

**НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА**

*Кваліфікаційна наукова
праця на правах рукопису*

ШАРУК ОЛЕКСАНДР ГРИГОРОВИЧ

УДК 342.95:351.822:351.72:336.74(477)

ДИСЕРТАЦІЯ

**МЕХАНІЗМ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ
ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО
СЕКТОРУ УКРАЇНИ**

12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право

Подається на здобуття наукового ступеня кандидата юридичних наук

Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело

_____ О.Г. Шарук

Науковий керівник: доктор юридичних наук, професор
Сорока Лариса Володимирівна

Київ – 2024

АНОТАЦІЯ

Шарук О. Г. Механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Науково-дослідний інститут публічного права, Науково-дослідний інститут публічного права, Київ, 2024.

У дисертаційному дослідженні за рахунок комплексного та системного підходу до аналізу адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України викладено сучасні основи доктринального розуміння правового концепту «критична інфраструктура фінансового сектору України», розкрито особливості адміністративно-правового захисту цих об'єктів, а також визначено напрямки вдосконалення адміністративного законодавства у цій сфері.

Визначено, що семантичний аналіз правового концепту «критична інфраструктура фінансового сектору України» свідчить, що опорним елементом у цьому контексті є термін «критична інфраструктура», залежним – «фінансовий сектор». Уточнено, що термін «критична інфраструктура» також диференціюється на дві самостійні складові: «критична» та «інфраструктура», однак з'ясовано, що це самостійна юридична конструкція з власним термінологічним змістом. Обґрунтовується, що цей правовий концепт позначає коло суспільних відносин виникнення яких обумовлено необхідністю забезпечення безперебійного функціонування окремих складових фінансового сектору, які є критично важливими в аспекті спроможності держави обслуговувати свої потреби і розвиватись у руслі автономності та самодостатності, а також утвердження як правової, демократичної, суверенної держави, яка належним чином виконує своє соціальне призначення з дискурсу гарантування кожному непорушності його

прав та законних інтересів. Висунуто припущення, що така інтерпретація не зумовлює виникнення сумнівів чи дискусій щодо того, що держава має створити усі необхідні умови задля того, щоб усі критично важливі складові фінансового сектору перебували у стані захисту, тобто були забезпеченими можливістю здійснення адекватної, належної, допустимої, необхідної та ефективної реакції на фактори, чинники, обставини, події тощо, які потенційно чи реально здатні або завдають негативного впливу на функціональність їхньої роботи.

Доведено, що адміністративно-правовий захист, як і адміністративно-правова охорона чи адміністративно-правове забезпечення, логічніше розглядати з позиції самостійних врегульованих процесів, що мають різні завдання та механізми реалізації. Узагальнено та схематично їхнє співвідношення представлено так: забезпечення спрямовується на охорону та захист, а охорона та захист – реалізуються у тісній взаємодії. Причому саме визначення адміністративно-правового захисту має розглядатись з дуальної інтерпретації об'єктної складової. Мається на увазі, що окрім юридичного відношення особи до конкретного інтересу (як правило, права на щось) має враховуватись його безпосередній стан з позиції убезпечення від зміни властивостей чи характеристик, руйнування або загалом знищення.

Визначено, що адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України є системою заходів охоронного та захисного спрямування, реалізованих уповноваженими суб'єктами національної системи захисту критичної інфраструктури задля забезпечення стійкості та безпеки сегментів ринку фінансових послуг та окремих фінансових операцій, що формують фінансовий сектор критичної інфраструктури України. Констатується, що у досліджуваній площині ризику мають два різновиди: ті, що пов'язані із виникненням загроз (неврахування ризику веде до загрози); ті, що існують паралельно з ймовірністю виникнення загроз (самостійні ризики, що наявними є постійно). Причому другий контекст є значно ширшим. Більшою мірою саме про нього йдеться у

нормах чинного законодавства. Натомість загрозою, за таким баченням, є фізичний прояв небезпеки від наявності (виникнення) певного явища. З точки зору наукового суб'єктивізму визначається, що ризик має бути пов'язаним із загрозою, точніше зумовлювати наявність останніх.

Доведено, що механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України: а) є сукупним терміном, термінологічний аспект якого формується шляхом поєднання базових характерних ознак адміністративно-правових механізмів загалом та адміністративно-правового механізму захисту – зокрема; б) є репрезентацією практичного прояву дії охоронних та захисних заходів у цій сфері; в) має власну сферу об'єктивізації – суспільні відносини, породжені необхідністю забезпечення схоронності об'єктів критичної інфраструктури фінансового сектору України; г) як правове явище діяльнісного характеру має власну систему завдань, функцій та цілей; д) з внутрішньо організаційного дискурсу має свій структурний склад, відмінний від тих, що встановлені для інших механізмів адміністративно-правового забезпечення об'єктів критичної інфраструктури фінансового сектору України. Запропоновано такими вбачати: а) організаційні складові – відповідають на запитання для чого потрібно реалізовувати адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України. Йдеться про мету, завдання та функції означеного механізму; б) нормативні складові – відповідають на запитання що потрібно реалізовувати у спосіб адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. Цей блок репрезентує систему нормативних основ, які деталізують загальні та спеціальні заходи здійснення охоронного та захисного впливу на суспільні відносини, породжені необхідністю забезпечення безперебійної роботи окремих складових фінансового сектору України; в) інституційні складові – відповідають на запитання ким потрібно реалізовувати адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України. Йдеться про систему суб'єктів, уповноважених чи залучених до

цього процесу; г) цільові складові – відповідають на запитання як здійснюється адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України. Традиційно означене включає перелік знарядь для здійснення цілеспрямованих дій. За загальним правилом знаряддям в адміністративному праві позначається інструмент реалізації повноважень конкретних органів влади, а отже слід вести мову про форми та методи реалізації адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України.

Нормативно-правові основи захисту об'єктів критичної інфраструктури фінансового сектору України диференційовано на: 1) міжнародні – наприклад, Рекомендації та Керівництва Групи з розробки фінансових заходів боротьби з відмиванням грошей, акти Міжнародного валютного фонду, Світового банку, Міжнародної організації з стандартизації; 2) регіональні – наприклад, Директива Ради ЄС 2008/114/ЄС, Директива Ради ЄС 2016/1148, Директива Ради ЄС 2018/843, Регламент ЄС 2021/23, Директива Ради ЄС 2022/2557, Рекомендації Ради ЄС 2023/C 20/01); 3) національні – законодавство у сферах сталого розвитку, національної безпеки та її складових, захисту критичної інфраструктури, регулювання ринку фінансових послуг, бюджетного регулювання, економічного розвитку та протидії фінансуванню злочинів. Однак констатується, що досліджувані нормативно-правові основи національного рівня перебувають на стадії формування своєї повноцінної правової структури, адже наразі розпочато процес оптимізації їх змісту. Виявлено, що основоположними з таких є акти секторальних органів, проте основна проблема полягає у відсутності їх публічності.

Запропоновано принципи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України визначати через загальнотеоретичні (загальноправові), галузеві та спеціальні принципи. Загальнотеоретичними (загальноправовими) принципами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору

України названо ті, що віддзеркалюють особливості сучасного стану державотворення в Україні, особливості його ідеологічного підґрунтя. До числа таких віднесено принцип верховенства права, принцип законності, принцип правової визначеності та прозорості. Окремо схарактеризовано проблематику реалізації останнього. Галузевими принципами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України визначено групу з таких, що акцентують на особливостях забезпечення безпеки та стійкості суспільного розвитку, регулювання ринку фінансових послуг та загальних вимогах до діяльності суб'єктів національної системи захисту критичної інфраструктури в Україні. Серед ключових з-поміж таких виділено принцип пропорційності, принцип ефективності, принцип координованості, принцип розподілу відповідальності, принцип взаємодії, принцип завчасної превенції, принцип безпеки, захисту та охорони інформації з обмеженим доступом, принцип оперативності, принцип своєчасності, принцип передбачуваності; принцип адаптивності та мобільності; принцип безперервності, принцип ресурсної достатності, принцип довгострокової стійкості, принцип гнучкості, принцип системності та цілісності, принцип безперервного вдосконалення.

Визначено, що спеціальними принципами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є ті, що мають безпосереднє відношення до процедур забезпечення організаційної та функціональної стійкості об'єктів критичної інфраструктури, ідентифікації її вразливості, обміну інформацією зовнішнього та внутрішнього рівнів, управління ризиками та здійснення превентивної діяльності на постійній основі. Такими названо принцип організаційної стійкості, принцип інституційної спроможності регуляторів, принцип цільової спрямованості, принцип комплексного моніторингу, принцип динамічності, принцип макропруденційного регулювання, принцип сприяння прибутковості; принцип мінімізації фінансового стресу, принцип очікуваних збитків (втрат), принцип вільного руху капіталу.

Запропоновано виокремлювати класичний розподіл суб'єктів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України на секторальних (Міністерство фінансів України, Національний банк України), функціональних (наприклад, органи сектору безпеки, кібербезпеки) і уповноваженого (наразі – Державна служба спеціального зв'язку та захисту інформації України) органів. Сформовано альтернативний варіант розподілу, який дозволяє їх згрупувати за приналежністю до виконуваних задач на тих, що: 1) є репрезентацією цієї системи (Міністерство фінансів України, Національний банк України, Державна служба спеціального зв'язку та захисту інформації України, Національна комісія з цінних паперів та фондового ринку, Фонд гарантування вкладів фізичних осіб); 2) функціонують для виконання задач секторальних, функціональних та уповноваженого органів захисту критичної інфраструктури в Україні (наприклад, Центр кіберзахисту Національного банку України або Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України); 3) є самостійним міжвідомчим органом з виконанням спеціалізованих функцій (Рада з фінансової стабільності).

Визначено, що категорії «форми» та «методи» в контексті адміністративно-правового захисту можна розглядати з позиції функціональної єдності, що дозволяє інтерпретувати їх зміст через категорію «інструментів», тобто знарядь, які є застосовними уповноваженими суб'єктами задля виконання їх завдань та функцій. Уточнюється, що знаряддям є правовий засіб, який як явище-регулятор правової дійсності, перетворює правову норму в конкретні дії та рішення, які реалізуються на практиці.

Доведено, що позитивний досвід США та ЄС у сфері захисту критичної інфраструктури фінансового сектору може стати корисним прикладом для України в контексті: 1) наявності спеціальних планів захисту критичної інфраструктури фінансового сектору, що визначають особливості її захисту

від системних загроз і ризиків; 2) інституційної різноманітності, що має прояв широким колом суб'єктів захисту та чіткістю процедур обміну інформацією між ними; 3) активної участі приватного сектору та ефективної координації між державними та приватними суб'єктами; 4) встановлення єдиних вимоги до кібербезпеки для критичних секторів, включно з фінансовим; 5) розвинутих систем партнерства між державними та приватними установами; 6) чіткого розподілу обов'язків та відповідальності суб'єктів реалізації такого захисту; 7) дієвості механізмів оцінки кіберстійкості об'єктів критичної інфраструктури фінансового сектору.

Визначено, що основним напрямком розвитку адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України є нормативний, що передбачає формування якісної основи для захисту об'єктів критичної інфраструктури фінансового сектору України. Аналогічно досвіду США запропоновано розробити та затвердити План захисту об'єктів критичної інфраструктури фінансового сектору України, як специфічної деталізації Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури. Наступним напрямком розвитку адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України визначено адаптаційний, який передбачає подальшу імплементацію європейських стандартів, а також впровадження інших позитивних практик. Останнім напрямком розвитку адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України названо функціональний, який має вирішити низку практичних проблем його здійснення, наприклад, запропоновано: 1) переглянути інституційну структуру системи цього захисту, тим самим вирішити питання наявного дисбалансу у сфері реалізації громадського нагляду, зокрема і проведення незалежного аудиту діяльності уповноважених представників; 2) збільшити фінансування для програм тестування об'єктів критичної інфраструктури на предмет вразливостей; 3) стандартизувати процедури, що забезпечують

організаційну стійкість; 4) сформувати безпечні канали для обміну інформацією між різними представниками національної системи захисту критичних інфраструктур; 5) забезпечити розвиток платформ для публічного обговорення проблем функціональності об'єктів критичної інфраструктури фінансового сектору та сформувати ефективні механізми обміну досвідом з міжнародними партнерами; 6) системно здійснювати підвищення кваліфікації кадрового ресурсу через програми професійного розвитку та навчання.

Ключові слова: адміністративно-правовий захист, критична інфраструктура, механізм, Національний банк, управління ризиками, фінансовий сектор, фінансові послуги.

SUMMARY

Sharuk, O. H. Mechanism of Administrative and Legal Protection of Critical Infrastructure Facilities of the Financial Sector of Ukraine. – *Qualification scientific work on the rights of the manuscript.*

The thesis for obtaining a scientific degree of Candidate of Juridical Science in speciality 12.00.07 «Administrative Law and Procedure; Financial Law; Information Law». – Scientific Institute of Public Law, Scientific Institute of Public Law, Kyiv, 2024.

The thesis, relying on a comprehensive and systematic approach to the analysis of administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine, provides the modern foundations of the doctrinal understanding of the legal concept of ‘critical infrastructure of the financial sector of Ukraine’, reveals the specific features of administrative and legal protection of these facilities, and identifies the areas for improvement of administrative legislation in this field.

It is determined that the semantic analysis of the legal concept of ‘critical infrastructure of the financial sector of Ukraine’ reveals that the term ‘critical infrastructure’ is the main element in this context, and the term ‘financial sector’ is the dependent element. It is specified that the term ‘critical infrastructure’ is also differentiated into two independent components: ‘critical’ and “infrastructure”, but it is found that this is an independent legal construction with its own terminological content. It is proved the legal concept of "critical infrastructure of the financial sector of Ukraine" refers to the range of social relations which arise due to the need to ensure the smooth functioning of certain components of the financial sector which are critical in terms of the State’s ability to meet its needs and develop towards autonomy and self-sufficiency, as well as to assert itself as a legal, democratic, sovereign state that properly fulfils its social purpose in the discourse of guaranteeing everyone the inviolability of their rights and legitimate interests. It is assumed that this interpretation does not give rise to any doubt or

discussion that the state should create all conditions necessary to ensure that all critical components of the financial sector are protected, that is, provided with the ability to make an adequate, appropriate, permissible, necessary and effective response to factors, causes, circumstances, events, etc. that are potentially or actually capable of or have a negative impact on the functionality of their work.

It is proved that administrative and legal protection, as well as administrative and legal security or administrative and legal support, should be considered more logically from the perspective of independent regulatory processes with different tasks and mechanisms of implementation. Generally and schematically, their correlation can be represented as follows: support is focused on security and protection, and security and protection are implemented in close interaction. Moreover, the very definition of administrative and legal protection should be considered from the dual interpretation of the objective component. This means that in addition to the legal relationship of a person to a particular interest (usually the right to something), its immediate state should be regarded from the perspective of ensuring protection against changes in properties or characteristics, damage or destruction in general.

It is determined that administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine is a system of security and protective measures implemented by authorised actors of the national critical infrastructure protection system to ensure the stability and security of the financial services market segments which form the financial sector of critical infrastructure of Ukraine. It is stated that in the field under study, risks are of two types: those associated with the emergence of threats (failure to address the risk leads to a threat); those that exist in parallel with the probability of threats (independent risks that are always present). The second context is much broader. To a greater extent, it is the context that is addressed in the current legislation. By contrast, a threat, according to this view, is a physical manifestation of the danger from the presence (occurrence) of a certain phenomenon. From the perspective of scientific

subjectivism, it is determined that the risk should be related to the threat, or rather, determine the presence of the latter.

It is proved that the mechanism of administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine: a) is an aggregate term, the terminological aspect of which is formed by combining the basic characteristics of administrative and legal mechanisms in general and the administrative and legal mechanism of protection in particular; b) represents the practical manifestation of the effect of protective and defensive measures in this field; c) has its own objectification scope comprising social relations generated by the need to ensure the safety of critical infrastructure facilities of the financial sector of Ukraine; d) has its own system of tasks, functions and goals as a legal phenomenon of an active nature; e) has its own structural composition in terms of internal organisational discourse, which differs from those established for other mechanisms of administrative and legal support of critical infrastructure facilities of the financial sector of Ukraine. It is proposed that the following should be considered: a) organisational components answering the question of why it is necessary to implement administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine. This refers to the purpose, objectives and goals of the mechanism; b) regulatory components answering the question of what should be implemented as administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine. This block represents a system of regulatory frameworks that detail general and special measures to implement security and protective impact on social relations caused by the need to ensure the smooth operation of certain components of the financial sector of Ukraine; c) institutional components answering the question of who should implement administrative and legal protection of critical infrastructure of the financial sector of Ukraine. This refers to the system of actors authorised or involved in this process; d) targeted components answering the question of how administrative and legal protection of critical infrastructure of the financial sector of Ukraine is carried out. Traditionally, the latter includes a list of tools for

targeted actions. As a general rule, a tool in administrative law is an instrument for exercising the powers of specific authorities, and therefore we should talk about the forms and methods of implementing administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine.

It is proposed to differentiate the regulatory framework for protection of critical infrastructure of the financial sector of Ukraine into: 1) international, for example, the Recommendations and Guidelines of the Financial Action Task Force on Money Laundering, acts of the International Monetary Fund, the World Bank, and the International Organisation for Standardisation; 2) regional, for example, EU Council Directive 2008/114/EC, EU Council Directive 2016/1148, EU Council Directive 2018/843, EU Regulation 2021/23, EU Council Directive 2022/2557, EU Council Recommendation 2023/C 20/01); 3) national, for example, legislation on sustainable development, national security and its components, protection of critical infrastructure, regulatory frameworks for financial services, budgetary regulation, economic development and countering the financing of crime. However, it is noted that the national-level regulatory framework under study is at the stage of forming its full-fledged legal structure, since the process of optimising its content has now begun. It is found that the most fundamental of these are regulations of sectoral bodies, but the main problem is the lack of their publicity.

It is proposed that the principles of administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine should be determined through general theoretical (general legal), sectoral and special principles. The general theoretical (general legal) principles of administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine are those which reflect the specific features of the current state of the State in Ukraine and the peculiarities of its ideological basis. These include the rule of law, the principle of legality, the principle of legal certainty and transparency. The issues of implementation of the latter are described. The sectoral principles of administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine include a group of those which focus on the specifics of

ensuring security and sustainability of social development, regulation of the financial services market, and general requirements for the activities of entities of the national system of critical infrastructure protection in Ukraine. The key ones include the principle of proportionality, the principle of efficiency, the principle of coordination, the principle of division of responsibilities, the principle of interaction, the principle of early prevention, the principle of security, protection and safeguarding of classified information, the principle of efficiency, the principle of timeliness, the principle of predictability; the principle of adaptability and mobility; the principle of continuity, the principle of resource sufficiency, the principle of long-term sustainability, the principle of flexibility, the principle of systemicity and integrity, the principle of continuous improvement.

It is determined that the special principles of administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine are those which are directly related to the procedures for ensuring organisational and functional resilience of critical infrastructure facilities, identifying its vulnerability, exchanging information at the external and internal levels, managing risks and carrying out preventive activities on an ongoing basis. These include the principle of organisational sustainability, the principle of institutional capacity of regulators, the principle of targeting, the principle of comprehensive monitoring, the principle of dynamism, the principle of macroprudential regulation, the principle of promoting profitability, the principle of minimising financial stress, the principle of expected losses, and the principle of free movement of capital.

It is proposed to distinguish between the classical distribution of actors involved in administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine into sectoral (the Ministry of Finance of Ukraine, the National Bank of Ukraine), functional (e.g., security sector bodies, cybersecurity) and authorised (currently the State Service for Special Communications and Information Protection of Ukraine) bodies. An alternative variant of distribution has been formed, enabling them to be grouped according to their tasks into those that: 1) represent the system (the Ministry of Finance of

Ukraine, the National Bank of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the National Securities and Stock Market Commission, the Deposit Guarantee Fund); 2) operate to fulfil the tasks of sectoral, functional and authorised bodies for the protection of critical infrastructure in Ukraine (for example, the Cyber Defence Centre of the National Bank of Ukraine or the State Centre for Cyber Defence of the State Service for Special Communications and Information Protection of Ukraine); 3) are an independent interagency body with specialised functions (Financial Stability Council).

It is proposed to consider the categories of ‘forms’ and ‘methods’ in the context of administrative and legal protection from the perspective of functional unity, thereby allowing to interpret their content through the category of ‘instruments’, that is, tools which are used by authorised actors to perform their tasks and functions. It is specified that a tool is a legal instrument which, as a phenomenon regulating legal reality, transforms a legal provision into specific actions and decisions which are implemented in practice.

It is proved that the positive experience of the USA and the EU in the field of protection of critical infrastructure of the financial sector can be a useful example for Ukraine in the context of: 1) the availability of special plans for the protection of critical infrastructure of the financial sector, which define the specifics of its protection against systemic threats and risks; 2) institutional diversity, which is manifested by a wide range of protection entities and clear procedures for information exchange between them; 3) active participation of the private sector and effective coordination between public and private entities; 4) establishment of uniform cybersecurity requirements for critical sectors, including the financial sector; 5) developed systems of partnership between public and private institutions; 6) clear distribution of duties and responsibilities of entities implementing such protection; 7) effective mechanisms for assessing the cyber resilience of critical infrastructure of the financial sector.

It is determined that the main area of development of administrative legislation on protection of critical infrastructure facilities of the financial sector of Ukraine is the regulatory one, which provides for the formation of a qualitative basis for protection of critical infrastructure facilities of the financial sector of Ukraine. Similarly to the US experience, it is proposed to develop and approve the Critical Infrastructure Protection Plan for the financial sector of Ukraine as a specific detail of the National Plan for the Protection and Security and Resilience of Critical Infrastructure. The next area of development of administrative legislation in the field of protection of critical infrastructure of the financial sector of Ukraine is the adaptation one, which provides for further implementation of European standards, as well as the introduction of other positive practices. The last area of development of administrative legislation in the field of protection of critical infrastructure facilities of the financial sector of Ukraine is the functional one, which should solve a number of practical problems of its implementation, for example, the author suggests: 1) to review the institutional structure of the system of this protection, thereby addressing the existing imbalance in the field of public supervision, including independent audits of the activities of authorised representatives; 2) to increase funding for programmes to test critical infrastructure for vulnerabilities; 3) to standardise procedures that ensure organisational resilience; 4) to create secure channels for the exchange of information between different representatives of the national critical infrastructure protection system; 5) to ensure the development of platforms for public discussion of the problems of the functionality of financial sector critical infrastructure facilities and to create effective mechanisms for the exchange of experience with international partners; 6) to systematically improve the skills of human resources through professional development and training programmes.

Keywords: administrative and legal protection, critical infrastructure, mechanism, National Bank, risk management, financial sector, financial services.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ
в яких опубліковані основні наукові результати дисертації:

1. Sharuk O. «Critical infrastructure of the financial sector of Ukraine»: identification of content and essence as a legal concept. *Entrepreneurship, Economy and Law*. 2023. № 7. P. 99–104.

2. Sharuk O. Essence of administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine. *Entrepreneurship, Economy and Law*. 2023. № 8. P. 76–80.

3. Шарук О.Г. Механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України: термінологічні аспекти. *Науковий вісник публічного та приватного права*. 2024. Вип. 2. С. 139–143.

4. Шарук О.Г. Основні загрози для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України. *Науковий вісник публічного та приватного права*. 2024. Вип. 3. С. 177–182.

5. Шарук О.Г. Система суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. *KELM*. 2024. № 3 (63). С. 89–96 (Республіка Польща).

які засвідчують апробацію матеріалів дисертації:

6. Шарук О.Г. Структура механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. *Проблемні питання юридичної науки в контексті реформування правової системи України*: матеріали міжнародної науково-практичної конференції (м. Київ, 19–20 жовтня 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 221–223.

7. Шарук О.Г. До необхідності забезпечення міжвідомчих механізмів реалізації адміністративно-правового забезпечення захисту об'єктів критичної інфраструктури фінансового сектору України. *Науково-практичні засади розвитку юридичної науки на сучасному етапі державотворення*: матеріали міжнародної науково-практичної конференції (м. Київ, 15–16

лютого 2023 р.). Київ: Науково-дослідний інститут публічного права, 2023. С. 117–120.

8. Шарук О.Г. Варіації класифікації суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. *Реформування українського законодавства: проблемні питання та шляхи їх вирішення*: матеріали міжнародної науково-практичної конференції (м. Київ, 7–8 лютого 2024 р). Київ: Науково-дослідний інститут публічного права, 2024. С. 171–173.

ЗМІСТ

ВСТУП.....	21
РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО СЕКТОРУ УКРАЇНИ	33
1.1. Критична інфраструктура фінансового сектору України як об’єкт адміністративно-правового захисту	33
1.2. Детермінація сутності адміністративно-правового захисту об’єктів критичної інфраструктури фінансового сектору України крізь призму актуальних загроз	46
1.3. Поняття та структура механізму адміністративно-правового захисту об’єктів критичної інфраструктури фінансового сектору України	65
Висновки до Розділу 1	79
РОЗДІЛ 2. ХАРАКТЕРИСТИКА ОКРЕМИХ ЕЛЕМЕНТІВ МЕХАНІЗМУ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО СЕКТОРУ УКРАЇНИ.	90
2.1. Нормативно-правові основи захисту об’єктів критичної інфраструктури фінансового сектору України	90
2.2. Принципи адміністративно-правового захисту об’єктів критичної інфраструктури фінансового сектору України	108
2.3. Суб’єкти адміністративно-правового захисту об’єктів критичної інфраструктури фінансового сектору України	123
2.4. Форми та методи адміністративно-правового захисту об’єктів критичної інфраструктури фінансового сектору України	139
Висновки до Розділу 2.....	155

РОЗДІЛ 3. ШЛЯХИ ВДОСКОНАЛЕННЯ МЕХАНІЗМУ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО СЕКТОРУ УКРАЇНИ.....	169
3.1. Зарубіжний досвід адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору та можливість його адаптації в Україні	169
3.2. Напрямки розвитку адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України	184
Висновки до Розділу 3.....	199
ВИСНОВКИ	205
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	210
ДОДАТКИ	243

ВСТУП

Обґрунтування вибору теми дослідження. Стійкість, як ключовий постулат розвитку суспільства та держави, нині є не тільки глобальним трендом, а й основним викликом для сучасного етапу державотворення в Україні. Зіштовхнувшись із низкою загроз для національної безпеки, представники влади, як власне і саме суспільство, досить чітко і швидко усвідомили цінність безперебійності роботи усіх визначальних ланок підтримки життєво важливих систем та процесів, їхню вразливість до системних і потенційних ризиків.

Свідченням цього є спланована, розроблена та впроваджена система заходів щодо підвищення стійкості та безпеки основних сфер життєдіяльності суспільства і держави, основним зі способів об'єктивізації яких є систематично здійснюваний адміністративно-правовий захист об'єктів критичної інфраструктури в Україні. Не може бути піддане критиці твердження про те, що саме фінансовий сектор, будучи важливою складовою останніх, є одним з ключових системоутворюючих елементів розбудови державності, адже від ефективності його функціонування залежить не тільки стабільність економічних процесів, а й результативність діяльності державного апарату загалом. Відтак, наявність та адекватна здатність механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України репрезентувати належне управління ризиками, що виникають у сучасному динамічному середовищі, дієвість правових норм та стандартів, які регулюють діяльність уповноважених представників національної системи її захисту, а також їх взаємодію між собою, – це не лише актуальне завдання сьогодення, а й необхідна умова забезпечення окремих його складових від тенденцій негативного впливу.

Варто зауважити, що останнім часом нормативно-правові основи в означеному напрямі зазнали суттєвих змін і оновлень, що зумовлено

наявністю різних факторів закономірного характеру. Оперативність реагування на виклики безпеки відповідних органів влади, що зумовлено їхнім розумінням потреби в адаптації до наявних умов, була належною та своєчасною. Однак, невирішеними остаточно залишаються низка суттєвих практичних питань. Зокрема, аналіз положень Стратегії розвитку фінансового сектору України до 2025 року, затвердженої рішенням Правління Національного банку України від 29 серпня 2023 р. № 299-рш, переконливо засвідчує факт того, що питання забезпечення стійкості об'єктів критичної інфраструктури є пріоритетним, проте інституційна спроможність суб'єктів її реалізації є недостатньою, адже відзначається: 1) обмеженість ресурсів для тестування до вразливостей; 2) недостатня організаційна забезпеченість процедур здійснення такого захисту; 3) слабка взаємодія між регуляторами та іншими суб'єктами національної системи її захисту; 4) наявність проблем з імплементацією актів права ЄС; 5) брак механізмів обміну досвідом з міжнародними та іноземними партнерами; 6) низький рівень кадрового ресурсу та його компетентності тощо.

Відповідно, існує цілком обґрунтована необхідність оптимізації процедур здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України.

Зв'язок теми дисертації із сучасними дослідженнями. Представлена до аналізу проблематика має тісний зв'язок із сучасними дослідженнями в галузі фінансової безпеки, державного управління, а також розвитку фінансового сектору України. Серед комплексних наукових робіт, що розкривають окремі аспекти цієї теми, варто відзначити дослідження таких учених як: Д. Хоружий, який розкрив теоретичні засади та вдосконалив методологічні положення механізму запобігання фінансовим кризам в банківському секторі України (Київ, 2019); О. Казарян, яка обґрунтувала теоретико-методичні засади та розробила практичні рекомендації з удосконалення механізму фінансового регулювання банківського сектору України для забезпечення стійкості його функціонування (Чернігів, 2020); Д. Дорофеев, який вивчав

закономірності розвитку науково-методичних підходів і розробив практичні рекомендації щодо впровадження та використання фінансових інновацій у небанківському фінансовому секторі України з метою підвищення ефективності управління інноваційними процесами та забезпечення стійкого розвитку фінансового сектору (Львів, 2020); В. Косинський, який визначив теоретичні засади, механізм та особливості адміністративно-правового забезпечення безпеки критичної інфраструктури в Україні (Київ, 2020); І. Осипчук, який запропонував власний підхід до інституціональних змін у Службі безпеки України щодо забезпечення критичної інфраструктури шляхом перегляду сутності та особливостей діяльності останньої (Київ, 2021); В. Крикун, який схарактеризував сутність та особливості адміністративно-правового механізму захисту об'єктів критичної інфраструктури в Україні (Харків, 2021); С. Теленик, який розробив теоретико-концептуальні та адміністративно-правові засади створення державної системи захисту критичної інфраструктури і сформулював новітні підходи до її ефективного адміністративно-правового регулювання (Запоріжжя, 2021); А. Федець, який обґрунтував теоретичні засади формування сучасної державної політики фінансової безпеки в контексті національних інтересів та надав практичні рекомендації із реалізації ефективного комплексу механізмів державного управління для безпечного функціонування банківського сектору України (Харків, 2023); Б. Федорущенко, який поглибив теоретико-методологічні засади формування системи забезпечення фінансової безпеки банківського сектору національної економіки, розробив методичні підходи і практичні рекомендації з підвищення рівня фінансової безпеки банківського сектору в Україні (Львів, 2023).

Джерельною базою для вивчення порушених питань слугували також праці таких вчених як: В. Авер'янов, О. Андрійко, В. Андріяш, Д. Бірюков, В. Боровікова, С. Булавина, А. Вархов, Ю. Гаруст, Є. Гетьман, О. Гетьманець, Т. Давидова, О. Джафарова, Є. Дуліба, Ю. Дяченко, Т. Жук, Л. Золотухіна,

О. Кобзар, Л. Кожура, Т. Коломоєць, В. Кремень, А. Крилова, В. Курило, К. Куркова, Д. Левченко, А. Манжула, Л. Миськів, С. Міщенко, В. Новіков, В. Оксінь, О. Остапенко, Н. Петрина, О. Резнік, Т. Романчик, А. Русецький, А. Семенов, Р. Сербин, А. Собакар, Є. Соболев, М. Сокіран, Л. Сорока, Я. Страхніцький, О. Суходол, Т. Тарахович, Н. Троцюк, А. Чубенко, Р. Шаповал, К. Шкарупа та ін. Разом із тим переважна більшість робіт зазначених вчених лише фрагментарно висвітлює окремі питання механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, що є додатковим обґрунтуванням необхідності їхнього наукового розроблення.

Таким чином, нагальна потреба у розв'язанні наукових і практичних питань забезпечення функціональності механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України обумовили вибір теми дисертаційної роботи, визначили його мету, завдання, логіку та зміст.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження узгоджується з основними положеннями Угоди про асоціацію між Україною та Європейським Союзом, ратифікованої Законом України від 16 вересня 2014 р. № 1678-VII; Плану заходів з виконання Програми діяльності Кабінету Міністрів України та Стратегії сталого розвитку «Україна-2020», затвердженого розпорядженням Кабінету Міністрів України від 4 березня 2015 р. № 213-р.; Концепції створення державної системи захисту критичної інфраструктури, схваленої розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009 р; Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 р. № 392; Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 р. № 447/2021; Концепції забезпечення національної системи стійкості, затвердженої Указом Президента України від 27 вересня 2021 р. № 479/2021 та плану заходів з її реалізації до 2025 року, затвердженого розпорядженням Кабінету Міністрів

України від 10 листопада 2023 р. № 1025-р; Стратегії розвитку фінансового сектору України до 2025 року, затвердженої рішенням Правління Національного банку України від 29 серпня 2023 р. № 299-рш. Дисертацію виконано відповідно до плану науково-дослідних робіт Науково-дослідного інституту публічного права «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації 0120U105390).

Мета і завдання дослідження. *Мета* роботи полягає у розробці підходів до визначення змісту й сутності механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, формуванні практичних рекомендацій щодо оптимізації його функціональності.

Для досягнення поставленої мети в дисертації потрібно виконати такі *завдання*:

– визначити сутність правового концепту «критична інфраструктура фінансового сектору України» з точки зору об'єкта адміністративно-правового захисту;

– схарактеризувати юридичну природу адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, визначити актуальні загрози для їх функціональності;

– розкрити поняття, ознаки та структуру механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України;

– з'ясувати нормативно-правові основи захисту об'єктів критичної інфраструктури фінансового сектору України;

– сформулювати систему принципів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України;

– виявити особливості суб'єктної складової адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України;

– визначити форми та методи адміністративно-правового захисту об’єктів критичної інфраструктури фінансового сектору України;

– розкрити зарубіжний досвід адміністративно-правового захисту об’єктів критичної інфраструктури фінансового сектору та можливість його адаптації в Україні;

– окреслити напрямки розвитку адміністративного законодавства у сфері захисту об’єктів критичної інфраструктури фінансового сектору України.

Об’єктом дослідження є суспільні відносини, що виникають у сфері організації та здійснення адміністративно-правового захисту об’єктів критичної інфраструктури фінансового сектору в Україні.

Предмет дослідження – механізм адміністративно-правового захисту об’єктів критичної інфраструктури фінансового сектору України.

Методи дослідження. У роботі відповідно до поставлених завдань використано загальнонаукові, емпіричні та спеціально наукові методи пізнання. Сутність правового концепту «критична інфраструктура фінансового сектору України» (підрозділ 1.1) визначена за сприяння методів: а) *наукової абстракції*, який дозволив абстрагуватися від несуттєвих його характеристик; б) *аналізу та синтезу*, які забезпечили можливість проведення семантичного аналізу його складових; в) *логіко-семантичного методу*, що забезпечив аналіз правової термінології. Юридична природа адміністративно-правового захисту об’єктів критичної інфраструктури (підрозділ 1.2) схарактеризована за допомогою: а) *системно-структурного методу*, що дозволив співвіднести категорії «охорона» та «захист», а також визначити останню як таку, що є концептуальною; б) *діалектичного методу*, який допоміг простежити еволюцію розвитку наукових знань та практики реалізації адміністративно-правового захисту у цій сфері, а також виявити ключові загрози для стійкості функціонування об’єктів критичної інфраструктури фінансового сектору України; в) *логіко-семантичного методу*, що забезпечив розкриття категорій «загроза» та «ризик» з позиції

диференціації їх спільних характеристик. Поняття, ознаки та структура механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України (підрозділ 1.3) були розкриті за допомогою методів: а) *класифікації та групування*, що дозволило запропонувати варіанти елементного складу цього механізму; б) *системного аналізу*, який допоміг з'ясувати його завдання, мету та цілі кожного елемента в загальному механізмі. Нормативно-правові основи захисту об'єктів критичної інфраструктури фінансового сектору України (підрозділ 2.1) досліджено за сприяння: а) методу *порівняльного аналізу*, який дозволив зіставити вітчизняне законодавство з міжнародним та регіональним; б) методу *системного підходу*, що сприяв аналізу нормативно-правових актів як частини загальної системи національної безпеки; в) методу *класифікації та групування*, який допоміг визначити їх систему. Принципи адміністративно-правового захисту у цій сфері (підрозділ 2.2) визначені за допомогою: а) методу *логічного узагальнення*, що дозволив виділити ключові з таких; б) методу *наукової абстракції*, який сприяв визначенню фундаментальних принципів, відкинувши другорядні. Суб'єкти адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України (підрозділ 2.3) ідентифіковані за допомогою: а) *системно-структурного* методу, який допоміг виявити взаємодію між суб'єктами та їхню ієрархію; б) методу *кореляційного аналізу*, який дозволив вивчити взаємозв'язки між різними суб'єктами та рівень їхнього впливу на перебіг досліджуваних правовідносин. Форми та методи адміністративно-правового досліджуваного захисту (підрозділ 2.4) досліджені на основі: а) методу *кількісного та якісного порівняння*, що дозволило визначити ступінь відповідності між категоріями «інструменти», «форми», «методи» в аналізованому контексті; б) методу *системного аналізу*, який допоміг визначити взаємодію між формами та методами, їхню сутність у межах ефективності такого захисту. Зарубіжний досвід (підрозділ 3.1) досліджено із застосуванням: а) методу *порівняльного аналізу*, який дав змогу вивчити

підходи до захисту критичної інфраструктури фінансового сектору в інших країнах і адаптувати найкращі практики для України; б) *формально-юридичного* методу, що забезпечив аналіз відповідного законодавства. Розвиток адміністративного законодавства у цій сфері (підрозділ 3.2) представлено завдяки: а) *діалектичному* методу, який дозволив виявити динаміку розвитку законодавства в контексті змін у безпековому середовищі; б) методу *логічного узагальнення*, який забезпечив формулювання рекомендацій щодо вдосконалення вітчизняного адміністративного законодавства; в) методу *правового прогнозування*, що використано для визначення можливих сценаріїв розвитку запропонованих ініціатив.

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним з перших монографічних досліджень у межах науки адміністративного права, у якому за рахунок комплексного та системного підходу до аналізу адміністративно-правового захисту критичної інфраструктури фінансового сектору України викладено сучасні основи доктринального розуміння правового концепту «критична інфраструктура фінансового сектору України», розкрито особливості адміністративно-правового захисту цих об'єктів, а також визначено напрямки вдосконалення адміністративного законодавства у цій сфері. За результатами проведеного аналізу сформульовано наукові положення та висновки, запропоновані особисто здобувачем. Основні з них такі:

вперше:

– визначено сутність адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України через його ключові ознаки, зокрема: а) є складовою механізму забезпечення національної безпеки; б) виникає у відповідь на необхідність захисту критично важливих фінансових операцій та адміністративних дій, порушення яких завдає шкоди економіці та взаємодіям, залежним від стабільного функціонування грошових потоків та фінансово-адміністративних функцій державних органів; в) реалізується на основі наявності законодавчого та відомчого

нормативно-правового забезпечення; г) має комплексний характер, що об'єктивує можливість (при необхідності) без зміни інституційної чи процедурної складової його здійснення виникнення перехідної трансформації вчинюваних дій з суто охоронних до безпосередньо захисних; д) як сукупність відповідних заходів є репрезентацією існування у правореалізаційній площині спеціалізованої діяльності, що має власну мету, завдання та функції; е) є безперервним процесом, інтенсивність якого (активність, готовність) залежить від стану внутрішнього та зовнішнього безпекового середовища;

– нормативно-правові основи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України схарактеризовано через дуальність інтерпретаційної складової, де: 1) ідейно-концепційний складник визначений як актуальний, належно сформований та такий, що не вимагає додаткової уваги **в контексті оптимізаційних змін якісно новим ідеологічним наповненням**; 2) практико-реалізаційний складник відзначається фрагментарністю, відсутністю публічності механізмів прояву означеної діяльності, а також недостатньою інтеграцією з міжнародними стандартами у сфері захисту критичної інфраструктури;

– розкрито кореляційний взаємозв'язок між принципом публічності та принципом безпеки, захисту й охорони інформації з обмеженим доступом у контексті сформованих правил здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України з узагальненням про необхідність дотримання балансу між забезпеченням прозорості й збереженням секретності, що вимагає чіткої ідентифікації меж щодо того, яка інформація є публічною, а яка підлягає захисту, адже наразі: 1) принцип публічності репрезентується через опубліковані звіти про стан фінансової стабільності та загальний річний звіт діяльності Національного банку, а не окремий щорічний звіт щодо забезпечення захисту критичної інфраструктури у фінансовому секторі; 2) детальна інформація про вразливості та наявні прогалини в механізмах захисту об'єктів критичної

інфраструктури фінансового сектору України є небезпечною з точки зору високого рівня ризику можливих зловживань;

– визначено трьох векторну структуру оптимізаційних змін вітчизняного адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України, що передбачає: 1) нормативний аспект (розробка та затвердження Плану захисту об'єктів критичної інфраструктури фінансового сектору України); 2) адаптаційний (подальша імплементація європейських стандартів, а також впровадження інших позитивних практик); 3) функціональний (вирішення низки практичних проблем його здійснення);

удосконалено:

– наукове розуміння юридичної природи механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, як такого, що репрезентує наявність системи об'єднаних спільним ідейним орієнтиром правових засобів (визначених правовою нормою), практичне втілення яких вимагає координації та злагодженої діяльності уповноважених виконавців певної дії захисного характеру, що має забезпечити дотримання, виконання чи реалізацію відповідної адміністративно-правової норми;

– класифікаційний підхід до групування суб'єктів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, який окрім класичної їх диференціації ґрунтується також на альтернативній;

отримали подальший розвиток:

– висунуті та обґрунтовані припущення, що «критична інфраструктура фінансового сектору України» є складним словосполученням, семантичний аналіз якого доцільно проводити через концептуальний підхід, що дозволяє глибше осягнути його сутність і значення, враховуючи багатогранність складових понять «критична інфраструктура» та «фінансовий сектор» (як опорного та залежного слова, що формують його граматичну структуру) та

пояснює специфіку об'єднаних спільним змістом самостійних категорій, що описують явище, ймовірно яке є об'єктом адміністративно-правового захисту;

– теоретичні розмірковування в контексті того, що інструментальний бік механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України характеризується через зв'язок із категоріями «форми», «методи», які мають розглядатись з позиції функціональної єдності, як правові засоби, що забезпечують прийняття та реалізацію ефективних управлінських рішень;

– результати компаративістичного аналізу, які узагальнено до необхідності впровадження до національної правової системи таких позитивних практик у сфері захисту об'єктів критичної інфраструктури фінансового сектору як: розробка спеціалізованих стратегічних планів; встановлення чітких процедур обміну інформацією; розвиток стимулів для залучення приватного сектора до процесів підвищення загальної стійкості фінансової системи; запровадження єдиних вимог до кібербезпеки фінансового сектору; створення платформ для обміну публічною інформацією; чітке визначення обов'язків і відповідальності суб'єктів захисту об'єктів критичної інфраструктури фінансового сектору та впровадження механізмів оцінки їх кіберстійкості.

