ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ ЕЛЕКТРОННОГО БАНКІНГУ

THEORETICAL ASPECTS OF ELECTRONIC BANKING RISK MANAGEMENT

УДК 336.717

Домінова І.В.
аспірант кафедри менеджменту
банківської діяльності
Київський національний
економічний університет
імені Вадима Гетьмана

У статті висвітлені теоретичні аспекти управління ризиками електронного банкінгу. Описано доцільність впровадження системи електронного банкінгу банківськими установами. Розглянуто сутність ключових ризиків електронного банкінгу. Проаналізовано впроваджені Базельським комітетом принципи управління ризиками електронного банкінгу. Висвітлено необхідність побудови ефективної системи ризик-менеджменту електронного банкінгу з урахуванням міжнародних стандартів.

Ключові слова: *електронний банкінг, Інтернет-банкінг, мобільний банкінг, ризики електронного банкінгу, принципи управління ризиками електронного банкінгу.*

В статье освещены теоретические аспекты управления рисками электронного банкинга. Описана целесообразность внедрения системы электронного банкинга банковскими учреждениями. Рассмотрена сущность ключевых рисков электронного банкинга. Проанализировано внедренные Базельским комитетом принципы управления рисками электронного банкинга. Освещена необходимость построения эффективной системы риск-менеджмента электронного банкинга с учетом международных стандартов.

Ключевые слова: *электронный банкинг, Интернет-банкинг, мобильный банкинг, риски электронного банкинга, принципы управления рисками электронного банкинга.*

The article covers the theoretical aspects of electronic banking risk management. The expediency of introduction of electronic banking system by banking institutions is described. The essence of key risks of electronic banking is considered. The principles of electronic banking risk management which introduced by the Basel Committee have been analyzed. The necessity of building an effective system of electronic banking risk management with consideration of international standards is highlighted.

Key words: *e-banking, Internet banking, mobile banking, e-banking risks, principles of electronic banking risk management.*

Постановка проблеми. Стрімкий розвиток Інтернет-технологій значно вплинув на розвиток ринку банківських послуг, шляхом впровадження інформаційних систем у процес функціонування банківської установи. Як результат, в умовах сьогодення банки для утримання конкурентних позицій на ринку банківських послуг здійснюють трансформацію процесу продажу та надання банківських операцій та послуг шляхом переходу від традиційних форм банківського обслуговування до альтернативних – електронного банківського обслуговування. Цей вид обслуговування є значно привабливішим для клієнтів (низька вартість послуг, цілодобовий доступ до фінансових ресурсів, швидкість обслуговування) та дозволяє банківській установі значно розширити власний ринок збуту, знизити витрати на утримання персоналу і відділень та утримати конкурентні позиції на ринку банківських послуг.

Однак, впровадження систем електронного банківського обслуговування пов'язане з ризиками, які можуть негативно вплинути на фінансовий стан банківської установи та її клієнтів, тому аналіз теоретичних аспектів управління ризиками електронного банкінгу є актуальною темою дослідження.

Аналіз останніх досліджень і публікацій. Питання розвитку та доцільності впровадження у банківський бізнес електронного банківського обслуговування наразі є предметом активних досліджень багатьох вітчизняних і зарубіжних учених. Серед зарубіжних фахівців слід назвати таких, як: В. Бауер, М. Енгстлер, Б. Кінг, Дж. Сінкі, К. Скіннер, Д. Шпат. Д. І. Гафурова, Л. В. Лямин, П. В. Ревекою. Суттєвий внесок у дослідження інноваційного розвитку банків на основі використання систем електронного банкінгу зробили такі вітчизняні вчені, як: С. Б. Єгоричева, Л. О. Примостка, Н. Циганова, О. О. Чуб, Т. С. Шалига, А. В. Нікітін, І. Я. Карчева.

Постановка завдання. Метою статті є аналіз існуючих теоретичних аспектів управляння ризиками електронного банкінгу та обґрунтування доцільності їх врахування вітчизняними банками при побудові системи ризик-менеджменту електронного банкінгу.

