УДК 336.71.021:[004.73:005.334]

ОПЕРАЦІЙНО-ТЕХНОЛОГІЧНИЙ РИЗИК І ЙОГО ВПЛИВ НА ФІНАНСОВИЙ СТАН СУЧАСНОЇ БАНКІВСЬКОЇ УСТАНОВИ

©2018 **ПРИМАК Ю. Р.**

УДК 336.71.021:[004.73:005.334]

Примак Ю. Р. Операційно-технологічний ризик і його вплив на фінансовий стан сучасної банківської установи

Метою статті є вияв особливостей поняття «ризик банківської діяльності» та класифікація загроз банківській установі в розрізі групи операційно-технологічних ризиків, що здатні активно впливати на фінансовий стан і ділову репутацію банку. Проведено аналіз та оцінку класифікації ризиків банківської діяльності у відповідності до міжнародних і національних нормативів. Розроблено рекомендації щодо оптимізації детермінації ризиків, які віднесено до операційно-технологічної групи. Надано характеристику базовим факторам, які впливають на операційно-технологічні ризики діяльності фінансової установи. Описано динаміку та базові види контролю над кібернетичними загрозами. Визначено головні види та складові кібернетичних атак на програмне забезпечення організації. Виділено основні напрямки по вдосконаленню виявлення та оцінки операційно-технологічних ризиків на основі методики стрес-тестування банків. Цінність статті полягає в актуалізації підходів до класифікації ризиків та пошуку способів отримання більш точних результатів стосовно фінансового стану банку.

Ключові слова: *ризик банківської діяльності, операційно-технологічний ризик, кібернетичні загрози, кіберсередовище, стрес-тестування.*
Рис.: *7.* ***Табл.:*** *1.* ***Бібл.:*** *14.*

Примак Юліана Ростиславівна *– аспірантка, здобувач, кафедра обліку в кредитних і бюджетних установах та економічного аналізу, Київський національний економічний університет ім. В. Гетьмана (просп. Перемоги, 54/1, Київ, 03057, Україна)*
E-mail: *juliana07priviar@gmail.com*

УДК 336.71.021:[004.73:005.334]

Примак Ю. Р. Операционно-технологический риск и его влияние на состояние современного банковского учреждения

Целью статьи является выявление особенностей понятия «риск банковской деятельности» и классификация угроз банковскому учреждению в разрезе группы операционно-технологических рисков, которые способны активно влиять на финансовое состояние и деловую репутацию банка. Проведены анализ и оценка классификации рисков банковской деятельности в соответствии с международными и национальными нормативами. Разработаны рекомендации по оптимизации детерминации рисков, которые отнесены к операционно-технологической группе. Представлена характеристика базовых факторов, влияющих на операционно-технологические риски деятельности финансового учреждения. Описана динамика и основные виды контроля над кибернетическими угрозами. Определены базовые виды и составляющие кибернетических атак на программное обеспечение организации. Выделены основные направления по совершенствованию выявления и оценки операционно-технологических рисков на основе методики стресс-тестирования банков. Ценность статьи заключается в актуализации подходов к классификации рисков и поиске способов получения более точных результатов относительно финансового состояния банка.

Ключевые слова: *риск, операционно-технологический риск, кибернетические угрозы, киберсреда, стресс-тестирование.*
Рис.: *7.* ***Табл.:*** *1.* ***Библ.:*** *14.*

Примак Юлиана Ростиславовна *– аспирантка, соискатель, кафедра учета в кредитных и бюджетных учреждениях и экономического анализа, Киевский национальный экономический университет им. В. Гетьмана (просп. Победы, 54/1, Киев, 03057, Украина)*
E-mail: *juliana07priviar@gmail.com*

UDC 336.71.021:[004.73:005.334]

Prymak Ju. R. The Operational-Technological Risk and its Impact on the Status of a Contemporary Banking Institution

The article is aimed at identifying peculiarities of the concept of «risk of banking activity» and classification of threats to a banking institution in the context of a group of the operational-technological risks, which are able to actively influence the financial condition and business reputation of a bank. An analysis and an evaluation of the classification of risks of banking activity in accordance with international and national regulations are carried out. The recommendations on optimization of determination of the risks which are assigned to the operational-technological group are elaborated. A characterization of the basic factors influencing operational-technological risks of activity of financial institution is presented. The dynamics and main types of control over cyber threats are described. The basic types and components of cybernetic attacks on the software of organization are defined. The main directions on improvement of detection and estimation of operational-technological risks on the basis of methods of stress-testing of banks are allocated. The value of the article consists in updating the approaches to classifying risks and finding ways to obtain more accurate results regarding the bank's financial condition.

Keywords: *risk, operational-technological risk, cyber threats, cyberenvironment, stress testing.*
Fig.: *7.* ***Tbl.:*** *1.* ***Bibl.:*** *14.*

Prymak Juliana R. *– Graduate Student, Applicant, Department of Accounting in Credit and Budgetary Institutions and Economic Analysis, Kyiv National Economic University named after V. Hetman (54/1 Peremohy Ave., Kyiv, 03057, Ukraine)*
E-mail: *juliana07priviar@gmail.com*

Сучасні процеси глобалізації та розвитку науково-технологічного прогресу зумовлюють необхідність адаптації українських банківських установ до рівня міжнародних фінансових відносин. Міжнародні інтеграційні процеси здійснюються із застосуванням базових принципів та форм зовнішньоекономічних зв'язків, а саме: провадження активної підприємницької діяльності, здійснення операцій торгівлі товарами та послугами, міжнародне співробітництво. Під впливом глобальних процесів пропорційно зростає обсяг і масштаби кризових явищ та дестибілізаційних впливів на фінансовий сектор економіки, ефективний контроль та моніторинг яких здатні стабілізувати фінансовий стан і підтримати імідж банку.