Практичне значення отриманих результатів полягає в тому, що сформульовані й аргументовані в дисертаційному дослідженні висновки, теоретичні положення та конкретні пропозиції використовуються та можуть бути використані у:

– *науково-дослідній сфері* – для подальшого наукового вивчення теоретико-методологічних проблем науки адміністративного права (акт впровадження Науково-дослідного інституту публічного права);

– *освітньому процесі* – під час розроблення та викладання навчальної дисципліни «Адміністративне право та процес: доктринальні та практичні

проблеми (акт впровадження Науково-дослідного інституту публічного права);

– *практичній діяльності* – для вдосконалення чинного адміністративного законодавства щодо оптимізації процедур захисту об'єктів критичної інфраструктури фінансового сектору України.

Апробація матеріалів дисертації. Підсумки розроблення проблеми загалом, окремі її аспекти, одержані узагальнення та висновки оприлюднено на трьох міжнародних науково-практичних конференціях: «Проблемні питання юридичної науки в контексті реформування правової системи України» (м. Київ, 19–20 жовтня 2022 р.), «Науково-практичні засади розвитку юридичної науки на сучасному етапі державотворення» (м. Київ, 15–16 лютого 2023 р.), «Реформування українського законодавства: проблемні питання та шляхи їх вирішення» (м. Київ, 7–8 лютого 2024 р.).

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, що містять дев'ять підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 244 сторінки. Робота містить список використаних джерел з 288 найменувань на 33 сторінках.

РОЗДІЛ 1

ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО СЕКТОРУ УКРАЇНИ

1.1. Критична інфраструктура фінансового сектору України як об'єкт адміністративно-правового захисту

Комплексне розуміння сутності складних словосполучень, осягнення їхньої глибини з урахуванням усіх можливих контекстів та значень спонукає вчених до застосування такого наукового інструменту як «концепт», що дозволяє їм розширювати межі існуючого знання про те чи інше явище.

Вартими уваги є твердження Л. Сороки, що термінопоняття «концепт» ще не надто поширене у правовій науці [196, с. 183]. Воно вживається здебільшого у філософії, лінгвістиці (тут найбільше) та культурології [219, с. 70], і будь-яка спроба осягнути його сутність призводить до усвідомлення факту існування цілої низки суміжних понять і їхніх позначень [188, с. 156].

Цікавими є узагальнення Г. Садовнікова, що одним з варіантів інтерпретації концепту є його розуміння у вияві глобальної одиниці розумової діяльності, яка належить до світу свідомості і служить засобом збереження інформації та її обміну. Вони виникають у процесі побудови інформації про об'єкти та їх властивості, причому ця інформація може включати як об'єктивні дані про об'єкти, так і припущення щодо їх якостей і властивостей. Зокрема на відміну від поняття, концепт немає чітких меж, він динамічний і перебуває в постійному русі. Причому він відображає не просто суттєві ознаки об'єкта чи явища, достатні для розуміння його сутності, а всі ті ознаки, які в певному мовному колективі заповнюються знаннями про навколишній світ [188, с. 157, 159].

Кандидат філологічних наук В. Літяга також зазначає, що критичний аналіз сучасних підходів до визначення і аналізу концепту показав складність

цього поняття та неоднозначність його інтерпретації [103, с. 7], адже окрім ототожнення їх з поняттями (що є логічним, оскільки саме поняття «концепт» походить від латинського *conceptus* – «думка», «поняття»), вченими вони співвіднесені з тими значеннями, якими оперує людина в процесі інтелектуального освоєння світу, які характеризують нашу свідомість і нашу пам'ять. Причому тільки частина концептів пов'язана з мовними структурами [104, с. 24, 25], що свідчить про необхідність виваженого та точного його застосування науковцями для опиту того чи іншого явища.

Підтримуємо думку Л. Сороки, що концепт формують елементи, що породжують якісно нове смислове навантаження окремої конструкції, пояснюючи сутність самостійних одиниць її будови, й в абстрактній формі надає уявлення про неї, описуючи не тільки суттєві ознаки й усі можливі фактори, що впливають на її зміст без безпосередньої зміни форми (тобто назви феномену). Мається на увазі, що поняттям чи терміном позначаються явища, процеси чи дії одного смислового виміру, сутність яких ґрунтується на одній сталій характеристиці, що формує ядро його розуміння. Тоді як концепт поєднує кілька різноманітних ознак за характером і спрямуванням, однак позначає одну конкретну дійсність, що безпосередньо описується. Відповідно, під концептом (як категорії адміністративно-правової науки) слід розуміти низку самостійних категорій, які мають власні характерні риси, однак сукупно формують якісно нову юридичну конструкцію [196, с. 185].

З розумінням означеного логічним вбачається висновок, що словосполучення «критична інфраструктура фінансового сектору України» цілком виправдано може бути визначене через концептуальний вираз його сутності, тобто представлене у вигляді правового концепту, який пояснює специфіку об'єднаних спільним змістом самостійних категорій, що описують явище, ймовірно яке є об'єктом адміністративно-правового захисту [277].

Задля підтвердження чи спростування тезису про можливість або відсутність такої щодо визначення цього явища з позиції об'єкта адміністративно-правового захисту вбачаємо доцільним здійснити розгляд

правового концепту «критична інфраструктура фінансового сектору України» через призму семантичного аналізу [277].

Опорним елементом, на нашу думку, у цьому контексті є термін «критична інфраструктура», залежним – «фінансовий сектор». Перший, відповідно, також сформований поєднанням змісту двох слів: «критична», «інфраструктура». Вчений Д. Бірюков визначає, що прикметник «критичний» у різному роді, відмінку чи числі нині з'являється у вітчизняних офіційних документах та нормативно-законодавчих актах в переважній більшості випадків в поєднанні із такими поняттями як «стан», «ситуація» та «зношеність основних фондів» [14, с. 155]. За твердженнями В. Косинського, традиційно в поняття інфраструктури в першу чергу включаються великі автомагістралі, дороги, мости, мережі громадського транспорту, аеропорти, мережі постачання води, обробку та ліквідацію відходів, поводження з небезпечними відходами, виробництво і подачу електроенергії, телекомунікації. Однак цим переліком не слід обмежуватися. В умовах, коли на суші і на морі, в повітрі, космосі і кіберпросторі держави готові вести війни гібридні і проксі-війни, асиметричні війни і війни, які тепер називають «конфлікт», власне поняття «інфраструктура» і «критична інфраструктура» зазнають змін, точніше – наповнюються новим змістом. Тому наразі при класифікації інфраструктур їх прийнято розділяти на два типи: «жорстка інфраструктура» – це фізичні мережі, необхідні для функціонування сучасно розвиненої нації; і «м'яка інфраструктура» – це інститути, необхідні для підтримки соціально-економічної системи, такі як здоров'я, культурні та соціальні стандарти країни, а також фінансова система, системи освіти, охорони здоров'я, державного управління та діяльності правоохоронних органів, і служб екстреної допомоги. [88, с. 24–25].

Але є важливе уточнення: утворення термінологічного сполучення «критична інфраструктура» не є механічним поєднанням двох відомих елементів, а виступає своєрідною нерозривною формулою, запозиченою з інших мов у своєму невід'ємному злитті [208, с. 36].

Загалом значення терміна «критична інфраструктура» (англ. critical infrastructure) дещо відрізняється в різних країнах, але ці відмінності не є суттєвими [17, с. 113]. Частіше всього йдеться про: «системи та об'єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об'єктів підриває національну безпеку, економіку, здоров'я або безпеку населення, або має своїм результатом будь-яку комбінацію з переліченого вище» [15; 206, с. 134].

Уточнимо, що у процесі роботи Євроатлантичної ради НАТО у 2002 році було зазначено, що «критична інфраструктура включає в себе фізичні та кібернетичні системи забезпечення важливих і необхідних видів діяльності економіки та державного управління». У Директиві Європейської Комісії 2008/114 критичну інфраструктуру трактували як «об'єкти, системи чи їх частини, розташовані в країнах-членах ЄС, які є суттєвими для підтримки життєво важливих функцій суспільства, здоров'я, безпеки, захищеності, економічного та соціального благополуччя людей, порушення функціонування або знищення яких матимуть значний вплив у країні-члені ЄС та призведуть до нездатності забезпечувати вказані функції» [240]. Наприклад, у законодавстві Німеччини визначення «критична інфраструктура» можна віднайти у Національній стратегії захисту критичної інфраструктури [264]. Там її визначено як «фізичні та організаційні структури та засоби, які мають життєво важливе значення для суспільства та економіки країни, збій або дисфункція у роботі яких призведе до хронічного дефіциту поставок, суттєвого порушення громадської безпеки та інших драматичних наслідків» [204].

Водночас світовий банк визначає термін «критична інфраструктура» через сфери, що потребують посиленого захисту, а саме: енергетика, транспорт, вода, інформаційні та комунікаційні технології, охорона здоров'я та фінанси. Деякі економіки включають у критичні сфери – освіту, економічні та виробничі сектори [248]. Й загалом питання віднесення тих чи інших об'єктів до критичних розглядаються багатьма авторами як

вітчизняними, так і зарубіжними у різних варіаціях та водночас між ними є багато спільного, що ймовірно пов'язано із цільовим змістом таких об'єктів [88, с. 26].

Зокрема Я. Страхніцький зазначає, що всі потенційні об'єкти критичної інфраструктури можна узагальнити у квадро-комплекс: 1) великі об'єкти критичної інфраструктури загальнодержавного значення; 2) життєво важливі об'єкти критичної інфраструктури; 3) важливі об'єкти критичної інфраструктури; 4) необхідні об'єкти критичної інфраструктури [204].

Окремим аспектом є те, що визначення критичної інфраструктури не повинно бути статичним, а його перегляд може бути відповіддю на динамічний національний та міжнародний ландшафт ризиків. Наприклад, Швейцарія наразі переглядає та спрощує своє визначення критичної інфраструктури як процесу, системи та засобів, які мають важливе значення для функціонування економіки та добробуту населення відповідно. Це спрощення дозволить легше пристосувати сферу своєї критичної інфраструктурної програми до мінливих умов, ніж раніше, коли визначення було більш розпорядчим. Аналогічно, у Великій Британії це визначення перетворилося на включення впливу на національну безпеку, національну оборону чи функціонування держави серед критеріїв для визначення критичної національної інфраструктури [88, с. 30].

З вітчизняного дискурсу Закон України «Про критичну інфраструктуру», описуючи сектори критичної інфраструктури, розкриває їхній зміст через «життєво важливі функції та/або послуги» [204]. До таких послуг належать: 1) урядування та надання найважливіших публічних (адміністративних) послуг; 2) енергозабезпечення (у тому числі постачання теплової енергії); 3) водопостачання та водовідведення; 4) продовольче забезпечення; 5) охорона здоров'я; 6) фармацевтична промисловість; 7) виготовлення вакцин, стале функціонування біолабораторій; 8) інформаційні послуги; 9) електронні комунікації; 10) фінансові послуги; 11) транспортне забезпечення; 12) оборона, державна безпека;

13) правопорядок, здійснення правосуддя, тримання під вартою; 14) цивільний захист населення та територій, служби порятунку; 15) космічна діяльність, космічні технології та послуги; 16) хімічна промисловість; 17) дослідницька діяльність [166]. Однак В. Крикун зазначає, що вітчизняний законодавець не називає якогось конкретного переліку об'єктів критичної інфраструктури й здебільш згадки про них містяться у положеннях підзаконних нормативно-правових актів. Так, наприклад, з метою визначення механізму формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави постановою Кабінету Міністрів України від 23 серпня 2016 року № 563 було затверджено Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Зокрема в даному нормативно-правовому акті надається визначення сутності власне критичної інфраструктури, під якою розуміється сукупність об'єктів держави, які є найбільш важливими для економіки та промисловості, функціонування суспільства та безпеки населення і виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків і людських жертв. При цьому здійснюється спроба визначити об'єкти критичної інфраструктури через їх приблизний перелік – підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки і безпеки держави, суспільства та населення [161]. Унаслідок прийняття постанови Кабінету Міністрів України «Деякі питання об'єктів критичної інформаційної інфраструктури» від 9 жовтня 2020 року № 943 [52] вищенаведений нормативно-правовий акт було визнано таким, що втратив чинність. І хоча вказаною постановою Кабінету Міністрів України затверджено Порядок формування об'єктів критичної інформаційної

інфраструктури задля визначення механізму формування національного та секторальних переліків таких об'єктів [52], сутність останніх не розкривається [92, с. 47].

Більш інформативною є постанова Кабінету Міністрів України від 9 жовтня 2020 року № 1109 «Деякі питання об'єктів критичної інфраструктури», адже саме у ній наводиться перелік секторів критичної інфраструктури, одним з яких визначений і фінансовий.

Варто зауважити, що у вітчизняному законодавстві відсутнє чітке визначення правової категорії «фінансовий сектор України». Так у Комплексній програмі розвитку фінансового сектору України до 2020 року, яка була затверджена Постановою Правління Національного банку України від 18 червня 2015 року № 391 [156], йде мова про сегменти фінансового сектору, – банківський сектор, сектор небанківських фінансових установ, фондовий ринок та ринок капіталу.

Маємо вказати, що відповідно до європейських документів, фінансовий сектор означає сектор, який складається з одного або декількох таких суб'єктів: а) кредитної установи, фінансової установи або компанії з надання допоміжних послуг у розумінні статті 4(1), (5) або (21) Директиви 2006/48/ЄС (так званий «банківський сектор»); б) страхової компанії, перестрахової компанії або страхової холдингової компанії у розумінні статті 13(1), (2), (4) або (5) або статті 212(1) (f) Директиви 2009/138/ЄС (тобто «страховий сектор»); с) інвестиційної фірми в розумінні статті 3(1)(b) Директиви 2006/49/ЄС (йдеться про «сектор інвестиційних послуг») [56].

Водночас проєкт Стратегії розвитку фінансового сектору України до 2015 року (підготовленого робочою групою у складі представників Державної комісії з регулювання ринків фінансових послуг України, Національного банку України та Державної комісії з цінних паперів та фондового ринку [91, с. 29]) передбачав, що фінансовим сектором є фінансовий ринок, який забезпечує накопичення і розподіл інвестиційних ресурсів, взаємодію виробників та споживачів фінансових послуг за

правилами, визначеними державою та її регуляторними органами. Складовими фінансового ринку виступають грошово-кредитний ринок, страховий ринок, фондовий, ринок послуг спільного інвестування, недержавних пенсійних послуг та інші ринки фінансових послуг [201]. Означене визначення піддається критиці з боку вітчизняної наукової думки, адже автори документа ототожнюють його із фінансовим ринком, що не є цілком правомірним [231, с. 33].

Англомовні джерела визначають, що фінансовий сектор складається з банків, інвестиційних організацій, страхових компаній, брокерів з нерухомості, кредитних компаній, іпотечних кредиторів та інвестиційних фондів нерухомості [249]. Саме ж трактування цього терміну зводиться до визначення його сегментом економіки, що складається з компаній та установ, які надають фінансові послуги [249].

Окремі вітчизняні вчені схильні до думки, що поняття «фінансовий сектор» є узагальнюючим для позначення сукупності всіх організацій, головною метою діяльності яких виступає фінансове посередництво (банківська система, до складу якої входять органи грошово-кредитного регулювання, грошово-депозитні банки та інші фінансові установи, що включають пенсійні фонди, страхові компанії, взаємні фонди, кредитні спілки) [114]. А деякі з таких уточнюють, що в умовах ринкової перебудови вітчизняної економіки фінансовий сектор не лише виконує функції грошово-розрахункового забезпечення, а й мобілізує і трансформує вільні заощадження в інвестиційні ресурси для розширеного відтворення економіки, задовольняє потреби суб'єктів у фінансових послугах і тим самим забезпечує економічне зростання [231, с. 31].

Більш вірогідним вважається визначення, згідно з яким фінансовий сектор є цілеспрямованою самоорганізуючою підсистемою фінансової системи і являє собою сукупність фінансових інститутів, що здійснюють операції з надання фінансових послуг і пов'язані з іншими секторами економіки [61]. Такі інститути виконують функції мобілізації заощаджень,

управління ризиками і борговими зобов'язаннями, надання прозорого інформаційного поля, проведення моніторингу фінансових операцій, здійснення корпоративного контролю, забезпечення спеціалізації надання фінансових послуг [36; 231, с. 33–34].

Отже, можемо узагальнити, що з економічної точки зору фінансовий сектор характеризується через сукупність операцій фінансового характеру державних чи комерційних суб'єктів у вияві посередницької діяльності, яка об'єктивує розподіл фінансового капіталу в економіці [277].

Своєю чергою, правовий дискурс порушених питань вимагає детермінації цього явища з іншого ракурсу. Доцільно вказати, що будь-які легітимні суспільні відносини з моменту свого виникнення, існування та до припинення функціонування зазнають на себе впливу значної кількості правових норм, які можуть належати найрізноманітнішим галузям права. При цьому одними з найчисельніших серед них будуть норми права адміністративного, які здійснюють свій регулюючий [92, с. 36], забезпечувальний, охоронний чи захисний вплив майже на кожен сферу суспільних відносин або ж так чи інакше торкаються її. Зокрема, досліджуючи особливості класифікації адміністративно-правових режимів, В. Белєвцева цілком слушно зауважує щодо того, що «існуюча нині розмитість меж регулювання адміністративного права зовсім не говорить про його розчинення в інших галузях, навпаки, при ретельному аналізі виявляється, що багато нових комплексних галузей, які поки формуються, є за своїм змістом фактично масштабним адміністративно-правовим режимом, і в дійсності мають характеризуватися з позиції адміністративного права як його структурно-функціональна невід'ємна складова» [12, с. 110]. Підпадаючи під вплив норм адміністративного права, відповідні суспільні відносини вже можуть бути розглянуті як об'єкт, на який спрямована дія права, тобто є об'єктом адміністративно-правового регулювання [92, с. 36], забезпечення, охорони чи захисту [277].

Відповідно, з цього дискурсу фінансовий сектор може бути розглянутим з боку наявності певних інституцій (суб'єктів правових відносин), які у спосіб дотримання встановлених правил здійснення господарської чи регулятивної діяльності забезпечують суспільний запит на надання якісних фінансових послуг та пов'язаних з ними операцій [277].

Вартими уваги є положення Закону України «Про критичну інфраструктуру», які передбачають, що: «об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам» підлягають охороні та захисту [166]. У контексті критичної інфраструктури фінансового сектору йдеться про два різновиди об'єктів захисту у його межах: 1) ті, що визначаються Національним банком; 2) ті, що визначаються Міністерством фінансів України [277].

У випадку першого це: а) банківська система (надання банківських послуг, зберігання банками запасів готівки Національного банку та проведення операцій із ними); б) ринок небанківських фінансових послуг, крім ринків капіталу та організованих товарних ринків (надання електронних довірчих послуг у банківській системі, надання небанківських фінансових послуг); в) ринок платіжних послуг (надання платіжних послуг) [53].

Щодо другого, це: «планування, виконання та моніторинг виконання бюджетів; розрахунково-касове обслуговування розпорядників та одержувачів бюджетних коштів; здійснення контролю за надходженням до бюджетів та державних цільових фондів податків, зборів, платежів; запобігання та протидія легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення; забезпечення функціонування системи гарантування вкладів фізичних осіб та виведення банків з ринку; здійснення контролю за надходженням митних платежів до державного

бюджету, валютного контролю, пропуск товарів, транспортних засобів через митний кордон України» [53].

Про необхідність диференціації різновидів об'єктів захисту критичної інфраструктури у межах фінансового сектору йдеться й у профільному Законі України «Про критичну інфраструктуру». Так, в ньому визначається, що: «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, встановленому Національним банком України» ... «Віднесення об'єктів до критичної інфраструктури, що здійснюють діяльність на ринках послуг, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, здійснюється в порядку, встановленому такими державними органами» [166].

Постанова Кабінету Міністрів України «Деякі питання об'єктів критичної інфраструктури» від 9 жовтня 2020 року № 1109 уточнює, що секторальні органи у сфері захисту критичної інфраструктури (у цьому випадку – Національний банк та Міністерство фінансів України), використовуючи перелік секторів критичної інфраструктури, ідентифікують об'єкти критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури [53].

Загалом віднесення об'єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, зокрема такими як: 1) виконання функцій із забезпечення життєво важливих національних інтересів; 2) існування викликів і загроз, що можуть виникати щодо об'єктів критичної інфраструктури; 3) ймовірність завдання значної шкоди нормальним умовам життєдіяльності населення; 4) уразливість таких об'єктів, тяжкість можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода здоров'ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення);

соціальної сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); державному суверенітету (зниження обороноздатності, дискредитація іміджу країни, дестабілізація системи державного управління та унеможливлення виконання державою своїх функцій); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного та місцевого значення; 5) масштабність негативних наслідків для держави, які впливають на діяльність стратегічно важливих об'єктів для кількох секторів життєзабезпечення чи призводять до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаться на діяльності ряду інших секторів; 6) тривалість ліквідації таких наслідків та дія подальшого негативного впливу на інші сектори держави; 7) вплив на функціонування суміжних секторів критичної інфраструктури [166].

Крім зазначених критеріїв, існує категоризація об'єктів критичної інфраструктури фінансового сектору. Так, якщо знищення, пошкодження або порушення функціонування такого об'єкта призведе до ненадання об'єктом основних послуг для більш як 100000 клієнтів, тоді такі наслідки відносяться до катастрофічних, для більш як 50000 клієнтів – до критичних, а для більш як 10000 клієнтів – до значних [53].

Відповідно, можемо узагальнити, що правовий концепт «критична інфраструктура фінансового сектору України» позначає коло суспільних відносин виникнення яких обумовлено необхідністю забезпечення безперебійного функціонування окремих складових фінансового сектору, які є критично важливими в аспекті спроможності держави обслуговувати свої потреби і розвиватись у руслі автономності та самодостатності, а також утвердження як правової, демократичної, суверенної держави, яка належним чином виконує своє соціальне призначення з дискурсу гарантування кожному непорушності його прав та законних інтересів.

Таким чином, маємо такі ключові висновки:

– термін «критична інфраструктура» як такий, що має власні ідентифікаційні характеристики, за сучасних умов має два підходи до наукового осмислення його сутності. За умов першого акцентуація здійснюється на об'єктах забезпечення функціональності життєво важливих функцій щодо розвитку економіки та належного розвитку суспільних відносин у тому числі їхньої охорони та захисту (функціональний підхід). Другий підхід полягає у визначенні критичної інфраструктури через галузевий підхід, який фокусується на конкретних секторах або галузях економіки, збій у діяльності яких матиме низку негативних наслідків для національної безпеки;

– зарубіжний досвід свідчить, що чим простішим є визначення терміну «критична інфраструктура», тим якіснішими є стратегії та підходи до її захисту. З вітчизняного дискурсу Закон України «Про критичну інфраструктуру» ідентифікує її через об'єктну характеристику, а точніше – сукупність об'єктів, основне призначення яких забезпечувати безперервність реалізації процедур охорони та захисту національних інтересів України;

– фінансовий сектор нормативно визначений як самостійний з переліку таких, що є важливими для життєдіяльності суспільства та держави. Ідентифікація його категорійно-поняттєвої визначеності має два аспекти: економічний та правовий;

– держава має створити усі необхідні умови задля того, щоб усі критично важливі складові фінансового сектору перебували у стані захисту, тобто були забезпеченими можливістю здійснення адекватної, належної, допустимої, необхідної та ефективної реакції на фактори, чинники, обставини, події тощо, які потенційно чи реально здатні або завдають негативного впливу на функціональність їхньої роботи.

1.2. Детермінація сутності адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України крізь призму актуальних загроз

Логічним продовженням попередньо висвітлених питань є детермінація сутності адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. Причому важливо зауважити, що за загальним контекстом категорії «охорона» та «захист» вживаються як синоніми чи подібні за значенням поняття стосовно мети, завдань, методів. При цьому науковці також інколи не розмежовують ці терміни [21, с. 28]. Додамо також, що Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту містить норму, яка визначає, що «охорона та захист» є єдиним поняттям, що охоплює всі види діяльності, спрямовані на забезпечення функціональності, безперервності і цілісності критичних інфраструктур з метою недопущення, зменшення наслідків і нейтралізації загрози, ризику або вразливості [58; 64, с. 39].

При більш поглибленому аналізі розуміння сутності категорій «захист» та «охорона», так і щодо їх співвідношення, побачимо, що в більшості випадків перша з них сприймається як складова другої. Наприклад, Д. Горбась вказує на те, що зміст остаточної розкривається як комплекс заходів, спрямованих на недопущення порушень тих чи інших суспільно важливих об'єктів і цінностей, так і на їх захист. Підсумовуючи, вчений вказує на те, що в такому випадку поняття «захист» поглинається поняттям «охорона» [42, с. 35]. Аналогічною є позиція авторів підручника з Адміністративного права за загальною редакцією В. Галуцька [3], які вказують на те, що «охорона» є ширшим поняттям, яке включає в себе попередження порушень прав і свобод, тоді як «захист» є його складовою і

полягає у вжитті заходів після порушення прав. Охорона передбачає методи переконання, а захист – методи примусу.

Підтримуємо позицію В. Крикуна, що така позиція не відповідає дійсності, оскільки, як свідчить аналіз положень чинного національного законодавства, здебільшого прослідковується протилежна ситуація. Із чого слідує, що незалежно від різновиду суспільних відносин, на які спрямовано охорону, у всіх випадках, а також в більшості інших законодавчих визначень категорії «охорона», її сутність розкривається через запобігання або ж недопущення настання відповідних небажаних наслідків. Якщо ж проаналізувати підходи законодавця щодо розуміння сутності категорії «захист», побачимо, що окрім запобігання буде називатися ще низка її складових даного явища. Так, наприклад, відповідно до статті 4 Кодексу цивільного захисту України від 2 жовтня 2012 року цивільний захист – це функція держави, спрямована на захист населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій шляхом запобігання таким ситуаціям, ліквідації їх наслідків і надання допомоги постраждалим у мирний час та в особливий період [80; 92, с. 44].

Ми погоджуємось, що охорона передбачає застосування превентивних заходів та використання методу переконання, щоб уникнути порушень встановлених правил. Натомість захист більш орієнтований на реагування вже наявних порушень із застосуванням примусових методів, але водночас існує певна взаємопов'язаність між охоронними та захисними заходами [278].

Власне, як влучно зазначили С. Булавіна та Т. Давидова, охороною прав здійснюється запобігання порушення прав і обов'язків, а захист, спрямований на поновлення порушених прав і обов'язків чи компенсацію втраченого права, як наслідок порушеного права. Вони відрізняються за часовими межами застосування. Охорона діє постійно, як превенція у тому числі, а захист – в результаті порушення прав та обов'язків. Розрізняються вони і за інструментарієм, що застосовується. Охорона характеризується

більш широким переліком заходів – ідеологічних, економічних, правових тощо у той час, як захист – це використання суто правових методів. Рішення проблеми ефективної охорони і захисту прав перебуває у безпосередній залежності від розвитку нормативно-правових актів, що регулюють відносини охорони і захисту, здатності науковців шукати межі їх нетотожності [21, с. 30].

Відповідно, наукові підходи до визначення понять охорони та захисту прав людини підкреслюють їхню різницю за змістом, методами та структурою, водночас визнаючи їхню взаємозалежність в контексті більш загальних процесів [278].

Однак, ми не спростовуємо того, що захист можна тлумачити ширше, включаючи до нього процеси зародження, формування, розвитку, стабілізації та згасання потреб, інтересів і прав. Це передбачає здійснення захисту не після того, як вчинено [220, с. 184] протиправні дії, а до їх здійснення. З огляду на це більш правильно визначати захист як дії, спрямовані на припинення або недопущення порушень [220, с. 184–185], а також ліквідацію наслідків у випадку його здійснення.

У досліджуваному контексті така інтерпретація також має місце, адже відповідно до положень чинного законодавства захист критичної інфраструктури передбачає всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації [166].

Як бачимо, законодавець вирішив розглядати це питання з позиції включення охорони до системи захисту, що загалом не є помилковим, адже досліджувана сфера характеризується наявністю національної системи захисту критичної інфраструктури (у інституційному аспекті), яка цілком об'єктивно в змозі поєднувати реалізацію як превентивних заходів, так і реагування на факти відхилення від норми [278].

Маємо визначити, що термін «правовий захист» в адміністративному праві здебільшого зводиться до діяльності компетентних органів державної влади, органів управління і місцевого самоуправління [213, с. 116–117], яка об'єктивує реалізацію відповідних заходів. Спеціалізовано означена діяльність іменується як адміністративно-правовий захист.

Щодо сутності адміністративно-правового захисту, першочергово, слід відзначити його приналежність до відповідної галузі права. Однак важливо зауважити, що українське законодавство та наукові праці не містять єдиної точки зору щодо розуміння цієї правової категорії. Досить часто вказане поняття ототожнюється з такими термінами, як «адміністративно-правова охорона» чи навіть «адміністративно-правове забезпечення», а також використовується у вузькому та широкому розумінні з різним змістовним навантаженням [81, с. 119].

Важливим у зазначеному є те, що за загальним контекстом означений термін є застосовним до правовідносин захисту прав, свобод та законних інтересів особи (осіб). Так, наприклад, автори підручника з адміністративного права за загальною редакцією В. Галунька адміністративно-правовий захист розуміють як динамічні (активні) дії публічної адміністрації, спрямовані на відновлення порушених прав, свобод та законних інтересів фізичних і юридичних осіб, усунення перешкод щодо їх здійснення засобами адміністративного права з можливістю застосування заходів адміністративного примусу та притягнення винних до адміністративної відповідальності [3, с. 247]. Або ж вчена Л. Кожура визначає її як організаційно-правову діяльність органів публічної адміністрації, яка здійснюється на основі адміністративно-правових норм, підкріплена системою правових гарантій; сутністю якої є забезпечення та захист за допомогою правових засобів прав осіб від протиправних діянь з притягненням правопорушників до юридичної відповідальності [81, с. 121].

Загалом вчені у своїх інтерпретаціях сутності цієї категорії досить чітко і правильно зазначають про сукупність правовідносин, які підлягають

захисту через встановлену нормативну вказівку на це і розроблений процедурний аспект здійснення відповідних заходів нормами адміністративного права, але дизоб'єктивізуючи цю категорію припускаються помилки автоматичного розкриття її сутності через правовідносини, що пов'язані з правами людини та громадянина, які хоч і є основним, однак не єдиним об'єктом протиправного посягання. Зокрема доцільніше вести мову про охоронювані законом цінності та інтереси, які можуть належати як конкретній особі, так і їх групі чи державі загалом. Тобто є два основних об'єкти протиправного посягання – одиничний чи публічний охоронюваних законом інтерес (цінність, благо) [278]. Зокрема щодо останнього вартими уваги є висновки Великої Палати Верховного Суду, який зазначає, що важливі для значної кількості фізичних і юридичних осіб потреби, які, відповідно до законодавчо встановленої компетенції, забезпечуються суб'єктами публічної адміністрації [143] формують категорію «публічні інтереси».

Означений тезис дає можливість для твердження, що адміністративно-правовий захист, як і адміністративно-правова охорона чи адміністративно-правове забезпечення, логічніше розглядати з позиції самостійних врегульованих процесів, що мають різні завдання та механізми реалізації. Узагальнено та схематично їхнє співвідношення можна представити так: забезпечення спрямовується на охорону та захист, а охорона та захист – реалізуються у тісній взаємодії. Причому саме визначення адміністративно-правового захисту має розглядатись з дуальної інтерпретації об'єктної складової. Мається на увазі, що окрім юридичного відношення особи до конкретного інтересу (як правило, права на щось) має враховуватись його безпосередній стан з позиції убезпечення від зміни властивостей чи характеристик, руйнування або загалом знищення [278].

Наприклад, вбачається спірною думка В. Пітателева, що адміністративно-правовий захист земель сільськогосподарського призначення – це динамічні дії публічної адміністрації, які спрямовують свій

вектор на відновлення порушеного права на землі сільськогосподарського призначення в Україні, мінімізацію перешкод щодо законного володіння нею, що здійснюються засобами адміністративного права з можливістю застосування заходів адміністративного примусу та притягнення винних до адміністративної відповідальності [135, с. 25]. Автор занадто звузив її зміст юридичним відношенням особи до такого блага, у той час коли доречніше було б вести мову також і про самі землі сільськогосподарського призначення як цінність, що потребує комплексного захисту та збереження. За такого контексту адміністративно-правовий захист не обмежений аспектами володіння та користування землею, а включає також екологічні, економічні та соціальні фактори впливу на стан та якість земельних ресурсів [278].

Отже, можемо підсумувати, що за нашим баченням адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України доцільно визначити як систему заходів охоронного та захисного спрямування, реалізовану уповноваженими суб'єктами національної системи захисту критичної інфраструктури задля забезпечення стійкості та безпеки сегментів ринку фінансових послуг та окремих фінансових операцій, що формують фінансовий сектор критичної інфраструктури України [278].

Характеризуючи його сутність вбачаємо доцільним обмежитись такими положеннями: а) адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України є складовою механізму забезпечення національної безпеки; б) адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України виникає у відповідь на необхідність захисту критично важливих фінансових операцій та адміністративних дій, порушення яких завдає шкоди економіці та взаємодіям, залежним від стабільного функціонування грошових потоків та фінансово-адміністративних функцій державних органів; в) адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України реалізується на основі наявності законодавчого та відомчого

нормативно-правового забезпечення; г) адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України має комплексний характер, що об'єктивує можливість (при необхідності) без зміни інституційної чи процедурної складової його здійснення виникнення перехідної трансформації вчинюваних дій з суто охоронних до безпосередньо захисних; д) адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України як сукупність відповідних заходів є репрезентацією існування у правореалізаційній площині спеціалізованої діяльності, що має власну мету, завдання та функції; е) адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України є безперервним процесом, інтенсивність якого (активність, готовність) залежить від стану внутрішнього та зовнішнього безпекового середовища [278].

У контексті деталізації останнього варто зауважити, що безпека та стійкість за загальним контекстом перебувають у кореляційному взаємозв'язку. Стійкість є невід'ємною складовою безпеки, що досягається шляхом забезпечення можливості для конкретної системи ефективно реагувати на загрози та ризики [228].

Для повноти розгляду цього питання, зазначимо, що вчений М. Сокіран [279] виявив, що: «у законодавстві термін «ризик» тлумачиться як: 1) можливість виникнення шкідливого впливу на здоров'я людини та ступінь цього впливу, що походить з небезпечного (небезпечних) фактора (факторів) у харчовому продукті (Про основні принципи та вимоги до безпечності та якості харчових продуктів [170]); 2) можливість наявності та вірогідний масштаб наслідків несприятливої події протягом визначеного періоду (Про карантин рослин [165]); 3) імовірність виникнення будь-якої небезпечної події протягом певного періоду або за певних обставин (Про об'єкти підвищеної небезпеки [168]); 4) можливість виникнення та вірогідні масштаби наслідків негативного впливу протягом певного періоду часу (Про технічні регламенти та оцінку відповідності [175]); 5) комбінація повної

імовірності або частоти події з негативним ефектом, що обумовлена небезпекою або серйозністю цього ефекту (Про затвердження Правил сертифікації суб'єктів, що надають послуги з аеронавігаційного обслуговування [163], Про затвердження Положення про нагляд за безпекою польотів у системі організації повітряного руху та змін до деяких нормативно-правових актів [158]); 6) ймовірність виникнення негативних наслідків від провадження господарської діяльності та можливий розмір втрат від них, що вимірюється у кількісних та якісних показниках (Про основні засади державного нагляду (контролю) у сфері господарської діяльності [169]); 7) ймовірність виникнення обставин та причин, що обумовлюють виникнення ДТП, катастроф, аварій (Про затвердження Порядку технічного розслідування дорожньо-транспортних пригод, катастроф, аварій на автомобільному та міському електричному (трамвай, тролейбус) транспорті [160]); 8) будь-яка обставина чи подія, яку можна розумно виявити, що має потенційний негативний вплив на безпеку мережевих та інформаційних систем (Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу [54]). Своєю чергою, термін «загроза» розуміється як: а) наявні та потенційно можливі явища і чинники, що негативно впливають на будь-що (наприклад: 1) на сферу безпеки державного кордону (Про затвердження Інструкції з проведення аналізу ризиків у Державній прикордонній службі України [155]); 2) охоронювані законом цінності або суспільні відносини (Деякі питання запровадження в діяльність центральних органів виконавчої влади системи оцінки СОСТА Україна [51])); б) природна властивість небезпечної речовини або фізичної ситуації, що потенційно може спричинити шкоду довкіллю і здоров'ю людини (Про контроль загроз виникнення значних аварій, пов'язаних із використанням небезпечних речовин, та про внесення змін і подальше скасування Директиви Ради 96/82/ЄС) [57]; в) потенційна можливість реалізації вразливості (Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих

послуг та їхніх відокремлених пунктів реєстрації [152]» [279, с. 99]. До матеріалів аналізу науковця можемо додати, що законодавець також апелює термінами: 1) «загроза заподіяння значної шкоди», який розуміється як неминуча загроза заподіяння значної шкоди, що базується на фактах, а не на голослівних твердженнях, припущеннях або маловірогідній можливості (Про застосування спеціальних заходів щодо імпорту в Україну [154]); 2) «безпосередня загроза безпеці», що означає ситуацію, коли є доказ того, що продукт, послуга, система, компонент, обладнання чи об'єкт, або перебувають у такому стані, або використовуються, постачаються чи обслуговуються таким чином, що існує ймовірність травмування людей, якщо тільки ситуацію не буде негайно виправлено (Імплементативний Регламент Комісії (ЄС) № 628/2013 від 28 червня 2013 року про методи роботи Європейського агентства з безпеки авіації при проведенні стандартизаційних інспектувань та при здійсненні моніторингу застосування правил Регламенту Європейського Парламенту і Ради (ЄС) № 216/2008 та про скасування Регламенту Комісії (ЄС) № 736/2006 [72]); 3) «проектна загроза об'єкта критичної інфраструктури» як документ встановленої форми, який визначає властивості, характеристики реальних і потенційних загроз об'єкта критичної інфраструктури, на зниження ймовірності реалізації яких має бути спрямовано функціонування системи захисту критичної інфраструктури» (Про критичну інфраструктуру[166]).

З наведеного маємо, що аналізовані терміни пов'язані з явищем «небезпеки», тобто за властивість мають настання негативних наслідків у випадку активації механізмів їх реалізації в практичну площину. Також маємо, що: 1) загроза є більш статичним явищем, тоді як ризик характеризується оціночним припущенням про негативний вплив в перспективі; 2) ризик як оціночне явище є комбінацією ймовірностей, тоді як загроза може бути реальною та потенційною; 3) ризик за загальним контекстом має якісні і кількісні показники, а загроза існує незалежно від того, реалізована вона чи ні [228].

Вчений М. Сокіран узагальнює аналіз визначених ним ідентифікаційних характеристик означених явищ таким чином: категорія «ризик» у контексті забезпечення безпеки та стійкості критичної інформаційної інфраструктури в Україні є формою вияву небезпеки, обумовленою наявністю явищ, чинників, обставини, подій тощо, яка потенційно має завдати наслідків негативного впливу на перебіг суспільних відносин, функціональність об'єктів чи конкретним охоронюваним законом інтересам у цій сфері; під категорією загрози слід розуміти також форму вияву небезпеки, яка обумовлена наявністю явищ, чинників, обставин, подій тощо, однак тільки тої, однак тільки тої, яка в майбутньому завдасть шкоди безпеці та стійкості критичної інформаційної інфраструктури в Україні (зокрема у разі відсутності дій щодо її нейтралізації вона переросте у ризик) [279, с. 100].

Іншої думки вчений Т. Романчик, який при дослідженні небезпеки, загрози та ризику прийшов до висновку, що: «небезпеку можна розглядати як стан, загрозу – як дію, ризик – як імовірність втрати частини ресурсів під негативним впливом випадкових подій, які погано прогножуються» [185].

Аналізуючи положення Закону України «Про критичну інфраструктуру», зокрема пункт 4 частини 2 статті 4 де зазначено, що: «Державна політика у сфері захисту критичної інфраструктури ґрунтується на засадах створення умов та впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, на зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів» вбачаємо, що загроза у цьому контексті є основним явищем на мінімізацію наслідків якої спрямовуються дії уповноважених суб'єктів. Водночас ризик визначається як імовірність виникнення цих загроз (зрозуміло, що ризик має свої негативні наслідки, зокрема у цьому контексті у вияві загроз), протидія яким є першим кроком для убезпечення систем від негативного впливу неконтрольованих процесів різного характеру [228].

З урахуванням нашого бачення розмежування досліджуваних категорій варто зауважити, що загрози для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України доцільно диференціювати на два різновиди: універсальні, тобто такі, що можуть або спричиняють негативні наслідки для більшості або навіть для усіх об'єктів критичної інфраструктури в Україні та індивідуальні, сутність яких нами зведено до виключно досліджуваної сфери [228].

