УДК 336.71 https://doi 10.31548/economics14(4).2023.048

РОЗВИТОК ДІДЖИТАЛ-БАНКІНГУ В УМОВАХ ВІЙСЬКОВОГО СТАНУ В УКРАЇНІ

О.В.ФАЙЧУК,
кандидат економічних наук,
доцент кафедри банківської справи та страхування, Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0003-4056-0849
E-mail: faychuk_olga@ukr.net
В.А. КОСТЮК,
кандидат економічних наук, доцент,
завідувач кафедри банківської справи та страхування, Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0001-7671-3603
E-mail: vika-kostiuk@ukr.net
Я.О. СТЕПАНЕНКО,
магістр з фінансів,
банківської справи, страхування та фондового ринку,
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0009-0006-4642-1857
E-mail: Stepanenko039@ukr.net

Анотація. *У статті підкреслюється важливість сучасного цифрового розвитку банківської сфери. Розглядається вплив дистанційного банкінгу на позиції банків, підтримку економіки та основні аспекти його функціонування в Україні. Важлива увага спрямована на основні проблеми кібербезпеки в механізмі дистанційного банківського обслуговування: дефіцит кадрів, необізнаність співробітників, відсутність відповідного якісного бюджету, проблемні місця облікових даних, прогалини в мобільних додатках банків. Дослідження вказує на ключові елементи функціонування дистанційного банкінгу під час воєнного стану, такі як скорочення територіальної мережі банків, розвиток технологічних рішень, операційна стабільність, довіра вкладників, інвестування в кібербезпеку та роботу персоналу.*

Відображено виклики і загрози поточного функціонування банків України під час військового стану, визначено особливості перетворень на сучасному етапі механізму дистанційного банківського обслуговування. Звертається увага на важливість впровадження практичних тренінгів, кейсів, симуляцій кібератак при навчанні персоналу й клієнтів; вказана важливість використання штучного інтелекту та машинного навчання. Штучний інтелект і машинне навчання

важливі для розпізнавання кіберзагроз і протидії їм у режимі реального часу. Автором розширено напрями використання штучного інтелекту в напрямі створення прогностичних моделей, виконання обробки природної мови для аналізу неструктурованих даних, створення систем для повної автоматизації, забезпечення навчання з підкріпленням, впровадження генеративних моделей із виявлення шахрайства, боротьба з відмиванням грошей і аналіз поведінки клієнтів. Зроблено висновки, що застосування інноваційних технологій дозволить банкам автоматизувати виявлення аномальних і підозрілих активностей, забезпечуючи високий рівень безпеки та захисту фінансових операцій. Запропоновано поліпшення сучасного механізму діджитал-середовища на основі кіберстрахування, вказано на практичні аспекти функціонування схеми страхування за участі банка – страхового агента.

Ключові слова: *банківський бізнес; банківський менеджмент; дистанційне банківське обслуговування; діджитал-банкінг на ринку фінансових послуг; фінансове шахрайство.*

Актуальність

Поточні загрози й військовий стан створили виклики для системи дистанційного банківського обслуговування (далі – ДБО). В умовах підвищених ризиків для безпеки фінансові установи зобов'язані забезпечити безперервність і стійкість своєї цифрової інфраструктури. Такий аспект окреслює впровадження надійних заходів кібербезпеки зі створення захисту від потенційних атак, несанкціонованого доступу до конфіденційних фінансових даних і шахрайства. Окрім того, конфлікти й геополітична напруженість порушують роботу світових фінансових мереж і транскордонних транзакцій, які потенційно впливають на якісне і безперебійне функціонування дистанційного банківського обслуговування.

Банки, виходячи з поточної ситуації, уважно стежать за геополітичними подіями, розробляють сценарії подій і створюють плани на випадок надзвичайних ситуацій, щоб забезпечити безперервність надання послуг навіть за несприятливих обставин. Ефективність такої роботи забезпечують сучасні технології діджитал-банкінгу, в тому числі штучний інтелект (AI) та машинне навчання (ML).

Аналіз останніх досліджень і публікацій

Серед дослідників діджитал-банкінгу загалом і інструментів його розвитку варто виділити праці вітчизняних і зарубіжних вчених І. Артемєвої [1], С. Залюбовської [2], Р. Сніщенка [5], І. Баришевської, О. Лисяк, Л. Прицюк, О. Ткаченка [6], Н. Матвійчук [13], Г. Вестермана, О. Ящик [9] та ін. У дослідженнях таких науковців, як С.С. Залюбовська, І.О. Артемєва, О.В. Прокофєва, Р.Г. Сніщенко, М. Карліна розкриваються існуючий стан і перспективні напрями інноваційного розвитку, тенденції розвитку цифрових технологій, штучного інтелекту та технологій ідентифікації клієнтів. На особливості трансформації фінансового управління в банківськогму секторі саме під час військових дій звернули увагу

дослідники О. Ткаченко, Я. Ящик, Т. Савчик, Л. Гільтай та ін. Незважаючи на значну кількість досліджень і публікацій з питання дистанційного банківського обслуговування, на сьогодні сформована потреба в пошуку шляхів поліпшення існуючого механізму з врахуванням умов військового стану та активним розвитком діджитал-середовища.

Мета дослідження: виявлення сучасних проблем і розгляд особливостей розвитку діджитал-банкінгу в структурі механізму дистанційного обслуговування банку та пошук шляхів удосконалення діджитал банкінгу в умовах військового стану.