Виклад основного матеріалу дослідження. Електронний банкінг – це специфічний, інноваційний інструмент дистанційного банківського обслуговування, за допомогою якого надаються традиційні послуги банківського обслуговування, а також комунікаційні та інформаційні послуги, через різні електронні канали, які видозмінюються та вдосконалюються відповідно до розвитку інформаційних технологій.

Електронне банківське обслуговування здійснюється за допомогою різних форм електронного банкінгу. На цей час функціонує близько десяти форм електронного банкінгу, які пройшли певний шлях еволюції від АТМ-банкоматів та технологій «home-banking» до Інтернет-банкінгу, мобільного банкінгу та навіть відеобанкінгу, які є доступними в будь-який час, з будь-якої частини земної кулі за умов підключення до мережі Інтернет.

Сьогодні системи електронного банкінгу використовують багато українських фінансових установ, і найпопулярнішими серед них є системи Інтернет-

банкінг та мобільний банкінг. Найбільшими і найбільш технологічними учасники ринку вважають інтернет-сервіси Приватбанку, Альфа-Банку, VTB Банку, ПУМБ, Райффайзен Банку Аваль, УкрСиббанку, Укрсоцбанку та Ощадбанку. Проте, лідером на ринку Інтернет-банкінгу та мобільного банкінгу традиційно залишається Приватбанк, онлайн-послугами якого користується максимальна кількість клієнтів, оскільки усі операції в режимі дистанційного обслуговування опрацьовуються банком цілодобово та без вихідних у режимі 24/7/365. Проведення платежів між клієнтами банку відбувається миттєво. Комісія за переказ коштів між клієнтами банку – 0%, між клієнтами різних банків – 1%. Передбачені цілодобові безкоштовні консультації у телефонному режимі та режимі online. Обрана стратегія лідерства дозволила забезпечити Приватбанку лідируючі позиції на ринку електронних банківських послуг, про що свідчив приріст депозитної бази банку протягом останніх 10 років (включно до III кварталу 2016 року), однак, націоналізація Приватбанку у IV кварталі 2016 року зумовила відтік коштів клієнтів (депозитів фізичних осіб скоротились на 0,5 млрд грн, юридичних осіб – на 2 млрд грн) за умов зниження рівня довіри до Приватбанку. На сьогодні Приватбанк є єдиним банком не тільки в Україні, а навіть у світі, який дозволяє здійснити більше, ніж 40 банківських операцій дистанційно в режимі online.

Відзначимо, що впровадження технологій електронного банкінгу зумовлює появу нових нетипових для традиційної банківської діяльності джерел компонентів банківських ризиків. Банки і клієнти в такій ситуації опиняються незахищеними від загроз, які можуть виникнути через впровадження недостатньо надійних технологій електронного банкінгу та банківських автоматизованих систем, що їх реалізовують. У зв'язку з цим прийнято виділяти три основні «системні» фактори, що обумовлюють виникнення нових джерел компонентів банківських ризиків при впровадженні систем електронного банкінгу: 1)поява у банку клієнтів нового типу, які часто фактично самі відіграють роль операціоністів; 2)залучення третьої сторони, зокрема, провайдерів, для забезпечення формування і підтримання функціонування систем ДБО; 3)потенційна доступність банківських автоматизованих систем банків для несанкціонованого доступу та мережевих атак [1, с. 123].

На нашу думку, доцільним є доповнити вищевказані «системні» фактори ще однією особливістю – віддаленість клієнта від банківської установи у процесі обслуговування. Ця особливість пояснюється складністю ідентифікації клієнта банківською установою в умовах дистанційного обслуговування, що в результаті зумовлює виникнення нових нетипових джерел, що розширюють профіль банківських ризиків.