Уточнимо, що загрози критичній інфраструктурі, як правило, розподіляються на три групи, що включають аварії й технічні збої, природні лиха та небезпечні природні явища, зловмисні дії (груп або окремих осіб, таких як терористи, злочинці й диверсанти, промислове шпигунство, а також бойові дії). Особливо небезпечними є комбіновані загрози й загрози, реалізація яких може призвести до катастрофічних і різноманітних каскадних ефектів унаслідок взаємозалежності елементів критичної інфраструктури [65]. Додатково вкажемо, що закордонні вчені, проаналізувавши набір даних у 29 європейських країнах, вказують про те, що на енергетичний сектор припадає 60% усіх каскадів, 28% – на інформаційний сектор (телекомунікацій та Інтернету), 5% – на транспортний сектор, 3% – на водний [261]. Означене свідчить, що енергетичний та інформаційний сектори є найбільш вразливими [194, с. 289], порушення функціональності яких може стати причиною каскадних збоїв в інших сферах, зокрема і у фінансовій [228].

Маємо також вказати, що у 2015 році експерти вперше запропонували наступні категорії загроз, на які має бути налаштований захист критичної інфраструктури, а саме: 1) аварії та технічні збої, зокрема, авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин, відмови систем, аварії та надзвичайні події обумовлені недбалістю, організаційними помилками тощо; 2) небезпечні природні явища, зокрема, надзвичайні погодні умови, лісові, степові та торф'яні пожежі, сейсмічні явища, епідемії та пандемії, космічні явища,

урагани, торнадо, землетруси, цунамі, повені і т. ін.; 3) зловмисні дії, зокрема, зловмисні дії груп або окремих осіб, таких як терористи, злочинці і диверсанти, а також військові дії в умовах війни [16].

Доречно навести й думку А. Собакаря, який вказує, що залежно від типу інфраструктури, загрози її безпечному та сталому функціонуванню класифікуються на дві групи: фізичні загрози та кібератаки. Зрозуміло, що трубопроводи, підстанції, склади, комунікаційна інфраструктура та промислові заводи в основному піддаються фізичним загрозам. На противагу ним, кіберзагрози піддають небезпеці системи моніторингу та контролю, бази даних, функціональні системи, програмне забезпечення, автоматизовані виробничі засоби тощо [193, с. 266–267].

Враховуючи зазначене та опираючись на власний суб'єктивізм, вбачаємо, що серед основних універсальних загроз, які є актуальними для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України можна виділити:

1) технічні збої або інші невідворотні обставини, які об'єктивно унеможливили проведення відповідних операцій. Яскравий приклад такого стався першого вересня 2022 року, коли тимчасово перестали працювати термінали, картки та онлайн-банкінг Ощадбанку. Начальник управління банку зі зв'язків із громадськістю та ЗМІ Я. Титова пояснила, що банк проводив планові технічні роботи. За її словами, зазвичай такий процес відбувається непомітно для клієнтів, але цього разу стався технічний збій. При цьому він тривав близько 1,5 години [23]. На основі цього прикладу можемо обґрунтувати, що представники банку не врахували усіх ризиків при проведенні планових технічних робіт, що стало загрозою для безперервності здійснення фінансових операцій з такими наслідками: тимчасове призупинення доступу клієнтів до їхніх рахунків; виникнення паніки серед клієнтів; втрати у вигляді недоотриманих доходів та репутаційні збитки для банку. Цей випадок демонструє, наскільки важливою є підготовка та управління ризиками для підтримки стійкості роботи банківської системи;

2) вчинення терористичних актів і диверсійних операцій. Зокрема напружена воєнно-політична ситуація, в умовах якої наша держава відстоює власну територіальну цілісність і суверенітет, характеризується значним зростанням рівня таких загроз зловмисних дій, як вчинення терористичних актів і диверсійних операцій на території України, спрямованих на об'єкти критичної інфраструктури [261]. Фінансовий сектор не є виключенням, адже майже щоденно стикається з кібератаками ворога. Власне масштабні хакерські атаки на органи влади, Національний банк та банківські застосунки відбувалися і до 24 лютого. Зокрема, віртуальну підготовку до реального нападу на Україну росіяни провели 13-14 січня та 15-16 лютого. Причому, як правило, інтенсивність хакерських атак посилюється, наприклад, під час оголошення українськими волонтерами масштабних зборів. Загалом українська система кіберзахисту виявилася напрочуд стійкою та підготовленою до ударів агресора [27]. Однак тимчасових збоїв у роботі фінансового ринку інколи вдавалось досягти. Як зазначає О. Гороховський (співзасновник проекту «Монобанк»): «За дев'ять місяців вони змогли лише на кілька годин «покласти» сайт, який не впливає на обслуговування клієнтів. Усі атаки були передбачені в архітектурі системи безпеки» [27]. Згодом ситуація дещо погіршилась, адже масштабного збою у роботі «Монобанк» все ж таки вдалося досягти. Варто також зазначити, що банки стають об'єктами власне і терористичних актів і диверсійних операцій. Наприклад, у центрі Чернігова близько 4 ранку 6 травня 2024 року підірвали відділення банку «Південний». Це відділення було ключовим для банку у Чернігові – єдине у місті, яке працювало навіть під час відключення електроенергії [215];

3) світові фінансово-економічні кризи. Причини, через які в економіці виникають кризи, можуть бути різні. Це й невміле фінансово-економічне управління. І перенасичення ринків пропозицією, тобто надмірна конкуренція. І стихійні явища – катаклізми, війни, катастрофи, епідемії [189]. Їхні наслідки значні, адже викликають дестабілізацію всього фінансового

сектора або його частини, що проявляється у неспроможності його складовими виконувати свої функції внаслідок критичного погіршення фінансових показників. Вони також можуть супроводжуватися скороченням кількості суб'єктів фінансового ринку і застосуванням державою заходів надзвичайного характеру [7];

4) не ефективність регулятивних, контрольно-наглядових та моніторингових заходів. Наприклад, збільшення випадків шахрайства та відмивання грошей корелює з результативністю означеної діяльності. Заслабкі регулятивні рамки здатні завдати значної шкоди фінансовій системі загалом, а надмірне регулювання може обмежувати гнучкість і інновації в механізмах її розвитку;

5) соціально-політична нестабільність. Будь-які зміни політичного чи соціального характеру здатні завдати шкоди фінансовому сектору як через функціональний вплив (наприклад, масове зняття готівки чи депозитів), так і фізичний вплив (наприклад, порушення роботи банківських установ через акції протесту). Як свого часу зазначив В. Заплатинський, – «сьогодні слід вжити усіх невідкладних заходів, щоб запобігти впливу політичної ситуації на економічну сферу» [197];

б) пошкодження чи знищення матеріальних актів суб'єктів фінансового сектору через воєнні дії. Безпосередніх інфраструктурних втрат зазнали чисельні суб'єкти ринку фінансових послуг. Як приклад, це банк «ПУМБ» у якого під час нічної ракетної атаки РФ на Запоріжжя 18 жовтня 2023 року постраждало відділення за адресою: пр-т Соборний, 149 [146]. Загалом збитки банків від знищення нерухомості сягнули 750 млн грн уже на кінець 2022 року. За очікуваннями Національного банку України, втрати банків унаслідок війни можуть зрости до 20% довоєнного працюючого портфеля. Попри те, що втрати банків зростуть, більшість банків зможе їх поглинути за рахунок прибутку та запасу капіталу [203].

Щодо індивідуальних загроз маємо вказати, що аналізуючи положення оновленої Стратегії розвитку фінансового сектору України [203], загрозами

для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України можуть бути:

1) спад економічної активності – наразі економічна активність почала поступово відновлюватися завдяки усуненню перебоїв у ланцюгах постачання, релокації підприємств, звільненню окупованих територій і поверненню частини переміщених осіб [203];

2) інфляційні процеси – зараз також спостерігається контрольоване середовище інфляційного тиску;

3) втрата міжнародної підтримки – оскільки значна частина дефіциту державного бюджету покривається за рахунок міжнародної допомоги, її втрата чи зменшення обсягів можуть бути катастрофічними для вітчизняної економіки;

4) відсутність стратегічного бачення та плановірності здійснення реформаційних змін – наразі це питання не є критичним в досліджуваній сфері, адже швидка реакція Національного банку України на зміни векторів руху є показником адаптивності та оперативності. Проте все ще не вистачає налагодженого комунікаційного механізму між різними органами влади, що негативно позначається на загальному векторі розвитку держави;

5) недотримання міжнародних зобов'язань – зокрема в аспекті боротьби з корупцією може уповільнити інтеграційні процеси;

6) втрата прибутковості банків – наразі банки мають запас капіталу та ліквідності, є операційно стійкими та ефективними, адже мали плани дій на випадок несприятливих подій [203];

7) спад попиту на кредитування – у кінці 2022 року Національний банк України оприлюднив опитування, яке провели серед банків. У ньому банки проаналізували поведінку своїх клієнтів та надали певні прогнози стосовно своєї діяльності. Виявилось, що: а) у III кварталі зафіксовано незначне відновлення попиту на корпоративні кредити; б) рівень схвалення заявок на корпоративні та роздрібні кредити скорочується від початку повномасштабного вторгнення; в) окремі банки поліпшили оцінки боргового

навантаження бізнесу, але погіршили для населення. Загалом банки оцінюють боргове навантаження клієнтів як середнє; г) у наступні 12 місяців очікувалось погіршення якості позик та зростання обсягів фондування [226]. Наприкінці 2023 року банки все ж таки фіксують відновлення попиту на кредити та очікують на подальше зростання корпоративного і роздрібного портфелів [8];

8) втрата спроможностей системи гарантування вкладів – наразі система гарантування вкладів в змозі демонструвати стійкість та ефективність [203];

9) неефективне нормативне регулювання небанківського фінансового ринку – розвиток небанківського фінансового ринку потребує законодавчих змін у напрямі наближення регуляторного середовища до міжнародних стандартів [203];

10) втрата банками ліквідності – загалом обсяг безготівкових операцій зростає, розширюється перелік фінансових операцій, які здійснюються дистанційно [203];

11) неефективність та недостатня розвиненість інфраструктури ринків капіталу та організованих товарних ринків – сьогодні означене є проблемою, адже питання наявності дієвих механізмів залучення інвестицій (як внутрішніх, так і іноземних) у приватний та державний сектор є ключовою передумовою для швидкого та ефективного повоєнного відновлення України [203];

12) відсутність доступності фінансових послуг – активно впроваджуються інноваційні технології, здатні задовольнити сучасний попит на фінансові послуги.

Окремо зазначимо, що, на нашу думку, система означених має доповнитись ще однією, – неспроможність регулятора ефективно здійснювати свої повноваження. Наприклад, донедавна існувала законодавча проблема щодо виведення з ринку системно важливого банку. Така необхідність виникла на тлі військової агресії з боку рф, адже власниками

фінансових устав України з-поміж інших є представники громадянства цієї країни. У зв'язку з цим було удосконалено чинне законодавство в частині запровадження можливості впливу на банки, які або власники істотної участі у яких є особами, до яких застосовано санкції. Національний банк України отримав ефективний механізм впливу на підсанкційних осіб, що є власниками істотної участі у банку та які, з огляду на застосування до них санкцій, не відповідатимуть вимогам Національного банку України, зокрема щодо ділової репутації. Застосовані санкції ставлять під сумнів платоспроможність підсанкційних осіб і можливість виконання ними грошових зобов'язань, що в подальшому може призвести до невідповідності майнового стану вимогам закону щодо підтримки належного рівня капіталу банку. Тож Національний банк України має можливість відмовляти в допуску підсанкційних осіб до володіння істотною участю в банках України [145].

Означені зміни також дозволяють Національному банку України націоналізувати банки підсанкційних власників. Яскравий приклад тому «Сенс банк» (до 1 грудня 2022 року – «Альфа-Банк»). Зокрема Національний банк України ухвалив рішення про виведення з ринку АТ «Сенс Банк» і звернувся до уряду з пропозицією про його націоналізацію. Як повідомляється на сайті Національного банку України, за інформацією «Сенс Банку», власниками прямої істотної участі в Банку є АВН Ukraine Limited (Кіпр) та АВН Holdings S.A. (Люксембург), власниками опосередкованої істотної участі – громадянин рф та Ізраїлю М. Фрідман, громадянин росії та Латвії П. Авен, громадянин рф А. Косошов. Зазначені фізичні особи є остаточними ключовими учасниками в структурі власності банку. Національний банк України з посиланням на звіт незалежного аудитора ТОВ «РСМ Україна» за 2022 рік зазначає, що зв'язок власників опосередкованої істотної участі в АТ «Сенс Банк» М. Фрідмана та П. Авена з рф, їхня підтримка дій та політики, які загрожують територіальній цілісності, суверенітету та незалежності України, завдає значного репутаційного ризику

та має негативний вплив на діяльність банку. Аудитор також звертає увагу на висновки управлінського персоналу банку щодо наявності суттєвої невизначеності, яка може поставити під значний сумнів спроможність банку продовжувати свою діяльність на безперервній основі та динаміку окремих показників його діяльності, а також погіршення платіжної дисципліни позичальників банку, що вплинуло на його регулятивний капітал, який за період з 1 березня 2022 року до 1 липня 2023 року зменшився на 50%, водночас в інших системно важливих банків він загалом збільшився на 29% [119].

У липні 2023 року держава націоналізувала «Сенс-банк». Уряд придбав його у Фонду гарантування вкладів за одну гривню. До того, 20 липня, уряд вивів його з ринку, що й дозволило націоналізацію. Також у липні Служба безпеки України повідомила, що ексвласники «Сенс банку» хотіли довести його до банкрутства та вивести кошти до росії. Вони організували схему зі зміни номінальних власників [5].

Наостанок зазначимо і щодо системних ризиків фінансового сектору. Зокрема доцільно вказати, що систему таких визначає та відслідковує їх рівень Рада з фінансової стабільності. Кожне засідання Ради традиційно починається з їхнього огляду. До числа таких у 2023 році віднесено: світова економіка, зовнішня кон'юнктура, економічні умови, державні фінанси, валютний ринок, геополітика [68, с. 5]. Окрім того, Секретаріат Ради відстежує системні ризики, виявлені міжнародними і національними радами та комітетами з фінансової стабільності, а також їхні рекомендації [68, с. 9].

Таким чином, маємо такі ключові висновки:

– без адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України навряд чи вдасться забезпечити належний рівень безпеки та стабільності ринку фінансових послуг та пов'язаних з ними операцій в Україні, адже ризики та загрози є постійними, різноманітними, а недостатня увага та реагування на них можуть мати катастрофічні наслідки;

– загрози та ризики можна розглядати з різних боків та з різним інтерпретаційним контекстом. Чинне законодавство у досліджуваній сфері не надає вичерпного визначення означених термінів, чим, власне, зумовлює виникнення актуальних наукових дискусій;

– з огляду на проаналізовані нормативні положення можна зробити висновок, що ризики мають два різновиди: ті, що пов'язані із виникненням загроз (неврахування ризику веде до загрози); ті, що існують паралельно з ймовірністю виникнення загроз (самостійні ризики, що наявними є постійно). Причому другий контекст є значно ширшим. Більшою мірою саме про нього йдеться у нормах чинного законодавства. Натомість загрозою, за таким баченням, є фізичний прояв небезпеки від наявності (виникнення) певного явища;

– з точки зору наукового суб'єктивізму нам більше імпонує думка, що ризик має бути пов'язаним із загрозою, точніше зумовлювати наявність останніх. У такій інтерпретації актуальними загрозами для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України наразі є: технічні збої або інші невідворотні обставини, які об'єктивно унеможливають проведення відповідних операцій; вчинення терористичних актів і диверсійних операцій, зокрема і кібератак на фінансову інфраструктуру; світові фінансово-економічні кризи; неефективність регулятивних, контрольних-наглядних та моніторингових заходів; соціально-політична нестабільність; пошкодження чи знищення матеріальних активів суб'єктів фінансового сектору через військові дії; втрата міжнародної підтримки; недотримання міжнародних зобов'язань; спад попиту на кредитування; неефективне нормативне регулювання небанківського фінансового ринку; неефективність та недостатня розвиненість інфраструктури ринків капіталу та організованих товарних ринків; неспроможність регулятора ефективно здійснювати свої повноваження.

1.3. Поняття та структура механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України

Маємо визнати, що основне завдання адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України об'єктивується через необхідність здійснення вкладу до механізму забезпечення її функціональності, безперервності роботи, відновлюваності, цілісності і стійкості [166] як таких характеристик, що сукупно створюють умови для її стабільного функціонування, тобто перебуття у стані безпеки. Причому головний акцент законодавця проставлено на «стійкості», яка має забезпечити її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду [166]. Висунемо припущення, що фактично йдеться про стан захищеності критичної інфраструктури, забезпечення якого залежить від спільних зусиль держави, місцевої влади, бізнесу та громадян [67]. Першочерговим в означеному є необхідність усвідомлення важливості координації дій, розподілу обов'язків та здійснення постійного інформаційного обміну між ними. Зокрема Концепцію запровадження національної системи стійкості України, ухваленої рішенням Ради національної безпеки і оборони України 20 серпня 2021 року та введеного в дію Указом Президента України №479 від 27 вересня 2021 року передбачено, що усі суб'єкти забезпечення національної стійкості постійно обмінюються необхідною інформацією, комунікують між собою у різних форматах, спільно виконують визначені завдання у межах своєї відповідальності. Також міститься норма, яка визначає, що безпека та захищеність об'єктів критичної інфраструктури є базовим елементом забезпечення її функціонування. Такий порядок речей є цілком логічним, адже згідно із Концепцією, стійкість визначається як здатність держави та суспільства вчасно виявляти загрози і вразливості, оцінювати ризики для

національної безпеки, швидко і ефективно реагувати, повністю відновлюватися після загроз, у тому числі гібридних, надзвичайних ситуацій та криз будь-якого характеру [173].

Національним планом захисту та забезпечення безпеки та стійкості критичної інфраструктури передбачено ряд заходів постійного чи строкового виконання, що мають підтримувати стан захищеності критичної інфраструктури, зокрема і у фінансовому секторі України. Тому цілком логічно, що зазначена діяльність має бути реалізована у певних нормативних рамках, забезпечених чіткою деталізацією організаційного та процедурного аспектів [26, с. 81]. За загальним правилом таке завдання репрезентується через зміст та сутність адміністративно-правового механізму [26, с. 81], в поняття якого вченими закладається різний інтерпретаційний зміст.

Причому, на нашу думку, розкриття піднятого у межах цього етапу дослідження питання унеможливлене без визначення базових термінологічних одиниць, що формують поняттєве значення категорії «механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України»

Маємо визначити, що у юридичній літературі існує багато підходів до розуміння категорії «механізм», використання якої [182, с. 70] зводиться до трьох основних значень, а саме: 1) механізм – це пристрій, що передає або перетворює рух; 2) механізм – це внутрішня будова, система чого-небудь; 3) механізм – це сукупність станів і процесів, з яких складається певне фізичне, хімічне та інше явище [28, с. 398].

Тому в юридичній науці під механізмом традиційно розуміють спосіб функціонування, систему засобів взаємодії [124, с. 244], тобто як сукупність взаємоузгоджених частин, які повинні функціонувати і передбачати певну стадійність [129, с. 263]. Наприклад, Н. Оніщенко визначає механізм як сукупність компонентів, через цілісність існування яких можна розкрити сам механізм як ціле. Умовами функціонування механізму є узгодженість і єдність його елементів. Кожен із системних елементів механізму є органічно

зумовленим усіма іншими його елементами й функціонуванням системи загалом. По-третє, «структурованість» – інша ключова категорія механізму. Структурованість являє собою можливість опису механізму як системи через установлення його структури, тобто комплексу зв'язків і відносин системи, зумовленість поведінки механізму не стільки поведінкою його окремих елементів, скільки властивостями його структури [126, с. 10–11; 150; 186].

Варто зауважити, що як предмет дослідження в юридичній науці механізм цікавив учених і активно розроблявся в 60-ті роки ХХ ст. З того часу досліджувався механізм правового регулювання, механізм дії права, механізм забезпечення прав [120, с. 47], механізм реалізації прав тощо в дискурсі їхньої правової основи, функціональності та взаємозв'язку. Зокрема вбачається, що правовий механізм як основоположна категорія щодо вище зазначених, є певною конструкцією, яка передбачає дію послідовно організованих юридичних засобів, які дають можливість досягти конкретну юридичну ціль з дотриманням відповідної процедури. Кожна ланка такого механізму є самостійним комплексом юридичних засобів [71; 129, с. 263; 207, с. 13].

У контексті приналежності цієї категорії до відомчого поля адміністративного права, вченими її зміст розкривається, як приклад, так: 1) система правових засобів, які інтегровані та організовані таким чином, що дозволяють уповноваженим суб'єктам послідовно та ефективно здійснювати діяльність за допомогою заходів організаційно-правового характеру та заходів адміністративного примусу [6, с. 7; 86, с. 41]; 2) засоби функціонування єдиної системи адміністративно-правового регулювання з метою забезпечення прав, свобод і публічних законних інтересів фізичних та юридичних осіб, функціонування громадянського суспільства і держави [1, с. 92–93]; 3) система наділених владними повноваженнями суб'єктів (органи державної влади і управління) щодо застосування правових засобів з метою правового впливу на суспільні відносини в інтересах фізичних і юридичних осіб [131, с. 145]; 4) сукупність правових і організаційних засобів

(інструментів), спрямованих [209, с. 14] на виконання конкретного завдання суб'єкта владних повноважень [25, с. 36]; 5) система адміністративно-правових засобів, які спрямовані на врегулювання суспільних відносин, що представляє собою процес, що містить визначені стадії (етапи) реалізації та елементи (складові частини) [60, с. 14]; 6) взаємопов'язана та взаємозалежна система заходів та засобів, що реалізуються органами державної влади та місцевого самоврядування, в порядку та в межах встановлених адміністративно-правовими нормами, з метою створення усіх необхідних умов для ефективного здійснення [112, с. 137] певної діяльності [25, с. 36]; 7) визначена законом сукупність взаємопов'язаних адміністративно-правових засобів, за допомогою яких здійснюється регулюючий вплив на суспільні відносини [45, с. 72]; 8) складна комплексна структурована система врегулювання відносин між органами публічного управління та суб'єктами владного впливу [70, с. 63]; 9) цілісна система правових засобів, що характеризується єдністю взаємозумовлених та взаємозалежних елементів [100, с. 99]. Доречним вбачаємо щодо цього узагальнення А. Вархова, який стверджує наступне: «як правило, адміністративно-правовий механізм визначається вченими через сукупність адміністративно-правових засобів, що визначені положеннями чинного законодавства як такі, що можуть чинити вплив на розвиток певного кола суспільних відносин. Причому вони є чинниками, що забезпечують ефективне виконання конкретної функції держави» [25, с. 36].

Висловлюючи власну думку щодо означеного можемо визначити, що без категорії «механізм» навряд чи вдасться повно та вичерпно описати взаємозв'язок між певними явищами, які сукупно репрезентують досягнення певної кінцевої мети. Для адміністративно-правової галузі наукових знань ця категорія має особливе значення, адже репрезентує діяльнісний підхід до розкриття забезпечувального, регулятивного, управлінського, охоронного чи захисного впливу держави на розвиток адміністративно-правових відносин, систематизуючи та структуруючи його вияв [227].

Щодо механізму адміністративно-правового захисту маємо вказати, що думки вчених репрезентують такі його ознаки:

– це комплексна категорія адміністративного права, що являє собою систему взаємопов'язаних самостійних складових, що сприяють захисту [13, с. 66] об'єкта охорони;

– є специфічним адміністративно-правовим комплексним утворенням, що поєднує інтереси суб'єктів адміністративного права з цінностями, що перебувають під охороною [63, с. 169];

– це сукупність адміністративно-правових засобів, що здійснюється органами державної влади, підприємствами, установами, організаціями чи посадовими особами з приводу забезпечення реалізації та відновлення прав [40, с. 68] у визначеній сфері;

– сукупність елементів, що репрезентує засоби функціонування єдиної системи адміністративно-правового регулювання [3];

– сукупність елементів, що функціонують на основі норм адміністративного права [92, с. 99];

– закріплена на нормативно-правовому рівні упорядкована сукупність взаємозалежних засобів, із використанням яких компетентні суб'єкти забезпечують стан захищеності та безперебійного функціонування об'єктів критичної інфраструктури [93; 94].

Якщо узагальнити наведений матеріал, механізмом адміністративно-правового захисту слід позначати систему об'єднаних спільним ідейним орієнтиром правових засобів (визначених правовою нормою), практичне втілення яких вимагає координації та злагодженої діяльності уповноважених виконавців певної дії захисного характеру, що має забезпечити дотримання, виконання чи реалізацію відповідної адміністративно-правової норми [227].

Таким чином, інтерпретуючи зазначений аналіз до потреб цього дослідження, маємо наступне:

– механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є сукупним терміном,

термінологічний аспект якого формується шляхом поєднання базових характерних ознак адміністративно-правових механізмів загалом та адміністративно-правового механізму захисту – зокрема;

– механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є репрезентацією практичного прояву дії охоронних та захисних заходів у цій сфері;

– механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України має власну сферу об'єктивізації – суспільні відносини, породжені необхідністю забезпечення схоронності об'єктів критичної інфраструктури фінансового сектору України;

– механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України як правове явище діяльнісного характеру має власну систему завдань, функцій та цілей;

– механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України з внутрішньо організаційного дискурсу має свій структурний склад, відмінний від тих, що встановлені для інших правових механізмів забезпечення безпеки та стійкості об'єктів критичної інфраструктури фінансового сектору України [227].

Щодо останнього варто зауважити, що за переконаннями В. Плішкіна та Ю. Кравченко структура є сукупністю зв'язків і відносин між елементами. Сам же набір елементів та їх властивості прийнято розглядати окремо [136, с. 155]. Із приводу вищенаведеної думки В. Крикун зазначає, що встановлення структури відповідного явища, в тому числі адміністративно-правового механізму захисту об'єктів критичної інфраструктури, нерозривно пов'язано із визначенням власне його структурних елементів. А тому повною мірою не можна відділяти змістовні елементи системи від її структури – дані явища взаємопов'язані й лише в сукупності обумовлюють функціонування системи як цілого. Однак не можна і підтримати позицію тих вчених, які сутність структури безпосередньо визначають через елементи системи [92, с. 101]. Зокрема вчений наводить думку Ю. Кунєва, який наголошує на тому, що

структурою є не тільки зв'язки елементів системи, але й самі елементи об'єднані зв'язками, що утворюють систему. Структура, підкреслює вчений, є сукупністю функціональних елементів системи, об'єднаних зв'язками [98, с. 87]. З розумінням означеного В. Крикун визначає, що відбувається змішування таких категорій як структура та система, оскільки сутність останньої майже збігається з першою. Більш вірно було б вказати на те, що структура відповідної системи відображає особливості її побудови, вказує як на набір елементів, так і на спосіб їх взаємозв'язку та розташування один відносно одного [92, с. 101]. З урахуванням чого більш вдалою виглядає позиція В. Грохольського, який наголошує на тому, що структурою є сукупність утворюючих систему взаємозалежних ланок, які відображають найбільш стійкі, істотні властивості системи та відносини між її елементами [43, с. 243–244].

Аналізуючи думки вчених щодо структури адміністративно-правового механізму захисту певної цінності виявляємо, наприклад, таке: «втільнення державної влади в діяльність органів держави відбувається через функціонування державно-владного механізму. Частиною останнього є адміністративно-правовий механізм. І тому, враховуючи дію принципу верховенства права, цілком доречно вести мову про те, що визначення структури адміністративно-правового механізму пов'язується зі встановленням структури механізму правового регулювання [78, с. 263–264; 149]. Існують декілька варіантів, які відображають позиції певних науковців стосовно складових елементів механізму адміністративно-правового регулювання. В цілому всі елементи можна розділити на дві групи: функціональні та органічні [101, с. 393]. Переважна більшість вчених виділяють три основних обов'язкових елементи механізму адміністративно-правового регулювання – це: адміністративно-правові норми, адміністративно-правові відносини та акти реалізації суб'єктивних прав та обов'язків [24, с. 85]» [9, с. 62].

Така наукова думка є досить поширеною, адже, наприклад, досліджуючи структуру (внутрішню будову) механізму адміністративно-правового захисту, В. Кравчук відносить до таких елементів систему різноманітних юридичних засобів, за допомогою яких здійснюється правове регулювання, тобто владний вплив на суспільні відносини [3, с. 248; 89, с. 232]; З. Гладун зараховує правові норми, юридичні факти, правовідносини, норми тлумачення права, реалізацію правових норм [39, с. 715]; С. Гончарук – систему адміністративно-правових засобів (елементів), за допомогою яких здійснюється правове регулювання (упорядкування) суспільних відносин у сфері державного управління [3, с. 248; 41, с. 23]. Як окремий елемент механізму адміністративно-правового захисту О. Красногор відносить цілі як його змістовну ознаку [13, с. 65; 90, с. 217].

Іншої думки є В. Барчук, адже вважає, що адміністративно-правовий механізм охорони лісового фонду в Україні є частиною комплексного механізму публічного адміністрування у сфері лісового господарства, що мотивувало його до висновку про необхідність розгляду його структури крізь призму ознак цільових механізмів публічного адміністрування. Він уточнює, що цільові механізми публічного адміністрування використовуються як органами державної влади, так і органами місцевого самоврядування як знаряддя для здійснення цілеспрямованих перетворень у функціонуванні або розвитку конкретних об'єктів публічного адміністрування. Частіше за все механізми цього типу трактуються як сукупність способів, методів, важелів, через які суб'єкт публічного адміністрування впливає на об'єкт чи групу об'єктів адміністрування для досягнення певної мети. При цьому кожний цільовий механізм публічного адміністрування являє собою сукупність спеціально підібраних для вирішення проблемної ситуації взаємоузгоджених методів управління, через використання яких здійснюється практичний вплив органів публічного адміністрування на соціально-економічну систему країни для забезпечення досягнення конкретної мети в обраному стратегічному напрямку [225, с. 65]. Тож інтерпретуючи зазначені

положення, вчений вважає, що структура адміністративно-правового механізму охорони лісового фонду в Україні передбачає сукупність взаємопов'язаних складових, необхідних для виконання його функцій, а до числа яких необхідно віднести: суб'єктів та об'єкти управління, принципи, а також інструменти їхньої реалізації [9, с. 65].

Більш принагідною до потреб цього дослідження є думка В. Крикуна, який зазначає, що: «В якості одного з провідних елементів адміністративно-правового механізму захисту об'єктів критичної інфраструктури слід розглядати правові норми, на рівні яких зафіксовано нормативні основи його функціонування, а також визначено правила поведінки його суб'єктів. Закріплення таких правових норм є одним із напрямків діяльності уповноважених державою суб'єктів, у межах чого відбувається правове забезпечення функціонування досліджуваного механізму. Від того, наскільки повно й якісно здійснюється таке правове забезпечення, безпосередньо залежить ефективність функціонування механізму захисту об'єктів критичної інфраструктури, а значить і захист інтересів національної безпеки взагалі» ... «Як свідчить аналіз позицій учених-правознавців, які в своїх дослідженнях вивчали проблематику функціонування відповідних правових механізмів, набір їх структурних елементів, як правило є стандартним. Мова може йти лише про певні особливості таких структурних елементів, що пов'язано зі специфікою правовідносин, у межах яких функціонує відповідний механізм. Також окремі з вчених при визначенні структури відповідного механізму можуть не включати до його складу окремі з його елементів» ... «Структура адміністративно-правового механізму захисту об'єктів критичної інфраструктури може бути представлена наступним чином: адміністративно-правові норми, на основі й на виконання яких відбувається діяльність із захисту об'єктів критичної інфраструктури; суб'єкти, відповідальні за захист об'єктів критичної інфраструктури; об'єкти критичної інфраструктури, різновид та специфіка яких обумовлюють особливості функціонування механізму їх захисту; форми та методи захисту об'єктів критичної

інфраструктури; адміністративна відповідальність за порушення законодавства в сфері захисту об'єктів критичної інфраструктури [92, с. 102, 104, 109].

З урахуванням зазначеного, найбільш обґрунтованою слід вважати точку зору тих науковців, які при дослідженні юридичних механізмів виділяють у їх структурі два взаємопов'язаних елементи: правову основу (сукупність правових засобів) та інституційний блок (структура і діяльність відповідних органів, державно-владних інститутів) [151, с. 48; 210, с. 208]. Однак нам імпонує думка, що не слід забувати й про організаційний блок. У такій інтерпретації можемо вести мову про:

1) організаційні складові – відповідають на запитання для чого потрібно реалізовувати адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України. Йдеться про мету, завдання та функції означеного механізму;

2) нормативні складові – відповідають на запитання що потрібно реалізовувати у спосіб адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. Цей блок репрезентує систему нормативних основ, які деталізують загальні та спеціальні заходи здійснення охоронного та захисного впливу на суспільні відносини, породжені необхідністю забезпечення безперебійної роботи окремих складових фінансового сектору України;

3) інституційні складові – відповідають на запитання ким потрібно реалізовувати адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України. Йдеться про систему суб'єктів, уповноважених чи залучених до цього процесу;

4) цільові складові – відповідають на запитання як здійснюється адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України. Традиційно означене включає перелік знарядь для здійснення цілеспрямованих дій. За загальним правилом знаряддям в адміністративному праві позначається інструмент реалізації повноважень

конкретних органів влади, а отже слід вести мову про форми та методи реалізації адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України [230].

Наголосимо, що таке виокремлення складових структури механізму адміністративно-правового захисту загалом не є традиційним, однак, на наш погляд, в контексті об'єктів критичної інфраструктури фінансового сектору України найбільш інформативним та доречним. Обґрунтувати зазначений тезис можемо тим, що аналіз таких складових дає чітке розуміння змісту та сутності цього механізму. Зокрема як уточнює В. Барчук, – сутністю такого механізму є його внутрішня особливість, тобто ті ознаки та характерні риси, що відмежовують даний процес від суміжних. Так з позиції філософії це щось головне, визначальне, що зумовлене глибинними зв'язками й тенденціями розвитку та пізнається на рівні теоретичного мислення [10]. Відповідно, сутність цього процесу якнайкраще розкривається через мету, завдання та його функції [9, с. 65].

Нам імпонує думка В. Оксіня, що мета як явище правової дійсності може розглядатися в кількох варіаціях. Все залежить від описуваного процесу, до якого, власне, ця категорія належить, оскільки досить часто мету плутають з цілями, цілі з функціями, а функції з завданнями певного правового процесу чи явища [123, с. 89]. Наприклад, В. Гладкий розуміє мету як прогнозований, формально описаний юридично значущий орієнтир на досягнення протягом визначеного часового проміжку певного правового стану чи статусу предметів, об'єктів або суб'єктів шляхом здійснення чи утримання від здійснення компетентних дій та використання певних інструментів [256]. Мета є заздалегідь запланованим результатом, досягнення якого є можливим за допомогою відповідних засобів і способів. Водночас завдання являють собою поняття, що відображають необхідність для суб'єкта здійснити певні дії, спрямовані на досягнення мети. Отже, мета зумовлює наявність комплексу відповідних завдань, вирішення яких дає змогу досягти поставленої мети. На взаємопов'язаність, але нетотожність понять «мета» і

«завдання» вказують і інші науковці [144, с. 109]. Зокрема, А. Кузьменко відзначає, що мета розкривається через завдання [96].

З вищезазначених положень чітко відстежується наша думка, що метою формування та реалізації механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є забезпечення їхньої схоронності у спосіб ефективно сформованої та реалізованої системи управління ризиками.

Водночас його завдання, на нашу думку, є кореляційними з тими, що встановлені законодавцем для належної реалізації державної політики у сфері захисту критичної інфраструктури загалом. Такими є: 1) запобігання проявам несанкціонованого втручання до їх функціонування, прогнозування та запобігання кризовим ситуаціям; 2) попередження кризових ситуацій, що порушують безпеку об'єктів критичної інфраструктури фінансового сектору України; 3) формування основ та відомчих рамок для діяльності уповноважених суб'єктів захисту об'єктів критичної інфраструктури фінансового сектору України; 4) розроблення нормативно-правової та нормативно-технічної бази з питань забезпечення безпеки об'єктів критичної інфраструктури фінансового сектору України; 5) розроблення та реалізація планів захисту об'єктів критичної інфраструктури фінансового сектору України; 6) розроблення та реалізація комплексу заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об'єктах критичної інфраструктури фінансового сектору України; 7) встановлення обов'язкових вимог із забезпечення безпеки об'єктів критичної інфраструктури фінансового сектору України, їх захищеності на всіх етапах життєвого циклу, у тому числі під час створення, прийняття в експлуатацію, модернізації; 8) аналіз викликів та загроз, що впливають на стійкість об'єктів критичної інфраструктури фінансового сектору України, оцінка стану її захищеності; 9) розроблення методології аналізу результативності реалізованих заходів забезпечення безпеки та захисту об'єктів критичної інфраструктури фінансового сектору України;

10) підготовка, перепідготовка, підвищення кваліфікації, тренування працівників суб'єктів здійснення захисту об'єктів критичної інфраструктури фінансового сектору України; 11) забезпечення взаємодії суб'єктів захисту об'єктів критичної інфраструктури фінансового сектору України з іншими представникам національної системи захисту критичної інфраструктури загалом, а також відповідними міжнародними системами, насамперед європейськими та євроатлантичними [166].

Щодо функцій досліджуваного механізму маємо вказати, що загалом під функцією в системному аналізі розуміється характеристика, яка визначає зміну її станів, призначення та необхідність існування певної системи [38, с. 263]. Функції системи є інтегративним результатом функціонування її компонентів. Вони виступають як форми, способи вияву активності, життєдіяльності системи та її компонентів, як форми поведінки, що сприяють збереженню компонентів і системи, як взаємозв'язок, що визначає порядок включення компонентів, частин у ціле. Функції компонентів по відношенню до системи мають доцільний характер, інакше компонент випадає із системи. Тобто це роль, яку виконує [115] система. Загальним формулюванням функцій будь-якої організаційної системи з цих позицій є перетворення ресурсів і знань на задоволення суспільних потреб [9, с. 59; 38, с. 264].

Аналіз положень Закону України «Про критичну інфраструктуру», зокрема статті 5, дозволяє визначити такі функції механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України:

1) функція комплексної безпеки, що полягає у забезпеченні фізичної безпеки та кібербезпеки об'єктів критичної інфраструктури фінансового сектору;

2) превентивна функція, яка спрямована на запобігання порушенням цілісності процесів функціонування об'єктів критичної інфраструктури фінансового сектору;

3) прогностична функція, що передбачає прогнозування й оцінку ймовірності виникнення порушень цілісності та безперебійності роботи об'єктів критичної інфраструктури фінансового сектору, а також у визначенні їх можливого впливу на їхнє функціонування.

Водночас змістом, як правило, вважається сукупність елементів, сторін, властивостей, зв'язків та тенденцій, що складають предмет, процес, явище [48, с. 246]. Тому логічно, що в контексті механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України такими елементами нами було визначено систему нормативних основ здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, суб'єктів його здійснення та інструментів реалізації.

Таким чином, маємо такі ключові висновки:

– механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України: а) є сукупним терміном, термінологічний аспект якого формується шляхом поєднання базових характерних ознак адміністративно-правових механізмів загалом та адміністративно-правового механізму захисту – зокрема; б) є репрезентацією практичного прояву дії охоронних та захисних заходів у цій сфері; в) має власну сферу об'єктивізації – суспільні відносини, породжені необхідністю забезпечення схоронності об'єктів критичної інфраструктури фінансового сектору України; г) як правове явище діяльнісного характеру має власну систему завдань, функцій та цілей; д) з внутрішньо організаційного дискурсу має свій структурний склад, відмінний від тих, що встановлені для інших правових механізмів забезпечення безпеки та стійкості об'єктів критичної інфраструктури фінансового сектору України;

– підтримуємо необхідність наукового розвитку сформованої думки, що механізм адміністративно-правового захисту загалом, у тому числі об'єктів критичної інфраструктури фінансового сектору України, у структурному контексті має декілька взаємопов'язаних складових

(організаційний, нормативний, інституційний та цільовий блоки), що сукупно забезпечують його функціональність, а також репрезентують його зміст та сутність. Зокрема організаційний блок є сутністю цього механізму, а нормативний, інституційний та цільовий, – змістом.

Висновки до Розділу 1

1. Висунуто припущення, що «критична інфраструктура фінансового сектору України» є складним словосполученням, осягнення глибини розуміння якого, з урахуванням усіх можливих контекстів та значень, доречніше здійснювати через такий науковий інструмент як «концепт», який дозволяє розширювати межі існуючого знання про те чи інше явище. Доведено, що така думка є цілком виправданою, адже концептуальний вираз його сутності пояснює специфіку об'єднаних спільним змістом самостійних категорій, що описують явище, ймовірно яке є об'єктом адміністративно-правового захисту.

2. Визначено, що семантичний аналіз правового концепту «критична інфраструктура фінансового сектору України» свідчить, що опорним елементом у цьому контексті є термін «критична інфраструктура», залежним – «фінансовий сектор». Уточнено, що перший також диференціюється на дві самостійні складові: «критична» та «інфраструктура», однак з'ясовано, що це самостійна юридична конструкція з власним термінологічним змістом.

3. Виявлено, що термін «критична інфраструктура» як такий, що має власні ідентифікаційні характеристики, за сучасних умов має два підходи до наукового осмислення його сутності. За умов першого акцентуація здійснюється на об'єктах забезпечення функціональності життєво важливих функцій щодо економіки та стабільності суспільних відносин у тому числі їхньої охорони та захисту (функціональний підхід). Другий підхід полягає у визначенні критичної інфраструктури через галузевий підхід, який

фокусується на конкретних секторах або галузях економіки, збій у діяльності яких матиме низку негативних наслідків для національної безпеки.

4. Зарубіжний досвід свідчить, що чим простішим є визначення терміну «критична інфраструктура», тим якіснішими є стратегії та підходи до її захисту. Виявлено, що з вітчизняного дискурсу Закон України «Про критичну інфраструктуру» ідентифікує її через об'єктну характеристику, а точніше – сукупність об'єктів, основне призначення яких забезпечувати безперервність реалізації процедур охорони та захисту національних інтересів України.

