КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.930
УДК 004.8

Усік Павло Сергійовий
доктор філософії, старший викладач кафедри кібербезпеки та програмного забезпечення
Центрально український національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0002-3268-342X
usikps@kntu.kr.ua

Смірнова Тетяна Віталіївна
к.т.н., старший викладач кафедри автоматизації виробничих процесів
Центрально український національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0001-6896-0612
sm.tetyana@gmail.com

Буравченко Костянтин Олегович
к.т.н., доцент, доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0001-6195-7533
buravchenkok@gmail.com

Смірнов Олексій Анатолійович
д.т.н., професор, завідувач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0001-9543-874X
dr.smirnovoa@gmail.com

Улічев Олександр Сергійович
к.т.н., старший викладач кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0003-3736-9613
askin79@gmail.com

Смірнов Сергій Анатолійович
кандидат технічних наук, доцент, доцент кафедри кібербезпеки та програмного забезпечення
Центральноукраїнський національний технічний університет, Кропивницький, Україна
ORCID ID: 0000-0002-7649-7442
smirnov.ser.81@gmail.com

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БАНКІВСЬКИХ СИСТЕМ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. У статті досліджується застосування сучасних технологій штучного інтелекту (ШІ) як інструменту забезпечення кібербезпеки в банківських системах. В умовах зростаючої кількості складних кібератак традиційні методи захисту вже не можуть забезпечити належний рівень безпеки, тому актуальним є впровадження інтелектуальних систем, які здатні автоматично аналізувати великі обсяги даних і оперативно реагувати на загрози. У роботі досліджуються основні підходи до інтеграції штучного інтелекту в процеси виявлення аномалій та кіберзлочинів у банківській сфері. Проаналізовано ключові технології ШІ, які використовуються для виявлення шахрайства в реальному часі, поведінкової біометрії, протидії фішинговим атакам і автоматизації комплаєнсу та аудиту. На основі практичних кейсів продемонстровано високу ефективність штучного інтелекту у підвищенні точності виявлення загроз, скороченні часу реакції та зменшенні хибнопозитивних спрацьовувань. Особливу увагу приділено питанням адаптивності та самонавчання інтелектуальних систем захисту в умовах динамічного середовища загроз. Наведено переваги інтеграції ШІ в інфраструктуру банківської безпеки, а також окреслено основні виклики, пов’язані з реалізацією таких рішень. Результати дослідження підтверджують перспективність

використання штучного інтелекту як ефективного інструменту кіберзахисту в банківських системах.

Ключові слова: кібербезпека; банківські системи; штучний інтелект; машинне навчання; інформаційна безпека; виявлення шахрайства; поведінкова біометрія; фішинг; комплаєнс.

ВСТУП

Постановка завдання дослідження

Банківські установи, як критичні елементи фінансової інфраструктури, дедалі більше покладаються на цифрові технології. Це призводить до зростання обсягів оброблюваної інформації, а також до ускладнення завдань щодо захисту інформаційних систем. Штучний інтелект (ШІ) відкриває нові можливості в автоматизації, адаптації та підвищенні ефективності систем кіберзахисту. Інструменти на основі ШІ здатні здійснювати поведінковий аналіз користувачів, виявляти аномальні дії, прогнозувати потенційні загрози та адаптувати алгоритми реагування у режимі реального часу.

Постановка проблеми. Сучасні банківські системи зазнають зростаючого рівня кіберзагроз, що еволюціонують як за технічним рівнем, так і за формами реалізації. Водночас традиційні методи кіберзахисту, засновані на фіксованих правилах і відомих сигнатурах атак, дедалі частіше демонструють недостатню ефективність у протидії динамічним і складним загрозам. Шкідливе програмне забезпечення (ПЗ), фішинг, соціальна інженерія, а також атаки із використанням алгоритмів машинного навчання стали реальністю для банківських установ. У зв’язку з цим виникає потреба у впровадженні адаптивних та самонавчальних систем безпеки, здатних оперативно реагувати на нові загрози. Однак інтеграція технологій штучного інтелекту у сферу банківської кібербезпеки супроводжується низкою проблем: недосконалістю технічних рішень, питаннями конфіденційності, відповідальності та відсутністю чітких регуляторних норм. Отже, постає проблема визначення ефективних та безпечних шляхів використання ШІ в банківських системах для протидії актуальним викликам у сфері кіберзахисту.

Аналіз останніх досліджень і публікацій. У роботі [1] розглянуто загальні тенденції впровадження штучного інтелекту в банківській сфері, з акцентом на цифрову трансформацію, оптимізацію клієнтського обслуговування та зниження витрат завдяки автоматизації. У статті [2] визначено та проаналізовано основні напрями застосування ШІ, зокрема у сфері кібербезпеки, виявлення шахрайських дій та управління ризиками, на прикладах реальних банківських установ. У дослідженні [3] подано розгорнутий огляд практичних рішень на основі ШІ, включаючи використання чат-ботів, автоматизоване кредитування, аналітику великих даних і захист від кібератак. Не зважаючи на те що темі впровадження штучного інтелекту в кібербезпеку банківських систем було присвячено досить багато досліджень, темпи розвитку в галузі інформаційних технологій сприяють виникненню нових підходів. Тому виникає потреба в новому дослідженні ключових напрямів використання штучного інтелекту у кібербезпеці банківських систем.

