DOI 10.52363/2414-5866-2024-1-26
УДК 351.82:336.7

Жилін С.В., *аспірант НАУ, м. Київ, ORCID: 0009-0004-4717-1736*

Zhylin S., *Postgraduate student of the National Aviation University, Kyiv*

ПЕРСПЕКТИВИ РОЗВИТКУ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БАНКІВСЬКИХ УСТАНОВ У КОНТЕКСТІ ФОРМУВАННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

PROSPECTS FOR THE DEVELOPMENT OF STATE REGULATION REGARDING ENSURING THE SECURITY OF BANKING INSTITUTIONS IN THE CONTEXT OF THE FORMATION OF THE INFORMATION SOCIETY

Визначено перспективні напрямки розвитку державного регулювання щодо забезпечення безпеки банківських установ у контексті формування інформаційного суспільства в Україні. Серед цих напрямків обґрунтована важливість забезпечення безпеки як для громадян-користувачів банківських послуг, так і для самих банківських установ. Аргументовано це безпеку для цих суб'єктів забезпечувати, зокрема, за допомогою виваженого використання цифрових технологій і розвитку інформаційного суспільства. При цьому акцентовано, що банківські установи відносяться до об'єктів критичної інфраструктури, що зумовлює підвищення уваги до них. Проаналізовано чинне законодавство України у сфері функціонування зазначених об'єктів, що дозволило визначити напрямки удосконалення інституційного забезпечення безпеки у такій сфері.

Ключові слова: *державне регулювання, банківські установи, система безпеки, забезпечення безпеки банківських установ, розвиток інформаційного суспільства, цифрові технології, законодавство, Україна.*

Prospective directions for the development of state regulation regarding ensuring the security of banking institutions in the context of the formation of the information society in Ukraine have been determined. Among these directions, the importance of ensuring security for both citizens who use banking services and for the banking institutions themselves is substantiated. It is argued that security for these subjects should be ensured, in particular, with the help of a balanced use of digital technologies and the development of the information society. At the same time, it is emphasized that banking institutions are critical infrastructure objects, which causes increased attention to them. The current legislation of Ukraine in the field of operation of the specified objects was

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

analyzed, which allowed to determine directions for improving institutional security in this field.

Keywords: *state regulation, banking institutions, security system, security of banking institutions, development of information society, digital technologies, legislation, Ukraine.*

Постановка проблеми. Повномасштабна агресія рф проти України актуалізувала низку проблемних питань, зокрема, у сфері діяльності банківських установ, інформаційної безпеки, соціального забезпечення, функціонування критичної інфраструктури та ін. Складності ситуації додає те, що ці сфери взаємопов'язані та зумовлюють кристалізацію наявних вже проблем. Так, банківські установи відносяться до об'єктів критичної інфраструктури, які піддаються різнохарактерним зовнішнім впливам. Серед останніх можемо виокремити загрози інформаційного характеру (активізувалися кібератаки серверів банків), окрім того, через обстріли рф відбувається руйнування будівель банків, гинуть або зазнають пошкоджень їх співробітники, самі банківські установи вимушені працювати в умовах відсутності електроенергетики та зруйнованої транспортної інфраструктури тощо. У свою чергу, підкреслимо, що ці проблеми позначаються на рівні соціального забезпечення громадян, адже частина з них, перебуваючи на окупованих територіях, не мають змоги користуватися послугами банків у повній мірі через закриття останніх з позиції гарантування безпеки як для самих громадян, так і для банківських працівників. Відтак, можемо наполягати на важливості наукового дослідження вищевказаних проблем, що кристалізуються та можуть зумовлювати зниження рівня як безпеки банківської сфери, так і соціальної безпеки в Україні.

Аналіз останніх досліджень і публікацій. Організаційним, правовим, економічним, антикризовим, ресурсним та іншим аспектам формування та реалізації державного регулювання у фінансовій і банківській сфері присвячені публікації закордонних і вітчизняних науковців Л. Антонової, В. Гейця, Е. Дмитренко, Я. Жаліло, М. Зубок, Дж. Кейнса, Я. Коваль, Л. Кузнецової, А. Лелеченко, М. Литвин, Н. Надьон, А. Помаза-Пономаренко, Л. Сергієнко, Т. Смовженко, Л. Стрельбицької, Н. Стукало, М. Сугоняка, В. Тридід, Ф. Хайєка, С. Шейн та ін. [2; 3; 5; 6; 9; 10; 13; 14; 15]. У той же час, поза увагою залишається низка безпекових питань у сфері забезпечення належного функціонування банківських установ і гарантування повноцінної реалізації прав громадян України, що ускладнюється через повномасштабну агресію рф.

