УДК 330.4
Гіваргізов І. Г.
ДВНЗ "Київський національний економічний університет ім. В. Гетьмана", м. Київ

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ СТІЙКОГО РОЗВИТКУ БАНКІВ

In the article the basic terms and processes for sustainable development banks and of the banking institution is to ensure the stability and efficiency of the safety components. This paper describes the economic security of the bank, as an important link of bank security, as focused on the main direction of banking activities where concentrated main assets of the bank. Factors taken into account security issues, not only as from external influence on the bank, as well as internal exposure. This paper describes the main requirements to protect the confidentiality, integrity and availability of information assets of the bank, as well as important business processes in information security of banks by building management system for information security. Job analysis information security management system, based on an approach that takes into account business processes, and is designed for the development, implementation, operation, monitoring, reviewing, maintaining and improving information security.

У статті розглянуто основні умови та процеси для забезпечення стійкого розвитку банків та організації роботи банківської установи, що полягає у забезпеченні стабільності й ефективності функціонування складових безпеки. В роботі описано забезпечення економічної безпеки банку, як важливої ланки безпеки банку, оскільки зосереджена на головному напрямі банківської діяльності де сконцентровані основні активи банку. Враховуються фактори проблеми безпеки не тільки як з зовнішнього впливу на діяльність банку, а також і внутрішнього впливу. В роботі описані основні вимоги до забезпечення захисту конфіденційності, цілісності та доступності інформаційних активів банку, а також значення бізнес-процесів в інформаційній безпеці банків за рахунок побудови системи управління інформаційної безпеки. Проаналізовано роботу системи управління інформаційною безпекою, яка базується на підході, що враховує бізнес-процеси, і яка призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Постановка проблеми. Стан банківської системи України і прогнози розвитку на найближче майбутнє змушує усвідомити актуальність таких характеристик та показників для стійкого розвитку банків, як безпека банківської діяльності.

Аналіз останніх джерел досліджень і публікацій. Дослідженню безпеки банківської діяльності присвячено праці багатьох вітчизняних і зарубіжних учених. Значний внесок у дослідження цих проблем зробили українські вчені М. Зубок, О. Баранівський, С. Букін, І. Бланк, Вовчак, П. Гайдуцький, В. Геєць, В. Гіжевський, Р. Гриценко, а також зарубіжні — Л.Абалкін, Д. Артеменко, О. Бочаров, В. Гамза, С. Ілляшенко, В. Ларічев, Б. Райзберг та інші.

Серед робіт, які опубліковані за останнє десятиліття, та які внесли значний внесок у розвиток концепції проектування систем інформаційної безпеки на сучасному етапі та безпеки банківської діяльності, можна назвати наукові дослідження В.А. Герасименко [7, 8], В.В.Мельникова [11]. Перша робота, орієнтована на територіально-зосереджені автоматизовані системи обробки даних і організацію робіт по розвитку захисту інформації. У другій

роботі запропонована концепція, принципи побудови захисту і оцінки рівня безпеки інформації в обчислювальних системах і автоматизованих системах управління.

Метою статті. Розглянути питання стійкого розвитку банків з урахуванням інформаційної та економічної безпеки.

Виклад основного матеріалу. Банки відіграють важливу роль у економічному розвитку країни та світу, слугуючи фінансовими посередниками в розподілі кредитно-фінансових потоків та спрямуванні їх від кредиторів до позичальників, а надійність і стійкість банківської системи в цілому створює позитивні умови для ведення бізнесу. Як наголошують К. Менз, Н. Аттіг, стверджуючи, що кредитний ринок спричиняє більший тиск на корпорації щодо впровадження практик із корпоративно-соціальної відповідальності, ніж ринок цінних паперів [18, 19]. Твердження є справедливим для фінансових ринків з банкоцентричною моделлю, якою є вітчизняна модель фінансового ринку. Саме банківські установи, по суті будучи основними постачальниками фінансового капіталу для переважної більшості вітчизняних корпорацій, через механізм кредитування мають суттєвий вплив на корпоративну поведінку та стратегію.

