

УДК 336.71 (477)

Я.В. Жарій, канд. техн. наук, доцент**Л.В. Дохтаренко**, студентка

Чернігівський державний технологічний університет, м. Чернігів, Україна

АКТУАЛЬНІ ПРОБЛЕМИ ФІНАНСОВО-ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКОЇ СИСТЕМИ УКРАЇНИ

У статті досліджено існуючі підходи до визначення поняття «банківська безпека» та виокремлено основні складові банківської безпеки. Виявлено актуальні проблеми фінансової й інформаційної безпеки банківської системи України та розглянуто можливості підвищення їх рівня.

Ключові слова: банківська безпека, фінансова безпека банку, інформаційна безпека банку, внутрішні загрози, зовнішні загрози, Європейський центр кіберзлочинності.

В статье исследованы существующие подходы к определению понятия «банковская безопасность» и выделены основные составляющие банковской безопасности. Определены актуальные проблемы финансовой и информационной безопасности банковской системы Украины и рассмотрены возможности повышения их уровня.

Ключевые слова: банковская безопасность, финансовая безопасность банка, информационная безопасность банка, внутренние угрозы, внешние угрозы, Европейский центр киберпреступности.

In the article are investigated the existing approaches to the determination of concept "bank safety" and fundamental component of bank safety are isolated. The vital problems of financial and information safety of the banking system of the Ukraine are determined and are examined versions of raising its level.

Key words: bank safety, financial safety of bank, information safety of bank, internal threats, external threats, European Cybercrime Centre.

Постановка проблеми. У сучасних соціально-економічних умовах слід приділяти особливу увагу розвитку фінансової сфери України та важливої її складової – банківської системи. Світова фінансова криза негативно вплинула на діяльність вітчизняної банківської системи, виявивши неспроможність багатьох банківських установ протистояти впливу зовнішніх і внутрішніх чинників. Для виправлення ситуації та підвищення ефективності діяльності комерційних банків необхідно постійно вдосконалювати систему управління банком та підтримувати належний рівень банківської безпеки як важливого елементу банківського менеджменту.

Кожний комерційний банк функціонує не відособлено, а в спільному просторі, і його дії повинні бути узгоджені з інтересами клієнтів, інвесторів, конкурентів, держави. Питання банківської безпеки є актуальним для його власників, акціонерів, оскільки від того, наскільки буде захищеним банк, залежатиме ступінь розвитку бізнесу, рівень отриманого прибутку. Важливу роль відіграє безпека банку для його клієнтів як уже існуючих, так і майбутніх, особливо вкладників. Розглядаючи питання банківської безпеки, слід враховувати й партнерів по бізнесу, а також конкурентів, які тісно співпрацюють у межах банківської системи і є взаємопов'язаними.

Отже, питання безпеки банку є актуальним не лише безпосередньо для банків, а й для решти суб'єктів ринку та держави. Для банківського сектору України найбільш актуальними є питання фінансової та інформаційної безпеки, оскільки це стосується ключових аспектів діяльності кожного окремого банку та банківської системи у цілому.

Аналіз останніх досліджень і публікацій. Проблема банківської безпеки присвячено чимало досліджень вітчизняних та зарубіжних учених. Серед них наукові праці О. Барановського, В. Богомолова, Т. Болгар, С. Григоріної, М. Зубка, О. Криклія, А. Єпіфанова, Г. Конаховича, Ю. Корнієнко, О. Користіна, С. Побережного, О. Хитріна, Н. Островської, С. Соколовського, В. Соловйова, З. Сороківської та інших. Науковцями приділено значну увагу теоретичним засадам банківської безпеки на макро- і мікрорівні. У працях висвітлено сутність та складові банківської безпеки, її місце у системі економічної та фінансової безпеки держави. Розглянуто основні види загроз та чинників, що негативно впливають на безпеку банківської діяльності. Підкреслено необхідність формування системи заходів для підвищення рівня фінансової та інформаційної безпеки банків у сучасних умовах.

Виділення не вирішених раніше частин загальної проблеми. При більш детальному аналізі матеріалів публікацій слід відзначити, що питання банківської безпеки ще вимагають досліджень за всіма її складовими, оскільки на сьогодні навіть поняття «банківська безпека» розглядається авторами по-різному. Малодослідженим залишається й питання формування системи показників для розрахунку як рівня безпеки кожного окремого банку, так і всієї банківської системи країни.