Постановка завдання. Метою статті є дослідження стану реалізації державного регулювання щодо забезпечення безпеки банківських установ у контексті формування інформаційного суспільства.

Виклад основного матеріалу. Вирішення проблем у сфері безпеки

банківських установ (фінансової, інформаційної, соціальної та ін.) нерозривно пов'язано із визначенням особливостей державно-правового забезпечення такої безпеки. У сучасній науці висловлюється думка, що інститут безпеки необхідно закріпити в системі права України [2, с. 14; 9]. Вирішуючи таке завдання, виникає потреба у визначенні, які відносини із забезпечення безпеки банківських установ загалом належать до сфери публічного управління. Ураховуючи, що державно-правове забезпечення безпеки банків належить до сфери публічного права, необхідно виділити ті характеристики цих відносин, які відображають галузеву своєрідність зазначених правовідносин.

При здійсненні правотворчої діяльності в процесі державно-правового забезпечення безпеки банків слід ураховувати, що відносини, які складаються під час управління фінансовими потоками, спрямовані на забезпечення безпеки банків загалом і прав громадян на соцзабезпечення. При цьому процес публічного управління фінансовими потоками банків вказує на приналежність такого управління до сфери публічного права та забезпечення національної безпеки загалом та безпеки банків України зокрема. Адже як відомо, «безпека для суспільства» становить підґрунтя для безпеки, що виходить з боку соціуму [1; 9-10; 14; 18]. Саме в процесі публічного управління фінансовими потоками банків спостерігається виникнення правовідносин із забезпечення безпеки банків. Погоджуємось із ученими, що управлінські відносини як складні відносини людей, різних соціальних колективів виникають у процесі здійснення управлінських функцій на основі загальних принципів управління [там само].

Крім того, переважна більшість способів вирішення фінансових, організаційних та інших проблем банків в Україні сьогодні зосереджена у економічній площині. Однак із метою запобігання майбутнім загрозам і ризикам безпеці банків фундаментальна наука має обґрунтувати шляхи та способи вдосконалення чинного законодавства, яке регулює питання безпеки банків в умовах розвитку інформаційного суспільства та посилення зовнішнього впливу на діяльність таких установ [9, с. 100-101; 13-14].

На підставі зазначеного можемо зробити проміжний висновок, що науковці застосовують правовий та економічний підходи до характеристики безпеки банківських установ в умовах збільшення зовнішніх загроз та розвитку інформаційного суспільства. У той же час, відзначимо, що гібридна війна, розпочата рф, проти України зумовила необхідність застосування міждисциплінарних підходів до вирішення проблемних питань, наявних в означеній сфері. На наше переконання, методологічний базис цього підходу сформований значною мірою у межах галузі науки «Публічне управління та адміністрування». Підтвердженням цього є, зокрема, вищевказані управлінські принципи, серед яких виокремлюють загальні та спеціальні. Уважаємо, що застосування даного підходу потребує

врахування також положень теорії інституціоналізму, що набуває останнім часом усе більшої актуальності. Оскільки ця теорія дозволяє чіткіше представити особливості взаємного впливу публічних інститутів на приватні, зокрема, крізь призму розробки та впровадження правових норм, а також участі в цьому процесі соціальних інститутів, на які сьогодні чинить значний вплив рф як держава-творець інформаційних та інших загроз. Саме таким чином вона асоціюється в усьому світі, і буде асоціюватися так ще багато років, що є беззаперечним фактом.

Інформаційна безпека кожної держави безпосередньо пов'язана з соціальною безпекою, адже будь-яка інформація спрямована саме на людей. Ці види безпеки забезпечуються шляхом формування виваженої державної політики відповідно до прийнятих управлінських рішень і правових документів, що як раз втілюються в межах функціонуючої системи інституційного забезпечення.

В останні роки законодавці прийняли низку важливих правових актів, які окреслили організаційно-правове підґрунтя і для експлуатації критичної інфраструктури, і гарантування інформаційної та іншої безпеки (табл. 1). Свідченням цього є Закон України «Про критичну інфраструктуру» (2021 року), Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.), Стратегія інформаційної безпеки України (2021 р.), Концепції створення державної системи захисту критичної інфраструктури (2017 р.), Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури (2023 р.), постанова правління Національного банку України «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг» (2021 р.) тощо [11].