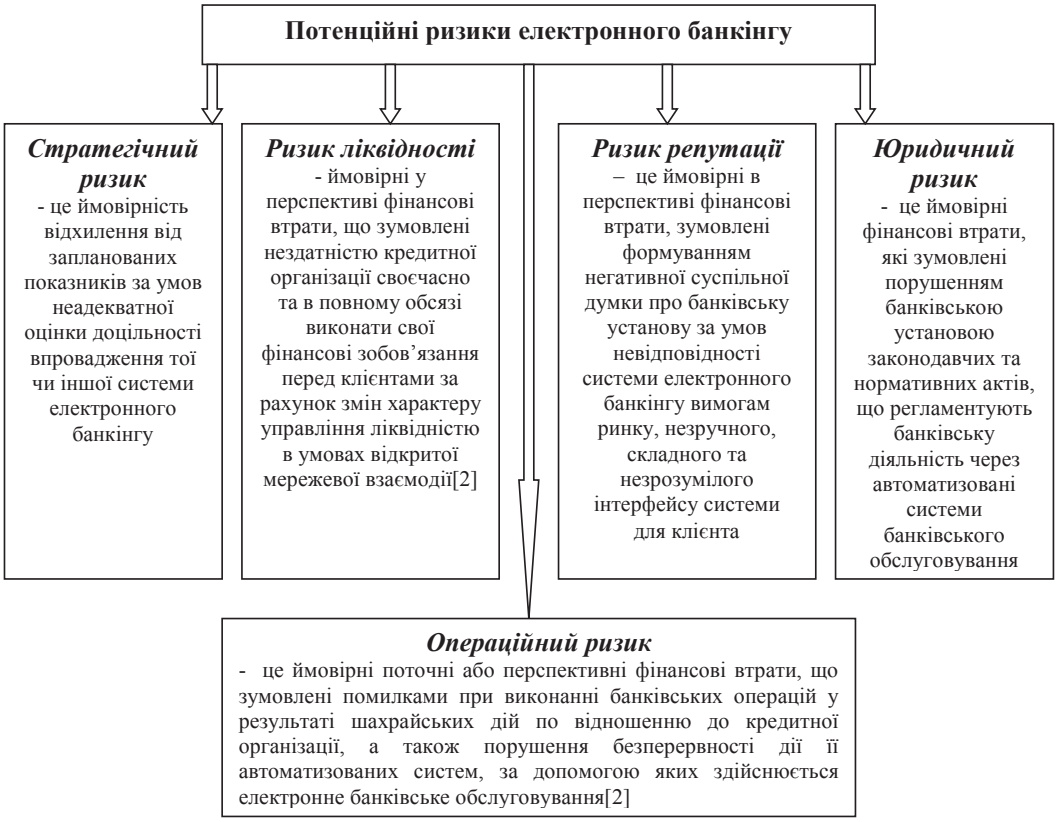

Рис. 1. Потенційні ризики електронного банкінгу

Джерело: сформовано автором

На даний момент не сформувалася єдина класифікація ризиків електронного банкінгу, однак, зарубіжні та вітчизняні вчені відзначають, що до ризиків, профіль яких значно розширюється в умовах впровадження систем електронного банкінгу, доцільно відносити операційний, юридичний, стратегічний, репутаційний та ризик ліквідності (рис. 1).

Появу того чи іншого ризику зумовлюють різні джерела. Наприклад, ймовірність операційного ризику зростає за умов шахрайських дій через систему електронного банкінгу; збої в роботі системи обслуговування або компанії-провайдера; недостатній рівень захищеності системи інформаційних технологій як з боку банку, так і з боку провайдера, що її обслуговує і т.д. Ймовірність ризику репутації зростає за умов: 1) розкриття або викрадання конфіденційної інформації про клієнта або інформації, яка є банківською таємницею; 2) неможливість забезпечення безперебійного функціонування системи електронного банкінгу; 3) запровадження незручної системи електронного банкінгу, яка є складною у використанні для клієнта тощо.

Варто зазначити, що ризики електронного банкінгу перебувають у тісній взаємодії. Такі банківські ризики, як юридичний та операційний, дуже сильно пов'язані з репутаційним ризиком і особливо чітка кореляція між ними прослідковується саме в умовах функціонування електронного банкінгу. Шахрайські дії, невиконання обов'язків перед клієнтом, розкриття конфіденційної інформації, збої в роботі автоматизованої системи електронного банкінгу – все це впливає на репутацію банку та породжує реалізацію операційного та юридичного ризиків за умов їх невчасної ідентифікації, що в подальшому призводить до значних фінансових втрат. Імовірним першоджерелом вищевказаних ризиків можуть стати недоліки в стратегічному плануванні, які спровокували реалізацію стратегічного ризику. Наступним ризиком, який має схильність до взаємозалежності з іншими ризиками є ризик ліквідності, оскільки процес управління ліквідністю стає ще більш складним, за умов цілодобового доступу клієнтів до власних фінансових ресурсів, що в результаті провокує значну волатильність ресурсів на рахунках. Як правило, саме через ризик ліквідності опосередковано реалізуються інші ризики: репутаційний, правовий та стратегічний ризики.