Мета статті – дослідити стан безпеки банківської системи України, виявити найбільш актуальні проблеми фінансово-інформаційної безпеки банків та розглянути можливості підвищення її рівня в умовах загальносвітової фінансової нестабільності.

Виклад основного матеріалу дослідження. Розглядаючи питання банківської безпеки, варто дослідити існуючі підходи до визначення самого поняття, оскільки авторами багатьох наукових досліджень не досягнуто згоди з цього приводу.

Так, М. Зубок дає таке визначення безпеки банку: «стан стійкої життєдіяльності, за якого забезпечується реалізація основних інтересів і пріоритетних цілей банку, захист від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від умов функціонування». Основною метою безпеки банку автор вважає виключення можливостей нанесення йому збитків або упущення вигоди та забезпечення ефективної його діяльності з якісною реалізацією всіх операцій та угод [5].

З. Сороківська розглядає безпеку банківської діяльності як систему заходів, спрямованих на захист та раціональне використання сукупності ресурсів, що є у розпорядженні банківської установи з метою запобігання загроз його діяльності задля максимального отримання прибутку [13].

При цьому потенційними суб'єктами загроз безпеці банківській системі, чії дії можуть завдавати фінансової шкоди, слід розглядати: юридичних осіб (підприємців, фірми, фонди та благодійні організації, державні підприємства й інші суб'єкти господарювання); фізичних осіб (приватних підприємців і виробників, які не мають статусу юридичної особи; керівників підприємств, які провадять господарські операції; співробітників державних організацій і установ тощо); іноземних юридичних осіб (валютні фонди, банки, організації, фірми спецслужб); злочинні елементи (злочинців, організовану злочинність як у межах країни, так і за кордоном) [12].

О. Барановським безпека банку трактується різнопланово: як захищеність інтересів власників, клієнтів, працівників і керівництва банку від зовнішніх і внутрішніх загроз; як стан зовнішнього та внутрішнього середовища банку; як один з основних елементів банківського менеджменту; як організація заходів щодо запобігання можливим загрозам його діяльності [1].

Узагальнюючи наведене, можна зазначити, що, оскільки проблема банківської безпеки є актуальною як для власників банку, так і для клієнтів, працівників банку та партнерів по бізнесу, то під безпекою банківської діяльності слід розуміти: безпеку банку як організації; безпеку банківського персоналу; безпеку банківських операцій.

Розглядаючи безпеку банку через призму організації, важливо акцентувати увагу як на її зовнішньому, так і внутрішньому середовищі. У зовнішньому середовищі необхідно розглядати дії з боку клієнтів, партнерів, конкурентів, державних установ і громадян, а також кримінального середовища. У внутрішньому – дії персоналу банку в особі спеціалістів і менеджерів відділів банку (його підрозділів), неформальних груп, а також адміністрації банку та його власників. Фоном для цього досить часто є некомпетентність окремих менеджерів і спеціалістів банку, а іноді їх навмисні дії та бажання особисто збагатитися за рахунок можливостей банку, у тому числі, за рахунок зговору з клієнтурою чи криміналом, а також з потенційними конкурентами.

Безпека персоналу банку відбиває стан його внутрішнього середовища, де особливо актуальною є особиста безпека персоналу банку, що не гарантується жодним власником. Цей процес не є однозначним і нерідко на практиці виражається через небажання банківського персоналу брати участь у кримінальних чи тіньових операціях і вимогу банківського персоналу за кваліфіковану і понаднормовану працю отримувати більш справедливую оплату з урахуванням її специфіки, включаючи вплив характеру потенційних загроз під час проведення конкретних банківських операцій.

Безпека банківських операцій становить не менший інтерес, оскільки торкається сутності банківського бізнесу і безпосередньо пов'язана не лише з безпекою організаційного характеру, а й з фінансовою та інформаційно-технологічною безпекою банку.

Враховуючи важливість питань банківської безпеки, очевидно стає необхідність оцінювання її рівня як для окремого банку, так і для всієї банківської системи. На поточний момент оцінювання стану банківської безпеки для банківської системи України у цілому проводиться за Методикою розрахунку рівня економічної безпеки України [8]. До розрахунку включено всього два показники:

- частка іноземного капіталу в загальному обсязі банківського капіталу, %;
- обсяг кредитування банками реального сектору економіки, % до ВВП.