У той же час, повномасштабне збройне вторгненням рф на територію України спрямоване на дестабілізацію роботи інституцій публічного та приватного сектору, частина з яких входить до об'єктів критичної інфраструктури (далі – ОКІ) [7; 12]. Ми не випадково закцентували увагу на ОКІ, адже законодавець до цих об'єктів належного життєзабезпечення населення відносить 17 секторів. Згідно з п. 10 ч. 4 ст. 9 Закону України «Про критичну інфраструктуру» серед законодавчо затвердженого переліку секторів, як об'єктів критичної інфраструктури, є й сектор, що надає фінансові послуги, тобто це банківський сектор [11]. За твердженням вітчизняного законодавця ОКІ покликані забезпечувати виконання життєво важливих функцій та/або надання послуг, порушення яких призводить до негативних наслідків для національної безпеки України [11, ч. 4 ст. 9]. Крім того, законодавець визначає рівні забезпечення безпеки ОКІ: загальнодержавний; регіональний та галузевий рівні; місцевий; об'єктовий [там само, ч. 1 ст. 7].

Відповідно до ст. 7 аналізованого закону суб'єктами, які

безпосередньо повинні вживати заходів із забезпечення безпеки ОКІ, [11; 12] є: 1) міністерства та інші центральні органи виконавчої влади; 2) місцеві державні адміністрації; 3) органи місцевого самоврядування; 4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; 5) ЗСУ та інші військові формування; 6) Національний банк України; 7) підприємства, установи та організації, віднесені до ОКІ; 8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації. У межах своєї компетенції суб'єкти забезпечення безпеки ОКІ здійснюють й інші заходи, передбачені положеннями закону [11].

Таблиця 1

Правовий механізм державного регулювання безпеки банківських установ як об'єктів критичної інфраструктури в умовах впливу інформаційних та інших загроз

Рівень державного регулювання	Правові акти, в яких визначені законодавчі державного регулювання безпекою банківських установ як ОКІ
Загальнодержавний	1. Концепція створення державної системи захисту критичної інфраструктури (2017 р.): передбачає створення загальнодержавної системи захисту ОКІ; узгодження правового регулювання цієї сфери; створення відповідального за координацію у цій сфері державного органу управління; визначення повноважень, відповідальності, функцій центральних органів виконавчої влади, інших органів державної влади, прав та обов'язків власників КІ; встановлення критеріїв, розробку методології категоризації, паспортизації ОКІ за галузевим та функціональним підходом; розробка методології проведення оцінки загроз КІ; розвиток державно-приватного партнерства в цій сфері. 2. Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури (2023 р.), що передбачає актуалізацію налагодження механізму міжнародного співробітництва у сфері функціонуваня ОКІ. 3. Закон України «Про критичну інфраструктуру» (2021 р.), що визначає правові, організаційні основи створення й функціонування національної системи захисту критичної інфраструктури, серед секторів якого виділено енергетичну, банківську, оборонну, космічну та інші сфери.

	4. Закон України «Про основні засади забезпечення кібербезпеки України» (2024 р.), що закріплює правові й організаційні основи забезпечення захисту важливих інтересів громадянина, суспільства, держави, національних інтересів країни у кіберпросторі; цілі, напрями, принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їх діяльності із забезпечення кібербезпеки.
Регіональний або галузевий	1. Закон України «Про місцеве самоврядування», в якому визначені повноваження щодо організації, забезпечення цивільного захисту на ОКІ та об'єктах підвищеної небезпеки, адже частина ОКІ входить до об'єктів, що становлять потенційну небезпеку для населення та територій. 2. Закон України «Про місцеві державні адміністрації», що окреслює повноваження місцевих органів виконавчої влади, зокрема,в військових адміністрацій, у різних секторах економіки (містобудування, житлово-комунального господарства, побутового, торговельного обслуговування, транспорту та зв'язку, фінансової сфери тощо), а також фактично відповідає за стан та фінансування розвиток різних секторів ОКІ, які виконують суспільно важливі функції.
Місцевий	
Об'єктовий	1. Постанова КМУ «Деякі питання ідентифікації об'єктів підвищеної небезпеки» (2022 р.), у якій закріплено обов'язок на рівні юридичних осіб проводити ідентифікацію об'єктів підвищеної небезпеки, інформація про які розміщується у відповідному реєстрі та на сайтах місцевих адміністрацій та органів місцевого самоврядування. 2. Постанова правління Національного банку України «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг» (2021 р.), що встановлює порядок організації та здійснення НБУ заходів із контролю за дотриманням банками вимог законодавства, яке регулює відносини у сферах кіберзахисту, інформаційної безпеки та електронних довірчих послуг.

