DOI: https://doi.org/10.25140/2411-5215-2024-1(37)-310-328
УДК 336.7:004:316.772.5
JEL classification: G10, G18, E44, O32

Марина Валеріївна Рябокінь
кандидат економічних наук, доцент,
проректор з навчально-методичної роботи
Київський інститут бізнесу та технологій (Київ, Україна)
E-mail: marina.riabokin@gmail.com. **ORCID:** https://orcid.org/0000-0002-6724-9498
ResearcherID: AGZ-6858-2022. **Scopus:** 59171974600

Євген Володимирович Котух
кандидат технічних наук, доцент
Національний технічний університет «Дніпровська політехніка» (Дніпро, Україна)
E-mail: yevgenkotukh@gmail.com. **ORCID:** https://orcid.org/0000-0003-4997-620X
SCOPUS ID: 57215274481. **ResearcherID:** 15779883

Олексій Ігорович Папилев
технічний продакт овнер, ТОВ «Лайфселл» (Київ, Україна)
E-mail: alex.papylev@gmail.com. **ORCID:** https://orcid.org/0009-0009-9806-8743

ВПЛИВ ТЕХНОЛОГІЇ DEEPFAKE НА FINTECH СЕКТОР: ПОТОЧНИЙ СТАН В УКРАЇНІ ТА СТРАТЕГІЇ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

У статті розглянуто вплив технології deepfake на FinTech сектор України та наведено стратегії запобігання кібершахрайству. З метою визначення рівня готовності українського FinTech сектору до викликів, пов'язаних з deepfake, було проведено опитування, яке виявило недостатню готовність учасників ринку до подібного роду ризиків. Особливу увагу приділено методам, які дозволяють зловмисникам імітувати клієнтів та фінансових посадових осіб для доступу до конфіденційної інформації та здійснення шахрайських транзакцій. У статті наведено аналіз найбільш ефективних стратегій запобігання таким загрозам, включаючи впровадження технологій виявлення deepfake, покращення цифрової гігієни користувачів та удосконалення правових і регуляторних рамок.

Ключові слова: *технологія deepfake; інновації; фінтех; кіберзлочинність; штучний інтелект; шахрайство.*
Рис.: 9. Табл.: 2. Бібл.: 20.

Постановка проблеми. Будь-які інновації завжди неоднозначно сприймаються суспільством, адже вони спричиняють зміни у звичних процесах та загострюють відчуття невизначеності у користувачів. Інновації у FinTech секторі не є винятком, адже клієнти більше звикли довіряти традиційним фінансовим установам, які мають багаторічну репутацію. І хоча FinTech інновації забезпечують зручність та пришвидшують здійснення фінансових операцій, вони також відкривають нові можливості для зловживань і шахрайства.

Одна з таких загроз – технологія deepfake. Вона може стати причиною хаосу та зловживань не лише у сфері FinTech, але й у кількох інших галузях, якщо залишити її без контролю.

Deepfake в галузі FinTech, з їхньою дивовижною здатністю переконливо відтворювати автентичну взаємодію, підривають довіру користувачів до цифрових фінансових систем. Масштаб цієї екзистенційної загрози підкреслюється відсутністю комплексних гарантій і неадекватністю механізмів виявлення. Майбутнє FinTech знаходиться на хиткому роздоріжжі, де ризики deepfakes є значною перешкодою для довіри та надійності фінансових послуг.

Зростання deepfake та генеративного ШІ становить собою серйозний виклик, до якого потрібно бути готовим учасникам FinTech ринку та застосовувати превентивну стратегію.

Відповідно до нещодавнього звіту платформи перевірки особи Sumsub, у 2023 році кількість інцидентів deepfake у секторі фінансових технологій зросла на 700 % порівняно з попереднім роком.

Аналіз останніх досліджень і публікацій. У статті [3] Т. Нгуен та співавтори надають огляд технологій глибокого навчання, що використовуються для створення та виявлення deepfakes, включаючи певні приклади застосування у фінансовому секторі. І. Гудфеллоу та співавтори у [5] розкривають алгоритми роботи Generative Adversarial Networks (GANs) - базової технології, що використовується deepfakes. П. Коршунов [10] та інші роблять оцінку загроз, які представляють deepfakes для систем розпізнавання облич, зокрема використовуючи сценарії притаманні фінансовому сектору. М. Вестерлунд [18] пропонує огляд розвитку технології deepfakes і її потенційних загроз у різних секторах, включаючи фінансовий. С. Агарвал та співавтори у [13] дослідили методи захисту від deepfakes, які можуть бути корисним для фінансового сектору. Ю. Мірскі та інші у [11] пропонують докладний огляд методів створення та виявлення deepfakes, з оцінкою впливу на різні галузі, включаючи фінансову. Р. Чесні та співавтори [2] обговорюють правові та етичні наслідки deepfakes, які можуть вплинути на фінансовий сектор через загрози приватності та безпеки. Дж. Чжан та колеги у [19] пропонують аналіз ризиків та заходів зменшення впливу deepfakes у фінансовому секторі. Брати Гупта у [8] також приділяють увагу більш систематичному огляду впливу deepfakes на фінансові ринки, включаючи потенційні загрози та стратегії їхнього усунення.

Виділення недосліджених частин загальної проблеми. Проблема впливу технології deepfake та стратегії запобігання кіберзлочинності у FinTech секторі є малодослідженою в українському науковому просторі та потребує глибшого дослідження.

Формулювання цілей статті (постановка завдання). Метою статті є визначення сутності та способів, якими deepfakes можуть становити значну загрозу індустрії FinTech, аналіз поточного стану готовності українського FinTech сектору до протидії deepfake-шахрайству та визначення ефективних стратегій запобігання/мінімізації ризиків deepfake у FinTech сфері.

Виклад основного матеріалу дослідження. Deepfake – це слово, утворене від «глибоке навчання» та «підробка». Deepfake – це методика синтезу автентичної інформації щодо людини, яка базується на штучному інтелекті.

Найчастіше використовується зловмисниками для поєднання і накладення одних зображень та відео на інші зображення або відеоролики. Результати належать до гіперреалістичних відео чи аудіозаписів, що створюються за допомогою штучного інтелекту (ШІ). Ці ілюзії, створені ШІ, настільки переконливі, що можуть імітувати вигляд та голоси людей з дивною точністю.

