https://doi.org/10.31891/2219-9365-2025-84-51
УДК 621.396

ПАРХОМЕЙ Ігор
Київський національний університет імені Тараса Шевченка
https://orcid.org/0000-0002-9510-7657
e-mail: ihor.parhomey@knu.ua
БОЙКО Юлій
Хмельницький національний університет
https://orcid.org/0000-0003-0603-7827
e-mail: boiko_julius@ukr.net
БОЙКО Дмитро
Київський національний університет імені Тараса Шевченка
https://orcid.org/0009-0006-1195-1065
e-mail: boyko.dmytro@knu.ua

ІНТЕЛЕКТУАЛЬНИЙ ПРОТОКОЛ ВІДЕОАУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ БАНКОМАТІВ ДЛЯ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ

В статті запропоновано інтелектуальний метод підвищення безпеки аутентифікації користувачів під час опрацювання фінансової інформації цифровими терміналами (банкоматами) шляхом використання відеоканалу пристрою з автоматичним розпізнаванням особи та аналізом її поведінкових ознак у процесі взаємодії з системою. Розроблено модель протоколу відеоаутентифікації, який поєднує біометричну ідентифікацію, поведінковий аналіз та криптографічний захист каналів обміну. Проведено моделювання логіки прийняття рішень у вигляді марківського процесу (Marcov Descsion Process, MDP), що враховує баланс між швидкодією та рівнем безпеки. Запропонований підхід забезпечує адаптивність до мережевих умов, стійкість до типових атак (replay, spoofing, substitution) та можливість інтеграції з існуючими банківськими інфраструктурами.

Ключові слова: відеоаутентифікація, біометрична ідентифікація, поведінковий аналіз, марківський процес прийняття рішень, кібербезпека фінансових систем

PARKHOMEY Igor, BOIKO Dmytro
Taras Shevchenko National University of Kyiv
BOIKO Juliy
Khmelnytskyi National University

INTELLIGENT VIDEO AUTHENTICATION PROTOCOL FOR ATM USERS TO ENHANCE CYBERSECURITY

This paper proposes an intelligent protocol for enhancing the cybersecurity of user authentication in automated teller machines (ATMs) through the integration of a video channel that performs both biometric identification and behavioral analysis. The proposed approach enables the system to recognize a user's identity and verify the authenticity of their actions in real time, thereby reducing the probability of spoofing, replay, and substitution attacks. The architecture of the video authentication protocol unifies visual feature extraction, liveness detection, and encrypted data exchange within a formalized interaction model between the user, terminal, and decision-making server. The protocol's decision logic is modeled as a Markov Decision Process (MDP) with a reward function that balances security confidence and response time. In the event of network degradation, the system performs a graceful fallback, shifting critical verification tasks to the terminal and executing asynchronous server-side validation with deferred confirmation. Data confidentiality is ensured through on-device template storage, pseudonymization, and differential privacy mechanisms, while integrity is maintained using digital signatures and nonce-based freshness control. Simulation results demonstrate the feasibility of integrating the proposed protocol into existing banking infrastructures without significant latency overhead. The developed model provides a foundation for further research in intelligent multimodal authentication systems that combine video analytics, behavioral biometrics, and adaptive cybersecurity frameworks for next-generation financial technologies. The research contributes to the development of resilient, user-centric authentication mechanisms that enhance trust and operational security in digital financial ecosystems.

Keywords: video authentication, biometric identification, behavioral analysis, Markov decision process, financial cybersecurity

Стаття надійшла до редакції / Received 04.11.2025
Прийнята до друку / Accepted 06.12.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Забезпечення кібербезпеки фінансових операцій, що здійснюються через автоматизовані термінали самообслуговування (банкомати, POS-термінали тощо), є одним із ключових викликів сучасної фінансово-інформаційної інфраструктури. Традиційні методи аутентифікації користувачів — зокрема за допомогою PIN-кодів чи банківських карток — дедалі частіше піддаються ризикам компрометації, соціальної інженерії та фішингових атак. У зв'язку з цим актуальним є впровадження нових технологій ідентифікації, які поєднують високий рівень надійності з комфортом користувача.

