УДК 347.73
DOI 10.33244/2617-4154.3(12).2023.364-371

І. Є. Швайко,
здобувач першого (бакалаврського) рівня вищої освіти,
Державний податковий університет
e-mail: svaikoivan@gmail.com
ORCID ID 0009-0003-6429-2620

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БАНКАХ

Актуальність цієї теми є безперечною, оскільки забезпечення інформаційної безпеки в банках є однією із складових національної безпеки. Забезпечення захисту інформації в банках на сьогодні є зміцнення самої української держави. У зв'язку з цим є потреба у попередженні та протидії загрозам інформаційної безпеки в банках, пошуку принципово нових, нестандартних форм діяльності, удосконаленні всіх засобів, спрямованих на забезпечення процесу управління загрозами та небезпеками.

Визначено, що забезпечення інформаційної безпеки України ґрунтується на принципах верховенства права, законності та пріоритету додержання прав і свобод людини та громадянина; своєчасності й адекватності заходів захисту національних інтересів України від зовнішніх і внутрішніх загроз в інформаційній сфері; невідворотності відповідальності за вчинення злочинів та правопорушень; комплексності і безперервності заходів у сфері забезпечення інформаційної безпеки і захисту інформації; пріоритетності запобіжних заходів; взаємодії органів державної влади та чіткого розмежування їх повноважень; дієвості, комплексності і постійності заходів із захисту інформації та інформаційних ресурсів в інформаційному просторі; пріоритетності національної інформаційної продукції; зниження рівня технічної анонімності з одночасним підвищенням захисту персональних даних.

***У статті проаналізовано генезис наукових думок про сутність та понятійний апарат «інформаційної безпеки». Особлива увага зверталася на** особливості, принципи та цілі, **аналіз, способи, засоби щодо забезпечення інформаційної безпеки в банках.** Отже, розвиток України як суверенної, демократичної, правової, економічні та стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки в усіх сферах суспільного життя.*

***Ключові слова:** інформаційна безпека, інформаційні технології, забезпечення інформаційної безпеки, захист інформації, банківський захист.*

У зв'язку із швидким формуванням і розвитком інформаційного суспільства в Україні та постійним використанням інформаційно-комунікаційних технологій у всіх сферах суспільного життя виникає потреба в інформаційній безпеці, зокрема в банках.

Банк – це юридична особа, яка на підставі банківської ліцензії має виключне право надавати банківські послуги [1].

Забезпечення інформаційної безпеки в банках є досить важливою складовою банківської діяльності. Під інформаційною безпекою розуміється захищеність банківської інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного чи штучного характеру, які можуть завдати збитків суб'єктам інформаційних відносин і банківських правовідносин.

На сьогодні питання щодо протидії загрозам інформаційній безпеці в банках є актуальним, оскільки останнім часом досить багато науковців та аналітиків приділяють увагу інформаційній безпеці в банківській діяльності, справедливо вважаючи, що вона є однією з основних складових національної безпеки України.

Забезпечення інформаційної безпеки в банківській діяльності, шляхи попередження загроз і цілісність банківської інформації розглядали такі вітчизняні та зарубіжні вчені, як: Б. П. Адамик, В. А. Гамза, М. І. Зубок, І. С. Литвин, А. І. Марущак, І. Б. Ткачук, В. О. Ткачук, О. П. Орлюк, С. М. Побережний, Т. В. Субіна тощо. Але це питання потребує постійного вивчення, оскільки загрози в банківській сфері з кожним днем стрімко зростають.

Відповідно до положень Доктрини інформаційної безпеки України є створення розвиненого національного інформаційного простору і захист її інформаційного суверенітету.

Забезпечення інформаційної безпеки України ґрунтується на принципах:

– верховенства права, законності та пріоритету додержання прав і свобод людини та громадянина;

– своєчасності й адекватності заходів захисту національних інтересів України від зовнішніх і внутрішніх загроз в інформаційній сфері;

– невідворотності відповідальності за вчинення злочинів і правопорушень в інформаційній сфері та забезпечення відновлення порушених прав і законних інтересів, відшкодування збитків, шкоди, завданої цими злочинами;

– комплексності та безперервності заходів у сфері забезпечення інформаційної безпеки і захисту інформації;

– пріоритетності запобіжних заходів;

– взаємодії органів державної влади та чіткого розмежування їх повноважень у вирішенні питань забезпечення інформаційної безпеки;

– партнерства держави та приватного сектору у виробленні нових, оптимальних рішень у сфері інформаційної безпеки та участі інституцій громадянського суспільства у забезпеченні інформаційної безпеки держави;

– дієвості, комплексності і постійності заходів із захисту інформації та інформаційних ресурсів в інформаційному просторі;

– пріоритетності національної інформаційної продукції;

– зниження рівня технічної анонімності з одночасним підвищенням захисту персональних даних [2].