Порогове значення для першого показника – не більше 30 %, для другого – не менше 30 % [9].

Якщо розглянути динаміку першого показника банківської безпеки (рис.), то він не відповідає пороговому значенню. Цей показник у 2011 році збільшився у порівнянні з даними 2010 року, а у 2012 році зменшився та становив 39,5 %. Скоріше за все, це пов'язано з приходом значної кількості банків з іноземним капіталом (у 2012 році – 54 банки або 30,68 % від загальної кількості зареєстрованих банківських установ, з них 22 банки мають 100 % іноземного капіталу у складі статутного, а це 12,5 % від загальної кількості зареєстрованих банків).

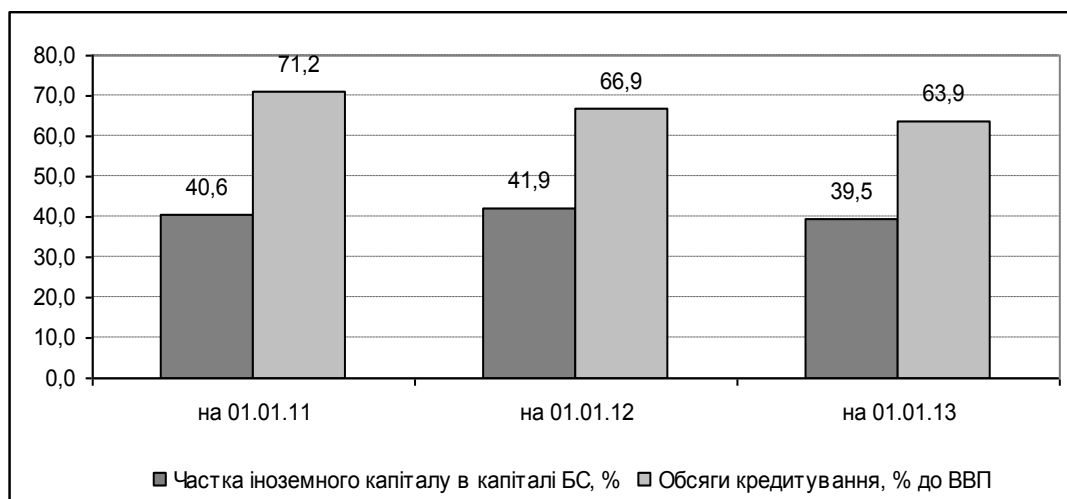


Рис. Динаміка показників безпеки для банківської системи України

Обсяг кредитування банками реального сектору економіки щодо ВВП зменшується, що є наслідком зростання обсягу ВВП більш високими темпами, ніж темпи зростання обсягів кредитів, наданих суб'єктам господарювання [9; 14]. Цей показник відповідає значенню, встановленому Методикою, однак це не означає, що він є оптимальним для вітчизняної економіки. Для країн, що розвиваються, МВФ рекомендовано не завищувати цей показник, щоб не викликати кризи перекредитування економіки. Так, за даними міжнародного рейтингового агентства Fitch Ratings, відношення обсягу кредитів до ВВП у середньому для країн, що розвиваються, у 2012 році становило 53 %.

Очевидно, що для оцінювання стану банківської безпеки банківської системи України двох показників недостатньо. Необхідно розширювати перелік індикаторів банківської безпеки з урахуванням різних аспектів цього поняття. Щонайменше, це можуть бути показники, пов'язані з основними складовими банківської безпеки: безпеки персоналу, правової, фінансової та інформаційної безпеки банку [13].

Хоча погіршення стану банківської безпеки за будь-якою зі складових обов'язково призведе до фінансових проблем як окремого банку, так і банківської системи в цілому, більш детально зупинимось на двох останніх складових, оскільки вони є ключовими в банківському бізнесі.

Поняття «фінансова безпека банку» як і поняття «безпека банківської діяльності» не має єдиного трактування. Кожен автор, що проводить дослідження з цих питань, дає своє визначення.

Наприклад, О. Хитрін визначає фінансову безпеку банку як динамічний стан, при якому банк [15]:

- юридично і технічно здатний виконувати та реально виконує властиві йому функції;
- забезпечує стійкий захист життєво важливих соціально-економічних інтересів громадян, господарюючих суб'єктів, суспільства та держави від негативного впливу внутрішніх і зовнішніх загроз;
- володіє потенціалом як для кількісного, так і для якісного зростання і має у своєму розпорядженні механізми для реалізації цього потенціалу.