Мета даної статті полягає в комплексному дослідженні сучасних підходів до використання штучного інтелекту в кіберзахисті банківських систем, оцінці їхньої практичної ефективності та визначенні перспектив розвитку цієї технології у фінансовій сфері. У рамках дослідження розглядаються ключові технології ШІ, приклади їхнього застосування для захисту банківських даних і операцій, а також переваги й недоліки, пов’язані з їхньою імплементацією. Окремий акцент зроблено на огляді актуальної літератури, що відображає сучасний стан досліджень у цій галузі, та формуванні науково

обґрунтованих рекомендацій для підвищення рівня кібербезпеки банківських установ. Таким чином, стаття має на меті не лише систематизувати знання про роль ШІ в захисті банківських систем, але й сприяти розвитку стратегій їхньої адаптації до умов цифрової епохи, що постійно трансформується.

Об'єктом дослідження є процес застосування штучного інтелекту.

Предметом дослідження є класифікація інструментів штучного інтелекту для забезпечення кібербезпеки банківських систем.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Штучний інтелект (ШІ) є однією з найбільш трансформаційних технологій XXI століття, що охоплює розробку систем, здатних виконувати завдання, які традиційно асоціюються з людським інтелектом, наприклад, аналіз даних, прогнозування та прийняття рішень. ШІ визначається як набір алгоритмів і моделей, які дозволяють машинам адаптуватися до нових умов і вирішувати проблеми без чіткого програмування. Ця здатність робить ШІ незамінним інструментом у кібербезпеці банківських систем, де швидке реагування на загрози та обробка великих обсягів даних є критично важливими.

Розвиток штучного інтелекту є логічним етапом еволюції постіндустріального суспільства, яке характеризується інтенсивною інформатизацією всіх сфер діяльності людини та суспільства в цілому. Методи та технології ШІ вже інтегровані в повсякденне життя у вигляді інтелектуальних систем, мобільних додатків та веб-сервісів, що підвищують ефективність виробництва, покращують комунікацію та забезпечують безпеку. Особливістю цих систем є здатність до навчання та самонавчання, що дозволяє їм обробляти великі обсяги даних, виявляти причинно-наслідкові зв'язки та прогнозувати події на основі наявної інформації [4]. Це робить ШІ ефективним інструментом у різних галузях, включаючи економіку, охорону здоров'я та виробництво [24].

Теоретична база ШІ спирається на кілька ключових технологій, серед яких особливе місце займають машинне навчання (МН), глибоке навчання (Deep Learning), нейронні мережі (НМ), обробка природної мови (Natural Language Processing, NLP) та експертні системи[25]. Ці підходи лежать в основі інтелектуальних систем, що застосовуються для захисту фінансових установ від кібератак. ШІ інтегрує досягнення математики, інформатики та статистики для створення систем, здатних прогнозувати та нейтралізувати загрози [5]. Розглянемо детальніше ці технології, їхні принципи та значення для кіберзахисту.

Машинне навчання (Machine Learning, ML) є підгалуззю ШІ, яка фокусується на розробці алгоритмів, що дозволяють системам навчатися на основі даних. Замість того, щоб бути явно запрограмованими для виконання конкретних завдань, системи ML аналізують великі обсяги інформації, виявляють закономірності та роблять прогнози або приймають рішення на основі цих даних. Це особливо корисно в кіберзахисті, де ML може допомагати виявляти аномалії та потенційні загрози [26]. Застосування ML у кібербезпеці включає системи виявлення вторгнень (IDS), які аналізують поведінкові моделі користувачів та ідентифікують підозрілі дії. Наприклад, у банківських системах ML використовується для аналізу транзакцій у режимі реального часу, визначаючи потенційно шахрайські операції [6].

Глибоке навчання (Deep Learning) є спеціалізованою підгалуззю машинного навчання, яка використовує багатошарові нейронні мережі для аналізу складних патернів у даних. Цей підхід дозволяє моделювати високорівневі абстракції та виявляти приховані взаємозв'язки, що робить його надзвичайно ефективним у завданнях, пов'язаних з

обробкою зображень, природної мови та виявленням шахрайства в банківських системах. У кіберзахисті глибоке навчання використовується для аналізу мережевого трафіку та розпізнавання складних атак, зокрема атак нульового дня, які неможливо ідентифікувати за відомими сигнатурами [6], [27].

Нейронні мережі є основою глибокого навчання. Вони складаються з взаємопов'язаних вузлів (нейронів), організованих у шари: вхідний, приховані та вихідний. Кожен нейрон отримує вхідні дані, обробляє їх та передає результат наступному шару. Цей процес дозволяє системі навчатися складним функціям та взаємозв'язкам у даних, що є критично важливим для розпізнавання складних кіберзагроз. Прикладом застосування нейронних мереж у кіберзахисті є аналіз поведінкових характеристик користувачів для запобігання несанкціонованому доступу до банківських акаунтів [6].

Обробка природної мови (Natural Language Processing, NLP) займається взаємодією між комп'ютерами та людською мовою. Технології NLP дозволяють системам розуміти, інтерпретувати та генерувати людську мову. У контексті кіберзахисту це може бути використано для аналізу текстових даних, виявлення фішингових повідомлень або автоматизації обробки запитів клієнтів у банківських установах. Завдяки NLP можна ефективно ідентифікувати шкідливі електронні листи та повідомлення, запобігаючи фішинговим атакам, які спрямовані на викрадення банківських даних [6], [28].