При реалізації банківських продуктів розмір збитків від виникнення ризику відрізняється залежно від його виду. Оскільки банківська діяльність, порівняно з іншими видами підприємництва, характеризується підвищеним рівнем вразливості до негативних

факторів, банківські установи потребують постійного вдосконалення відповідної системи управління та попередження вірогідних загроз, шляхом вдосконалення ризик-менеджменту та застосування концепції корпоративного управління.

Цифровізація та впровадження в банківських установах сучасних інформаційних технологій зумовила зростання рівня операційно-технологічного ризику, тому відстеження особливостей моніторингу та управління саме цією групою ризиків зумовлює актуальність обраної теми дослідження.

Дослідженням у сфері класифікації ризиків банківської діяльності та провадження дієвого ризик-менеджменту з метою підтримки достатнього рівня фінансової стійкості та іміджу фінансових організацій, присвячують свої роботи такі вітчизняні та закордонні вчені, як: Данілова Л. [7], Каднічанська В. [8], Криклій О. [9], Крухмаль О. [9], Заднепровська С. [13], Торяник Ж. [8], Манжос С. [11], Парасій-Вергуненко І. [12; 13], Люта О. [10], Волков Д. [6], Школьник І. [10] та ін.

Узагальнюючи цінність результатів проведених раніше досліджень по обраній темі, варто зауважити, що певна кількість питань потребують більш ретельного розкриття та подальшого розвитку. Зокрема, це стосується пошуку сучасних шляхів відстеження та управління операційно-технологічним ризиком банківської діяльності з метою подальшого нівелювання його негативного впливу на банківські установи, а також вияв можливих шляхів попередження та прогнозування в умовах сучасної економічної ситуації.

Метою статті є вияв особливостей характеристики та класифікації загроз банківської діяльності в розрізі групи операційно-технологічних ризиків та аналіз впливу як його традиційних складових, так і абсолютно нових різновидів на фінансовий стан банку.

Виходячи з мети дослідження виокремлено такі *завдання*:

- визначення поняття «ризик» та охарактеризувати головні види ризиків банківських установ на основі аналізу міжнародних і національних положень;
- надання характеристики поняття «операційно-технологічного ризику» на основі огляду останніх публікацій та досліджень в цьому напрямку;
- детермінування основних факторів, що впливають на операційно-технологічний ризик та виділити нові загрози банківській діяльності;
- виявлення базових елементів загроз, що виникають у процесі провадження діяльності в умовах кібернетичного середовища;
- пошук шляхів мінімізації та моніторингу операційно-технологічного ризику з використанням методу стрес-тестування.

На сьогоднішній день не існує загальноприйнятого визначення поняття «ризик банківської діяльності». Це твердження підтримують у своїй роботі Каднічанська В. М., Торяник Ж. І. та Зорянський В. А., які відзначають, що розбіжності простежуються навіть із нормативно-правового боку [8, с. 72].

Ризик у загальному тлумаченні – це неминуча загроза, що виникає в ході провадження будь-якої діяльності.

Парасій-Вергуненко І. М. відзначає, що під банківським ризиком розуміють можливість зазнати втрат у разі виникнення несприятливих для банку обставин [12, с. 178].

Відповідно до визначення НБУ ризик банківської діяльності (*banking risks*) – це ймовірність того, що події, очікувані або неочікувані, можуть мати негативний вплив на капітал та/або надходження банку [14]. Відповідно банківські ризики класифікують на групу прямих (зменшення або втрата доходів, зростання збитків чи знецінення капіталу) та непрямих ризиків (опосередкований негативний вплив на банківську діяльність шляхом накладення відповідних обмежень та санкцій або виникнення несприятливих економічних умов на рівні країни чи світу). Але це не виключна класифікація ризиків, що здатні впливати на банк.

Волков Д. П. стверджує, що при дослідженні поняття «банківський ризик» у більшості випадків науковці намагаються адаптувати визначення категорії «ризик» до специфічних умов його виникнення в банківській діяльності [6, с. 134].

Вперше групи банківських ризиків були чітко окреслені в Угоді про капітал, що згодом отримала назву Базель I, у 1988 р. Подальший розвиток банківської системи світу зумовив необхідність удосконалення даної Угоди, тому у 2005 р. була оприлюднена «Міжнародна конвергенція вимірювання капіталу та стандартів капіталу: нові підходи» [4], відома як Базель II. Вже у 2010 р. був прийнятий Базель III, який містив певні доповнення до попередніх частин, водночас не відміняючи їх дію [5]. Відповідно до класифікації, яка наведена в базельських Угодах, виділено такі групи ризиків (*рис. 1*).

З метою здійснення банківського нагляду Національний банк на основі тверджень, запроваджених Базельським комітетом, виділив дев'ять категорій ризику, а саме: кредитний ризик, ризик ліквідності, ризик зміни процентної ставки, ринковий ризик, валютний ризик, операційно-технологічний ризик, ризик репутації, юридичний та стратегічний ризики [2]. При цьому кожна з цих категорій має відповідні підкатегорії, які можуть діяти самостійно, завдаючи збитків фінансовій організації (*рис. 2*).

