ІВАНОВ Юрій Анатолійович

СПІВВІДНОШЕННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БАНКІВСЬКІЙ СИСТЕМІ УКРАЇНИ ТА БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Постановка проблеми. В умовах гібридної війни проти нашої держави застосовуються різноманітні засоби, здатні завдати шкоди життєво важливим господарським об'єктам чи економіці держави загалом. При цьому однією з перших під удар потрапляє банківська система України, зокрема, її інформаційні ресурси. Тому інформаційна безпека в банківській системі потребує посиленої уваги при напрацюванні заходів щодо забезпечення безпеки критичної інфраструктури. Викладене зумовлює актуальність цієї статті.

Аналіз останніх досліджень і публікацій. Різні аспекти правового регулювання діяльності банків та банківської системи досліджують у своїх працях Ю. В. Ващенко, Д. О. Гетьманцев, А. І. Марущак, О. П. Орлюк та багато інших науковців. Безпосередньо на проблемах банківської безпеки зосередили свій науковий пошук М. П. Стрельбицький, Л. М. Стрельбицька та В. К. Гіжевський [1]. Захисту критичної інфраструктури присвячено системні багаторічні дослідження фахівців Національного інституту стратегічних досліджень, квінтесенцією яких стала опублікована у 2017 році колективна монографія за загальною редакцією О. Суходолі [2]. Водночас роль інформаційної безпеки у банківській системі в контексті захисту критичної інфраструктури детально не розглядалася.

Отже, **метою статті** є з'ясування співвідношення забезпечення інформаційної безпеки в банківській системі та безпеки критичної інфраструктури держави.

Виклад основного матеріалу. Актуалізація проблем у безпековій сфері зумовила прийняття у 2015 році оновленого варіанта Стратегії національної безпеки України [3], у якій значна увага приділена критичній інфраструктурі держави. Зокрема, пріоритетами забезпечення безпеки критичної інфраструктури визначено:

– комплексне вдосконалення правової основи захисту критичної інфраструктури, створення системи державного управління її безпекою;

– посилення охорони об'єктів критичної інфраструктури, зокрема енергетичної і транспортної;

– налагодження співробітництва між суб'єктами захисту критичної інфраструктури, розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям та реагування на них;

– розробка та запровадження механізмів обміну інформацією між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту чутливої інформації у цій сфері;

– профілактика техногенних аварій та оперативне і адекватне реагування на них, локалізація і мінімізація їх наслідків;

– розвиток міжнародного співробітництва у цій сфері.

Окремо визначено необхідність забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, що в подальшому деталізовано в Стратегії кібербезпеки України.

Наприкінці 2016 року питання захисту критичної інфраструктури стали предметом розгляду РНБО України. Відповідним рішенням було передбачено розробити за участю Служби безпеки України, Служби зовнішньої розвідки України і Національного банку України та внести в установленому порядку на розгляд Верховної Ради України проект Закону України «Про критичну інфраструктуру та її захист» [4]. При цьому чітко окреслено перелік питань, котрі мають бути врегульовані, зокрема, щодо:

1) створення державної системи захисту критичної інфраструктури;

2) визначення органу, відповідального за координацію діяльності із захисту критичної інфраструктури в мирний час та в умовах особливого періоду;

3) визначення функцій, повноважень та відповідальності центральних органів виконавчої влади та інших органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів об'єктів критичної інфраструктури;

4) запровадження єдиної методології проведення оцінювання загроз критичній інфраструктурі та реагування на них, зокрема, щодо аварій і технічних збоїв, небезпечних природних явищ, зловмисних дій;

5) запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації;

6) засад державно-приватного партнерства та ресурсного забезпечення у сфері захисту критичної інфраструктури;

7) міжнародного співробітництва у сфері захисту критичної інфраструктури.

Відповідний законопроект підготовлений та розміщений на офіційному сайті Мінекономрозвитку України [5]. На відміну від усталеного розуміння інфраструктури як галузей, що «обслуговують» населення або інші галузі економіки (транспорт, енергетика, житлово-комунальне господарство тощо), у пропонованому законопроекті втілено концепцію розширювального тлумачення цього поняття, зокрема, у контексті визначення критичної інфраструктури та об'єктів, що до неї належать. Критичну інфраструктуру визначено як об'єкти, які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Згідно зі статтею 8 зазначеного проекту до об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи, організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема, у сферах централізованого водопостачання, централізованого водовідведення, постачання теплової енергії, гарячої води, електричної енергії і газу, виробництва продуктів, харчування, охорони здоров'я;

3) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

4) підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду;

5) є об'єктами підвищеної небезпеки;

6) є об'єктами, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру;

7) є об'єктами, порушення функціонування яких призведе до кризової ситуації регіонального значення.