В економічній теорії "стійкість" розглядають як одне з понять концепції економічної рівноваги, згідно з котрою досягнення та утримання рівноважного стану в економіці належить до найважливіших мікро- і макроекономічних завдань. Із даної концепції випливає, що економічні суб'єкти намагаються перевести економічну систему в оптимальний стан, розглядаючи його як рівноважний, котрий у даному контексті асоціюється з поняттям стійкості. У "Великому економічному словнику" категорія "стійкість" трактується "як сталість, постійність, непідвладність ризику втрат і збитків" [16]. Таким чином, у загальному розумінні сутність поняття "стійкість" (firmness, stability) можна розуміти, як характеристику стану рівноваги (об'єкта, системи), що відображає здатність зберігати певні властивості, функціональне призначення незмінним, незважаючи на можливі ризики, вплив зовнішніх факторів та внутрішні трансформації (випадкові чи передбачувані). Аналіз наукових розробок щодо діяльності банків та ознак, які її характеризують, дає змогу зазначити, що поширені у банківській практиці фінансові категорії "надійність", "стабільність", "стійкість" ототожнюють, розглядають одна через іншу. Проте чіткого обґрунтування, розподілу, схеми взаємозв'язку між ними немає. Зокрема, сутність поняття надійності розглядають як "стійкість" банку до змін на фінансовому ринку і здатність без затримок виконувати зобов'язання (щодо безпеки коштів, надання позикових коштів за укладеними кредитними договорами, здійснення платежів за виданими ґарантіями, авальованими векселями та ін.)" [17].

Заходи, яких вживають банки щодо забезпечення своєї безпеки, не мають виваженого систематичного характеру, а спрямовуються лише на захист від окремих загроз, що в підсумку не забезпечує необхідного рівня банківської безпеки. Основними причинами є неправильно обрані пріоритети в процесі організації безпеки банків, ототожнення безпеки лише з діяльністю спеціально

створених підрозділів, а не поширення її заходів на функції всіх підрозділів банків, відсутність комплексного підходу до забезпечення банківської безпеки.

Водночас банки, організовуючи свою безпеку, спрямовують зусилля окремо по кожному з видів безпеки – інформаційної, економічної, кадрової і тощо – і не пов'язують їх з інтересами економічної безпеки, від чого вжиті заходи не мають суттєвого впливу на економічний стан банку. Разом з тим, дослідження ролі, місця, видів безпеки у захисті інтересів банків показує, що банківська безпека має концентрувати свої зусилля насамперед навколо забезпечення саме економічної безпеки банків та інформаційної безпеки, створюючи умови для формування високого рівня стійкості банків до впливу загроз, підтримання ними своєї ліквідності та платоспроможності, у тому числі і під дією різного роду дестабілізуючих факторів [1].

Поняття "безпеки банківської діяльності" слід розуміти, як стан стійкого розвитку, за яким забезпечується реалізація основних інтересів, пріоритетних цілей банку, захист від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від умов його функціонування.