У міру того, як deepfake стає більш вдосконаленим та доступним, фінансові установи стикаються з новими загрозами шахрайства, які ставлять під сумнів основи довіри, безпеки та конфіденційності даних у секторі, від онлайн-банкінгу до комунікацій.

Потенціал deepfake для імітації клієнтів, чиновників чи будь-якої ключової особи у фінансових транзакціях відкриває «скриньку Пандори» з можливостями шахрайства.

В основі технології deepfake лежить перетин ШІ та машинного навчання. Інакше кажучи, deepfakes створюються за допомогою складних алгоритмів, які вчаться на величезних обсягах даних, включаючи зображення, відео та аудіозаписи реальних людей. Ці алгоритми аналізують тонкощі людських виразів обличчя, жестів та мовленнєвих моделей. З часом вони стають вправними у синтезі контенту, що імітує ці людські характеристики, що призводить до відео або аудіозаписів, які виглядають абсолютно реальними [15].

Шахрайство у фінансовій сфері вже не нове явище: воно таке ж старе, як сама галузь [20]. Традиційно фінансове шахрайство охоплює ряд обманних практик, від підроблення чеків до крадіжки ідентичності, спрямованих на нелегальне отримання грошей або майна. Однак цифровізація призвела до виникнення вдосконалених тактик кібершахрайства – і технологія deepfake є ще одним потужним інструментом в арсеналі шахраїв.

Технологія deepfake збільшує загрозу шахрайства, дозволяючи зловмисникам створювати дуже переконливі фальшиві аудіо та відеозаписи. Ці записи можуть бути використані для імітації ключових осіб у фінансових транзакціях, таких як банківські працівники, керівники компаній або самі клієнти.

GSMA провели опитування по всьому світу стосовно цифрової гігієни та усвідомлення захисту власних даних. Результати опитування наведені на табл. 1.

З наведених даних видно, що не зважаючи на те, що зйомка та зберігання фотографій і відео є популярними у більшості країнах, користувачі смартфонів також часто використовують свої телефони для взаємодії з банківськими рахунками. Респонденти з Азії, Африки та Латинської Америки частіше використовують свої телефони для роботи.

Поліція Сінгапуру (SPF) опублікували свій звіт про шахрайство та кіберзлочинність за 2023 рік, у якому наведені ключові тенденції, пов’язані з шахрайством та кіберзлочинністю за минулий рік (рис. 1).

Таблиця 1

Результати опитування GSMA щодо використання респондентами можливостей смартфонів, %

Дія	США	Велика Британія	Іспанія	Франція	Німеччина	Японія	Корея	Індія	Китай	Бразилія	ПАР
Багато знімаю і зберігаю фотографії та відео	67	73	75	74	55	52	65	72	75	72	72
Взаємодію зі своїм банківським рахунком або іншими фінансовими інструментами	63	78	69	62	46	48	50	66	70	73	78
Зберігаю платіжну інформацію, що використовується для покупки товарів онлайн або в магазинах	57	69	62	49	45	40	57	65	61	60	55
Зберігаю паролі та/або PIN-коди для різних облікових записів	45	46	47	44	41	39	47	58	56	57	49
Зберігаю медичну інформацію або інформацію про здоров'я	42	35	30	30	30	33	30	47	51	41	49
Використовую телефон для роботи	32	30	32	29	32	31	28	36	41	35	28
Зберігаю паспорт, водійські права або іншу конфіденційну інформацію	30	34	25	33	23	27	29	35	39	34	30
Зберігаю інформацію з вище переліченого	30	32	27	26	24	25	25	32	32	28	25
Нічого з вищепереліченого	7	4	5	6	9	7	5	6	6	4	6

Джерело: [6].

Кількість випадків шахрайства та кіберзлочинності за даними SPF зросла на 49,6 % до 50 376 у 2023 році порівняно з 33 669 випадками у 2022 році. Шахрайство (включаючи шахрайство зі шкідливим програмним забезпеченням) становило 92,4 % випадків у 2023 році, причому загальна кількість випадків шахрайства зросла на 46,8 % до 46 563 у 2023 році з 31 728 випадків у 2022 році. Шахрайство з працевлаштуванням, шахрайство з електронною комерцією, фальшиві дзвінки друзів, шахрайство з фішингом та інвестиційне шахрайство також залишаються п’ятіркою найпоширеніших видів шахрайства у 2023 році [16].