Основним міжнародним нормативним актом, що контролює процес управління ризиками електронного банкінгу є «Принципи ризик-менеджменту електронного банкінгу» [2], що розроблені Базельським комітетом питань банківського нагляду. Базельський комітет для побудови надій-

Таблиця 1

Принципи групи А. Нагляд з позиції вищого керівництва банку

№	Назва принципу	Короткий зміст
1.	Створення ефективної системи нагляду за операціями, що здійснюються через систему електронного банкінгу	а) Впровадження різних форм електронного банкінгу зумовлюють зростання ймовірності впливу на конфігурацію банківського ризику і реалізацію прийнятої стратегії банком, тому Рада директорів і Правління банку повинні враховувати ці особливості та піддавати їх глибокому стратегічного аналізу з точки зору співвідношення очікуваних витрат і прибутків у ретроспективі; б) Керівництво банку повинно впроваджувати електронне банківське обслуговування клієнтів лише за умови підготовки відповідного рівня кваліфікації менеджерів і персоналу у сфері ІТ; в) Управлінський нагляд повинен бути гнучким і ефективно реагувати на будь-які проблеми та інцидентів у цій сфері діяльності; г) Система ризик-менеджменту електронного банкінгу повинна бути інтегрована та узгоджена із загальним процесом управління банківськими ризиками.
2.	Створення всебічної процедури контролю за додержанням належного рівня безпеки	Найважливішим обов'язком Ради директорів і Правління банку є забезпечення процесу збереження активів банку, тому для виконання цього завдання керівництво банку повинно: 1) призначити конкретних осіб, які несуть відповідальність за стан справ у цій сфері; 2) розробити жорстві правил, що дозволяють відслідковувати спроби вторгнення в комунікаційні мережі банку та запобігати несанкціонованому доступу до комп'ютерних технологій, програмного забезпечення і баз даних; 3) здійснювати регулярний огляд та вдосконалення заходів щодо забезпечення безпеки з метою впровадження нових технологій і своєчасної модернізації програм, що використовуються банком.
3.	Організація процесу всебічного нагляду за взаємодією з партнерами, які забезпечують процес надання певних видів електронних банківських послуг	Керівництву банку слід здійснювати постійну оцінку доцільності та ефективності співпраці із компаніями-провайдерами та усвідомлювати пов'язані з аутсорсингом ризики. Також якісно оцінювати рівень професіоналізму і фінансового становища цих компаній та чітко прописувати межі відповідальності, план заходів у надзвичайних ситуаціях та частоту аудиторських перевірок з позиції ефективності управління ризиками обох сторін при укладанні контрактів.

Джерело: сформовано автором на основі [3]

ної системи ризик-менеджменту електронного банкінгу сформував 14 основних принципів управління ризиками у сфері електронного банківського обслуговування. Сформовані принципи управління ризиками електронного банкінгу згруповані у три групи:

- А. Нагляд з боку вищого керівництва банку (принципи 1-3);
- В. Управління безпекою (принципи 4-10);
- С. Управління правовим та репутаційним ризиками (принципи 11-14).

Перша група ***А. Нагляд з позиції вищого керівництва банку***, яка включає перші три принципи (табл. 1), спрямована на регулювання дій Ради Директорів та Правління банку з позиції розроблення чітких стратегічних бізнес-планів стосовно впровадження електронного банкінгу та їх інтеграцію і узгодження із загальнокорпоративними стратегічними цілями банківської установи. Крім того, вище керівництво банку повинно забезпечити процес аналізу ризиків функціонування електронного банкінгу та побудувати ефективну систему контролю та моніторингу цих ризиків, а також розробити методи безперервної оцінки ефективності впровадження електронного банківського обслуговування банком.

