ДЕЯКІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВ

ЛИТВИН Наталія Анатоліївна - доктор юридичних наук, професор, професор кафедри службового та медичного права, Київський національний університет імені Тараса Шевченка, Київ, Україна.
https://orcid.org/0000-0003-4199-1413
СУБІНА Тетяна Володимирівна - кандидат юридичних наук, доцент кафедри фінансового права, Університету державної фіскальної служби України
https://orcid.org/0000-0001-7806-7828
DOI

За умов швидкого формування і розвитку інформаційного суспільства в Україні, глобального інформаційного простору та широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають питання інформаційної безпеки у сфері банківської діяльності. Актуальність даного питання є безперечною, оскільки банківська інформація повинна залишатися захищеною в будь-яких умовах, а захист банківської інформації є однією із складових національної безпеки України. Відповідно із цим 1 травня 2014 року виконуючий обов'язки Президента України, голова Верховної Ради України Олександр Турчинов підписав Указ № 449/2014 про рішення РНБО від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [1].

Окрема увага зверталася на види інформаційних загроз та кіберзлочинності у банківській діяльності.

У статті досліджено генезис думок провідних фахівців у сфері забезпечення інформаційної безпеки банків, розкрито основні об'єкти та суб'єкти інформаційної безпеки банків. Проаналізовано правові, технічні (програмні), організаційні заходи забезпечення інформаційної безпеки банків.

Визначено, що одним із основних напрямів удосконалення правового регулювання інформаційної безпеки у сфері банківської діяльності є прийняття «Банківського кодексу», який повинен містити норми, що будуть розкривати стан чинних нормативно-правових актів та прямо чи опосередковано регулювати відносини у банківській діяльності.

Ключові слова: інформаційна безпека, захист інформації, банківська інформація, банк, банківські установи, банківська діяльність.

Постановка проблеми

Аналіз суспільних процесів, що відбуваються останніми роками під натиском інформаційного розширення у всіх сферах життя в Україні та світі, дозволяє говорити про підхід до глобального інформаційного суспільства. Водночас створюються можливості для настання бажаних та загрозливих наслідків як для суспільства в цілому, так і для окремої людини. Сучасна людина в інформаційному суспільстві занурена у світ технологій та всеохоплюючої інформації. Інформаційні технології (ІТ) активно використовуються в кожній сфері життя суспільства, що призводить до зростання інформаційного впливу. Динамічний розвиток реальності також потребує перегляду підходів до розуміння безпеки суспільства, держави та, насамперед, людини. Бачення безпеки, яке виникло наприкінці XX століття, базувалося на відсутності небезпеки чи нейтралізації загроз і було, насамперед, адаптоване до потреб держави, було не здатне відобразити сутність людської безпеки в сучасному глобалізованому та інформаційно- збагаченому світі [2, с. 477 – 478].

Відповідно до ст. 17 Конституції України захист інформаційної безпеки, нарівні із за-

хистом суверенітету та територіальної цілісності України, є найважливішою функцією держави та справою всього Українського народу, тож інформаційна безпека, безперечно, є однією з найважливіших складових національної безпеки України. Оскільки інформаційна сфера має своїм змістом знання про інші сфери життєдіяльності суспільства, вона одночасно існує як самостійно, так і у взаємозв'язку з іншими сферами, так як здійснює їх «інформаційне обслуговування» за допомогою інформації [3 с. 90]. Між тим, інформаційна безпека в банках є одним із найпотужніших важелів існування демократичного інформаційного суспільства, що дозволяє забезпечити конфіденційність, цілісність та доступність банківської інформації.

У свою чергу, конфіденційність, цілісність та доступність банківської інформації є стан стійкої життєдіяльності, за допомогою якої забезпечується реалізація основних інтересів, пріоритетних цілей банків, захисту від зовнішніх і внутрішніх дестабілізуючих факторів незалежно від їх умов функціонування. Стабільність фінансового та економічного стану банків та банківських установ є основним критерієм ефективної та безперервної роботи банків [4, с. 211 – 215].

Таким чином, розвиток інформаційно-комунікаційних технологій в усіх сферах життєдіяльності зумовлює дослідити питання забезпечення інформаційної безпеки в банках, що є актуальним на сьогодні, оскільки банківська інформація повинна залишатися захищеною за будь-яких умов, а інформаційна безпека є однією із складових національної безпеки держави.

