забезпечення для розпізнавання шаблонів, алгоритми біометричної ідентифікації, системи управління доступом та інше.

– *Інтеграція з наявними системами.* Якщо біометричну систему потрібно інтегрувати з наявними системами безпеки або управління доступом, вартість інтеграції може бути значною. Це може включати розроблення API, забезпечення сумісності з наявними системами та налагодження інтеграції.

– *Навчання персоналу.* Вартість навчання персоналу з використання біометричних систем також треба враховувати. Персонал має бути навчений користуватися обладнанням, встановлювати та налаштовувати системи, а також вирішувати можливі проблеми.

– *Підтримка та обслуговування.* Вартість підтримки та обслуговування біометричних систем також потрібно враховувати. Це може включати вартість технічної підтримки, оновлення програмного забезпечення, регулярні аудити та технічне обслуговування обладнання.

Отже, вартість реалізації біометричних систем може бути значною, але вона може бути виправдана значним покращенням безпеки, ефективності та зручності для користувачів.

У реальних умовах під час зчитування біометричного зразка (наприклад венозного рисунка долоні руки) для виправлення можливих неточностей і помилок, які можуть виникнути через зміну або обертання зображення венозного рисунка в зареєстрованому шаблоні порівняно з контрольним, використовується процедура перетворення абсолютних значень параметрів мінуцій на відносні за допомогою таких формул:

$$\begin{cases} d_{ij} = \sqrt{(x_i - y_j)^2 + (y_i - y_j)^2} \\ \alpha - 1_{ij} = \alpha_{ij} - \alpha_i \\ \alpha - 2_{ij} = \alpha_j - \alpha_i \\ \alpha - 3_{ij} = \alpha_{ij} - (\alpha_i + \alpha_j), \end{cases} \quad (1)$$

де i, j – мінуції; d_{ij} – відстань між точками i та j; $\alpha - 1_{ij}$ – кут між напрямом точки i та напрямом на точку j; $\alpha - 2_{ij}$ – кут роздвоєння між напрямом

точки i та напрямом точки j ; $\alpha - 3_{ij}$ – кут збігу напряму точки i та напрямом точки j у дугу.

Біометричними характеристиками людини (БХЛ) називається її вимірювана фізична характеристика або персональна поведінкова риса. Ідентифікація людини реалізується в процесі перевірки БХЛ на ідентичність зареєстрованому користувачеві [6]. Ідеальна характеристика має легко збиратись, бути універсальною, унікальною і постійною. Універсальність – можливість представлення людини однією характеристикою. Унікальність означає, що не повинно бути двох осіб з ідентичними характеристиками. Сталість (перманентність) – характеристика не повинна змінюватися з часом. Збирання (вимірюваність) – можливість швидко і легко одержати і деталізувати характеристику від індивідуума [7]. Експертна оцінка біометричних ідентифікаторів людини наведена на рис. 1.

Експертна оцінка властивостей БХЛ: (+ + + – висока оцінка, + + – середня, + – низька)

Характеристика	Універсальність	Унікальність	Сталість	Вимірюваність
Відеообраз обличчя	+++	+	++	+++
Термограмма обличчя	+++	+++	+	+++
Відбиток пальця	++	+++	+++	++
Геометрія руки	++	++	++	+++
Райдужна оболонка ока	+++	+++	+++	++
Сітківка	+++	+++	++	+
Підпис	+	+	+	+++
Голос	++	+	+	++
Відбиток губ	+++	+++	++	+
Особливості вуха	++	++	++	++
Динаміка підпису	+++	+++	+	+++
Хода	+++	++	+	+

Рисунок 1 – Експертна оцінка властивостей БХЛ

У сучасному цифровому світі проблема забезпечення безпеки ідентифікації користувачів стає все більш актуальною і складною через швидкий розвиток технологій штучного інтелекту (ШІ). Один з найважливіших аспектів цієї проблеми полягає у фальсифікації зображень, створених за допомогою штучного інтелекту, для обходу систем аутентифікації та входу в захищені системи.

Штучний інтелект здатний створювати високоякісні фотографії та відео, які майже не відрізняються від реальних зразків. Це може включати синтез обличчя людини, рухи, мовлення і навіть індивідуальні біометричні параметри, такі як відбитки пальців чи структура радужки.