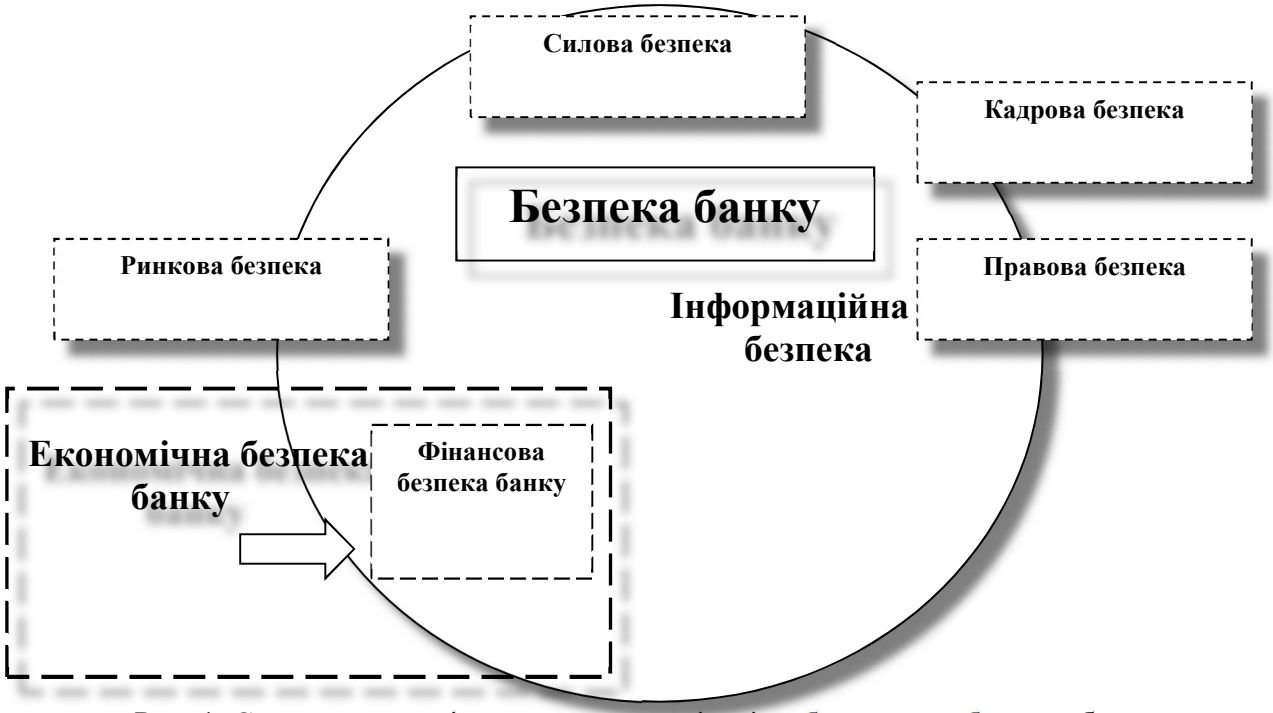

Рис. 1. Структурно-логічна модель організації забезпечення безпеки банку [Розроблено автором].

На Рис. 1. схематично представлена модель забезпечення безпеки банку котра включає основні складові, такі як:

1.*Інформаційна безпека* - це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, або комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення [20]. Одна із домінуючих ролей у системі безпеки банку, оскільки в сучасному суспільстві, де найважливішим ресурсом будь-якої компанії (банку) цілком

обґрунтовано є інформація, закономірно встає питання про створення моделей, або систем, які б забезпечили її збереження.

2.*Економічна безпека* – стан, за якого забезпечується економічний розвиток і стабільність діяльності банку, гарантований захист його ресурсів, здатність адекватно і без істотних втрат реагувати на зміни внутрішньої і зовнішньої ситуації [3]. Не менш важлива ланка банківської безпеки ніж інформаційна безпека, оскільки зосереджена на головних напрямах банківської діяльності, насамперед тих, де сконцентровані фінанси банків – матеріальному і фінансовому.

3. *Фінансова безпека* – є таким станом банківської установи, що характеризується збалансованістю і стійкістю до впливу зовнішніх і внутрішніх загроз, її здатністю досягати поставлених цілей і генерувати достатній обсяг фінансових ресурсів для забезпечення стійкого розвитку.

4.*Правова безпека* – стан правової захищеності важливих інтересів банку, в зв'язку з функціонуванням цього суб'єкта у сфері господарських відносин, здатність юридичними засобами протистояти зовнішнім і внутрішнім загрозам.

5.*Ринкова безпека* – це такий стан банку, який характеризується реалізацією потенціалу фінансово-кредитної установи на ринку банківських послуг за допомогою інструментів маркетингової діяльності, які спрямовані на забезпечення недопущення неправомірних дій конкурентів і зловмисників, захищеність від недобросовісної конкуренції, захист та посилення ділової репутації установи [21].

6. *Силова безпека* – такий стан банку, який досягається комплексом організаційно-правових, економічних та соціально-психологічних методів, які спрямовані на забезпечення цілісності власності, іміджу і персоналу банку, протистояння, подолання і нейтралізації дії небезпечних чинників [21].

7. *Кадрова безпека* – це процес запобігання негативним впливам на безпеку банку через ризики, загрози та небезпеки, пов'язані з персоналом, його інтелектуальним потенціалом і трудовими відносинами.

На показники діяльності банків, як уже зазначалося, впливають зміни, що відбуваються у навколишньому середовищі не тільки на рівні держави, але і на рівні міжнародної торгівлі та світового бізнесу.

Довготривала історія розвитку банківської діяльності вчить необхідності адекватно і миттєво реагувати на зміни. Зовнішні фактори – це ті фактори, що впливають на банківську діяльність із-зовні, і вони можуть буди як сприятливі для ефективного функціонування банку, так і нищівними. Для виявлення і врахування їх впливу зовнішні чинники поділяють на дві групи: фактори безпосереднього впливу і фактори опосередкованого впливу [22].

Під час вирішення проблем безпеки банку необхідно враховувати як зовнішні, так і внутрішні фактори впливу на їх діяльність. Стан середовища і чинники впливу на розвиток банківської діяльності потрібно максимально враховувати під час розроблення завдань, які постають перед банком на кожному етапі його розвитку. [2]

Досягнення належного рівня безпеки банку здебільшого залежить від побудованого механізму його управління. При цьому особливе значення

відводиться формуванню базових визначень, принципів забезпечення безпеки, класифікації загроз і методів управління нею [22].