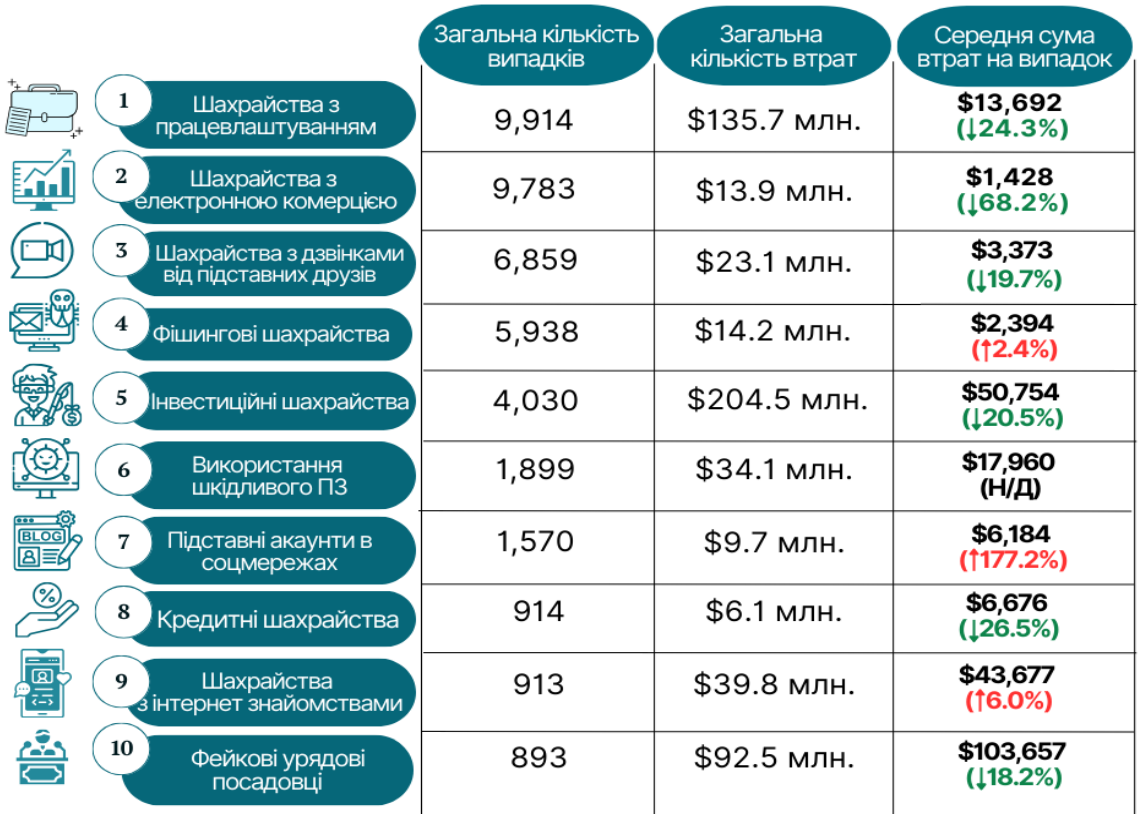

Рис. 1. Найпоширеніші шахрайства, які були зареєстровані в Сінгапурі у 2023 році

Джерело: [16].

Довіра є дуже важливим елементом відносин фінансової установи та клієнта, адже клієнти довіряють свої особисті та фінансові дані установам з очікуванням максимальної конфіденційності та безпеки. deepfakes вносять розлад у цей зв'язок. Якщо клієнт не може бути впевненим, що працівник фінустанови, з яким він спілкується відразу на відеодзвінку, є справжнім, або якщо установа не може довіряти автентичності інструкцій, отриманих від людини, яка, мабуть, є високопоставленим керівником, то сама основа довіри починає руйнуватися. Зниження довіри може мати довготривалі наслідки та стримувати клієнтів від співпраці з цифровими банківськими та фінансовими послугами або підривати довіру інвесторів.

Технології deepfakes можуть негативно впливати на індустрію FinTech таким чином (рис. 2):

1. Крадіжка ідентичності та шахрайські транзакції. Технологія deepfake дозволяє зловмисникам створювати дуже переконливі фальшиві відео або аудіозаписи осіб. У контексті FinTech це може бути використано для підробки клієнтів або навіть вищих керівників у фінансових установах. За допомогою цих відео зловмисники можуть потенційно отримати доступ до конфіденційної інформації, маніпулювати фінансовими транзакціями або авторизовувати шахрайські платежі.

Рис. 2. Вплив технологій deepfakes на FinTech сектор

Джерело: складено авторами за матеріалами [12].

2. Атаки з використанням соціальної інженерії. Технологія deepfakes використовується для підвищення ефективності атак з використанням соціальної інженерії. Все, що ще вчора шахраї робили використовуючи велику кількість різноманітних рішень, сьогодні втілюється в життя завдяки технологічній еволюції «human enginering» та автоматизується за допомогою генеративних моделей. Шляхом створення фальшивих відео або аудіозаписів довірених осіб шахраї можуть ввести в оману працівників або клієнтів, щоб вони розкрили конфіденційну інформацію або виконали несанкціоновані дії. Це може призвести до витоку даних, фінансових втрат або навіть зміни репутації для фінансових установ.

3. Маніпулювання ринком. У світі фінансів довіра та авторитет надзвичайно важливі. deepfakes можуть підірвати цю довіру, поширюючи недостовірну інформацію або маніпулюючи настроями на ринку. Наприклад, фальшиві відео впливових осіб, які роблять недостовірні заяви про акції або криптовалюти, можуть спричинити панічний продаж або штучні коливання цін, що призведе до значних фінансових втрат для інвесторів.

4. Фальшиві докази в судових процесах. Технологія deepfakes може негативно впливати на судові процеси в індустрії FinTech. Шахраї можуть використовувати підроблені аудіо або відеодокази, щоб підтримати хибні твердження або анулювати законні транзакції. Це може ускладнювати розслідування, подовжувати судові процеси і, в кінцевому підсумку, підривати цілісність правової системи.

5. Фішинг та атаки з використанням шкідливого програмного забезпечення. Deepfakes також можуть бути використані в атаках фішингу та шкідливого програмного забезпечення, які спрямовані на фізичних або юридичних осіб у FinTech секторі. Шляхом підробки довірених сутностей через фальшиві відео або аудіозаписи кіберзлочинці можуть заманювати жертв до клікання на шкідливі посилання, завантаження файлів з вірусами або надання конфіденційної інформації. Це може призвести до витоку даних, фінансової крадіжки або компрометації систем.

6. «Підрив» репутації. Збереження гарної репутації має вирішальне значення для приваблення клієнтів та інвесторів для FinTech компаній. Однак технологія deepfakes становить серйозну загрозу збереженню позитивної репутації. Один переконливий відеоролик, у якому генеральний директор підтримує неетичні практики або робить образливі висловлювання, може завдати величезної шкоди репутації всієї організації, призводячи до втрати довіри та авторитету на ринку.

7. Виклики відповідності регулятивним вимогам. Зростання deepfakes створює виклики відповідності регулятивним вимогам для індустрії FinTech. Регуляторні органи можуть мати складнощі у виявленні та запобіганні поширенню шахрайського вмісту deepfakes, що призводить до прогалин у регулятивних рамках. До того ж використання deepfake у фінансових злочинах може змусити регуляторів запроваджувати більш суворі правила та вимоги відповідності, що збільшує операційне навантаження для фінансових установ.

8. Зниження довіри до цифрових ідентичностей. У цифровому світі довіра до цифрових ідентичностей є вирішальною. Однак поширення технології deepfakes загрожує цій довірі. Зі зростанням складності й поширенням deepfakes люди можуть стати більш скептичними до цифрових комунікацій та транзакцій, що призведе до неприйняття FinTech-рішень та стримуванню темпів розвитку галузі [1].

З метою визначення поточного стану готовності українського FinTech сектору до deepfakes нами було ініційовано та, за підтримки Асоціації фінтех та інноваційних компаній (далі – UAFIC), проведено опитування. Опитування мало на меті визначити рівень розуміння учасників FinTech-ринку сутності, каналів впливу та потенційних ризиків deepfakes на їхні бізнес-процеси.