Матеріали та методи дослідження

Під час підготовки та обробки підібраних матеріалів використовувалися відповідні загальнонаукові методи: абстрактно-логічний, синтезу, аналізу, порівняння (під час дослідження та оцінювання системи ДБО), логічного узагальнення (під час пошуку й формування шляхів удосконалення механізму ДБО клієнтів в умовах військового стану). Основою дослідження стали дані статистики фінансового сектору Національного банку України, офіційні дані сучасних банків України, що активно впроваджують діджитал-банкінг.

Результати дослідження та їх обговорення

Вітчизняні банківські установи в умовах сьогодення інтенсивно досліджують новітні розробки в сфері дистанційного обслуговування та переймають найкращий досвід, у тому числі зарубіжний, удосконалюють систему управління для підтримки конкурентоспроможності й задоволення потреб клієнтів. У результаті клієнтам надаються послуги, які вирізняються якісним функціоналом і швидкістю виконання/отримання. Банки надають клієнтам значну кількість електронних послуг, які формуються на основі сучасних автоматизованих систем, інформаційних технологіях, засобах телекомунікаційного зв'язку тощо. Система ДБО активно використовується в діяльності значної кількості комерційних банків світу та є важливою в умовах жорсткої конкурентної боротьби банківського сектору. Функціонування механізму ДБО побудовано на базі нових платформ Web 3.0, хмарних технологій, задіяння віртуального взаємодіяння, блокчейн-технологій і впровадження системи штучного інтелекту (AI – Artificial Intelligence). Водночас, дія військового стану в Україні активізувала механізм ДБО в напрямі поліпшення нормативно-правого регулювання, введення належних методів управління (управління ризиками, дистанційного менеджменту, хеджування (аутсорсингу), антикризового менеджменту тощо).

Базисними принципами механізму ДБО в умовах війни є принципи варіативності, прозорості (розмаїття підходів із вирішенням означених цілей), рефлексивності (обґрунтованість впливу на зміни), ієрархічності/інформаційності (організованість взаємовідносин), адаптивності (гнучкість і оперативність відповідно посталих реалій), корпоративності (систематичність оновлення наявних цінностей) та ін. [6].

Для комерційного банку застосування дистанційного обслуговування сприяє зростанню показників

ефективності діяльності, дозволяє створити якісний продукт-послугу, оптимізувати рівень витрат до їх скорочення, забезпечити приріст клієнтів без зниження якості їх обслуговування (за рахунок зручності і гнучкості, онлайн-банкінгу, мобільного банкінгу, дистанційного управління рахунками, електронних переказів і платежів, безпеки та авторизації). Умови війни й перехід до онлайн-банкінгу створили можливості щодо зручності, доступності, посилення заходів безпеки, що позитивно позначилось на економічному розвитку не тільки банківського сектору держави, а й економіки загалом.

Поточний механізм дистанційного обслуговування банківським сектором, який було налагоджено ще в період пандемії (2019-2021 рр.), сприяє укріпленню позицій комерційних банків, стабілізації й підтримці економіки України. З початку повномасштабного вторгнення, станом на друге півріччя 2023 р., кількість діючих банків в Україні зменшилася на 9,2% та становить 65 банків, і з них лише 51 надають послуги ДБО (78,5%). Серед лідерів онлайн-банкінгу варто виокремити ПриватБанк, Альфа Банк, Monobank, ОТП Банк, А-Банк, Ощадбанк, ПУМБ та ін. Відповідно перераховані банки показують найвищі показники за критеріями функціональності ДБО: високий рівень захисту, якість сервісу аутентифікації/авторизації, формування виписок і рахунків, спрощений порядок проведення платежів, ефективний картковий сервіс і його підтримка мобільними застосунками, система депозитів/кредитів онлайн, можливості здійснення валютних операцій, якісна сервісна підтримка й канали зворотного зв'язку [4, 7].

Першочерговими елементами функціонування ДБО у воєнний період в Україні стали:

– зменшення територіальної сітки банків на 20% (або зменшення на 1349 одиниць підрозділів за період військового стану – окупація південно-східних територій держави, й під час періоду повномасштабного вторгнення російських військ в Україну) й швидке відновлення роботи мереж банків за рахунок дистанційного доступу [8];

– розвиток технологічних сервісів і рішень (розробка мобільних додатків у різних комерційних банках (до війни було створено 38 мобільних застосунків із діючого 71 банку системи ДБО і станом на 01.11.2023 р. – 42 мобільних застосунки при функціонуванні 65 банків. Позитивним є ребрендинг банківських додатків у напрямі поліпшення їх якості та рівня захисту (Креді Агріколь, Альфа-Банк Україна, ОТП Банк, Банк Південний, Кредобанк, Укргазбанк, Правекс Банк та ін.), активізація інтернет-еквайрингу в різних сферах бізнесу, перехід до хмарних сервісів, задіяння резервних технологічних майданчиків). За повномасштабного вторгнення в Україну до серпня 2023 р. мобільний банківський трафік було збільшено на 85%, а нові цифрові реєстрації підвищилися в 2 рази. Серед українського онлайн-банкінгу найбільш відомими є: Mono, Приват24, Sense, OTP Smart, ПУМБ (через Дію), А-банк, Укргазбанк, Ощад 24/7 тощо. Лідери за кількістю користувачів – Monobank (+5%), Приват24 (+11%), Ощад24/7 (+3,5%), OTP Smart (+1,5%);

– утримання операційної стабільності при значному навантаженні на мобільний банкінг, картковий

бізнес (операції транзакцій, переказу коштів за картковими рахунками) з врахуванням вимог регулятора;

– збереження й утримання довіри клієнтів, вкладників, зростання коштів на поточних рахунках, поліпшення відсоткових ставок за строковими вкладами, збільшення об'ємів чистих активів банку. Разом із тим, спостерігається незначний попит на кредити й відбулося зростання частини непрацюючих кредитів;

– забезпечення безперебійної роботи банкоматів, відділень банків, POS-терміналів, дата-центрів в умовах блекаутів (>30% відділень банків забезпечено генераторами, задіяно автономне електропостачання до 3 діб);

– збільшено інвестування в кібербезпеку, безперебійність роботи IT-систем (щодня спостерігається до 10 кібератак, ріст кібератак збільшено 3,5 рази) [3];

– персонал банку стає базисним елементом збереження стійкості банківської системи України (активно проводяться міри з забезпечення безпеки співробітників, створено віддалений режим роботи, забезпечена фінансова підтримка мобілізованих працівників та ЗСУ банками).