Одним із найперспективніших напрямів є використання біометричних засобів розпізнавання — зокрема аналізу обличчя, відбитків пальців, райдужної оболонки ока чи поведінкових характеристик користувача. Особливу увагу наукової спільноти привертають методи динамічної або поведінкової аутентифікації, які дозволяють оцінювати факт реальної присутності користувача та його реакцію на візуальні запити в режимі реального часу. Такі технології, засновані на 3D-ознаках та аналізі руху, демонструють точність понад 97 % при визначенні життєздатності та ідентифікації особи [1].

Світова практика свідчить, що комбінація різних біометричних факторів забезпечує найвищий рівень захисту. Наприклад, у Японії ряд компаній впровадили банкомати з технологією ідентифікації за венозним малюнком долоні [2], у США — системи «cardless transaction» із підтвердженням через розпізнавання обличчя або QR-код, у Китаї — інтегровані системи відеоідентифікації з національною базою даних громадян (банкомати з розпізнаванням обличчя у реальному часі, тоді наприклад, в ICBC (Industrial and Commercial Bank of China) користувач може здійснити транзакцію лише після підтвердження особи через камеру банкомата), а в Індії — багатофакторні рішення, що поєднують PIN-код, відбиток пальця та «facial ID». У країнах ЄС розробляються системи відеоаналітики, які додатково оцінюють поведінку користувача під час взаємодії з банкоматом. Рішення з відеоаналітики — це розподілена система відеоконтролю, яка інтегрує камери з системою транзакцій банкоматів. Вона забезпечує цілодобовий моніторинг, запис, передачу і зберігання інформації, а також миттєве оповіщення у разі непередбаченої ситуації [3].

У Європі, зокрема в Німеччині, розробляються банкомати з інтелектуальними системами виявлення шахрайства, де відеоаналіз поведінки користувача дозволяє виявити підозрілі дії (наприклад, присутність сторонніх осіб поблизу або незвичні рухи). Це реалізовано як доповнення до класичної біометрії.

Окрім відео- та безконтактних технологій, на ринку також представлені системи апаратного контролю доступу. Наприклад, система обмеження доступу до банкоматів, яка автоматично вмикає освітлення при вході клієнта і вимикає його у разі відсутності людей, також проводить мовне інформування та працює з усіма типами платіжних карток [4].

Є моделі, пристосовані для роботи з великою кількістю периферійних пристроїв. Одне з таких рішень, наприклад, пропонує вбудовані комп'ютери та серійні розширення, які дозволяють забезпечити надійне управління додатковими пристроями безпеки, камерами, зчитувачами та сенсорами біометрії [5].

У категорії багатофакторної біометрії використовуються комбінації відбитків пальців, райдужної оболонки ока та розпізнавання обличчя, що істотно підвищує надійність аутентифікації в безкарткових системах АТМ [6]. Крім того, існують рішення, які інтегрують візуальний канал таким чином, що відображається активний запит чи шаблон, а користувач повинен реагувати на нього певним чином — наприклад, утримувати обличчя у вказаній області кадру чи повторювати рух — що допомагає виявляти шахрайські дії із застосуванням відео, фальшивих зображень чи deepfake–моделі [7].

В Україні також спостерігається активний розвиток технологій безкарткової ідентифікації та інклюзивних сервісів. Зокрема, запроваджено банкомати, що підтримують Apple Wallet і Google Wallet, рішення з голосовими помічниками для осіб із вадами зору, а також системи апаратного відеоконтролю та моніторингу [8].

У результаті, ринок банкоматів вже пропонує комплексні рішення для банкоматів — від безконтактної аутентифікації до голосового помічника, відеомоніторингу та апаратного контролю доступу, які разом формують надійну та передову інфраструктуру безпеки.

Разом із тим, незважаючи на швидкий розвиток біометричних технологій, відсутні уніфіковані протоколи відеоаутентифікації, які б забезпечували інтеграцію відеоаналізу, визначення життєздатності користувача та верифікації його дій у межах єдиного процесу фінансової транзакції. Це зумовлює потребу в розробленні методів, що поєднують алгоритмічну обробку відеоданих із системою прийняття рішень, орієнтованою на підвищення стійкості до шахрайства.