Джерело: систематизовано автором за даними [11]

Варто підкреслити, що повноваження у сфері формування та забезпечення функціонування реєстру ОКІ у банківській сфері покладаються на Національний банк України. Відповідно до ч. 2 ст. 8

Закону України «Про критичну інфраструктуру» «віднесення банків, інших об'єктів, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури здійснюється в порядку» [11].

Слід зауважити, що ст. 7 Закону України «Про критичну інфраструктуру» і ст. 8 Закону України «Про ратифікацію Конвенції про кіберзлочинність» містять положення, які зумовлюють появу зайвих наукових дискусій щодо інституційного забезпечення без пеків ОКІ. Власне кажучи, суб'єкти законодавчо визначені у ст. 7 де-юре не належать до Національної системи кібербезпеки, склад якої наведено у ст. 8 Закону України «Про ратифікацію Конвенції про кіберзлочинність». Це, з нашого погляду, є некоректним, адже кожна система складається з керівної (центральної) та керованої (субрегіональної, місцевої, локальної) підсистеми. Їх структурні елементи взаємодіють за певними ієрархічними рівнями, що визначені законодавцем з огляду на адміністративно-територіальний устрій нашої держави.

У продовження також відзначимо, що такий підхід, застосований вітчизняним законодавцем під час визначення суб'єктів у сфері безпеки ОКІ, не дає можливості чітко визначити цілісний механізм інституційного забезпечення такої безпеки. Відтак, поза увагою законодавця залишається визначення суб'єктності реалізації тих чи інших заходів у зазначеній сфері, критеріїв їхньої реалізації, не персоніфікованою є відповідальність суб'єктів тощо. Крім того, невизначеною залишається роль Кабінету Міністрів України у забезпеченні формування та реалізації державної політики у сфері кібербезпеки банківського сектору. Хоча Уряд України має через відповідні міністерства (економіки, цифрової трансформації, оборони тощо), що входять у національну систему кібербезпеки, зреалізовувати заходи, які стосуються центральних органів виконавчої влади, які, власне, до такої системи не належать (табл. 2).

Крім того, те саме стосується сфери компетенції та функцій Парламенту України, що не визначений як суб'єкт національної системи захисту критичної інфраструктури [11, ст. 7]. До речі, Верховна Рада України не визначена також і серед суб'єктів Національної системи кібербезпеки. Це суперечить нормам Основного Закону України, зокрема, у частині того, що контроль за дотриманням законодавства у сфері забезпечення інформаційної та кібербезпеки здійснюється саме Парламентом України у порядку, визначеному її Конституцією.

Також цікавим є законодавче визначення «секторальних і функціональних органів», а також «уповноваженого органу», що виконують повноваження у сфері ідентифікації та забезпечення безпеки ОКІ. Згідно з ч. 2 ст. 13 Закону України «Про критичну інфраструктуру» секторальні та

функціональні органи у сфері захисту критичної інфраструктури здійснюють формування та реалізацію державної політики в окремих секторах критичної інфраструктури.

Таблиця 2

Організаційно-управлінські засади державного регулювання ОКІ та безпеки банківського сектору