5. Доведено, що фінансовий сектор нормативно визначений як самостійний з переліку таких, що є важливими для життєдіяльності суспільства та держави. Зауважено, що у вітчизняному законодавстві відсутнє чітке визначення правової категорії «фінансовий сектор України».

6. Визначено, що з економічної точки зору фінансовий сектор характеризується через сукупність операцій фінансового характеру державних чи комерційних суб'єктів у вияві посередницької діяльності, яка об'єктивує розподіл фінансового капіталу в економіці. Своєю чергою, за правового дискурсу фінансовий сектор може бути розглянутим з боку наявності певних інституцій (суб'єктів правових відносин), які у спосіб дотримання встановлених правил здійснення господарської чи регулятивної діяльності забезпечують суспільний запит на надання якісних фінансових послуг та пов'язаних з ними операцій.

7. З'ясовано, що у контексті критичної інфраструктури фінансового сектору йдеться про два різновиди об'єктів захисту у його межах: 1) ті, що визначаються Національним банком; 2) ті, що визначаються Міністерством фінансів України.

8. Узагальнено, що правовий концепт «критична інфраструктура фінансового сектору України» позначає коло суспільних відносин виникнення яких обумовлено необхідністю забезпечення безперебійного функціонування окремих складових фінансового сектору, які є критично

важливими в аспекті спроможності держави обслуговувати свої потреби і розвиватись у руслі автономності та самодостатності, а також утвердження як правової, демократичної, суверенної держави, яка належним чином виконує своє соціальне призначення з дискурсу гарантування кожному непорушності його прав та законних інтересів. Висунуто припущення, що така інтерпретація не зумовлює виникнення сумнівів чи дискусій щодо того, що держава має створити усі необхідні умови задля того, щоб усі критично важливі складові фінансового сектору перебували у стані захисту, тобто були забезпеченими можливістю здійснення адекватної, належної, допустимої, необхідної та ефективної реакції на фактори, чинники, обставини, події тощо, які потенційно чи реально здатні або завдають негативного впливу на функціональність їхньої роботи.

9. Звернено увагу на проблематику диференціації категорій «охорона» та «захист». З'ясовано, що європейські стандарти у сфері ідентифікації і визначення критичних інфраструктур використовують їх у якості єдиного поняття. При більш поглибленому аналізі з'ясовано, що охорона передбачає застосування превентивних заходів та використання методу переконання, щоб уникнути порушень встановлених правил. Натомість захист більш орієнтований на реагування вже наявних порушень із застосуванням примусових методів, але водночас існує певна взаємопов'язаність між охоронними та захисними заходами. Однак не спростовується думка щодо того, що захист можна тлумачити ширше, зокрема і з позиції, запропонованої законодавцем у межах положень Закону України «Про критичну інфраструктуру». Йдеться про включення охорони до системи захисту, що загалом не є помилковим, адже досліджувана сфера характеризується наявністю національної системи захисту критичної інфраструктури (у інституційному аспекті), яка цілком об'єктивно в змозі поєднувати реалізацію як превентивних заходів, так і реагування на факти відхилення від норми.

10. Щодо сутності адміністративно-правового захисту уточнюється, що вчені досить чітко і правильно зазначають про сукупність правовідносин, які підлягають захисту через встановлену нормативну вказівку на це і розроблений процедурний аспект здійснення відповідних заходів нормами адміністративного права, але дизоб'єктивізуючи цю категорію припускаються помилки автоматичного розкриття її сутності через правовідносини, що пов'язані з правами людини та громадянина, які хоч і є основним, однак не єдиним об'єктом протиправного посягання. Зокрема доцільніше вести мову про охоронювані законом цінності та інтереси, які можуть належати як конкретній особі, так і їх групі чи державі загалом. Тобто є два основних об'єкти протиправного посягання – одиничний чи публічний охоронюваних законом інтерес (цінність, благо).

11. Доведено, що адміністративно-правовий захист, як і адміністративно-правова охорона чи адміністративно-правове забезпечення, логічніше розглядати з позиції самостійних врегулівних процесів, що мають різні завдання та механізми реалізації. Узагальнено та схематично їхнє співвідношення можна представити так: забезпечення спрямовується на охорону та захист, а охорона та захист – реалізуються у тісній взаємодії. Причому саме визначення адміністративно-правового захисту має розглядатись з дуальної інтерпретації об'єктної складової. Мається на увазі, що окрім юридичного відношення особи до конкретного інтересу (як правило, права на щось) має враховуватись його безпосередній стан з позиції убезпечення від зміни властивостей чи характеристик, руйнування або загалом знищення.

12. Визначено, що адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України є системою заходів охоронного та захисного спрямування, реалізованих уповноваженими суб'єктами національної системи захисту критичної інфраструктури задля забезпечення стійкості та безпеки сегментів ринку фінансових послуг та окремих

фінансових операцій, що формують фінансовий сектор критичної інфраструктури України.

13. Сутність адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України схарактеризована через його ключові ознаки, зокрема: а) є складовою механізму забезпечення національної безпеки; б) виникає у відповідь на необхідність захисту критично важливих фінансових операцій та адміністративних дій, порушення яких завдає шкоди економіці та взаємодіям, залежним від стабільного функціонування грошових потоків та фінансово-адміністративних функцій державних органів; в) реалізується на основі наявності законодавчого та відомчого нормативно-правового забезпечення; г) має комплексний характер, що об'єктивує можливість (при необхідності) без зміни інституційної чи процедурної складової його здійснення виникнення перехідної трансформації вчинюваних дій з суто охоронних до безпосередньо захисних; д) як сукупність відповідних заходів є репрезентацією існування у правореалізаційній площині спеціалізованої діяльності, що має власну мету, завдання та функції; е) є безперервним процесом, інтенсивність якого (активність, готовність) залежить від стану внутрішнього та зовнішнього безпекового середовища.

14. Уточнюється, що безпека та стійкість за загальним контекстом перебувають у кореляційному взаємозв'язку. Стійкість є невід'ємною складовою безпеки, що досягається шляхом забезпечення можливості для конкретної системи ефективно реагувати на загрози та ризики. Констатується, що загрози та ризики можна розглядати з різних боків та з різним інтерпретаційним контекстом. Чинне законодавство у досліджуваній сфері не надає вичерпного визначення означених термінів, чим, власне, зумовлює виникнення актуальних наукових дискусій.

15. У контексті визначення співвідношення між категоріями «загроза» та «ризик» стверджується, що вони пов'язані з явищем «небезпеки», тобто за властивість мають настання негативних наслідків у випадку активації

механізмів їх реалізації в практичну площину. Визначається, що: 1) загроза є більш статичним явищем, тоді як ризик характеризується оціночним припущенням про негативний вплив в перспективі; 2) ризик як оціночне явище є комбінацією ймовірностей, тоді як загроза може бути реальною та потенційною; 3) ризик за загальним контекстом має якісні і кількісні показники, а загроза існує незалежно від того, реалізована вона чи ні. Аналізуючи положення Закону України «Про критичну інфраструктуру», зокрема пункт 4 частини 2 статті 4 формується висновок, що загроза у цьому контексті є основним явищем на мінімізацію наслідків якої спрямовуються дії уповноважених суб'єктів. Водночас ризик визначається як імовірність виникнення цих загроз (зрозуміло, що ризик має свої негативні наслідки, зокрема у цьому контексті у вияві загроз), протидія яким є першим кроком для забезпечення систем від негативного впливу неконтрольованих процесів різного характеру.

16. Запропоновано загрози для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України диференціювати на два різновиди: універсальні, тобто такі, що можуть або спричиняють негативні наслідки для більшості або навіть для усіх об'єктів критичної інфраструктури в Україні та індивідуальні, сутність яких зведено до виключно досліджуваної сфери.

17. Серед основних універсальних загроз, які є актуальними для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України виокремлено: а) технічні збої або інші невідворотні обставини, які об'єктивно унеможливили проведення відповідних операцій; б) вчинення терористичних актів і диверсійних операцій; в) світові фінансово-економічні кризи; г) не ефективність регулятивних, контрольних, наглядових та моніторингових заходів; д) соціально-політична нестабільність; е) пошкодження чи знищення матеріальних активів суб'єктів фінансового сектору через воєнні дії.

18. Індивідуальними загрозами для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України названо: а) спад економічної активності; б) інфляційні процеси; в) втрата міжнародної підтримки; г) відсутність стратегічного бачення та плановірності здійснення реформаційних змін; д) недотримання міжнародних зобов'язань; е) втрата прибутковості банків; ж) спад попиту на кредитування; з) втрата спроможностей системи гарантування вкладів; и) неефективне нормативне регулювання небанківського фінансового ринку; к) втрата банками ліквідності; л) неефективність та недостатня розвиненість інфраструктури ринків капіталу та організованих товарних ринків; м) відсутність доступності фінансових послуг; н) неспроможність регулятора ефективно здійснювати свої повноваження.

19. Окремо визначається доцільність виокремлення системних ризиків фінансового сектору, визначення та відстеження рівня інтенсивності яких є сферою відповідальності Ради з фінансової стабільності.

20. Узагальнено, що без адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України навряд чи вдасться забезпечити належний рівень безпеки та стабільності ринку фінансових послуг та пов'язаних з ними операцій в Україні, адже ризики та загрози є постійними, різноманітними, а недостатня увага та реагування на них можуть мати катастрофічні наслідки. Сформовано висновок, що ризики мають два різновиди: ті, що пов'язані із виникненням загроз (неврахування ризику веде до загрози); ті, що існують паралельно з ймовірністю виникнення загроз (самостійні ризики, що наявними є постійно). Причому другий контекст є значно ширшим. Більшою мірою саме про нього йдеться у нормах чинного законодавства. Натомість загрозою, за таким баченням, є фізичний прояв небезпеки від наявності (виникнення) певного явища. З точки зору наукового суб'єктивізму визначається, що ризик має бути пов'язаним із загрозою, точніше зумовлювати наявність останніх.

21. З'ясовано, що стан захищеності критичної інфраструктури вітчизняного фінансового сектору залежить від ефективності процедур комунікації між державою, місцевою владою, бізнесом та громадянами, чіткості розподілу їхніх обов'язків, що підтриманий системою координаційних відносин, а також постійного інформаційного обміну між ними.

22. Констатується, що ряд заходів щодо підтримки стану захищеності критичної інфраструктури вітчизняного фінансового сектору формує зміст та сутність відповідного адміністративно-правового механізму, який має забезпечити їхню реалізацію нормативним та організаційним контекстом.

23. У межах визначення базових термінологічних одиниць, що формують поняттєве значення категорії «механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України», обґрунтовується думка, що без категорії «механізм» навряд чи вдасться повно та вичерпно описати взаємозв'язок між певними явищами, які сукупно репрезентують досягнення певної кінцевої мети. Для адміністративно-правової галузі наукових знань ця категорія має особливе значення, адже репрезентує діяльнісний підхід до розкриття забезпечувального, регулятивного, управлінського, охоронного чи захисного впливу держави на розвиток адміністративно-правових відносин, систематизуючи та структуруючи його вияв.

24. Визначено, що механізмом адміністративно-правового захисту слід позначати систему об'єднаних спільним ідейним орієнтиром правових засобів (визначених правовою нормою), практичне втілення яких вимагає координації та злагодженої діяльності уповноважених виконавців певної дії захисного характеру, що має забезпечити дотримання, виконання чи реалізацію відповідної адміністративно-правової норми.

25. Доведено, що механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України: а) є сукупним терміном, термінологічний аспект якого формується шляхом поєднання

базових характерних ознак адміністративно-правових механізмів загалом та адміністративно-правового механізму захисту – зокрема; б) є репрезентацією практичного прояву дії охоронних та захисних заходів у цій сфері; в) має власну сферу об'єктивізації – суспільні відносини, породжені необхідністю забезпечення схоронності об'єктів критичної інфраструктури фінансового сектору України; г) як правове явище діяльнісного характеру має власну систему завдань, функцій та цілей; д) з внутрішньо організаційного дискурсу має свій структурний склад, відмінний від тих, що встановлені для інших правових механізмів забезпечення безпеки та стійкості об'єктів критичної інфраструктури фінансового сектору України.

26. Підтримано необхідність наукового розвитку сформованої думки, що механізм адміністративно-правового захисту загалом, у тому числі об'єктів критичної інфраструктури фінансового сектору України, у структурному контексті має декілька взаємопов'язаних складових, що сукупно забезпечують його функціональність. Обґрунтовано, що такими є: а) організаційні складові – відповідають на запитання для чого потрібно реалізовувати адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України. Йдеться про мету, завдання та функції означеного механізму; б) нормативні складові – відповідають на запитання що потрібно реалізовувати у спосіб адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. Цей блок репрезентує систему нормативних основ, які деталізують загальні та спеціальні заходи здійснення охоронного та захисного впливу на суспільні відносини, породжені необхідністю забезпечення безперебійної роботи окремих складових фінансового сектору України; в) інституційні складові – відповідають на запитання ким потрібно реалізовувати адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України. Йдеться про систему суб'єктів, уповноважених чи залучених до цього процесу; г) цільові складові – відповідають на запитання як здійснюється адміністративно-правовий захист об'єктів критичної

інфраструктури фінансового сектору України. Традиційно означене включає перелік знарядь для здійснення цілеспрямованих дій. За загальним правилом знаряддям в адміністративному праві позначається інструмент реалізації повноважень конкретних органів влади, а отже слід вести мову про форми та методи реалізації адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України.

27. Констатується, що сформована система структурного складу механізму адміністративно-правового захисту загалом не є традиційною, адже у більш узагальненому вигляді вона репрезентується через практико-реалізаційні та нормативно-правові складові. Однак зауважено, що авторське виокремлення таких складових в контексті об'єктів критичної інфраструктури фінансового сектору України вбачається більш інформативним та доречним.

28. Визначено мету, завдання та функції механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України з узагальненням, що це сутнісна сторона цього механізму. Констатується, що метою формування та реалізації механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є забезпечення їхньої схоронності у спосіб ефективно сформованої та реалізованої системи управління ризиками. Водночас його завдання розкрито через кореляційний взаємозв'язок з тими, що встановлені законодавцем для належної реалізації державної політики у сфері захисту критичної інфраструктури загалом. Щодо функцій цього механізму, ними названо такі які основні з них як: 1) функція комплексної безпеки, що полягає у забезпеченні фізичної безпеки та кібербезпеки об'єктів критичної інфраструктури фінансового сектору; 2) превентивна функція, яка спрямована на запобігання порушенням цілісності процесів функціонування об'єктів критичної інфраструктури фінансового сектору; 3) прогностична функція, що передбачає прогнозування й оцінку ймовірності виникнення порушень цілісності та безперебійності роботи об'єктів критичної

інфраструктури фінансового сектору, а також у визначенні їх можливого впливу на їхнє функціонування.

29. Обґрунтовується, що система нормативних основ здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, суб'єкти його здійснення та інструменти реалізації формують зміст механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України.

РОЗДІЛ 2

ХАРАКТЕРИСТИКА ОКРЕМИХ ЕЛЕМЕНТІВ МЕХАНІЗМУ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО СЕКТОРУ УКРАЇНИ

2.1. Нормативно-правові основи захисту об'єктів критичної інфраструктури фінансового сектору України

«Нормативно-правові засади», «нормативно-правові основи» «правовий базис», – ключові базові категорії, якими позначають організаційне та практико-реалізаційне підґрунтя діяльності будь-якого органу публічної влади, функціонування певного правового явища чи процесу [116, с. 161]. Причому вченими акцентується на їх синонімічності [233, с. 134]. Зазначену думку підтримує вчена В. Боняк, яка здійснивши аналіз інтерпретацій слів «засади» та «основи» стверджує, що схожий зміст цих понять дозволяє вважати їх взаємозамінними та такими, що належать до одного поняттєвого ряду[20, с. 74].

За загальним правилом йдеться про нормативно-правове поле для здійснення чи утримання від певної дії, що є результатом здійснення нормативно-правового забезпечення розвитку певного кола суспільних відносин. Тому без додаткової аргументації вбачаємо, що нормативно-правовими основами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є сукупність правових документів різної юридичної сили, виданих (прийнятих) з метою врегулювання питань: а) кіберзахисту, інформаційної безпеки, інституційної збалансованості цієї сфери загалом; б) реалізації міжвідомчих механізмів взаємодії між регуляторами та іншими суб'єктами національної системи її захисту; в) управління та моніторингу ризиків, пов'язаних із фінансовими операціями та діяльністю установ, які входять до переліку об'єктів критичної

інфраструктури; г) контрольно-наглядової діяльності у цій сфері, включаючи імплементацію міжнародних стандартів та рекомендацій.

Умовно означену систему можна класифікувати на міжнародні, регіональні та національні регуляторні або рекомендаційні акти.

У контексті міжнародних актів особливої уваги заслуговують Базельські принципи (Базель I, II, III), які встановлюють стандарти для регулювання, нагляду та управління ризиками в банківському секторі. Ці принципи допомагають зміцнити фінансову стабільність та зменшити ризики, пов'язані з банківською діяльністю. Вперше вони були опубліковані Базельським комітетом з банківського нагляду в 1997 році та використовуються різними країнами як орієнтири для оцінки якості їхніх наглядових систем та для визначення майбутніх заходів, спрямованих на досягнення базового рівня надійної наглядової практики. Основні принципи також використовуються Міжнародним валютним фондом та Світовим банком в контексті Програми оцінки фінансового сектору («FSAP») для оцінки ефективності систем і практики банківського нагляду в різних країнах. Наразі ці принципи поділяються на дві групи: перша група (від 1 по 13 принцип) зосереджується на повноваженнях, обов'язках та функціях органів нагляду, а друга (від 14 по 29 принцип) – на пруденційному регулюванні та вимогах до банків [130].

Щодо Міжнародного валютного фонду та Світового банку слід зауважити, що окрім оцінки фінансового сектору вони також видають значну частку міжнародних рекомендацій. До числа таких можна віднести, наприклад, Глобальний звіт про фінансову стабільність Міжнародного валютного фонду (квітень 2024 року), який містить перелік рекомендацій щодо поліпшення політик забезпечення стійкості фінансового сектору або ж технічний огляд Світового банку щодо «стійкості інфраструктури, державно-приватного партнерства: політика, контракти та фінанси», де висвітлюються уроки та рекомендації з порівняльних тематичних досліджень в Індії, Японії та Кенії, щоб допомогти інформувати уряди, які мають намір запровадити

підхід управління ризиками стихійних лих у розвиток інфраструктури та державно-приватного партнерства, зокрема [280].

Також доречно вказати й про Рекомендації та Керівництва Групи з розробки фінансових заходів боротьби з відмиванням грошей («FATF»), які включають заходи для захисту фінансових інституцій від використання їх інфраструктури в злочинних цілях. Рекомендації «FATF» також часто називають Стандартами «FATF». Вони включають самі рекомендації та пояснювальні примітки разом із відповідними визначеннями в глосарії. Оскільки країни мають різноманітні правові, адміністративні та операційні рамки та різні фінансові системи, вони повинні адаптувати впровадження рекомендацій до своїх конкретних обставин [246]. Наприклад, в Декларації міністрів Групи розробки фінансових заходів від 18 квітня 2024 зазначено, що необхідно зосередитися на нових ризиках для глобальної фінансової системи, включаючи зростаючі загрози, пов'язані з транснаціональним кібершахрайством, торгівлею синтетичними опіоїдами, зловживанням віртуальними активами, ризиками, пов'язаними з програмами-вимагачами та зловживанням платформами краудфінансування для фінансування тероризму та потенційне зловживання предметами мистецтва і старовиною як інструментами для відмивання грошей і фінансування тероризму [281]. Зауважимо, що у співпраці з іншими міжнародними партнерами, «FATF» веде роботу з виявлення вразливостей на національному рівні з метою захисту міжнародної фінансової системи від зловживань [44]. Щодо керівництв, виданих цією організацією, варто виділити: 1) «Керівництво FATF із застосування суб'єктами державного фінансового моніторингу ризикоорієнтованого нагляду», ціль якого полягає в чіткому визначенні та поясненні того, як наглядові органи повинні застосовувати ризикорієнтований підхід у своїй діяльності відповідно до Стандартів FATF. На додаток до пояснень щодо очікувань загалом, Керівництво також скеровано на майбутнє, у ньому окреслено інноваційні практики, які зможуть допомогти підвищити ефективність нагляду за протидією відмиванню коштів

/ фінансуванню тероризму і в такий спосіб удосконалити всю систему протидії відмиванню коштів / фінансуванню тероризму [76]; 2) «Керівництво FATF щодо бенефіціарної власності юридичних осіб», аудиторією якого є, перш за все, ті, хто розробляють політики та практики в національних органах влади, а також зацікавлені сторони приватного сектору, такі як фінансові установи, визначені нефінансові установи та професії та компанії, які зобов'язані відповідати національним вимогам з протидії відмиванню коштів / фінансуванню тероризму, що засновані на стандартах «FATF». Мета цього керівництва – допомогти розробникам політик та практик визначити, розробити та реалізувати відповідні заходи щодо запобігання неправомірному використанню юридичних осіб відповідно до стандартів «FATF» [11].

Важливим є також, наприклад, Стандарт з управління інформаційною безпекою ISO/IEC 27001 [259], розроблений Міжнародною організацією з стандартизації («ISO»), адже забезпечує захист інформаційних активів фінансових установ. Цей Стандарт просуває цілісний підхід до інформаційної безпеки, який включає перевірку як людей, так і політик та технологій. Система управління інформаційною безпекою, впроваджена відповідно до цього стандарту, є інструментом управління ризиками, забезпечення кіберстійкості та оптимізації бізнес-процесів взагалі та у фінансовому секторі – зокрема. Інший документ «ISO» – Стандарт з управління ризиками 31000 [258]. Він допомагає фінансовим установам ідентифікувати та керувати ризиками. Його застосування допомагає більш ефективно виявляти загрози, а також більш ефективно розподіляти та застосувати ресурси під час моніторингу ризиків.

З усім тим варто зауважити й на тому, що під головуванням Міністра закордонних справ України П. Клімкіна Рада Безпеки ООН 13 лютого 2017 року одностайно ухвалила першу в історії резолюцію S/RES/2341 щодо захисту критичної інфраструктури від терористичних загроз, ініціатором якої виступила Україна. Співавторами документа стали 47 держав [121]. У ній

наголошувалося на необхідності комплексного підходу до захисту об'єктів критичної інфраструктури з використанням секторального підходу, який характеризується використанням таких інструментів як: планування, обмін розвіданими, оперативна координація, скринінг, кіберзахист тощо.

Європейський Союз також прийняв низку директив та рекомендацій, що прямо чи побічно стосуються досліджуваних питань. Зокрема можна вести мову про попередньо згадані нами такі акти як: Директива 2006/48/ЄС (про започаткування та здійснення діяльності кредитних установ), Директива 2006/49/ЄС (про достатність основного капіталу інвестиційних компаній та кредитних установ), Директива 2008/114 (про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту), Директива 2009/138/ЄС (про започаткування та ведення діяльності у сфері страхування та перестраховання).

Зазначимо, що 17 листопада 2005 року Європейська Комісія ухвалила Зелену книгу з питань європейської програми охорони та захисту критичних інфраструктур, що визначала кілька варіантів політики щодо створення програми попередження, підготованості та реагування на терористичні акти, пов'язані з критичними інфраструктурами та Інформаційної мережі попередження щодо загроз критичній інфраструктурі. У квітні 2007 року Рада схвалила висновки щодо Європейської програми захисту критичної інфраструктури («ERCIP»), нагадуючи, що держави-члени несуть цілковиту відповідальність за управління механізмами охорони та захисту критичних інфраструктур в межах національних кордонів, вітаючи зусилля Комісії з розроблення європейської процедури ідентифікації та визначення європейських критичних інфраструктур, а також оцінювання необхідності покращення їх охорони та захисту. Зокрема Директива 2008/114 стала першим кроком поступового підходу до ідентифікації і визначення європейських критичних інфраструктур, а також оцінювання необхідності покращення їх охорони та захисту. Фактично, ця Директива робить основний

акцент на енергетичному і транспортному секторах, та вимагає перегляду для оцінки її впливу і необхідності додати до сфери її застосування інші сектори, між іншим, сектор інформаційно-комунікаційних технологій [58].

Вартою уваги є також Директива ЄС 2016/1148 (NIS Directive), яка встановила заходи для забезпечення високого рівня безпеки мереж та інформаційних систем у Європейському Союзі. Передбачається, що операційний ризик є важливою частиною пруденційного регулювання та нагляду у банківському секторі та секторі інфраструктур фінансового ринку. Він охоплює всі операції, у тому числі безпеку, цілісність та стійкість мережевих та інформаційних систем. Вимоги відносно таких систем, які часто перевищують вимоги, передбачені в цій Директиві, викладені у низці правових актів Союзу, у тому числі: правилах щодо доступу до діяльності кредитних установ та пруденційного нагляду за кредитними установами та інвестиційними компаніями, та правилах щодо пруденційних вимог до кредитних установ та інвестиційних компаній, котрі включають вимоги відносно операційного ризику; правилах щодо ринків фінансових інструментів, котрі включають вимоги стосовно оцінювання ризику для інвестиційних компаній та регульованих ринків; правилах щодо позабіржових похідних фінансових інструментів, центральних контрагентів та реєстрів трансакцій, що включають вимоги відносно операційного ризику для центральних контрагентів та реєстрів трансакцій; правилах щодо вдосконалення розрахунків за цінними паперами у Союзі та щодо центральних депозитаріїв цінних паперів, котрі включають вимоги відносно операційного ризику. Крім того, вимоги до повідомлення про інциденти входять до звичайної наглядової практики у фінансовому секторі та часто містяться у посібниках з нагляду [54].

Попри те, що безпека інформаційно-комунікаційних технологій і цифрова стійкість є частиною операційного ризику, вони були меншою мірою в центрі регуляторної програми після фінансової кризи та розвивалися лише в деяких сферах політики ЄС щодо фінансових послуг та регуляторний

ландшафт, або лише в кількох державах-членах. У своєму Повідомленні від 8 березня 2018 року під назвою «План дій у сфері фінансових технологій: для більш конкурентоспроможного та інноваційного європейського фінансового сектору» Комісія наголосила на першорядній важливості зробити фінансовий сектор Союзу більш стійким, у тому числі з операційної точки зору, щоб забезпечити його технологічну безпеку та належне функціонування, його швидке відновлення після порушень інформаційно-комунікаційних технологій та інцидентів, що в кінцевому підсумку забезпечує ефективне та безперебійне надання фінансових послуг у всьому Союзі, у тому числі в ситуаціях стресу, зберігаючи при цьому довіру та впевненість споживачів і ринку [275].

У цьому контексті варто зауважити на значенні Регламенту ЄС 2021/23, що є відповідним правовим актом, який є доповнення та об'єктивізацією розвитку підходу, встановленого Регламентом (ЄС) № 648/2012 (передбачає єдині пруденційні вимоги, що застосовуються до центральних контрагентів). Його положення визначають, що основними цілями врегулювання має бути забезпечення безперервності критичних функцій, уникнення негативного впливу на фінансову стабільність та захист державних коштів [276].

Водночас Директива Європейського Парламенту і Ради (ЄС) 2015/849 (⁴) є основним правовим інструментом запобігання використанню фінансової системи Союзу для цілей відмивання грошей та фінансування тероризму. Зазначена Директива, кінцевим строком транспозиції якої було 26 червня 2017 року, визначає ефективну та всеосяжні правові рамки для вирішення проблеми зі стягненням грошей чи майна, пов'язаних з терористичними цілями, вимагаючи від держав-членів визначити, зрозуміти та зменшити ризики, пов'язані з відмиванням грошей та фінансуванням тероризму. Директивою Ради ЄС 2018/843 до неї були внесені відповідні зміни для того, щоб досягнення її цілей мало належний розвиток [55].

З усім тим, основоположною в досліджуваному контексті слід вбачати й Директиву Ради ЄС 2022/2557, а також Рекомендації Ради ЄС 2023/С 20/01. Зокрема Директивою встановлено рамки для підвищення стійкості критично важливих суб'єктів внутрішнього ринку шляхом встановлення узгоджених мінімальних правил та вимог до надання їм допомоги у спосіб узгоджених і цілеспрямованих заходів підтримки та нагляду. Ця Директива зосереджена виключно на захисті європейської критичної інфраструктури та скасовує Директиву Ради 2008/114/ЄС, адже необхідно було змінити підхід до забезпечення кращого обліку ризиків, кращого визначення та узгодженості ролі та обов'язків критично важливих суб'єктів як постачальників послуг, необхідних для функціонування внутрішнього ринку, а також прийняття правил Союзу для підвищення стійкості критичних об'єктів. Основна ідея в тому, що критично важливі суб'єкти повинні бути в змозі посилити свою здатність запобігати, захищати, реагувати, протистояти, пом'якшувати, поглинати, пристосовуватись і відновлюватись після інцидентів, які потенційно можуть порушити надання основних послуг [244]. Важливо, що Європейська комісія визнала різноманітні недоліки початкової Директиви 2008/114/ЄС. Одним із прикладів був той факт, що директива 2008 року включала лише два сектори: енергетика і транспорт. Тепер таких секторів одинадцять, включаючи банківську справу та інфраструктуру фінансового ринку [245].

Своєю чергою, Рекомендації Ради ЄС 2023/С 20/01 акцентує на необхідності підвищення стійкості критичної інфраструктури з урахуванням відповідних ризиків, особливо ефектів каскаду, порушення ланцюга постачання, залежності, наслідків зміни клімату, ненадійних постачальників і партнерів, а також гібридних загроз і кампаній, включаючи маніпулювання іноземною інформацією та втручання. Передбачається, що держави-члени повинні, відповідно до законодавства Союзу та національного законодавства, використовувати всі доступні інструменти для просування вперед і сприяння посиленню фізичної та кібернетостійкості критичної інфраструктури [241].

Маємо констатувати, що ці європейські, а також низка інших міжнародних документів забезпечують комплексний підхід до захисту критичної інфраструктури фінансового сектору, включаючи регулювання, управління ризиками, інформаційну безпеку та заходи протидії злочинній діяльності. Вони встановлюють стандарти, які сприяють зміцненню стабільності та стійкості фінансових систем у глобальному масштабі.

У контексті національного рівня, на нашу думку, нормативно-правові основи захисту об'єктів критичної інфраструктури фінансового сектору України об'єктивуються через законодавство у сферах сталого розвитку, національної безпеки та її складових, захисту критичної інфраструктури, регулювання ринку фінансових послуг, бюджетного регулювання, економічного розвитку та протидії фінансуванню злочинів.

Однак варто зауважити, що Національний інститут стратегічних досліджень із залученням українських та зарубіжних експертів і за підтримки Офісу зв'язку НАТО в Україні, на основі вивчення досвіду країн-членів ЄС та НАТО з врахуванням безпекової ситуації в Україні та особливостей розбудови елементів сектору безпеки країни у 2015 році підготували Зелену книгу. В ній сформульовані першочергові кроки із побудови державної системи захисту критичної інфраструктури в Україні [16]. Загалом Зелена книга з питань захисту критичної інфраструктури в Україні є документом, спрямованим на формування систематичного підходу до захисту критичної інфраструктури країни загалом та фінансового сектору – зокрема. Документ розроблений з метою окреслення основних проблем, викликів та підходів до захисту критичної інфраструктури в умовах сучасних загроз та ризиків, включаючи терористичні акти, природні катастрофи, техногенні аварії та інші небезпеки. Він також наголошує на кількох важливих аспектах: 1) мультидисциплінарний підхід, – захист об'єктів критичної інфраструктури потребує інтеграції знань та досвіду з різних галузей, включаючи безпеку, інженерію, економіку та інформаційні технології; 2) превентивні заходи, – важливість запобігання загрозам через вчасне виявлення вразливостей та їх

усунення; 3) освіта та підготовка, – необхідність постійного навчання та підвищення кваліфікації фахівців, що займаються захистом об'єктів критичної інфраструктури.

Отже, Зелена книга з питань захисту критичної інфраструктури в Україні є важливим стратегічним документом, який задає напрямки розвитку системи захисту критичної інфраструктури, зокрема і фінансового сектору. Однак слід враховувати, що підготовка та публікація «зелених книг» є поширеною практикою стимулювання і організації професійних дискусій щодо актуальних безпекових проблем і шляхів їх вирішення як на національному, так й на міжнародному рівнях, проте її текст не є офіційним. Як правило видання «зеленої книги» з певної проблематики передує наступному етапу – розробці та виданню офіційного документа, де формулюються основи державної політики, спрямованої на розв'язання окресленої проблеми [16]. Тому повертаючись до теми законодавства, що формує нормативно-правові основи захисту об'єктів критичної інфраструктури фінансового сектору України, маємо вказати, що основними актами з таких є:

1) Укази Президента України «Про Стратегію сталого розвитку «Україна - 2020»» від 12 січня 2015 року № 5/2015; «Про Цілі сталого розвитку України на період до 2030 року» 30 вересня 2019 року № 722/2019; розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року» від 10 липня 2019 року № 526-р; постанова Кабінету Міністрів України «Про затвердження Державної стратегії регіонального розвитку на 2021-2027 роки» від 5 серпня 2020 року № 695. Варто зауважити, що у грудні 2020 року Кабінет Міністрів України вніс зміни до Регламенту Кабінету Міністрів України, затвердженого постановою Кабінету Міністрів України від 18 липня 2007 року № 950, яким відтепер встановлено, що необхідність досягнення Цілей сталого розвитку враховується у процесі формування та реалізації державної політики України. Таким чином на державному рівні Цілі сталого

розвитку закріплено у якості орієнтирів для розроблення програмних та прогнозних документів [222];

2) Закони України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», «Про правовий режим воєнного стану»; Укази Президента України «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»» від 14 вересня 2020 року № 392/2020; «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості»» від 27 вересня 2021 року № 479/2021; «Про рішення Ради національної безпеки і оборони України від 11 серпня 2021 року «Про Стратегію економічної безпеки України на період до 2025 року»» від 11 серпня 2021 року № 347/2021; розпорядження Кабінету Міністрів України «Про затвердження плану заходів з реалізації Концепції забезпечення національної системи стійкості до 2025 року» від 10 листопада 2023 року № 1025-р тощо;

3) Закон України «Про критичну інфраструктуру», «Про захист інформації в інформаційно-телекомунікаційних системах»; постанови Кабінету Міністрів України «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» від 3 вересня 2014 року № 411; «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 року № 518; «Деякі питання об'єктів критичної інфраструктури» від 9 жовтня 2020 року № 1109; «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури» від 14 жовтня 2022 року № 1174; «Про затвердження Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього» від 28 квітня 2023 року № 415; «Про затвердження Порядку та критеріїв визначення підприємств, установ і організацій, які є критично важливими для функціонування економіки та забезпечення життєдіяльності населення в

особливий період» від 27 січня 2023 року № 76; розпорядження Кабінету Міністрів України «Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури» від 19 вересня 2023 року № 825-р; Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури» від 15 січня 2021 року № 23; національні стандарти України з питань інформаційної безпеки ДСТУ ISO/IEC 27000:2015 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник»; ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»; ДСТУ ISO/IEC 27002:2015 «Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки», які прийняті наказом Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» від 18 грудня 2015 року № 193 [159] тощо;

4) Закони України «Про банки і банківську діяльність», «Про платіжні послуги», «Про фінансові послуги та фінансові компанії», «Про Національний банк України», постанови Кабінету Міністрів України «Про затвердження Положення про Міністерство фінансів України» від 20 серпня 2014 року № 375; «Про затвердження Методики оцінювання фіскальних ризиків» від 24 квітня 2019 року №351; «Про затвердження Методики оцінювання фіскальних ризиків, пов'язаних з діяльністю суб'єктів господарювання державного сектору економіки» від 11 січня 2018 року № 7; «Про затвердження Національної економічної стратегії на період до 2030 року» від 3 березня 2021 року № 179; рішення Правління Національного банку України «Про затвердження Стратегії розвитку фінансового сектору України до 2025 року» від 29 серпня 2023 року № 299-рш; розпорядження Кабінету Міністрів України «Про схвалення Стратегії реформування системи

управління державними фінансами на 2022–2025 роки та плану заходів з її реалізації» від 29 грудня 2021 року № 1805-р та багато інших.

З системи таких актів нами прийнято рішення виокремити в окрему групу ті, що є функціональними, тобто мають безпосереднє відношення до досліджуваної сфери. Насамперед йдеться про акти секторальних органів. Маємо констатувати, що Національний банк України визначив, наприклад:

– критерії віднесення об'єктів банківської системи до критичної інфраструктури (Постанова Правління Національного банку України «Про затвердження Положення про визначення об'єктів критичної інфраструктури в банківській системі України» від 30 листопада 2020 року №151). Так, до об'єктів критичної інфраструктури в банківській системі України належать банки, стає функціонування яких забезпечує стабільність банківської системи, має суттєве значення для економіки та безпеки держави, функціонування суспільства, та які становлять значний суспільний інтерес. Зокрема, це: Національний банк; банки, які відповідають хоча б одному з таких критеріїв: банк, який включено до переліку системно важливих банків; банк, який включено до переліку банків України, уповноважених для роботи (здійснення операцій) в особливий період; банк, у якому держава прямо чи опосередковано володіє часткою понад 75% від статутного капіталу банку [32];

– перелік банків, що є об'єктами критичної інфраструктури в банківській системі України (такі повноваження Національному банку надає Закон України «Про основні засади забезпечення кібербезпеки України» [30]);

– положення про організацію кіберзахисту в банківській системі України (затверджене Постановою Правління Національного банку України від 12 серпня 2022 року № 178), яке розроблено з метою унормування питань організації та забезпечення кіберзахисту і визначає: а) основні засади функціонування системи кіберзахисту в банківській системі України; 2) принципи забезпечення інформаційного обміну між Центром кіберзахисту

і банками України; 3) вимоги стосовно заходів щодо забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури в банківській системі України; 4) вимоги щодо проведення незалежного аудиту інформаційної безпеки в банківській системі України [140];

– положення про порядок визначення Національним банком України юридичних осіб, що є критично важливими для функціонування економіки та забезпечення життєдіяльності населення в особливий період (затверджене Постановою Правління Національного банку України від 24 березня 2023 року № 32), яке визначає процедуру прийняття Національним банком України відповідних рішень, за якими здійснюється визначення юридичних осіб, що мають важливе значення для галузі національної економіки чи задоволення потреб територіальної громади, у межах повноважень Національного банку з урахуванням Порядку та критеріїв визначення підприємств, установ і організацій, які є критично важливими для функціонування економіки та забезпечення життєдіяльності населення в особливий період, затверджених постановою Кабінету Міністрів України від 27 січня 2023 року № 76. Зокрема Національний банк приймає рішення про визначення критично важливими такі установи як: а) банки; б) небанківські фінансові установи та юридичні особи, які не є фінансовими установами, але мають право надавати окремі фінансові послуги, державне регулювання та нагляд за діяльністю яких здійснює Національний банк; в) небанківські надавачі платіжних послуг, визначені Законом України «Про платіжні послуги», оператори платіжних систем, технологічні оператори платіжних послуг, державне регулювання та нагляд за діяльністю яких/оверсайт платіжної інфраструктури щодо яких здійснює Національний банк (тобто – учасники платіжного ринку); г) юридичні особи, які отримали ліцензію Національного банку на надання банкам послуг з інкасації та погодження Національного банку на здійснення операцій з оброблення та зберігання готівки; д) єдине об'єднання страховиків, які здійснюють обов'язкове страхування цивільно-правової відповідальності власників наземних

транспортних засобів за шкоду, заподіяну третім особам; е) юридичні особи, які надають послуги системно важливим банкам, що є допоміжними до платіжних послуг, і їхня діяльність безпосередньо пов'язана з обслуговуванням банківських автоматів, платіжних терміналів, виконанням міжбанківських платіжних операцій [141].

Окремо зазначимо, що з початком повномасштабного вторгнення росії на територію України та введення воєнного стану для забезпечення надійного та стабільного функціонування фінансової системи країни та максимального забезпечення діяльності Збройних Сил України, а також безперебійної роботи об'єктів критичної інфраструктури [198] було прийнято ряд нормативно-правових актів. Так, Національним банком було прийнято Постанову «Про роботу банківської системи в період запровадження воєнного стану» від 24 лютого 2022 року № 18 [174], після прийняття якої в фінансовому секторі, а саме в банківській системі були запроваджені нові правила та обмеження. Зокрема з 24 лютого 2022 року тимчасово призупинив свою роботу валютний ринок, крім операцій по обміну валюти на гривню. Було зафіксовано офіційний курс валют на цю ж дату та заборонено видачу іноземної валюти з рахунків клієнтів, крім тих підприємств, на які покладался обов'язок по виконанню мобілізаційних планів. Транскордонні валютні платежі були заборонені введенням мораторію. І хоча безготівкові операції проводились в звичному режимі, емісія, обіг електронних грошей та поповнення електронних гаманців також було зупинено [224]. Зараз Національний банк поступово вирішує ці питання.

Однак необхідно констатувати, що інші ключові акти не є публічними. Також слід вказати про відсутність у публічному доступі будь-яких з таких щодо сфери компетенції Міністерства фінансів України.

Ще одним важливим аспектом є те, що вітчизняне законодавство перебуває у процесі активної адаптації встановлених та рекомендованих міжнародних стандартів до національної правової системи, проте ще не повністю відповідає всім висунутим вимогам до результативності здійснення

адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України.

Обґрунтувати зазначений тезис можна щонайменше тим, що Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури ґрунтується на таких постулатах як: захист, забезпечення безпеки та стійкість. Причому йдеться про стійкість до викликів сьогодення, стійкість до військових дій, стійкість до небезпеки, стійкість до збоїв, до нестабільності при яких система захисту має працювати. І на цьому власне законодавець та інституції реалізації його рішень у сфері захисту критичної інфраструктури фінансового сектору обмежуються. Наприклад, в грудні 2023 року було створене Управління захисту критичної інфраструктури, де ця організаційна структура була виділена із Департаменту Безпеки Національного банку і створена в секторі платіжних систем та грошового обігу, в наслідок чого розуміємо основний функціонал цієї структури: забезпечення безперервної роботи об'єктів критичної інфраструктури фінансового сектору, що переводячи на рівень побутового споживача виглядає як ефективний захист від загроз та безперебійного надання послуг населенню та має прояв як єдина функція захисту об'єктів критичної інфраструктури – це стійкість.