Складові банківської безпеки повинні створити умови для надійного і ефективного функціонування банківських установ, недопущення або своєчасного виявлення загроз фінансовим, матеріальним та інформаційним ресурсам банку. Показниками ефективної безпеки банку є сталий розвиток у банківської установи згідно з плановими завданнями [22].

Проблема аналізу і управління економічною безпекою банківської установи є безумовно актуальною, оскільки банки є найважливішою складовою фінансово-кредитної сфери держави та посередниками в розподілі кредитно-фінансових потоків. Отже, саме стійкість і надійність банківського сектору багато в чому визначає рівень фінансової безпеки держави. Фінансова безпека окремого банку тісно пов’язана з безпекою банківської системи в цілому, оскільки вони взаємно впливають одна на одну: наприклад, з одного боку, будь-яка недовіра з боку населення до окремого банку може викликати масовий відтік депозитів з банківської системи, з іншого боку, структурні проблеми банківського сектору підривають довіру до будь-якого окремого банку. Фінансова безпека банку визначається:

- стійкістю фінансового стану банку;
- ступенем ефективності його фінансово-економічної діяльності;
- рівнем контролю за зовнішніми і внутрішніми ризиками;
- рівнем достатності власного капіталу;
- ступенем захищеності інтересів акціонерів. [4]

На рис. 2. наведені основні завдання фінансової безпеки банку.

Рис. 2. Завдання фінансової безпеки банку
[Авторська розробка].

Аналіз динаміки розвитку банків України в контексті рівня її безпеки здійснюється, виходячи з аналізу змінювання окремих важливих показників:

- загальні активи;
- кредити, надані суб’єктам господарювання;

• кредити, надані фізичним особам;
• власний капітал;
• рентабельність активів;
• адекватність регулятивного капіталу.

Вивчення вказаних показників демонструє наявність суттєвих коректив, які загальноекономічна криза внесла у розвиток банківської системи. Але побоювання викликають не тільки кількісні характеристики діяльності банків, але і рівень їх захищеності та фінансової стійкості, які становлять основу фінансової безпеки. З цієї точки зору необхідний аналіз динаміки показників, що характеризують потенційні загрози в діяльності банків (достатність капіталу, структура активів та пасивів тощо) і можуть свідчити про наявність негативних тенденцій, які знижують рівень фінансової безпеки як банківської системи в цілому, так і окремих банків, потребують постійного моніторингу, аналізу та прогнозування. [23]

Як наголошує Карчева Г.Т. [4], визначені наступні основні індикатори фінансової безпеки банківського сектору України, які потребують постійного аналізу, у тому числі, кількісного і в динаміці:

- рівень капіталізації банків;
- адекватність регулятивного капіталу;
- питома вага активів банківської системи у ВВП;
- показник обсягу вкладів населення відносно ВВП;
- рівень монетизації економіки;
- рівень кредитів банків
- вартість банківських кредитів;
- питома вага проблемних кредитів;
- фінансова залежність національної економіки від зовнішніх джерел;
- питома вага високоліквідних коштів в обсязі чистих активів банку

Для аналізу рівня фінансової безпеки банків України необхідно дослідити факт знаходження вказаних показників в допустимих межах, а також динаміку цих показників, що може свідчити про певні позитивні чи негативні зміни [23]. Це, насамперед, стосується рівня капіталізації банків, який за останні роки має тенденцію до значного збільшення, долі проблемних кредитів, що почала збільшуватися останнім часом, показників динаміки зростання банківського сектора, зокрема, обсягів активів, кредитного портфеля.

Питання, пов’язані із інформаційною безпекою банків, останнім часом набувають особливої актуальності, оскільки банки є найбільш вразливими до такого виду загроз, як наявність витоку інформації, це у свою чергу викликає необхідність перегляду підходів до забезпечення інформаційної безпеки банків та необхідність створення відповідних систем та підходів її захисту.

Інформація є ресурсом, який подібно іншим важливим бізнес-ресурсам, є суттєвим для бізнесу організації і тому потребує відповідного захисту. Це суттєво важливо у все більш взаємопов’язаному діловому середовищі. Внаслідок цієї зростаючої взаємопов’язаності інформація тепер наражається на зростаючу кількість і більшу різноманітність загроз та вразливостей.