Класифікація, розглянута на рис. 1 і рис. 2, не є оптимальною, оскільки в процесі свого існування та активного впливу з боку як суспільства, так і науково-технологічного прогресу, банківські установи під-

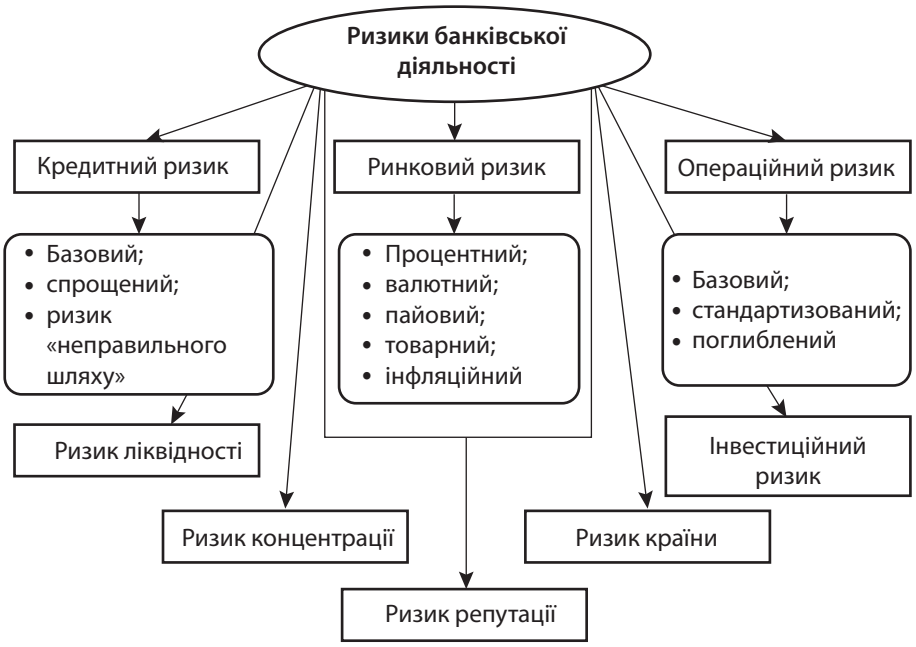

Рис. 1. Класифікація ризиків банківської діяльності

Джерело: авторська розробка на основі [4; 5; 10, с. 166].

даються впливу все більшої кількості різноманітних ризиків.

Як видно з рис. 2, однією з найбільших груп ризиків є операційно-технологічні. Відповідно до визначення Базельського комітету операційний ризик – це ризик збитків у результаті неадекватних або невдалих внутрішніх процесів, людей і систем або зовнішніх подій. Це визначення включає юридичний ризик, але виключає стратегічний ризик і ризик репутації [3, с. 34]. Відповідно, головні складові групи операційного ризику в міжнародному та національному тлумаченні відрізняються. Це також стосується базових складових, що віднесені до цієї групи: 1) процеси; 2) людський фактор; 3) системи/технології; 4) зовнішні події [9].

На операційно-технологічні ризики діяльності здійснюють вплив певні фактори. Їх склад може бути змінений залежно від потреб і цілей фінансового аналізу. На основі даних постійно діючої системи внутрішнього контролю ризиків забезпечується визначення сукупної оцінки та створюються умови для подальшого прийняття ефективних управлінських рішень. Загальний перелік факторів, на основі яких може бути визначений рівень операційно-технологічного ризику, наведено на *рис. 3*.

З розвитком науково-технологічного прогресу та комп'ютерних технологій зростає ймовірність виникнення загроз абсолютно нового типу. Ці загрози на поточний момент відносять до групи операційно-технологічних ризиків, хоча негативні фактори безпосередньо пов'язані з інформаційною, інтелектуальною та інтерактивною безпекою фінансової організації та потребують виокремлення в окрему категорію. Це необхідно, оскільки відстеження, контроль та усунення кібернетичних ризиків вимагають запровадження ряду нових методів по збереженню фінансової стійкості банку.

На сьогоднішній день виокремлюють такі базові складові системи контрою над операційно-технологічними ризиками:

- політику контролю за операційно-технологічним ризиком;
- процедури й засоби контролю за операційно-технологічним ризиком (дотримання облікової політики, особливості функціонування інформаційних систем, програми управління тощо);
- технологічні схеми продуктів та послуг банку;
- розгалуженість інфраструктури банку;
- запровадження дієвої системи внутрішнього контролю та інформаційної безпеки банку;
- забезпечення надійного позаофісного зберігання всіх важливих резервних документів і файлів банку.

О. Криклій також відзначає, що у зв'язку з початковою стадією інтеграції концепції управління операційними ризиками в українську банківську систему етап ідентифікації/збору інформації про ризики є наразі чи не основним реалізованим етапом управління ними [9].

Для подолання та попередження можливих кібернетичних загроз у банківській установі має бути створений відділ, що безпосередньо займається інформаційною безпекою установи. Цілі інформаційної безпеки – встановлення відповідних функцій та рівнів безпеки, певних вимог до внутрішніх і зовнішніх комунікацій організації тощо. Актуальність інформаційної безпеки проілюстровано в *табл. 1*, яка відо-