Таким чином, науково-практичне завдання та мета даної статті полягають у розробленні протоколу відеоаутентифікації користувачів банкоматів, який підвищує рівень кібербезпеки фінансових операцій шляхом інтеграції біометричної ідентифікації та поведінкового аналізу користувача в єдину систему захисту.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Технічні рішення систем розпізнавання облич (Face Recognition) сьогодні охоплюють як класичні алгоритмічні підходи, так і сучасні нейромережеві моделі, які стали стандартом для практичного використання [9].

Найбільш ранні реалізації базувалися на геометричних методах, коли ключові точки обличчя (відстань між очима, форма носа, контури рота) описувалися у вигляді векторів ознак. До них належали алгоритми Eigenfaces (метод головних компонент, PCA) та Fisherfaces (метод лінійного дискримінантного аналізу, LDA) [10]. Такі підходи швидко обчислювалися, проте виявилися чутливими до освітлення, поворотів голови і зміни міміки.

Наступним кроком стали локальні дескриптори – наприклад, Local Binary Patterns (LBP) або Histogram of Oriented Gradients (HOG) [11], які виділяли текстурні особливості обличчя. Вони підвищили

стійкість до зовнішніх умов, але все одно поступалися у точності новим методам.

Справжній прорив відбувся з появою глибинних згорткових нейронних мереж (CNN) [12]. Системи на основі моделей DeepFace (Facebook, 2014), FaceNet (Google, 2015) та DeepID (Chinese University of Hong Kong) досягли точності понад 99% на стандартних наборах даних (наприклад, LFW – Labeled Faces in the Wild). Ці системи формують для кожного обличчя «вектор ознак» у багатовимірному просторі, що дозволяє з високою надійністю ідентифікувати особу навіть при різних кутах огляду, освітленні чи з віковими змінами.

У сучасній практиці активно застосовуються відкриті бібліотеки та фреймворки. Однією з найбільш популярних є Dlib [12], яка реалізує CNN-підхід до детектування та порівняння облич. Інший приклад – OpenFace, проєкт з відкритим кодом, який базується на FaceNet. Для комерційних рішень поширені сервіси Microsoft Azure Face API, Amazon Rekognition, Face++, що пропонують готові хмарні модулі для виявлення та ідентифікації осіб у реальному часі.

Важливою тенденцією є впровадження edge-computing рішень [13], коли алгоритми працюють безпосередньо на пристроях (смартфонах, камерах чи навіть банкоматах) без передачі даних у хмару. Так, технології Apple Face ID чи Huawei 3D Face Recognition використовують спеціалізовані сенсори для побудови глибинної карти обличчя, що значно підвищує захист від підробок за допомогою фотографій або відео.

У сучасних умовах автоматизованого обслуговування клієнтів банківських терміналів і банкоматів виникає низка актуальних викликів, які значною мірою впливають на надійність, безпеку та комфорт використання цих пристроїв. Зокрема, одним із поширених проявів є вандалізм і навмисне блокування роботи термінала шляхом вкладення сторонніх предметів у прийомні щілини. Часто зловмисники вставляють мотузки, дроти, клей, чужі картки чи інші предмети, що ускладнюють роботу картоприймача чи купюроприймача (рис. 1). Такі атаки не тільки перешкоджають транзакціям, але і створюють ризик пошкодження механізмів і потребу в дорогому технічному обслуговуванні, особливо коли мова про ресайклінгові банкомати.

Рис. 1. Приклади навмисного блокування роботи термінала

Другий виклик — це аналіз емоційного стану клієнта як елемент безпеки. У ситуаціях, коли поруч знаходиться інша особа чи до клієнта щойно зателефонував хтось з наміром примусити до видачі коштів, клієнт піддається сильному емоційному тиску. Сучасні алгоритми аналізу відеопотоку повинні бути здатними визначати ознаки стресу або страху — наприклад, тремтячі руки, прискорене дихання, неспокійну міміку — щоб оперативно вживати заходів: видавати попереджувальні сигнали на екрані, ініціювати «тихий» сигнал охороні, тимчасово блокувати термінал або переключати його в режим додаткової аутентифікації.