Друга група ***В. Управління безпекою***, що акумулює сім принципів (табл. 2), описує дії

Таблиця 2

Принципи групи В. Управління безпекою

№	Назва принципу	Короткий зміст
4.	Ідентифікація клієнтів електронного банкінгу	Банківська установа, яка здійснює обслуговування клієнтів у електронному режимі повинна: 1) вжити заходів для побудови ефективного процесу ідентифікації клієнта (засвідчення справжності особи, що здійснює транзакцію online) та його авторизації (встановлення легітимності доступу цієї особи до банківського рахунку або наявності у нього права на проведення операцій за рахунком) у системі електронного банкінгу; 2) ретельно контролюватись процес підключення до системи (для уникнення несанкціонованого доступу); 3) здійснювати повторну ідентифікацію у разі збоїв web-сеансів.
5.	Недопущення відмови проведення фінансових операцій через канали електронного банкінгу та відповідальність за їх виконання.	Банківська установа повинна забезпечити процес проведення фінансових операцій клієнтами не допускаючи відмов у їх здійсненні, тому важливим є розробити секретні та відкриті ключі для кожного клієнта. За допомогою секретного ключа генерується цифровий підпис і зашифровується текст, а за допомогою відкритого – здійснюється розшифровка і перевірка справжності документа. Банк може самостійно це здійснювати, або передати це партнерам (в останньому випадку необхідно вибирати такі організації, які забезпечують той же рівень ідентифікації, що і банк).
6.	Належні заходи для забезпечення розмежування функцій	Між банківськими працівниками повинен існувати чіткий розподіл функцій при роботі у системах електронного банкінгу, базах даних та прикладних програмах. Права на ініціацію, авторизацію і завершення транзакції повинні розмежовуватись між працівниками чи партнерами. Різні працівники повинні збирати та перевіряти інформацію на цілісність і т. д. Банк повинен унеможливити нехтування цим принципом.
7.	Ефективний контроль за авторизацією в системах електронного банкінгу, базах даних та прикладних програмах.	Головна ціль даного контролю – забезпечити та гарантувати цілісність та збереженість баз даних, які містять інформацію про права на авторизацію та доступ до проведення тих чи інших операцій, оскільки неефективний контроль за розподілом функцій між працівниками (розподілення прав на авторизацію та доступ) збільшує ймовірність несанкціонованого доступу до баз даних.
8.	Забезпечення повноти даних про транзакції каналами електронного банкінгу, реєстрації цих даних, а також іншої інформації.	Всі процеси, що здійснюються у системі електронного банкінгу повинні бути стійкими до злому та несанкціонованих змін. Банківська установа повинна розробити чіткий процес їх моніторингу та контролю для забезпечення цілісності даних. Цей принцип особливо актуальний в умовах модернізації програмного забезпечення банку.
9.	Введення точного хронологічного простежування фінансових операцій електронного банкінгу.	Служба внутрішнього контролю банку повинна здійснювати періодичний аудит операцій, що здійснюються в електронній формі. Найбільш важливим є процес аудиту операцій: відкриття, зміна і закриття клієнтського рахунку; проведення операцій, що показують зміни на балансі рахунку; оформлення заяв на збільшення раніше обумовленого з клієнтом ліміту; надання, модифікація або анулювання права на доступ до системи електронного банкінгу.
10.	Збереження конфіденційності ключової банківської інформації	Банки повинні вжити заходів для забезпечення конфіденційності ключової банківської інформації, яка передається через системи електронного банкінгу і/або зберігається у базах даних, від доступу третіх осіб. Розроблені банком стандарти щодо збереження конфіденційності інформації слід використовувати і в організаціях, які залучаються до надання електронних послуг. Всі випадки доступу до такого роду даних необхідно реєструвати, а зареєстрованим файлам потрібно надати підвищену стійкість до розкрадань і спотворень.

Джерело: сформовано автором на основі [3]

та обов'язки спеціалістів, які безпосередньо забезпечують процес функціонування електронного банківського обслуговування у банківській установі в контексті забезпечення безпеки банку та його клієнтів.