Експертні системи — це програми, які імітують процес прийняття рішень експерта в конкретній галузі. Вони використовують базу знань та набір правил для аналізу інформації та надання рекомендацій. У банківському секторі експертні системи можуть допомагати в оцінці кредитоспроможності клієнтів або виявленні підозрілих транзакцій. Ці системи використовуються для автоматизованого аналізу ризиків та оцінки кредитного рейтингу клієнтів на основі історії транзакцій та поведінкових моделей [6].

Застосування ШІ в банківській кібербезпеці

Завдяки високій обчислювальній потужності й здатності до самонавчання, ШІ вже сьогодні трансформує підходи до забезпечення кібербезпеки фінансових установ. Далі буде розглянуто приклади конкретних напрямів застосування штучного інтелекту.

Виявлення шахрайства в реальному часі

Штучний інтелект (ШІ) на базі методів машинного та глибинного навчання дедалі частіше застосовується для виявлення шахрайства в банківській сфері. Сучасні системи обробляють великі масиви транзакційних даних в режимі реального часу, зумівши ідентифікувати підозрілі операції швидше й точніше, ніж традиційні алгоритми на основі жорстких правил [7]. Наприклад, за результатами систематичного огляду, AI-платформи, що використовують Teradata або Feedzai, «значно скорочують час виявлення шахрайства завдяки аналізу великих обсягів транзакційних даних у реальному часі» [7]. Із досліджень також відомо, що ML/DL-системи «володіють надзвичайними можливостями» для обробки великих даних у реальному часі та адаптації до нових схем шахрайства, що робить їх ефективнішими за традиційні методи детекції [7].

Для реального часу характерне використання потокової аналітики та алгоритмів виявлення аномалій. Зазвичай навчають ансамблі класифікаторів (дерева рішень, SVM) і глибинні нейронні мережі на історичних транзакціях та відомих випадках шахрайства. Так, у експерименті Навіна Коккалаконда порівнювали різні моделі й дійшли висновку, що нейронні мережі дають найкращий результат (96,1% точності при часі відповіді близько 32 мс) [8]. Інший приклад наукової розробки — система Varun Kumar (2022), яка поєднує в реальному часі потокові дані з поведінковою аналітикою та автокодерами (autoencoder) для виявлення аномалій. Авторам вдалося «досягти кращих результатів порівняно з

традиційними методами: вищої точності, кращого часу реакції і зниження хибнопозитивних спрацьовувань» [9]. Такі рішення «навчаються» на нових схемах шахрайства, тому їх ефективність підвищується з накопиченням даних та зворотним зв'язком.

Реальні впровадження підтверджують перспективність ШІ-підходів. Так, один великий банк використав глибоку нейромережу на платформі TensorFlow для перевірки зображень чеків у режимі реального часу. Нова система аналізувала оригінальні та підроблені чеки з історичної бази даних і присвоювала кожному скану експертний бал довіри. В результаті банк зафіксував скорочення шахрайських чекових операцій на 50% та економію близько $20 млн на рік (час обробки становив <70 мс на чек, ≈1200 чеків/с) [10]. Аналогічно, компанія Visa, яка у 2024 році впровадила систему Visa Account Attack Intelligence (VAAI) Score на основі генеративного ШІ для виявлення атак типу enumeration у транзакціях без фізичної присутності картки. Система аналізує кожну операцію у режимі реального часу (≈20 мс), присвоюючи їй ризиковий бал, і дозволяє миттєво блокувати потенційно шахрайські дії. За даними Visa, це дозволило знизити хибнопозитивні спрацьовування на 85% [11]. Ці приклади демонструють, що сучасні інструменти ШІ — від нейронних мереж до спеціалізованих аналітичних платформ — реально підвищують ефективність та швидкість детекції фінансового шахрайства.

Поведінковий аналіз клієнтів (Behavioral Biometrics)

Поведінкова біометрія передбачає аналіз унікальних патернів взаємодії користувача з пристроєм (ритм набору тексту, рухи миші, жести на сенсорному екрані тощо) [12]. За допомогою алгоритмів машинного навчання формується персональний «поведінковий профіль» клієнта, і кожна нова дія під час сесії порівнюється з навченим шаблоном. У разі суттєвого відхилення система спрацьовує як детектор аномалій – на відміну від статичних методів автентифікації (пароль, PIN-код) вона може виявити складні шахрайські дії без додаткових дій користувача, оскільки, «специфічність того, як людина користується своїм пристроєм, вкрай важко підробити».

Для класифікації таких поведінкових даних застосовують різноманітні алгоритми машинного навчання. Типовими прикладами є метод опорних векторів (Support Vector Machine, SVM), алгоритм випадкового лісу (Random Forest), алгоритм k-найближчих сусідів (k-NN) та наївний байєсівський класифікатор [13]. У сучасних системах також широко використовують глибокі нейронні мережі (зокрема згорткові та рекурентні), які дозволяють моделювати послідовні патерни поведінки. Наприклад, гібридна CNN+RNN-модель для аналізу рухів миші ідентифікувала користувача з точністю ~99.4% [14]. Крім того, платформи поведінкової біометрії зазвичай обробляють сотні й тисячі ознак одночасно, формуючи багатовимірний профіль користувача.