Із початком військового вторгнення в Україну, продовжено швидкий перехід населення країни в онлайн. При небезпечних ситуація й неможливості відвідувати відділення фізично, відбувся різкий спад попиту на фінансові послуги банків, більша частина відділень під час військових подій була зачинена (безпекові фактори). Частина клієнтів змушена була взаємодіяти з банком-обслуговувачем дистанційно: застосовувався інтернет, мобільні застосунки, месенджери на основі чат-ботів. Відповідно, зростав і показник цифровізації банківських послуг у державі. Вияв зацікавленості українців до цифрових технологій з роками лише зростає, а саме бажання перейти в діджитал-банкінг виявили 51% опитаних, проти 22% в пандемійний період (рис. 1).

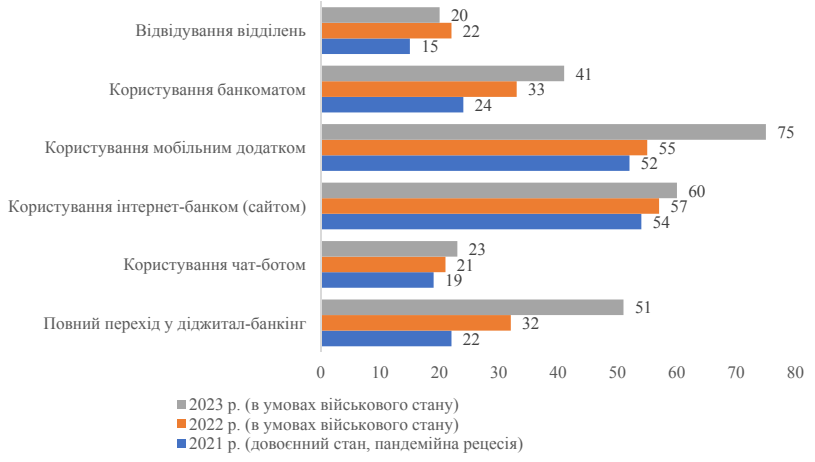

Рис. 1. Питома вага клієнтів, які застосовують різні канали ДБО в умовах військового стану в Україні, 2022-2023 рр., %

Джерело: сформовано авторами за [2].

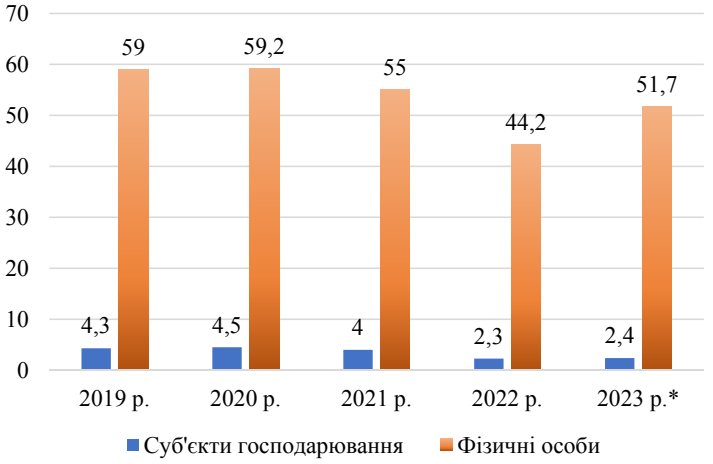

Рис. 2. Кількість клієнтів, які використовують дистанційне банківське обслуговування в Україні, 2019-2023 рр., млн. клієнтів

* дані зазначено за період 8 міс. 2023 року

Джерело: узагальнено авторами за [8].

Клієнти, переймаючись наслідками військового періоду, часто обирали смартфони та веб-браузери для виконання банківських операцій. Така зміна підходу викликана закономірністю дотримання правил соціального дистанціювання під час рецесійного впливу пандемії та згодом забезпечення власного захисту під час масованих атак країни-терориста.

У результаті, кількість клієнтів ДБО зростала швидкими темпами (на 17% зросла кількість фізичних осіб) (рис. 2). Кількість юридичних осіб, які користуються послугами ДБО зросла лише на 4%, що в більшій мірі пов'язано з кризою в державі, внутрішнім переміщенням бізнесів і значним відсотком їх закриття.

Такий перехід у першу чергу був можливий у результаті впровадження нових технологій в банківську систему, масової цифровізації (розвиток смартфонів (як з функцією NPC, так і без неї), гаджетів і їх відповідне здешевлення для населення). Завдяки прогресу в інформаційних технологіях і створенню відповідної законодавчої та нормативної бази, перехід від веб-банкінгу до м-банкінгу є помітною тенденцією, коли все більше людей віддають перевагу здійснювати свою банківську діяльність через мобільні пристрої замість використання традиційних настільних комп'ютерів або ноутбуків [15].

Відносно особливостей користування мобільними додатками в механізмі ДБО під час військового стану виявили: 75% опитаних українців надали перевагу застосування мобільних застосунків і тільки незначний відсоток користується лише онлайн-банкінгом (11%) – в більшості відбувається користування змішаного типу.