Третя група ***С. Управління правовим та репутаційним ризиками*** акумулює в собі з 11 по 14 принципи (табл. 3), які описують рівень відповідальності банківської установи перед клієнтом (захист його приватної та конфіденційної інформації від третіх осіб) та спрямовані на формування довіри клієнтів до банківської установи, яка використовує систему електронного банкінгу.

Варто зазначити, що основна частина розроблених принципів спрямована на управління безпекою, яка стає особливо уразлива в умовах запровадження інформаційних систем у процес функціонування банківської установи. За даними дослідження «Лабораторії Касперського», банківські установи України та Росії протягом року в середньому зазнають від 10 до 20 хакерських атак, які спрямовані на дестабілізацію банківської установи та викрадення фінансових ресурсів клієнтів банку, тільки у І півріччі 2017 року відбулось 10 хакерських атак [4]. Найбільш масштабна була у кінці червня 2017 року – Атака вірусу-шифрувальника Petya, яка дестабілізувала роботу більше, ніж десяти державних установ України та банків. У світі постраждало понад 60 країн, збитки від вірусу Petya досягають 8 млрд доларів.

Іншою актуальною загрозою для банківських клієнтів є фішинг (вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів банку (номер карти, термін дії карти, тризначний код безпеки зі зворотного боку картки (код CVV2/CVC2), а також код з банківських смс-повідомлень.). Зростання кількості фішингових веб-ресурсів – це проблема «світова», тобто стосується всіх країн, а не тільки України. За даними Anti-Phishing Working Group (міжнародної організації із захисту кібербезпеки), зростання числа фішингових сайтів склало 65% (у період з 2015 по 2016 рік) [5]. Це виявився «рекордний» показник, який перевищив всі попередні. В Україні кількість шахрайських сайтів у 2016 році зросла в 4,5 рази (174 фішингових ресурсу у 2016 році проти 38 – у 2015 році) [6].

Ще одна сфера підвищеного ризику – банкомати. Причому, лише 19% банків стурбовані загрозою атак на них, у той час, як у 2016 році обсяг шкідливого програмного контенту для банкоматів виріс на 20% у порівнянні з 2015 роком. За інформацією «Лабораторії Касперського» у середньому банки у рік на кібербезпеку витрачають 58 млн.

Таблиця 3

Принципи групи С. Управління правовим та репутаційним ризиками

№	Назва принципу	Короткий зміст
11.	Розкриття необхідної інформації стосовно електронних банківських послуг	Банківська установа повинна на власному сайті у відкритому доступі розмістити адекватну інформацію про банк: назва банку та фізичне розташування головного офісу та відділень; інформацію про членів Правління банку; інформація про зворотній зв'язок з банком у питаннях обслуговування, надсилання скарг та пропозицій; інформація про систему електронного банкінгу; інформація про політику конфіденційності клієнтів та захист клієнтської інформації; інформація про страхування депозитів і т. д. На сайті повинна зображатися інформація, яка допоможе сформувати клієнту позитивну думку про банківську установу.
12.	Збереження таємниці інформації про клієнта	Ключовою відповідальністю банківської установи перед клієнтом є збереження його конфіденційної інформації. База даних інформації про клієнтів, що накопичується банком у процесі надання онлайнових послуг, повинна відповідати всім вимогам законодавчих актів про збереження приватної інформації клієнтів тих держав, на території яких функціонує електронний банкінг. Провайдери, з якими співпрацює банк, також повинні дотримуватись цих стандартів. Банк зобов'язаний дати своїм вкладникам і позичальникам право забороняти передачу відомостей про себе третім особам, які бажають використовувати їх у маркетингових цілях.
13.	Підтримання системи електронного банкінгу в режимі експлуатаційної готовності	Банки повинні забезпечити безперервний процес надання обслуговування через різні форми електронного банкінгу та розробити план дій для підтримки роботи системи в критичних умовах, тому банківським установам потрібно: забезпечити безперебійну подачу потужного рівня електроенергії та використовувати потужні сервери для обробки даних; постійно оцінювати та переоцінювати рівень потужності електромереж необхідних для якісного функціонування електронного банкінгу та здійснювати прогноз в динаміці; системи слід періодично випробовувати на стійкість до стресових ситуацій та атак.
14.	Створення ефективного механізму реагування на неочікувані інциденти	Плани реагування на неочікувані інциденти повинні містити наступну інформацію: методи виявлення негативного інциденту (зовнішньої чи внутрішньої атаки) та рівня загроз; шляхи відновлення функціонування систем електронного обслуговування; шляхи взаємодії банку з клієнтами та засобами масової інформації; взаємозв'язок з керівництвом банку та регулятором банківської системи; формування команди для ліквідації інциденту та наслідків; збір та аналіз інформації про кризову ситуацію після її ліквідації та притягнення до відповідальності винних осіб.