Стан дослідження

Забезпечення інформаційної безпеки та кібербезпеки в банківських установах представлено у роботах вітчизняних та зарубіжних учених, а саме: А. Баланди, О. Василика, Є. Бєлоусова, А. Даниленка, М. Зубка, А. Марущака, Д. Мороза, А. Нікіфорова, О. Орлюк, О. Пилипченка, А. Шапки та ін. Але із стрімким розвитком інформатизації в усіх сферах діяльності питання захисту банківської інформації ще потребує подальшого вивчення, зокрема у сфері забезпечення інформаційної безпеки банків.

Метою статті є аналіз сучасного стану інформаційної безпеки та її правового забезпечення в банківських установах України.

Виклад основних положень

Постійна цифрова трансформація фінансового сектора, яка спричинена COVID-19, призвела до зростання інформаційних загроз та кіберзлочинності.

Зростання жорстоких кібератак на фінансові установи у 2020 році показало, що 10% даних порушень були пов'язані з фінансовою індустрією. Згідно з повідомленнями про зазначені порушення Міністерства фінансів США та Центрального банку Нової Зеландії за 2021 р. орієнтовний збиток від кібератак на фінансові установи склав понад 18,3 млн доларів [5].

Зважаючи на це, можна виокремити п'ять кібер-ризиків, які кожна фінансова установа повинна передбачити та захиститися від них, а саме:

1. Наповнення довірених даних - це тип кібератаки, який зазвичай націлений на особисті дані клієнтів банків. Використовуючи викрадені дані облікових записів, хакери можуть отримати несанкціонований доступ до облікових записів користувачів за допомогою автоматизованих масштабних запитів на вхід. Потім викрадену інформацію можна використовувати для бомбардування вебсайтів та серверів, щоб спробувати отримати доступ до критичної IT-інфраструктури. Ця практика відома як обліковий запис.

2. Хмарні постачальники. Тобто хмарні сервіси, які допомагають банкам компенсувати витрати на інформаційні технології, а саме збільшують час роботи системи та забезпечують безпечне зберігання їх даних.

3. Фішинг атаки, а саме фішинг - це поширений тип кібератаки, який часто використовується для крадіжки даних користувачів, включаючи облікові дані для входу та номери кредитних карт. Останнім часом спостерігається зростання фішинг-атак, спрямованих на працівників банку.

4. Ransomware (викуп) - це тип зловмисного програмного забезпечення, яке шиф-

рує дані, унеможливлюючи доступ власників цих даних до них, якщо вони не сплачують відповідну плату.

5. Проблемна експлуатація, що випливає з неналежної експлуатації та вразливості програмного забезпечення та частин обладнання. Усе, від пристрою працівника до маршрутизатора, підключеного до незахищеної мережі, може поставити під загрозу цифрову інфраструктуру всієї організації [6].

Заросило В.О. зазначає, що у режимі реального часу (on-line), саме інформаційно-комунікаційними засобами підвищується імовірність злочинного проникнення в інформаційні системи банків. Отже, високопродуктивні інтегровані системи повинні працювати в режимі безперервного і безвідмовного оброблення банківської інформації з використанням специфічного програмного забезпечення та систем управління баз даних банків, які повинні забезпечувати не лише багатофункціональність, а й інформаційну безпеку [7].

Відповідно доцільно вказати на те, що діяльність будь якої установи чи організації стосовно питань інформаційної безпеки повинна ґрунтуватися на системі заходів безпеки. Основними джерелами вимог інформаційної безпеки в банках є:

1) результат оцінювання ризиків для організації, який враховує загальну бізнес-стратегію та цілі (під час оцінювання ризику ідентифікують загрози ресурсам СУІБ і оцінюють вразливість та ймовірність подій і визначають величину потенційного впливу);

2) правові вимоги, визначені законодавством, договорами і угодами організації з партнерами;

3) власний набір принципів, цілей та бізнес-вимог щодо оброблення інформації, який розроблено організацією для підтримки свого функціонування [8].