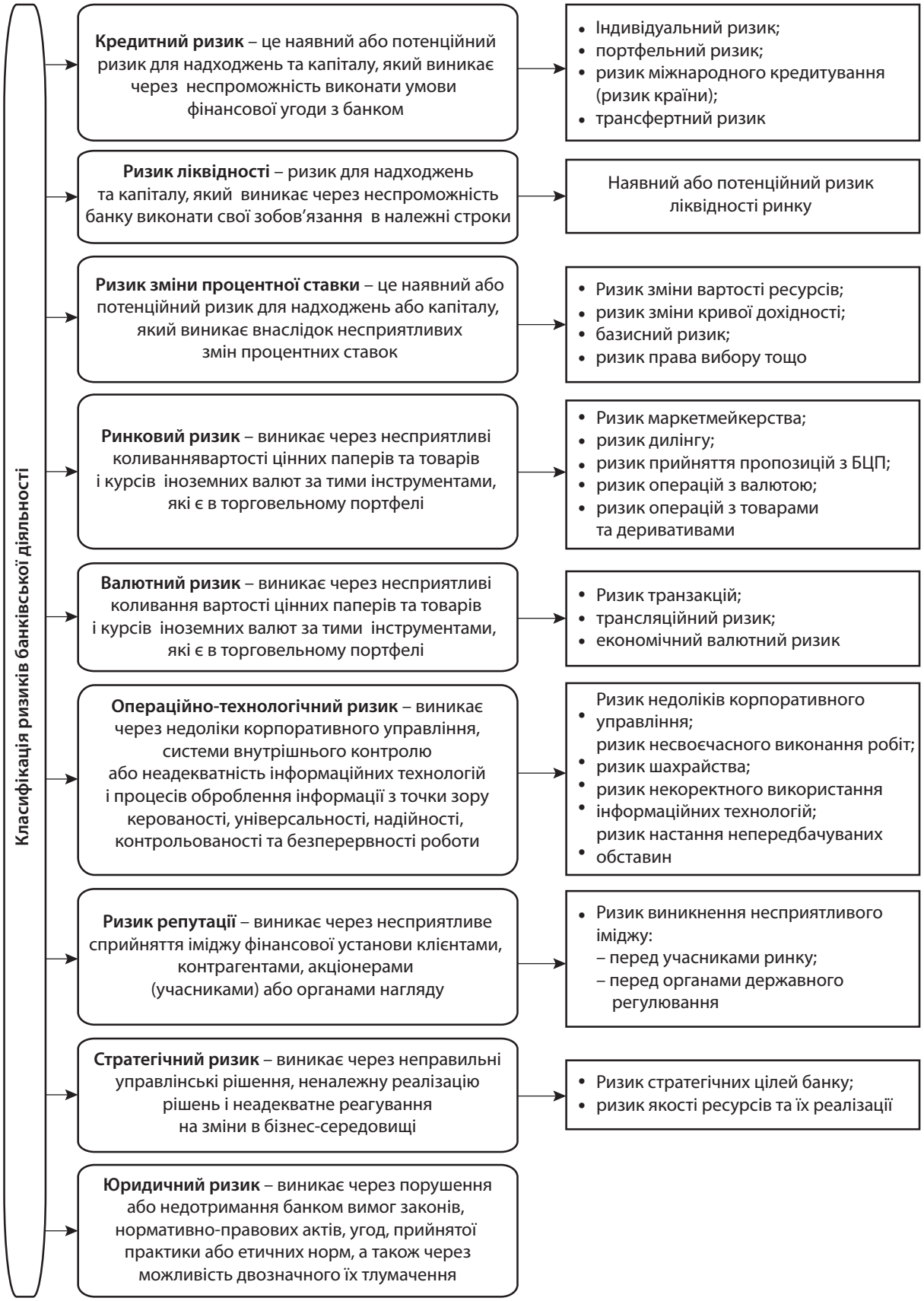

Рис. 2. Класифікація ризиків банківської діяльності у відповідності до тлумачення НБУ

Джерело: авторська розробка на основі [2; 14].

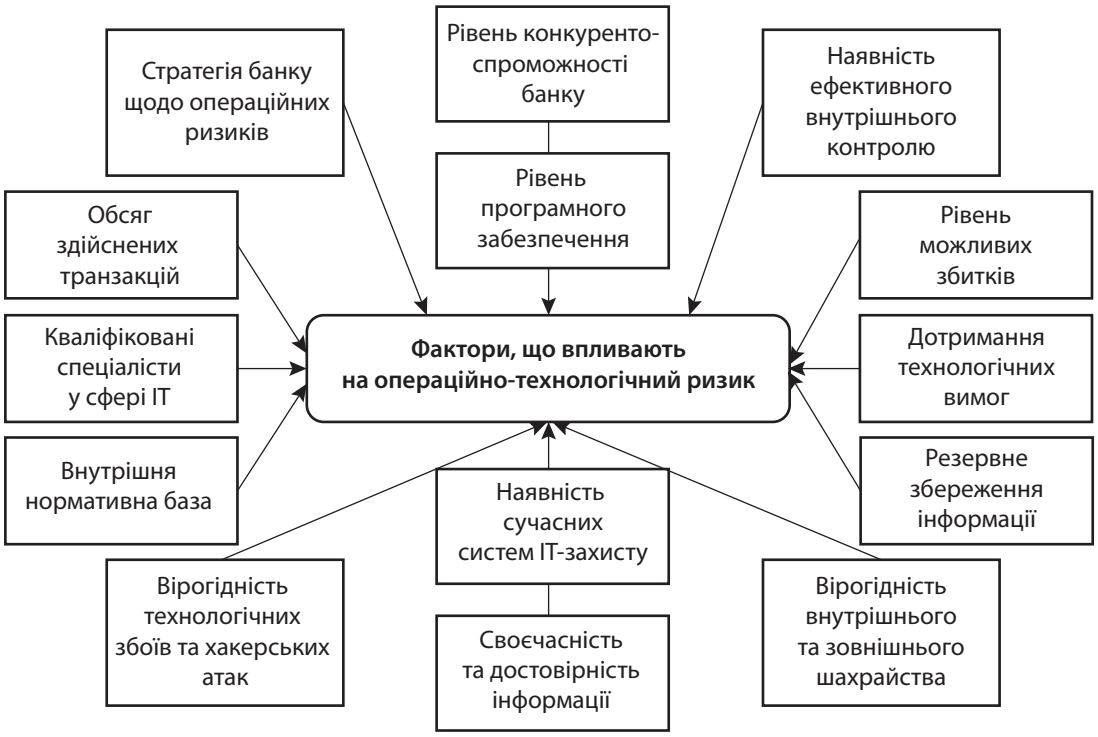

Рис. 3. Фактори, які безпосередньо впливають на групу операційно-технологічних ризиків

Джерело: авторська розробка на основі [13].

бражає зростання кількості вірусних атак, здійснених протягом останніх років.

Головними принципами забезпечення безпеки кіберсередовища є такі:

- середовище, в якому діє банк, є ворожим;
- підтримання постійної ешелонованої оборони інформаційних систем (включає фізичну безпеку, велику кількість точок доступу; аналітичні ПО; багатоступінчату систему безпеки);
- ізоляція окремих елементів системи від масового доступу;
- збереження, резервування та накопичення історичних даних;
- систематичний аналіз та перевірка основних місць ураження.