Дійсно, з одного боку все логічно, правильно та відповідно до європейських нормативів. Однак є одне важливе застереження, – коли Європейська Комісія почала приділяти увагу питанням критичних інфраструктур, зокрема, започаткувавши в середині 2000-х років Європейську програму захисту критичної інфраструктури («ЕССІР»), основна увага була зосереджена на захисті критичних інфраструктур, тобто питання здебільшого стосувалося традиційного управління ризиками з метою уникнення та запобігання небажаним подіям у певних секторах критичних інфраструктур. Через двадцять років питання вже ставиться так: «необхідно докорінно змінити нинішній підхід із захисту конкретних активів на посилення стійкості критично важливих суб'єктів, які ними керують». Зміна

парадигми пояснюється, з одного боку, зростанням кількості держав-членів, які «дедалі більше усвідомлюють важливість мислення щодо стійкості, в якому захист є лише одним з елементів поряд із запобіганням та пом'якшенням ризиків, безперервністю бізнесу та відновленням» [269].

Сучасний стан безпекового середовища України, а також низка інших факторів переконливо свідчать, що зміна парадигми від захисту до справжньої стійкості навряд чи буде реалізована на практиці, а лише створить хибне відчуття стійкості критичних інфраструктур [269]. Оскільки базовий рівень захисту об'єктів критичної інфраструктури фінансового сектору ще не досяг належного рівня відповідності, про повноцінний перехід до концепції стійкості наразі вести мову ще занадто рано, адже першочергово необхідно створити функціональну базу захисних заходів, що дозволять ефективно управляти ризиками на всіх рівнях. Це свідчить про необхідність розробки та впровадження механізмів, стратегій та планів захисту об'єктів критичних інфраструктур фінансового сектору, зокрема і в контексті актуальності протидії конкретним загрозам (наприклад, кібератаки чи збройні конфлікти). Наразі це питання перебуває у площині правового вакууму, що створює розрив між наявними механізмами її захисту та вимогами стійкості, що декларуються на міжнародному рівні.

Отже, можемо узагальнити, що нормативно-правові основи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України доцільно визначати через дуальність інтерпретаційної складової, де:

1) ідейно-концепційний складник є актуальним, належно сформований та таким, що не вимагає додаткової уваги в контексті оптимізаційних змін якісно новим ідеологічним наповненням;

2) практико-реалізаційний складник відзначається фрагментарністю, відсутністю публічності механізмів прояву означеної діяльності, а також недостатньою інтеграцією з міжнародними стандартами у сфері захисту критичної інфраструктури.

Таким чином, маємо такі ключові висновки:

– нормативно-правові основи є репрезентацією чинних регуляторних або рекомендаційних актів, які встановлюють правила, стандарти та вимоги до реалізації чи утримання від певної дії уповноважених суб'єктів у межах здійснення ними адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України;

– наявні нормативно-правові основи захисту об'єктів критичної інфраструктури фінансового сектору України є результатом здійснення нормативно-правового забезпечення розвитку досліджуваного кола адміністративно-правових відносин;

– пропонуємо нормативно-правові основи захисту об'єктів критичної інфраструктури фінансового сектору України диференціювати на:

1) міжнародні – наприклад, Рекомендації та Керівництва Групи з розробки фінансових заходів боротьби з відмиванням грошей, акти Міжнародного валютного фонду, Світового банку, Міжнародної організації з стандартизації;

2) регіональні – наприклад, Директива Ради ЄС 2008/114/ЄС, Директива Ради ЄС 2016/1148, Директива Ради ЄС 2018/843, Регламент ЄС 2021/23, Директива Ради ЄС 2022/2557, Рекомендації Ради ЄС 2023/C 20/01);

3) національні – законодавство у сферах сталого розвитку, національної безпеки та її складових, захисту критичної інфраструктури, регулювання ринку фінансових послуг, бюджетного регулювання, економічного розвитку та протидії фінансуванню злочинів;

– нормативно-правові основи досліджуваної діяльності у контексті національного рівня перебувають на стадії формування своєї повноцінної правової структури, адже наразі продовжується процес оптимізації їх змісту.

2.2. Принципи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України

Принципи визнаються результатом осмислення закономірностей розвитку суспільства, втілення його демократичної та гуманістичної традицій, є стрижнем будь-яких суспільних відносин, який відображає найбільш істотні їх ознаки [191, с. 220–221]. Варто підтримати наукове узагальнення, що недотримання або порушення принципів не дозволить досягти мети адміністративно-правового захисту [82, с. 74], тому актуальність виокремлення їхньої системи має як теоретичне, так і практичне значення.

З метою виведення власної дефініції «принципи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України» та виокремлення їх певних груп, звернемося до теоретичних положень категорії «принцип» та їх класифікації. Попри значну кількість досліджень цього феномену в теорії права, він є все ще одним з найбільш дискусійних, а проблема принципів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України взагалі лишається поза увагою науковців [82, с. 74].

Перш за все необхідно дослідити семантику поняття «принцип» та «принцип права» [137, с. 48]. Термін «принцип» походить від лат. *principium* – початок, це основні, найзагальніші, вихідні положення, засоби, правила, що визначають природу і соціальну сутність явища, його спрямованість і найсуттєвіші властивості [84, с. 43]. В юридичних тлумачниках поняття принцип тлумачиться також як: «1. Принцип як основоположна правда, закон, доктрина або припущення (підгрупи: 1) принцип як загальне правило або стандарт; 2) принцип як сукупність моральних та етичних стандартів). 2. Принцип як наперед визначена політика або спосіб дії. 3. Принцип як основна або необхідна якісна складова або елемент, що визначає внутрішню природу чи окремі характеристики поведінки. 4. Принцип як правило або

закон, що стосується функціонування природних феноменів чи механічних процесів» [179, с. 15]. В. Плукар узагальнює, що в юридичній літературі під принципами розуміються загальні керуючі, вихідні положення, які визначають найсуттєвіші сторони певного виду державної діяльності [138, с. 42].

Принципи, які складають основу правових норм у загальнотеоретичній науці іменують принципами права. У юридичній науці існує багато дефініцій поняття «принципи права», у цьому питанні науковці усе ще не досягли єдності [137, с. 48]. Зокрема В. Омелян уточнює, що наразі сформувались дві основні концепції щодо їх визначення [125, с. 150]. Згідно з першою концепцією, що ґрунтується на теорії позитивізму, принципи права – це ідеї, теоретичні, нормативно-керівні положення того чи іншого виду людської діяльності, які конкретизуються в змісті правових норм та об'єктивно зумовлені матеріальними умовами існування суспільства. За другим поглядом, який сформувався з ідеї природного права, принципи права розуміють як керівні ідеї, об'єктивно властиві праву відправні начала, незаперечні вимоги (позитивні зобов'язання), які ставлять до учасників суспільних відносин із метою гармонійного поєднання індивідуальних, групових і громадських інтересів, та визначають зміст і спрямованість правового регулювання, відображають найважливіші закономірності соціально-економічної формації [199, с. 41]. Причому більш характерним для сучасних поглядів на теорію права загалом та на поняття принципів права зокрема є другий підхід, що був сформований представниками школи природного права [125, с. 150].

Наприклад, на думку М. Савчина, принципи представляють собою вихідні нормативно-керівні засади, що забезпечують суттєвий, стійкий, регулятивний правовий зв'язок між різними нормами права та іншими нормативними приписами, вони виконують роль основного засобу для орієнтира в правотворчості, систематизації, інтерпретації та реалізації права. Якщо виявлено невідповідність правових приписів, норм принципам права

останні повинні інтерпретуватися через призму принципів права або приводитися у відповідність до них [187, с. 127–128]. Виходячи із зазначеного, можна дійти висновку, що існує зв'язок між нормами права та принципами права, фактично вони є взаємозалежними, адже принципи служать основою, орієнтиром для законодавця [137, с. 48].

С. Погребняк пише, що при характеристиці принципу зазвичай звертається увага на те, що він, по-перше, є ідеєю, положенням, вимогою і, по-друге, є не простим положенням (ідеєю, вимогою), а основним, основоположним, засадничим, фундаментальним, вихідним, загальним, керівним, відправним, провідним, чільним [139, с. 24]. На перший погляд, наведені слова є синонімічними, проте між словами «ідея», «положення», «вимога» все ж таки існують певні відмінності [142, с. 56], особливо в контексті характеристики внутрішньої будови терміну «принцип».

Дійсно, в основі кожного принципу знаходиться певна ідея. Відомо, що будь-яка загальна ідея проходить крізь історію у своїх специфічних формах, обумовлених особливостями буття людей і рівнем їх цивілізації. Термін «ідея» відображає генетичний аспект принципу, допомагає продемонструвати, що принципи є інтелектуально-духовними засадами та надають принципам такої риси, як універсальність, самоочевидність, самодостатність [139, с. 25–26]. Своєю чергою, термін «положення» означає твердження, думку, що знаходиться в основі чого-небудь; тезу [28, с. 851]. Він надає принципам фундаментального, засновницького, засадничого характеру. Водночас вимога – це побажання, прохання, висловлене так, що не допускає заперечень [192, с. 183]. Причому в юридичній науці часто зустрічаються погляди авторів, відповідно до яких принципи права є вимогами. Наприклад, на думку Р. Дворкіна, принципи права є вимогами справедливості, чесності чи якогось іншого морального виміру [49, с. 47]. У зв'язку з цим визначення принципу через вимогу дозволяє відобразити його як імперативне, категоричне, обов'язкове, остаточне явище [147, с. 49–50].

Узагальнюючи наведений матеріал можемо констатувати, що принципи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України можна визначити через категорію «правило», яка поєднує своїм змістом ідейний, засадничий та імперативний контекст. Дефініція порушеного питання, на нашу думку, може бути представленою так: «це фундаментальні правила, які визначають особливості, специфіку та критерії ефективності здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України». Причому підтримуємо позицію Я. Ковальчук, що найсуттєвіша їх детермінація полягає у визначеності ними основних напрямків діяльності, спрямованості ресурсів та способів досягнення поставлених цілей [79, с. 206].

У контексті ідентифікації критеріїв для їх класифікації варто зауважити на відсутності належної уваги з боку нормотворців та дослідників до специфіки цієї проблематики. Тому звернувшись до загальних основ маємо, що багатоманітністю характеризується і класифікація принципів права. Так, за сферою дії принципи права поділяють на загальні принципи права (спільні засади правового регулювання), міжгалузеві, галузеві, інституційні; залежно від територіальної дії: міжнародні та національні; за предметом регулювання: цивільно-правові, конституційно-правові та інші. Крім цього, серед принципів права виділяють загально цивілізаційні, загальноправові, загальні принципи права, типологічні, конкретно-історичні тощо [235, с. 135]. Причому найбільш поширеним є їх поділ за сферою дії на загальні, міжгалузеві, галузеві принципи та принципи інститутів права. Однак на відміну від західної теорії права, де під загальними принципами розуміють принципи, що діють у всіх правових системах [18, с. 157], у вітчизняному загальнотеоретичному правознавстві загальними принципами права, як правило, іменуються ті, які поширюються на всю систему права країни, діють у всіх галузях та інститутах, тобто зводяться, як вже зазначалося, виключно до характеристики національної правової системи. Обмеження сфери дії загальних принципів права національною правовою системою,

очевидно, можна пояснити інерцією радянських методологічних підходів, відповідно до яких будь-яка всезагальність принципів права заперечувалася з огляду на несумісність сутності «соціалістичного права» з «буржуазним». Утім, заради справедливості слід зазначити, що й на Заході офіційне визнання існування спільних для правових систем принципів права (і то переважно в межах міжнародно-правових систем) відбулося порівняно нещодавно – тільки після Другої світової війни [83, с. 151].

Щодо тих принципів, які стосуються певної управлінської дії, як правило, вони поділяються на загальні принципи, що стосуються системи органів влади в цілому, і спеціальні, дія яких розповсюджується лише на окремі підсистеми, ланки цієї системи чи на окремих [35, с. 301] суб'єктів [79, с. 206].

Інтерпретуючи зазначений матеріал до потреб цього дослідження вважаємо, що принципи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України доцільно визначати через загальнотеоретичні (загальноправові), галузеві та спеціальні принципи.

На нашу думку, загальнотеоретичними (загальноправовими) принципами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є ті, що віддзеркалюють особливості сучасного стану державотворення в Україні, особливості його ідеологічного підґрунтя. До числа таких можна віднести принцип верховенства права, принцип законності, принцип правової визначеності та прозорості. Якщо коротко схарактеризувати значення кожного з таких, будемо мати такі результати:

– відповідно до частини першої статті 8 Конституції України в Україні визнається і діє принцип верховенства права. Верховенство права – це панування права в суспільстві. Верховенство права вимагає від держави його втілення у правотворчу та правозастосовну діяльність, зокрема у закони, які за своїм змістом мають бути проникнуті передусім ідеями соціальної справедливості, свободи, рівності тощо. Одним з проявів верховенства права

є те, що право не обмежується лише законодавством як однією з його форм, а включає й інші соціальні регулятори, зокрема норми моралі, традиції, звичаї тощо, які легітимовані суспільством і зумовлені історично досягнутим культурним рівнем суспільства. Всі ці елементи права об'єднуються якістю, що відповідає ідеології справедливості, ідеї права, яка значною мірою дістала відображення в Конституції України [184];

– законність як основоположний принцип функціонування всіх державно-правових явищ, має кілька основних методологічних підходів щодо сучасного його розуміння. Перший необхідно пов'язувати з функціонуванням законності як системи нормативних вимог щодо побудови системи правового регулювання у державі, і відповідно, реалізації правотворчої діяльності (нормотворчий аспект). Другий повинен передбачати усвідомлення законності з погляду її потенціалу для забезпечення правопорядку у суспільстві (аспект, пов'язаний з реалізацією права). Саме в останньому розумінні законність і виступає режимом (станом) діяльності усіх без винятку державних органів, громадських об'єднань, політичних партій, підприємств, установ, організацій, їх посадових осіб, окремих громадян, за якого необхідно точно і неухильно дотримуватись положень чинних законів України [128, с. 61–63];

– у широкому розумінні принцип правової визначеності являє собою сукупність вимог до організації та функціонування правової системи з метою забезпечення стабільного правового положення людини шляхом вдосконалення процесів правотворчості та правозастосування [18]. Його основу складає формальна визначеність змісту правових норм, яка досягається шляхом логічного, послідовного та повного врегулювання суспільних відносин і надання цим відносинам певної форми. Зміст принципу правової визначеності становить вимога якості законів та інших нормативно-правових актів, яка має такі ознаки, як чіткість, точність, зрозумілість та передбачуваність законодавства, що досягається в процесі нормотворення шляхом використання засобів нормопроектної техніки.

Законодавство може бути передбачуваними лише тоді, коли правові норми є зрозумілими, тобто точно та чітко сформульованими, і доступними. Отже, принцип правової визначеності становить також вимога про оприлюднення законів та нормативно-правових актів. Крім того, інший аспект принципу правової визначеності стосується принципу неможливості зворотної дії законодавства та захисту легітимних очікувань [109, с. 96–97];

– загалом українське законодавство ідентифікує поняття «прозорість» як необхідність дотримання принципів відкритості та підзвітності у різних сферах і в окремих випадках деталізує їх складові [31]. Загалом діяльність органу публічної влади має буквально проглядатись наскрізь. В окремих випадках при організації роботи органів влади такий підхід застосовують справді прямолінійно шляхом фактичного спорудження прозорих офісів (кабінетів) посадових осіб, а інколи й загалом прозорих будівель. Звісно, вимога наскрізності не передбачає застосування саме такого підходу. Адже окрім певних переваг (ефективніший контроль за діяльністю посадових та службових осіб, відповідальніше ставлення посадових осіб до службових обов'язків тощо) це матиме низку інших загроз порушення прав людини та ефективності функціонування такого органу влади. Отже, прозорість слід сприймати як здатність будь-якої особи за допомогою певних засобів побачити діяльність органу державної влади чи органу місцевого самоврядування наскрізь, тобто розуміючи усі внутрішні процеси, що впливають на спосіб, вид та строки прийняття рішення у кожній конкретній справі. Поєднання зазначених елементів (вимог) принципу прозорості дає можливість всебічного та повного аналізу рівня імплементації та забезпечення у кожному органі одного з невід'ємних прав людини – права на доступ до інформації. Більше того, дотримання зазначених вимог має запобігти неправомірному засекреченню, приховуванню чи ненаданню суспільно-важливої інформації. Як на законодавчому рівні, так і на рівні локального нормотворення мають бути розроблені та активно

використовуватись реальні механізми реалізації права людини на доступ до інформації [29, с. 81].

Своєю чергою, галузевими принципами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є група з таких, що акцентують на особливостях забезпечення безпеки та стійкості суспільного розвитку, регулювання ринку фінансових послуг та загальних вимогах до діяльності суб'єктів національної системи захисту критичної інфраструктури в Україні. Серед ключових з-поміж таких можна виділити, наприклад:

– принцип пропорційності – спрямований на забезпечення у правовому регулюванні балансу інтересів. Тобто для того, щоб виправдати певні обмеження прав, має існувати відповідне відношення («пропорційні» у вузькому сенсі слова) між результатом, який досягається при задоволенні легітимної мети, та шкодою, яка завдається правам через використання законних засобів [212, с. 72–73];

– принцип ефективності – визначає необхідність вибору із декількох варіантів діяльності той, практична реалізація якого забезпечує найвищий рівень максимально досяжного або заздалегідь запланованого результату. Також він передбачає, що запропоновані рішення втілюються в мінімально можливі терміни з розумним використанням потрібних ресурсів [203];

– принцип координованості – передбачає узгодження взаємодій між різними суб'єктами права задля досягнення збалансованості у межах прийняття та реалізації управлінських рішень. У межах досліджуваної сфери його сутність зводиться до того, що регуляторні рішення мають бути скоординовані та враховувати дії інших регуляторів для запобігання регуляторному арбітражу та дисбалансу фінансового сектору [203];

– принцип розподілу відповідальності – ідентифікує роль та межі сфери дії кожного учасника взаємодії чи процесу, щоб забезпечити ефективне прийняття рішення та його виконання;

– принцип взаємодії – це поєднання зусиль суб'єктів, що наділені повноваженнями чи мають відповідні права у конкретній сфері, які не знаходяться у підпорядкуванні один одного з метою ефективного задоволення своїх інтересів [102, с. 97];

– принцип завчасної превенції – передбачає наявність програм та заходів, спрямованих на попередження конкретних видів порушень стабільного розвитку суспільних відносин. У більш конкретній інтерпретації його сутності, це так зване «раннє втручання», що запобігає виникненню проблем або безпосередньо вирішує їх, коли вони виникають, до того, як проблеми загострюються [285];

– принцип безпеки, захисту та охорони інформації з обмеженим доступом – надає певній інформації статусу такої, що має обмеження до отримання доступу до неї, а також об'єктивує наявність процесів, спрямованих на її захист;

– принцип оперативності – для ефективного, своєчасного регулювання суспільних відносин, які стрімко розвиваються, постає необхідність своєчасного, швидкого реагування на зміни в суспільстві, державі та за її межами. Отже, положення цього принципу полягають у швидкому реагуванні на відповідні зміни і вимагають оперативного прийняття відповідного юридичного документа. Його зміст повинен адекватно відповідати змінам у суспільних відносинах, а форма виражена у вигляді закону, підзаконного акта [223, с. 90];

– принцип своєчасності – позначає необхідність діяти чи утримуватися від дій, ураховуючи їх вчасність і доречність. Вимоги цього принципу стосуються як службових або посадових осіб, так і суб'єктів приватного права. Цей принцип найбільш щільно пов'язаний з принципом доцільності (корисного ефекту). Це пояснюється тим, що досягнення відповідної корисної мети, що загалом є рушійною силою будь-якої діяльності, переплітається саме з часом цього досягнення, оскільки, окреслюючи певну ціль, суб'єкт разом із цим розраховує на відповідний корисний ефект,

актуальність котрого може тривати досить незначний проміжок часу. Іншими словами, вчасне настання позитивних очікувань завжди є бажаним і доречним [148, с. 33];

– принцип передбачуваності – корелює з принципом правової визначеності, однак як самостійний принцип вимагає від суб'єктів права наперед визначати юридичні наслідки своєї поведінки;

– принцип адаптивності та мобільності – полягає в гнучкості та оперативному реагуванні на зміну чинників зовнішнього та внутрішнього середовища, інтенсивності їх впливу, викликів сучасних тенденцій [232] державотворення;

– принцип безперервності – встановлює обов'язок для суб'єкта владних повноважень забезпечувати безперервне виконання своїх завдань та функцій;

– принцип ресурсної достатності – визначає, що для реалізації суб'єктом владних повноважень його завдань та функцій держава має створити належні умови і надати відповідні ресурси для їх належного виконання;

– принцип довгострокової стійкості – орієнтує політичних та адміністративних акторів на вектор розвитку суспільних відносин, що характеризується здатністю збереження та накопичення необхідних ресурсів для підтримання адекватного рівня рівноваги між сьогоденням та майбутнім. Передбачає наявність планів розвитку та реалізації окремих механізмів, відхилення від реалізації яких сприймається як порушення цілісності процесу розвитку;

– принцип гнучкості – як самостійний функціональний орієнтир, передбачає здатність організації чи певного процесу своєчасно адаптуватись до мінливих умов зовнішнього середовища або їх швидку перебудову відповідно до нових цілей функціонування [66]. У досліджуваній сфері це також обов'язок урахування зміни зовнішнього середовища, яке може мати вплив на перегляд окремих ініціатив чи заходів [203];

– принцип системності та цілісності – декларує, що кожна дія суб'єкта управління має відповідати загальній меті та визначеному плану чи стратегії розвитку всієї системи;

– принцип безперервного вдосконалення – постійне та циклічне покращення управлінських, технічних, організаційних процесів з метою підвищення ефективності роботи.

Варто зауважити, що проблематика реалізації принципу безпеки, захисту та охорони інформації з обмеженим доступом є особливо актуальною для досліджуваної сфери, адже має кореляційний взаємозв'язок із принципом публічності, який вимагає від суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України дотримання балансу між забезпеченням відкритості і прозорості їхньої діяльності та збереженням секретності. Зокрема розпорядчі документи щодо організації роботи з інформацією з обмеженим доступом, що не належить до державної таємниці, затверджені рішенням Правління Національного банку України від 15 серпня 2023 року № 282-рш, забезпечують запобігання розголошенню статистичної інформації банків щодо окремих суб'єктів та іншої конфіденційної інформації [122]. Означеного рішення немає у відкритому публічному доступі на офіційному вебсайті Національного банку України або інших публічних джерелах. Тому достовірно стверджувати, що розпорядчі акти, які стосуються захисту критичної інфраструктури фінансового сектору містять конфіденційну інформацію ми змоги не маємо, проте вважаємо, що цілком обґрунтовано вбачати це припущення правдоподібним, адже більшість з такої інформації має бути захищеною з міркувань необхідності мінімізації ризиків витоку інформації, що може поставити під загрозу національну безпеку та економічну стабільність.

Ми прибічники думки, що не вся інформація має бути секретною. Закон України «Про критичну інфраструктуру» акцентує на праві громадського нагляду у цій сфері й враховує особливості захисту державної

таємниці. Про обмеження доступу до інформації, яка такою не є, положень немає. Знову ж таки, констатувати про будь-які порушення принципу публічності достовірно не вдасться, адже не зрозуміло який статус має така інформація. Однак, на нашу думку, щонайменше широкий громадський загал має знати про дату прийняття, номер акту про утворення та коротку характеристику основ діяльності Управління захисту критичної інфраструктури як організаційної одиниці Національного банку України. Відзначимо, що наразі інформування громадськості про результати діяльності щодо реалізованих заходів захисту об'єктів критичної інфраструктури фінансового сектору України принаймні про загальні дані, які не порушують вимоги безпеки, здійснюється через опубліковані звіти про стан фінансової стабільності та загальний річний звіт діяльності Національного банку, а не окремий щорічний звіт щодо забезпечення захисту критичної інфраструктури у фінансовому секторі. Тому слід констатувати, що інформація, яка подається у їх межах є недостатньою для інформування громадськості про реалізовані заходи. Проте зауважимо, що детальна інформація про вразливості та наявні прогалини в механізмах захисту об'єктів критичної інфраструктури фінансового сектору України є небезпечною з точки зору високого рівня ризику можливих зловживань.

Завершуючи розгляд класифікаційних груп розподілу аналізованих принципів, варто вказати, що за нашим баченням спеціальними принципами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є ті, що мають безпосереднє відношення до процедур забезпечення організаційної та функціональної стійкості об'єктів критичної інфраструктури, ідентифікації її вразливості, обміну інформацією зовнішнього та внутрішнього рівнів, управління ризиками та здійснення превентивної діяльності на постійній основі. Такими, наприклад, є:

– принцип організаційної стійкості – вказує на те, що процес стратегічного планування й управління в державі має бути систематизованим, узгодженим на різних рівнях [234];

– принцип інституційної спроможності регуляторів – здатність регуляторів оперативно та адекватно реагувати на ризики та втрати фінансового сектора, ефективно застосовувати весь інструментарій механізму антикризового управління з метою забезпечення стабільного функціонування фінансової системи країни [95, с. 79];

– принцип цільової спрямованості – встановлює вимогу реалізації захисної дії виключно задля досягнення визначеної мети та виконання поставленого завдання, тобто це встановлення обов'язку її практичної реалізації тільки у межах необхідної площини;

– принцип комплексного моніторингу – декларує підхід, за якого має здійснюватись своєчасна ідентифікація загроз, оцінка ризиків для вжиття завчасних заходів для зменшення їхнього впливу на фінансову систему та діяльність об'єктів її системи, порушення функціональності яких матиме значні негативні наслідки;

– принцип динамічності – передбачає періодичну перевірку встановлених стандартів, правил та вимог до захисту критичної інфраструктури, приведення їх у відповідність до актуальних реалій та швидкоплинних змін;

– принцип макропруденційного регулювання – передбачає усунення чи обмеження системних ризиків, щоб запобігти кризам або зменшити втрати від них [105];

– принцип сприяння прибутковості – встановлює кореляцію між необхідністю вжиття охоронних чи захисних заходів та економічною доцільністю, вирівнюючи баланс між ними;

– принцип мінімізації фінансового стресу – визначає вимогу зменшення рівня напруги у фінансовому секторі України стабілізуючими заходами;

– принцип очікуваних збитків (втрат) – допускає, що заходи безпеки матимуть потенційну економічну збитковість;

– принцип вільного руху капіталу – орієнтир для продовження поступової лібералізації валютного ринку, оптимізації його заходів захисту та утвердження повної свободи проведення валютних операцій [33].

Варто вказати, що запропонована варіація досліджуваних принципів є суб'єктивною та не вичерпною, адже, наприклад, окремо можна виділити принципи діяльності Національного банку, як основного суб'єкта системи здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України або деталізувати принципи «культури управління ризиками» як результату нової філософії забезпечення безпеки, до якої входять: 1) відкритий обмін інформацією між державними органами, приватним сектором, населенням і окремими громадянами стосовно ризиків, враховуючи необхідність захисту певної (чутливої) інформації; 2) співробітництво між усіма суб'єктами процесу захисту критичної інфраструктури у запобіганні інцидентам та у реагуванні на них; 3) підвищення рівня самозахисту, самопомочі, власних можливостей громадян та організацій, уразливих до припинення або погіршення послуг, які забезпечує критична інфраструктура; 4) активне міжнародне співробітництво щодо захисту критичної інфраструктури з огляду на процеси глобалізації та зростання залежності безпекових, економічних, виробничих, фінансових і т. ін. процесів у багатьох країнах від постачання послуг та ресурсів, які здійснюються міжнародними мережами, системами, компаніями тощо [16, с. 14].

Також, наприклад, можна вести мову про принципи, що визначені Стратегією розвитку фінансового сектору України, до числа яких з-поміж окремих вище вказаних віднесено: 1) системність – наявність узгодженого набору напрямів діяльності, що створюють синергетичний ефект для досягнення цілей держави та фінансового сектору; 2) прозорість та підзвітність – реалізація заходів супроводжується звітуванням; 3) стійкість – заходи спрямовуються на посилення стійкості фінансового сектору до внутрішніх та зовнішніх шоків; 4) верховенство права, боротьба з корупцією,

запобігання та протидія фінансуванню тероризму, легалізації (відмиванню) доходів, одержаних злочинним шляхом [203].

Отже, можемо констатувати, що принципи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, як правила організаційного та практико-реалізаційного характеру, мають подвійну юридичну спрямованість сфери розповсюдження своєї дії. З одного боку, уповноважені представники національної системи їхнього захисту мають дотримуватись встановлених загальноправових, галузевих та спеціальних орієнтирів, щоб ефективно та результативно виконувати своє функціональне призначення. З іншого боку, вони покладають на державу обов'язок забезпечити цим суб'єктам належні умови для реалізації задекларованих принципів, зокрема через створення правового, організаційного та ресурсного забезпечення.

Таким чином, маємо такі ключові висновки:

– аналіз наукової та нормативної доктрини на предмет виявлення системи принципів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України свідчить про відсутність належної уваги з боку нормотворців та дослідників до специфіки цієї проблематики;

– пропонуємо принципи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України визначати через загальнотеоретичні (загальноправові), галузеві та спеціальні принципи;

– розвиток нової філософії забезпечення безпеки зумовив виникнення низки нових правил адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, обумовлених необхідністю розвитку «культури управління ризиками». Серед таких ключовими є: 1) принцип комунікативної взаємодії між представниками держави та приватним сектором; 2) принцип системно здійснюваної співпраці між усіма суб'єктами та учасниками захисту об'єктів критичної інфраструктури

фінансового сектору України; 3) принципом автономної стійкості; 4) принцип міжнародного співробітництва.

2.3. Суб'єкти адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України

Виклад попереднього матеріалу переконливо свідчить, що без ідентифікації системи суб'єктів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України навряд чи вдасться зрозуміти специфіку досліджуваного кола питань, їх особливості та правову природу. Аналогічно можна стверджувати і про інструментарій їхньої діяльності, що як логічне продовження порушених питань знайде своє відображення на наступному етапі цього дослідницького пошуку.

Зокрема нами виявлено, що державна політика захисту критичної інфраструктури передбачає певну стратегію діяльності представників національної системи її захисту. Аналізуючи сучасну структурно-функціональну характеристику державної політики у сфері захисту критичної інфраструктури в Україні, Я. Страхніцький визначає, що у цьому напрямку існує ряд паралельно функціонуючих систем: 1) єдина державна система цивільного захисту; 2) єдина державна система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків; 3) державна система фізичного захисту (функціонує відповідно до Закону України «Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання» [162]); 4) національна система кібербезпеки [204]. Дійсно, кожна з означених систем є важливою у механізмі забезпечення ефективного захисту критичної інфраструктури, але вченим, на нашу думку, не враховано секторальний аспект порушеного питання. Зокрема фінансовий сектор України має, наприклад, систему регуляторів фінансового ринку та окремо Фонд

гарантування вкладів фізичних осіб, які сукупно в очах закону не є самостійною інтегрованою системою, однак виконують функції, які сприяють стійкості та безпеці конкретно критичної інфраструктури фінансового сектору України [229].

Проте уточнимо, що сучасна парадигма державної політики у сфері захисту критичної інфраструктури в умовах військового стану в Україні в теоретичному плані достатньо не вивчена [204], особливо в контексті безпеки та стійкості фінансового сектору. А отже, проблематика визначення системи суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є не тільки практично цінною в аспекті цілого дослідження, а й теоретично значимою в контексті розвитку адміністративно-правової галузі наукових знань загалом.

Розпочинаючи аналіз порушеного питання варто нагадати, що впровадження захисту критичної інфраструктури в країні є амбіційним завданням, вирішення якого потребує як матеріальних ресурсів, так і ґрунтовної науково-технічної та експертної підтримки, кадрових ресурсів, і мабуть, ключовий момент – політичної волі. Відносно останнього потрібно сказати, що країна, яка виявиться нездатною організувати ефективно захист власної критичної інфраструктури не тільки закриває собі шлях розвитку, а приречена на загибель. На щастя в нашій державі [14, с. 157] все ж таки у 2023 році затверджено Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури [157]. Означений план спрямований на створення механізму, що забезпечить безперервність функціонування об'єктів критичної інфраструктури та узгодженість дій суб'єктів національної системи її захисту [73].

Семантичний аналіз категорії «система» свідчить про те, що нею в сучасній українській мові прийнято позначати доволі багато явищ, як-то: порядок, що зумовлений правильним, планомірним розташуванням і взаємним зв'язком чого-небудь; продуманий план; заведений, прийнятий порядок; форма організації, будови чого-небудь (державних, політичних,

господарських одиниць, установ і таке інше); сукупність яких-небудь елементів, одиниць, частин, об'єднаних за спільною ознакою, призначенням; сукупність принципів, які є основою певного вчення; сукупність способів, методів, прийомів здійснення чого-небудь; будова, структури, що становить єдність закономірно розташованих і функціонуючих частин; сукупність предметів, пристроїв і таке інше однакового призначення; сукупність господарчих одиниць, установ, об'єднаних організаційно [28, с. 1320–1321]. У цьому аспекті цілком слушним є зауваження Н. Оніщенко, висловлене під час дослідження теоретико-методологічних засад формування та розвитку правової системи. Учена наголошує на тому, що неоднозначне сприйняття категорії «система», в першу чергу, пов'язано з тим, що на сьогодні можна назвати близько п'ятдесяти визначень її сутності [127, с. 20]. Зауважимо, що для нас найбільший інтерес представляє те, що використання по відношенню до відповідного явища, в тому числі досліджуваного, категорії «система» позначає, що воно має системний характер, тобто утворюється із взаємопов'язаних елементів, які й визначають його як щось ціле [92, с. 94].

Нормами Закону України «Про критичну інфраструктуру» встановлено, що: «національна система захисту критичної інфраструктури – сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури» [166].

Маємо визначити, що державна політика є кінцевим оформленням політичних намірів чинної на певний період політичної влади реформувати (розвивати) певний напрям функціональності суспільних відносин; об'єктивізацією способів реалізації влади, де суб'єкт владних повноважень (як правило, що наділений політико-адміністративними функціями), виконуючи свої прямі обов'язки (аналіз сучасного стану конкретної

проблеми, оцінка майбутніх перспектив та формування плану заходів до впровадження, публічне обговорення тощо) формує стратегічну основу, а у конкретних випадках і реалізовує план дій, необхідний для вирішення проблем публічного значення [287, с. 92].

За загальним правилом формування та реалізація державної політики у сфері захисту критичної інфраструктури здійснюється: 1) Кабінетом Міністрів України, який забезпечує проведення державної політики у сфері захисту критичної інфраструктури України, організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи захисту критичної інфраструктури, визначає уповноважений орган з питань захисту критичної інфраструктури України, затверджує Регламент обміну інформацією для забезпечення обміну інформацією та взаємодії суб'єктів національної системи захисту критичної інфраструктури; 2) секторальними та функціональними органами у сфері захисту критичної інфраструктури, які відповідають за формування та реалізацію державної політики в окремих секторах критичної інфраструктури; 3) уповноваженим органом у сфері захисту критичної інфраструктури України, який відповідає за координацію діяльності суб'єктів національної системи захисту критичної інфраструктури [204]. Причому відповідальні за захист об'єктів критичної інфраструктури – безпосередньо її оператори [216], – юридичні особи будь-якої форми власності та/або фізичні особи-підприємці, що на правах власності, оренди або на інших законних підставах здійснюють управління об'єктом критичної інфраструктури та відповідають за його поточне функціонування [166].

З цього робимо висновок, що за захист об'єктів критичної інфраструктури фінансового сектору України відповідає значно ширша група суб'єктів у порівнянні з тими, що мають відповідні адміністративні повноваження.

Нагадаємо, що Постановою Кабінету Міністрів України «Деякі питання об'єктів критичної інфраструктури» від 9 жовтня 2020 року № 1109 [53]

передбачено, що секторальним органом у сфері захисту критичної інфраструктури фінансового сектору є Міністерство фінансів України та Національний банк України.

Нормами Закону України «Про критичну інфраструктуру» передбачається, що Національним банком України є представником загальнодержавного рівня управління національною системою захисту критичної інфраструктури. На нього покладено обов'язок категоризації об'єктів критичної інфраструктури в банківській та фінансовій системах, а також визначення порядку розроблення паспорта безпеки на об'єкти критичної інфраструктури, зміст і строки подання його банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, платіжними організаціями, учасниками платіжних систем, операторами послуг платіжної інфраструктури [166].

І якщо Кабінет Міністрів України встановлює вимоги щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності, то означене завдання щодо банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури здійснює Національний банк України [166].

Міститься також вказівка, що перелік об'єктів критичної інфраструктури фінансового сектору, включених до Реєстру, страхових ризиків настання кризової ситуації на таких об'єктах, які підлягають страхуванню, а також мінімальний ліміт відповідальності (у разі страхування відповідальності перед третіми особами) перед затвердженням Кабінетом Міністрів України погоджуються з Національним банком України [166].

Відповідно, профільне законодавство у сфері діяльності Національного банку України передбачає, що Національний банк виконує такі функції: «забезпечує формування та ведення переліку об'єктів критичної інфраструктури, а також реєстру об'єктів критичної інформаційної

інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю на яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг, визначає критерії та порядок віднесення об'єктів у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю на яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг до об'єктів критичної інфраструктури та об'єктів критичної інформаційної інфраструктури, встановлює вимоги до проведення аудиту інформаційної безпеки у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю на яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг», «забезпечує формування та реалізацію державної політики у сфері захисту критичної інфраструктури щодо банків, інших осіб, що здійснюють діяльність на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг відповідно до закону, що визначає правові та організаційні засади функціонування і захисту критичної інфраструктури» [167].

Додамо, що у нормативно-правових актах, прийнятих під час запровадження воєнного стану передбачена можливість Національного банку надавати підтримку державному бюджету (тимчасова інституціональна можливість чого випливає із законодавства про військовий стан), а також, усвідомлюючи потенційні ризики монетизації дефіциту державного бюджету, Національний банк фінансує лише критичні видатки Уряду в обмежених обсягах. Попри появу таких додаткових повноважень Регулятора, Національний банк має виходити з потреби збереження власної

інституційної, фінансової та операційної незалежності для належного виконання своїх функцій. З огляду на вказане, цілком логічним виглядає формулювання нової стратегічної мети у Стратегії 2023 року – інституційна спроможність Регулятора [95, с. 81].

Визначимо також, що забезпечення формування та реалізації Національним банком України державної політики у сфері захисту критичної інфраструктури, зокрема забезпечення виконання Національним банком України завдань та функцій суб'єкта національної системи захисту критичної інфраструктури, секторального органу у сфері захисту критичної інфраструктури та оператора критичної інфраструктури відповідно до Закону України «Про критичну інфраструктуру» здійснює Управління захисту критичної інфраструктури Національного банку України. Ми вже зазначали, що раніше частину функцій із захисту критичної інфраструктури виконував Департамент безпеки Національного банку. Водночас з огляду на розширення функцій із захисту критичної інфраструктури у фінансовому секторі та з метою підвищення ефективності виконання відповідних завдань за цим напрямом Національний банк створив у своїй структурі окреме управління. Наразі Управління захисту критичної інфраструктури входить до вертикалі підпорядкування «Платіжні системи та грошовий обіг», загальне керівництво якою здійснює заступник Голови Національного банку [117].

Слід вказати й про Колегіальний орган, якому Правління Національного банку делегувало окремі повноваження щодо здійснення банківського регулювання та нагляду, валютного нагляду, державного регулювання та нагляду у сфері фінансового моніторингу, оверсайту платіжної інфраструктури – Комітет з питань нагляду та регулювання діяльності банків, оверсайту платіжної інфраструктури. Серед його повноважень можна виділити таке як застосування заходів впливу/санкцій за порушення банківського, валютного законодавства України, законодавства України з питань фінансового моніторингу, нормативно-правових актів Національного банку, уключаючи нормативно-правові акти Національного

банку, якими запроваджені обмеження щодо проведення операцій, які мають на меті/порушують, сприяють або можуть сприяти уникненню/порушенню обмежень, установлених персональними спеціальними економічними та іншими обмежувальними заходами (санкціями), вимог Національного банку, установлених відповідно до статей 66, 67 Закону про банки, законодавства України з питань захисту критичної інфраструктури, кіберзахисту та інформаційної безпеки, про захист прав споживачів фінансових послуг, у тому числі вимог щодо взаємодії зі споживачами при врегулюванні простроченої заборгованості (вимог щодо етичної поведінки), законодавства, що регулює діяльність на платіжному ринку, та в разі недостатності заходів з управління ризиками, що вживаються для захисту інтересів споживачів платіжних послуг, або в разі здійснення банками ризикової діяльності, що загрожує інтересам вкладників чи інших кредиторів банку, а також у разі застосування іноземними державами або міждержавними об'єднаннями, або міжнародними організаціями санкцій до банків чи власників істотної участі в банках, що становлять загрозу інтересам вкладників чи інших кредиторів банку та/або стабільності банківської системи [217, с. 19].

Окремо зазначимо, що з метою ефективного функціонування системи кіберзахисту банківського та небанківського фінансового секторів України у 2017 році був створений Центр кіберзахисту Національного банку України. Основна його візія зосереджена на поєднанні та координації зусиль суб'єктів кіберзахисту фінансового сектору в протистоянні актуальним кіберзагрозам, підвищенні рівня кіберзахисту суб'єктів фінансового сектору України. Задля цього Центр уповноважений на: 1) моніторинг, виявлення та реагування на кіберінциденти, збір, накопичення та аналіз даних про виявлені кіберінциденти у фінансовому секторі; 2) аналіз сучасних кіберзагроз, вивчення зразків шкідливого програмного забезпечення, формування індикаторів кіберзагроз та розроблення рекомендацій з протидії; 3) оперативне інформування суб'єктів кіберзахисту про зафіксовані спроби вчинення кібератак, поширення інформації про індикатори кіберзагроз;

4) надання фінансовому сектору консультативної допомоги з питань організації кіберзахисту, виявлення кіберінцидентів, реагування та протидії кіберзагрозам, усунення наслідків кіберінцидентів; 5) розроблення рекомендацій для кіберзахисту; 6) співпрацю та обмін інформацією з міжнародними організаціями, довіреними зовнішніми джерелами інформації з питань реагування на кібератаки [221].