Переваги поведінкової біометрії очевидні: вона непомітна для користувача і забезпечує безперервну верифікацію протягом усього сеансу. Моделі ШІ адаптуються до еволюції звичок клієнта і, як правило, важчі для підробки, ніж фіксовані паролі чи токени [12]. Практична ефективність методів поведінкового аналізу підтверджена численними кейсами. Наприклад, після впровадження платформи ARIC Risk Hub (Visa/Featurespace) втрати від фішингових атак у фінансовій групі Eika скоротилися приблизно на 90% [15]. Аналогічно, інтеграція рішення Mastercard і Feedzai з використанням поведінкових даних зменшила рівень шахрайства з push-платежами більш ніж на 12% [16]. Ще одним прикладом є партнерство Synchrony та Adobe Commerce, яке включає інтелектуальні рішення з елементами поведінкового аналізу для безпечнішої верифікації покупців під час фінансування покупок онлайн — це дозволяє покращити як користувацький досвід, так і

виявлення нетипової поведінки в реальному часі, знижуючи ризики шахрайства у цифрових транзакціях [17].

Виявлення фішингових атак

Застосування штучного інтелекту у протидії фішинговим атакам у банківських системах передбачає побудову моделей класифікації, які навчаються на великих наборах даних легітимної та фішингової інформації. Такі моделі, зазвичай, використовують алгоритми машинного навчання [18] і здатні виявляти характерні ознаки фішингу у вмісті листів чи запитів. Ключову роль відіграють методи обробки природної мови: вони дозволяють аналізувати текст електронних повідомлень і виявляти лінгвістичні патерни фішингових повідомлень. Поєднання класичного навчання з учителем із ансамблевими методами (AdaBoost, градієнтне підсилення) та глибокими нейромережами (згорткові — CNN, рекурентні — RNN) забезпечує високу точність класифікації [18]. У контексті цифрового банкінгу основними кіберзагрозами є фішинг та суміжні атаки, для виявлення яких застосовують алгоритми на кшталт SVM, RNN, прихованих марковських моделей (HMM) та виявлення аномалій (LOF) [18].

Реальним прикладом використання штучного інтелекту для виявлення фішингових атак є впровадження фреймворку EXPLICATE, який поєднує машинне навчання, пояснюваний ШІ (XAI) та великі мовні моделі (LLM). Ця система була представлена у науковій роботі [19] в березні 2025 року. EXPLICATE інтегрує класифікатор фішингових повідомлень, модулі інтерпретації рішень на основі SHAP і LIME, а також модель DeepSeek v3, яка генерує пояснення у зручній для користувача формі. Це дозволяє не лише точно визначати шкідливі електронні листи (з точністю 98,4%), а й пояснювати причини класифікації, що критично важливо для підвищення довіри з боку співробітників банку та IT-фахівців. Ще одним прикладом використання інноваційних підходів до виявлення фішингових атак є система RAIDER (Reinforcement-Aided Spear Phishing Detector), розроблена Evans та ін. (2021) [20]. Вона базується на методах підкріпленого навчання, що дозволяє динамічно обирати найбільш релевантні ознаки з вхідних даних електронної пошти та значно зменшити їхню кількість (до 55 %), не втрачаючи при цьому ефективності. RAIDER досягає точності виявлення атак до 94 % і є особливо ефективною проти цільових фішингових атак (spear phishing), які важко виявити традиційними фільтрами. Ці приклади демонструють ефективність впровадження сучасних ШІ-рішень у банківські системи безпеки, забезпечуючи не лише високу точність виявлення фішингових загроз, а й прозорість та інтерпретованість рішень, що сприяє зростанню довіри до таких технологій.

Автоматизований комплаєнс та аудит

Автоматизований комплаєнс та аудит у банківській сфері — це процеси перевірки дотримання внутрішніх політик безпеки та зовнішніх нормативно-правових вимог із використанням цифрових технологій. У контексті кібербезпеки ці підходи спрямовані на виявлення ризиків, зловживань, шахрайських операцій, порушень доступу до конфіденційної інформації та інших відхилень, які можуть загрожувати цілісності банківської IT-інфраструктури. Штучний інтелект дозволяє автоматизувати аналіз журналів подій, моніторинг транзакцій, контроль доступу до критичних систем, а також постійне оновлення правил відповідно до змін у нормативній базі. AI-моделі аналізують великі масиви транзакційних та системних даних і здатні виявляти аномалії або порушення, які важко помітити людиною [21]. За допомогою машинного навчання банки можуть ефективніше виявляти шахрайські операції, перевіряти транзакції на відповідність правилам, а також оперативно оцінювати ризики клієнтів [20]. Наприклад, AI-системи можуть автоматично порівнювати внутрішні політики з регуляторними нормами й виводити

попередження про можливі невідповідності, а також генерувати звіти про підозрілі фінансові операції на основі аналізу поведінкових патернів клієнтів [22]. Крім того, моделі ШІ застосовуються й у безпеці ІТ-інфраструктури банків: вони можуть автоматично перевіряти програмний код на вразливості, формувати правила виявлення атак та аналізувати події безпеки, що пришвидшує виявлення інцидентів і реагування на них [22].