Метою проведення систематичного аналізу та перевірки основних місць ураження є пошук та оцінка всіх відомих слабких місць інформаційних систем установи. Ці заходи підтримують та актуалізують програмне забезпечення задля виявлення нетипових явищ у системі, незвичайної мережевої активності (вхід у систему «не в той час», дії з незрозумілою кінцевою метою), внутрішні зміни (перевантаження мережі, зміни в регістрах та іменах користувачів тощо), попередження інтервенції в мережу тощо. У результаті стає можливим отримання переліку найбільш уразливих місць, які першими можуть постраждати в разі дії операційно-технологічного ризику.

Головними видами контролю програмного забезпечення та інформаційних систем банківської установи є: моніторинг; розподіл повноважень між адміністраторами; управління ризиковими точками; створення резервних (офлайн) копій; ство-

Таблиця 1

Динаміка кібератак, які були здійснені в Україні протягом 2014–2017 рр.

Рік	Назва вірусу	Період здійснення атаки	Об'єкт ураження
2014	DDOS	26.05.2014 р.	Вибори Президента України
2015	BlackEnergy	15.12.2015 р.	Прикарпаття обленерго
2016	APT	02.–06.2016 р.	SWIFT-Банки
		17.12.2016 р.	Укренерго
2017	WannaCry	12.05.2017 р.	Віруси масового ураження
	XData	18.05.2017 р.	
	Petya / Nyetya	27.06.2017 р.	
	BadRabbit	24.10.2017 р.	Підприємства транспортної галузі

рення дієвої організаційної структури; запровадження новітніх систем шифрування; ведення відповідного документообігу.

Як додаткові засоби безпеки інформаційних систем банку, якщо неможливе застосування паролів або певного програмного забезпечення, використовують засоби додаткового контролю: білий список процесів; виключення з домену; захист на системному рівні; контроль інтернет-трафіку; ручний контроль операцій «входу/виходу».

Залежно від мети та рівня складності кібератаки поділяються на чотири основні види: ті, що здійснюються дилетантами, хакерами, інсайдерами та АСД (атаки, спровоковані державою) (*рис. 4*).

ризиком, сукупний ризик і напрям ризику. Для ефективного використання системи оцінки ризиків наглядовці мають враховувати як поточний стан банку, так і фактори, які можуть вказувати на зростання ризиків. Згідно із системою оцінки ризиків існує чотири основні компоненти визначення параметрів ризику банку: кількість ризику, тобто рівень або обсяг ризику; якість управління ризиком; сукупний ризик; напрям ризику, тобто ймовірна зміна сукупного рівня ризику протягом наступних 12 місяців [2].

НБУ, окрім переліку відповідних факторів операційно-технологічного ризику, також надає перелік кількісних параметрів, за допомогою яких визначається його обсяг.

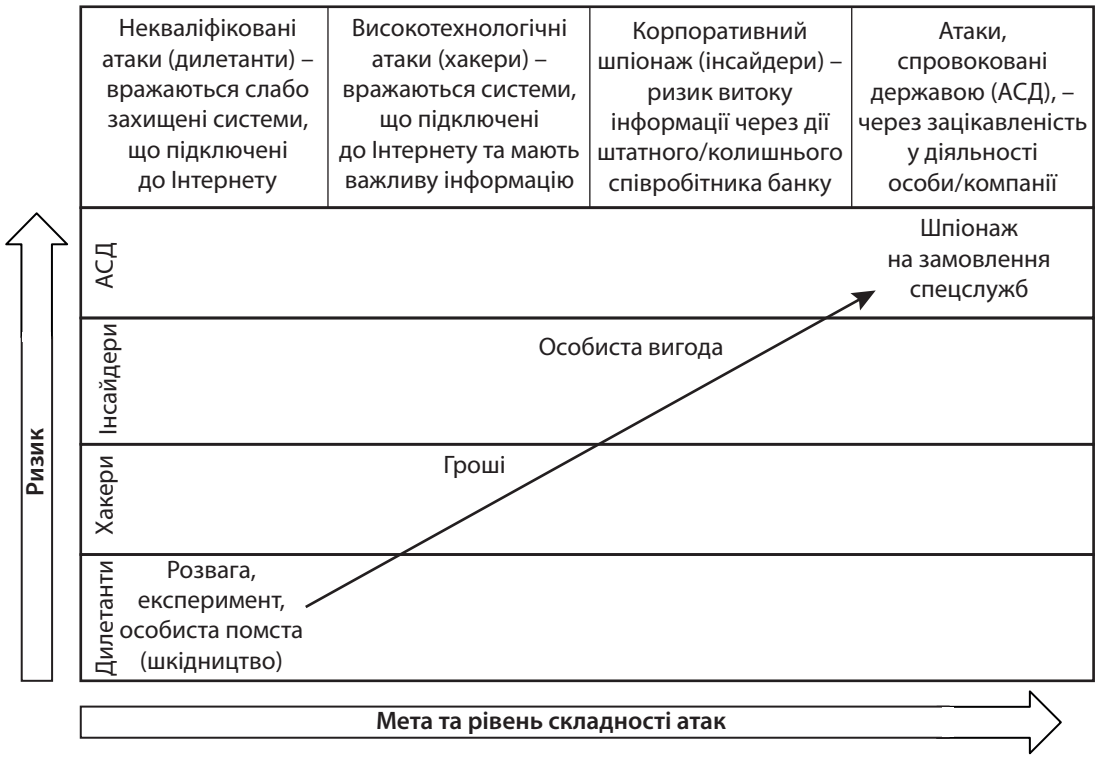

Рис. 4. Класифікація атак залежно від рівня складності

У результаті ураження системи атакою з використанням кібернетичних технологій можливі такі наслідки: крадіжка особистих даних і коштів; крадіжка особистих даних і коштів клієнтів; шантаж; ураження та паралізування роботи системи; втрата фінансових коштів та репутації; втрата сервісу або його можлива деградація; санкції з боку держави.