Не випадково автори законопроекту на чільне місце серед об'єктів критичної інфраструктури, поряд з підприємствами, установами та організаціями, які провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, поставили об'єкти, що функціонують у банківському та фінансовому секторах. Такий підхід цілком віддзеркалює реалії сьогодення, адже саме банківська система опосередковує фінансові стосунки всіх без виключення суб'єктів господарювання, незалежно від форми власності та підпорядкування. Тому стабільність функціонування всіх інших об'єктів критичної інфраструктури значною мірою детерміновано стабільністю як банківської системи загалом, так і окремих банків у її складі.

Серед суб'єктів державної системи захисту критичної інфраструктури у статті 14 законопроекту названо й Службу безпеки України. При цьому варто уточнити, що йдеться про особливий різновид захисту – контррозвідувальний захист. Так, відповідно до статті 19 Закону України «Про національну безпеку України» [6] на СБ України покладається, серед іншого, контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, економічної та інформаційної безпеки держави, об'єктів критичної інфраструктури. Аналіз наведеного переліку об'єктів контррозвідувального захисту засвідчує, що банківська система у цілому підлягає захисту за напрямами кібербезпеки, економічної та інформаційної безпеки, а окремі банки – ще і як об'єкти критичної інфраструктури. При цьому очевидно недоцільно відносити до числа об'єктів критичної інфраструктури у банківській сфері всі існуючі в державі банки, адже впровадження системи заходів щодо їх захисту вимагатиме залучення значних фінансових та інших ресурсів. Натомість доцільно виокремити лише НБУ, як центральний банк держави, та ті банки, які є найбільш важливими в контексті стабільності банківської системи. Для цього необхідно визначитись із об'єктивними критеріями. З цією метою можна використати передбачений Законом України «Про банки і банківську діяльність» [7] інститут системно важливих банків. У статті 2 зазначеного закону визначено, що системно важливий банк – банк, що відповідає критеріям, встановленим Національним банком України, діяльність якого впливає на стабільність банківської системи. Відповідно до п. 3 Положення про порядок визначення системно важливих банків [8] НБУ визначає системно важливі банки за такими критеріями:

1) розмір банку. Показники, що характеризують цей критерій, такі:

– загальні активи;

– кошти фізичних осіб, суб'єктів господарювання та небанківських фінансових установ;

2) ступінь фінансових взаємозв'язків. Показники, що характеризують цей критерій, такі:

– кошти, розміщені в інших банках;

– кошти, залучені від інших банків;

3) напрям діяльності. Показником, що характеризують цей критерій, є кредити, що надані суб'єктам господарювання у промисловість, сільське господарство та будівництво.

Аналізуючи наведені критерії, можна зробити висновок, що вони цілком придатні й для характеристики банків в системі критичної інфраструктури. До того ж механізм оцінювання конкретного банку за цими критеріями достатнім чином формалізований і полягає у визначенні з математичною точністю показника системної важливості за формулою, наведеною у додатку до зазначеного вище Положення.

Стабільність функціонування банківської системи не в останню чергу залежить від ефективності дій НБУ, який в межах своєї компетенції має реалізовувати заходи щодо зміцнення банківської безпеки. При цьому слід враховувати, що на сьогодні банківська діяльність неможлива без широкого використання комп'ютерних технологій та інформаційно-телекомунікаційних мереж різного рівня та призначення. Тому, природно, що НБУ, як регулятор, зосередив увагу передусім на найбільш уразливому аспекті безпеки банківської системи – інформаційній безпеці. Зокрема, було розроблене та затверджене Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, в якому встановлено:

1) обов'язкові мінімальні вимоги щодо вжиття заходів із забезпечення інформаційної безпеки та кіберзахисту;

2) принципи управління інформаційною безпекою;

3) вимоги до інформаційних систем банку, що взаємодіють з інформаційними системами НБУ, з урахуванням напрямів розвитку криптографічного захисту інформації в інформаційних системах Національного банку.