Організація цих завдань об'єктивує наявних чотири сервіси: «Incident Response», «Proactive Risk Monitoring», «Information services», «Training and education». Так «Incident Response» відповідає за надання допомоги банкам у вирішенні питань технічного характеру під час реагування на кіберінциденти: прийняття звіту про інцидент, аналіз інциденту, підтримка в реагуванні на інцидент, координація дій під час реагування на інцидент. «Proactive Risk Monitoring» здійснює проактивний моніторинг ризиків, що включає розвідку актуальних кіберзагроз та потенційних вразливостей, збір інформації з використанням різноманітних джерел, дослідження та аналіз даних: виявлення фішингових доменів, виявлення витоків даних, виявлення скомпрометованих даних облікових записів користувачів та клієнтів банку, моніторинг потенційних вразливостей. «Information services» інформує банки про актуальні кіберзагрози та вразливості, заходи протидії кібератакам та заходи безпеки, необхідні для захисту інформаційних систем клієнтів. «Training and education» проводить тренінги та навчальні сесії з метою підвищення рівня обізнаності та проінформованості у сфері кіберзахисту, реагування на кіберінциденти, протидії актуальним кіберзагрозам [190].

Причому важливо, що 2 серпня 2019 року Центр кіберзахисту Національного банку України та Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України підписали Меморандум про взаємодію та співробітництво в сфері кібербезпеки та кіберзахисту, спрямовану на попередження, виявлення, ефективне реагування та протидію актуальним кіберзагрозам, підвищення рівня інформаційної безпеки та ситуаційної обізнаності у сфері кібербезпеки та

кіберзахисту. Така взаємодія суттєво підвищує кіберстійкість банківської системи України до сучасних викликів і загроз, надає змогу ефективніше реагувати та протистояти актуальним кіберзагрозам, насамперед високого ступеня складності, що загалом сприяє стабільності банківської системи України [118].

Своєю чергою, варто звернути увагу на той факт, що Положення про Міністерство фінансів України, затверджене постановою Кабінету Міністрів України від 20 серпня 2014 року № 375 не передбачає жодних положень, пов'язаних з визначенням означеного суб'єкта секторальним органом у цій сфері. Однак маємо вказати, що у його структурі, наприклад, функціонують: Департамент прогнозування доходів бюджету, що відповідає за планування, виконання та моніторинг виконання бюджетів; Державна казначейська служба України, що відповідає за розрахунково-касове обслуговування розпорядників та одержувачів бюджетних коштів; Державна податкова служба України, що відповідає за здійснення контролю за надходженням до бюджетів та державних цільових фондів податків, зборів, платежів.

Щодо функціональних органів, уточнимо, що вони беруть участь у реагуванні на кризові ситуації, пов'язані із забезпеченням безпеки та стійкості критичної інфраструктури фінансового сектору. Йдеться, наприклад, про Службу безпеки України – проти диверсій, Державну службу спеціального зв'язку та захисту інформації України – проти кібератак [216]. Водночас Державна служба захисту критичної інфраструктури та забезпечення національної системи стійкості України є уповноваженим органом у сфері захисту критичної інфраструктури України [176]. Однак важливо, що на час дії воєнного стану та протягом 12 місяців після його припинення чи скасування уповноваженим органом у сфері захисту критичної інфраструктури України визначена Державна служба спеціального зв'язку та захисту інформації України [50].

Наразі у межах її організаційної структури для виконання функцій уповноваженого органу з питань захисту критичної інфраструктури створено

окремий департамент захисту критичної інфраструктури, який займається виключно цим питанням. Його створювали з нуля. Причому на це не виділялись кошти з держбюджету. Перерозподілили ті, що мали. Частина фахівців було переведено з існуючої структури. Адже певна кількість посад звільнилися після того, як було передано Міністерству цифрової трансформації функції контролю за електронними комунікаціями, сферами цивільного зв'язку та інтернету. Але більшість спеціалістів до цього департаменту були набраними. Практично департамент на 95% сформований з нових людей. Варто вказати, що не просто заповнювався штат, а здійснювався підбір саме тих спеціалістів, в яких була потреба. Частина спеціалістів перед тим, як приєднатись до департаменту, працювали в Державній службі України з надзвичайних ситуацій, Нацгвардії, в правоохоронних органах, у сфері енергетики. Загалом станом на кінець 2023 року нараховувалось вже близько 40 фахівців. Однак цього замало, тому розширення йдуть плановим шляхом, адже є 21 сектор, 25 підсекторів критичної інфраструктури, в яких є критичні об'єкти, але не у тій мірі, яка вимагається потребами, оскільки функціонал департаменту не надає можливості набрання 100 працівників, як було передбачено для окремої Державної служби захисту критичної інфраструктури [107].

У підтвердження нашого попередньо сформованого тезису про те, що «базовий рівень захисту об'єктів критичної інфраструктури фінансового сектору в Україні ще не досяг належного рівня відповідності, а тому про повноцінний перехід до концепції стійкості наразі вести мову ще занадто рано» можемо навести цитати з інтерв'ю голови Державної служби спеціального зв'язку та захисту інформації, бригадного генерала Ю. Щиголя, який вказав, що: «система критичної інфраструктури в Україні будується з нуля. Маємо визначити не тільки як захищати, а й що захищати, як розставляти пріоритети. Всі ці напрацювання мають бути втілені в дієві механізми чинної регуляторної бази. Ось ця робота наразі й виконується департаментом в складі Державної служби захисту критичної

інфраструктури. Завдання – побудувати реєстр об’єктів критичної інфраструктури й екосистему навколо нього» [107].

Також маємо вказати, що на українському фінансовому ринку діють два регулятори: Національний банк України та Національна комісія з цінних паперів та фондового ринку. Примітно, що до 2020 року їх було три, зокрема функціонувала Національна комісія, що здійснює державне регулювання у сфері ринків фінансових послуг. Однак зі скороченням регуляторних та контролюючих органів на ринках небанківських фінансових послуг, її функції було передано двом іншим регуляторам [69]. Власне, положеннями Стратегії розвитку фінансового сектору України планується, що регулятори фінансового ринку та Фонд гарантування вкладів фізичних осіб на момент її виконання мають створити та оновлювати плани забезпечення організаційної стійкості (безперервності основних бізнес-процесів), забезпечувати стійкість об’єктів критичної інфраструктури, проводити навчання та тестування стійкості критичної інфраструктури до вразливостей, обмінюються інформацією про кіберінциденти між собою та з іншими установами критичної інфраструктури, впроваджуватимуть проектні методики управління, безперервне вдосконалення процесів, розвиватимуть компетенції персоналу на постійній основі [203].

Доцільно зауважити, що у попередньо чинній стратегії серед стратегічних цілей не було названо такої пріоритетної мети як досягнення інституційної спроможності та фінансової незалежності Регуляторів [95, с. 79]. Зокрема О. Баштанник як представниця сучасної науки державного управління, пропонує інституційну спроможність для інституції трактувати як здатність виконувати свої функції на основі нормативно-правового, організаційного та ресурсного забезпечення (структурний аспект сутності інституції). В якості складових дослідження інституційної спроможності науковиця виділяє такі параметри: 1) нормативно-правова складова – наявність узгодженої нормативно-правової бази; 2) організаційна складова – наявність необхідного рівня структурної диференціації; 3) ресурсна складова

– наявність достатнього обсягу людських і матеріальних ресурсів [10, с. 14]. К. Кузьменко зауважує, що сьогодні, попри війну, в Україні створено нормативне підґрунтя для функціонування Національного банку та Національної комісії з цінних паперів та фондового ринку як спроможних та незалежних Регуляторів діяльності з надання фінансових послуг [95, с. 82].

На останок слід вказати і про Раду з фінансової стабільності, що є міжвідомчим органом, який здійснює обмін інформацією та своєчасне виявлення поточних та потенційних зовнішніх і внутрішніх загроз та системних ризиків для забезпечення фінансової стабільності й мінімізації їх негативного впливу на фінансову систему держави, а також узгодження упереджувальних заходів та заходів швидкого реагування (антикризовий менеджмент) за наявності ознак нестійкого фінансового стану банківської системи, а також обставин, які загрожують стабільності банківської та/або фінансової системи держави [171]. До її складу входять: Міністр фінансів України, Голова Національного банку України, заступник Міністра фінансів України з питань європейської інтеграції, Голова Національної комісії з цінних паперів та фондового ринку, заступник Голови Національного банку України, директор-розпорядник Фонду гарантування вкладів фізичних осіб, перший заступник Голови Національного банку України, Перший віцепрем'єр-міністр України – Міністр економіки України, заступник Керівника Офісу Президента України [68].

Раду можна сприймати і як майданчик для фахових дискусій про фінансову стабільність. Її рішення є рекомендаційними, адже вона не втручається в діяльність органів, які входять до її складу, але колективно напрацьовує пропозиції щодо заходів державної політики на досягнення фінансової стабільності. Засідання Ради з фінансової стабільності відбуваються щонайменше один раз на квартал. Інформаційно-аналітичне та організаційне забезпечення діяльності Ради здійснює Національний банк України. Задля ефективності роботи Рада створила декілька робочих груп (комітетів). Така структура спрямована на розроблення механізмів

співробітництва й координацію дій із забезпечення фінансової стабільності в державі, а також якісну підготовку рекомендацій щодо мінімізації системних ризиків, що загрожують стабільності банківської та/або фінансової системи України. Саме на рівні комітетів відбувається узгодження законодавчо-нормативного регулювання у фінансовій сфері між різними регулюючими органами [181].

Додамо, що із серпня 2022 року до липня 2023 року Рада з фінансової стабільності провела п'ять засідань. У цей час порядок денний засідань Ради насамперед визначали виклики, пов'язані з продовженням повномасштабної війни росії проти України. Пріоритетним питанням порядку денного Ради стала підтримка роботи банківського сектору та його клієнтів під час війни. Зокрема, члени Ради розглянули та підтримали пропозиції уряду та Національного банку України з оптимізації Державної програми «Доступні кредити 5-7-9%» та реалізацію проекту «Power Banking» для сприяння кредитуванню та фінансовій стабільності [68].

Вартим уваги також є те, що 13 грудня 2019 року Рада з фінансової стабільності ухвалила рішення утворити Робочу групу (Комітет) з фінансового розвитку при Раді з фінансової стабільності. Функції та склад Комітету оновлено відповідно до рішення Ради в травні 2023 року. Відповідно основні завдання Комітету є такими: 1) визначення напрямів та пріоритетів, спрямованих на впровадження Стратегії розвитку фінансового сектору України; 2) сприяння скоординованій реалізації заходів, передбачених Стратегією розвитку фінансового сектору, забезпечення моніторингу ефективності їхньої реалізації; 3) розгляд пропозицій щодо планування заходів із розвитку фінансового сектору. Наразі при Комітеті створена комунікаційна платформа за участі представників ринку та профільних експертів. Загалом їхні засідання проводяться за наявності потреби [202].

Оновленого звіту про діяльність Ради ще немає, однак серед основного, наприклад, на засіданні 5 лютого 2024 року Рада розглянула і взяла до відома

оновлений макроекономічний прогноз Національного банку та огляд системних ризиків для фінансового сектору. Зокрема констатовано, що економіка України відновлювалася впродовж 2023 року, і, попри війну, зростання триватиме й надалі, а рівень ризиків у фінансовому секторі контрольований. Уточнимо, що основним припущенням прогнозу є відчутне зниження високих безпекових ризиків із 2025 року. Довше збереження таких ризиків негативно впливатиме на ділові та споживчі настрої, водночас значний стимул економіці може надати реалізація масштабних проєктів відбудови України та отримання заморожених російських активів. Нині ключовим системним ризиком є неритмічність надходження міжнародної допомоги [180].

Підводячи підсумок варто зауважити, що система суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України – це цілісне інституційне утворення, що має функціонувати на засадах єдності та диференціації, гармонійності та кооперації. В умовах сучасності можна вести мову про її сформованість, однак не публічність. Йдеться зокрема про те, що переважна частина прийнятих рішень та реалізованих заходів є внутрішньоорганізаційним аспектом розвитку означеної сфери, а отже – широкий громадський загал не має до неї доступу навіть в інформаційному аспекті. Яскраво це демонструється на прикладі Міністерства фінансів України, яке нормативно визначене як секторальний орган у сфері захисту критичної інфраструктури фінансового сектору України, що має низку необхідних повноважень, доступ до аналізу практичної реалізації яких фактично відсутній. Аналогічно й щодо рішень Національного банку України.

На рівні представників влади це обґрунтовується тим, що обізнаність пересічного громадянина про означене не впливає ні на що. Впливає тільки на рівень вразливості цієї інформації і ризик бути розкритою для ворога, бо тоді він зможе прорахувати наші наступні кроки по захисту об'єктів, і це матиме дуже трагічні наслідки [107].

Однак зазначене не створює суттєвих перешкод для визначення представників складу системи суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, адже норми Закону України «Про критичну інфраструктуру» досить чітко встановлюють її обриси. Наразі можна вести мову про класичний їхній розподіл на секторальних (Міністерство фінансів України, Національний банк України), функціональних (наприклад, органи сектору безпеки, кібербезпеки) і уповноваженого (наразі – Державна служба спеціального зв'язку та захисту інформації України) органів або можемо запропонувати альтернативний, який дозволяє їх згрупувати за приналежністю до виконуваних задач на тих, що: 1) є репрезентацією цієї системи (Міністерство фінансів України, Національний банк України, Державна служба спеціального зв'язку та захисту інформації України, Національна комісія з цінних паперів та фондового ринку, Фонд гарантування вкладів фізичних осіб); 2) функціонують для виконання задач секторальних, функціональних та уповноваженого органів захисту критичної інфраструктури в Україні (наприклад, Центр кіберзахисту Національного банку України або Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України); 3) є самостійним міжвідомчим органом з виконанням спеціалізованих функцій (Рада з фінансової стабільності) [229].

Таким чином, маємо такі ключові висновки:

– нами критично аналізується наукова думка щодо сучасної структурно-функціональної характеристики державної політики у сфері захисту критичної інфраструктури в Україні в контексті існування функціонуючих систем у її межах, адже вченими не враховується секторальний аспект досліджуваного питання. Зокрема фінансовий сектор України має, наприклад, систему регуляторів фінансового ринку та окремо Фонд гарантування вкладів фізичних осіб, які сукупно в очах закону не є самостійною інтегрованою системою, однак виконують функції, які

сприяють стійкості та безпеці конкретно критичної інфраструктури фінансового сектору України;

– ключовими суб'єктами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України названо Національний банк та Міністерством фінансів України, однак система таких не обмежується виключно ними;

– пропонуємо використовувати класифікаційний підхід до групування суб'єктів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, який окрім класичної їх диференціації ґрунтується також на альтернативній.

2.4. Форми та методи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України

Реалізація повноважень суб'єктів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України унеможливлена відсутністю адміністративно-правової норми, яка, своєю чергою, зумовлює наявність низки адміністративно-правових відносин різнобічного об'єктно-суб'єктного складу.

Загалом адміністративно-правові відносини донедавна характеризували виключно виконавчо-розпорядчу діяльність у межах державного управління [59, с. 176]. Зараз з цього приводу слушну думку висловлює В. Курило, який виокремлює основну сутність адміністративно-правових відносин, якою виступає формування і зміцнення в українському суспільстві нової доктрини адміністративного права – доктрини публічно-сервісного права, основним призначенням якого є служіння держави інтересам людини [99, с. 16]. Очевидним є той факт, що адміністративне право за радянської доби та адміністративне право за доби незалежної України функціонує за принципово різних умов [74, с. 79]. Тобто тепер виокремлюючи ознаки

адміністративно-правових відносин, необхідно виходити з доктрини адміністративного права та людиноцентристської ідеології, яка формує відповідні правові підходи до здійснення публічного адміністрування. Залежно від того, який прояв або вид публічного адміністрування реалізується – владно-розпорядчий (державноуправлінський) або публічно-сервісний, необхідно й виокремлювати загальні та спеціальні ознаки адміністративно-правових відносин. При цьому варто зауважити, що натепер вже є розподіл ознак вказаних відносин на загальні та спеціальні. Так, до загальних ознак належать ті ознаки, які притаманні будь-яким адміністративно-правовим відносинам, а до спеціальних – ті, які притаманні для певної сфери суспільного життя або галузі. Однак варто підтримати думку О. Дніпрова, що ознаки адміністративно-правових відносин необхідно поділяти на три групи: загальні, спеціальні та особливі. У даному контексті загальними мають бути ті риси, які характеризують будь-які адміністративні правовідносини, спеціальні риси – ті, які впливають із предмета адміністративного права та пов'язані або з виконавчо-розпорядчою діяльністю суб'єктів публічного адміністрування, або з публічно-сервісною діяльністю таких суб'єктів. Своєю чергою, особливими ознаками мають бути ті, які притаманні конкретній сфері суспільного життя [59, с. 176].

Ці загальновідомі положення є актуальними в контексті порушених питань, адже провокують науковий дискурс осягнення глибини взаємозв'язків між елементами механізму здійснення цієї діяльності. Зокрема є суб'єкт, який на основі адміністративно-правової норми та з урахуванням принципів належності вчинення певної дії обирає з арсеналу інструментів той, що якнайкраще допоможе йому реалізувати його права та обов'язки в контексті втілення в правореалізацію відповідних функцій. Все ці аспекти опосередковуються наявністю адміністративно-правових відносин, які, як з'ясовано нами попередньо, вченими виокремлюються в окремий елемент його структури. Ми ж прибічники думки, що адміністративно-правові відносини у сфері захисту об'єктів критичної інфраструктури фінансового

сектору України є сполучною ланкою, що забезпечує цілісність цього механізму, а також різномірні взаємодії у його межах. Причому провідною особливістю таких є їхній динамічний характер, оскільки вони безпосередньо залежать від зовнішніх та внутрішніх викликів, загроз та змін у правовому середовищі.

Однак, адміністративно-правові відносини у сфері захисту об'єктів критичної інфраструктури фінансового сектору України можна також трактувати через призму інструментального підходу, адже у будь-якому разі змістовний їх контекст залежить від повноважень конкретного представника національної системи захисту критичної інфраструктури фінансового сектору України, який застосувавши/використавши необхідну форму та доцільний метод діяльності активізує чи забезпечує їхній розвиток.

Зауважимо, що наукова доктрина вміщує різні погляди на категорії «форми», «методи» та «інструменти» в контексті використання їх в категорійному апараті науки адміністративного права.

Як зазначає К. Бондаренко, форми та методи посідають вагоме місце в інституті державного управління, оскільки допомагають визначити механізм здійснення державного управління, простежити його динаміку та проаналізувати сутність. Річ у тім, що поняття «форма» використовується майже всіма галузями знань, оскільки нерозривно пов'язується з категорією «зміст». Філософія розуміє форму як упорядкованість змісту, його внутрішній зв'язок і порядок. Тобто без вивчення форми будь-якого явища неможливо осягнути його сутність та зміст. Не менш важливим є поняття методів, які є засобами, за допомогою яких досліджуються й аналізуються навіть найскладніші категорії. Зокрема вчений вказує, що через стрімкий розвиток державного управління на сучасному етапі розвитку України вивчення форм і методів державного управління залишається актуальним для науки адміністративного права [19, с. 112].

Відразу слід уточнити, що більшість вчених адміністративістів підтримують думку відмови від апелювання у межах правової доктрини

України категорією «державне управління», сприймаючи її або застарілим аналогом категорії «публічне адміністрування», або самостійним правовим явищем, що вичерпало свою соціальну значимість [288, с. 61]. Як приклад, за твердженнями О. Митя та О. Світового: «державне управління є одним із найскладніших інститутів і категорій адміністративного права у зв'язку з комплексним характером, специфікою суб'єктів і об'єктів державного управління і взаємозв'язків між ними. Трансформаційні процеси, що відбуваються в українській державі і суспільстві, адміністративна реформа, що триває, зумовили науковий пошук нових підходів до розуміння суті державного управління і можливостей його оновлення, що виразилося в підвищенні уваги до такої категорії як «публічне адміністрування» [113, с. 124]. Вчений П. Петровський також зазначає: «За переконаннями більшості вчених державне управління реформується в публічне» [134, с. 21]. За іншого підходу державне управління – це організація державного сектору, що передбачає відсутність варіативності моделі поведінки чи організаційної структури об'єкта управління, репрезентує встановлення та виконання імперативної норми у виключних сферах, що становлять державний інтерес. Такими сферами є ті, що повністю або частково апріорі не можуть бути публічними – внутрішня безпека, сфери із областями, що місять інформацію, яка є державною таємницею, територіальний поділ адміністративних одиниць, економічні аспекти забезпечення конкурентоспроможності держави, міжнародні відносини [47, с. 36; 288, с. 61].

Одночасно з поняттям «публічне адміністрування» вчені нерідко звертаються до поняття «урядування», під яким розуміється процес прийняття і реалізації рішень. Воно є дещо ширше ніж поняття «адміністрування» та «управління», адже зосереджується на формальних і неформальних суб'єктах, структурах та зв'язках, що утворюються для прийняття та реалізації рішень [195; 205, с. 34].

З огляду це маємо, що вчені виокремлюють форми, методи, інструменти та способи реалізації державного управління, публічного

адміністрування, публічного врядування та окремо – адміністративної діяльності. Причому у більшості випадків мова йде про зміст та сутність останніх, які іменуються різними термінологічними одиницями.

Загалом у науковій літературі існують різні точки зору щодо визначення форм діяльності [87, с. 142]. Однак за загальним правилом, адміністративно-правова форма – це юридичне відображення конкретних дій і рішень суб'єктів адміністративного права у процесі здійснення виконавчої і розпорядчої діяльності [4, с. 147]. А. Гук зазначає, що будь-яка адміністративно-правова форма являє собою юридично значимі способи реалізації суб'єктами адміністративного права своїх повноважень, прав і обов'язків, що відображають особливості їх правового статусу. У правовій науці, на відміну від науки державного управління, правові форми втілюються в життя через різного характеру дії правомочних представників органів управління – службових осіб. Отже, зовнішнє вираження управлінської діяльності в конкретних практичних діях іменується формою управління, і тут форма розглядається як зовнішнє вираження будь-якого змісту [46, с. 81].

Своєю чергою, методи управління ідентифікуються способами: аналізу та оцінювання управлінської ситуації; використання правових і організаційних форм впливу на свідомість і поведінку людей [178, с. 145]. За функціональним змістом В. Малиновський розподіляє методи публічного управління на: адміністративні (розпорядчі, регламентаційні, нормативні); економічні (індикативне планування, державне регулювання, грошово-кредитна та фінансова політика, захист та заохочення конкуренції, ціноутворення, податкова політика, економічне стимулювання); правові (правове регулювання, переконання і примус, субординація і координація); соціально-психологічні (соціальні, морально-етичні, психологічні) [110, с. 419]. О. Кузьмін, О. Мельник класифікують методи менеджменту за: напрямом впливу (прямого або непрямого); способом урахування інтересів осіб (за матеріальними, владними, моральними ознаками); формою впливу

(кількісні, якісні); характером впливу (економічні, технологічні, соціально-психологічні, адміністративні) [106, с. 485]. А. Мельник також акцентує увагу на важливості використання у публічному управлінні соціально-політичних методів [97, с. 235; 178, с. 147].

Причому В. Конопльов зауважує, що проблему методів будь-якої діяльності можна розглядати з точки зору співвідношення більш загальних понять – мети та засобів її досягнення. У загальноприйнятому розумінні термін «метод» означає спосіб чи прийом здійснення чого-небудь. Виходячи з цього, під методами будь-якої діяльності слід розуміти способи, прийоми, засоби, які використовуються для досягнення поставленої мети і становлять зміст цієї діяльності [85, с. 180]. Власне тому поширеною є думка, що методи адміністративної діяльності – це прийоми та способи цілеспрямованого впливу владних суб'єктів на підпорядковані їм об'єкти, за допомогою яких забезпечується належне виконання зовнішньоадміністративних та внутрішньоорганізаційних завдань [87, с. 147] суб'єктів владних повноважень (публічної адміністрації).

Проте варто вказати, що безпосередній вплив на об'єкт управління здійснюється шляхом застосування суб'єктами управління необхідних інструментів [97, с. 237], які трактуються як засоби практичної реалізації управлінського рішення. Тобто до інструментів публічного управління відносять засоби, прийоми та методи, які передбачають трансформацію знань та дій органів влади для досягнення конкретної мети. Серед інструментів публічного управління виокремлюють дві підгрупи: загальні (універсальні) і локальні. Загальні інструменти управління – це чинні, закріплені в правових актах норми і правила управлінської діяльності, які мають форму законів, статутів, інструкцій, обмежень тощо. Локальні інструменти управління мають частковий вияв, підсилюючи виконання більш вагомого управлінського рішення, і можуть набувати форми постанов, наказів, розпоряджень, угод, контрактів, нарад тощо [211].

Е. Казміришин зауважує, що заміна категорій «форми і методи державного управління» категорією «інструменти публічного адміністрування» або її аналогом «адміністративно-правові інструменти» є логічним наслідком розвитку адміністративного права України, наближення його до європейського адміністративного простору [74, с. 79]. Зокрема правомірність застосування терміна «інструменти діяльності публічної адміністрації» замість «форм державного управління» І. Патерило обґрунтовує тим, що, по-перше, публічне управління в Україні представлено як органами виконавчої влади, так і відмінними від них суб'єктами (органи законодавчої та судової влади, органи місцевого самоврядування). По-друге, в процесах публічного управління передбачається участь фізичних та інших юридичних осіб. По-третє, публічні адміністрації поряд з виконавчо-розпорядчими функціями надають різноманітні послуги фізичним і юридичним особам та здійснюють державно-приватне партнерство. Основні ознаки інструментів публічної адміністрації: застосовуються безпосередньо нею; мають публічно-правовий характер; регулюються нормами адміністративного права; пов'язані з компетенцією органу управління, сферою та метою діяльності; призводять до настання правових наслідків, фактичних результатів [97, с. 237; 132, с. 97].

З усім тим, наукова полеміка з цього питання є досі актуальною через теоретичний характер означених категорій та відсутність єдиної концептуальної основи, яка б відповідала на основі дослідницькі запити. Зокрема маємо підтвердження, що за історичним контекстом розвитку адміністративного права категорії «форм» та «методів» мали власне і достатньо обґрунтоване поняттєве визначення, яке втратило своє значення з перехідними етапами становлення України як країни сервісного типу.

Варто відмітити те, що категорія «адміністративно-правовий інструмент» об'єднує широкий перелік інструментів діяльності публічної адміністрації, які різняться за своєю юридичною природою та призначенням. У науковій літературі можна зустріти різні підходи до виокремлення видів

інструментів діяльності публічної адміністрації. На думку Т. Карабіна, до основних видів інструментів діяльності публічної адміністрації необхідно віднести: нормативні акти, адміністративні акти та адміністративні договори [75, с. 164–169]. На думку І. Патерило, до різновидів інструментів діяльності публічної адміністрації варто віднести: підзаконні нормативно-правові акти, адміністративні акти, адміністративні договори, адміністративні акти-дії та акти-плани [132, с. 175]. Схожу систему інструментів публічного адміністрування можна зустріти у дослідженнях Р. Мельника та В. Галуцького. Так, вчені до переліку інструментів публічного адміністрування відносять: 1) нормативно-правовий акт; 2) адміністративні акти; 3) адміністративні договори; 4) плани; 5) фактичні дії [2, с. 160; 111, с. 188]. До цього переліку Є. Петров додає також приватноправові інструменти [74, с. 80; 133, с. 198].

Таким чином, за традиційного підходу основними інструментами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є видання нормативно-правових та індивідуальних актів, укладання адміністративних договорів та затвердження актів-планів, в основу яких закладено відповідний спосіб їхньої реалізації. Таким може бути, наприклад, контроль та нагляд, моніторинг, планування, консультування, координація, співпраця тощо.

Зокрема, наприклад, у сфері виявлення незаконно отриманих доходів та запобігання фінансуванню тероризму Національний банк здійснює фінансовий моніторинг, щоб запобігти використанню банківської системи України для легалізації доходів, одержаних злочинним шляхом. Здійснюючи фінансовий моніторинг, банки і небанківські фінансові установи перевіряють клієнтів та аналізують їхні фінансові операції. У разі виявлення підозрілих операцій банки інформують Державну службу фінансового моніторингу та правоохоронні органи України [218].

Своєю чергою, функціональні органи залучають фахівців департаменту захисту критичної інфраструктури Державної служби спеціального зв'язку та захисту інформації України для проведення моніторингу на місцях щодо

захисту об'єктів критичної інфраструктури. Вони разом проводять відповідні обстеження [107]. Також із залученням секторальних органів реалізуються спільні проекти. Наприклад, Державної служби спеціального зв'язку та захисту інформації України, Національний банк та Кіберполіція створили прості інструкції, які допоможуть розпізнавати злочинні схеми, а також надавати або отримувати допомогу в інтернеті безпечно, адже під час війни зловмисники постійно спекулюють на темі фінансової допомоги українцям, які постраждали від дій РФ [236]. Окрім того, в функції департаменту захисту критичної інфраструктури Державної служби спеціального зв'язку та захисту інформації України також входить координація роботи з міжнародними партнерами. Завдяки цьому не всі разом біжать до донорів із сотнями різнопланових прохань, а єдиний уповноважений орган збирає інформацію про існуючу потребу з усіх та ініціює виділення допомоги відповідним міністерствам та іншим отримувачам [107]. У зазначених випадках з початку видається нормативний акт, реалізація якого вимагає застосування відповідного методу втілення його приписів.

Однак припускаємо про можливість розгляду порушеної проблематики під іншим кутом зору. Зокрема категорії «форми» та «методи» в контексті адміністративно-правового захисту є сенс розглядати з позиції функціональної єдності, що дозволяє інтерпретувати їх зміст через категорію «інструментів», тобто знарядь, які є застосовними уповноваженими суб'єктами задля виконання їх завдань та функцій. У цьому випадку знаряддям є правовий засіб, який як явище-регулятор правової дійсності, перетворює правову норму в конкретні дії та рішення, які реалізуються на практиці.

Власне, за такої інтерпретації їхньої сутності інструментальний бік адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України стає основоположним при ідентифікації юридичної природи механізму його здійснення.

Уточнимо, що в юридичній літературі відсутня єдність у поглядах на класифікацію правових засобів, але ми зупинимось на таких, які є найбільш поширеними серед науковців у галузі теорії права. В залежності від ступеня складності їх поділяють на первинні (прості) і комплексні (складні). Якщо до перших належать найпростіші і неподільні приписи – суб'єктивні права та юридичні обов'язки, заохочення і покарання, пільги і заборони тощо, то до других – комбіновані, що складаються в свою чергу з найпростіших – договір, норма, інститут, правовий режим і ін. По виконуваний ролі вони поділяються на регулятивні (дозволи) та охоронні (заходи захисту); за предметом правового регулювання – на конституційні, адміністративні, цивільні, кримінальні та ін.; за характером – на матеріально-правові (рекомендації) і процесуальні (позов); значущості наслідків – на звичайні (штраф) і виняткові (смертна кара); за часом дії – на постійні (громадянство) і тимчасові (премія); по виду правового регулювання – на нормативні (встановлені в нормах права заборони) й індивідуальні (акт застосування права, акти реалізації прав і обов'язків); інформаційно-психологічної спрямованості – на стимулюючі (пільги) та обмежують (зупинення) тощо [22, с. 191].

Також виокремлюють засоби впливу та засоби реалізації права. Припускаємо, що у контексті першого йдеться про виявлення, запобігання та реагування на потенційні загрози або порушення роботи об'єктів критичної інфраструктури фінансового сектору України. Тоді як засоби реалізації права репрезентують практичне втілення встановлених правових норм.

З усім тим найбільший науковий інтерес цього дослідження об'єктивують заходи захисту, які є застосовними для забезпечення схоронності об'єктів критичної інфраструктури фінансового сектору України. Зазначимо, що Закон України «Про критичну інфраструктуру» щодо порушеного питання містить такі положення:

– заходи охорони диференціюються на режимні, інженерні, інженерно-технічні та інші заходи;

– безпосередньо захисними заходами є заходи із захисту інформації та кіберзахисту об'єктів критичної інформаційної інфраструктури;

– державна політика у сфері захисту критичної інфраструктури спрямовується на формування комплексу організаційних, нормативно-правових, інженерно-технічних, ресурсних, інформаційно-аналітичних та методологічних заходів;

– виокремлюються також: 1) заходи з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об'єктах критичної інфраструктури; 2) заходи реагування на кризову ситуацію; 3) заходи щодо повернення параметрів функціонування критичної інфраструктури до штатного режиму; 4) заходи із функціонування відповідних систем обміну інформацією, моніторингу рівня безпеки об'єктів критичної інфраструктури; 5) заходів щодо забезпечення безпеки і стійкості критичної інфраструктури; 6) заходи з реагування на інциденти; 7) заходи із захисту повітряного простору над визначеними об'єктами критичної інфраструктури; 8) евакуаційні заходи у разі виникнення надзвичайних ситуацій; 9) заходи з фізичного захисту, протидії загрозам, ефективного зниження та контролю за ризиками безпеки; 10) спільні заходи із захисту критичної інфраструктури та припинення протиправних дій проти об'єктів критичної інфраструктури; 11) заходи примусового виконання рішень; 12) заходи з підвищення рівня захищеності тощо;

– моніторинг рівня безпеки об'єктів критичної інфраструктури здійснюється шляхом проведення оцінки стану захищеності об'єктів критичної інфраструктури;

– джерелами фінансування робіт і заходів із забезпечення захисту критичної інфраструктури є кошти державного і місцевих бюджетів, власні кошти операторів критичної інфраструктури, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством [166].

Своєю чергою, Національний план захисту та забезпечення безпеки та стійкості критичної інфраструктури передбачає, що відповідні заходи об'єктивуються через виконання завдань, закріплених за відповідальними суб'єктами. Наприклад, для удосконалення законодавства, що регламентує діяльність суб'єктів національної системи захисту критичної інфраструктури Національний банк мав прийняти відповідний акт, який забезпечить визначення вимог до порядку розроблення паспорта безпеки на об'єкти критичної інфраструктури, змісту і строків подання його банками, іншими юридичними особами, що провадять діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких він здійснює. Також секторальні органи у цій сфері, як самостійно, так і взаємодії з іншими суб'єктами, уповноважені на: 1) складення та ведення переліків об'єктів критичної інфраструктури фінансового сектору; 2) подання повідомлень про внесення відомостей щодо об'єкта критичної інфраструктури до Реєстру об'єктів критичної інфраструктури; 3) погодження паспорта безпеки на об'єкт критичної інфраструктури; 4) розроблення та встановлення вимог, норм, регламентів захисту критичної інфраструктури; 5) створення структурних підрозділів з питань захисту критичної інфраструктури; 6) подання операторам критичної інфраструктури рекомендацій з питань захисту критичної інфраструктури та обов'язкових до виконання вимог щодо усунення причин і умов, які порушують стійкість критичної інфраструктури; 7) проведення моніторингу рівня безпеки об'єктів критичної інфраструктури; 8) затвердження планів проведення моніторингу рівня безпеки об'єктів критичної інфраструктури фінансового сектору; 9) підготовку та подання щорічного звіту щодо забезпечення захисту критичної інфраструктури у фінансовому секторі; 10) утворення за потреби консультативних рад з питань захисту критичної інфраструктури при секторальних органах у сфері захисту критичної інфраструктури; 11) розроблення та затвердження у відповідних секторах планів взаємодії та підтримання життєво важливих функцій та послуг на випадок порушення функціонування об'єктів критичної

інфраструктури фінансового сектору; 12) розроблення та затвердження галузевих, регіональних планів та програм з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань та тренувань; 13) розроблення та затвердження планів взаємодії функціональних органів у сфері захисту критичної інфраструктури для всіх режимів функціонування критичної інфраструктури; 14) вжиття заходів, спрямованих на забезпечення функціонування системи обміну інформацією та взаємодії між суб'єктами національної системи захисту критичної інфраструктури; 15) підготовку пропозицій щодо проектних ризиків та загроз критичній інфраструктурі національного рівня та проведення щорічної оцінки ризиків і загроз критичній інфраструктурі національного рівня; 16) розроблення та затвердження проектних загроз критичній інфраструктурі фінансового сектору; 17) затвердження секторальних програм підготовки персоналу щодо забезпечення стійкості та захисту критичної інфраструктури фінансового сектору; 18) розроблення та затвердження плану заходів цивільного захисту, пожежної та техногенної безпеки об'єктів критичної інфраструктури та його перегляд; 19) організацію та забезпечення охорони від пожеж об'єктів критичної інфраструктури в установленому Кабінетом Міністрів України порядку; 20) розроблення, затвердження та погодження із заінтересованими органами місцевих планів взаємодії залучених суб'єктів у кризовій ситуації з метою підтримання життєво важливих функцій та надання життєво важливих послуг, планів відновлення функціонування критичної інфраструктури; 21) затвердження за результатами погодження із заінтересованими органами програм навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування; 22) створення системи оповіщення населення та суб'єктів господарювання про інциденти та кризові ситуації на об'єктах критичної інфраструктури [157].

Аналізуючи положення Щорічного звіту Національного банку за 2022 рік маємо інформацію, що у лютому 2022 року були застосовними розроблені плани з підтримання безперебійної діяльності критичної інфраструктури. Уточнюється, що з перших хвилин повномасштабного збройного нападу росії найбільш пріоритетними завданнями у частині критичної інфраструктури ринків капіталу стали гарантоване запобігання втраті даних щодо фінансових інструментів та розгортання резервних потужностей для забезпечення безперервної діяльності. Наприклад, з метою підтримання ефективної роботи фінансової системи у 2022 році було скасовано тарифи на депозитарні послуги та послуги щодо обліку та обігу депозитних сертифікатів. Відміна тарифікації на депозитарні послуги дала змогу знизити витрати для кінцевих вкладників у облігації внутрішніх державних позик України та сприяла розширенню кола покупців облігацій внутрішніх державних позик України та обсягів запозичень Уряду України через розміщення цих цінних паперів. Акцентується, що значним проривом у 2022 році стало впровадження Депозитарієм Національного банку сучасних сервісів API-взаємодії із системами автоматизації депозитарних установ, а також викуп військових облігацій уряду на суму 400 млрд грн. Монетизація військових облігацій внутрішніх державних позик України дала змогу підтримати обороноздатність країни, забезпечити безперебійне функціонування критичної інфраструктури та системи державних фінансів загалом. Також зазначається, що на виконання вимог Закону України «Про критичну інфраструктуру» постановою Правління Національного банку України від 04 жовтня 2022 року № 169 затверджено зміни до Положення № 346, якими, зокрема, доповнено підстави для застосування Національним банком до банків заходів впливу за порушення ними законодавства України з питань захисту критичної інфраструктури, кіберзахисту та інформаційної безпеки [183, с. 90–91].

Річний звіт Національного банку за 2023 рік свідчить, що як і в попередньому році, пріоритетним завданням для елементів критичної

інфраструктури ринків капіталу залишалось підтримання безперебійної діяльності в умовах ракетних обстрілів, блекаутів та інших викликів воєнного часу. Тому всі елементи інфраструктури ринків капіталу продовжували вдосконалювати резервні потужності і протоколи роботи для забезпечення безпечної і безперервної діяльності. У результаті навіть в умовах воєнного стану 2023 рік став роком повноцінного функціонування ринків капіталу, а його інфраструктурним елементам удавалося удосконалювати наявні та впроваджувати нові сервіси. У 2023 році депозитарій Національного банку продовжував безперебійно здійснювати облік та обслуговувати обігу облігацій внутрішньої державної позики, у тому числі військових облігацій. Завдяки злагодженій взаємодії та спільним зусиллям уряду та Національного банку вдалося активізувати внутрішній борговий ринок [217, с. 102].

Серед основного також можна виділити те, що:

– повністю реалізовано проєкт «POWER BANKING», який забезпечує безперебійну роботу банків навіть у критичних ситуаціях – у разі блекаутів, кібератак чи відсутності зв'язку. Екстрені протоколи ретельно опрацьовано;

– в умовах безпрецедентної протидії агресору Центр кіберзахисту Національного банку та Команда реагування на кіберінциденти в банківській системі України (CSIRT-NBU) працювали в посиленому режимі та постійно моніторили ризики та кіберзагрози для інформаційних ресурсів і ресурсів банківської системи України, забезпечували вжиття своєчасних та адекватних заходів реагування та протидії. Упродовж 2023 року CSIRT-NBU виявив та провів аналіз близько 14 925 (у 2022 році – 11 280) зразків шкідливого програмного забезпечення та своєчасно інформував банки України про виявлені інциденти кібербезпеки й зафіксовані спроби вчинення кібератак. До платформи обміну інформацією про актуальні кіберзагрози «Malware Information Sharing Platform & Threat Sharing» (MISP-NBU), якою активно користуються банки, надіслано близько 116 повідомлень про кіберінциденти та індикатори кіберзагроз;

– запроваджено єдиний порядок обліку відомостей про об’єкти критичної інформаційної інфраструктури в банківській системі України та координації діяльності банків, Національного банку з питань, пов’язаних із забезпеченням їх кіберзахисту; забезпечено формування та підтримання в актуальному стані реєстру об’єктів критичної інформаційної інфраструктури в банківській системі України; для забезпечення кіберстійкості Національного банку запроваджено сучасні процедури оцінювання та оброблення ризиків інформаційної безпеки та кіберризиків інформаційних ресурсів, виявлення та оброблення вразливостей інформаційних систем, управління правами доступу до інформаційних ресурсів. Оновлено принципи забезпечення інформаційної безпеки та кіберзахисту під час віддаленої роботи [217, с. 135–136].

Таким чином, бачимо, що інструментальний бік механізму адміністративно-правового захисту об’єктів критичної інфраструктури фінансового сектору України характеризується через зв’язок із категоріями «форми», «методи», які мають розглядатись з позиції функціональної єдності, як правові засоби, що забезпечують прийняття та реалізацію ефективних управлінських рішень.