Серед популярних банківських операцій переважаючими є переказ коштів з карти на карту, поповнення мобільних рахунків і оплата комунальних послуг. Операціями, які на-

були поширення найбільше під час військового стану стали транзакції з карти на карту й донати (переведення коштів на допомогу українській армії), що зайняло 30% спрямувань. Перспективними функціями мобільних додатків можуть стати: придбання квитків на транспорт (27%), можливість оформляти банківські картки без візиту у відділення (кредитові/дебетові, в іноземній валюті) (61%), управління різними рахунками в одному мобільному додатку (52%), купівля криптовалюти (27%), якісний зворотній зв'язок і фінансове консультування з керування активами (22%), придбання акцій і цінних паперів (21%) [7].

Головною проблемою діджитал-банкінгу в умовах військового стану є все ж таки безпека даних споживачів. Кібератаки й витік інформації даних клієнтів призводять до вагомих фінансових втрат і завдають репутаційну шкоду [11, 12]. Кіберзлочинці, направляючи атаки на банки, можуть отримати несанкціонований доступ до особистих даних клієнтів, які містять фінансову інформацію, паролі та особисті дані. Прямими зразками хакерських атак стали віруси (поширюються е-поштою чи шляхом завантаження користувачем заражених файлів, переходом за посиланнями, що часто змінюють дані на комп'ютері), вішинг/фішинг (телефонне/електронне виманювання шахраями конфіденційних даних клієнта з використанням соціальної інженерії) й фармінг (є складною фішинговою атакою, що перенаправляє користувача на фальшивий банківський веб-сайт способом модифікації запису DNS) тощо.

Для подолання таких викликів, банки інвестують кошти в надійні безпекові заходи: багатофакторна автентифікація, хмарні технології, наскрізне шифрування й регулярне оновлення системи безпеки. Сучасну ситуацію щодо безпекових заходів ускладнює й військовий стан у державі. Такі обставини активізують такі додаткові небезпечні чинники, як перебої в роботі мережі не лише через кібератаки, а й через відключення електроенергії, які впливають на доступність ДБО в мережі банку. У даному випадку банківські установи приймають заходи щодо безперебійного функціонування банківської системи (резервні плани та альтернативні канали живлення і доступу), Національний банк утримує систему BankID, яка безперебійно надає послуги відповідно до вимог воєнного часу.

У зв’язку зі зростаючою складністю кіберзлочинності, фінансові установи активно впроваджують передові технології, спрямовані на забезпечення надійного захисту від сучасних кіберзагроз. Машинне навчання й штучний інтелект відіграють ключову роль у цьому контексті, допомагаючи банкам вдосконалювати системи безпеки та ефективно протидіяти зловмисним атакам. Серед важливих стратегій використання ШІ та ML у сфері кібербезпеки банків варто виділити виявлення потенційних загроз і розширення компетентностей персоналу через реалізацію методів – таких, як аналітика поведінки користувачів (UBA), створення поведінкових моделей, а також аналіз особливостей соціальної інженерії та інших векторів атак. У перспективі основне бачення надання банківських послуг – це повна відсутність людського втручання й посилений кіберзахист за допомогою таких тех-

нологій як 6G в поєднанні з AI та ML [10]. Система 6G відзначається архітектурною дезагрегацією, що передбачає розділення компонентів системи на окремі функціональні блоки з відкритими інтерфейсами для підвищення масштабованості й гнучкості. Ключовим принципом є хмарне проектування, яке дозволяє використовувати ресурси здоров'я широкосмугових мереж і вбудований штучний інтелект для оптимізації управління, контролю й обробки даних. Ця система також передбачає використання штучного інтелекту на рівні користувача та взаємодії з багатьма зацікавленими сторонами. Забезпечення надійності включає в себе гарантування працездатності пристроїв, стійкість підмережі перед різноманітними викликами та ресурси для гетерогенної хмари, що підтримують різні обчислення та сервіси. Також важливо забезпечити надійність програм і сервісів для забезпечення стійкості та якості обслуговування користувачів.

За умови сканування ймовірних шаблонів, які можуть свідчити про кіберзлочинність, варто звернути увагу на значний спектр червоних маркерів. Зокрема: «чи діють люди певним чином, що виходить за межі їхньої звичайної діяльності? Чи дехто отримує доступ до папок і файлів, до яких зазвичай відсутній доступу? Чи виконують пошук документів, які містять конфіденційну інформацію, неодноразово?». Формування культури кібербезпеки повинне поширюватися і на клієнтів.

Адаптацію вітчизняних банків до сучасних загроз дослідили на прикладі АТ «ОТП Банк». Так, беручи до уваги значну загрозу кібератак для АТ «ОТП Банк», важливо проводити навчальні тренінги для персоналу й забезпечувати виконання правильних дій у небезпечних ситуаціях.

Тренінг надасть персоналу необхідні інструменти для виявлення й запобігання фішинговим атакам, підвищуючи загальний рівень кібербезпеки банку. Зокрема, це:

– теоретична підготовка – огляд понять і технік, пов'язаних із вішингом/фішингом;

– розгляд реальних прикладів фішингових атак на банки за допомогою презентацій і кейсів;

– фішинговий симулятор – проведення симуляційних атак із використанням фішингових емейлів і веб-сайтів, які імітують реальні сценарії;

– ідентифікація підозрілих повідомлень – практичні вправи на виявлення підозрілих елементів у електронних листах і повідомленнях;

– заходи безпеки й реагування – навчання персоналу ефективно реагувати на виявлені фішингові атаки, включаючи відмову від відкриття непевних вкладень і посилань;

– технічний аналіз – аналіз реальних методів фішингу та їх виявлення за допомогою технічних засобів;

– співпраця з кібербезпекою – навчання ефективній комунікації та співпраці з кібербезпечним відділом при виявленні підозрілих активностей;

– оновлення знань – встановлення регулярних тренувань і оновлень для підтримки актуальних знань у сфері кібербезпеки.