Джерело: сформовано автором на основі [3]

доларів, це втричі більше, ніж витрати нефінансових установ на забезпечення кібербезпеки [4].

Ці статистичні дані красномовно підкреслюють необхідність побудови системи управління ризиками електронного банкінгу, тобто банківська установа повинна мати конкретний відділ, основними функціями якого буде ідентифікація, оцінка, управляння, контроль та моніторинг ризиками електронного банкінгу, ймовірність яких буде зростати відповідно до рівня впровадження інформаційних технологій у банківський бізнес. Схематично, відповідно до міжнародних рекомендацій, система управління ризиками може бути представленою так: (рис. 2).

Побудова такої системи дозволить ідентифікувати, управляти та контролювати ризики електронного банкінгу більш ефективно та здійснювати заходи з їх нівелювання, ще до етапу їх виникнення на всіх рівнях функціонування банківської установи. У процесі управління ризиками цієї категорії потрібно чітко та конкретно розмежовувати функції фахівців управління ризиками електронного банкінгу для більш точної та вчасної їх ідентифікації, однак, постійно враховувати їх взаємозалежність.

Розроблена банком система управління ризиками електронного банкінгу повинна обов'язково, відповідно до міжнародних стандартів, забезпечувати: 1) всебічний нагляд та контроль за операціями, що здійснюються через різні канали електронного банкінгу на належний рівень їх безпеки; 2) ретельний контроль процесу ідентифікації та авторизації клієнта у системі електронного банківського обслуговування для уникнення вторгнення в систему третіх осіб; 3) збереження конфіденційних даних клієнта та фінансовий стан його рахунків, а також конфіденційність ключової банківської інформації; 4) забезпечувати безперервне функціонування систем електронного банкінгу та підтримку її функціонування в процесі настання неочікуваних інцидентів.

При розробці та впровадженні системи ризик-менеджменту електронного банкінгу важливо розробити методику оцінки, контролю та нагляду за діями компанії провайдера, що забезпечує функціонування електронного банківського обслуговування, оскільки професіоналізм та фінансовий стан цієї компанії будуть прямо корелювати із якістю функціонування систем електронного банкінгу.

Запропоновані Базельським комітетом з питань банківського нагляду принципи допомагають виявити ключові джерела ризиків електронного банкінгу та сформувати основу ризик-менеджменту цих ризиків. Також аналіз цих принципів, які варто враховувати при розробці методів управління ризиками електронного обслуговування, дозволить оцінити можливість та доцільність для банківської установи впроваджувати електронне банківське обслуговування ще на етапі формування стратегічних цілей банку.

Висновки з проведеного дослідження. В умовах сьогодення, електронне банківське обслуговування є необхідною умовою для утримання конкурентних позицій на ринку банківських послуг, однак, впровадження цих технологій збільшує ймовірність появи банківських ризиків за умов виникнення певних подій чи збоїв у програмному забезпеченні, що ускладнить чи унеможливить здійснення банківських операцій чи послуг клієнтами у дистанційному режимі обслуговування. До ключових ризиків електронного банкінгу прийнято відносити операційний, юридичний, стратегічний, репутаційний та ризик ліквідності. Їх відмінність від звичайних банківських ризиків пов'язана із виникненням абсолютно нових джерел несприятливих подій, які значно розширюють профіль банківських