Однак маємо акцентувати на необхідності диференціації категорій «форми», «методи» та «інструменти» в контексті їх використання в управлінсько-організаційному, регуляторному чи іншому державно-владному процесі, адже у кожному з таких їм можна надати специфічного значення та функціонального навантаження.

Таким чином, маємо такі ключові висновки:

– у випадку цього дослідження інструментальний контекст адміністративно-правового захисту об’єктів критичної інфраструктури фінансового сектору України репрезентується через систему варіантів зовнішнього оформлення управлінського рішення та конкретного підходу, застосовного до досягнення поставлених у ньому цілей. Йдеться про знаряддя, яке покликане реалізувати поставлену задачу;

– цілями управлінського рішення у сфері захисту об'єктів критичної інфраструктури фінансового сектору України може бути як внутрішньоорганізаційне питання, що потребує вирішення, так і зовнішньо спрямовані завдання.

Висновки до Розділу 2

1. Визначено, що нормативно-правовими основами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є сукупність правових документів різної юридичної сили, виданих (прийнятих) з метою врегулювання питань: а) кіберзахисту, інформаційної безпеки, інституційної збалансованості цієї сфери загалом; б) реалізації міжвідомчих механізмів взаємодії між регуляторами та іншими суб'єктами національної системи її захисту; в) управління та моніторингу ризиків, пов'язаних із фінансовими операціями та діяльністю установ, які входять до переліку об'єктів критичної інфраструктури; г) контрольно-наглядової діяльності у цій сфері, включаючи імплементацію міжнародних стандартів та рекомендацій.

2. Запропоновано нормативно-правові основи захисту об'єктів критичної інфраструктури фінансового сектору України диференціювати на:

- 1) міжнародні – наприклад, Рекомендації та Керівництва Групи з розробки фінансових заходів боротьби з відмиванням грошей, акти Міжнародного валютного фонду, Світового банку, Міжнародної організації з стандартизації;
- 2) регіональні – наприклад, Директива Ради ЄС 2008/114/ЄС, Директива Ради ЄС 2016/1148, Директива Ради ЄС 2018/843, Регламент ЄС 2021/23, Директива Ради ЄС 2022/2557, Рекомендації Ради ЄС 2023/C 20/01);
- 3) національні – законодавство у сферах сталого розвитку, національної безпеки та її складових, захисту критичної інфраструктури, регулювання ринку фінансових послуг, бюджетного регулювання, економічного розвитку

та протидії фінансуванню злочинів (наприклад, Закони України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», «Про правовий режим воєнного стану», «Про критичну інфраструктуру», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про банки і банківську діяльність», «Про платіжні послуги», «Про фінансові послуги та фінансові компанії», «Про Національний банк України»; Укази Президента України «Про Стратегію сталого розвитку «Україна - 2020»» від 12 січня 2015 року № 5/2015; «Про Цілі сталого розвитку України на період до 2030 року» 30 вересня 2019 року № 722/2019; «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості»» від 27 вересня 2021 року № 479/2021; «Про рішення Ради національної безпеки і оборони України від 11 серпня 2021 року «Про Стратегію економічної безпеки України на період до 2025 року»» від 11 серпня 2021 року № 347/202; постанови Кабінету Міністрів України «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» від 3 вересня 2014 року № 411; «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 року № 518; «Деякі питання об'єктів критичної інфраструктури» від 9 жовтня 2020 року № 1109; «Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури» від 14 жовтня 2022 року № 1174; «Про затвердження Методики оцінювання фіскальних ризиків» від 24 квітня 2019 року №351; «Про затвердження Методики оцінювання фіскальних ризиків, пов'язаних з діяльністю суб'єктів господарювання державного сектору економіки» від 11 січня 2018 року № 7; «Про затвердження Національної економічної стратегії на період до 2030 року» від 3 березня 2021 року № 179; рішення Правління Національного банку України «Про затвердження Стратегії розвитку фінансового сектору України до 2025 року» від 29 серпня 2023 р. № 299-рш та багато інших).

3. З системи таких нормативно-правових основ виокремлено в окрему групу ті, що є функціональними, тобто мають безпосереднє відношення до врегулювання питань здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України (наприклад, Положення про визначення об'єктів критичної інфраструктури в банківській системі України, Положення про організацію кіберзахисту в банківській системі України, Положення про порядок визначення Національним банком України юридичних осіб, що є критично важливими для функціонування економіки та забезпечення життєдіяльності населення в особливий період, затверджені відповідними постановами Правління Національного банку України).

4. З'ясовано, що Зелена книга з питань захисту критичної інфраструктури в Україні є документом, спрямованим на формування систематичного підходу до захисту критичної інфраструктури країни загалом та фінансового сектору – зокрема. Документ розроблений з метою окреслення основних проблем, викликів та підходів до захисту критичної інфраструктури в умовах сучасних загроз та ризиків, включаючи терористичні акти, природні катастрофи, техногенні аварії та інші небезпеки. Він також наголошує на кількох важливих аспектах: 1) мультидисциплінарний підхід, – захист об'єктів критичної інфраструктури потребує інтеграції знань та досвіду з різних галузей, включаючи безпеку, інженерію, економіку та інформаційні технології; 2) превентивні заходи, – важливість запобігання загрозам через вчасне виявлення вразливостей та їх усунення; 3) освіта та підготовка, – необхідність постійного навчання та підвищення кваліфікації фахівців, що займаються захистом об'єктів критичної інфраструктури. Узагальнено, що Зелена книга з питань захисту критичної інфраструктури в Україні є важливим стратегічним документом, який задає напрямки розвитку системи захисту критичної інфраструктури, зокрема і фінансового сектору.

5. Виявлено, що європейські та міжнародні документи забезпечують комплексний підхід до захисту критичної інфраструктури фінансового сектору, включаючи регулювання, управління ризиками, інформаційну безпеку та заходи протидії злочинній діяльності. Вони встановлюють стандарти, які сприяють зміцненню стабільності та стійкості фінансових систем у глобальному масштабі. Своєю чергою, констатується, що вітчизняне законодавство перебуває у процесі активної адаптації встановлених та рекомендованих міжнародних стандартів до національної правової системи, проте ще не повністю відповідає всім висунутим вимогам до результативності здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. Уточнено, що базовий рівень захисту об'єктів критичної інфраструктури фінансового сектору ще не досяг належного рівня відповідності, а тому про повноцінний перехід до концепції стійкості наразі вести мову ще занадто рано, адже першочергово необхідно створити функціональну базу захисних заходів, що дозволять ефективно управляти ризиками на всіх рівнях. Це свідчить про необхідність розробки та впровадження механізмів, стратегій та планів захисту об'єктів критичних інфраструктур фінансового сектору, зокрема і в контексті актуальності протидії конкретним загрозам (наприклад, кібератаки чи збройні конфлікти). Наразі це питання перебуває у площині правового вакууму, що створює розрив між наявними механізмами її захисту та вимогами стійкості, що декларуються на міжнародному рівні.

6. Доведено, що нормативно-правові основи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України мають дуальність інтерпретаційної складової, де: 1) ідейно-концепційний складник визначений як актуальний, належно сформований та такий, що не вимагає додаткової уваги в контексті оптимізаційних змін якісно новим ідеологічним наповненням; 2) практико-реалізаційний складник відзначається фрагментарністю, відсутністю публічності механізмів прояву

означеної діяльності, а також недостатньою інтеграцією з міжнародними стандартами у сфері захисту критичної інфраструктури.

7. Узагальнено, що нормативно-правові основи є репрезентацією чинних регуляторних або рекомендаційних актів, які встановлюють правила, стандарти та вимоги до реалізації чи утримання від певної дії уповноважених суб'єктів у межах здійснення ними адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. Уточнюється, що наявні нормативно-правові основи захисту об'єктів критичної інфраструктури фінансового сектору України є результатом здійснення нормативно-правового забезпечення розвитку досліджуваного кола адміністративно-правових відносин, а основоположними з таких є акти секторальних органів, проте основна проблема полягає у відсутності їх публічності.

8. Проаналізовано провідні наукові позиції на предмет ідентифікації змісту та сутності категорії «принцип» та «принципи права». Констатовано, що принципи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України можна визначити через категорію «правило», яка поєднує своїм змістом ідейний, засадничий та імперативний контекст. Дефініція порушеного питання представлена так: «це фундаментальні правила, які визначають особливості, специфіку та критерії ефективності здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України».

9. Досліджено наукову та нормативну доктрину на предмет виявлення системи принципів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. Виявлено відсутність належної уваги з боку нормотворців та дослідників до специфіки цієї проблематики.

10. Запропоновано принципи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України визначати через загальнотеоретичні (загальноправові), галузеві та спеціальні принципи.

11. Загальнотеоретичними (загальноправовими) принципами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України названо ті, що віддзеркалюють особливості сучасного стану державотворення в Україні, особливості його ідеологічного підґрунтя. До числа таких віднесено принцип верховенства права, принцип законності, принцип правової визначеності та прозорості. Коротко схарактеризовано кожен з таких.

12. Галузевими принципами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України визначено групу з таких, що акцентують на особливостях забезпечення безпеки та стійкості суспільного розвитку, регулювання ринку фінансових послуг та загальних вимогах до діяльності суб'єктів національної системи захисту критичної інфраструктури в Україні. Серед ключових з-поміж таких виділено принцип пропорційності; принцип ефективності; принцип координованості; принцип розподілу відповідальності; принцип взаємодії; принцип завчасної превенції; принцип безпеки, захисту та охорони інформації з обмеженим доступом; принцип оперативності; принцип своєчасності; принцип передбачуваності; принцип адаптивності та мобільності; принцип безперервності; принцип ресурсної достатності; принцип довгострокової стійкості; принцип гнучкості; принцип системності та цілісності; принцип безперервного вдосконалення.

13. Визначено зміст та особливості галузевих принципів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. Наприклад, стверджується що: 1) принцип ефективності визначає необхідність вибору із декількох варіантів діяльності той, практична реалізація якого забезпечує найвищий рівень максимально досяжного або заздалегідь запланованого результату; 2) принцип координованості передбачає узгодження взаємодій між різними суб'єктами права задля досягнення збалансованості у межах прийняття та реалізації управлінських рішень; 3) принцип розподілу відповідальності ідентифікує

роль та межі сфери дії кожного учасника взаємодії чи процесу, щоб забезпечити ефективне прийняття рішення та його виконання; 4) принцип безпеки, захисту та охорони інформації з обмеженим доступом надає певній інформації статусу такої, що має обмеження до отримання доступу до неї, а також об'єктивує наявність процесів, спрямованих на її захист; 5) принцип безперервності встановлює обов'язок для суб'єкта владних повноважень забезпечувати безперервне виконання своїх завдань та функцій; 6) принцип довгострокової стійкості – орієнтує політичних та адміністративних акторів на вектор розвитку суспільних відносин, що характеризується здатністю збереження та накопичення необхідних ресурсів для підтримання адекватного рівня рівноваги між сьогоденням та майбутнім. Передбачає наявність планів розвитку та реалізації окремих механізмів, відхилення від реалізації яких сприймається як порушення цілісності процесу розвитку.

14. Констатується, що проблематика реалізації принципу безпеки, захисту та охорони інформації з обмеженим доступом є особливо актуальною для досліджуваної сфери, адже має кореляційний взаємозв'язок із принципом публічності, який вимагає від суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України дотримання балансу між забезпеченням відкритості і прозорості їхньої діяльності та збереженням секретності. Зокрема зауважено, що не вся інформація має бути секретною, адже Закон України «Про критичну інфраструктуру» акцентує на праві громадського нагляду у цій сфері й враховує особливості захисту державної таємниці. З'ясовано, що про обмеження доступу до інформації, яка такою не є, положень немає. Висунуто припущення, що щонайменше широкий громадський загаль має знати про дату прийняття, номер акту про утворення та коротку характеристику основ діяльності Управління захисту критичної інфраструктури як організаційної одиниці Національного банку України. Уточнюється, що наразі інформування громадськості про результати діяльності щодо реалізованих заходів захисту об'єктів критичної інфраструктури фінансового сектору

України принаймні про загальні дані, які не порушують вимоги безпеки, здійснюється через опубліковані звіти про стан фінансової стабільності та загальний річний звіт діяльності Національного банку, а не окремий щорічний звіт щодо забезпечення захисту критичної інфраструктури у фінансовому секторі. Стверджується, що інформація, яка подається у їх межах є недостатньою для інформування громадськості про реалізовані заходи. Проте наголошено, що детальна інформація про вразливості та наявні прогалини в механізмах захисту об'єктів критичної інфраструктури фінансового сектору України є небезпечною з точки зору високого рівня ризику можливих зловживань.

15. Визначено, що спеціальними принципами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є ті, що мають безпосереднє відношення до процедур забезпечення організаційної та функціональної стійкості об'єктів критичної інфраструктури, ідентифікації її вразливості, обміну інформацією зовнішнього та внутрішнього рівнів, управління ризиками та здійснення превентивної діяльності на постійній основі. Такими названо принцип організаційної стійкості, принцип інституційної спроможності регуляторів, принцип цільової спрямованості, принцип комплексного моніторингу, принцип динамічності, принцип макропруденційного регулювання, принцип сприяння прибутковості; принцип мінімізації фінансового стресу, принцип очікуваних збитків (втрат), принцип вільного руху капіталу. Стверджується, що, наприклад: 1) принцип цільової спрямованості встановлює вимогу реалізації захисної дії виключно задля досягнення визначеної мети та виконання поставленого завдання, тобто це встановлення обов'язку її практичної реалізації тільки у межах необхідної площини; 2) принцип комплексного моніторингу декларує підхід, за якого має здійснюватись своєчасна ідентифікація загроз, оцінка ризиків для вжиття завчасних заходів для зменшення їхнього впливу на фінансову систему та діяльність об'єктів її системи, порушення функціональності яких матиме значні негативні

наслідки; 3) принцип динамічності передбачає періодичну перевірку встановлених стандартів, правил та вимог до захисту критичної інфраструктури, приведення їх у відповідність до актуальних реалій та швидкоплинних змін; 4) принцип сприяння прибутковості встановлює кореляцію між необхідністю вжиття охоронних чи захисних заходів та економічною доцільністю, вирівнюючи баланс між ними; 5) принцип мінімізації фінансового стресу визначає вимогу зменшення рівня напруги у фінансовому секторі України стабілізуючими заходами; 6) принцип очікуваних збитків (втрат) допускає, що заходи безпеки матимуть потенційну економічну збитковість.

16. Окремо зазначається, що запропонована варіація досліджуваних принципів є суб'єктивною та не вичерпною, адже, наприклад, окремо можна виділити принципи діяльності Національного банку, як основного суб'єкта системи здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України або деталізувати принципи «культури управління ризиками». З'ясовано, що серед таких ключовими є: 1) принцип комунікативної взаємодії між представниками держави та приватним сектором; 2) принцип системно здійснюваної співпраці між усіма суб'єктами та учасниками захисту об'єктів критичної інфраструктури фінансового сектору України; 3) принципом автономної стійкості; 4) принцип міжнародного співробітництва).

17. Доведено, що принципи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, як правила організаційного та практико-реалізаційного характеру, мають подвійну юридичну спрямованість сфери розповсюдження своєї дії. З одного боку, уповноважені представники національної системи їхнього захисту мають дотримуватись встановлених загальноправових, галузевих та спеціальних орієнтирів, щоб ефективно та результативно виконувати своє функціональне призначення. З іншого боку, вони покладають на державу обов'язок забезпечити цим суб'єктам належні умови для реалізації задекларованих

принципів, зокрема через створення правового, організаційного та ресурсного забезпечення.

18. Зауважено, що без ідентифікації системи суб'єктів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України навряд чи вдасться зрозуміти специфіку досліджуваного кола питань, їх особливості та правову природу.

19. Критично аналізується наукова думка щодо сучасної структурно-функціональної характеристики державної політики у сфері захисту критичної інфраструктури в Україні в контексті існування функціонуючих систем у її межах, адже вченими не враховується секторальний аспект досліджуваного питання. Доведено, що фінансовий сектор України має, наприклад, систему регуляторів фінансового ринку та окремо Фонд гарантування вкладів фізичних осіб, які сукупно в очах закону не є самостійною інтегрованою системою, однак виконують функції, які сприяють стійкості та безпеці конкретно критичної інфраструктури фінансового сектору України.

20. На основі аналізу законодавчих положень виявлено, що за захист об'єктів критичної інфраструктури фінансового сектору України відповідає значно ширша група суб'єктів у порівнянні з тими, що мають відповідні адміністративні повноваження. Ключовими суб'єктами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України названо Національний банк та Міністерством фінансів України. Розкрито завдання та функції Національного банку України у цій сфері. З'ясовано, що Положення про Міністерство фінансів України, затверджене постановою Кабінету Міністрів України від 20 серпня 2014 року № 375 не передбачає жодних положень, пов'язаних з визначенням означеного суб'єкта секторальним органом у цій сфері. Однак зауважено, що у його структурі, наприклад, функціонують: Департамент прогнозування доходів бюджету, що відповідає за планування, виконання та моніторинг виконання бюджетів; Державна казначейська служба України, що відповідає за розрахунково-

касове обслуговування розпорядників та одержувачів бюджетних коштів; Державна податкова служба України, що відповідає за здійснення контролю за надходженням до бюджетів та державних цільових фондів податків, зборів, платежів.

21. Запропоновано виокремлювати класичний розподіл суб'єктів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України на секторальних (Міністерство фінансів України, Національний банк України), функціональних (наприклад, органи сектору безпеки, кібербезпеки) і уповноваженого (наразі – Державна служба спеціального зв'язку та захисту інформації України) органів. Сформовано альтернативний варіант розподілу, який дозволяє їх згрупувати за приналежністю до виконуваних задач на тих, що: 1) є репрезентацією цієї системи (Міністерство фінансів України, Національний банк України, Державна служба спеціального зв'язку та захисту інформації України, Національна комісія з цінних паперів та фондового ринку, Фонд гарантування вкладів фізичних осіб); 2) функціонують для виконання задач секторальних, функціональних та уповноваженого органів захисту критичної інфраструктури в Україні (наприклад, Центр кіберзахисту Національного банку України або Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України); 3) є самостійним міжвідомчим органом з виконанням спеціалізованих функцій (Рада з фінансової стабільності).

22. Доведено, що система суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України – це цілісне інституційне утворення, що має функціонувати на засадах єдності та диференціації, гармонійності та кооперації. Уточнено, що в умовах сучасності можна вести мову про її сформованість, однак не публічність. Йдеться зокрема про те, що переважна частина прийнятих рішень та реалізованих заходів є внутрішньоорганізаційним аспектом розвитку означеної сфери, а отже – широкий громадський загал не має до неї

доступу навіть в інформаційному аспекті. Яскраво це демонструється на прикладі Міністерства фінансів України, яке нормативно визначене як секторальний орган у сфері захисту критичної інфраструктури фінансового сектору України, що має низку необхідних повноважень, доступ до аналізу практичної реалізації яких фактично відсутній. Аналогічно й щодо рішень Національного банку України.

23. У контексті ідентифікації форм та методів адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України звернено увагу на зміст та сутність адміністративно-правових відносин у цій сфері. Обґрунтовується, що адміністративно-правові відносини у сфері захисту об'єктів критичної інфраструктури фінансового сектору України є сполучною ланкою, що забезпечує цілісність цього механізму, а також різномірні взаємодії у його межах. Причому провідною особливістю таких названо їхній динамічний характер, оскільки вони безпосередньо залежать від зовнішніх та внутрішніх викликів, загроз та змін у правовому середовищі. Однак зауважено, що адміністративно-правові відносини у сфері захисту об'єктів критичної інфраструктури фінансового сектору України можна також трактувати через призму інструментального підходу, адже у будь-якому разі змістовний їх контекст залежить від повноважень конкретного представника національної системи захисту критичної інфраструктури фінансового сектору України, який застосувавши/використавши необхідну форму та доцільний метод діяльності активізує чи забезпечує їхній розвиток.

24. З'ясовано, що наукова доктрина вміщує різні погляди на категорії «форми», «методи» та «інструменти» в контексті використання їх в категорійному апараті науки адміністративного права. Констатується, що вчені виокремлюють форми, методи, інструменти та способи реалізації державного управління, публічного адміністрування, публічного врядування та окремо – адміністративної діяльності. Причому у більшості випадків мова йде про зміст та сутність останніх, які іменуються різними термінологічними

одинацями. Доведено, що наукова полеміка з цього питання є досі актуальною через теоретичний характер означених категорій та відсутність єдиної концептуальної основи, яка б відповідала на основні дослідницькі запити. Зокрема маємо підтвердження, що за історичним контекстом розвитку адміністративного права категорії «форм» та «методів» мали власне і достатньо обґрунтоване поняттєве визначення, яке втратило своє значення з перехідними етапами становлення України як країни сервісного типу.

25. Визначено, що за традиційного підходу основними інструментами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є видання нормативно-правових та індивідуальних актів, укладання адміністративних договорів та затвердження актів-планів, в основу яких закладено відповідний спосіб їхньої реалізації. Таким може бути, наприклад, контроль та нагляд, моніторинг, планування, консультування, координація, співпраця тощо.

26. Висунуто припущення про можливість розгляду порушеної проблематики під іншим кутом зору. Зокрема категорії «форми» та «методи» в контексті адміністративно-правового захисту є сенс розглядати з позиції функціональної єдності, що дозволяє інтерпретувати їх зміст через категорію «інструментів», тобто знарядь, які є застосовними уповноваженими суб'єктами задля виконання їх завдань та функцій. У цьому випадку знаряддям є правовий засіб, який як явище-регулятор правової дійсності, перетворює правову норму в конкретні дії та рішення, які реалізуються на практиці. Уточнено, що за такої інтерпретації їхньої сутності інструментальний бік адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України стає основоположним при ідентифікації юридичної природи механізму його здійснення.

27. Звернено увагу на правові засоби, які об'єктивують охоронну групу з таких (заходи захисту, які є застосовними для забезпечення схоронності об'єктів критичної інфраструктури фінансового сектору України), а також зауважено на можливості виокремлення засобів впливу та засобів реалізації

права. Визначено, що у контексті першого йдеться про виявлення, запобігання та реагування на потенційні загрози або порушення роботи об'єктів критичної інфраструктури фінансового сектору України. Тоді як засоби реалізації права репрезентують практичне втілення встановлених правових норм.

28. Доведено, що інструментальний бік механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України характеризується через зв'язок із категоріями «форми», «методи». Однак наголошено на необхідності їх диференціації в контексті використання в управлінсько-організаційному, регуляторному чи іншому державно-владному процесі, адже у кожному з таких їм можна надати специфічного значення та функціонального навантаження. Узагальнено, що у випадку цього дослідження інструментальний контекст адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України репрезентується через систему варіантів зовнішнього оформлення управлінського рішення та конкретного підходу, застосовного до досягнення поставлених у ньому цілей. Йдеться про знаряддя, яке покликане реалізувати поставлену задачу. Причому цілями управлінського рішення у сфері захисту об'єктів критичної інфраструктури фінансового сектору України може бути як внутрішньоорганізаційне питання, що потребує вирішення, так і зовнішньо спрямовані завдання.

РОЗДІЛ 3

ШЛЯХИ ВДОСКОНАЛЕННЯ МЕХАНІЗМУ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО СЕКТОРУ УКРАЇНИ

3.1. Зарубіжний досвід адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору та можливість його адаптації в Україні

Відразу зауважимо, що оглядовий аналіз міжнародних та регіональних основ здійснення захисту об'єктів критичної інфраструктури фінансового сектору України переконливо свідчить про актуалізацію низки питань, яким в Україні приділено недостатньо уваги. Зокрема наразі досить гостро стоїть питання забезпечення кіберзахисту, адже у 2023 році спостерігалось суттєве зростання їхньої кількості, що були спрямовані на критичну інфраструктуру банківської системи України, зокрема на Національний банк та інші банки, а також значне збільшення проявів актів кібершахрайства та кіберзлочинності [217, с. 135]. Значна увага приділяється й захисту критичної інфраструктури від терористичних атак, а також забезпеченню глобальної фінансової стабільності.

Деталізуючи нормативи, що встановлені європейським законодавством, уточнимо, що головне правило об'єктивується через вказівку на обов'язку країн-членів ЄС забезпечити належний технічний та організаційний рівень безпеки за допомогою окремих законодавчих актів щодо критичної інфраструктури. Це включає режим реагування на інциденти, якого повинні дотримуватися фінансові установи. Власне, Загальний регламент захисту даних («GDPR») [254] було запроваджено для стандартизації регулювання захисту даних у ЄС і він поширюється на всі організації, які контролюють або обробляють персональні дані та працюють у межах ЄС чи продають товари в ЄС. Фінансові установи контролюють і обробляють великий обсяг

даних, тому на них суттєво впливає цей регламент. Причому одним із основних його зобов'язань, – конкретні вимоги щодо конфіденційності, безпеки та управління порушеннями [260].

Ведучи мову про сучасність, то в останні роки Європа зосередилася на законодавстві, що стосується інформаційно-комунікаційних технологій і кібербезпеки для європейського фінансового сектора. Вважається, що оскільки відповідність стандартам є одним із головних факторів кіберстійкості, розумна та послідовна регуляторна стратегія може допомогти забезпечити необхідну базову лінію безпеки у фінансовому секторі для пом'якшення інституційних і системних ризиків.

Нагадаємо, що загаром основна дискусія, яка проходила під час обговорення нових законопроектів щодо захисту критичних інфраструктур точилася навколо питання про те, які сектори слід вважати критично важливими для ЄС. Обговорювалося навіть питання чи може критична інформаційна інфраструктура розташовуватися за межами Європи, якщо вона впливає на ЄС.

Ця дискусія порівняно нещодавно була закрита. Європейська Комісія [271] спочатку запропонувала одинадцять секторів критичної інфраструктури та двадцять дев'ять її підсекторів. У процесі обговорення проекту Директиви про критичну інфраструктуру в Європейському Парламенті пропонувалося все більше і більше додаткових секторів. Це, очевидно, занепокоїло деякі держави-члени, які побачили загрозу своєму суверенітету в сфері захисту критичної інфраструктури. Власне тому в остаточно схваленій Директиві 2008 року лише два сектори – енергетика і транспорт – були визнані «європейськими», а потім деталізовані і поділені на вісім під секторів [240]. Це двосекторне рішення було ще більше обмежене інфраструктурою, розташованою в державах-членах, де перебої в роботі мали б значний вплив щонайменше на дві інші держави-члени. Обговорювалося багато варіантів того, скільки країн-членів повинно бути задіяно, але їх стало дві. У наступні роки інформаційно-комунікаційні технології часто згадувалися як можливий

новий сектор критичної інфраструктури, який можна було б додати до переліку європейської критичної інфраструктури, оскільки вони вважалися горизонтальним сектором критичної інфраструктури. За пропозицією Європейської Комісії, вона включає десять секторів, а саме: енергетику, транспорт, банківську справу, інфраструктуру фінансових ринків, охорону здоров'я, питну воду, водовідведення, цифрову інфраструктуру, державне управління та космос [272]. Для того, щоб зробити відповідні директиви більш сумісними, ці сектори такі самі, що й у запропонованій одночасно Директиві з кібербезпеки NIS2 [269; 270]. Однак зауважимо, що зараз цих секторів більше.

Щоб покращити цю ситуацію та усунути недоліки, у вересні 2020 року Європейська комісія запропонувала нове законодавство щодо стійкості до цифрових технологій для європейського фінансового сектора під назвою Закон про цифрову операційну стійкість («DORA») [275]. Цей закон має на меті запровадити узгоджену та всеохоплюючу структуру цифрової операційної стійкості для європейських фінансових установ із чіткими вимогами щодо вирішення та пом'якшення інформаційно-комунікаційних технологій та кіберризиків. Це пряма відповідь на спільні поради Європейських наглядових агентств (ESA), які визначили чотири сфери діяльності, на яких слід зосередитися в нормативних розробках у найближчому майбутньому: по-перше, вимоги щодо безпеки інформаційно-комунікаційних технологій та управління ризиками; по-друге, галузеві вимоги до звітності про кіберінциденти; по-третє, прямий контроль і нагляд за сторонніми постачальниками; і по-четверте, платформа тестування кіберстійкості [260]. Закон про цифрову операційну стійкість розглядає всі ці сфери та пропонує потенційні рішення для багатьох поточних прогалин.

Окремо варто наголосити, що правила кібербезпеки ЄС, запроваджені в 2016 році, були оновлені Директивою NIS2, яка набула чинності в 2023 році. Вона модернізувала існуючу законодавчу базу, щоб йти в ногу зі зростанням цифровізації та розвитком ландшафту загроз кібербезпеці. Розширюючи

сферу дії правил кібербезпеки на нові сектори та організації, це ще більше покращує стійкість і здатність реагувати на інциденти державних і приватних організацій, компетентних органів і ЄС в цілому [243]. Фінансові установи країн-членів ЄС після її прийняття почали розробляти і впроваджувати власні стандарти кібербезпеки.

Так, наприклад, 12 квітня 2024 року Європейський центральний банк отримав від Міністерства фінансів Латвійської Республіки запит на висновок щодо проекту закону про національну кібербезпеку [267], який вони розробили і пропонували «Latvijas Banka» (центральний банк Латвії) вважати об'єктом критичної інфраструктури.

У запиті зазначалось, що запропонований Законопроект поширюється на «Latvijas Banka» в повному обсязі. У консультативному листі, надісланому до Європейського центрального банку Міністром фінансів Латвії, пояснюється, що за останні два роки латвійські державні установи зазнали різкого зростання зловмисної кіберактивності. У 2022 році Латвія була об'єктом 16% усіх кібератак проти держав-членів, тоді як країни Балтії разом були об'єктом 32% усіх кібератак. Таким чином, консультативний орган вважає, що кібербезпеку всіх державних установ Латвії, включаючи «Latvijas Banka», слід посилити, і що його виключення зі сфери дії законопроекту створить серйозний ризик для національної безпеки Латвії та безпеки Євросистеми в цілому [267].

Отже, поточний європейський нормативно-правовий ландшафт у сфері інформаційно-комунікаційних технологій та кіберризиків для фінансового сектору є багаторівневим і складним. Він включає численні європейські та національні нормативні акти і галузеві стандарти. Фінансові установи мають дотримуватися правил щодо захисту об'єктів критичної інфраструктури, загального європейського законодавства з питань захисту даних, а також спеціальних норм у фінансовому секторі, які поділяються на підсектори: банківську справу, страхування та інфраструктури ринку. Причому важливо, що не всі країни-члени застосовують ці стандарти як національні, що

зумовлює відмінності здійснення ними адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору.

Враховуючи вище зазначене та думку провідних експертів, наприклад, можна визначити п'ять правил безпеки в банківській справі щодо кібератак: 1) знати свого клієнта; 2) знати свого працівника. Тут варто уточнити, що більшість кібершахрайств має певну пряму чи непряму роль внутрішньої особи, яка, як правило, є співробітником організації, яка стала об'єктом атаки на кібербезпеку. Існує нагальна потреба, щоб організація не тільки проводила попередню перевірку співробітника під час найму, але й постійно відстежувала поведінку співробітника, тенденції в оперативному використанні організаційних ресурсів, рівень взаємодії з іншими особами тощо. Сьогодні IT-інструменти надають багато інформації про поведінку та шаблони співробітників; дуже важливо, щоб організації приділяли належне значення цим аспектам; 3) підтримувати свої IT-системи в актуальному стані за відсутності усіх ризикованих компонентів, таких як віруси, спами, шкідливе програмне забезпечення, програмне забезпечення для підробки тощо; 4) забезпечити максимальне управління IT-системи шляхом створення окремої посади CISO (головний спеціаліст з інформаційної безпеки), який буде постійно контролювати якість і ефективність інформаційної безпеки в організації; 5) забезпечити постійну обізнаність щодо кібербезпеки серед усіх учасників ланцюжка. Якщо потрібно, необхідно забезпечити безперервне кібер-пильнування, безперервний процес підвищення обізнаності, навчання, посилення, тестування, випробування та оновлення [274].

Освоєння таких кроків, на нашу думку, сприятиме вдосконаленню банками та іншими об'єктами критичної інфраструктури досліджуваної сфери власних спроможностей для реагування на сучасні кіберзагрози, а також зміцненню кіберстійкості фінансової системи загалом [217, с. 137].

У продовження порушеного питання зауважимо, що для того, щоб досягти ефективнішого захисту глобальної фінансової системи від кіберзагроз, у листопаді 2020 року Фонд Карнегі опублікував звіт під назвою

«Міжнародна стратегія кращого захисту глобальної фінансової системи від кіберзагроз» [282]. Звіт, розроблений у співпраці зі Всесвітнім економічним форумом, рекомендує конкретні дії для зменшення фрагментації шляхом сприяння більшій співпраці як на міжнародному рівні, так і між урядовими установами, фінансовими компаніями та технологічними компаніями.

Запропонована Міжнародна стратегія кращого захисту глобальної фінансової системи від кіберзагроз базується на чотирьох принципах: по-перше, потрібна більша ясність щодо ролей і обов'язків. Лише кілька країн налагодили ефективні внутрішні відносини між своїми фінансовими органами, правоохоронними органами, дипломатами, іншими відповідними урядовими структурами та промисловістю. Існуюча фрагментація перешкоджає міжнародній співпраці та послаблює колективну стійкість міжнародної системи, її здатність до відновлення та реагування. По-друге, міжнародна співпраця є необхідною і терміною. Враховуючи масштаб загрози та глобальну взаємозалежність системи, окремі уряди, фінансові фірми та технологічні компанії не можуть ефективно захиститись від кіберзагроз, якщо вони працюють поодиночі. По-третє, зменшення фрагментації звільнить можливості для вирішення проблеми. Розпочато багато ініціатив щодо кращого захисту фінансових установ, але вони залишаються закритими. Деякі з цих зусиль дублюють одна одну, збільшуючи транзакційні витрати. Кілька з цих ініціатив достатньо зрілі, щоб ними можна було поділитися, краще їх координувати та надалі інтернаціоналізувати. По-четверте, захист міжнародної фінансової системи може бути моделлю для інших секторів. Фінансова система є однією з небагатьох сфер, у якій країни мають чіткий спільний інтерес до співпраці, навіть коли геополітична напруга висока. Зосередження уваги на фінансовому секторі є відправною точкою та може прокласти шлях до кращого захисту інших секторів у майбутньому [282].

Серед заходів для посилення кіберстійкості звіт рекомендує Раді з фінансової стабільності («FSB») розробити базову структуру для нагляду за

управлінням кіберризиками у фінансових установах [262]. Варто уточнити, що Рада з фінансової стабільності [237] – це один із міжнародних органів, який здійснює моніторинг і дає рекомендації щодо забезпечення глобальної фінансової системи. Рада сприяє міжнародній фінансовій стабільності; це робиться шляхом координації національних фінансових органів і міжнародних органів, що встановлюють стандарти для регуляторної, наглядової та іншої політики фінансового сектора. Вона допомагає створити рівні умов гри, заохочуючи узгоджену реалізацію цих політик у різних секторах і юрисдикціях. Працюючи через своїх членів, Рада прагне зміцнити фінансові системи та підвищити стабільність міжнародних фінансових ринків. Зокрема Рада з фінансової стабільності була створена для:

- 1) оцінювання вразливих місць, що впливають на глобальну фінансову систему, а також для своєчасного та постійного перегляду в макропруденційній перспективі регуляторні, наглядові та пов'язані дії, які необхідні для усунення цих вразливостей та їх результатів;
- 2) сприяння координації та обміну інформацією між органами, відповідальними за фінансову стабільність;
- 3) моніторингу та консультування щодо розвитку фінансового ринку та його наслідків для регуляторної політики;
- 4) моніторингу і консультування щодо найкращої практики щодо дотримання нормативних стандартів;
- 5) проведення спільних стратегічних оглядів міжнародних органів, що встановлюють стандарти, і координувати їх відповідну роботу з розробки політики, щоб забезпечити своєчасність, координацію, зосередженість на пріоритетах і усуненні прогалів;
- 6) встановлення керівних принципів для створення та підтримки наглядових колегій;
- 7) підтримки планування на випадок непередбачених ситуацій для транскордонного управління кризою, особливо щодо системно важливих фірм;
- 8) співпраці з Міжнародним валютним фондом для проведення навчань раннього попередження;
- 9) сприяння виконанню юрисдикціями-членами узгоджених зобов'язань, стандартів і політичних рекомендацій шляхом моніторингу впровадження, експертної оцінки та розкриття інформації [237].

Щодо положень звіту, то уряди та індустрія повинні зміцнювати безпеку, обмінюючись інформацією про загрози та створюючи фінансові комп'ютерні групи реагування на надзвичайні ситуації («CERT») за зразком ізраїльської «FinCERT». Фінансові органи також повинні приділяти пріоритет підвищення стійкості фінансового сектора проти атак, спрямованих на дані та алгоритми. Це має включати безпечне, зашифроване зберігання даних, яке дозволяє учасникам безпечно створювати резервні копії даних облікових записів клієнтів протягом ночі. Необхідно проводити регулярні тренування з імітації кібератак, щоб виявити слабкі місця та розробити плани дій. Щоб зміцнити міжнародні норми, звіт рекомендує урядам чітко визначити, як вони застосовуватимуть міжнародне право до кіберпростору та посилити норми для захисту цілісності фінансової системи. Уряди Австралії, Нідерландів і Великої Британії вже зробили перший крок із заявами про те, що кібератаки з-за кордону можуть розглядатися як незаконне застосування сили або втручання у внутрішні справи іншої держави. Кіберстійкість і посилені міжнародні норми можуть сприяти колективній реакції через дії правоохоронних органів або багатосторонню реакцію з промисловістю. Відповідь може включати санкції, арешти та вилучення активів [262].

Щодо конкретного досвіду адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору, вбачаємо актуальним піддати аналізу практики США, адже це країна, що вже багато років займає лідерські позиції у сфері захисту критичної інфраструктури, зокрема і фінансового сектору.

Варто зазначити, що фінансова криза, яка охопила світ у 2008 році, вимагала масштабної допомоги банкам, щоб уникнути ще більш глибокого економічного колапсу. У 2010 році законодавці США прийняли закон Додда-Френка («Dodd-Frank Wall Street Reform and Consumer Protection Act»), який мав на меті знизити ризики в банківській системі. Його положення обмежували банки в торгівлі власними коштами («правило Волкера»),

посилювали моніторинг системного ризику, регулювання фінансових продуктів і запроваджували ініціативи щодо захисту споживачів [238]. Закон на пряму не регулював захист об'єктів критичної інфраструктури, але передбачав положення, які були направлені на підвищення стійкості фінансових установ до системних ризиків.

Керівництво США розуміючи, що добробут країни залежить від безпечної та стійкої критичної інфраструктури – активів, систем і мереж, які є основою американського суспільства – розробило і впровадило Національний план захисту інфраструктури («NIPP») [266]. Національний план захисту інфраструктури 2013: Партнерство для забезпечення безпеки та стійкості критичної інфраструктури – описує як державні та приватні учасники системи захисту критичної інфраструктури працюють разом, щоб керувати ризиками та досягати результатів безпеки та стійкості [263].

Зазначений план являє собою еволюцію концепцій, представлених у початковій версії «NIPP», який вперше був випущений у 2006 році та переглянутий у 2009 році. Після кризи 2008 року, Національний план був оптимізований і адаптований до поточних ризиків, політики та стратегічного середовища. Він забезпечує основу для інтегрованого та спільного підходу для досягнення бачення: «Країна, в якій фізична та кібернетична інфраструктура залишається безпечною та стійкою, зі зниженими вразливими місцями, мінімізованими наслідками, ідентифікованими та зруйнованими загрозами, прискореним реагуванням і відновленням» [266]. «NIPP 2013» відповідає вимогам Президентської політичної директиви («PPD») 21: Безпека та стійкість критичної інфраструктури [268], підписаної в лютому 2013 року. План було розроблено шляхом спільного процесу за участю зацікавлених сторін з усіх 16 секторів критичної інфраструктури, усіх 50 штатів та всіх рівнів, – від уряду до промисловості. Він забезпечує чіткий заклик до дії, щоб залучити партнерство, інновації для управління ризиками та зосередитися на результатах [263].

Необхідно відмітити, що зазначений План як критично важливими, поряд з іншим, включив і фінансові послуги. Причому Федеральний уряд США давно визнає сектор фінансових послуг як найважливіший компонент інфраструктури нації. Сектор включає комерційні банки, брокерів і дилерів цінних паперів, а також постачальників ключових фінансових систем і послуг, які підтримують ці функції. Загалом цей сектор має активи на суму близько 108 трильйонів доларів і тому зрозуміло, що він постійно стикається з різними ризиками, пов'язаними з кібербезпекою. Відзначається, що основні ризики включають: 1) розширення доступу до фінансових даних через постачальників послуг інформаційних технологій і партнерів по ланцюгу поставок; 2) зростання складності зловмисного програмного забезпечення – програмного забезпечення, призначеного для заподіяння шкоди – і 3) збільшення взаємозв'язку через мережі, хмару та мобільні програми [242].

Ведучи мову про наявну систему захисту об'єктів критичної інфраструктури фінансового сектору США, варто зауважити, що існує кілька галузевих груп і фірм, які вживають заходів для підвищення безпеки та стійкості зазначеного сектору за допомогою широкого спектра заходів із зменшення кіберризиків. Ці зусилля включають координацію всередині сектору за допомогою таких груп, як Координаційна рада сектору фінансових послуг («Financial Services Sector Coordinating Council») [250] і Центр фінансового системного аналізу та стійкості («Financial Systemic Analysis and Resilience Center») [253]. Також ці структури регулярно проводять загальногалузеві навчання щодо реагування на інциденти, здійснюють обмін інформацією про загрози та вразливості, розробляють та надають вказівки щодо проведення оцінки ризиків, а також забезпечення кібербезпеки.