Також актуальним є питання захисту інформації в банківських системах. Для цього варто створити систему інформаційної безпеки банківської установи, яка буде полягати у розробці концепції формування системи інформаційного безпеки, створенні служби інформаційної безпеки або розподілі функцій між дійсними підрозділами, оцінці стану системи інформаційної безпеки та функціонуванні системи інформаційної безпеки банківської установи [11].

Серед загроз інформаційній безпеці банківських установ доцільно виділити:

– протиправне збирання інформації та її використання;

– порушення технології і правил опрацювання інформації;

– впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби;

– розроблення і поширення програм, що порушують нормальне функціонування інформаційно-телекомунікаційних систем банківських установ;

– несанкціонований доступ до інформації, що є в банківських установах і їхніх базах даних;

– перехоплення інформації, що циркулює в засобах і системах зв'язку та обчислювальної техніки, за допомогою технічних засобів негласного зняття інформації, несанкціонованого доступу до інформації та навмисних технічних впливів на них у процесі обробки та зберігання;

– підслуховування з використанням технічних засобів конфіденційних переговорів, що ведуться в службових приміщеннях [9, с. 37; 10, с. 22].

Отже, можна зазначити, що інформаційна безпека в банках складається із комплексу засобів організаційного-програмного забезпечення та заходів, які передбачають використання сучасних механізмів захисту інформації з обмеженим доступом, забезпечують конфіденційність та цілісність такої інформації, сприяють протидії поширенню інформаційних загроз.

Щодо заходів забезпечення інформаційної безпеки, то доцільно погодитись з думкою Мельниченка О. В., який узагальнив бачення різних науковців та виокремив наступні заходи забезпечення інформаційної безпеки:

– організаційні – підготовка персоналу, налагоджена структура служби охорони, наявність та якість аналітичних служб;

– технічні (програмні) – спрямовані на обмеження програмно-апаратного доступу до інформаційної системи;

– правові – полягають у формуванні правил поведінки персоналу, формуванні методик виявлення та розкриття правопорушень за допомогою інформаційних систем і технологій [12, с. 4, 6].

Розкриваючи ці три класифікаційні складові можна зазначити, що питання інформаційної безпеки в банках регулюється нормативно-правовими актами, а саме: Законами України «Про Національний банк України», «Про банки і банківську діяльність», «Про інформацію» «Про основні засади забезпечення кібербезпеки України», Про електронні документи та електронний документообіг», «Про електронні довірчі послуги», з урахуванням Директиви Європейського парламенту і Ради (ЄС) 2016/1148 від 06 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу щодо питань організації та управління інформаційною безпекою. Окреме місце займають положення Національного Банку України «Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», затвердженого постановою Правління Національного банку України від 28 вересня 2017 року № 95, «Положення про кваліфікованих надавачів електронних довірчих послуг», «Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг», що встановлює вимоги до проведення банками самооцінки стану інформаційної безпеки та кіберзахисту. Банки зобов'язані щорічно проводити відповідну самооцінку, складати і подавати Національному банку щорічний звіт з питань оцінювання ризиків інформаційної безпеки та кіберризиків [13]. Усі ці нормативно-правові акти ставлять за мету виявлення та усунення можливостей нанесення збитків банкам та їх клієнтам, а також регулюють ефективність і якість їх діяльності.

Можна говорити про те, що на теперішній час не існує єдиного систематизованого нормативно-правового акта, який би регулював питання інформаційної безпеки в банках.

Розкриваючи технічні (програмні) заходи забезпечення інформаційної безпеки відповідно до державного стандарту України 3396.2 – 97, можна визначити складові організації технічного захисту інформації, а саме:

1. Система технічного захисту інформації – це сукупність організаційних структур, нормативно-правових документів і матеріально-технічної бази. Основними елементами матеріально-технічної бази системи ТЗІ є технічні засоби із захистом, засоби технічного захисту інформації та засоби контролю за ефективністю технічного захисту інформації.

2. Зони безпеки інформації – це простір, у межах якого інформація убезпечена.

3. Рівень (технічного) захисту інформації – це сукупність вимог, у тому числі нормативних, що визначаються режимом доступу до інформації та загрозами її безпеці.

4. Ефективність (технічного) захисту інформації – це ступінь відповідності вжитих заходів щодо технічного захисту інформації встановленим вимогам [14, с. 9].