Зловмисники можуть використовувати такі штучно створені зображення для фальсифікації біометричних даних і обхідних атак на системи ідентифікації та аутентифікації. Наприклад, штучно створені відбитки пальців чи обличчя можуть бути використані для отримання несанкціонованого доступу до комп'ютерних систем, фінансових ресурсів або конфіденційної інформації.

Щоб боротися з цими загрозами, необхідно розвивати і вдосконалювати технології виявлення підроблених зображень та алгоритми біометричної перевірки, які можуть розрізняти реальні та штучно створені дані. Також важливо вдосконалювати правові норми та політику щодо захисту приватності і безпеки даних, щоб забезпечити ефективний захист від таких видів кібератак. Використання ШІ для створення фальсифікованих зображень для фальсифікації входу в систему є серйозною загрозою для кібербезпеки. На сьогодні вирішення цієї проблеми потребує комплексного підходу, що включає технічні інновації, правові заходи та освіту користувачів щодо кібербезпеки.

Розпізнавання зображень, створених штучним інтелектом, або підроблених відео може бути складним завданням через швидкий розвиток технологій обробки зображень і відео. Методи, які можуть допомогти розпізнати такі матеріали, наведені на рис. 2.

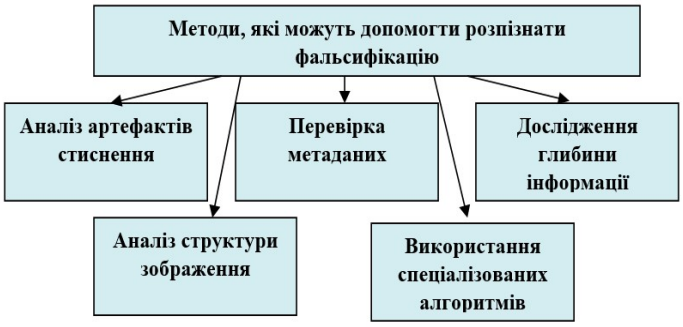

Рисунок 2 – Методи розпізнавання фальсифікації зображень

1. ***Аналіз артефактів стиснення***. Підроблені або синтезовані зображення часто мають артефакти стиснення (наприклад блокові артефакти у JPEG-зображеннях). Аналіз цих артефактів може допомогти виявити, чи було зображення синтезоване.

2. ***Перевірка метаданих***. Метадані (такі як час зйомки, тип камери, параметри фотоапарата) можуть розкрити, чи було зображення зроблене реальною камерою або синтезоване програмним засобом.

3. ***Дослідження глибини інформації***. У деяких випадках синтезовані зображення можуть містити несправжню або недосконалу інформацію про глибину (наприклад помилки у відтворенні перспективи або тіней).

4. ***Аналіз структури зображення***. Структура зображення і розподіл деталей можуть викликати підозру. Наприклад, синтезовані обличчя можуть мати нереалістичну текстуру або несправжні очі.

5. ***Використання спеціалізованих алгоритмів***. Деякі спеціалізовані програми або алгоритми можуть бути призначені для виявлення підроблених відео або зображень штучного походження.

Під час віддаленої автентифікації дані, що мають автентифікувати користувача, передаються

мережею, під час чого можуть бути спотворені завадами в каналах зв'язку та скомпрометовані в результаті різних типів атак.

На самому початку системи передавання даних можлива фальсифікація даних (spoofing attack) – використання фальсифікованих біометричних характеристик користувача, поновлення та використання старих даних, які використовувалися раніше під час автентифікації. Також існує ймовірність атаки у вигляді несанкціонованого доступу до сформованого біометричного шаблону під час автентифікації, його підміна або підміна шаблону (substitution attack) [8; 9], який зберігається в базі даних. Небезпечною є атака маскарад (masquerade attack), коли цифровий образ може бути створений із шаблону біометричного образу. Є ймовірність впливу з метою підміни рішення під час порівняння біометричних шаблонів [10].

Висновки

Основними висновками щодо недоліків використання біометричних ідентифікаторів у системах обмеження доступу є нижченаведене.

По-перше, за все, серйозним недоліком є питання приватності та безпеки даних. Біометричні дані, що використовуються для ідентифікації особи, є унікальними і незмінними, що робить їх особливо цінними для зловживань і крадіжок. Це створює потенційні загрози для користувачів, оскільки їхні персональні дані можуть бути скомпрометовані через кібератаки або фізичний доступ до систем зберігання біометричних даних.