Вимоги до захисту комп'ютерної інформації в банківській сфері, формуються на підставі аналізу змісту інформаційної безпеки та властивостей економічної інформації. Підкреслимо, що навіть у нормативних документах сфери захисту інформації спостерігаються певні розбіжності у трактуванні терміну "інформаційна безпека". Так у безпеці інформації (information security) ототожнюється зі станом інформації, в якому забезпечується збереження визначених політикою безпеки її властивостей [5]. Натомість у галузевому стандарті Національного банку України, інформаційна безпека розуміється як "…захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес-ризику і максимізації рентабельності інвестицій і бізнес-можливостей". Це найширше трактування інформаційної безпеки, яке однак, не дає змоги ідентифікувати вимоги до захисту комп'ютерних даних. Більш кращим є таке трактування інформаційна безпека: "інформаційна безпека (information security) – збереження конфіденційності, цілісності та доступності інформації…"[6]. Також зазначається потреба врахування у багатьох випадках додаткових властивостей, а саме: автентичності, неспростовності, надійності.

Надійна робота захисту інформації неможлива без дотримання принципів забезпечення інформаційної безпеки банківських систем.

Основними принципами, є:

1.Аналіз інформаційної системи з виявлення уразливості інформаційних активів банку.

2.Виявлення проблем, потенційно здатних вплинути на інформаційну безпеку банку та своєчасне корегування моделей загроз.

3.Контроль ефективності впроваджених заходів захисту.

4.Розподіл ролей між користувачами інформаційної системи банку.

5.Розробка і впровадження заходів захисту, адекватних характеру виявлених загроз, з урахуванням витрат на їх реалізацію і сумісності цих заходів з діючим банківським технологічним процесом.

6.Принцип «чотирьох очей», коли критичні операції та дії здійснюються або підтверджуються мінімум двома уповноваженими особами.

7.Знання банком своїх клієнтів і персоналу. [6]

Виходячи із принципів на яких ґрунтується робота інформаційної безпеки, будується система управління інформаційною безпекою, яка базується на підході, що враховує бізнес-процеси, і яка призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Система управління інформаційною безпекою – це забезпечення захисту конфіденційності, цілісності та доступності інформаційних активів. Вона складається з безлічі різних процесів, кожен з яких спрямований на обробку певних ризиків. Під словом "Ризик" слід розуміти ймовірність того, що визначена загроза, впливаючи на вразливості ресурсу або групи ресурсів, може спричинити шкоду банку.

Відповідно до системи управління інформаційної безпеки структура представлена на Рис.3. [10]

До описаної структури, ми розглянемо процеси системи управління інформаційної безпеки.

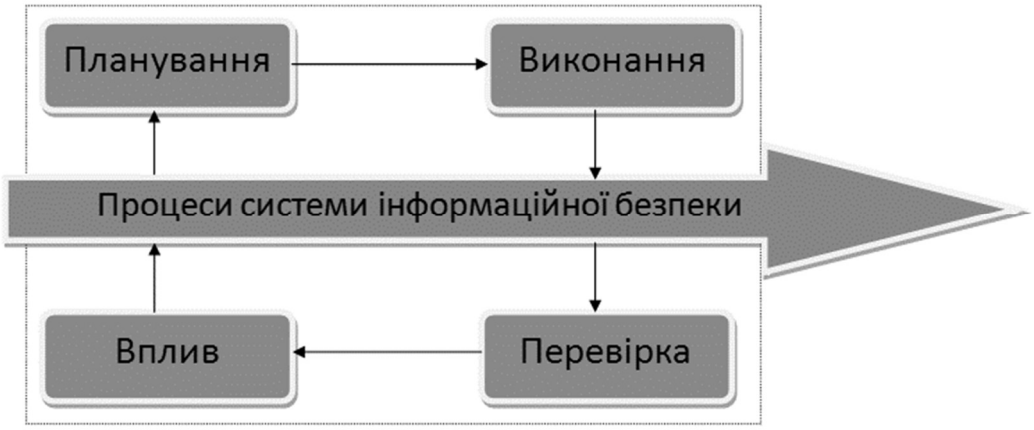

Рис.3. Структура системи управління інформаційної безпеки.
[СОУ Н НБУ 65.1 СУІБ 1.0:2010].