Суб'єкти державного регулювання	Основні функції, повноваження суб'єктів державного регулювання
Кабінет Міністрів України (ст. 14 ЗУ «Про критичну інфраструктуру»)	Розробка державної політики захисту та забезпечення безпеки та стійкості об'єктів КІ
Рада національної безпеки України	Формує, реалізовує державну політику захисту, розвитку ОКІ в різних секторах. У складі РНБО функціонує Національний координаційний центр кібербезпеки, що також здійснює низку важливих заходів у сфері забезпечення безпеки ОКІ
Міністерство енергетики України, Міністерство розвитку громад, територій та інфраструктури України та ін.	Беруть участь у реалізації державної політики у сфері захисту ОКІ в контексті цивільного захисту; здійснює заходи із запобігання, виявлення, припинення терористичної діяльності на об'єктах ПЕК; відновлення об'єктів КІ через збройну агресію тощо. Стратегічна ціль у межах енергетичної стратегії до 2030 року визначено: оновлення, модернізація енергетичної інфраструктури.
Національний банк України та інші інституції (ст. 18 ЗУ «Про критичну інфраструктуру»)	Діяльність Національного банку України, уповноваженого органу у сфері захисту критичної інфраструктури України, центрального органу виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту, Служби безпеки України, Національної гвардії України, Національної поліції України, Збройних Сил України, Державної спеціальної служби транспорту та Державної служби спеціального зв'язку та захисту інформації України з питань формування та/або реалізації державної політики у сфері захисту критичної інфраструктури здійснюється в рамках, визначених цим Законом, та у порядку, встановленому законами України, що регламентують правові засади організації та діяльності зазначених

	у цій статті органів.
Державна служба України з надзвичайних ситуацій, що відносяться до секторальних органів (ст. 19 ЗУ «Про критичну інфраструктуру»)	Реалізовує державну політику у сфері цивільного захисту зокрема, захисту населення, територій від НС, запобігання їх виникненню, ліквідації їхніх наслідків. ДСНС разом із центральними та місцевими органами виконавчої влади, органами місцевого самоврядування, підприємствами, установами здійснює прогнозування ймовірності настання НС, визначає показники потенційних ризиків, здійснює районування території України щодо їхнього виникнення. ДСНС із її територіальними підрозділами здійснюють ведення та оновлення даних щодо об'єктів підвищеної небезпеки, частина з яких входить до критичної інфраструктури.
Служба захисту критичної інфраструктури та забезпечення національної системи стійкості України	Уряд України координує діяльність цієї служби, яка відповідає за формування, реалізацію державної політики у сфері захисту ОКІ, створення, впровадження та забезпечення функціонування національної системи захисту ОКІ України

Джерело: систематизовано автором за даними [11]

Окрім формування та реалізації держполітики у цій сфері, уповноважений орган у сфері захисту критичної інфраструктури України забезпечує координацію діяльності суб'єктів національної системи захисту критичної інфраструктури забезпечує [11, ч. 3 ст. 13]. У цьому контексті сумнівним виглядає розподіл повноважень зазначених інституцій – секторальних і функціональних й уповноваженого органу, що вказує на дублювання сфер їхнього впливу. Це суперечить концептуальним положенням фундаментальної науки щодо єдності, взаємоузгодженості, централізованості – децентралізованості дій під час формування та реалізації державної політики. Кращою, проте, виглядає ситуація з визначенням функцій суб'єктів відповідальних за забезпечення безпеки у банківській і фінансовій сферах (у них відповідальним визнано Національний банк України).

Наразі Україна активно реалізує заходи, спрямовані на формування державної системи захисту ОКІ з урахуванням досвіду країн ЄС [7; 12]. У цій галузі серед пріоритетних завдань органів публічної влади в Україні є протидія іноземній економічній експансії, недопущення використання фінансових інструментів під час фінансування громадських організацій і для створення системних кризових явищ в економіці нашої держави.

У цьому контексті набувають актуальності унеможливлення кібератак

на фінансову сферу загалом і на банківську сферу зокрема. На жаль, можемо констатувати, що кількість атак на ці та інші життєво важливі сфери суспільної життєдіяльності в Україні збільшилися. Так, за даними кіберфахівців СБУ у 2022 році ними було нейтралізовано понад 4500 кібер атак, заблоковано понад 40 ботоферм, викрито понад 1200 інтернет-агітаторів і повідомлено про 600 підозр у сфері порушення кіберзаконодавства [16]. У 2023 році кіберполіція виявила понад 3600 кіберзлочинів [8]. У той же час, у 2024 році на вітчизняних теренах почастішали кібератаки банківського сектору, зокрема Monobank [17].