О. Барановський дає такі визначення поняття «фінансова безпека комерційного банку» [1]:

- це сукупність умов, за яких потенційно небезпечні для фінансового стану комерційного банку дії чи обставини попереджені чи зведені до такого рівня, за якого вони не здатні завдати шкоди встановленому порядку функціонування банку, збереженню й відтворенню його майна та інфраструктури і перешкодити досягненням банком статутних цілей;
- це стан захищеності фінансових інтересів комерційного банку, його фінансової стійкості, а також середовища, в якому він функціонує.

Розглядаючи питання фінансової безпеки банківської установи потрібно розглянути і загрози банківської діяльності. Їх прийнято поділяти на дві групи – внутрішні та зовнішні [1; 5; 13]. До внутрішніх загроз належать ті, які є частиною внутрішнього середовища банку або безпосередньо ним генеруються. До зовнішніх належать загрози, що є результатом впливу зовнішнього середовища на банк, зокрема дії держави, економічна кон'юнктура в країні та світі, конкуренти тощо (табл.).

Наведене в таблиці не є повним переліком усіх загроз фінансовій безпеці банків, їх може бути набагато більше. Менеджерам банку необхідно своєчасно виявляти такі загрози та вживати заходів щодо зниження їх наслідків, а при можливості й уникати їх.

Під час розроблення заходів для підтримання належного рівня фінансової безпеки головними індикаторами можуть стати ключові показники фінансового стану банку (показники фінансової стійкості, ділової активності, ліквідності, прибутковості та рентабельності). Хоча більшість учених вважають фінансову безпеку якісною характеристикою фінансового стану банку [1; 7; 13], наведені показники можуть дозволити ще й кількісно оцінити її рівень.

Дуже важливою складовою банківської безпеки є інформаційна безпека. Під інформаційною безпекою розуміється захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати збитків суб'єктам інформаційних відносин.

Таблиця

Основні загрози фінансовій безпеці комерційних банків

Внутрішні загрози	Зовнішні загрози
1. Неналежна організація діяльності банку. 2. Порушення банком чинного законодавства та договірних відносин. 3. Неефективна система фінансового менеджменту банку. 4. Помилки в стратегічному, тактичному та оперативному плануванні банку. 5. Неякісна система управління ризиками. 6. Низький рівень капіталізації банку. 7. Недостатня ліквідність банківських активів. 8. Ризикова та незважена кредитна діяльність. 9. Низька якість банківських активів. 10. Недосконала цінова політика банку 11. Недостатня диверсифікація банківських операцій. 12. Нерозвинена маркетингова діяльність банку. 13. Наявність зловживань або протиправних дій службовців банку. 14. Наявність каналів витоку банківської інформації	1. Несприятлива загальносвітова економічна ситуація. 2. Кризові явища в країні. 3. Недосконалість законодавчої бази. 4. Зміни в політиці та нормативних актах центрального банку. 5. Високий рівень інфляції та інфляційні очікування. 6. Нестійкість курсу національної валюти. 7. Постійний вплив ринкових ризиків. 8. Нерозвиненість фондового ринку країни. 9. Низький рівень інвестиційної активності. 10. Недосконала система страхування депозитів. 11. Низький рівень кредитоспроможності позичальників. 12. Невиконання клієнтами та партнерами зобов'язань перед банком. 13. Недобросовісна конкуренція на ринку банківських послуг. 14. Прихід на ринок банківських послуг нових сильних гравців. 15. Навмисні протиправні дії з боку клієнтів

Особливості інформаційної безпеки банку продиктовані специфікою і самої банківської інформації, і систем її оброблення. Основними ознаками цієї специфіки є:

– збережена й оброблювана в банківських системах інформація є величезною фінансовою цінністю (це реальні гроші і банку, і клієнтів). Зрозуміло, що незаконне маніпулювання такою інформацією може зацікавити шахраїв і призвести до серйозних збитків;

– інформація в банківських системах зачіпає інтереси великої кількості клієнтів – фізичних та юридичних осіб і, як правило, вона є конфіденційною. Тому банк зобов'язаний відповідати перед своїми клієнтами за забезпечення необхідного ступеня таємності. Її підроблення або витік можуть призвести до серйозних наслідків (для банку та його клієнтів);