Третя, не менш важлива проблема — забезпечення доступності для людей з вадами зору. Все більше сучасних систем обслуговування передбачають голосові команди і аудіосупровід, які вказують користувачу, куди встановити картку, який PIN-пінкод вводити, які кнопки натискати. Крім того, використання голосових підказок у поєднанні з інтерактивним голосовим помічником значно підвищує доступність таких терміналів. Однак розробка таких голосових інтерфейсів має враховувати чутливість до фонового шуму, мовну локалізацію, чіткість формулювань, а також забезпечувати конфіденційність (наприклад, можливість вибрати приватну навушникову взаємодію). Це додає складності програмній частині системного рішення, але істотно підвищує рівень інклюзивності.

Одним із сучасних викликів є інтеграція маркетингових пропозицій у процес обслуговування клієнта, зберігаючи при цьому баланс між персоналізацією і безпекою. Наприклад, після успішної аутентифікації на екрані банкомата можуть з’являтися адаптивні пропозиції — пропозиції про нові фінансові продукти, кредитні лінії, страхування або кешбек програми. Проте важливо, щоб такі рекламні повідомлення були

ненав'язливими, релевантними до профілю клієнта (з урахуванням його попередньої історії обслуговування) і не уповільнювали критичні операції. Також необхідно слідкувати, щоб маркетингові елементи не створювали додаткових ризиків — наприклад, не відволікали клієнта під час введення PIN-коду чи не сприяли маніпуляціям із психологічним тиском (наприклад, рекламна надмірна стимуляція швидкого реагування).

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Моделювання протоколу взаємодії

Моделювання протоколу взаємодії передбачає формалізацію обміну між трьома сутностями — користувачем, терміналом та системою прийняття рішень — як керованого автомату станів із чітко визначеними повідомленнями, часовими обмеженнями та політиками безпеки (рис. 2).