У загальному вигляді кібератаки мають такі етапи: розвідка; первинне зараження та проникнення; закріплення; отримання прав доступу; внутрішня розвідка та просування; досягнення цілі атаки; знищення слідів зламу.

Для шести категорій банківського ризику – кредитного ризику, ризику ліквідності, ризику зміни процентної ставки, ринкового ризику, валютного ризику та операційно-технологічного ризику – наглядовці оцінюють кількість ризику, якість управління

11.06.2018 р. НБУ була прийнята Постанова № 64 «Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах», відповідно до якого банківські установи Україні зобов'язані у відповідні терміни запровадити систему управління ризиками, яка відповідала б вимогам Постанови.

Банк організовує систему управління ризиками, яка ґрунтується на розподілі обов'язків між підрозділами банку із застосуванням моделі трьох ліній захисту:

1) *перша лінія* – на рівні бізнес-підрозділів банку та підрозділів підтримки діяльності банку. Ці підрозділи приймають ризики та несуть відповідальність за них, а також подають звіти щодо поточного управління такими ризиками;

2) *друга лінія* – на рівні підрозділу з управління ризиками та підрозділу контролю за дотриманням норм (комплаєнс);

3) *третя лінія* – на рівні підрозділу внутрішнього аудиту щодо перевірки та оцінки ефективності функціонування системи управління ризиками.

Система управління ризиками банку щонайменше має передбачати:

1) організаційну структуру з чіткими обов'язками та повноваженнями;

2) культуру управління ризиками та кодекс поведінки (етики);

3) внутрішньобанківські документи з питань управління ризиками;

4) інформаційну систему щодо управління ризиками та звітування;

5) інструменти для ефективного управління ризиками [1].

Однією з базових функцій підрозділу управління ризиками є проведення стрес-тестування. У процесі аналізу фінансового стану банківської установи стрес-тестування є одним з провідних методів для оцінки реальних операційно-технологічних ризиків діяльності (*рис. 5*).

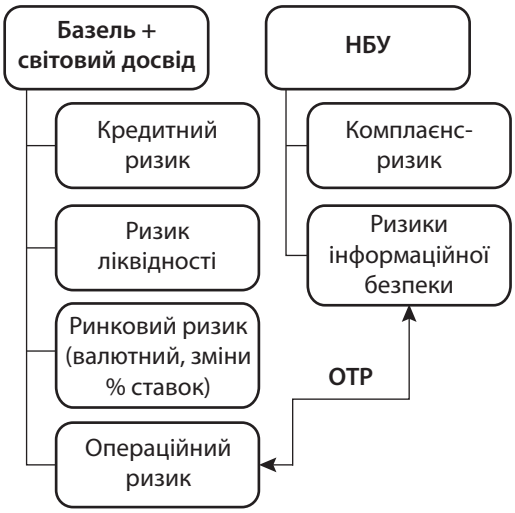

Рис. 5. Види ризиків, що аналізуються з використанням методу стрес-тестування

Джерело: авторська розробка на основі [5, с. 50; 7, с. 248].

Метою проведення стрес-тестування є кількісна та якісна оцінка ризиків, удосконалення системи внутрішнього контролю та визначення спроможності банківської установи протистояти потрясінням на фінансовому ринку, що можуть виникнути в майбутньому. Етапами для проведення стрес-тестування є:

1) ідентифікація – класифікація за класом виникнення (Кредитний/ Ринковий/ Операційний/Ліквідності/Комплаєнс);

2) аналіз та оцінка якісна/кількісна;

3) запланований комплекс заходів щодо управління ризиками.

На *рис. 6* відображено головні різновиди стрес-тестів, які використовуються при проведенні аналізу банківської установи. Кожний з цих видів мають свої переваги та недоліки.

Найбільш поширеними методами здійснення агрегованого стрес-тестування є сценарний аналіз (сценарій) і аналіз чутливості (чутливість). Існує декілька видів сценаріїв: базовий сценарій (у рамках найбільш імовірних змін факторів ризику); негативний сценарій розвитку (в рамках заданих змін факторів ризику, які відповідають досить імовірним подіям; максимально негативний сценарій розвитку (в рамках одночасної зміни ряду факторів ризику, які відповідають настанню екстремальних, але разом з тим імовірних подій.

Ефективність сценарного аналізу залежить від професіоналізму та підготовки експертів. Експертні припущення та судження є неформалізованими, однак дуже вагомими складовими сценарію. У зв'язку з багатогранністю та складністю економічних процесів спеціалісти змушені оперувати загальними закономірностями та тенденціями з урахуванням історичних взаємозв'язків і спиратися на власні спостереження та досвід.

Стрес-тестування може базуватися на історичних сценаріях з використанням варіантів подій, що мали місце в минулому, або на гіпотетичних сценаріях, з використанням варіантів подій, які не відбувалися, але теоретично можуть статися. За наявності певного ряду історичних даних можна розрахувати вірогідний діапазон можливих змін за допомогою методу математичної статистики. Якщо історичних даних немає, то ймовірність змін доцільно визначати гіпотетично.

Приклади факторів, які можуть вимагати коригування історичних сценаріїв, включають в себе: 1) демографічні зміни/міграція/еміграція; 2) нові технології, наприклад комп'ютери та Інтернет; 3) глобалізація/більш тісно пов'язані фінансові ринки; 4) нові класи активів; 5) використання різних підходів до оцінки; 6) вплив ЗМІ на політику; 7) зміни кон'юнктур ринкового та законодавчого секторів.