У процесі опитування ми попросили респондентів проранжувати ризики deepfakes, які описані вище, в порядку їх потенційної загрози для діяльності FinTech сектору (рис. 3). Результати підтвердили гіпотезу, що найбільшими ризиками респонденти вважають репутаційні ризики та ризики комплаєнсу. Очевидно, що ці ризики можна назвати стратегічними, бо їх вплив має значні негативні перспективи для будь-якого підприємства саме у часі. Фішинг, вразливості цифрової ідентичності, атаки, крадіжки, фальшиві транзакції та маніпулювання ринком – це прийоми та методи, що підтверджують тактичні

ризики середньої та короткострокової перспективи та мають менш негативний вплив і наслідки, але зазначаються респондентами як актуальні та релевантні. Українське правосуддя не має прецедентів зі створенням та/або маніпулюванням фальшивими доказами в судових процесах, але цей ризик також з'явився в результаті обробки зібраних даних.

Рис. 3. Ранжування ризиків deepfakes за рівнем їх потенційної загрози діяльності FinTech сектору України

Джерело: складено авторами за результатами проведеного опитування.

Очевидним є той факт, що кожен користувач цифрових сервісів має дотримуватись правил кібергігієни та з обережністю використовувати програмні додатки, що збирають біометричні дані, особливо в соціальних мережах. 83 % опитаних респондентів підтвердили, що вони постійно використовують біометричну автентифікацію (обличчя, голос чи відбиток пальця), 6 % – використовували, але відмовились. Зазначимо, що будь-який biometric fingerprint (біометричний слід, біометричні дані) зберігається у захищеній області пам'яті смартфона з обмеженими можливостями доступу для зловмисників. Процес порівняння «обличчя» із шаблоном в процесі біометричної аутентифікації також відбувається у захищеному режимі. З погляду клієнт-серверної архітектури «цифровий ключ» обличчя не передається у відкритому вигляді, використання асиметричної криптографії дозволяє використовувати лише публічний ключ, а приватна частина ключової пари знаходиться виключно на смартфоні в коді ОС. Тобто за умов використання біометричної автентифікації на смартфоні у якомусь фішинговому додатку, неможливо перевикористати «відбиток» у додатку банку. Аналогічна ситуація використанням додатків у соціальних мережах, які створюють нові образи з використанням ваших біометричних даних (фото, відео) (рис. 4).

Ці показники свідчать про доволі низьке усвідомлення користувачами потенційних ризиків deepfake-шахрайств з використанням їхніх персональних даних. При цьому 94 % опитаних представників FinTech-ринку знають, що таке deepfakes, проте, лише 45 % відповіли, що вважають це потенційною загрозою для їхнього бізнесу. На питання щодо потенційного рівня ризику deepfakes у FinTech секторі, за п'ятибальною шкалою, ми отримали середнє значення на рівні 4,5 бала.

Рис. 4. Поточний стан використання біометричної автентифікації фахівцями FinTech

Джерело: складено авторами за результатами проведеного опитування.

Респонденти засвідчили, що використовують у своїй діяльності відповідні заходи безпеки та ідентифікації клієнта (рис. 5).

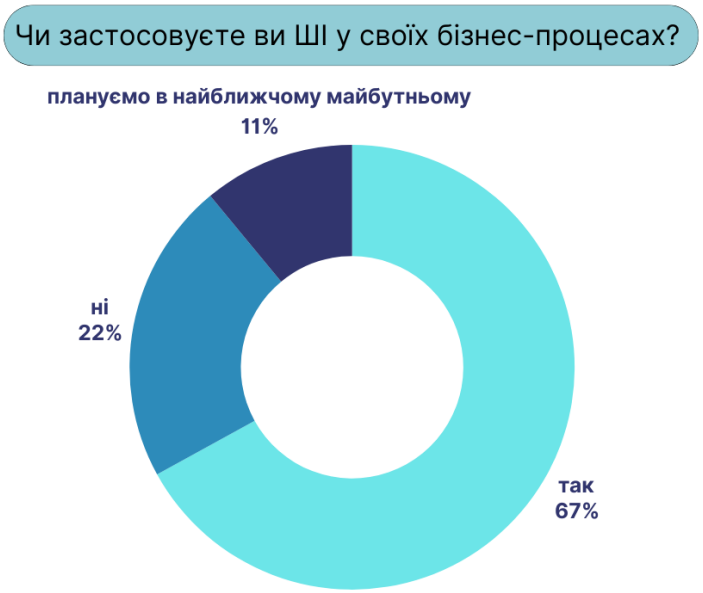

Рис. 5. Поточний стан використання технологій ШІ фахівцями FinTech

Джерело: складено авторами за результатами проведеного опитування.

Для мінімізації ризиків deepfake-шахрайства необхідний багатокомпонентний підхід до кіберзахисту та захисту даних. Цей підхід повинен бути активним, динамічним і охоплювати комбінацію технологій, відповідність регуляторним вимогам, постійний моніторинг та усвідомленість спільноти [15].

Рис. 6. Поточний стан використання фахівцями FinTech додатків, які створюють нові образи з використанням біометричних даних
Джерело: складено авторами за результатами проведеного опитування.

При ідентифікації клієнта FinTech компанії можуть використовувати різноманітні заходи, які мають на меті забезпечення цифрової безпеки. Опитані представники FinTech сектору найчастіше у своїй діяльності використовують багатофакторну автентифікацію – 74 %, та біометрію обличчя – 68 % (рис. 7).

Рис. 7. Заходи безпеки та ідентифікації, які використовують фахівці фінтеху
Джерело: складено авторами за результатами проведеного опитування.

При поєднанні кількох інструментів ідентифікації клієнтів суттєво підвищується ефективність заходів безпеки FinTech сервісів. За результатами опитування встановлено, що 67 % FinTech-компаній у своїй діяльності використовують більше ніж один інструмент ідентифікації клієнта (рис. 8).

Рис. 8. Кількість інструментів, які використовують фахівці FinTech для ідентифікації клієнта

Джерело: складено авторами за результатами проведеного опитування.