Згідно з п. 19 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» [11] ОКІ відносяться до комунікаційної або технологічної системи, кібератаки на яку можуть вплинути на стале функціонування й експлуатацію ОКІ, у т.ч. банківських установ, що, у свою чергу, ускладнить повноцінну реалізацію прав громадян. На цій підставі можемо рекомендувати застосування цифрових технологій, які дозволять гарантувати громадянам їхню безпеку, а також захист законних прав. Серед таких технологій можна виокремити відповідні чат-боти, мобільні додатки тощо, які допомагають оперативно надавати різні консультації та послуги, забезпечувати безпеку для населення за будь-яких умов (у мирний час, у воєнний період чи період надзвичайного стану). Як відомо, у Китаї активно застосовується WeChat для оперативного надання послуг населенню, у т.ч. щодо отримання заробітної плати чи користування банківськими послугами тощо. Це вказує на два важливі завдання будь-якої держави:

1) вона має забезпечувати розвиток власного «цифрового» та інформаційного суспільства, його фінансову грамотність;

2) слід паралельно і гарантувати права громадян, і захищати їх, навіть якщо реалізація таких відбувається у віртуальній площині.

У цьому контексті відзначимо, що в березні 2024 року Європарламент прийняв закон, у якому встановив обмеження щодо використання штучного інтелекту, зокрема, і в фінансовій, освітній та іншій сферах [4]. Фахівцями слушно зазначається, що громадянам має гарантуватися захист їхніх персональних даних, власне, установлюється заборона збирати та використовувати персональну інформацію, що може наносити шкоду інтересам держави, суспільства й окремих громадян. Це необхідно для того, щоб унеможливлювати вчинення шахрайських дій. Крім того, відтепер заборонено збирати й опрацьовувати інформацію щодо вподобань людей, які вони висловлюють під час реагування на ту чи іншу рекламу в мережі Інтернет, соціальних мережах тощо, що (реклама) спрямована на пропонування різнохарактерних товарів і послуг. Зважаючи на інтеграційні прагнення України, вона має дотримуватись цивілізованої загальноєвропейської традиції щодо виваженого використання цифрових технологій, у т.ч. штучного інтелекту.

Висновки. Проведене дослідження дозволило зробити такі висновки:

1. Установлено, що вітчизняне законодавство відносить банківську сферу до фінансової, яка, у свою чергу, входить до складу критичної інфраструктури. Остання загалом включає 17 секторів, об'єкти яких мають розроблятися функціонувати у відповідності до паспортів безпеки. Законодавець закріпив вимогу, що оператори ОКІ готують і подають паспорт безпеки на кожний об'єкт на погодження до відповідних секторальних органів у сфері захисту критичної інфраструктури. У цьому контексті слід наголосити, що державне регулювання у сфері ідентифікації та захисту ОКІ реалізується на таких рівнях управління, як загальнодержавний, регіональний (галузевий), місцевий та об'єктовий. Зважаючи на обраний предмет дослідження, аргументовано віднести Національний банк України до інституцій галузевого рівня, які покликані забезпечувати безпеку банківських установ.

2. З'ясовано, що формування та реалізація державної політики у сфері захисту об'єктів критичної інфраструктури здійснюється секторальним та функціональними органами, а також уповноваженим органом. Аналіз функцій цих органів дав змогу наполягати на тому, що має місце дублювання повноважень у сфері забезпечення безпеки ОКІ. Крім того, виявлено проблеми, пов'язані з інституційним визначенням ролі Парламенту України у забезпеченні безпеки таких об'єктів. На цій підставі рекомендовано внести зміни до чинного законодавства України в напрямку конкретизації місця та ролі ВРУ, адже цьому вищому органу державної влади надано можливість здійснювати парламентський контроль у різних сферах суспільної життєдіяльності. Акцентовано, що складності ситуації додає також розпорошеність вітчизняного законодавства, покликаного визначати заходи та шляхи із забезпечення безпеки ОКІ та фінансового сектору. Свідченням цього є наявність нормативно-правових актів, що врегульовують основні засади забезпечення кібербезпеки ОКІ, інформаційної безпеки та електронних довірчих послуг.

3. Ураховуючи важливість ОКІ у забезпеченні життєво важливих функцій та надання життєво важливих послуг, обґрунтовано, що на такі об'єкти чиниться вплив як внутрішніх, так і зовнішніх факторів. Визнано, що серед останніх особливу увагу слід приділяти позасистемних чинників, які складно прогнозувати, але можливо. Прикладом такого чинника є зовнішня агресія рф проти України. Ця держава-агресор створює різнохарактерні загрози, що зумовлюють виникнення кризових ситуацій через несанкціоноване втручання у функціонування ОКІ, наслідки чого вимагають значного часу на повне відновлення штатного режиму експлантації ОКІ. Підкреслено, що у 2024 році збільшилась кількість