В системі управління інформаційної безпеки, для обробки процесів використовуються чотири процеси СУІБ (Система управління інформаційною безпекою):

1.Процес планування, метою якого є виявлення, аналіз і проектування способів обробки ризиків інформаційної безпеки;

2.процес виконання спланованих методів обробки ризиків, що описує процедуру запуску нового процесу забезпечення інформаційної безпеки, або модернізації існуючого;

3.процес перевірки побудованих процесів впроваджених в СУІБ;

4.процес впливу, або вдосконалення процесів СУІБ відповідно до результатів моніторингу, який робить можливим реалізацію коригувальних і превентивних дій [10].

На практиці ці процеси описуються політикою управління інформаційної безпеки, яка є або частиною політики інформаційної безпеки, або самостійним документом, представленим на верхньому рівні структури бази нормативних документів [9].

Будь-яка діяльність, зокрема банківська діяльність що має вхідний продукт, а також додає вартість до нього, та забезпечує вихідний продукт для внутрішнього або зовнішнього споживача називається бізнес-процес. Бізнес-процеси - це потоки роботи в яких є свої межі, іншими словами початок і кінець.

Бізнес-процеси будуються за допомогою аналітичної диференціації загального процесу на елементарні складові, з подальшою синтетичною інтеграцією (узагальненням) споріднених елементів процесу по функціональним, інтелектуальним, технологічним, територіальним та іншими ознаками.

Метою розробки методології створення та функціонування системи економічної безпеки банку є визначення послідовності основних методів, використовуваних при її створенні, а також механізми, що забезпечують функціонування даної системи. В основу методології дослідження об'єкта і його

властивостей необхідно покласти вироблення моделі системи забезпечення економічної безпеки банку. Вибір моделювання як методу дослідження механізму формування і функціонування системи безпеки обумовлений здатністю моделі розкрити системний характер організації, а також можливістю включення в модель широкого кола об'єктів системи забезпечення економічної безпеки банку.

Під моделлю прийнято розуміти “спеціально створений об'єкт, на якому відтворюються певні характеристики досліджуваного явища, а моделювання – це конкретне відтворення цих характеристик, що дає змогу вивчати можливу поведінку явища без проведення експериментів над ним” [12].

Модель економічної безпеки банку повинна розкривати її як складну систему, на яку впливає зовнішнє середовище, а також внутрішнє, в якому відбуваються комерційні операції, що призводять до виникнення відповідного впливу банку на навколишнє середовище.

Отже як показав аналіз, оптимальна система економічної безпеки банку – це сукупність взаємопов'язаних елементів, об'єднаних спільною метою та завданням, необхідних для протидії внутрішнім та зовнішнім загрозам з метою захисту основних цілей бізнесу та створення безпечних умов розвитку (рис 1.4). При цьому структура системи економічної безпеки банку повинна містити такі обов'язкові елементи, як об’єкт, суб’єкт та механізм забезпечення економічної безпеки.

Система економічної безпеки банку формується відповідно до політики, яку проводить банк. Політика безпеки – це система поглядів, заходів, рішень, дій, які створюють умови та сприятливе середовище для досягнення цілей бізнесу. Іншими словами, політика безпеки, яку проводять у банку, дає змогу йому підвищувати ефективність здійснення банківських операцій, дає змогу отримувати необхідний прибуток і забезпечує високий рівень захищеності на ринку банківських послуг.

Концепція безпеки банку є науково обґрунтованою системою поглядів на визначення основних напрямів, умов і порядку практичного вирішення завдань захисту банку від протиправних дій позичальників і недобросовісної конкуренції [13; 14]. Інші науковці стверджують, що концепція комплексної системи економічної безпеки банку передбачає захист матеріальних цінностей, інформаційних ресурсів, інтересів керівництва банку, засновників і співробітників від різного роду загроз [15].

Таким чином, концепція визначає цілі та завдання системи безпеки, принципи її організації, функціонування і правові основи, види загроз безпеці і ресурси, що підлягають захисту, а також основні напрями розроблення системи безпеки, включаючи правовий, організаційний і інженерно-технічний захист.

Дослідження і аналіз інформаційної безпеки, а також розробка нових методів і моделей захисту і аналізу існуючої інформації в банківських системах, спирається на якість захисту цієї інформації. Автоматизовані банківські системи – це великий обсяг інформації, яка в більшості своїй є банківською таємницею. Для якісного механізму захисту інформації можемо виділити наступні кроки для захисту і планування захисту інформації в банках:

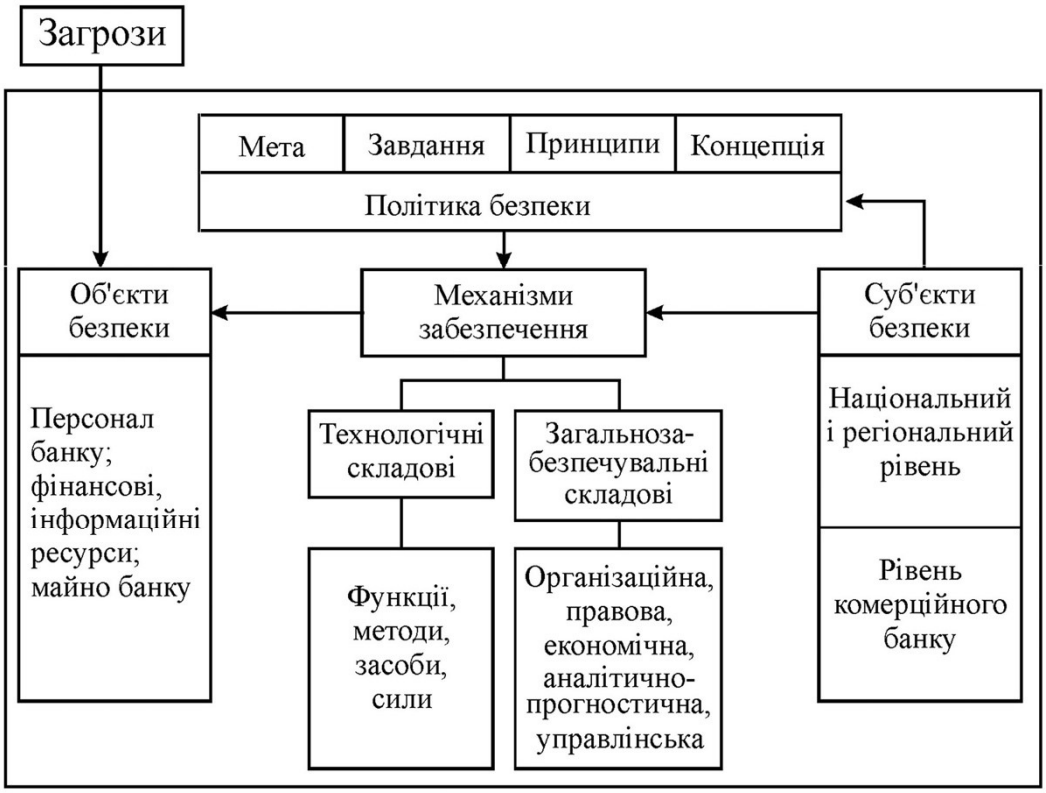

Рис.4. Теоретична модель системи економічної безпеки банку.
[За матеріалами: Зубка М. І., Безпека банківської діяльності[9]].

1. Ефект цілісності досягається тоді, коли усі використовувані методи і моделі об'єднуються в єдиний, цілісний механізм захисту інформації, при цьому потрібно дотримуватись всіх можливих політик інформаційної безпеки, для зменшення ризику компрометації інформації.

2. паралельне проектування для кращого інформаційного захисту автоматизованої банківської системи. Механізм захисту повинен проектуватися паралельно зі створенням систем обробки даних і проходити тестування.

3. процеси автоматизованої обробки інформації. Механізм функціонування захисту має плануватися і забезпечуватися з плануванням і забезпеченням процесів автоматизації обробки інформації.

4. модернізація та моніторинг. Необхідно здійснювати постійний контроль функціонування механізму захисту, або автоматизувати існуючий контроль з додаванням елементів моніторингу.

Таким чином, розглянувши особливості формування систем економічної та інформаційної безпеки банку, можна зробити висновок, що вони покликані створювати умови для досягнення цілей через якісну оцінку його інформаційного та технічного, фінансового стану, виявляти і максимально нейтралізувати дію різних небезпек та загроз в умовах конкуренції, а також зміцнення позицій на ринку банківських послуг. Тому для ефективного розвитку та забезпечення сталих показників банківського розвитку є передусім потреба у розробленні моделей систем економічної та інформаційної безпеки банку, головними елементами яких є: об'єкти безпеки та суб'єкти безпеки.

Система інформаційної та економічної безпеки банку має вирішувати, окрім головного свого завдання – формування системного підходу до забезпечення інформаційної та економічної безпеки, ще і завдання концентрації та маневрування силами і засобами згідно із визначеними цілями і завданнями з урахуванням змін у характері та інтенсивності загроз, що виникають.

Отже, визначивши основні наукові погляди побудови систем інформаційної та економічної безпеки банку, або його стійкого розвитку, можна сказати, що саме забезпечення основних складових економічної та інформаційної безпеки діяльності банківських установ, дає можливість стійкого розвитку банку.