Яскравим прикладом реального використання таких AI-систем є платформа KPMG Clara. KPMG описує Clara як «централізовану смарт-технологію аудиту», що забезпечує якісніші й ефективніші перевірки з глибшим аналізом [23]. У квітні 2025 року KPMG оголосила про інтеграцію генеративного ШІ у глобальну платформу KPMG Clara, що дозволило 95 000 аудиторів по всьому світу стандартизувати й автоматизувати рутинні аудиторські процедури та поглибити аналіз ризиків. AI-агенти в KPMG Clara виконують, зокрема, такі завдання, як автоматизована перевірка бізнес-витрат і пошук незареєстрованих зобов'язань клієнтів, що спрощує процес підтвердження транзакцій і зменшує ручну роботу аудитора [23].

Ефективність AI-інструментів у комплаєнсі підтверджують також дослідження та практичні кейси. Зокрема, опубліковане дослідження демонструє, що ML-системи для боротьби з відмиванням грошей (AML), які аналізують транзакції мільйонів рахунків, суттєво зменшують кількість хибних спрацьовувань (false positives) і пришвидшують розслідування підозрілих операцій [21]. Загалом, ці і подібні AI-моделі виявляють складні схеми шахрайства і невідповідної поведінки, що підвищує точність і швидкість аналізу ризиків і контролю відповідності нормативам [21]. Отже, впровадження AI для автоматизованого комплаєнсу й аудиту у банківській безпеці дозволяє посилити превентивні заходи та підвищити ефективність процесів контролю і аудиту.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Порівняльна таблиця демонструє системні зміни, які відбулися у сфері кібербезпеки банківських систем внаслідок впровадження штучного інтелекту. Впровадження штучного інтелекту сприяло трансформації традиційних малоефективних підходів у адаптивні системи, здатні діяти в режимі реального часу. Виявлення шахрайства більше не обмежується перевіркою за фіксованими правилами, а ґрунтується на комплексному аналізі поведінкових та транзакційних даних, що підвищує точність і адаптивність до нових схем зловживань.

Таблиця 1

Порівняльна таблиця

Напрямок застосування ШІ	До використання ШІ	Після використання ШІ
Виявлення шахрайства в реальному часі	Використання правил на основі фіксованих шаблонів; повільна реакція; висока кількість хибнопозитивних спрацьовувань	Аналіз великих обсягів даних у режимі реального часу; швидка і точна детекція аномалій; адаптація до нових схем шахрайства
Поведінковий аналіз клієнтів (Behavioral Biometrics)	Використання паролів та PIN-кодів; автентифікація лише на момент входу; легко підробити	Безперервна аутентифікація за поведінковими патернами; вища стійкість до атак; непомітність для користувача
Виявлення фішингових атак	Статичні фільтри та ручна перевірка листів; низька точність і масштабованість	Використання ML, NLP і XAI для точного виявлення фішингу;

		інтерпретовані результати; протидія цільовим атакам
Автоматизований комплаєнс та аудит	Ручні перевірки, повільна і трудомістка обробка; ризик пропущених порушень	ШІ-моделі для автоматичного виявлення порушень і генерації звітів; швидкий моніторинг; зниження навантаження на аудиторів

Поведінковий аналіз клієнтів, раніше обмежений простими шаблонами, трансформувався у безперервний процес автентифікації, здатний виявляти відхилення навіть на рівні мікроповедінки користувача. Це змінило саму логіку доступу до банківських систем — від одноразової перевірки до постійного моніторингу. У сфері протидії фішинговим атакам штучний інтелект забезпечив глибший семантичний аналіз текстів, що дозволяє ефективно розрізняти легітимні та шкідливі повідомлення. Крім того, автоматизація комплаєнсу та аудиту дозволила перейти від трудомістких перевірок до інтелектуального аналізу ризиків і дотримання нормативів. У результаті ці процеси стали не лише швидшими й точнішими, але й суттєво підвищили рівень операційної безпеки банківських установ.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У даній роботі було досліджено сучасні підходи до використання штучного інтелекту в кібербезпеці банківських систем. Розглянуто чотири ключові напрямки застосування ШІ: виявлення шахрайства в реальному часі, поведінкову біометрію клієнтів, протидію фішинговим атакам та автоматизований комплаєнс й аудит. Наведені приклади практичної реалізації таких рішень продемонстрували високу ефективність моделей штучного інтелекту у підвищенні точності виявлення загроз, скороченні часу реакції та зменшенні кількості помилкових спрацьовувань. Особливу увагу приділено інструментам, що забезпечують адаптивність систем до нових типів атак, а також тим, які поєднують аналітику з прозорістю інтерпретації рішень. Дослідження підкреслило практичну ефективність застосування штучного інтелекту, що дозволяє фінансовим установам ефективніше виявляти аномальні дії, запобігати шахрайству та забезпечувати відповідність нормативним вимогам у динамічному цифровому середовищі.