– клієнт повинен мати можливість швидко, без стомлюючих процедур розпоряджатися своїми грошима, йому має бути зручно працювати з банком, у т. ч. й на відстані. Технології доступу до рахунків у режимі реального часу (on-line) підвищують імовірність злочинного проникнення в інформаційні системи;

– для оброблення величезних обсягів інформації банку не достатньо простого набору програмних та апаратних засобів (на кшталт домашніх). Сьогодні це складні високопродуктивні інтегровані системи, які змушені працювати в режимі безперервного і безвідмовного оброблення інформації з використанням специфічного програмного забезпечення та систем управління базами даних. Банк, який бажає утримувати відповідні позиції на ринку, зобов'язаний забезпечувати не лише багатофункціональність, а й надійність і цілісність такої системи.

Отже, інформаційна система банку має бути не просто вмістилищем зібраних на законних підставах, актуальних, точних, релевантних і готових до оброблення (або вже оброблених) програмним шляхом даних. Вона має бути доступною для зручного використання клієнтами різних категорій, і при цьому бути надійно захищеною від несанкціонованого доступу, викрадення, зміни або розголошення інформації).

Тому при розробленні концепції інформаційної безпеки банку необхідний комплексний підхід. У цій концепції варто передбачати не тільки заходи, пов'язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користу-

вачів, їхньої ідентифікації й аутентифікації, “брандмауери” для захисту входів-виходів мережі і т. п.), але і заходи адміністративного і технічного характеру, включаючи жорсткі процедури контролю фізичного доступу до автоматизованої банківської системи, а також засоби синхронізації й обміну даними між модулем адміністрування інформаційної бази і системою охорони банку [3; 6; 10].

Щоб бути ефективною, система інформаційної безпеки банку має включати, щонайменше, такі складові:

- фізичний захист даних, пов’язаний зі створенням зовнішніх умов, в яких працюють комп’ютери (температура, вологість, запиленість); зі зберіганням у сейфах інформації на зовнішніх носіях (CD, DVD та інші диски); з контролем за доступом до приміщень із серверами та до баз даних;

- контроль даних та їх достовірності (під час збирання, введення, оброблення, пересилання та виведення даних);

- резервування інформації (регулярне створення резервних копій баз даних та окремих файлів);

- діагностику стану програмно-технічних засобів (починаючи з операційної системи, офісних та прикладних програм і завершуючи перевіркою працездатності апаратних компонентів);

- аудиторські пакети програм, які використовуються як допоміжні засоби для автоматизованого тестування комп’ютерних систем банку (в основному для виявлення випадкових або навмисних помилок під час оброблення даних). При цьому персонал банку повинен бути ізольований від такої системи тестування, оскільки правопорушення, пов’язані з комп’ютерами й обробленням даних, найчастіше здійснює персонал, який обслуговує відповідні системи;

- систему захисту конфіденційної інформації, наприклад, DLP (Data Loss Prevention) [2], яка заснована на аналізі потоків даних, що пересікають периметр інформаційної системи, що захищається. При виявленні у потоці конфіденційної інформації спрацьовує захист, і передача повідомлення (пакета, потоку, сесії) блокується або відслідковується.

Оскільки зараз набагато простіше й дешевше здобути інформацію нелегально, ніж отримати офіційно, відчутно стало розвиватися кібершахрайство. Зростають темпи розвитку технічних пристроїв та програмних засобів для крадіжки інформації, і в багатьох випадках програмно-технічна забезпеченість кібершахраїв значно перевищує рівень захищеності банків від несанкціонованого доступу до банківської інформації.

Питанням захисту від випадків кіберзлочинності активно займаються за кордоном. За рішенням Європейського Союзу від 9 січня 2013 року з 11 січня 2013 року почав діяти новий Європейський центр кіберзлочинності (European Cybercrime Centre), метою діяльності якого є захист підприємств та громадян Європейського Союзу від кіберзлочинності. Робота цього центру буде зосереджена на незаконній онлайн-діяльності, що здійснюється організованими злочинними групами. Зокрема, особливу увагу буде приділено нападам на електронні банківські операції та іншу фінансову онлайн-діяльність [4; 16].