По-друге, значущим аспектом є технічні проблеми, які включають в себе недостатню точність систем розпізнавання та вразливість до фальсифікації. Наприклад, низька точність у роботі систем розпізнавання обличчя може призводити до помилок у визначенні ідентичності осіб, особливо у змінних умовах освітлення або емоційного стану.

По-третє, недоліком є висока вартість впровадження та підтримки біометричних систем. Це включає в себе не лише витрати на придбання обладнання і програмного забезпечення, а й необхідність навчання персоналу та забезпечення регулярного технічного обслуговування. Такі витрати можуть виявитися значними для організацій, особливо великих підприємств чи установ.

Нарешті, важливо враховувати соціальні й етичні виклики використання біометричних систем. Не всі користувачі можуть бути зручні з таким видом ідентифікації через фізичні або медичні обмеження, такі як ушкодженість пальців або обличчя.

Усі ці недоліки вимагають комплексного підходу до впровадження біометричних систем, який враховуватиме технічні, приватностісні, економічні та соціальні аспекти. Вирішення цих проблем уможливить максимізувати переваги біометричних ідентифікаторів у системах обмеження доступу, забезпечуючи водночас ефективний захист особистих даних і комфорт для користувачів.

Список літератури

1. Пуріш С. В. Біометричні ідентифікатори в біометричних системах обмеження доступу. The 3rd International scientific and practical conference "Modern research in science and education" (November 9-11, 2023) BoScience Publisher, Chicago, USA. 2023. 1096 c.

2. Корчинський В., Тарасенко І., Рациборинський С., Акаєв О., Хаджиогло А. Автоматизовані системи керування доступом. Herald of Khmelnytskyi National University. Technical Sciences, 2024. 333(2). С.140–145.

3. Пастушенко М. О., Пастушенко М. С., Петраченко М. О. До питання оцінки ефективності біометричних систем Електронне наукове фахове видання. *Проблеми телекомунікацій.* 2023. № 1 (32). С. 37–44 URL: https://pt.nure.ua/wp-content/uploads/2023/12/123_Pastushenko_biometric_.pdf (дата звернення 15.06.2024).

4. Кулешник Я. Ф., Сеник В. В., Сорокач О. В. Застосування інформаційних технологій для автоматизованої ідентифікації осіб: навч. метод. посібник. Львів: ЛьвДУВС. 2019. 122 с.

5. Шабала Є. Є. Біометричні методи захисту від несанкціонованого доступу на територію аеропорту. *Управління розвитком складних систем*: зб. наук. пр. Київ: КНУБА, 2019. № 38. С. 51–55.

6. Jain Anil K. & Ross, Arun (2008). Introduction to Biometrics. In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp. 1–22.

7. Швець В. А., Фесенко А. А. Основні біометричні характеристики, сучасні системи та технології біометричної аутентифікації. Безпека інформації. 2013. №2, Том 19. С. 99 – 111.

8. Lutsenko M. S., Kuznetsov O. O., Prokopovich-Tkachenko D. I., and Zverev V. P., "Comparative analysis of biometric cryptosystems," Applied radio electronics, 2018. vol. 17, no. 3, 4, pp. 182–191.

9. Poongodi, and P. Betty, "A Study on Biometric Template Protection Techniques." International Journal of Engineering Trends and Technology (IJETT). 2014. Vol.7, no. 4. pp. 202-204.

10. Астраханцев А. А. Процес керування захищеністю даних під час віддаленої біометричної автентифікації. *Системні дослідження та інформаційні технології* : міжнародний науково-технічний журнал. 2022. № 3. С. 71–85.

Стаття надійшла до редколегії 30.08.2024

Shabala Yevheniia
Ph.D., associate professor, associate professor of Department of cyber security and Computer Engineering,
https://orcid.org/0000-0002-0428-9273
Kyiv National University of Construction and Architecture, Kyiv
Korniichuk Borys
Ph.D., associate professor, associate professor of Department of Vocation education, *https://orcid.org/0000-0003-3881-1581*
Kyiv National University of Construction and Architecture, Kyiv
Humennyi Dmytro
Ph.D., associate professor, associate professor of Department of cyber security and Computer Engineering,
https://orcid.org/0000-0001-6736-0543
Kyiv National University of Construction and Architecture, Kyiv