інформаційних і кібератак у банківському секторі, що свідчить про важливість забезпечення безпеки його функціонування та громадян, які користуються послугами банків. Доведено необхідність повсюдного застосування цифрових технологій із метою підвищення рівня безпеки як користувачів банківських установ, так їхніх працівників. Визначено заходи, що слід зреалізувати в цій сфері, а саме: виваженого використання цифрових технологій у банківській сфері, що передбачає певні обмеження у застосуванні алгоритмів штучного інтелекту, та забезпеченні його неупередженості щодо статі людини-користувача цими технологіями. На нашу думку, дані заходи доцільно закріпити законодавчо, що має стати предметом подальших наукових розвідок.

Список використаних джерел:

1. Бєлай С.В. Розроблення комплексного державного механізму протидії кризовим ситуаціям за масовою участю населення. URL: http://www.pa.stateandregions.zp.ua/archive/3_2013/11.pdf.
2. Дмитренко Е. С. Юридична відповідальність суб'єктів фінансового права у механізмі правового забезпечення фінансової безпеки України : монографія. К. : Юрінком Інтер, 2009. 592 с.
3. Зубок М.І. Безпека банківської діяльності. URL : http://shron.chtyvo.org. ua/Zubok_M_I/Bezpeka_bankivskoi_diialnosti.pdf.
4. Європарламент ухвалив перший у світі закон про обмеження штучного інтелекту // Вчені записки Університету «КРОК». 2018. № 4 (52). URL: https://www.pravda.com.ua/news/2024/03/13/.
5. Коваль Я.С. Державне регулювання економічною безпекою банківських установ України. URL: https://snku.krok.edu.ua/index.php/vcheni-zapiski-universitetu-krok/article/view/131.
6. Кузнєцова Л.В. Вплив глобалізації на розвиток банківської діяльності: кол. монографія. Одеса, 2011. 520 с.
7. Лазор О.Ф., Юник І.Г., Чемерпільська А.М. Організаційно-правові засади забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури України: формування та розвиток // Державне управління: удосконалення та розвиток. 2024. № 5. URL: https://www.nayka.com.ua/index.php/dy/article/view/3677.
8. Михайлов Д. За 2023 рік кіберполіція виявила понад 3600 кіберзлочинів. URL : https://suspilne.media.
9. Надьон О.В. Сучасні пріоритети адміністративно-правового забезпечення фінансової безпеки банків Україні // Тенденції та пріоритети реформування законодавства України : матеріали Всеукр. наук.-практ. конф. (9–10 грудня 2016 р.). Херсон : Видавничий дім «Гельветика», 2016. С. 100–101.
10. Надьон О.В., Помаза-Пономаренко А.Л. Правовий механізм державного регулювання фінансової безпеки банків України : монографія. Харків: НУЦЗ України, 2018. 198 с.

11. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/.

12. Помаза-Пономаренко А.Л., Тарадуда Д.В. Вектори забезпечення стійкого функціонування об'єктів критичної інфраструктури й об'єктів підвищеної небезпеки в Україні та за кордоном // Державне управління: удосконалення та розвиток. 2024. № 5. URL: https://www.nayka.com.ua/index.php/dy/issue/view/147.

13. Смовженко Т.С., Тридід О.М. Антикризове управління стратегічним розвитком банку: монографія. Київ, 2008. 473 с.

14. Стрельбицька Л.М., Стрельбицький М.П., Гіжевський В.К. Банківське безпекознавство: навчальний посібник. Київ : Кондор, 2007. 602 с.

15. Стукало Н., Литвин М. Державне антикризове регулювання банківського сектору: досвід ЄС та України. Вісник Національного банку України: наук. вісник : зб. наук. праць. Київ : Вид-во Національний банк України. 2010. № 6. С. 20-25.

16. Щорічний звіт СБУ «2022 рік: захист держави в умовах війни». URL: https://ssu.gov.ua/uploads/documents/2023/04/24/ssu-report-2022-web.pdf.

17. Monobank пережив масштабну DDoS-атаку. Хакери майже два роки постійно атакують українські банки. Як це впливає на їх бізнес. URL: https://forbes.ua/ru/innovations/tse-prosto-kosmos-monobank-perezhiv-masshtabnu-ddos-ataku-iz-navantazhennyam-580-mln-zapitiv-yak-podibni-ataki-vplivayut-na-biznes-22012024-18687.