У ст. 17 Конституції України захист інформаційної безпеки нарівні із захистом суверенітету та територіальної цілісності України є найважливішою функцією держави

та справою всього Українського народу, тому 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, тому що здійснює їх «інформаційне обслуговування» за допомогою інформації [3, с. 90].

Особливості інформаційної безпеки банку продиктовані специфікою і самою банківською інформацією, і систем її оброблення. Основні ознаки цієї специфіки:

– збережена й оброблювана в банківських системах інформація є великою 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 значної кількості клієнтів – фізичних та юридичних осіб і, як правило, вона є конфіденційною. Тому банк зобов'язаний відповідати перед своїми клієнтами та забезпечувати необхідний ступінь 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 [4].

Розкриваючи дефініції інформаційної безпеки, варто зазначити, що Л. Задорожня пропонує визначення інформаційної безпеки, з одного боку, як захист інформації і особливо як захист інформації з обмеженим доступом (зокрема, персональних даних), з іншого – як захист інформаційних систем, які фактично є засобом передачі банківської інформації [5, с. 20].

В. Лизанчук, який зазначив, що завдання інформаційної безпеки – це створення системи протидії інформаційним загрозам і захист власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави та банків зокрема [6].

О. Барановою, яка розглядає інформаційну безпеку, зокрема в банках, як стан захищеності життєво важливих інтересів особистості, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, несвоєчасність і недостовірність інформації, через негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [7].

Інформаційна безпека – це формування інформаційних ресурсів банку та організація гарантованого їх захисту. Досягається створенням у банку системи збору й обробки інформації, проведенням відповідних заходів щодо їх зберігання та розподілу, визначенням категорій і статусу банківської інформації, порядку і правил доступу до неї, дотриманням усіма працівниками, клієнтами й акціонерами банку норм і правил роботи з банківською інформацією, своєчасним виявленням спроб і можливих каналів витоку інформації зокрема та їх об'єднанням або перетинанням [8].

До основних цілей забезпечення інформаційної безпеки належать забезпечення таких властивостей інформації:

– конфіденційність (confidentiality) – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем та/або процесом;

– цілісність (integrity) – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем та/або процесом. Цілісність системи (system integrity) – властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки;

– доступність (availability) – властивість ресурсу системи, яка полягає в тому, що користувач та/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він перебуває у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний;

– спостережність (accountability) – властивість системи, що дає можливість фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно встановлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки та/або забезпечення відповідальності за певні дії [9].

Забезпечення інформаційної безпеки доцільно використання систем дистанційного банківського обслуговування, а саме:

– проведення аналізу програмного забезпечення, встановленого на вебсерверах систем «Клієнт-Інтернет-Банк», а також клієнтських частин систем дистанційного банківського обслуговування, встановлених у клієнтів;

– вжиття заходів щодо оновлення застарілих версій програмного забезпечення і встановлення актуальних оновлень безпеки та щодо усунення вразливостей програмного забезпечення банківського обслуговування, операційних систем;

– застосовування захищених носіїв ключової інформації для накладання електронного цифрового підпису та методи багатофакторної автентифікації;

– розробка порядок дій працівників і клієнтів банку у випадках виявлення несанкціонованого доступу (чи підозри у спробі доступу) до рахунку;

– визначити уповноважених осіб банку, які відповідатимуть за взаємодію з правоохоронними органами, та порядок такої взаємодії у разі виявлення несанкціонованих операцій, здійснених із використанням систем дистанційного банківського обслуговування;

– постійне проведення роз'яснювальної роботи серед клієнтів щодо:

а) необхідним дотримання вимог з питань захисту інформації на робочих місцях, де встановлено систему дистанційного банківського обслуговування;

б) належного поводження з носіями ключової інформації системи дистанційного банківського обслуговування (розроблення та доведення до клієнтів типових рекомендацій / інструкцій для роботи на комп'ютерах, де встановлюються клієнтські частини дистанційного банківського обслуговування;

в) правил використання та зберігання носіїв ключової інформації [10].

Після повномасштабного вторгнення та територію України був підписання Указ Президента України про запровадження воєнного стану, та Правлінням національного

банку України видано Постанову від 24.02.2022 № 18 «Про роботу банківської системи в період запровадження воєнного стану» [11].