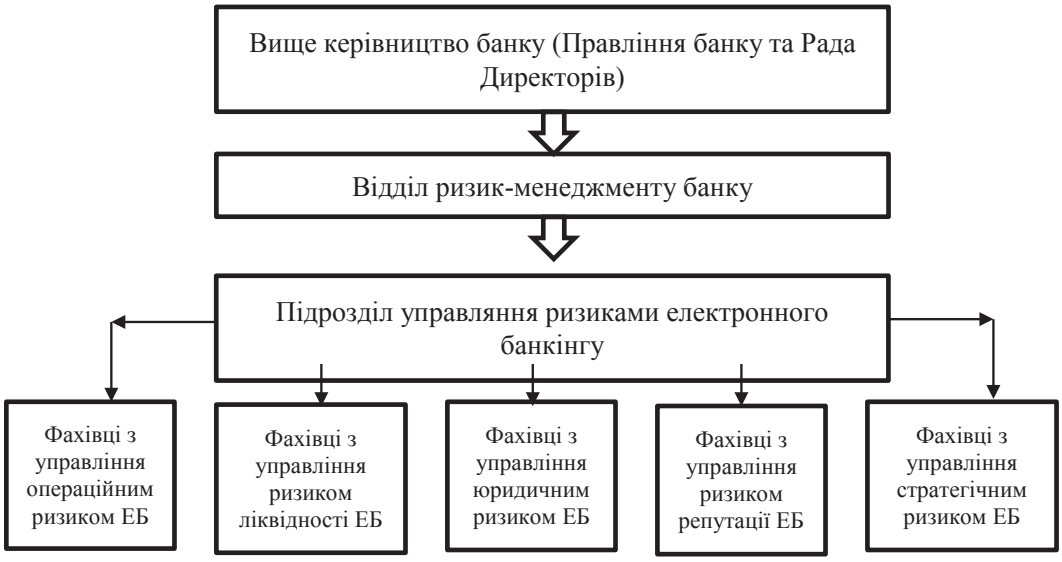

Рис. 2. Ієрархічна система управління ризиками електронного банкінгу

Джерело: сформовано автором

ризиків, внаслідок специфіки електронного обслуговування клієнтів.

Зазначені Базельським комітетом з питань банківського нагляду «Принципи ризик-менеджменту електронного банкінгу» є ключовими у процесі розробки методів та побудови системи управління ризиками електронного банкінгу, що спрямовані переважно на забезпечення інформаційно-технологічної безпеки електронних послуг та мінімізацію пов'язаних з цим ризиків. Однак, сукупність цих правил не є обов'язковою для виконання, проте, всі банківські установи, що займають передові позиції на ринку банківських послуг у розвинених країнах, дотримуються цих вимог. Імплементація цих принципів банківськими установами дозволяє сформувати основний фундамент системи ризик-менеджменту електронного банкінгу для якісного запровадження та розвитку електронного банківського обслуговування. Побудова ефективного процесу управління ризиками електронного банкінгу залишається потенційним напрямом подальших наукових досліджень.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Карчева Г.Т. Теоретичні та практичні аспекти управління ризиками електронного банкінгу / Г.Т. Карчева//Науковий вісник Полісся. – 2015. – № 2(2). – С. 121-126.

2. Ревенков П.В. Актуальные направления регулирования электронного банкинга / П.В. Ревенков, А.Л. Поспелов // Финансы и кредит. – 2015. – № 24(648). – С. 2-13.

3. Risk Management Principles for Electronic Banking. Basel Committee on Banking Supervision, Bank for International Settlements, Basel, July 2003. – 201 p.

4. Офіційний сайт компанії «Лабораторії Касперського» [Електронний ресурс]. – Режим доступу: https://www.kaspersky.ru/

5. Офіційний сайт міжнародної організації із захисту кібербезпеки Anti-Phishing Working Group [Електронний ресурс]. – Режим доступу: http://www.antiphishing.org/

6. Офіційний сайт Української міжбанківської асоціації платіжної системи ЄМА [Електронний ресурс]. – Режим доступу: http://ema.com.ua/payment-market-in-ukraine-infographics-2016/