Водночас вбачається, що у сфері кіберзахисту варто вдаватися до нестандартних рішень шляхом забезпечення постійної взаємодії НБУ, правоохоронних органів, банків, банківських спілок та асоціацій. Саме останні за сприяння НБУ могли б впровадити механізми недержавного фінансування заходів, адекватних сучасним загрозам. Використання принципу колективного захисту та поєднання зусиль державних органів й приватного сектору, сприятиме вдосконаленню системи кіберзахисту як окремих банків, так і банківської системи загалом.

Підсумовуючи викладене, можна сформулювати такі основні **висновки:**

– банківська система посідає особливе місце в економіці, оскільки обслуговує практично всі інші галузі і тому її належна захищеність від різноманітних загроз є неодмінною умовою забезпечення економічної безпеки держави;

– в умовах сьогодення інформаційна безпека у банківській системі є не лише ключовою складовою банківської безпеки, а й одним із визначальних чинників, що впливають на безпеку критичної інфраструктури держави;

– вдосконаленню системи забезпечення інформаційної безпеки у банківській системі може сприяти її доповнення недержавними механізмами, заснованими на принципі колективного захисту, які можуть бути реалізовані, зокрема, через банківські спілки та асоціації при збереженні загальної координуючої та спрямовуючої ролі НБУ.

Не применшуючи важливості інформаційної безпеки в банківській системі, необхідно також враховувати й інші аспекти банківської безпеки, на які доцільно спрямувати подальші дослідження.

Список використаних джерел

1. Стрельбицька Л. М. Банківське безпекознавство : навч. посіб. / Л. М. Стрельбицька, М. П. Стрельбицький, В. К. Гіжевський ; за ред. М. П. Стрельбицького. – Київ : Кондор, 2007. – 602 с.
2. Developing The Critical Infrastructure Protection System in Ukraine: monograph / [S. Kondratov, D. Bobro, V. Horbulin et al.] ; general editor O. Sukhodolia. – Kyiv : NISS, 2017. – 184 p.
3. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : Указ Президента України від 26 травня 2015 року № 287/2015 // Офіційний вісник України. – 2015. – № 43. – Ст. 1353.
4. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» : Указ Президента України від 16 січня 2017 року № 8/2017 // Офіційний вісник України. – 2017. – № 8. – Ст. 234.
5. Проект Закону України «Про критичну інфраструктуру та її захист» // Офіційний веб-сайт Міністерства економічного розвитку і торгівлі України [Електронний ресурс]. – Режим доступу : http:// www.me.gov.ua/Documents (дата звернення: 24.09.2018).
6. Про національну безпеку України : Закон України // Офіційний вісник України. – 2018. – № 55. – Ст. 1903.
7. Про банки і банківську діяльність : Закон України від 7 грудня 2000 року // Відомості Верховної Ради України. – 2001. – № 5–6. – Ст. 30.
8. Про затвердження Положення про порядок визначення системно важливих банків : постанова Правління НБУ від 25 грудня 2014 року № 863 // Офіційний вісник України. – 2015. – № 8. – Ст. 200.

Рецензенти:
доктор юридичних наук, професор
Л. Стрельбицька,
кандидат юридичних наук, доцент
В. Окіпнюк

Аннотация. В статье исследуются современные аспекты информационной безопасности в банковской системе в соотношении с безопасностью критической инфраструктуры государства.

Отмечается, что в условиях гибридной войны, когда против нашего государства применяются различные средства, способные нанести вред жизненно важным хозяйственным объектам или экономике государства в целом, одной из первых под удар попадает банковская система Украины, в частности ее информационные ресурсы. Поэтому информационная безопасность в банковской системе требует усиленного внимания при выработке мер по обеспечению безопасности критической инфраструктуры.
Ключевые слова: банковская система Украины, информационная безопасность, безопасность критической инфраструктуры.

Abstract. The article studies modern aspects of information security in the banking system in relation to the security of the critical infrastructure of the state. It is noted that in the conditions of hybrid war, when various means are used against our state that can harm the vital economic objects or the economy of the state as a whole. Banking system of Ukraine, in particular its information resources, is the first to be under the attack. That is why information security of the banking system should be in the focus of attention while developing the steps to provide critical infrastructure security.
Key words: banking system of Ukraine, information security, critical infrastructure security.