Дані по економічних кризах, що відбулися в минулому, необхідно коригувати та адаптувати до умов сьогодення, оскільки вони рідко повторюються в тому вигляді, у якому траплялися раніше. Вибір сценаріїв залежить від багатьох факторів та має враховувати взаємозв'язок між історичною подією та конкретною банківською установою.

Якщо історичні сценарії не можуть врахувати певних факторів ризику, то доцільно використовувати гіпотетичні сценарії. Перевагами такого виду сценаріїв є можливості гнучкішого формулювання можливих криз.

Рис. 6. Види стрес-тестів та їх основні недоліки

Джерело: складено за [11, с. 190–191].

Переваги стрес-тестування: передбачає тільки суттєві зміни факторів; під час розрахунку результативних показників ураховується більшість базових факторів ризику; дозволяює отримати правдоподібні, на думку експертів, прогнозовані події із заданою ймовірністю їх виникнення; забезпечує можливість визначення найгіршого сценарію розвитку подій; установлює розмір можливих збитків у випадку реалізації найгіршого сценарію; виявляє вразливі та слабкі місця в системі захисту від ризиків; дає можливість керівництву оперативно втручатись у процеси, які загрожують банку.

Базовими етапами для проведення стрес-тестування є:

1) Актуалізація параметрів для стрес-тестування.

2) Розроблення моделі стрес-тестування шляхом визначення основних факторів ризику та результативних показників і критеріїв.

3) Проведення стрес-тестування.

4) Трактування результатів і підготовка висновків щодо проведеного стрес-тестування.

У результаті проведеного аналізу управлінському персоналу банку надається звіт про результати стрес-тестування: професійне (мотивоване) судження, що містить оцінку впливу можливої реалізації ризиків на діяльність банку. Результати стрес-тестування дозволяють спеціалістам порівнювати вплив різних факторів ризику, визначати важливість різних видів сценаріїв та робити оцінку впливу різних чинників на діяльність банку.

Стрес-тести надають інформацію про зміни характеру факторів ризику та ступеня їх впливу протягом певного часу за умови їх регулярного проведення.

Аналіз результатів стрес-тестування є важливим не тільки з точки зору визначення запасу фінансової стійкості банку, а і з огляду на практичну можливість спостереження та контролю рівня ризиків (особливо операційно-технологічного), які наражають банк на небезпеку, та ідентифікації найбільш серйозних загроз.

Здійснення оцінки якості та адекватності системи стрес-тестування є необхідною умовою практичного використання результатів, отриманих за допомогою стрес-тестування (*рис. 7*).

Відповідно до рис. 7 стає можливим відібрати найбільш дієвий метод стрес-тестування як для окремої банківської установи, так і для групи банків у цілому. Операційно-технологічні ризики в більшості випадків оцінюють разом з іншими факторами впливу, оцінюючи їх взаємну кореляцію та можливі втрати від настання тієї чи іншої події. Але, застосовуючи такий різновид стрес-тестування, як історичний чи гіпотетичний методи, існує значна ймовірність недооцінки загрози з боку кібернетичних ризиків. Тому необхідно розробити та оновити існуючі методологічні підходи до оцінки банку зі збільшенням акценту на оцінці групи операційно-технологічних ризиків діяльності в розрізі цифрових загроз. А також запро-

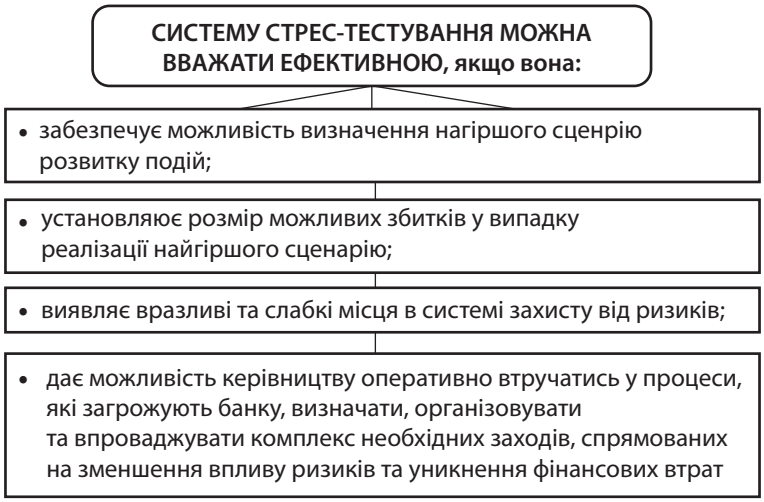

Рис. 7. Базові аспекти ефективності системи стрес-тестування

вадити систематичну оцінку операційно-технологічного ризику на основі стрес-тестування.

ВИСНОВКИ

На основі описаного вище варто зазначити, що від стабільності окремої банківської установи залежить ефективність функціонування банківського сектора країни в цілому. Специфічність банківської діяльності зумовлює виникнення різноманітних ризиків, які пов'язані з дією різноманітних зовнішніх і внутрішніх факторів.

Однією з найбільш широких і впливових груп ризиків є група операційно-технологічних ризиків. Але одна з чотирьох складових, яка включає в себе загрози технологічного, кібернетичного та інформаційного характеру, потребує виокремлення в окрему групу, оскільки стрімкий розвиток сучасних кібернетичних технологій зумовлюють стрімкий розвиток новітніх факторів ризику.