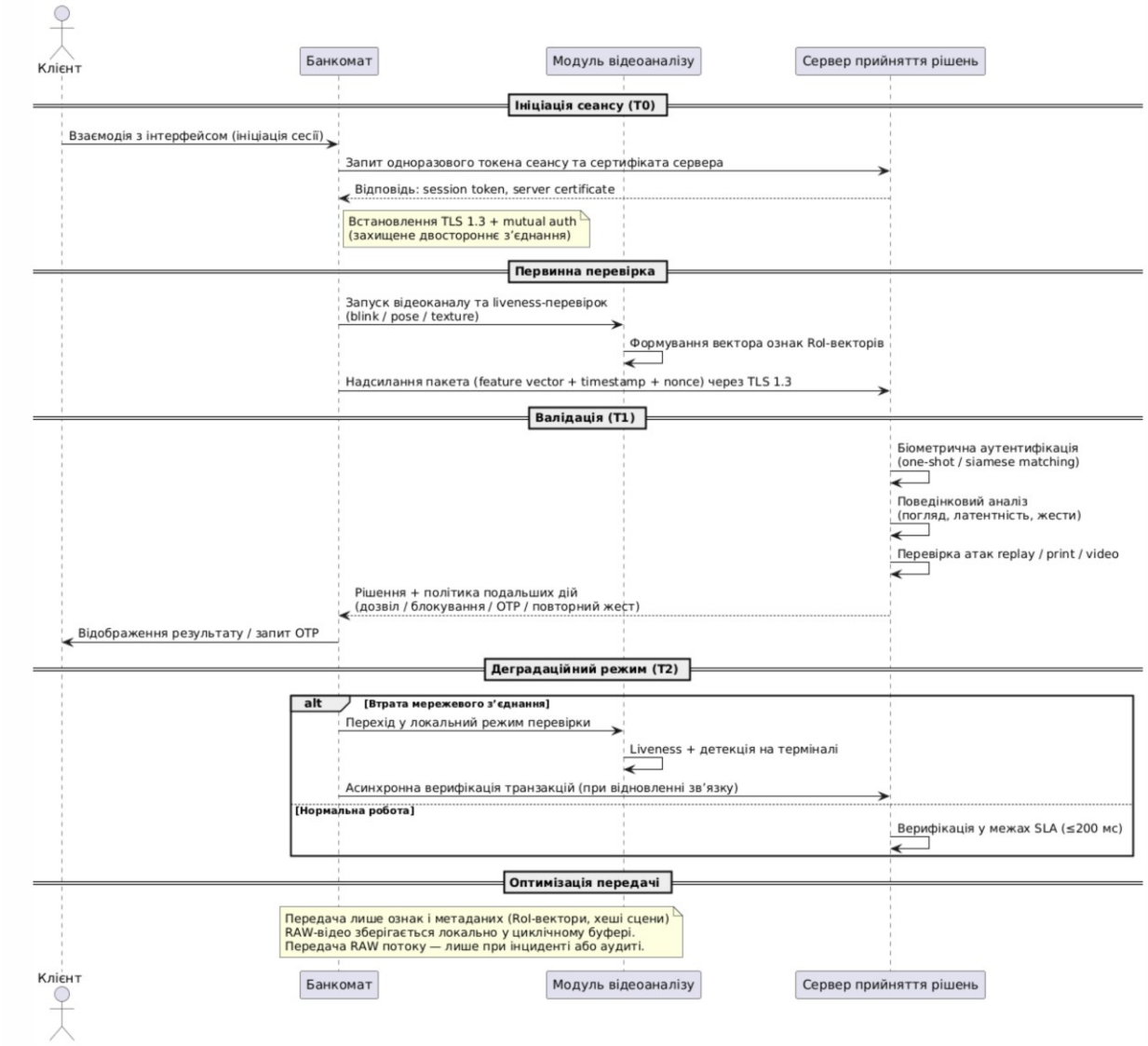

Рис. 2. Модель протоколу відеоаутентифікації користувача банкомата

Сеанс ініціюється встановленням сесії терміналу (T0) з отриманням одноразового токена сеансу та сертифіката сервера. Далі термінал запускає відеоканал і локальні процедури liveness-перевірки (blink/pose/texture), формує вектор ознак z_t та надсилає його в захищеному каналі (TLS 1.3 + mutual auth (Transport Layer Security, версія 1.3) - захищене з'єднання з двосторонньою автентифікацією) у вигляді компактного пакета з часовою міткою і нонсом.

Після первинної валідації (T1) сервер виконує двоканальну аутентифікацію: біометричну (зіставлення z_t із шаблонами або one-shot/siamese-порівнянням) і поведінкову (аналіз траєкторій погляду, латентностей натискань, геометрії жестів) із заданими порогами довіри, а також перевіряє відсутність ознак підміни (replay, print/video attack) за сигнатурами сцени та оптичними індикаторами. У разі достатньої впевненості формується рішення:

$$\alpha_t \in \{APPROVE, CHECK - AGAIN, REJECT\}, \quad (1)$$

та повертається терміналу разом із політикою подальших дій (вимога повторного жесту або One-Time Password/One-Time Token (OTP) (наявність одноразовго OTP-токену або session token на асоційований канал зв'язку), причому сумарна затримка для циклу «кадр → рішення» не перевищує заданого Service Level Agreement (SLA) тобто показники якості сервісу (наприклад, 150–200 мс при локальному передобчисленні). Протокол передбачає режим деградації, за якого у разі втрати мережевого з'єднання критичні перевірки liveness та детекції виконуються локально на терміналі, а серверна частина переходить у режим асинхронної верифікації транзакцій з відкладеним підтвердженням. Для зменшення витрат каналу відео передається у вигляді ознак та метаданих (Region of Interest vectors [14], тобто вектори області інтересу або RoI-вектори, ключові точки, хеші сцени), тоді як «сирий» (необроблений) потік зберігається локально з циклічним буфером і передається лише за умови інциденту або запиту аудитора. RoI-вектори - це компактний набір параметрів, які описують стан або ознаки конкретної області інтересу в кадрі:

$$z_{roi} = f(I_{roi}), \quad (2)$$

де I_{roi} - фрагмент зображення (Region of Interest); $f(\cdot)$ - функція ознак (нейромережевий екстрактор, CNN або transformer).