Центр також спрямовуватиме свою діяльність на проведення досліджень у сфері захисту інформації; забезпечення нарощування потенціалу серед правоохоронних органів, суддів і прокурорів; проведення аналізу тенденцій, прогнозів загроз та їх вчасне попередження. Також буде пропонувати оперативну підтримку країнам Європейського Союзу та забезпечувати високий рівень технічної, аналітичної та судово-медичної експертизи [16].

В Україні підтвердженням актуальності проблеми банківської безпеки та приверненням значної уваги до цих питань можуть слугувати такі факти, як збільшення кіль-

кості публікацій на цю тему та проведення I Міжнародної конференції «Банківська безпека: проблеми та рішення – 2012», що відбулася 10-11 липня 2012 року.

Форум викликав значний інтерес як з боку банків, так і виробників та постачальників засобів безпеки. У конференції взяли участь більше 90 представників ділових кіл з України, Росії, Білорусі, Молдови, Латвії та Азербайджану.

На конференції працювало п'ять секцій: «Економічна безпека», «Інформаційна безпека», «Протидія шахрайству в фінансових структурах. Безпека трансакцій», «Технічні засоби захисту. Фізичний захист», «Страховання ризиків у банківській діяльності». У межах форуму також працювала спеціалізована експозиція, на якій були представлені нові розробки у сфері безпеки.

Окремо було приділено увагу проблемам інформаційної безпеки банківської діяльності у зв'язку з активізацією останнім часом кіберзлочинності. Зазначалося, що з використанням новітніх ІТ-технологій протиправні дії кібершахраїв отримали цілеспрямований і масовий характер. Збитки в результаті цих дій важко підрахувати, оскільки відсутні достовірні дані, але вже на сьогодні вони становлять десятки мільйонів доларів. Протистояти цьому можна тільки за умови введення в дію сучасних систем управління інформаційною безпекою [11].

Учасники конференції відзначили й позитивні тенденції декількох останніх років у сфері банківської безпеки і перш за все в законодавчому і нормативно-правовому забезпеченні. Разом з тим залишаються невирішеними окремі гострі й актуальні питання, розв'язання яких, на думку учасників, призвело б до формування фінансово стабільної та безпечної банківської системи. До цих питань відносяться: відсутність єдиної державної політики в галузі захисту інтересів і забезпечення безпеки як банківської системи, так і клієнтів банків; недоробки під час створення профільних стандартів, що регламентують нормативи безпеки; вузьковідомчі інтереси різних структур, що регулюють ринок. Виправити ситуацію може відкритий діалог усіх зацікавлених сторін для вироблення спільних підходів до проблеми безпеки в суспільстві та економіці в цілому і в фінансовому секторі зокрема [11].

Висновки і пропозиції. Отже, розглянувши численні наукові дослідження можна з упевненістю стверджувати, що питання банківської безпеки в сучасних умовах економічного розвитку як України, так і світу, є досить актуальними. Неефективна діяльність у сфері захисту банківських установ прямо впливає як на результати діяльності самого банку, так і на стан клієнтів – суб'єктів господарювання і населення. Це неприпустимо, оскільки нестабільні банки не в змозі створити надійну банківську систему, погіршення стану економічних суб'єктів призводить до погіршення загальноекономічної ситуації в країні.

Слід також зазначити, що проблемам банківської безпеки приділяється недостатньо уваги й на державному рівні, оскільки навіть для оцінювання стану безпеки всієї банківської системи використовується методика розрахунку лише за двома показниками, що, звичайно, є недостатнім для комплексного аналізу.

Актуальною залишається проблема виміру фінансової безпеки кожного окремого банку, оскільки на сьогодні в умовах загальносвітової фінансової нестабільності не існує єдиної методики оцінювання рівня цієї безпеки для вітчизняних банків.

У зв'язку з активізацією останнім часом кіберзлочинності особливу увагу слід приділяти інформаційній безпеці банківської діяльності. На цьому етапі розвитку суспільства саме інформація стає найбільш цінною, обсяги інформації, що використовуються під час здійснення банківської діяльності, постійно зростають. Через втрату частини інформації або порушення її конфіденційності банківська установа не тільки несе збитки, а й втрачає партнерів по бізнесу та своїх клієнтів. Такі явища підривають довіру до банківських установ та здійснюють негативний вплив на фінансову систему й економі-

ку всієї країни, оскільки без стабільної і надійної банківської системи утримати фінансову безпеку держави на належному рівні неможливо.