Майже 70 % опитаних представників FinTech-сектору констатували, що їхні компанії мають дуже низький та низький рівень готовності до викликів deepfake-шахрайства. Проте, ряд компаній працюють над створенням стратегій запобігання таким шахрайствам (44 %), деякі вже її мають (17 %), а 39 % - не вбачають в цьому потреби сьогодні (рис. 9).

Рис. 9. Інформація щодо наявності/відсутності стратегій запобігання шахрайству у вітчизняних FinTech компаніях

Джерело: складено авторами за результатами проведеного опитування.

Опитані учасники FinTech-сектору зазначили, що обов'язковими заходами в контексті запобігання deepfakes у їхній діяльності мають бути:

- багатофакторна автентифікація;
- розширення переліку цифрових навичок;
- внутрішня корпоративна безпека;
- створені рекомендації для запобігання;
- моніторинг транзакцій та співпраця з правоохоронними органами.

З метою пом'якшення ризиків deepfake-шахрайства доцільно використовувати різноманітні комбінації інструментів та застосовувати різні заходи безпеки, вибір яких залежить від специфіки діяльності фінансової установи. До таких інструментів (заходів) відносяться:

1. Технологічні рішення та інновації:

- виявлення deepfake за допомогою ШІ та машинного навчання. Використовуючи ті ж технології, які дозволяють створювати deepfake, фінансові установи можуть запровадити вдосконалені алгоритми ШІ, призначені для виявлення аномалій і неузгодженостей у звукових та відеофайлах, які можуть вказувати на deepfake. Ці інструменти аналізують різні аспекти, такі як вираз обличчя, рухи губ та мовні моделі, для виявлення розбіжностей, які важко помітити людині;
- blockchain для цифрової верифікації. Впровадження технології блокчейну може покращити цілісність цифрових ідентичностей та транзакцій. Створюючи незмінний реєстр для перевірки автентичності документів та комунікацій, блокчейн може забезпечити надійний захист від маніпуляцій інформацією;
- покращена біометрична верифікація. Розробка більш удосконалених методів біометричної верифікації, що здатні виявляти «живість» суб'єкта, може допомогти протидіяти імітаціям deepfake. Техніки, такі як тривимірне картографування обличчя, розпізнавання райдужки та аналіз текстури шкіри, можуть додавати шари безпеки, які більш стійкі до технології deepfake.

2. Посилення політик та протоколів:

- регулярні аудити безпеки. Проведення ретельних та регулярних аудитів систем безпеки та протоколів гарантує, що вразливості виявляються та вирішуються негайно. Ці аудити повинні включати оцінку можливих загроз deepfake та ефективності інструментів їх виявлення.
- навчання співробітників. Обізнаність співробітників щодо природи та ризиків deepfake є ключовим. Програми навчання повинні включати виявлення ознак спроб deepfake, протоколи перевірки інформації та повідомлення про підозрілі дії;
- навчання клієнтів. Інформування клієнтів про потенційні ризики deepfake, надання порад щодо захисту їх облікових записів та особистої інформації може надати їм можливість бути більш обачними та обережними у своїх взаємодіях.

3. Регуляторна/галузева співпраця:

- обмін інформацією. Фінансові установи можуть скористатися обміном інформацією та найкращими практиками, що стосуються виявлення та запобігання deepfake. Спільні зусилля, через асоціації галузі або партнерства, можуть покращити загальну безпеку [14];
- просування регуляторних стандартів. Співпраця з політиками для розробки регуляцій та стандартів, спеціально призначених для технології deepfake, може допомогти встановити єдиний підхід до мінімізації її ризиків. GSMA активно працює над стратегією запобігання шахрайству у світі мобільного зв'язку [7].

4. *Етичні питання та приватність: п*ри реалізації цих заходів надзвичайно важливо забезпечити баланс між підвищенням рівня безпеки та повагою до приватності та етичними моментами. Будь-які технологічні або процедурні зміни повинні відповідати законам приватності та поважати права окремих осіб.

Існує безліч стратегій, доступних для професіоналів у сфері фінансових технологій, залежно від їх екосистеми, обмежень і конкретних потреб. Кожна з цих стратегій має свої переваги та недоліки (табл. 2). Вибір стратегії залежить від багатьох факторів та умов діяльності кожного конкретного суб'єкта FinTech ринку. Поєднання кількох методів може запропонувати більш комплексний захист від технології deepfake, яка постійно розвивається.

Наразі, Україна приєдналась до глобальної співпраці щодо безпечного розвитку ШІ. Міністерство цифрової трансформації України разом з партнерами та профільними експертами розробили рекомендації з відповідального використання штучного інтелекту в медіа та працюють над рекомендаціями щодо запобігання проявам шахрайства із застосуванням ШІ.

Також важливо, щоб держава нормативно урегульовувала процеси запобігання deepfakes у FinTech секторі. Цю тезу підтверджують представники опитаних FinTech компаній – 89 % вважають, що держава обов'язково має долучатись до цих процесів та створювати відповідні регуляторні механізми.

Загалом фахівці українського FinTech сектору прогнозують, що у середньостроковій перспективі вітчизняний ринок очікують прояви ризиків deepfake-шахрайств. Тому, фінтехам варто заздалегідь готуватись до подібних кейсів, запроваджувати відповідні правила безпеки та рекомендації, у тому числі у співпраці з органами державної влади.