Конфіденційність забезпечується політикою мінімізації даних (on-device шаблони, диференційна приватність для телеметрії, псевдонімізація), а цілісність — підписами повідомлень і перевіркою порядку (sequence numbers, nonce-based freshness). Логіка прийняття рішень моделюється як марківський процес прийняття рішень MDP (Markov Decision Process) [15] із нагородою за швидкість і безпеку, де дії включають вибір рівня перевірки, повторний запит кадру, ескалацію до оператора та блокування; навчання політики можливе офлайн на симульованих сценаріях атак і онлайн з безпечними обмеженнями:

$$M = (S, A, P, R, \gamma), \quad (3)$$

де S - множина можливих станів системи (етапи взаємодії користувача, результати перевірок, контекст сесії); A - множина дій (вибір рівня перевірки, повторний запит кадру, ескалація, блокування тощо), $P(s' | s, a)$ - ймовірність переходу зі стану s у стан s' після виконання дії a; $R(s, a)$ - функція нагороди, яка відображає баланс між швидкістю обробки та рівнем безпеки; $\gamma \in [0,1]$ - коефіцієнт дисконтування для майбутніх винагород.

Політика, яку позначимо як $\pi(a | s)$ і яка визначає вибір дії у кожному стані, може навчатися офлайн на симульованих сценаріях атак і онлайн — з урахуванням безпечних обмежень, які запобігають ризиковим або нестабільним стратегіям реагування.

Виявлення аномалій у протоколі реалізується окремим контуром, що аналізує послідовності подій (наприклад, нетипова частота скасувань, нестандартні траєкторії жестів, неконсистентність часових міток) і впливає на адаптивні пороги. Завершення сеансу супроводжується підсумковим підписаним звітом (audit record) із хешами ключових артефактів, політикою зберігання та маркерами згоди користувача, що гарантує відтворюваність і відповідність регуляторним вимогам. Така модель дозволяє інтегрувати відеоаналітику, багатофакторну аутентифікацію та кіберзахист у єдиний протокол з формально визначеними властивостями коректності, затримки і стійкості до типових атак.

Запропонований метод інтегрованої відеоаутентифікації користувача у фінансових терміналах має низку практичних сценаріїв застосування. Один із базових прикладів — розширення класичного банкомата, де стандартна перевірка картки та PIN-коду доповнюється автоматичною біометричною ідентифікацією за обличчям та поведінковими ознаками, що дозволяє знизити ризик компрометації PIN-кодів і карток. Подібний підхід може застосовуватись у платіжних кіосках самообслуговування, наприклад, при оплаті комунальних послуг чи поповненні рахунків, де автентифікація через відеоканал зменшує ймовірність використання вкрадених або підроблених реквізитів.

Ще одним прикладом є інтеграція методу у системи віддалених банківських офісів, де клієнт взаємодіє з терміналом без присутності оператора: відеоаналіз у реальному часі дозволяє верифікувати особу під час укладення угод чи підтвердження великих транзакцій. Перспективним напрямком є застосування у мобільних банкоматах, що розгортаються у місцях масового скупчення людей або в польових умовах, де класичні механізми безпеки обмежені. Також метод може бути використаний як додатковий рівень захисту при роботі корпоративних фінансових терміналів у великих компаніях, де відеоаутентифікація співробітників допомагає унеможливити доступ сторонніх осіб.

Загалом, приклади показують, що цей метод доречний скрізь, де існує ризик шахрайства з платіжними засобами та де критичною є швидка перевірка особи користувача без необхідності звернення до персоналу.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

В результаті проведеного дослідження розроблено модель протоколу відеоаутентифікації користувачів банкоматів, що поєднує біометричну ідентифікацію, поведінковий аналіз та адаптивні механізми прийняття рішень у єдиній архітектурі.

Запропонований підхід забезпечує підвищення рівня кібербезпеки фінансових транзакцій завдяки використанню відеоканалу для верифікації користувача в реальному часі, формалізованому MDP-моделюванню логіки дій системи та впровадженню політик конфіденційності і цілісності даних.

Розроблена модель характеризується такими перевагами: формальна описаність протоколу взаємодії з визначеними станами, діями та функцією нагороди; можливість адаптивного управління рівнем перевірки залежно від ризику, контексту або поведінкових ознак користувача; забезпечення конфіденційності та цілісності через криптографічні механізми, локальну обробку даних і контроль послідовності подій; підтримка деградованих режимів роботи при втраті мережі та механізмів відновлення транзакцій; інтеграція з системами аудиту через підписані звіти, що підвищує відтворюваність і регуляторну відповідність.