З огляду на тенденції розвитку, можна прогнозувати, що у подальшому роль ШІ в банківській кібербезпеці буде лише зростати. У найближчому майбутньому ключову роль відіграватимуть моделі, здатні самостійно виявляти, пояснювати та запобігати новим типам атак ще до їх реалізації. Застосування генеративного ШІ, інтерпретованих моделей, а також посилення автоматизації аудиту й моніторингу дозволить суттєво підвищити точність і швидкість реагування. Водночас зростає потреба у нормативному врегулюванні цих технологій, адже банківські установи мають не лише впроваджувати інновації, а й дотримуватись юридичних стандартів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ovcharenko, T. (2024). Trends in the development and use of artificial intelligence in the banking sector. *Economy and Society*. https://doi.org/10.32782/2524-0072/2024-67-44
2. Kholiavko, N., Sadchykova, I., & Kolotok, M. (2023). Directions of use of artificial intelligence in banking institutions. *Problems and Prospects of Economics and Management*. https://ir.stu.cn.ua/handle/123456789/28945

3. Danik, N., & Torlopov, A. (2024). Introducing artificial intelligence into banking: A revolution in service and security. *International Science Journal of Management Economics & Finance*. https://www.researchgate.net/publication/392319259_...
4. Sharov, S. (2023). Current state of artificial intelligence development and its applications. *Ukrainian Studies in the European Context*. http://obrii.org.ua/usec/storage/conference/zb_vol6_2023.pdf
5. BDO Global. (2024). The role of artificial intelligence in cybersecurity: Prediction and prevention of attacks. https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks
6. Willie, A. (2025). The evolution of AI in cybersecurity: From rule-based systems to generative AI. *ResearchGate*. https://www.researchgate.net/publication/388930668_...
7. Adhikari, P., Hamal, P., & Baidoo, F. (2024). Artificial intelligence in fraud detection: Revolutionizing financial security. *International Journal of Science and Research Archive*. https://ijsra.net/content/artificial-intelligence-fraud-detection-revolutionizing-financial-security
8. Kokkalakonda, N. K. (2022). AI-powered fraud detection in banking: Enhancing security with machine learning algorithms. *ResearchGate*. https://www.researchgate.net/publication/390357575_...
9. Tambi, V. K. (2022). AI-powered fraud detection in real-time financial transactions. *International Journal of Research in Electronics and Computer Engineering*. https://philpapers.org/archive/VARAFD-2.pdf
10. Cognizant. (2019). Advanced AI/ML solution detects check fraud for a global bank. https://www.cognizant.com/en_us/case-studies/documents/ai-driven-solution-reduces-fraud-risk-for-bank-codex3688.pdf
11. Visa. (n.d.). Visa announces generative AI-powered fraud solution to combat account attacks. *Visa Official Website*. https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.20661.html
12. Kokal, S., Vanamala, M., & Dave, R. (2023). Deep learning and machine learning, better together than apart: A review on biometrics mobile authentication. *Journal of Cybersecurity and Privacy*, *3*(2), 13. https://www.mdpi.com/2624-800X/3/2/13
13. Pryor, L., Dave, R., Seliya, J., & Boone, E. S. (2021). Machine learning algorithms in user authentication schemes. In *Proceedings of the International Conference on Electrical, Computer and Energy Technologies (ICECET)*. https://arxiv.org/pdf/2110.07826
14. Ackerson, J. M., Dave, R., & Seliya, N. (2021). Applications of recurrent neural network for biometric authentication & anomaly detection. *Information, 12*(7), 272. https://www.mdpi.com/2078-2489/12/7/272
15. Visa Navigate. (2025). Visa boosts AI capabilities to further reduce fraud. *Visa Navigate*. https://navigate.visa.com/europe/security/visa-boosts-ai-capabilities-to-further-reduce-fraud/
16. Liang, L.-H. (2025). Mastercard integrates Feedzai behavioral biometrics for fraud protection. *Biometrics News*. https://www.biometricupdate.com/202502/mastercard-integrates-feedzai-behavioral-biometrics-for-fraud-protection
17. PYMNTS. (2025). Banks, merchants turn to behavioral biometrics to fight fraud. https://www.pymnts.com/partnerships/2025/synchrony-teams-with-adobe-commerce-to-offer-flexible-financing/
18. Asmar, M., & Tuqan, A. (2023). Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon, 10*(1), e37571. https://doi.org/10.1016/j.heliyon.2024.e37571
19. Lim, B., Huerta, R., Sotelo, A., Quintela, A., & Kumar, P. (2025). EXPLICATE: Enhancing phishing detection through explainable AI and LLM-powered interpretability. *ResearchGate*. https://www.researchgate.net/publication/390248105_...
20. Evans, K., Abuadbba, A., Wu, T., Moore, K., Ahmed, M., Pogrebna, G., Nepal, S., & Johnstone, M. (2022). RAIDER: Reinforcement-aided spear phishing detector. In *Proceedings of the International Conference on Network and System Security*. https://www.researchgate.net/publication/366052395_...
21. Kothandapani, H. P. (2024). Automating financial compliance with AI: A new era in regulatory technology (RegTech). *International Journal of Science and Research Archive*. https://ijsra.net/sites/default/files/IJSRA-2024-0040.pdf
22. Agarwal, R., Kremer, A., Kristensen, I., & Luget, A. (2024). How generative AI can help banks manage risk and compliance. *McKinsey & Company*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/how-generative-ai-can-help-banks-manage-risk-and-compliance
23. KPMG. (2024). KPMG інтегрує штучний інтелект у власну аудиторську платформу KPMG Clara. https://kpmg.com/ua/uk/home/media/press-releases/2024/09/kpmg-intehruye-ai-u-vlasnu-audytorsku-platformu-kpmg-clara.html
24. Smirnov, O. A., Konstantynova, L. V., Konoplitska-Slobodeniuk, O. K., Kozirova, N. V., Yakymenko, N. M., Dorenskyi, O. P., & Buravchenko, K. O. (2025). Exploring artificial intelligence tools for working with

databases and data analysis. *Cybersecurity: Education, Science, Technology, 3*(27), 429–448. https://doi.org/10.28925/2663-4023.2025.27.763