Відповідно до положень вищезазначеної Постанови:

– банки продовжують роботу з урахуванням обмежень, визначених цією Постановою;

– банки забезпечують роботу відділень у безперебійному режимі в умовах відсутності загрози життю та здоров'ю населення;

– безготівкові розрахунки здійснюються без обмежень;

– банкомати поповнюються готівкою без обмежень;

– забезпечується доступ до сейфових скриньок у безперебійному режимі;

– платежі уряду здійснюються без обмежень згідно із законодавством про особливий період [12, с. 13].

Розкриваючи реалії сьогодення, а саме на прикладі ПриватБанку, то на початку війни Національний банк України дозволив створення резервних копій для всіх банків у хмарному сховищі. ПриватБанк оперативно за шість днів цілодобового зашифрованого копіювання забезпечив стабільність роботи банку.

Уся банківська система ПриватБанку працює над міграцією інформаційних технологій систем з фізичного центру зберігання даних у хмарі з метою мінімізувати залежність від фізичної присутності комп'ютерного обладнання, розташованого в різних регіонах України, яке могло бути знищено під час війни. У результаті усі основні застосунки ПриватБанку було успішно перенесено у хмарне сховище, щоб забезпечити доступ клієнтів до фінансових послуг у будь-який момент.

Ключові факти про цю міграцію у хмарне середовище:

– менше 45 днів знадобилося, щоб усі важливі застосунки безпечно розмістити і запустити в роботу з хмарного середовища;

– перенесено 3 500 серверів;

– понад 4 петабайт клієнтських даних і транзакцій завантажено у хмару;

– 270 важливих застосунків перенесено.

Для порівняння: обсяг робіт, який реалізував ПриватБанк щодо своєї фінансової безпеки для проєктів такої складності і такого масштабу у проєктному інформаційно-технологічному циклі, зазвичай займає 1,5 роки і більше [13].

Отже, під час уже тривалого часу в умовах війни банки забезпечують інформаційний захист банківської інформації та продовжують працювати і надавати послуги клієнтам. Але необхідним питання є забезпечення значного обігу коштів для того, щоб банки були достатньо прибутковими.

З вищевикладеного можна зробити висновки, що забезпечення інформаційної безпеки банків є однією із основних умов існування демократичного інформаційного суспільства, що дозволить забезпечити конфіденційність, цілісність, доступність інформації тощо. Це є одним із найпотужніших важелів в економічних відносинах, від якого значно залежить формування національної безпеки як у мирний час, так і під час війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про банки і банківську діяльність : Закон України від 28.04.2020 № 2121-III. URL : https://www.tax.gov.ua/zakonodavstvo/podatkove-zakonodavstvo/zakoni-ukraini/31131.html (дата звернення: 10.04.2023).

2. Про Доктрину інформаційної безпеки України / Законодавство України. *Відомості Верховної Ради України*. URL : http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025 (дата звернення: 14.04.2023).

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

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

5. Задорожня Л. До питання огляду законодавства в інформаційній сфері. 2004. № 3. С. 20.

6. Лизанчук В. Свобода слова в контексті українського державотворення. URL : http://www.franko.lviv.ua/faculty/jur/Internet/PART-1_7.htm (дата звернення: 10.04.2023).

7. Інформаційна безпека України. Сутність та проблеми : матеріали круглого столу. URL : http://www.niurr.gov.ua/ukr/publishing/panorama3_4/ kr_stil_a.htm (дата звернення: 15.04.2023).

8. Банківська безпека / Офіційний вебсайт Вікіпедії. URL : http://surl.li/akwny (дата звернення: 15.04.2023).

9. Охорона банківської таємниці правові засади. URL : http://obt.inf.ua/page10.html (дата звернення: 20.04.2023).

10. Захист прав споживачів фінансових послуг на деокупованих територіях України : практичний посібник клініциста / Шолкова Т. О., Кармаліта М. В., Мацелик Т. О. Субіна Т. В. Київ : Алерта, 2020. 270 с.

11. Про роботу банківської системи в період запровадження воєнного стану : постанова Правління національного банку України від 24.02.2022 № 18. URL : https://zakon.rada.gov.ua/laws/show/v0018500-22#Text (дата звернення: 25.04.2023).

12. Бугера Д. М. Робота банківської системи в умовах воєнного стану. *Реалії сьогодення у банківській діяльності України* : матеріали наукового семінару. м. Ірпінь, 18 жовтня 2022 року. Ірпінь. 2022. С. 76.

13. Чорноіван Я. С. Фінансова безпека ПриватБанку під час воєнного стану. *Реалії сьогодення у банківській діяльності України* : матеріали наукового семінару. м. Ірпінь, 18 жовтня 2022 року. Ірпінь. 2022. С. 76.