Напрями розвитку технічного захисту інформації визначаються необхідністю у своєчасному вжитті заходів, адекватних масштабам загроз для інформації, і ґрунтуються на засадах правової демократичної держави відповідно до прав суб'єктів інформаційних відносин на доступ до інформації та її захист. Технічний захист інформації – є частиною забезпечення інформаційної безпеки України. Якщо їх розглядати тільки як сукупність, то інформаційна безпека як система є досить умовною, яка так чи інакше екстраполюється на якісні ознаки системності.

Розглянемо поняття «технічний захист інформації» за його системними ознаками. Технічний захист інформації є частиною організації інформаційної безпеки. Він може розглядатися як діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства держави [15].

Крім того, технічний захист інформації визначено як діяльність, що спрямована на запобігання витоку інформації технічними каналами, її блокування та порушення цілісності [14, с. 7].

Відповідно до організаційних заходів забезпечення інформаційної безпеки банку відноситься: розробка інструкцій для користувачів та обслуговуючого персоналу, адміністрування компонентів системи, обліку, зберігання, розмноження, знищення носіїв, конфіденційної інформації користувачів, розробка правил дій у разі виявлення спроб несанкціонованого доступу до ресурсів системи засобів захисту, виникнення надзвичайних ситуацій і навчання правилам інформаційної безпеки банків. Національний банк України та комерційні банки як юридичні особи створюють нормативні та локальні документи, у яких визначаються правила про інформаційну безпеку.

Інформаційна безпека має виключати будь-який несанкціонований доступ до інформації, що має забезпечуватися зберіганням конфіденційності, цілісності й доступності інформації. Також можуть враховуватися і інші властивості, а саме: автентичність, відстежуваність, неспростовність та надійність. Для банків України відстежуваність, неспростовність, надійність та автентифікація користувачів та інформаційних ресурсів є обов'язковими вимогами інформаційної безпеки [16, с. 81].

Висновок

Аналіз локальних документів дійсних банків на сьогодні показав, що вони регулюються своїми правовими актами, які видані правлінням банку, що забезпечують політику інформаційної безпеки. Положення про політику інформаційної безпеки кожного банку включає в себе основні цілі та визначення щодо забезпечення інформаційної безпеки.

Банківська діяльність в умовах сьогодення повинна ґрунтуватися на системі заходів безпеки і залежить від надійної інформаційної безпеки як в організаційній, технічній (програмній), так і в правовій сферах. Але відсутність єдиного комплексу заходів щодо забезпечення інформаційної безпеки банків ускладнює захист банківської інформації від загроз, зокрема кібератак.

Для забезпечення інформаційної безпеки в банківських установах України доцільно узгодити вже чинні нормативно-правові акти у сфері забезпечення інформаційної безпеки шляхом їх систематизації, а саме прийняття «Банківського кодексу» у якому комплексно розглядалися б питання (або заходи), що дозволять забезпечити конфіденційність, цілісність та доступність банківської інформації.

Література

1. Заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України: Указ № 449/2014 про рішення РНБО від 28 квітня 2014 року. URL: https://zakon.rada.gov.ua/laws/show/n0004525-14 (дата звернення 09.10.2021).

2. Fedorenko, V.; Lytvyn, N.; Luchenko, D.; Panova, I.; Tsybulnyk, N. Legal aspects of information security management in the conditions of Ukraine's European integration. *Journal of Security and Sustainability Issues* 10 (2) : 2020 Volume 10 Number 2 December. P. 477 – 489. http://www.tb.lt/Leidiniai/Journal%20of%20Security%20and%20Sustainability%20Issues/10/10-2/2020-10(2)-full.pdf.

3. Довгань О., Ткачук Т. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. 2018. № 1(24)- С. 89 – 103

4. Орлюк О. П. Банківське право : навч. пос. Київ : Юрінком Інтер, 2004. 376 с.

5. Top 5 Cyber Threats Facing Banks in 2021 : веб-сайт. ULR: https://hubsecurity.io/top-cyber-threats-facing-banks-in-2021/ (дата звернення 13.10.2021).

6. Top 5 Cyber Threats Facing Banks in 2020 : веб-сайт. ULR: https://hubsecurity.io/top-5-cyber-threats-facing-banks/ (дата звернення 13.10.2021).