Частину структури практичного тренінгу пропонуємо поєднувати з симуляцією кібератаки, розпізнавання загроз, ситуаційними кейсами тощо (табл. 1).

Співробітники на розглянутих тренінгах навчаються реагувати на

1. Розробка тренінгу кібербезпеки на прикладі АТ «ОТП Банк»

Етапи тренінгу	Характеристика	Зразок поведінки
1.Активна фаза симуляції кібератаки	Реалізація симуляції кібератак з використанням тестового середовища. Реалістичні сценарії	Розробка сценарію: Фішингова атака на онлайн банкінг та його відповіді на корпоративному рівні.
2.Пасивна фаза розпізнавання загроз	Навчання персоналу виявляти нестандартну активність та підозрілу поведінку в мережі.	Розпізнання сумнівних повідомлень та подолання ризиків: виявлення потенційно фішингових повідомлень, електронних листів та посилань у банківській поштовій системі; повідомлення про виявлені підозрілі елементи кібербезпечному відділу та вищому керівництву; відмова від відкриття вкладених файлів або переходу за посиланнями для уникнення можливого зараження шкідливим вмістом.
3.Забезпечення безпеки даних	Засвоєння персоналом навичок захисту конфіденційних даних під час кібератаки.	Управління підозрілими повідомленнями: збір та передача всіх підозрілих повідомлень для подальшого аналізу кібербезпечним спеціалістам; розробка стратегічного плану та протоколів повідомлення.
4.Відновлення структури в результаті	Пояснення процесів відновлення нормальної функціональності систем після кібератаки.	Реагування на фішингову атаку та запобігання подальшому розповсюдженню: ізоляція компрометованих об'єктів у випадку впливу атаки на банківські системи; інформування клієнтської бази про можливий ризик та надання рекомендацій щодо зміни паролів та підвищення безпеки облікових записів.
5. Супровід та тестування отриманих знань	Проведення оцінювання для перевірки рівня освоєння матеріалу.	Підготовка та навчання персоналу: визначення відповідальних осіб та навчання їх термінології, технологічних аспектів та процедур виявлення інцидентів; проведення практичних занять, включаючи ситуаційні кейси та вправи типу Escape Room для ефективного реагування на інциденти.
6.Забезпечення постійного навчання	Впровадження систематичних тренувань і актуалізація навичок у галузі кібербезпеки.	Проведення аналізу та розробка стратегій: аналіз методів та джерел фішингової атаки після її ізоляції; розробка стратегій для запобігання майбутнім подібним атакам; проведення тренувань для підвищення навичок виявлення фішингу та ефективної реакції під час атаки.
7.Виконання аналізу і вдосконалення результатів	Проведення аналізу тренінгового процесу та впровадження вдосконалень	Інформаційне сповіщення та публічний відгук: розповсюдження інформації серед персоналу про нові види фішингу та застосування актуальних методів захисту; забезпечення своєчасного та інформативного відгуку щодо фішингової атаки, якщо інцидент став публічним.

Джерело: розроблено авторами.

фішинг, класифікації даних, вміння формувати складні паролі, фізичну безпеку, елементи криптографії тощо.

Навчання кінцевих користувачів у сфері кібербезпеки є суттєвим елементом в механізмі ДБО, враховуючи їхні звички й поведінку. Рекомен-

Рис. 3. План тренінгу «Дії персоналу банку та клієнтів при фішингових атаках»

Джерело: розроблено авторами.

дується провести навчання у формі вебінарів або інтерактивних семінарів для максимальної ефективності й можливості відповіді на запитання учасників [14]. Серед учасників рекомендується вибирати представників різних вікових категорій, включаючи студентів і учнів шкіл, що є прикладом дієвої практики.

Впровадження стандартних шаблонів у робочі процеси й виявлення будь-яких відхилень від них може мати суттєве значення для попередження кіберзлочинності. Цей підхід сприяє створенню основи безпеки, що дозволяє вчасно реагувати на можливі загрози та забезпечує високий рівень захищеності в механізмі дистанційного банківського обслуговування.

Штучний інтелект є критично важливим для виокремлення патернів, які потім застосовують у практичному механізмі ДБО (рис. 3). AI допомагає швидше виконувати аналіз, що в результаті сприяє швидкому вияву потенційних інцидентів небезпеки, які варто розслідувати.

Однак тоді й виникають етичні питання щодо конфіденційності інформації, щодо автоматизації процесів і роботизації, відсутності відповідальності за рішення і дії кіберзахисту, наприклад і такого вагомого принципу як аккаунтовість (відповідальність за заходи кіберзахисту, проведення аудиту кіберзахисту, відповідальність за власні вчинки персоналу в сфері безпеки).