Для детермінації загроз з боку кібернетичної складової операційно-технологічних ризиків одним із найдієвіших методів є стрес-тестування банків. Але для отримання найбільш достовірного прогнозу необхідно пристосувати існуючі засоби стрес-тестування для ефективного аналізу цифрових загроз. ■

ЛІТЕРАТУРА

1. Постанова Правління Національного банку України «Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах» від 11.06.2018 р. № 64. URL: https://bank.gov.ua/document/download?docId=71600453

2. Постанова Правління Національного банку України «Методичні вказівки з інспектування банків «Система оцінки ризиків» від 15.03.2004 р. № 104 (зі змінами та доповненнями). URL: http://zakon3.rada.gov.ua/laws/show/v0104500-04

3. Методологічні роз'яснення до Основних принципів ефективного банківського нагляду / Базельський комітет з питань банківського нагляду. Базель, 2006. 66 с. URL: https://www.bank.gov.ua/doccatalog/document?id=45064

4. Международная конвергенция измерения капитала и стандартов капитала: Уточненные рамочные подходы // Банк международных расчетов. Июнь 2004. 262 с. URL: http://safbd.ru/sites/default/files/basel.pdf

5. Basel III: A global regulatory framework for more resilient banks and banking systems. December 2010. URL: https://www.bis.org/publ/bcbs189_dec2010.pdf

6. Волков Д. П. Аналіз банківських ризиків: основні підходи до визначення. *Економічні науки. Серія : Облік і фінанси*. 2013. Вип. 10 (3). С. 131–139.

7. Данілова Л. І., Савочка В. В. Стрес-тестування в системі ризик-менеджменту банку. *Економічний аналіз.* 2014. Т. 15 (1). С. 244–252.

8. Каднічанська В. М., Торяник Ж. І., Зорянський В. А. Банківські ризики в контексті стійкої діяльності банківських установ. *Вісник Університету банківської справи.* 2015. № 2. С. 70–75.

9. Криклій О., Крухмаль О. Інструментарій оцінки операційного ризику банку. *Економічний аналіз.* 2011. № 1 (9). С. 168–172.

10. Люта О. В., Школьник І. О. Базель II: основні складові та їх характеристика. *Проблеми і перспективи розвитку банківської системи України*.2008. Т. 20. С. 165–171.

11. Манжос С. Б. Стрес-тестування банків: огляд методологій. *Финансы, учет, банки*. 2014. Вып. 1. С. 188–195.

12. Парасій–Вергуненко І. М. Аналіз банківської діяльності : навч.-метод. посіб. Київ : КНЕУ, 2003. 347 с.

13. Парасій-Вергуненко І. М., Заднепровська С. П. Облік, аналіз та аудит операцій з платіжними картами в банківських установах : монографія. Київ : КНЕУ, 2016. 304 с.

14. Офіційне інтернет-представництво Національного банку України. URL: https://bank.gov.ua/control/uk/publish/article ?art_id=123614

Науковий керівник – Парасій-Вергуненко І. М., доктор економічних наук, професор кафедри обліку в кредитних і бюджетних установах та економічного аналізу, факультет обліку та податкового менеджменту, ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана»

REFERENCES

"Basel III: A global regulatory framework for more resilient banks and banking systems. December 2010". https://www.bis.org/publ/bcbs189_dec2010.pdf

Danilova, L. I., and Savochka, V. V. "Stres-testuvannia v systemi ryzyk-menedzhmentu banku" [Stress testing in the system of risk management of the bank]. *Ekonomichnyi analiz.* Vol. 15 (1) (2014): 244-252.

Kadnichanska, V. M., Torianyk, Zh. I., and Zorianskyi, V. A. "Bankivski ryzyky v konteksti stiikoi diialnosti bankivskykh ustanov" [Banking Risks in the Context of Sustainable Activities of Banking Institutions]. *Visnyk Universytetu bankivskoi spravy,* no. 2 (2015): 70-75.

Kryklii, O., and Krukhmal, O. "Instrumentarii otsinky operatsiinoho ryzyku banku" [Instruments for assessing operational risk of a bank]. *Ekonomichnyi analiz*, no. 1 (9) (2011): 168-172.

[Legal Act of Ukraine] (2004). http://zakon3.rada.gov.ua/laws/show/v0104500-04

[Legal Act of Ukraine] (2018). https://bank.gov.ua/document/download?docId=71600453

Liuta, O. V., and Shkolnyk, I. O. "Bazel II: osnovni skladovi ta yikh kharakterystyka" [Basel II: The main components and their characteristics]. *Problemy i perspektyvy rozvytku bankivskoi systemy Ukrainy.* Vol. 20 (2008): 165-171.

"Metodolohichni roziasnennia do Osnovnykh pryntsypiv efektyvnoho bankivskoho nahliadu" [Methodological Explanations to the Basic Principles of Effective Banking Supervision]. Bazelskyi komitet z pytan bankivskoho nahliadu. 2006. https://www.bank.gov.ua/doccatalog/document?id=45064

"Mezhdunarodnaya konvergentsiya izmereniya kapitala i standartov kapitala: Utochnennyye ramochnyye podkhody" [International convergence of capital measurement and capital standards: Refined framework approaches]. Bank mezhdunarodnykh raschetov. http://safbd.ru/sites/default/files/basel.pdf

Manzhos, S. B. "Stres-testuvannia bankiv: ohliad metodolohii" [Stress testing of banks: an overview of methodologies]. *Fynansy, uchet, banky,* no. 1 (2014): 188-195.

Ofitsiinyi sait Natsionalnoho banku Ukrainy. https://bank.gov.ua/control/uk/publish/article?art_id=123614

Parasii-Verhunenko, I. M. *Analiz bankivskoi diialnosti* [Banking analysis]. Kyiv: KNEU, 2003.

Volkov, D. P. "Analiz bankivskykh ryzykiv: osnovni pidkhody do vyznachennia" [Banking Risk Analysis: Basic Approaches to Definition]. *Ekonomichni nauky. Ser. : Oblik i finansy*, no. 10 (3) (2013): 131-139.

Zadneprovska (Polishchuk), S. P., and Parasii-Verhunenko, I. M. *Oblik, analiz ta audyt operatsii z platizhnymy kartamy v bankivskykh ustanovakh* [Accounting, analysis and audit of operations with payment cards in banking institutions]. Kyiv: KNEU, 2016.