Отримані результати створюють основу для подальших досліджень у напрямах: удосконалення моделей нагороди і навчання політики в MDP для підвищення точності та стабільності прийняття рішень; дослідження методів реального відеолайвнес-аналізу з урахуванням умов освітлення, кутів огляду та атак deepfake; впровадження мультимодальних схем аутентифікації (комбінація обличчя, голосу, жестів); розроблення прототипу апаратно-програмного комплексу для експериментальної перевірки протоколу в реальних банківських терміналах; розширення системи аудиту на основі блокчейн-зберігання записів для забезпечення незмінності доказів.

Таким чином, представлений підхід формує технологічну і методологічну базу для створення інтелектуальних безкарткових систем аутентифікації, орієнтованих на стійкість до сучасних кіберзагроз і відповідність вимогам фінансової безпеки.

Література

1. Castelblanco, A., Rivera, E., Solano, J., Tengana, L., López, C., & Ochoa, M. (2022). Dynamic face authentication systems: Deep learning verification for camera close-up and head rotation paradigms. Computers & Security, 115, Article 102629. https://doi.org/10.1016/j.cose.2022.102629.

2. Yamada, S., Aoki, T., Shimoyama, T., & Mori, S. (2019). Biometric authentication technology facilitating protection and management of biometric data. Fujitsu Scientific & Technical Journal, 55(5), 53–58. Retrieved from: https://surl.li/ptwcgg.

3. Пультова охорона, системи безпеки (BSP Group). [Електронний ресурс]: Режим доступу - https://bsi-group.com.ua/ (дата звернення 03.11.2025).

4. Системи обмеження доступу до банкомату «ШЕРИФ-БАНК». [Електронний ресурс]: Режим доступу - https://surl.li/ydlinf (дата звернення 03.11.2025).

5. MOXA – банкомати. [Електронний ресурс]: Редим доступу - https://surl.li/cgwalq (дата звернення 03.11.2025).

6. Aljuaid, S. M., & Ansari, A. S. (2022). Automated Teller Machine Authentication Using Biometric. Computer Systems Science and Engineering, 41(3), 1009–1025. https://doi.org/10.32604/csse.2022.020785.

7. Ironvest, Inc. (Assignee). (2024). User authentication and transaction verification via a shared video stream (Publication No. WO 2024194747A1). World Intellectual Property Organization. Filed March 13, 2024; published September 26, 2024. Priority claimed from US 18/123,279 (filed March 19, 2023).

8. Viatec. (2024). U-PROX – зручний та безпечний доступ до банкоматів за допомогою карток. Viatec. Отримано з Viatec: U-PROX – зручний та безпечний доступ до банкоматів за допомогою карток. [Електронний ресурс]. – Режим доступу - https://surl.li/nbntzz (дата звернення 03.11.2025).

9. Diebold Nixdorf & Samsung SDS America. (2017, June 12). Diebold Nixdorf and Samsung SDS demonstrate next step in cardless ATM transactions with mobile-based biometric authentication [Press release]. Diebold Nixdorf. Retrieved from: https://surl.lu/ldlhfm.

10. Ghadekar, P., Pradhan, M. R., Swain, D., & Acharya, B. (2024). EmoSecure: Enhancing smart home security with FisherFace emotion recognition and biometric access control. IEEE Access, 12, 93133–93144. https://doi.org/10.1109/ACCESS.2024.3423783.

11. Zhou, W., Gao, S., Zhang, L., & Lou, X. (2020). Histogram of oriented gradients feature extraction from raw Bayer pattern images. IEEE Transactions on Circuits and Systems II: Express Briefs, 67(5), 946–950. https://doi.org/10.1109/TCSII.2020.2980557.

12. IEEE. (2022). IEEE standard for artificial intelligence (AI) model representation, compression, distribution, and management (IEEE Std 2941-2021, pp. 1–226). IEEE. https://doi.org/10.1109/IEEESTD.2022.9739118.