Плавний розвиток ML та AI (рис. 4) забезпечить для АТ «ОТП Банк» вже на 2024-2025 рр. можливості:

– створення прогностичних моделей із виявлення шахрайства та

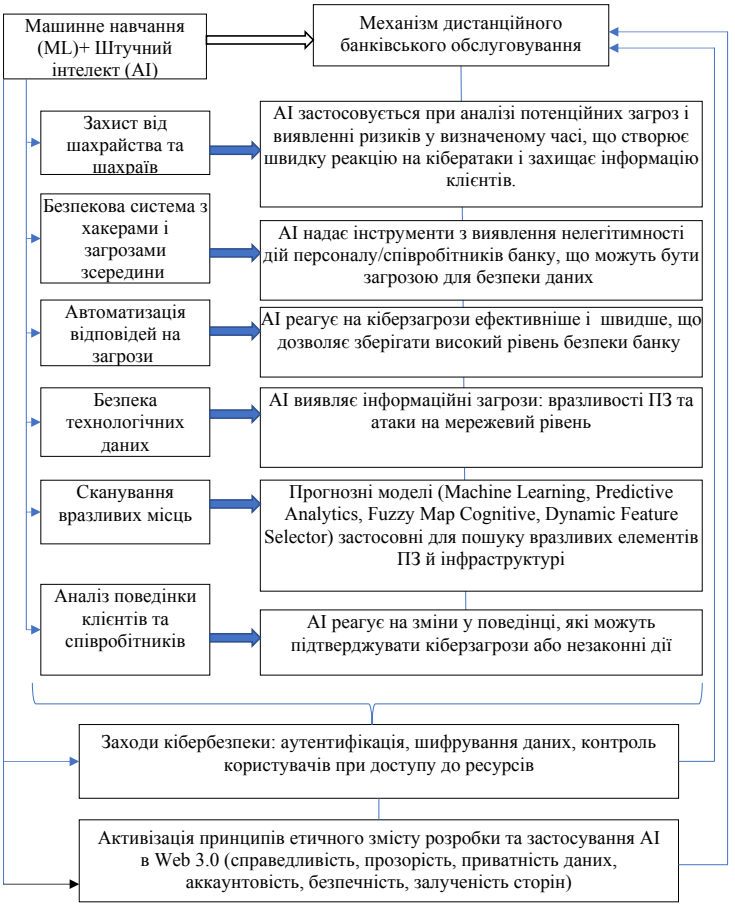

Рис. 4. Сфери впровадження ML і AI в механізм ДБО АТ «ОТП Банк»
Джерело: розроблено авторами.

вішингових/ фішингових афер ще до завдання шкоди;

– виконання обробки природної мови (NLP) для дослідження неструктурованих даних;

– створення систем на основі AI для вивільнення ресурсів і більш комплексної автоматизації людської праці – рутинних завдань безпеки (коригування даних, управління виправленнями, відслідковування вразливих елементів системи, вияв відмивання грошей, відповідність дій нормативним вимогам тощо);

– забезпечення навчання з підкріпленням, активізація генеративних моделей і інших передових методів із виявлення шахрайства та аналіз викликів соціальної інженерії для боротьби з кіберзлочинністю.

Необхідно відзначити ініціативу вдосконалення діджитал-середовища банку, зосереджуючись на безпеці, що базується на аналізі ризиків і можливих втрат, особливо в умовах воєнного стану в країні. Введенням кіберстрахування АТ «ОТП Банк» може забезпечити ефективний механізм захисту

для своїх клієнтів, спрямований на ліквідацію кіберзагроз у дистанційному банківському обслуговуванні.

Кіберстрахування представляє собою інноваційний страховий продукт, спрямований на захист бізнес-власників від наслідків кібератак і хакерських загроз. Воно також відоме як страхування від кіберризиків, страхування порушення даних і кібербезпеки. Передача цього ризику страховій компанії спрямована на оптимізацію впливу ризику для фізичних і юридичних осіб, які використовують банківські послуги, шляхом компенсації збитків.

Для забезпечення ефективності кіберстрахування для клієнтів важливо акцентувати увагу на конкретних ризиках, таких як фішинг (вимагання коштів під шахрайським тиском), телефонне шахрайство (вішинг) і зняття коштів із втрачених або викрадених карток. Рекомендується розглядати можливі схеми кіберстрахування клієнтів банку (рис. 5), що надаються у вигляді електронного поліса в онлайн-режимі.

Для підтримки клієнта дієвим засобом буде активізувати чат-bot у Viber, Telegram або в мобільному застосунку OTPBank-UA на основі штучного інтелекту, головним завданням якого є якісний зворотній зв'язок і ведення клієнта в надзвичайних ситуаціях.

Висновки та перспективи подальших досліджень

Сучасний розвиток діджитал-банкінгу має тенденцію до активного зростання, а сучасні події й загрози, поточний військовий стан значно підсилив ці процеси, насамперед перехід значної кількості населення в систему дистанційного банківського обслуговування. Важливими напрямами розвитку діджитал-банкінгу залишається забезпечення кіберзахисту та налагодження якісного обслуговування клієнтів, що й враховують у своєму механізмі дистанційного обслуговування сучасні інноваційні банки. Штучний інтелект (AI) та машинне навчання (ML) виступають як важливі технології, спрямовані на підтримку фінансових установ у забезпеченні безпеки їхніх систем і даних від зловмисних атак. Однією з ключових стратегій використання AI та ML у кібербезпеці банків є виявлення потенційних загроз і підвищення кваліфікації фахівців, застосовуючи аналітику поведінки користувачів (UBA), розробку поведінкових моде-

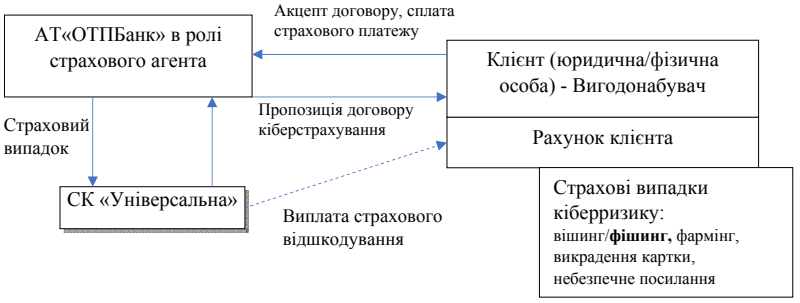

Рис. 5. Схема кіберстрахування рахунку клієнта від вішингу/фішингу
Джерело: розроблено авторами.