Література:

1. Яременко С. М. , Забезпечення економічної безпеки діяльності банків : автореф. дис. на здобуття наук. ступеня канд. ек. наук : спец. 08.00.08 "Гроші, фінанси і кредит" / – Київ, 2010.
2. Прокопенко Н. С. , Складові безпеки банківської діяльності / Н. С. Прокопенко, М. І. Виклюк. // Науковий вісник НЛТУ України. – 2014. – №24.
3. Васильчак С.В. ,Економічна безпека банків та методи її забезпечення / С.В. Васильчак, Р.Ю. Моцьо // Науковий вісник НЛТУ України : зб. наук.-техн. праць. – Львів : РВВ НЛТУ України. – 2009. – Вип. 19.12. – С. 287-293.
4. Карчева Г.Т. ,Ефективність функціонування та перспективи розвитку банківської системи України / Г.Т.Карчева // НАН України Ін-т екон. та прогнозув. – К.: 2012. – 520 с.
5. Постанова Правління НБУ від 28 жовтня 2010 року N 474 «Про набрання чинності стандартами з управління інформаційною безпекою в банківській системі України». [Електронний ресурс] // – Режим доступу: http://www.zakon.rada.gov.ua.
6. С. В. Кавун, В. В. Носов, О. В. Манжай // Інформаційна безпека. Навчальний посібник /— Харків: Вид. ХНЕУ, 200’. — 352 с.
7. Герасименко В.А. Захист інформації в автоматизовану систему обробки даних / В.А. Герасименко. - У 2 кн .: Кн. 1. - М .: Вища школа, 1994. - 400 с;
8. Герасименко В.Г. Проблеми забезпечення інформаційної безпеки при використанні відкритих інформаційних технологій в системах критичних додатків / В.Г. Герасименко // Інформація і безпека: Регіон. наук.-техн;
9. Зубок М. І. Безпека банківської діяльності: навч. посіб. / М. І. Зубок. – К. : КНЕУ, 2002. – 190 с
10. СОУ Н НБУ 65.1 СУІБ 1.0:2010 «Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою» (ISO/IES 27001:2005, MOD). [Електронний ресурс] // – Режим доступу: http://www.zakon.rada.gov.ua.
11. Мельников В.В. Захист інформації в комп'ютерних системах / В.В. Мельников. - М .: Фінанси і статистика; Електроінформ, 1997. - 368 с;

12. ISO/IEC 15408-1:2009, Information technology -- Security techniques -- Evaluation criteria for IT security. [Електронний ресурс] // – Режим доступу: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341
13. Тагирбеков К.Р. Основы банковской деятельности / К.Р. Тагирбеков. – М. : Изд-во "Ось- 89", 2003. – 446 с.
14. Охрана банка – концепція безопасности и организация охраны банков. [Электронный ресурс]. – Доступный с http://www.spo-pult.ru/.
15. Решения по безопасности для банков. [Электронный ресурс]. – Доступный с http://www.iss.incom.ua/content/category/41/125/189.
16. Большой экономический словарь / [под. ред. А. Н. Азрилиана]. – М.: Институт новой экономики, 1997. – 864 с.
17. Бліндюк О. Надійність комерційного банку і фактори, що її визначають / О. Бліндюк // Все про бухгалтерський облік. – 2003. – № 11 (799). – С. 13–16.
18. Menz K. M. Corporate social responsibility: Is it rewarded by the corporate bond market A critical note / K. M. Menz // Journal of Business Ethics. – 2010. – Volume 96. – P. 117–134.
19. Corporate Social Responsibility and Credit Ratings / N. Attig, S. El Ghoul, O. Guedhami, J. Suh // Journal of Business Ethics. – 2013. – Volume 117. – P. 679–694.
20. Інформаційна безпека. [Електронний ресурс] // – Режим доступу: https://uk.wikipedia.org/wiki/Інформаційна_безпека
21. Безпека банківської діяльності. [Електронний ресурс] // – Режим доступу: http://elib.lutsk-ntu.com.ua/book/fof/bs/2011/11-15/
22. Виклюк М. І. Складові безпеки банківської діяльності / М. І. Виклюк. // Науковий вісник НЛТУ України. – 2014. – №24. – С. 302–307.
23. Гадецька С.В. Моделювання систем фінансової безпеки банку – Харків: ХІБС УБС НБУ, 2014 – 72 с.