Список використаних джерел

1. Барановський О. І. Банківська безпека: проблема виміру / О. І. Барановський // Економічне прогнозування. – 2006. – № 1. – С. 7-32.
2. Глобальное исследование утечек корпоративной информации и конфиденциальных данных, 2011 [Электронный ресурс] / Аналитический центр InfoWatch. – Режим доступа : <http://www.infowatch.ru/>.
3. Григорина С. В. Захист інформаційної безпеки у вітчизняних банках України [Електронний ресурс] / С. В. Григорина, О. Г. Борисов // Сучасний стан інформаційної безпеки : збірник матеріалів XIII Міжнародної науково-практичної конференції 28 травня 2010 р. Ч. 2. – К. : УДУФМТ, 2010. – С. 65-68. – Режим доступу : http://www.nbuv.gov.ua/portal/soc_gum/uazt/2010_2k.pdf.
4. Еврокомиссия представила стратегию борьбы с киберпреступностью [Электронный ресурс] / Центр исследования компьютерной преступности. – 2013. – Режим доступа : <http://www.crime-research.ru/news/08.02.2013/7451/>.
5. Зубок М. І. Безпека банківської діяльності : навч. посіб. / М. І. Зубок. – К. : КНЕУ, 2002. – 190 с.
6. Конахович Г. Ф. Захист інформації від витоку по технічних каналах [Електронний ресурс] / Г. Ф. Конахович, Є. Л. Назаренко, В. М. Свириденко // Наукоємні технології. – 2009. – № 2. – С. 90-93. – Режим доступу : http://www.nbuv.gov.ua/Portal/natural/Nt/2009_2/20.pdf.
7. Корнієнко Ю. В. Фінансова безпека банків як об'єкт наукового дослідження [Електронний ресурс] / Ю. В. Корнієнко. – Режим доступу : <http://irbis.kneu.kiev.ua:8080/bitstream/2010/918/1/Kornienko.pdf>.
8. Методика розрахунку рівня економічної безпеки України від 02.03.2007 р. № 60 [Електронний ресурс] / Міністерство економіки України. – Режим доступу : http://www.me.gov.ua/control/uk/publish/printable_article?art_id=97980.
9. Основні показники діяльності банків України [Електронний ресурс] / Національний банк України. – Режим доступу : http://www.bank.gov.ua/control/uk/publish/article?art_id=36807&cat_id=36798.
10. Островська Н. С. Основні аспекти інформаційно-технічної безпеки комерційних банків України та їх вплив на спроможність виконувати ними свою місію [Електронний ресурс] / Н. С. Островська, І. М. Якуб'як // Фінансово-кредитна діяльність: проблеми теорії та практики : збірник наукових праць. – 2009. – № 1 (6). – Режим доступу : http://www.nbuv.gov.ua/Portal/Soc_Gum/Fkd/2009_1/R1/11.pdf.
11. Соколовский С. «Банковская безопасность – 2012»: на новые вызовы должны быть адекватные ответы [Электронный ресурс] / С. Соколовский // Банкирь. – 2012. – № 2 (40). – С. 22-23. – Режим доступа : <http://www.banksinfo.kiev.ua/files/Banker40/banker40.pdf>.
12. Соловійов В. І. Сучасний стан банківської безпеки України [Електронний ресурс] / В. І. Соловійов // Науковий вісник: Фінанси, банки, інвестиції. – 2011. – № 4. – С. 79-82. – Режим доступу : http://www.nbuv.gov.ua/portal/Soc_Gum/Nvfbi/2011_4/15.pdf.
13. Сороківська З. До питання фінансової безпеки в умовах світової економічної кризи [Електронний ресурс] / З. Сороківська // Економічний аналіз. – 2011. – № 8 (1). – С. 404-408. – Режим доступу : http://www.nbuv.gov.ua/portal/Soc_Gum/Ecan/2011_8_1/pdf/sorokivska.pdf.
14. Соціально-економічний розвиток України (щомісячна інформація) [Електронний ресурс] / Державна статистика України. – Режим доступу : <http://www.ukrstat.gov.ua/>.
15. Хитрін О. І. Фінансова безпека комерційних банків / О. І. Хитрін // Фінанси України. – 2004. – № 11. – С. 118-124.
16. European Cybercrime Centre (EC3) opens on 11 January [Electronic resource] / European Commission. – 2013. – Access mode : http://europa.eu/rapid/press-release_IP-13-13_en.htm?locale=en.