7. Заросило В. Загрози фінансовій безпеці та їх класифікація. *Міжрегіональна Академія управління персоналом*. 2017. № 52 (1). С.17 – 22.

8. Інформаційна безпека банківської установи. ULR: http://obt.inf.ua/page10.html (дата звернення 26.10.2021).

9. Бєлоусова К.І., Бєлоусов Я.І. Забезпечення інформаційної безпеки – реалізація стратегії банківської установи. *Науковий-вісник ДУІКТ*. 2010. С. 33-38.

10. Марущак А.І. Інформаційна безпека банківської установи: структура та система забезпечення. *Протидія злочинам, які вчиняються з використанням комп'ютерних мереж* [Текст] : тези доповідей Міжнародної науково-практичної конференції (м. Севастополь, 1–2 жовтня 2010 року) / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». Суми : ДВНЗ «УАБС НБУ», 2010. С. 21-24.

11. Кібальник Л. О., Напора І. Ю. Концептуальний підхід до формування інформаційної безпеки банківських установ в системі економічної безпеки. *Ефективна економіка*. 2016. № 12. ULR: http://www.economy.nayka.com.ua/?op=1&z=530 (дата звернення 17.10.2021).

12. Мельниченко О.В. Аудит інформаційної безпеки банку при роботі з електронними грошима. *Проблеми економіки*. 2013 № 4. С. 341 – 347.

13. Контроль за кіберзахистом та інформаційною безпекою банків посилюється : веб-сайт. ULR: https://bank.gov.ua/ua/news/all/kontrol-za-kiberzahistom-ta-informatsiynoyu-bezpekoyu-bankiv-posilyuyetsya (дата звернення 09.10.2021).

14. ДСТУ 3396.2 – 97. Технічний захист інформації. Державний стандарт [Чинний від 1998-01-01]. Вид. офіц. Київ: Держкомстат України, 1997. 15 с.

15. Концепція технічного захисту інформації в Україні : Постанова Кабінету Міністрів України від 08.10.1997 р. № 1126. ULR: http://zakon.rada.gov.ua/cgi-bin/laws/main. cgi?nreg=1126-97-%EF (дата звернення 09.10.2021).

16. Отенко І. П. Мішин О. Ю. Мішина С. В. Організація та управління фінансово-економічною безпекою банківських установ : навч. посіб. Херсон : ХНЕУ ім.-С. Кузнеця, 2015. 240 с.

***Lytvyn Nataliia Anatoliivna**, Doctor of Law, Professor, Professor of the Department of Service and Medical Law, Taras Shevchenko National University of Kyiv*
64/13, Volodymyrska Street, City of Kyiv, Ukraine, 01601
Lna_70@ukr.net
https://orcid.org/0000-0003-4199-1413
***Subina Tatiana Volodymyrivna,** Candidate of Juridical Sciences, Associate Professor of Department of Financial Law, University of State Fiscal Service of Ukraine, Universytetska Str., 31, City of Irpin, Bouchansky District, the Kyiv Region, 08205*
Subinatv@ukr.net
https://orcid.org/0000-0001-7806-7828

SOME ASPECTS OF INFORMATION SECURITY OF BANKS

In the context of the rapid formation and development of the information society in Ukraine, the global information space and the widespread use of information and communication technologies in all spheres of life, the issues of information security in the field of banking are of particular importance. The relevance of this issue is indisputable, since banking information must remain protected in any conditions, and the protection of banking information is one of the components of the national security of Ukraine. In accordance with this, on May 1, 2014, Acting President of Ukraine, Chairman of the Verkhovna Rada of Ukraine Alexander Turchinov signed Decree № 449/2014 on the decision of the National Security and Defense Council of April 28, 2014 "On measures to improve the formation and implementation of state policy in information security of Ukraine".

Special attention was paid to the types of information threats and cybercrime in banking.

The article examines the genesis of the opinions of leading experts in the field of ensuring information security of banks, discloses the main objects and subjects of information security of banks. The legal, technical (software), organizational measures to ensure the information security of banks have analyzed.

It was determined that one of the main directions of improving the legal regulation of information security in the field of banking is the adoption of the "Banking Code", which should contain norms that disclose the state of the current regulatory legal acts and directly or indirectly regulate relations in banking.

Key words: information security, data protection, banking information, bank, banking institutions, banking.