Таблиця 2

Стратегії запобігання/мінімізації ризиків deepfake у FinTech сфері

Стратегія	Суть	Переваги	Недоліки
1	2	3	4
Біометрія обличчя та 3D Liveness	Біометрія обличчя аналізує просторову глибину та унікальні риси обличчя користувача у порівнянні зі збереженими даними. Виявлення 3D Liveness вимагає від користувача виконання певних дій (моргання або посмішка) для підтвердження фізичної присутності під час автентифікації	✔ Посилює захист від маніпуляцій із відео deepfake за рахунок поєднання біометрії обличчя та 3D Liveness шляхом перевірки автентичності ідентифікаторів користувачів. ✔ Покращена взаємодія з користувачем: впровадження біометрії обличчя та 3D Liveness зменшує потребу в громіздких методах автентифікації, таких як введення довгих паролів або відповіді на контрольні запитання	✔ Може знадобитися значний обсяг пам’яті для даних користувача. ✔ Хибнопозитивні та хибнонегативні помилки: біометричні системи обличчя можуть час від часу генерувати хибні прийоми або відхилення, що призводить до неточної автентифікації.
Voice Liveness Detection	Технологія боротьби з шахрайством, яка перевіряє автентичність абонентів, аналізуючи їхні унікальні голосові шаблони. Ця технологія аналізує не лише зміст мови, але й висоту, тон та інші вокальні атрибути, унікальні для кожної людини.	✔ Підвищує безпеку фінансових операцій, що проводяться телефоном, як з погляду автентифікації клієнта, так і перевірки співробітників; ✔ Зменшує ризик використання згенерованих deepfake голосів для маніпулювання конфіденційною інформацією, доступу до зон обмеженого доступу або вчинення шахрайства	✔ Вимагає збору та підтримки голосових даних для кожного користувача, що може мати наслідки для зберігання та конфіденційності. ✔ Помилкові спрацьовування можуть призвести до непотрібної відмови в доступі або затримок в обробці запитів
Відбитки пальців пристрою та браузера	Відбитки пальців працюють шляхом збору кількох точок даних на пристрої користувача та атрибутах браузера, таких як операційна система, версія браузера, роздільна здатність екрана та встановлені плагіни. Потім ці атрибути об’єднуються в унікальний ідентифікатор – відбиток пальця.	✔ Покращує безпеку, додаючи додатковий рівень автентифікації, крім облікових даних. ✔ Запобігає атакам на захоплення облікових записів, виявляючи підозрілі пристрої, які мають доступ до облікових записів користувачів. ✔ Потенційно може виявити шаблони шахрайських пристроїв і застосувати профілактичні заходи.	✔ Може викликати занепокоєння щодо конфіденційності для клієнтів, оскільки він збирає дані про їхні пристрої та звички вебперегляду. ✔ Реалізація може вплинути на взаємодію з користувачем, оскільки деякі користувачі можуть сприймати відбитки пальців як нав’язливі.

Закінчення табл. 2

1	2	3	4
Виявлення емулятора та віртуальної машини	Технологія базується на аналізі багатьох атрибутів пристрою або середовища користувача, таких як характеристики апаратного забезпечення, запущені процеси та унікальні конфігурації системи. Потім ці деталі порівнюються з шаблонами, які зазвичай асоціюються з емульованими пристроями або віртуальними машинами. Якщо система виявить збіг, вона заблокує доступ або позначить транзакцію як потенційно зловмисну, спонукаючи до подальшого дослідження та виправлення.	✔ Покращений рівень безпеки за рахунок посилення загальної системи безпеки фінансових програм і служб від складних кібератак та deepfake. ✔ Протидія експлойтам API та внутрішнім загрозам. ✔ Покращена розвідка про загрози (використання технології дозволяє організації отримати більше розуміння нових загроз і тенденцій, допомагаючи їм випереджати кіберзлочинців).	✔ Помилкові спрацьовування (технологія може давати хибні спрацьовування, потенційно блокуючи законних користувачів або транзакції). ✔ Необхідні постійні оновлення, адже кіберзлочинці постійно розробляють нові методи та контрзаходи, щоб обійти системи виявлення.
KYC Solutions «Знай свого клієнта»	Ці рішення включають комплексний процес перевірки клієнтів, спрямований на мінімізацію ризику шахрайства з особистими даними та інших форм фінансових злочинів. Процеси KYC складаються з різних компонентів, таких як перевірка документів, біометрична автентифікація та оцінка ризиків, щоб забезпечити повне розуміння досвіду та легітимності клієнта	✔ Зводить до мінімуму ризик шахрайства зі штучною ідентифікацією та інших атак, керованих deepfake, захищаючи таким чином репутацію та фінансові активи організації ✔ Відповідність нормативним вимогам і найкращим галузевим практикам ✔ Підвищена довіра клієнтів завдяки надійним і безпечним процесам ідентифікації	✔ Може збільшити час адаптації та інвестиції ресурсів, потенційно вплинувши на взаємодію з користувачем ✔ Може викликати занепокоєння щодо конфіденційності клієнтів, оскільки їхня конфіденційна інформація збирається, обробляється та зберігається

Джерело: складено авторами за даними [17].

Деякі іноземні банки вже змінюють підходи до ідентифікації клієнтів [9]. Наприклад, Simmons Bank просить клієнтів фотографувати свої водійські права через банківський додаток, а потім робити селфі замість того, щоб завантажувати вже існуюче фото. Щоб уникнути ситуацій, коли вони підносять камери до екрана зі згенерованим штучним інтелектом візуальним зображенням чиїхось облич, додаток дає вказівки користувачам дивитися вліво, вправо, вгору або вниз, оскільки загальний AI deepfake не обов'язково буде готовий це зробити. так само [4].

Висновки та пропозиції. Треба зазначити, що технологія deepfakes становить багатогранну загрозу для індустрії FinTech, від крадіжки ідентичності та шахрайства до маніпулювання ринком та завдання шкоди репутації.

Для зменшення цих ризиків, фінансові установи повинні інвестувати в надійні заходи кібербезпеки, покращувати навчання співробітників з виявлення штучного контенту, співпрацювати з регуляторами для розробки ефективних методів протидії, та навчати клієнтів про ризики технології deepfakes.

Щоб протистояти викликам, пов'язаним з deepfakes в індустрії фінансових технологій важливим є єдиний фронт технологічних інновацій і надійних заходів безпеки. Оскільки FinTech-ландшафт продовжує розвиватися, проактивна позиція проти deepfakes стає надважливим для забезпечення стійкої довіри користувачів до цифрових фінансових екосистем. Лише шляхом визнання, усунення та мінімізації ризиків, пов'язаних із deepfakes, галузь FinTech зможе зміцнити свої позиції та продовжувати шлях до безпечного, стійкого та надійного фінансового майбутнього.

Список використаних джерел

1. Ady B. The Rising Threat of Deepfakes: 8 Ways It Can Impact the Fintech Industry [Electronic recourse] / B. Ady. – 2024. – Accessed mode: https://diro.io/impact-of-DeepFake-ai-fraud-in-fintech-industry.

2. Chesney R. Deep fakes: A looming challenge for privacy, democracy, and national security [Electronic recourse] / R. Chesney, D. Citron // California Law Review. – 2019. – Vol. 107(6). – Pp. 1753-1820. – Accessed mode: https://scholarship.law.bu.edu/faculty_scholarship/640/.