13. IEEE. (2025). IEEE draft standard for data acquisition, filtering and buffering protocols for edge computing node (IEEE P2805.2/D05, pp. 1–45). IEEE.

14. Sawabe, Y., Ikehata, S., & Aizawa, K. (2022). Saliency-based multiple region of interest detection from a single 360° image. IEEE Access, 10, 89124–89133. https://doi.org/10.1109/ACCESS.2022.3200486.

15. Jayaweera, S. K. (2015). Markov decision processes. In Signal processing for cognitive radios (pp. 207–268). Wiley. https://doi.org/10.1002/9781118824818.ch7.

References

1. Castelblanco, A., Rivera, E., Solano, J., Tengana, L., López, C., & Ochoa, M. (2022). Dynamic face authentication systems: Deep learning verification for camera close-up and head rotation paradigms. Computers & Security, 115, Article 102629. https://doi.org/10.1016/j.cose.2022.102629.

2. Yamada, S., Aoki, T., Shimoyama, T., & Mori, S. (2019). Biometric authentication technology facilitating protection and management of biometric data. Fujitsu Scientific & Technical Journal, 55(5), 53–58. Retrieved from: https://surl.li/ptwcgg.
3. Pultova okhorona, systemy bezpeky (BSP Group). [Electronic resource]. Retrieved from https://bsi-group.com.ua/ (accessed November 3, 2025).
4. Systemy obmezhennia dostupu do bankomatu "SHERYF-BANK". [Electronic resource]. Retrieved from https://surl.li/ydlinf (accessed November 3, 2025).
5. MOXA – bankomaty. [Electronic resource]. Retrieved from https://surl.li/cgwalq (accessed November 3, 2025).
6. Aljuaid, S. M., & Ansari, A. S. (2022). Automated Teller Machine Authentication Using Biometric. Computer Systems Science and Engineering, 41(3), 1009–1025. https://doi.org/10.32604/csse.2022.020785
7. Ironvest, Inc. (Assignee). (2024). User authentication and transaction verification via a shared video stream (Publication No. WO 2024194747A1). World Intellectual Property Organization. Filed March 13, 2024; published September 26, 2024. Priority claimed from US 18/123,279 (filed March 19, 2023).
8. Viatec. (2024). U-PROX – zruchnyi ta bezpechnyi dostup do bankomativ za dopomohoiu kartok. Viatec. [Electronic resource]. Retrieved from https://surl.li/nbntzz (accessed November 3, 2025).
9. Diebold Nixdorf & Samsung SDS America. (2017, June 12). Diebold Nixdorf and Samsung SDS demonstrate next step in cardless ATM transactions with mobile-based biometric authentication [Press release]. Diebold Nixdorf. Retrieved from: https://surl.lu/ldlhfm
10. Ghadekar, P., Pradhan, M. R., Swain, D., & Acharya, B. (2024). EmoSecure: Enhancing smart home security with FisherFace emotion recognition and biometric access control. IEEE Access, 12, 93133–93144. https://doi.org/10.1109/ACCESS.2024.3423783
11. Zhou, W., Gao, S., Zhang, L., & Lou, X. (2020). Histogram of oriented gradients feature extraction from raw Bayer pattern images. IEEE Transactions on Circuits and Systems II: Express Briefs, 67(5), 946–950. https://doi.org/10.1109/TCSII.2020.2980557
12. IEEE. (2022). IEEE standard for artificial intelligence (AI) model representation, compression, distribution, and management (IEEE Std 2941-2021, pp. 1–226). IEEE. https://doi.org/10.1109/IEEESTD.2022.9739118
13. IEEE. (2025). IEEE draft standard for data acquisition, filtering and buffering protocols for edge computing node (IEEE P2805.2/D05, pp. 1–45). IEEE.
14. Sawabe, Y., Ikehata, S., & Aizawa, K. (2022). Saliency-based multiple region of interest detection from a single 360° image. IEEE Access, 10, 89124–89133. https://doi.org/10.1109/ACCESS.2022.3200486
15. Jayaweera, S. K. (2015). Markov decision processes. In Signal processing for cognitive radios (pp. 207–268). Wiley. https://doi.org/10.1002/9781118824818.ch7