18. Pomaza-Ponomarenko A., Hren L., Durman O., Bondarchuk N., Vorobets V. Management mechanisms in the context of digitalization of all spheres of society // Revista San Gregorio. SPECIAL EDITION-2020. Núm. 42. URL: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/issue/view/RSAN42/showToc.

References:

1. Belai S.V. Development of a complex state mechanism for countering crisis situations with the mass participation of the population. URL: http://www.pa.stateandregions.zp.ua/archive/3_2013/11.pdf.

2. Dmytrenko E. S. Legal responsibility of subjects of financial law in the mechanism of legal support of financial security of Ukraine: monograph. K.: Yurinkom Inter, 2009. 592 p.

3. Zubok M.I. Security of banking activity. URL: http://shron.chtyvo.org.ua/Zubok_M_I/Bezpeka_bankivskoi_diialnosti.pdf.

4. The European Parliament adopted the world's first law on limiting artificial intelligence // Scientific notes of the KROC University. 2018. No. 4 (52). URL: https://www.pravda.com.ua/news/2024/03/13/.

5. Koval J.S. State regulation of economic security of banking institutions of Ukraine. URL: https://snku.krok.edu.ua/index.php/vcheni-zapiski-universitetu-krok/article/view/131.

6. Kuznetsova L.V. The impact of globalization on the development of banking activity: col. monograph. Odesa, 2011. 520 p.

7. Lazor O.F., Yunyk I.G., Chemerpilska A.M. Organizational and legal principles of ensuring cyber security of objects of critical information infrastructure of Ukraine: formation and development // State management: improvement and development. 2024. No. 5. URL: https://www.nayka.com.ua/index.php/dy/article/view/3677.

8. Mykhaylov D. In 2023, the cyber police detected more than 3,600 cyber crimes. URL: https://suspilne.media.

9. Nadion O.V. Modern priorities of administrative and legal provision of financial security of banks in Ukraine // Tendencies and priorities of reforming the legislation of Ukraine: materials Vseukr. science and practice conf. (December 9–10, 2016). Kherson: Helvetica Publishing House, 2016. P. 100–101.

10. Nadion O.V., Pomaza-Ponomarenko A.L. Legal mechanism of state regulation of financial security of Ukrainian banks: monograph. Kharkiv: NUTSZ of Ukraine, 2018. 198 p.

11. Official website of the Verkhovna Rada of Ukraine. URL: https://zakon.rada.gov.ua/laws/.

12. Pomaza-Ponomarenko A.L., Taraduda D.V. Vectors of ensuring sustainable functioning of critical infrastructure facilities and high-risk facilities in Ukraine and abroad // State administration: improvement and development. 2024. No. 5. URL: https://www.nayka.com.ua/index.php/dy/issue/view/147.

13. Smovzhenko T.S., Tridid O.M. Anti-crisis management of the bank's strategic development: monograph. Kyiv, 2008. 473 p.

14. Strelbytska L.M., Strelbytskyi M.P., Gizhevskyi V.K. Banking security: a study guide. Kyiv: Condor, 2007. 602 p.

15. Stukalo N., Lytvyn M. State anti-crisis regulation of the banking sector: the experience of the EU and Ukraine. Bulletin of the National Bank of Ukraine: science. herald: coll. of science works Kyiv: Office of the National Bank of Ukraine. 2010. No. 6. C. 20-25.

16. Annual report of the SBU "Year 2022: Defense of the State in War Conditions." URL: https://ssu.gov.ua/uploads/documents/2023/04/24/ssu-report-2022-web.pdf.

17. Monobank survived a large-scale DDoS attack. Hackers have been constantly attacking Ukrainian banks for almost two years. How it affects their business. URL: https://forbes.ua/ru/innovations/tse-prosto-kosmos-monobank-perezhiv-masshtabnu-ddos-ataku-iz-navantazhennyam-580-mln-zapitiv-yak-podibni-ataki-vplivayut-na- business-22012024-18687.

18. Pomaza-Ponomarenko A., Hren L., Durman O., Bondarchuk N., Vorobets V. Management mechanisms in the context of digitalization of all spheres of society // Revista San Gregorio. SPECIAL EDITION-2020. Núm. 42 . URL: http://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO /issue/view/RSAN42/showToc.

дата надходження статті: 08.05.2024
дата прийняття статті: 21.05.2024
дата публікації: 28.06.2024