DISADVANTAGES OF USING BIOMETRIC IDENTIFIERS IN ACCESS RESTRICTION SYSTEMS

Abstract. *Biometric systems identify a person based on their unique physical characteristics, such as fingerprints, facial recognition, iris, voice, etc. These systems are widely used in various fields, including security, access control, banking and healthcare. However, they also face a number of technical, ethical and legal challenges that need to be addressed to ensure their effective implementation and use. The advantages of biometric systems include high accuracy and reliability of identification, which is ensured by the uniqueness of each person's biometric data. This makes them effective in ensuring the security of objects and information, access control and automation of various processes. Biometric systems are also known for their convenience for users, who can avoid the need to remember complex passwords or carry keys. However, there are also serious limitations. One of the biggest issues is privacy and data security. Biometric data, which at the same time are immutable, can become the object of theft or misuse. This can lead to serious consequences for users, including identity fraud and crime. In addition, it is important to consider that not all people can comfortably use biometric systems due to physical or medical limitations. The second key aspect is technical problems, such as insufficient accuracy of systems, vulnerability to falsification and instability in different operating conditions. For example, facial recognition systems may not work accurately enough when emotions or lighting change. To solve these problems, it is necessary to develop comprehensive approaches that include not only technical, but also ethical and legal data protection mechanisms. It is also important to ensure a high level of user education regarding the security and privacy of the use of biometric systems. In conclusion, biometric systems represent a powerful tool for security and identification in various fields, but their effective implementation requires attention to technical, ethical and legal aspects.*

Keywords: biometric systems; identification of the person; data security; recognition accuracy; identifier

References

1. Purish, S. (2023). Biometric identifiers in biometric access control systems. The 3rd International scientific and practical conference “Modern research in science and education” (November 9-11, 2023) BoScience Publisher, Chicago, USA, 1096.
2. Korchynskyi, V., Tarasenko, I., Ratsyborynskyi, S., Akayev, O., Khadzhioglo, A. (2024). Automated access control systems. *Herald of Khmelnytskyi National University*, *Technical Sciences*, 333 (2), 140–145.
3. Pastushenko, M. O, Pastushenko, M. S, Petrachenko, M. O. (2023). On the issue of assessing the effectiveness of biometric systems. *Electronic scientific specialist publication – journal "Telecommunications Problems»*, 1 (32), 37–44. URL: https://pt.nure.ua/wp-content/uploads/2023/12/123_Pastushenko_biometric_.pdf
4. Kuleshnyk, Y., Senyk, V., Sorokach, O. (2019). Application of information technologies for automated identification of persons: training manual. Lviv: LvDUVS, 122.
5. Shabala, Ye. & Klyuyeva, V. (2019). Biometric methods of protection against unpassed to the airport territory. *Management of Development of Complex Systems*, 38, 51–55, [in Ukrainian], dx.doi.org\10.6084/m9.figshare.9788444.
6. Jain, Anil K. & Ross, Arun. (2008). Introduction to Biometrics. In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer, 1–22.
7. Shvets, V., Fesenko, A. (2013). Basic biometric characteristics, modern biometric authentication systems and technologies. *Information security*, 2, 19, 99–111.
8. Lutsenko, M., Kuznetsov, O., Prokopovich-Tkachenko, D., Zverev, V. (2018). Comparative analysis of biometric cryptosystems. *Applied radio electronics*, 17, 3, 4, 182–191.
9. Poongodi, P., Betty, P. (2014). A Study on Biometric Template Protection Techniques. *International Journal of Engineering Trends and Technology (IJETT),* 7, 4, 202–204.
10. Astrakhantsev, A. (2022). Data security management process during remote biometric authentication. *System research and information technologies: an international scientific and technical journal*, 3, 71–85.

Посиланя на публікацію

APA Shabala, Ye., Korniichuk, B., & Humennyi, D. (2024). Disadvantages of using biometric identifiers in access restriction systems. *Management of Development of Complex Systems*, 59, 131–137, dx.doi.org\10.32347/2412-9933.2024.59.131-137.

ДСТУ Шабала Є. Є., Корнійчук Б. В., Гуменний, Д. О. Недоліки використання біометричних ідентифікаторів у системах обмеження доступу. *Управління розвитком складних систем.* Київ, 2024. № 59. С. 131 – 137, dx.doi.org\10.32347/2412-9933.2024.59.131-137.