25. Smirnova, T. V., Konoplitska-Slobodeniuk, O. K., Buravchenko, K. O., Smirnov, S. A., Kravchuk, O. V., Kozirova, N. L., & Smirnov, O. A. (2024). Research on cybersecurity technologies for cloud services: IaaS, PaaS, and SaaS. *Cybersecurity: Education, Science, Technology, 4*(24), 6–27. https://doi.org/10.28925/2663-4023.2024.24.627
26. Kuznetsov, O., Smirnov, O., Mormul, M., Kotukh, Y., & Zvieriev, V. (2024). Comparative research on cryptocurrency efficiency: An objective analysis of key metrics. *International Journal of Computing, 23*(4), 563–573. https://doi.org/10.47839/ijc.23.4.3755
27. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Smirnov, O., & Kostenko, V. (2024). Blockchain applications in metaverse environments: New horizons. In *Advanced Metaverse Wireless Communication Systems* (pp. 255–293). https://doi.org/10.1049/PBTE112E_ch10
28. Kuznetsov, O., Frontoni, E., Chevardin, V., Smirnov, O., & Imoize, A. L. (2024). Advancing metaverse security with cryptographic innovations. In *Advanced Metaverse Wireless Communication Systems* (pp. 351–386). https://doi.org/10.1049/PBTE112E_ch13

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Pavlo Usik
Doctor of Philosophy (PhD),
Senior Lecturer of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0002-3268-342X
usikps@kntu.kr.ua

Tetiana Smirnova
Candidate of Science (Engineering),
Senior Lecturer, Department of Automation of Production Processes
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID:0000-0001-6896-0612
sm.tetyana.gmail.com

Kostiantyn Buravchenko
Candidate of Technical Sciences, Associate Professor,
Associate Professor of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-6195-7533
buravchenkok@gmail.com

Oleksii Smirnov
Doctor of Technical Sciences, Professor,
Head of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0001-9543-874X
dr.smirnovoa@gmail.com

Oleksandr Ulichev
Candidate of Technical Sciences,
Senior Lecturer of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0003-3736-9613
askin79@gmail.com

Serhii Smirnov
Candidate of Science (Engineering), associate professor, associate professor of Cybersecurity & Software Academic Department
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine
ORCID ID: 0000-0002-7649-7442
smirnov.ser.81@gmail.com

RESEARCH ON CYBERSECURITY TECHNOLOGIES FOR BANKING SYSTEMS USING ARTIFICIAL INTELLIGENCE

Abstract. The article explores the application of modern artificial intelligence (AI) technologies as a tool for ensuring cybersecurity in banking systems. Amid the growing number of sophisticated cyberattacks, traditional protection methods are no longer sufficient to provide an adequate level of security, making the implementation of intelligent systems capable of automatically analyzing large volumes of data and promptly responding to threats highly relevant. The study examines key approaches to integrating AI into the processes of detecting anomalies and cybercrimes in the banking sector. It analyzes core AI technologies used for real-time fraud detection, behavioral biometrics, countering phishing attacks, and automating compliance and audit processes. Based on practical case studies, the high efficiency of AI in enhancing threat detection accuracy, reducing response times, and minimizing false positives is demonstrated. Particular attention is given to the adaptability and self-learning capabilities of intelligent security systems in a dynamic threat environment. The advantages of integrating AI into the banking security infrastructure are highlighted, alongside the main challenges associated with implementing such solutions. The research results confirm the promising potential of AI as an effective cybersecurity tool in banking systems.