3. Deep learning for deep fakes creation and detection: A survey [Electronic recourse] / T. Nguyen, C. Nguyen, D. Nguyen, T. Nguyen // arXiv preprint arXiv:1909.11573. – 2019. – Accessed mode: https://www.arxiv.org/abs/1909.11573.

4. DeepFakes are coming for the financial sector [Electronic recourse]. – Accessed mode: https://www.wsj.com/articles/DeepFakes-are-coming-for-the-financial-sector-0c72d1e5?trk=article-ssr-frontend-pulse_little-text-block.

5. Generative adversarial nets [Electronic recourse] / Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. // Advances in neural information processing systems. – 2014. – Pp. 2672-2680. – Accessed mode: https://www.researchgate.net/publication/263012109_Generative_Adversarial_Networks.

6. GSMA [Electronic recourse]. – Accessed mode: https://www.gsma.com.

7. GSMA Fraud Typologies [Electronic recourse]. – Accessed mode: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/03/GSMA-Fraud-Typologies-04-03-24.pdf.

8. Gupta A. The Impact of Deepfakes on Financial Markets: A Systematic Review [Electronic recourse] / A. Gupta, M. Gupta // International Journal of Financial Studies. – 2021. – Vol. 9(3). – Pp. 45-60.

9. Impact of Digitalization On the Banking System Transformation / Shcherbatykh D., Shpileva V., Riabokin M., Zham O. // International Journal of Computer Science and Network Security. – 2021. – Vol. 21(12). – Pp. 513–520. DOI: https://doi.org/10.22937/IJCSNS.2021.21.12.71.

10. Korshunov P. Deepfakes: a new threat to face recognition? Assessment and detection [Electronic recourse] / P. Korshunov, S. Marcel // arXiv preprint arXiv:1812.08685. – 2018. – Accessed mode: https://www.researchgate.net/publication/329841498_DeepFakes_a_New_Threat_to_Face_Recognition_Assessment_and_Detection.

11. Mirsky Y. The creation and detection of deepfakes: A survey [Electronic recourse] / Y. Mirsky, W. Lee // ACM Computing Surveys (CSUR). – 2020. – Vol. 54(1). – Pp. 1-41. – Accessed mode: https://www.researchgate.net/publication/348178897_The_Creation_and_Detection_of_Deepfakes_A_Survey.

12. Mistry H. Deepfakes in Fintech Industry: 8 Ways How it Can Be a Rising Threat [Electronic recourse] / H. Mistry. – 2023. – Accessed mode: https://digiqt.com/blog/deepfakes-in-fintech-indutry.

13. Protecting world leaders against deep fakes [Electronic recourse] / S. Agarwal, H. Farid, Y. Gu, M. He, K. Nagano, H. Li // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. – 2019. – Pp. 38-45. – Accessed mode: https://farid.berkeley.edu/downloads/publications/cvpr19/cvpr19a.pdf.

14. State regulation of the development of the digital economy infrastructure: Regulación estatal del desarrollo de la infraestructura de la economía digital / S. Matiukh, N. Priamukhina, M. Riabokin, D. Kotelevets, V. Lopatovskyi // Cuestiones Políticas. – 2022. – Vol. 40(73). – Pp. 713-725. DOI: https://doi.org/10.46398/cuestpol.4073.40.

15. Taylor R. The Risk of Deepfake Fraud for Financial Institutions [Electronic recourse] / R. Taylor. – 2024. – Accessed mode: https://www.threatadvice.com/blog/the-risk-of-DeepFake-fraud-for-financial-institutions.

16. Three Things you Should Know About the Annual Scams and Cybercrime Brief 2023 [Electronic recourse]. – Accessed mode: https://www.police.gov.sg/Media-Room/Police-Life/2024/02/Three-Things-you-Should-Know-About-the-Annual-Scams-and-Cybercrime-Brief-2023#:~:text=The%20number%20of%20scam%20and,from%2031%2C728%20cases%20in%202022.

17. Top 5 Deepfake Prevention Strategies for Fintech and Financial Professionals [Electronic recourse]. – Accessed mode: https://www.verisoul.ai/blog-post/top-5-deepfake-prevention-strategies-for-fintech-and-financial-professionals.

18. Westerlund M. The emergence of deepfake technology: A review [Electronic recourse] / M. Westerlund // Technology Innovation Management Review. – 2019. – Vol. 9(11). – Pp. 39-52. Accessed mode: https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf.

19. Zhang J. The Rise of Deepfakes in Finance: Risks and Mitigations [Electronic recourse] / J. Zhang, Y. Hu // Journal of Financial Technology. – 2021. – Vol. 5(2). – Pp. 65-78.

20. Рябокінь М. Зростання ролі фінансових технологій в умовах розвитку цифрової економіки / М. Рябокінь, Є. Котух // Вісник Київського інституту бізнесу та технологій/ – 2024. – Vol. 50(1). – Pp. 60-78. DOI: https://doi.org/10.37203/kibit.2024.50.06.

References

1. Ady, B. (2024). *The Rising Threat of Deepfakes: 8 Ways It Can Impact the Fintech Industry*. https://diro.io/impact-of-DeepFake-ai-fraud-in-fintech-industry.

2. Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753-1820. https://scholarship.law.bu.edu/faculty_scholarship/640.

3. Nguyen, T., Nguyen, C., Nguyen, D., & Nguyen, T. (2019). Deep learning for deep fakes creation and detection: A survey. *arXiv preprint arXiv*:1909.11573. https://www.arxiv.org/abs/1909.11573.

4. Wall Street Journal. (2024). DeepFakes are coming for the financial sector. https://www.wsj.com/articles/DeepFakes-are-coming-for-the-financial-sector-0c72d1e5?trk=article-ssr-frontend-pulse_little-text-block.

5. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative adversarial nets. In *Advances in neural information processing systems* (pp. 2672-2680). https://www.researchgate.net/publication/263012109_Generative_Adversarial_Networks.

6. GSMA. (2024). https://www.gsma.com.

7. GSMA. (2024). Fraud Typologies. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/03/GSMA-Fraud-Typologies-04-03-24.pdf.