REFERENCES

1. Pro banky i bankivsku diialnist : Zakon Ukrainy vid 28.04.2020 № 2121-III. URL : https://www.tax.gov.ua/zakonodavstvo/podatkove-zakonodavstvo/zakoni-ukraini/31131.html (data zvernennia: 10.04.2023).

2. Pro Doktrynu informatsiinoi bezpeky Ukrainy / Zakonodavstvo Ukrainy. *Vidomosti Verkhovnoi Rady Ukrainy*. URL : http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025 (data zvernennia: 14.04.2023).

3. Dovhan O., Tkachuk T. Systema informatsiinoi bezpeky Ukrainy: ontolohichni vymiry. *Informatsiia i pravo.* 2018. № 1(24) S. 89–103.

4. Zarosylo V. O. Zahrozy finansovii bezpetsi ta yikh klasyfikatsiia. *Mizhrehionalna Akademiia upravlinnia personalom.* Kyiv, 2017. № 52(1). S. 17–22.

5. Zadorozhnia L. Do pytannia ohliadu zakonodavstva v informatsiinii sferi. 2004. № 3. S. 20.

6. Lyzanchuk V. Svoboda slova v konteksti ukrainskoho derzhavotvorennia. URL : http://www.franko.lviv.ua/faculty/jur/Internet/PART-1_7.htm (data zvernennia: 10.04.2023).

7. Informatsiina bezpeka Ukrainy. Sutnist ta problemy : materialy kruhloho stolu. URL : http://www.niurr.gov.ua/ukr/publishing/panorama3_4/kr_stil_a.htm (data zvernennia: 15.04.2023).

8. Bankivska bezpeka / Ofitsiinyi vebsait Vikipedii. URL : http://surl.li/akwny (data zvernennia: 15.04.2023).

9. Okhorona bankivskoi taiemnytsi pravovi zasady. URL : http://obt.inf.ua/page10.html (data zvernennia: 20.04.2023).

10. Zakhyst prav spozhyvachiv finansovykh posluh na deokupovanykh terytoriiakh Ukrainy : praktychnyi posibnyk klinitsysta / Sholkova T. O., Karmalita M. V., Matselyk T. O. Subina T. V. Kyiv : Alerta, 2020. 270 s.

11. Pro robotu bankivskoi systemy v period zaprovadzhennia voiennoho stanu : postanova Pravlinnia natsionalnoho banku Ukrainy vid 24.02.2022 № 18. URL : https://zakon.rada.gov.ua/laws/show/v0018500-22#Text (data zvernennia: 25.04.2023).

12. Buhera D. M. Robota bankivskoi systemy v umovakh voiennoho stanu. *Realii sohodennia u bankivskii diialnosti Ukrainy* : materialy naukovoho seminaru. m. Irpin, 18 zhovtnia 2022 roku. Irpin, 2022. S. 76.

13. Chornoivan Ya. S. Finansova bezpeka PryvatBanku pid chas voiennoho stanu. *Realii sohodennia u bankivskii diialnosti Ukrainy* : materialy naukovoho seminaru. m. Irpin, 18 zhovtnia 2022 roku. Irpin, 2022. S. 76.

I. Shvayko. Ensuring information security in banks

The relevance of this topic is indisputable, since ensuring information security in banks is one of the components of national security. Ensuring the protection of information in banks today is the strengthening of the Ukrainian state itself. In this regard, there is a need to prevent and counter threats to information security in banks, to find fundamentally new, non-standard forms of activity, to improve all means aimed at ensuring the process of managing threats and dangers.

It was determined that ensuring the information security of Ukraine is based on the principles of: the rule of law, legality and the priority of observing the rights and freedoms of a person and a citizen; the timeliness and adequacy of measures to protect the national interests of Ukraine from external and internal threats in the information sphere; the

inevitability of responsibility for committing crimes and offenses; the complexity and continuity of measures in the field of ensuring information security and information protection; priorities of preventive measures; interaction of state authorities and clear demarcation of their powers; the effectiveness, complexity and permanence of measures to protect information and information resources in the information space; priority of national information products; reducing the level of technical anonymity while simultaneously increasing the protection of personal data.

The article analyzes the genesis of scientific opinions about the essence and conceptual apparatus of "information security". Particular attention was paid to features, principles and goals, analysis, methods, means of ensuring information security in banks. Therefore, the development of Ukraine as a sovereign, democratic, legal, economically and stable state is possible only under the condition of ensuring the appropriate level of its information security in all spheres of public life.

Keywords: *information security, information technologies, ensuring information security, information protection, bank protection.*

Стаття надійшла до редколегії 11 квітня 2023 року