лей і врахування особливостей соціальної інженерії.

У ході дослідження розвитку діджитал-банкінгу як одного з видів дистанційного банківського обслуговування в умовах військового стану на прикладі АТ «ОТП Банк», виявили, що, акцентуючи увагу на своїх перевагах, АТ «ОТП Банк» стратегічно адаптує свою політику, використовуючи інноваційні технології для створення нових продуктів і вдосконалення сервісу. Запити користувачів зростають у контексті постійного розвитку технологій. Ідеї та рішення, які нещодавно були вторинними, нині є необхідною частиною стандартного функціонування банку в діджитал-середовищі. Відтак, представлені інструменти, апробовані АТ «ОТП Банк», розглядаємо як дієві шляхи вдосконалення діджитал банкінгу в умовах військового стану та розглядаємо як такі, що можна рекомендувати для застосування іншим банківським установам.

Список використаних джерел

1. Залюбовська С.С., Артем'єва І.О. Цифрові трансформації банківського сектору. *Науковий вісник Національної академії статистики, обліку та аудиту: зб. наук. праць.* 2023. № 1-2. С. 96–103.
2. Карлін М.І., Шматковська Т.О., Борисюк О.В. Банківські інновації в умовах формування цифрової економіки. *Економіка і суспільство.* 2021. №27. URL: https://doi.org/10.32782/2524-0072/2021-27-24
3. Прасад А. Google прогнозує збільшення кібератак росії на Україну та членів НАТО у 2023 році. 2023. URL: https://forbes.ua/news/google-prognozue-zbilshennya-kiberatak-rosii-na-ukrainu-i-chleniv-nato-u-2023-rotsi-16022023-11778
4. Прокоф'єва О.В. Розвиток банківського сектору України в умовах воєнного стану. *Інвестиції: практика та досвід*. 2023. № 8. С. 108-112.
5. Сніщенко Р.Г. Напрями впровадження банківських інновацій. *Трансформаційна економіка*. 2023. № 2. С. 53-56.
6. Ткаченко О.Є. Трансформація фінуправління в банківському секторі в умовах війни. *Наукові записки НУ «Острозька академія»*. *Економіка*. 2022. №27. С.73-80.
7. Українці назвали найбільш очікувані функції, які хотіли б бачити в цифровому банкінгу (інфографіка). 2023. URL: https://news.finance.ua/ua/ukrainci-nazvaly-naybil-sh-ochikuvani-funkcii-yaki-hotily-b-bachyty-v-cyfrovomu-bankinhu-infohrafika
8. Фінансовий сектор. Офіційні дані НБУ. 2023. URL: https://bank.gov.ua/ua/statistic/sector-financial
9. Ящик О., Гільтай Л., Савчин Т., Гевко І. Кібербезпека в децентралізованій інтернет-екосистемі web 3.0. *Наукові записки ТНПУ ім. В. Гнатюка.* 2023. № 1. С. 61-68.
10. Ahokangas P., Gordon J., Matinmikko-Blue M., Gisca O., Yrjölä S. Toward an integrated framework for developing European 6G innovation. Telecommunications Policy. 2023. Vol. 47, Is. 9. URL: https://doi.org/10.1016/j.telpol.2023.102641 (BD Scopus).
11. Gambacorta L., Aldasoro I., Leach T. Giudici P. The drivers of cyber risk. *Journal of Financial Stability.* 2022. Vol. 60. URL: https://doi.org/10.1016/j.jfs.2022.100989
12. Feijóo C., Bauer J., Xia J., Kwon Y., Bohlin E., Jain R. Howell B., Harnessing AI to increase wellbeing for all: The case for a new technology diplomacy. Telecommunications Policy. 2020. Vol. 44, Iss. 6 URL: https://doi.org/10.1016/j.telpol.2020.101988
13. Tesliuk S., Matviichuk N. Main trends in the development of banking innovations in Ukraine. *Economic journal of Lesya Ukrainka Volyn National University*. 2021. 1 (25). Mar. pp. 79–87.

14. Rodrigues L., Oliveira A., Rodrigues H. Technology management has a significant impact on digital transformation in the banking sector. *International Review of Economics&Finance*. 2023. URL: https://doi.org/10.1016/j.iref.2023.07.040
15. Wu L., Lv Y., Yu D. Digital banking and deposit: Substitution effect of mobile applications on web services. *Finance Research Letters.* 2023. Vol. 56. URL: https://doi.org/10.1016/j.frl.2023.104138