8. Gupta, A., & Gupta, M. (2021). The Impact of Deepfakes on Financial Markets: A Systematic Review. *International Journal of Financial Studies, 9*(3), 45-60.

9. Shcherbatykh, D., Shpileva, V., Riabokin, M., Zham, O. (2021). Impact of Digitalization On the Banking System Transformation. *International Journal of Computer Science and Network Security, 21*(12), 513–520. https://doi.org/10.22937/IJCSNS.2021.21.12.71.

10. Korshunov, P., & Marcel, S. (2018). Deepfakes: a new threat to face recognition? Assessment and detection. *arXiv preprint arXiv*:1812.08685. https://www.researchgate.net/publication/329841498_DeepFakes_a_New_Threat_to_Face_Recognition_Assessment_and_Detection.

11. Mirsky, Y., & Lee, W. (2020). The creation and detection of deepfakes: A survey. *ACM Computing Surveys (CSUR), 54*(1), 1-41. https://www.researchgate.net/publication/348178897_The_Creation_and_Detection_of_Deepfakes_A_Survey.

12. Mistry, H. (2023). *Deepfakes in Fintech Industry: 8 Ways How it Can Be a Rising Threat*. URL: https://digiqt.com/blog/deepfakes-in-fintech-indutry.

13. Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H. (2019). Protecting world leaders against deep fakes. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops* (pp. 38-45). https://farid.berkeley.edu/downloads/publications/cvpr19/cvpr19a.pdf.

14. Matiukh, S., Priamukhina, N., Riabokin, M., Kotelevets, D., & Lopatovskyi, V. (2022). State regulation of the development of the digital economy infrastructure: Regulación estatal del desarrollo de la infraestructura de la economía digital. *Cuestiones Políticas, 40*(73), 713-725. https://doi.org/10.46398/cuestpol.4073.40.

15. Taylor, R. (2024). *The Risk of Deepfake Fraud for Financial Institutions*. https://www.threatadvice.com/blog/the-risk-of-DeepFake-fraud-for-financial-institutions.

16. Singapore Police Force. (2024). Three Things you Should Know About the Annual Scams and Cybercrime Brief 2023. https://www.police.gov.sg/Media-Room/Police-Life/2024/02/Three-Things-you-Should-Know-About-the-Annual-Scams-and-Cybercrime-Brief-2023#:~:text=The%20number%20of%20scam%20and,from%2031%2C728%20cases%20in%202022.

17. Verisoul. (2024). Top 5 Deepfake Prevention Strategies for Fintech and Financial Professionals. https://www.verisoul.ai/blog-post/top-5-deepfake-prevention-strategies-for-fintech-and-financial-professionals.

18. Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11), 39-52. https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf.

19. Zhang, J., & Hu, Y. (2021). The Rise of Deepfakes in Finance: Risks and Mitigations. *Journal of Financial Technology, 5*(2), 65-78.

20. Riabokin, M., & Kotukh, Y. (2024). The Growing Role of Financial Technologies in the Context of Digital Economy Development. *Herald of Kyiv Institute of Business and Technology, 50*(1), 60-78. https://doi.org/10.37203/kibit.2024.50.06.

Отримано 11.02.2024

UDC 336.7:004:316.772.5

Maryna Riabokin
PhD in Economics, Associate Professor, Vice-Rector for Educational and Methodological Work
Kyiv Institute of Business and Technologies (Kyiv, Ukraine)
E-mail: marina.riabokin@gmail.com. **ORCID:** https://orcid.org/0000-0002-6724-9498
ResearcherID: AGZ-6858-2022. **Scopus:** 59171974600

Yevgen Kotukh
PhD in Technical Sciences, Associate Professor
National Technical University "Dnipro Polytechnic" (Dnipro, Ukraine)
E-mail: yevgenkotukh@gmail.com. **ORCID:** https://orcid.org/0000-0003-4997-620X
SCOPUS ID: 57215274481. **ResearcherID:** 15779883

Oleksiy Papylev
Technical Product Owner, «Lifecell» LLC (Kyiv, Ukraine)
E-mail: alex.papylev@gmail.com. **ORCID:** https://orcid.org/0009-0009-9806-8743

IMPACT OF DEEPFAKE TECHNOLOGY ON THE FINTECH SECTOR: CURRENT STATE IN UKRAINE AND CYBERCRIME PREVENTION STRATEGIES

This article examines the impact of deepfake technology on Ukraine's FinTech sector and provides strategies for preventing cybercrime. The authors analyze the current state and main risks associated with the use of deepfake, including reputational risks, phishing, identity theft, and market manipulation. A study was conducted to determine the readiness of Ukraine's FinTech sector for the challenges posed by deepfake, revealing a significant increase in the number of incidents involving this technology in cybercriminal schemes. Special attention is given to the methods that allow criminals to impersonate clients and financial officials to access confidential information and conduct fraudulent transactions.

One of the primary focuses of the study is identifying and implementing effective strategies to combat these threats. Among the suggested measures are the adoption of advanced deepfake detection technologies that utilize artificial intelligence and machine learning to identify synthetic media. The article discusses the importance of ongoing research and development in this area to stay ahead of evolving deepfake techniques.

Moreover, the article emphasizes the role of enhancing digital hygiene among users as a preventative measure. Educating users about the potential dangers of deepfake and how to recognize signs of fraudulent activity can significantly reduce the risk of falling victim to such schemes. Financial institutions are encouraged to invest in comprehensive training programs for both their employees and clients to foster a culture of awareness and vigilance.

The findings of the study underscore the urgent need for financial institutions and regulators to prioritize the issue of deepfake technology. The article calls for a coordinated approach that combines technological innovation, user education, and robust regulatory measures to safeguard the integrity and security of the FinTech sector in Ukraine. By proactively addressing these challenges, the FinTech sector can mitigate the risks associated with deepfake technology and ensure a secure environment for financial transactions and operations.

Keywords: *deepfake technology; innovation; fintech; cybercrime; artificial intelligence; fraud.*
Fig.: 9. Table: 2. References: 20.

Рябокінь М. В., Котух Є. В., Папилев О. І. Вплив технології Deepfake на Fintech сектор: поточний стан в Україні та стратегії запобігання кіберзлочинності. *Проблеми і перспективи економіки та управління.* 2024. № 1(37). С. 310-328.