Keywords: cybersecurity; banking systems; artificial intelligence; machine learning; information security; fraud detection; behavioral biometrics; phishing; compliance.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Ovcharenko, T. (2024). Trends in the development and use of artificial intelligence in the banking sector. *Economy and Society*. https://doi.org/10.32782/2524-0072/2024-67-44
2. Kholiavko, N., Sadchykova, I., & Kolotok, M. (2023). Directions of use of artificial intelligence in banking institutions. *Problems and Prospects of Economics and Management*. https://ir.stu.cn.ua/handle/123456789/28945
3. Danik, N., & Torlopov, A. (2024). Introducing artificial intelligence into banking: A revolution in service and security. *International Science Journal of Management Economics & Finance*. https://www.researchgate.net/publication/392319259_...
4. Sharov, S. (2023). Current state of artificial intelligence development and its applications. *Ukrainian Studies in the European Context*. http://obrii.org.ua/usec/storage/conference/zb_vol6_2023.pdf
5. BDO Global. (2024). The role of artificial intelligence in cybersecurity: Prediction and prevention of attacks. https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks
6. Willie, A. (2025). The evolution of AI in cybersecurity: From rule-based systems to generative AI. *ResearchGate*. https://www.researchgate.net/publication/388930668_...
7. Adhikari, P., Hamal, P., & Baidoo, F. (2024). Artificial intelligence in fraud detection: Revolutionizing financial security. *International Journal of Science and Research Archive*. https://ijsra.net/content/artificial-intelligence-fraud-detection-revolutionizing-financial-security
8. Kokkalakonda, N. K. (2022). AI-powered fraud detection in banking: Enhancing security with machine learning algorithms. *ResearchGate*. https://www.researchgate.net/publication/390357575_...
9. Tambi, V. K. (2022). AI-powered fraud detection in real-time financial transactions. *International Journal of Research in Electronics and Computer Engineering*. https://philpapers.org/archive/VARAFD-2.pdf
10. Cognizant. (2019). Advanced AI/ML solution detects check fraud for a global bank. https://www.cognizant.com/en_us/case-studies/documents/ai-driven-solution-reduces-fraud-risk-for-bank-codex3688.pdf
11. Visa. (n.d.). Visa announces generative AI-powered fraud solution to combat account attacks. *Visa Official Website*. https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.20661.html
12. Kokal, S., Vanamala, M., & Dave, R. (2023). Deep learning and machine learning, better together than apart: A review on biometrics mobile authentication. *Journal of Cybersecurity and Privacy*, *3*(2), 13. https://www.mdpi.com/2624-800X/3/2/13
13. Pryor, L., Dave, R., Seliya, J., & Boone, E. S. (2021). Machine learning algorithms in user authentication schemes. In *Proceedings of the International Conference on Electrical, Computer and Energy Technologies (ICECET)*. https://arxiv.org/pdf/2110.07826
14. Ackerson, J. M., Dave, R., & Seliya, N. (2021). Applications of recurrent neural network for biometric authentication & anomaly detection. *Information, 12*(7), 272. https://www.mdpi.com/2078-2489/12/7/272
15. Visa Navigate. (2025). Visa boosts AI capabilities to further reduce fraud. *Visa Navigate*. https://navigate.visa.com/europe/security/visa-boosts-ai-capabilities-to-further-reduce-fraud/
16. Liang, L.-H. (2025). Mastercard integrates Feedzai behavioral biometrics for fraud protection. *Biometrics News*. https://www.biometricupdate.com/202502/mastercard-integrates-feedzai-behavioral-biometrics-for-fraud-protection
17. PYMNTS. (2025). Banks, merchants turn to behavioral biometrics to fight fraud. https://www.pymnts.com/partnerships/2025/synchrony-teams-with-adobe-commerce-to-offer-flexible-financing/
18. Asmar, M., & Tuqan, A. (2023). Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon, 10*(1), e37571. https://doi.org/10.1016/j.heliyon.2024.e37571
19. Lim, B., Huerta, R., Sotelo, A., Quintela, A., & Kumar, P. (2025). EXPLICATE: Enhancing phishing detection through explainable AI and LLM-powered interpretability. *ResearchGate*. https://www.researchgate.net/publication/390248105_...
20. Evans, K., Abuadbba, A., Wu, T., Moore, K., Ahmed, M., Pogrebna, G., Nepal, S., & Johnstone, M. (2022). RAIDER: Reinforcement-aided spear phishing detector. In *Proceedings of the International Conference on Network and System Security*. https://www.researchgate.net/publication/366052395_...

21. Kothandapani, H. P. (2024). Automating financial compliance with AI: A new era in regulatory technology (RegTech). *International Journal of Science and Research Archive*. https://ijsra.net/sites/default/files/IJSRA-2024-0040.pdf
22. Agarwal, R., Kremer, A., Kristensen, I., & Luget, A. (2024). How generative AI can help banks manage risk and compliance. *McKinsey & Company*. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/how-generative-ai-can-help-banks-manage-risk-and-compliance
23. KPMG. (2024). KPMG інтегрує штучний інтелект у власну аудиторську платформу KPMG Clara. https://kpmg.com/ua/uk/home/media/press-releases/2024/09/kpmg-intehruye-ai-u-vlasnu-audytorsku-platformu-kpmg-clara.html
24. Smirnov, O. A., Konstantynova, L. V., Konoplitska-Slobodeniuk, O. K., Kozirova, N. V., Yakymenko, N. M., Dorenskyi, O. P., & Buravchenko, K. O. (2025). Exploring artificial intelligence tools for working with databases and data analysis. *Cybersecurity: Education, Science, Technology, 3*(27), 429–448. https://doi.org/10.28925/2663-4023.2025.27.763
25. Smirnova, T. V., Konoplitska-Slobodeniuk, O. K., Buravchenko, K. O., Smirnov, S. A., Kravchuk, O. V., Kozirova, N. L., & Smirnov, O. A. (2024). Research on cybersecurity technologies for cloud services: IaaS, PaaS, and SaaS. *Cybersecurity: Education, Science, Technology*, *4*(24), 6–27. https://doi.org/10.28925/2663-4023.2024.24.627
26. Kuznetsov, O., Smirnov, O., Mormul, M., Kotukh, Y., & Zvieriev, V. (2024). Comparative research on cryptocurrency efficiency: An objective analysis of key metrics. *International Journal of Computing, 23*(4), 563–573. https://doi.org/10.47839/ijc.23.4.3755
27. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Smirnov, O., & Kostenko, V. (2024). Blockchain applications in metaverse environments: New horizons. In *Advanced Metaverse Wireless Communication Systems* (pp. 255–293). https://doi.org/10.1049/PBTE112E_ch10
28. Kuznetsov, O., Frontoni, E., Chevardin, V., Smirnov, O., & Imoize, A. L. (2024). Advancing metaverse security with cryptographic innovations. In *Advanced Metaverse Wireless Communication Systems* (pp. 351–386). https://doi.org/10.1049/PBTE112E_ch13