References

1. Zaliubovska, S.S., Artem'ieva, I.O. (2023). Tsyfrovi transformatsii bankivskoho sektoru [Digital transformations of the banking sector]. *Naukovyi visnyk Natsionalnoi akademii statystyky, obliku ta audytu: zb. nauk. prats*, 1-2, 96–103.
2. Karlin, M.I., Shmatkovska, T.O., Borysiuk, O.V. (2021). Bankivski innovatsii v umovakh formuvannia tsyfrovoi ekonomiky. *Ekonomika i suspilstvo,* 27. Retrieved from https://doi.org/10.32782/2524-0072/2021-27-24
3. Prasad, A. (2023). Google prohnozuie zbilshennia kiberatak rosii na Ukrainu ta chleniv NATO u 2023 rotsi [Google predicts an increase in Russian cyberattacks on Ukraine and NATO members in 2023]. Retrieved from https://forbes.ua/news/google-prognozue-zbilshennya-kiberatak-rosii-na-ukrainu-i-chleniv-nato-u-2023-rotsi-16022023-11778
4. Prokof'ieva, O.V. (2023). Rozvytok bankivskoho sektoru Ukrainy v umovakh voiennoho stanu [Development of the banking sector of Ukraine in the conditions of martial law]. Investytsii: praktyka ta dosvid, 8, 108-112.
5. Snishchenko, R.H. (2023). Napriamy vprovadzhennia bankivskykh innovatsii [Directions of implementation of banking innovations]. *Transformatsiina ekonomika*, 2, 53-56.
6. Tkachenko, O.Ye. (2022). Transformatsiia finupravlinnia v bankivskomu sektori v umovakh viiny [Transformation of financial management in the banking sector in the conditions of war]. *Naukovi zapysky NU «Ostrozka akademiia». Ekonomika*, 27, 73-80.
7. Ukraintsi nazvaly naibilsh ochikuvani funktsii, yaki khotily b bachyty v tsyfrovomu bankinhu (infohrafika) [Ukrainians named the most anticipated functions they would like to see in digital banking (infographic)]. 2023. Retrieved from https://news.finance.ua/ua/ukrainci-nazvaly-naybil-sh-ochikuvani-funkcii-yaki-hotily-b-bachyty-v-cyfrovomu-bankinhu-infohrafika
8. Finansovyi sektor [Financial sector]. (2023). Ofitsiini dani NBU. Retrieved from https://bank.gov.ua/ua/statistic/sector-financial
9. Yashchyk, O., Hiltai, L., Savchyn, T., Hevko, I. (2023). Kiberbezpeka v detsentralizovanii internet-ekosystemi web 3.0. *Naukovi zapysky TNPU im. V. Hnatiuka,* 1, 61-68.
10. Ahokangas, P., Gordon, J., Matinmikko-Blue, M., Gisca, O., Yrjölä, S. (2023). Toward an integrated framework for developing European 6G innovation. Telecommunications Policy, 47, 9. URL: https://doi.org/10.1016/j.telpol.2023.102641
11. Gambacorta, L., Aldasoro, I., Leach, T. Giudici, P. (2022). The drivers of cyber risk. *Journal of Financial Stability*, 60. URL: https://doi.org/10.1016/j.jfs.2022.100989
12. Feijóo, C., Bauer, J., Xia, J., Kwon, Y., Bohlin, E., Jain, R. Howell, B., Harnessing, A. (2020). I to increase wellbeing for all: The case for a new technology diplomacy. Telecommunications Policy, 44, 6 URL: https://doi.org/10.1016/j.telpol.2020.101988
13. Tesliuk, S., Matviichuk, N. (2021). Main trends in the development of banking innovations in Ukraine. *Economic journal of Lesya Ukrainka Volyn National University*, 1 (25), 79–87.
14. Rodrigues, L., Oliveira, A., Rodrigues, H. (2023). Technology management has a sig-

nificant impact on digital transformation in the banking sector. *International Review of Economics&Finance*. URL: https://doi.org/10.1016/j.iref.2023.07.040

15. Wu, L., Lv, Y., Yu, D. (2023). Digital banking and deposit: Substitution effect of mobile applications on web services. *Finance Research Letters,* 56. URL: https://doi.org/10.1016/j.frl.2023.104138

Faichuk O., Kostyuk V., Stepanenko Y. (2023).
DEVELOPMENT OF DIGITAL BANKING IN THE STRUCTURE OF THE BANK'S REMOTE SERVICE MECHANISM UNDER MARTIAL LAW
BIOECONOMY AND AGRARIAN BUSINESS, 14(4): 54-68.
https://journals.nubip.edu.ua/index.php/bioeconomy/article/view/48648
https://doi 10.31548/economics14(4).2023.048

Abstract. *The article emphasizes the importance of modern digital development of the banking sector towards the digitalization of the remote banking mechanism. The author considers the impact of remote banking on the positions of banks, support for the economy and the main aspects of its functioning in Ukraine. Special attention is paid to the main cybersecurity issues in the e-banking mechanism: shortage of personnel, lack of awareness of employees, lack of an appropriate quality budget, credentials problem areas, gaps in mobile applications of banks. The study identifies key elements of remote banking during martial law, such as reducing the territorial network of banks, developing technological solutions, operational stability, depositor confidence, investing in cybersecurity and staff.*

The article reflects the challenges and threats to the current functioning of Ukrainian banks during martial law, and highlights the peculiarities of transformations at the current stage of the remote banking mechanism.

Attention is drawn to the importance of introducing practical trainings, case studies, and cyberattack simulations in the training of staff and customers; the importance of using artificial intelligence and machine learning is also emphasized.

Artificial intelligence and machine learning are important for recognizing and countering cyber threats in real time. Training of end users - awareness - is an important cybersecurity asset in the RBS mechanism, depending on their habits and behavior. The author suggests stages of training in the form of a webinar or interactive seminars for greater efficiency and the ability to answer questions from participants. The importance of all consumers of bank services of different age groups is emphasized.

The author extends the use of artificial intelligence in the areas of creating predictive models, performing natural language processing for analyzing unstructured data, creating systems for full automation, providing reinforcement learning, implementing generative models for fraud detection, combating money laundering, and analyzing customer behavior. It is concluded that the use of innovative technologies will allow banks to automate the detection of abnormal and suspicious activities, ensuring a high level of security and protection of financial transactions. The author proposes to improve the current mechanism of the digital environment on the basis of cyber insurance, and indicates the practical aspects of the functioning of the insurance scheme with the participation of a bank as an insurance agent. For greater effectiveness of this type of insurance, it is proposed to focus on the risk of extortion - phishing (Internet extortion, fake payment sites), vishing (telephone fraud), withdrawal of funds from a lost/stolen card, etc.

Keywords: *banking business; bank management; remote banking; digital banking in the market of financial services; financial fraud.*