Наприклад, Координаційна рада сектору фінансових послуг, або скорочено «FSSCC», була створена у 2002 році фінансовими установами для співпраці з ключовими державними установами під час координації діяльності з критичної інфраструктури та внутрішньої безпеки в галузі фінансових послуг. Це галузева некомерційна організація, що об'єднує

надавачів фінансових послуг, торгових асоціацій та інших лідерів галузі, щоб допомогти сектору реагувати на стихійні лиха, загрози з боку терористів і проблеми кібербезпеки всіх типів. «FSSCC» співпрацює з державним сектором у питаннях ефективності політики для підвищення безпеки та стійкості фінансової системи США [250].

Важливо, що Міністерство національної безпеки США визнає «FSSCC» членом Консультативної ради партнерства з критичної інфраструктури як представників банківського та фінансового сектору, адже вона спрямовує свою діяльність на: посилення співпраці та обізнаності між сектором фінансових послуг, державним сектором та іншими секторами критичної інфраструктури; сприяння здійсненню державно-приватного партнерства для вирішення проблем стійкості сектору фінансових послуг США; зміцнення сектору фінансових послуг шляхом внутрішньогалузевої координації; співпрацю над ініціативами щодо операційного ризику з членами асоціації торгівлі фінансовими послугами та іншими організаціями; розроблення і сприяння розвитку стратегічного бачення для вирішення проблеми конвергенції кібербезпеки та стійкості в ширшому середовищі операційних ризиків [273].

Інші суб'єкти, що входять в систему захисту об'єктів критичної інфраструктури фінансового сектору США це: Міністерство фінансів і федеральні фінансові регулятори. Наприклад, федеральні агентства надають експертизу з кібербезпеки та проводять симуляційні навчання, пов'язані з реагуванням на кіберінциденти та відновленням. Міністерство фінансів, як провідний державний орган у сфері надання фінансових послуг, відіграє ключову роль у підтримці багатьох зусиль щодо підвищення кібербезпеки та стійкості фінансового сектора. Наприклад, помічник міністра фінансів у справах фінансових установ є головою комітету державних установ, які відповідають за цю галузь [242].

Також функціонує Комітет фінансової та банківської інформаційної інфраструктури («ФВІС»), який створений під керівництвом Президентської

робочої групи з фінансових ринків та відповідає за покращення координації і комунікації між фінансовими регуляторами, сприяє розвитку державно-приватного партнерства у фінансовому секторі та займається підвищенням стійкості фінансового сектора в цілому [247].

Можемо узагальнити, що головний і провідний акцент у цій країні проставлено на державно-приватному партнерстві, адже вже доведеним є факт того, що це дієвий інструмент, здатний створити умови для успішного захисту об'єктів критичної інфраструктури фінансового сектору. Причому не тільки США, а й інші країни світу усвідомили його переваги. Причому у багатьох країнах світу значна частина об'єктів критичної інфраструктури перебуває в приватній власності, що потребує відповідного правового регулювання державно-приватного партнерства. Наприклад, у Німеччині положення щодо доцільності зміцнення державно-приватного партнерства закріплено у Стратегії кібербезпеки від 2011 року. У Великій Британії основи взаємодії державного та приватного секторів закладені Стратегією національної безпеки, Антитерористичною стратегією, Стратегією захисту кіберпростору та урядовому Плані розвитку національної інфраструктури. У Національній стратегії (безпеки) критичної інфраструктури Канади підкреслюється, що «головна відповідальність за підвищення стійкості/здатності до швидкого відновлення (resilience) критичної інфраструктури залишається за власниками та операторами [62; 265]». У зв'язку з цим ефективно державно-приватне партнерство у сфері безпеки загалом і захисту критичної інфраструктури зокрема є чи не найважливішою складовою державної політики в цьому напрямі [108].

Яскравим прикладом тому є ініціатива приватного сектора щодо обміну інформацією між різними суб'єктами, які уповноважені забезпечувати кіберзахист у фінансовому секторі.

Зокрема Фінансовий центр аналізу та обміну інформацією (іменований як «FS-ISAC») – це глобальна спільнота з обміну кіберрозвідувальними даними, яка зосереджена виключно на фінансових послугах. Вона

складається з експертів із різних галузей фінансового сектору, академічних кіл та державних органів, що встановлюють відповідні стандарти. Організація зі штаб-квартирою в США має представництва у Великій Британії та Сінгапурі та членські фінансові установи приблизно в 70 країнах [286]. Обслуговуючи фінансові установи та, відповідно, їхніх клієнтів, організація використовує свою інтелектуальну платформу, ресурси стійкості та надійну однорангову мережу, щоб передбачати, пом'якшувати та реагувати на кіберзагрози.

Таким чином, державно-приватне партнерство у сфері захисту об'єктів критичної інфраструктури у фінансовому секторі за міжнародним контекстом передбачає будь-який тип взаємовигідної співпраці, неформальної або формальної, між двома або більше організаціями приватного та державного сектору з метою підвищення рівня безпеки та стійкості таких об'єктів.

Однак варто наголосити, що досвід досліджуваної країни не обмежується зазначеними положеннями. Найголовніше, на нашу думку, що у цій країні системно та планомірно розробляються нормативно-правові основи для підвищення стійкості фінансових установ до системних ризиків. Умовно їх можемо диференціювати на загальні та спеціальні. Загальні об'єктивуються, наприклад, у межах Директиви Президента про національну безпеку №7, яка встановлює національну політику для федеральних департаментів та агентств щодо ідентифікації та пріоритизації об'єктів критичної інфраструктури та їх захисту від терористичних атак. Ключовим з таких також є вищезгаданий Національний план захисту інфраструктури, який постійно оновлюється, демонструючи еволюційність концепцій координації національних зусиль з управління ризиками для критичної інфраструктури країни. Своєю чергою, до числа спеціальних відносимо Спеціальний план для сектору фінансових послуг, що адаптує положення Національного плану до унікальних характеристик та ризиків, притаманних цьому сектору.

Уточнюючи зазначене детальніше варто вказати, що згідно законодавчих вимог цієї країни кожне секторальне агентство з управління ризиками розробляє план для конкретного сектора шляхом скоординованих зусиль із залученням партнерів з державного та приватного секторів. Власне саме Міністерство фінансів призначено Агентством з управління ризиками сектору фінансових послуг. Однак актуально зазначити, що Президентська політична директива 21 у 2013 році змінила назву банківського та фінансового сектору на сектор фінансових послуг [251].

Доречно також уточнити, що Міністерство фінансів публікує спеціальні огляди, присвячені конкретній актуальній темі. Наприклад, на вимогу Виконавчого наказу (ЕО) 14110 «Безпечна, надійна та заслуговуюча на довіру розробка та використання штучного інтелекту», що передбачає обов'язок Міністерства опублікувати звіт про найкращі практики для фінансових установ щодо управління кіберризиками, пов'язаними зі штучним інтелектом, у березні 2024 року у публічному доступі з'явився відповідний звіт. Він надає огляд використання штучного інтелекту у фінансовому секторі для цілей кібербезпеки та розглядає його наслідки для фінансових установ на основі 42 інтерв'ю з учасниками ринку. Хоча основна увага в цьому звіті зосереджена на використанні штучного інтелекту для кібербезпеки та ризиках, що супроводжують це використання, багато висновків і найкращих практик можуть бути застосовані і до інших сценаріїв використання штучного інтелекту. Зауважимо, що цей звіт не охоплює багато інших питань, пов'язаних з штучним інтелектом та фінансовими послугами, зокрема захисту прав споживачів та інвесторів, нерівного впливу, фінансової стабільності та регуляторних питань у фінансовій сфері. Міністерство фінансів планує продовжувати вивчення впливу штучного інтелекту на фінансові послуги у найближчі місяці та роки. Спостереження відображають сприйняття зацікавлених сторін щодо стану штучного інтелекту та не є авторитетною оцінкою фактичного використання штучного інтелекту або термінології [284].

Структурно звіт складається з п'яти основних компонентів, починаючи з розділу «Штучний інтелект у фінансових послугах: кібербезпека та захист від шахрайства». У цьому розділі надається огляд того, як фінансові установи різного розміру використовують штучний інтелект, зосереджуючись на кібербезпеці та випадках боротьби з шахрайством. Далі звіт окреслює «Кібербезпеку та загрози шахрайства для фінансових установ, пов'язані зі штучним інтелектом». Наступний розділ, «Регуляторне середовище для штучного інтелекту у фінансових послугах», надає огляд поточного регуляторного середовища щодо використання штучного інтелекту для кібербезпеки та боротьби з шахрайством у фінансових установах. Потім звіт описує «Найкращі практики управління кіберризиками, пов'язаними зі штучним інтелектом». Нарешті, звіт завершується рекомендаціями щодо «Наступних кроків: виклики та можливості», які Міністерство фінансів визначило під час підготовки цього звіту, та пропонує подальші дії щодо найактуальніших питань [284].

Відповідно приватний сектор не тільки залучений до процедур оптимізації здійснення адміністративно-правового захисту у цій сфері, а й належним чином інформаційно забезпечений, адже публічними є не тільки звіти про діяльність уповноважених органів, а й огляди щодо вивчення впливу окремих явищ на стабільність функціонування сектору загалом. Провідною особливістю досвіду цієї країни також можемо визначити інтеграцію фізичної та кібернетичної безпеки і стійкості критичних інфраструктур.

Таким чином, маємо такі ключові висновки:

– позитивний досвід США та ЄС у сфері захисту критичної інфраструктури фінансового сектору може стати корисним прикладом для України в контексті: 1) наявності спеціальних планів захисту критичної інфраструктури фінансового сектору, що визначають особливості її захисту від системних загроз і ризиків; 2) інституційної різноманітності, що має прояв широким колом суб'єктів захисту та чіткістю процедур обміну

інформацією між ними; 3) активної участі приватного сектору та ефективної координації між державними та приватними суб'єктами; 4) встановлення єдиних вимоги до кібербезпеки для критичних секторів, включно з фінансовим; 5) розвинутих систем партнерства між державними та приватними установами; 6) чіткого розподілу обов'язків та відповідальності суб'єктів реалізації такого захисту; 7) дієвості механізмів оцінки кіберстійкості об'єктів критичної інфраструктури фінансового сектору;

– ураховуючи цей досвід, доцільними для впровадження до національної правової системи можемо визначити такі позитивні практики у сфері захисту об'єктів критичної інфраструктури фінансового сектору як: розробка спеціалізованих стратегічних планів; встановлення чітких процедур обміну інформацією; розвиток стимулів для залучення приватного сектора до процесів підвищення загальної стійкості фінансової системи; запровадження єдиних вимог до кібербезпеки фінансового сектору; створення платформ для обміну публічною інформацією; чітке визначення обов'язків і відповідальності суб'єктів захисту об'єктів критичної інфраструктури фінансового сектору та впровадження механізмів оцінки їх кіберстійкості.

3.2. Напрямки розвитку адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України

Підсумовуючи результати проведених розвідок маємо констатувати, що досліджувана сфера має ряд позитивних тенденцій для подальшого вдосконалення адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України.

Перш за все, вбачаємо, що основним напрямком розвитку адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України є нормативний, що передбачає

формування якісної основи для захисту об'єктів критичної інфраструктури фінансового сектору України.

Причому варто зауважити, що у цьому контексті йдеться не про зміни та доповнення до чинного законодавства України, а про необхідність аналогічно досвіду США розробити та затвердити План захисту об'єктів критичної інфраструктури фінансового сектору України, як специфічної деталізації Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури.

Уточнимо, що в США цей план надає огляд сектора, а також кібербезпекових і фізичних ризиків, з якими він стикається, встановлює стратегічну основу, що слугує керівництвом для пріоритизації щоденної діяльності сектора, та описує ключові механізми, через які ця стратегічна основа реалізується та оцінюється. Цей план був розроблений завдяки тісній співпраці між Міністерством фінансів США, Координаційною радою сектору фінансових послуг, Комітетом з інформаційної інфраструктури фінансово-банківського сектору та Міністерством національної безпеки США. Усі ці організації об'єднали зусилля сотень представників як державного, так і приватного сектору, що представляють усі аспекти сектору [252].

Зокрема уповноважені суб'єкти визнають, що організації, які становлять фінансовий сектор, є основою фінансової системи країни і важливим компонентом глобальної економіки. Вони пов'язані через мережу електронних систем із незліченною кількістю точок доступу. Будь-який інцидент, як рукотворний, так і природний, що впливає на ці системи, може мати серйозні наслідки для всієї економіки. Тому цей план надає спільну стратегію для зменшення ризиків, пов'язаних із такими подіями. Він відповідає на змінювану ризикову обстановку, зокрема зростаючу важливість кібербезпеки для сектора, та відображає досягнутий прогрес у побудові спільного державного-приватного партнерства з моменту публікації такого плану 2010 року. Відзначається, що досягнення сектора фінансових послуг після публікації плану 2010 року включають: 1) створення програми

кібербезпекових навчань для тестування та покращення процесів реагування на інциденти; 2) значне розширення можливостей обміну інформацією про кібербезпеку, зокрема через швидкий розвиток Фінансового центру аналізу та обміну інформацією («FS-ISAC») та створення Групи кіберрозвідки фінансового сектора Міністерства фінансів («CIG»); 3) створення формалізованої структури спільних робочих груп для просування конкретних завдань; 4) формалізація процесів координації технічної допомоги; 5) розширення співпраці з міжсекторальними та міжнародними партнерами [252].

Відповідно План захисту об'єктів критичної інфраструктури фінансового сектору України в контексті структури та змісту основних положень має: 1) розкривати результати огляду фінансової стабільності сектору та містити перелік відповідних ризиків; 2) встановлювати стратегічну основу, яка буде орієнтиром для визначення пріоритетів у повсякденній роботі сектору; 3) визначати ключові механізми, за допомогою яких стратегічна основа має бути впровадженою та оціненою у межах звітного періоду. Важливо, щоб над розробкою та впровадженням цього плану працювали усі зацікавлені суб'єкти, адже результати попередніх розвідок чітко демонструють факт того, що найбільш значущі результати функціонування механізму захисту об'єктів критичної інфраструктури можуть бути досягнуті внаслідок спільних, погоджених дій його суб'єктів. Здійснення відповідними суб'єктами погоджених дій задля досягнення спільної мети їхньої діяльності в фахових джерелах прийнято позначати як їх взаємодію. Значення взаємодії, як форми організації взаємозв'язку та взаємної підтримки, полягає у тому, що відповідні суб'єкти у взаємодії один з одним досягають значно більших результатів у менші строки із найменшими витратами сил [34, с. 58]. Іншими словами, взаємодія має вкрай позитивний вплив на підвищення ефективності відповідної діяльності. У межах функціонування адміністративно-правового механізму захисту об'єктів критичної інфраструктури фінансового сектору однією з провідних

форм взаємодії буде державно-приватна взаємодія, яка до того ж розглядається як і один з провідних принципів, на основі якого він побудований [92, с. 339].

Однак, варто зауважити, що реалізація державно-приватної взаємодії у сфері захисту критичної інфраструктури України потребує законодавчого врегулювання, методологічного та організаційно-технічного забезпечення узгоджених дій [108, с. 3–4]. І попри те, що Закон України «Про критичну інфраструктуру» містить окрему статтю, присвячену цій проблематиці, низка актуальних проблем досі існує. Зокрема державно-приватні партнерства, які не зовсім точно продумані, ризикують стати «порожніми коробками», приносячи обмежену або нульову додану вартість для захисту критично важливих об'єктів інфраструктури. Тому Н. Трушкіна та І. Жукова обґрунтовують думку, що доцільно внести зміни й доповнення до законів України «Про критичну інфраструктуру», «Про державно-приватне партнерство», Концепції створення державної системи захисту критичної інфраструктури, Стратегії національної безпеки України, Стратегії забезпечення державної безпеки, Стратегії кібербезпеки України, Стратегії інформаційної безпеки, Стратегії економічної безпеки, Енергетичної стратегії України, Національної транспортної стратегії України в частині створення належних інституційних умов для розвитку критичної інфраструктури на засадах публічно-приватного партнерства у контексті повоєнної відбудови національної економіки [214, с. 16].

Відповідно, аналіз наведеного матеріалу свідчить, що в якості однієї з основних проблем функціонування адміністративно-правового механізму захисту об'єктів критичної інфраструктури загалом, зокрема і фінансового сектору є вкрай низька якість законодавчої регламентації державно-приватної взаємодії та партнерства в цій сфері. Загостренню цієї проблематики сприяє недостатнє її опрацювання науковцями. Такий стан справ має негативний вплив як на ефективне функціонування відносин державно-приватної взаємодії та партнерства в сфері захисту об'єктів

критичної інфраструктури, так і на дотичні до неї суспільні відносини, як-то забезпечення національної безпеки й оборони, кіберзахисту інтересів держави тощо [92, с. 351].

Проаналізувавши різні документи [239; 255] щодо розбудови державно-приватного партнерства у сфері захисту об'єктів критичної інфраструктури в різних країнах вважаємо, що в Україні необхідно розробити та прийняти Концепцію сприяння розвитку державно-приватного партнерства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України. Для цього необхідно здійснити ряд заходів, а саме:

- провести діалог з лідерами юрисдикцій;
- встановити цілі щодо захисту об'єктів критичної інфраструктури фінансового сектору та роль кожного суб'єкта в цьому захисті;
- розробити стандарти очікуваних послуг та стабілізаційних цілей для систем життєзабезпечення, інфраструктури та ланцюгів постачання;
- сприяти діалогу для розуміння та інформування про фінансовий розвиток та пріоритети реагування і відновлення в разі настання кризових ситуацій;
- визначити внутрішні/зовнішні ресурси для розбудови/підвищення стійкості критичної інфраструктури у фінансовому секторі;
- впровадити та здійснювати моніторинг та оцінку ефективності проектів з пом'якшення наслідків кризових ситуацій;
- узгодити організаційні стратегії з юрисдикційними пріоритетами стійкості.

Таким чином, продовжуючи розгляд питання про основні положення майбутнього плану захисту об'єктів критичної інфраструктури фінансового сектору України, його стратегічна основа має репрезентувати забезпечення безперервного покращення безпеки та реагування на загрози через співпрацю регуляторів, приватного сектору, державних установ та міжнародних партнерів. Завданнями при цьому мають бути: а) виявлення, запобігання, припинення та завчасна підготовка до загроз та небезпек; б) зменшення

вразливостей; в) мінімізування потенційних наслідків від інцидентів або несприятливих подій, які можуть відбутися.

Акцентуємо, що для забезпечення безпеки та стійкості сектора необхідна ефективна публічна політика, яка враховує інтереси приватного сектору [252]. Тому актуальним є розвиток механізмів для саморегулювання, які стимулюватимуть представників сектору об'єднуватись в асоціації, ради чи комітети для можливості таких бути учасниками розробки політики захисту об'єктів критичної інфраструктури у досліджуваній сфері.

Наприклад, у США «FSSCC» та «FBIIС» проводять спільні засідання для обговорення прогресу у досягненні цілей сектора і визначення областей, де потрібна додаткова робота. Вони також зустрічаються окремо принаймні раз на місяць, щоб надати звіти про стан проектів та ініціативи та координувати нові та існуючі програми. Це дозволяє «FSSCC» та «FBIIС» відстежувати прогрес на основі розвиваючих проектних етапів. Цей підхід дав змогу, зокрема, розробити та реалізувати безперервну програму кібербезпекових вправ між державним і приватним секторами, координувати регулярні аналітичні обговорення загроз кібербезпеки та вдосконалити процеси реагування на інциденти. Крім того, постійна оцінка прогресу сектора, розробка нових програм за потреби та закриття програм, що виконали своє призначення, допомагає забезпечити, щоб окремі дії відповідали потребам зацікавлених сторін і могли бути ефективно адаптовані до змінювального середовища загроз [252].

Зокрема на фінансовому ринку України саморегулівні організації почали створюватися у першій половині 90-х років ХХ ст. Зараз на фінансовому ринку України існує значна кількість таких організацій (асоціації, ліги, об'єднання), які могли б претендувати на статус саморегулівних організацій в тому чи іншому сегменті фінансового ринку. Наприклад, на страховому сегменті фінансового ринку України здійснюють діяльність Ліга страхових організацій України, Федерація Страхових Посередників України, Асоціація «Страховий бізнес», Товариство актуаріїв

України, Моторне (транспортне) страхове бюро України, Авіаційне страхове бюро, Морське страхове бюро, Всеукраїнська громадська організація «Всеукраїнська асоціація аварійних комісарів», Українська федерація убезпечення, Аграрне страхове бюро. У банківському сегменті фінансового ринку України важливою є діяльність Асоціації українських банків, Асоціації «Український кредитно-банківський союз», Форуму провідних фінансових міжнародних інститутів, Української національної іпотечної асоціації, Української міжбанківської асоціації членів платіжних систем «ЄМА». Окрім того, численні неурядові організації створені у сфері надання послуг фінансовими компаніями (Українське товариство фінансових аналітиків, Всеукраїнська асоціація ломбардів, Асоціація «Українське об'єднання лізингодавців», Професійна асоціація корпоративного управління, Професійна асоціація фінансових компаній-управителів, Асоціація незалежних фінансових консультантів «Фінконсул») [37, с. 77–78].

Держава повинна стати ініціатором запровадження повноцінного саморегулювання у цій сфері. Першочерговим завданням на шляху до цього є вирішення питання збалансування інтересів державних органів і учасників ринку у процесі діяльності саморегулювних організацій. При цьому, не виключаючи обов'язковості державного нагляду і контролю діяльності суб'єктів ринку, цим інститутам можуть бути делеговані нормотворча, представницька, інформаційна та освітня функції регуляторів [37, с. 78].

Наступним напрямком розвитку адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України є адаптаційний, який передбачає подальшу імплементацію європейських стандартів, а також впровадження інших позитивних практик.

Уточнимо, що метою адаптації законодавства України до законодавства ЄС є досягнення відповідності правової системи України *acquis communautaire* з урахуванням критеріїв, що висуваються ЄС до держав, які мають намір вступити до нього. Адаптація законодавства України до законодавства ЄС є пріоритетною складовою процесу інтеграції України

до ЄС, що своєю чергою є пріоритетним напрямом української зовнішньої політики. Тому державна політика України щодо адаптації законодавства формується як складова частина правової реформи в Україні та спрямовується на забезпечення єдиних підходів до нормопроекування, обов'язкового врахування вимог законодавства ЄС під час нормопроекування, підготовки кваліфікованих спеціалістів, створення належних умов для інституціонального, науково-освітнього, нормопроектного, технічного, фінансового забезпечення процесу адаптації законодавства України [153].

Загалом передбачається, що питання про належність регулювання фінансових послуг до права ЄС базується на головній меті Європейського Союзу – створенні Єдиного Ринку в межах ЄС (перша опора ЄС). Узагальнимо, що зокрема вторинне законодавство ЄС сформоване на основі Регламенту (ЄС) № 2560/2001 Європейського Парламенту та Ради від 19 грудня 2001 року щодо транскордонних платежів у євро; Директива Європейського Парламенту та Ради 2002/47/ЄС від 6 червня 2002 року щодо угод про використання фінансових активів в якості предмета забезпечення виконання зобов'язання; Директива Європейського парламенту та Ради 2001/24/ЄС від 4 квітня 2001 стосовно заходів щодо відновлення платоспроможності та ліквідації кредитних установ; Директива Європейського парламенту та Ради 2000/46/ЄС від 18 вересня 2000 року щодо започаткування діяльності та її ведення установами, які проводять електронні розрахунки, та пруденційного нагляду за ними; Директива Європейського Парламенту та Ради 2000/12/ЄС від 20 березня 2000 року щодо започаткування діяльності кредитних установ та її ведення; Директива Європейського парламенту та Ради 97/5/ЄС від 27 січня 1997 року щодо транскордонних переказів; Директива Європейського парламенту та Ради 94/19/ЄС від 30 травня 1994 року щодо схем гарантування депозитів; Директива Ради 93/6/ЄЕС від 15 березня 1993 року щодо відповідності капіталу інвестиційних фірм та кредитних установ; Директива

Ради 89/117/ЄЕС від 13 лютого 1989 щодо зобов'язання стосовно публікації щорічних бухгалтерських документів структурними підрозділами кредитних та фінансових установ, що створені у державах-членах, головний офіс яких знаходиться на території іншої держави-члена; Директива Ради 87/102/ЄЕС Ради від 22 грудня 1986 року щодо наближення законів, підзаконних і адміністративних положень держав-членів щодо споживчого кредиту; Директива Ради 86/635/ЄЕС від 8 грудня 1986 року щодо річних звітів та консолідованих звітів банків та інших фінансових установ; 2000/408/ЄС: Рекомендація Комісії від 23 червня 2000 року щодо опублікування інформації про фінансові інструменти та про інші питання, спрямовані на уточнення інформації, яка повинна надаватися у відповідності до Директиви Ради 86/635/ЄЕС від 8 грудня 1986 року щодо річних бухгалтерських звітів та консолідованих звітів банків та інших фінансових установ (що повідомлена у документі за номером С (2000) 1372); 90/109/ЄЕС: Рекомендація Комісії від 14 лютого 1990 р. щодо прозорості банківських вимог щодо транскордонних фінансових операцій; 87/62/ЄЕС: Рекомендація Комісії від 22 грудня 1986 року щодо моніторингу та контролю за великими ризиками кредитних установ [153]. Загалом українське законодавство наближено до законодавства ЄС у сфері фінансових послуг, однак все ще актуально забезпечити належний розвиток державного внутрішнього фінансового контролю, привести цю сферу у відповідність до норм ЄС.

Щодо сфери критичної інфраструктури загалом, у тому числі її об'єктів у межах фінансового сектору маємо вказати, що держави – члени ЄС з-поміж іншого мають: 1) розвивати й надалі власні механізми координації залучених акторів у процесі реагування, забезпечити підготовку оглядів міжсекторального реагування на суттєві збої в основних послугах, що надаються критичною інфраструктурою. Започаткувати розроблення плану скоординованого реагування на збої в роботі критичної інфраструктури зі значним транскордонним значенням; 2) збільшити обмін інформацією на оперативному рівні з «ERCC» у контексті «UCPM», щоб покращити ранне

попередження та координувати реагування на збої в роботі критичної інфраструктури зі значним транскордонним значенням, забезпечуючи швидшу реакцію ЄС за потреби; 3) заохочувати операторів критичної інфраструктури та відповідні національні органи влади збільшувати свій потенціал, щоб мати можливість швидко відновити виконання життєво важливих функцій, що забезпечуються операторами критичної інфраструктури; 4) заохочувати операторів критичної інфраструктури під час реконструкції своєї інфраструктури будувати її так, щоб вона була максимально стійкою до повного спектра значних ризиків, беручи до уваги пропорційність заходів стосовно оцінки ризику та витрат; 5) прискорити підготовку до запровадження посилених вимог щодо кібербезпеки, маючи на меті розвиток спроможностей національних «CSIRT», перегляд стратегій кібербезпеки та національних планів реагування на інциденти й кризи в кібербезпеці; 6) утілювати в життя заходи, спрямовані на усвідомлення відповідними зацікавленими сторонами необхідності підвищення стійкості критичної інфраструктури; приділяти увагу проактивним стратегічним комунікаціям у контексті протидії гібридним загрозам і кампаніям, спрямованим на критичну інфраструктуру [200].

Варто зауважити, що деякі з цих заходів вже впровадженні чи впроваджуються в Україні, зокрема в частині розвитку кібербезпеки та координації з міжнародними партнерами.

Водночас для підвищення готовності ЄС до кризових ситуацій держави – члени ЄС мають: а) застосовувати методологію оцінювання ризиків критичної інфраструктури на основі аналізу впливу загроз будь-яких типів («all-hazard approach») при подальшій адаптації національних підходів до ризик-аналізу; б) розпочати розроблення заходів щодо підвищення стійкості критичної інфраструктури згідно з положеннями нового законодавства в цій сфері. Особливий акцент має бути на співпраці та обміні відповідною інформацією між державами-членами та Єврокомісією, виявленні загроз критичної інфраструктури транскордонного характеру та посиленні

підтримки операторів для забезпечення стійкості критичної інфраструктури; в) підтримувати проведення навчань і тренінгів з питань стійкості критичної інфраструктури, залучати експертів, заохочувати їх брати участь у навчальних тренінгових програмах; г) заохочувати та підтримувати операторів критичної інфраструктури, проводити стрес-тести, дотримуючись принципів, узгоджених на рівні ЄС. Стрес-тести мають оцінювати стійкість критичної інфраструктури до цілеспрямованих руйнівних атак; д) виділяти достатні фінансові ресурси для зміцнення спроможності відповідних національних органів, щоб мати можливість підвищувати стійкість критичної інфраструктури; е) використовувати потенційні можливості фінансування на рівні ЄС та держав-членів для підвищення стійкості критичної інфраструктури, а також заохочувати операторів критичної інфраструктури використовувати такі можливості фінансування. Зокрема, наголошується на доцільності використання програм, що фінансуються Фондом внутрішньої безпеки ЄС, Європейським фондом регіонального розвитку, Механізму цивільного захисту ЄС («UCPM»), Плану «REPowerEU», а також використовувати результати відповідних проектів у рамках дослідницьких програм, таких як «Horizon Europe»; ж) розвивати використання можливостей програми «Copernicus», системи «Galileo» та Європейської геостационарної навігаційної служби («EGNOS») для спостереження та обміну інформацією, а також використовувати можливості, які пропонуються на рівні ЄС, зокрема Урядовий супутниковий зв'язок («GOVSATCOM») космічної програми ЄС, для моніторингу критичної інфраструктури та підтримки прогнозування кризових ситуацій і реагування на них [200].

Також зауважимо, що в контексті зростаючої стурбованості щодо макрофінансової стабільності Міжнародний валютний фонд рекомендує:

– кіберстійкість фінансового сектора повинна бути посилена шляхом розробки адекватної національної стратегії кібербезпеки, відповідних регуляторних і наглядових рамок, здатної робочої сили в галузі кібербезпеки, а також внутрішніх та міжнародних механізмів обміну інформацією;

– звітність про кіберінциденти фінансовими установами перед наглядовими органами повинна бути посилена для забезпечення більш ефективного моніторингу кіберризиків;

– наглядові органи повинні покласти відповідальність на членів ради директорів за управління кібербезпекою фінансових установ і за сприяння розвитку відповідної культури ризику, кібергігієни та навчання та підвищення обізнаності у сфері кібербезпеки;

– фінансові установи повинні розробити та протестувати процедури реагування і відновлення, щоб залишатися оперативними в умовах кіберінцидентів. Національні органи влади також повинні розробити ефективні протоколи реагування та рамки управління кризами для вирішення системних кіберкриз [257].

Останнім напрямком розвитку адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України ми визначаємо функціональний, що має вирішити низку практичних проблем його здійснення. Саме до цього блоку ми відносимо ініціативи щодо необхідності розвитку механізмів для саморегулювання, належних нормативних основ для стимулювання державно-приватного партнерства у цій сфері, а також доцільності, наприклад:

– перегляду інституційної структури системи цього захисту, тим самим вирішити питання наявного дисбалансу у сфері реалізації громадського нагляду, зокрема і проведення незалежного аудиту діяльності уповноважених представників. На нашу думку, нині сформована інституційна система захисту критичної інфраструктури фінансового сектору потребує оптимізаційних змін у контексті розширення до загальнонаціонального рівня. Рада національної безпеки та оборони України має бути тим провідним органом, що контролює превентивність захисних дій, не обмежуючись функціями забезпечення стійкості, а від вертикалі якого функціонують інші інституції по горизонталі у тісній взаємодії між собою. Уточнимо, що Рада національної безпеки та оборони України відповідно до Конституції України

є координаційним органом з питань національної безпеки і оборони при Президентові України. Її функціями є: 1) внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони; 2) координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час; 3) координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України [172]. Однак варто зауважити, що пропоновані нами контрольні функції Ради мають обмежуватись інформаційно-аналітичним забезпеченням, оскільки це відповідає його основному призначенню. Вона не має здійснювати оперативне управління чи координацію дій інших органів, але виконуватиме роль органу, який збирає, аналізує та інформує про потенційні загрози і ризики у всіх секторах, де визначеними є об'єкти критичної інфраструктури, тим самим сприяючи своєчасному прийняттю рішень на найвищому рівні. Тобто ми відстоюємо необхідність збереження за такими суб'єктами їхньої самостійності та зведення повноважень Ради національної безпеки та оборони України до мінімально необхідних. Це вимагає проведення уніфікації чинного законодавства, зокрема і в контексті ідентифікації обов'язків кожного з представників означеної системи, що будуть підкріплені мірами відповідальності за порушення законодавства у сфері захисту об'єктів критичної інфраструктури;

– збільшення фінансування для програм тестування об'єктів критичної інфраструктури на предмет вразливостей – наразі існує значна кількість актуальних програм підтримки бізнесу від міжнародних організацій в Україні. Наприклад, Програма USAID «Кібербезпека критично важливої інфраструктури в Україні» спрямована на зміцнення кіберготовності та кіберстійкості України шляхом системних реформ, формування кадрового потенціалу України у сфері кібербезпеки, партнерства із приватним

сектором. Програма з менторства включає підвищення рівня підготовки країни до кіберзагроз, здатність збудувати міцний захист навколо критичної інфраструктури в Україні та поглиблення знань та навичок у сфері кібербезпеки [177]. Також надають гранти на реалізацію креативних та ефективних ініціатив і рішень, спрямованих на посилення національної готовності, зменшення вразливостей у сфері кібербезпеки та зміцнення критичної інфраструктури України у секторі кібербезпеки. Важливо, щоб такі ініціативи та рішення були спрямовані на досягнення однієї або кількох з наступних цілей: 1) зміцнення умов, що сприяють кібербезпеці, щоб створити безпечне та надійне середовище для прискорення розвитку людей, процесів і технологій на підтримку кібербезпеки у всіх секторах і об'єктах критичної інфраструктури в Україні; 2) розвиток кібербезпекової робочої сили України для зміцнення України як суверенної держави, побудованої на безпечній, захищеній та динамічній економіці, підтримуваній талановитим кадровим потенціалом; 3) створення стійкої індустрії кібербезпеки для стимулювання попиту та пропозиції українських рішень і постачальників послуг з кібербезпеки, щоб надати можливості, обладнання та фінансування підприємцям і компаніям у сфері кібербезпеки [77]. Зрозуміло, що зараз в Україні є критична потреба зібрати додаткові кошти на обороноздатність, однак збільшення фінансування для програм тестування об'єктів критичної інфраструктури на предмет вразливостей теж повинно бути в пріоритеті, адже сприятиме зменшенню ризиків виникнення критичних інцидентів;

– стандартизації процедур, що забезпечують організаційну стійкість – встановлення і використання чітких правил з метою забезпечення здатності об'єктів критичної інфраструктури фінансового сектору функціонувати під час кризових ситуацій;

– формування безпечних каналів для обміну інформацією між різними представниками національної системи захисту критичних інфраструктур. Уточнимо, що Регламент обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури, затверджений постановою

Кабінету Міністрів України від 14 жовтня 2022 року № 1174 визначає механізм інформаційної взаємодії між суб'єктами національної системи захисту критичної інфраструктури з метою забезпечення захисту та стійкості критичної інфраструктури. Передбачається, що інформаційна взаємодія забезпечується шляхом послідовного обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури, що здійснюється відповідальними особами, визначеними такими суб'єктами, з використанням засобів електронних комунікацій, національної системи конфіденційного зв'язку, спеціального зв'язку, шифрувального зв'язку та інформаційно-комунікаційних систем [164]. І попри сформованість цього механізму, він відзначається рядом недоліків, головним з яких є обмеження площини здійснення інформаційної взаємодії між визначеним колом суб'єктів без урахування необхідності залучення сторонніх учасників, наприклад, інших секторальних органів. Тобто необхідним є більш відкритий підхід до інформаційного обміну, використання для цього сучасних інструментів комунікації. Окрім того, Регламент не враховує можливість виникнення перебоїв в системах зв'язку, зумовлених, наприклад, кіберзагрозами чи технічними збоями;

- забезпечення розвитку платформ для публічного обговорення проблем функціональності об'єктів критичної інфраструктури фінансового сектору та формування ефективних механізмів обміну досвідом з міжнародними партнерами;

- системного здійснення підвищення кваліфікації кадрового ресурсу через програми професійного розвитку та навчання.

Таким чином, маємо такі ключові висновки:

- беручи до уваги останні оптимізаційні зміни чинного законодавства, можемо впевнено стверджувати, що більшість модернізацій була актуальною вже досить тривалий час;

- пропонуємо трьох векторну структуру оптимізаційних змін вітчизняного адміністративного законодавства у сфері захисту об'єктів

критичної інфраструктури фінансового сектору України, що передбачає: 1) нормативний аспект (розробка та затвердження Плану захисту об'єктів критичної інфраструктури фінансового сектору України); 2) адаптаційний (подальша імплементація європейських стандартів, а також впровадження інших позитивних практик); 3) функціональний (вирішення низки практичних проблем його здійснення).

Висновки до Розділу 3

1. Зауважено, що оглядовий аналіз міжнародних та регіональних основ здійснення захисту об'єктів критичної інфраструктури фінансового сектору України переконливо свідчить про актуалізацію низки питань, яким в Україні приділено недостатньо уваги. Визначено, що наразі досить гостро стоїть питання забезпечення кіберзахисту, а також захисту критичної інфраструктури від терористичних атак, забезпечення глобальної фінансової стабільності.

2. З'ясовано, що в останні роки Європа зосередилася на законодавстві, що стосується інформаційно-комунікаційних технологій і кібербезпеки для європейського фінансового сектора. Вважається, що оскільки відповідність стандартам є одним із головних факторів кіберстійкості, розумна та послідовна регуляторна стратегія може допомогти забезпечити необхідну базову лінію безпеки у фінансовому секторі для пом'якшення інституційних і системних ризиків.

3. Доведено, що поточний європейський нормативно-правовий ландшафт у сфері інформаційно-комунікаційних технологій та кіберризиків для фінансового сектору є багаторівневим і складним. Він включає численні європейські та національні нормативні акти і галузеві стандарти. Фінансові установи мають дотримуватися правил щодо захисту об'єктів критичної інфраструктури, загального європейського законодавства з питань захисту

даних, а також спеціальних норм у фінансовому секторі, які поділяються на підсектори: банківську справу, страхування та інфраструктури ринку. Причому важливо, що не всі країни-члени застосовують ці стандарти як національні, що зумовлює відмінності здійснення ними адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору.

4. Щодо конкретного досвіду адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору, піддано аналізу практики США, адже це країна, що вже багато років займає лідерські позиції у сфері захисту критичної інфраструктури, зокрема і фінансового сектору.

5. Виявлено, що у США системно та планомірно розробляються нормативно-правові основи для підвищення стійкості фінансових установ до системних ризиків. Вони диференціюються на загальні та спеціальні. Загальні об'єктивуються, наприклад, у межах Директиви Президента про національну безпеку №7, яка встановлює національну політику для федеральних департаментів та агентств щодо ідентифікації та пріоритизації об'єктів критичної інфраструктури та їх захисту від терористичних атак. Ключовим з таких також є Національний план захисту інфраструктури, який постійно оновлюється, демонструючи еволюційність концепцій координації національних зусиль з управління ризиками для критичної інфраструктури країни. До числа спеціальних віднесено Спеціальний план для сектору фінансових послуг, що адаптує положення Національного плану до унікальних характеристик та ризиків, притаманних цьому сектору.

6. З'ясовано, що ключовими суб'єктами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору США є: Міністерство національної безпеки США, Міністерство фінансів США (секторальний орган), федеральні фінансові регулятори, Комітет з інформаційної інфраструктури фінансових і банківських послуг. Виявлено, що приватний сектор не тільки залучений до процедур оптимізації здійснення адміністративно-правового захисту у цій сфері, а й належним чином інформаційно забезпечений, адже публічними є не тільки звіти про

діяльність уповноважених органів, а й огляди щодо вивчення впливу окремих явищ на стабільність функціонування сектору загалом. Провідною особливістю досвіду цієї країни також визначено інтеграцію фізичної та кібернетичної безпеки і стійкості критичних інфраструктур.

7. Узагальнено, що позитивний досвід США та ЄС у сфері захисту критичної інфраструктури фінансового сектору може стати корисним прикладом для України в контексті: 1) наявності спеціальних планів захисту критичної інфраструктури фінансового сектору, що визначають особливості її захисту від системних загроз і ризиків; 2) інституційної різноманітності, що має прояв широким колом суб'єктів захисту та чіткістю процедур обміну інформацією між ними; 3) активної участі приватного сектору та ефективної координації між державними та приватними суб'єктами; 4) встановлення єдиних вимоги до кібербезпеки для критичних секторів, включно з фінансовим; 5) розвинутих систем партнерства між державними та приватними установами; 6) чіткого розподілу обов'язків та відповідальності суб'єктів реалізації такого захисту; 7) дієвості механізмів оцінки кіберстійкості об'єктів критичної інфраструктури фінансового сектору.

8. Визначено доцільними для впровадження до національної правової системи такі позитивні практики у сфері захисту об'єктів критичної інфраструктури фінансового сектору як: розробка спеціалізованих стратегічних планів; встановлення чітких процедур обміну інформацією; розвиток стимулів для залучення приватного сектора до процесів підвищення загальної стійкості фінансової системи; запровадження єдиних вимог до кібербезпеки фінансового сектору; створення платформ для обміну публічною інформацією; чітке визначення обов'язків і відповідальності суб'єктів захисту об'єктів критичної інфраструктури фінансового сектору та впровадження механізмів оцінки їх кіберстійкості.

9. Констатовано, що досліджувана сфера має ряд позитивних тенденцій для подальшого вдосконалення адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України.

10. Визначено, що основним напрямком розвитку адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України є нормативний, що передбачає формування якісної основи для захисту об'єктів критичної інфраструктури фінансового сектору України. Зауважено, що у цьому контексті йдеться не про зміни та доповнення до чинного законодавства України, а про необхідність аналогічно досвіду США розробити та затвердити План захисту об'єктів критичної інфраструктури фінансового сектору України, як специфічної деталізації Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури.

11. Запропоновано, щоб план захисту об'єктів критичної інфраструктури фінансового сектору України в контексті структури та змісту основних положень: 1) розкривав результати огляду фінансової стабільності сектору та містити перелік відповідних ризиків; 2) встановлював стратегічну основу, яка буде орієнтиром для визначення пріоритетів у повсякденній роботі сектору; 3) визначав ключові механізми, за допомогою яких стратегічна основа має бути впровадженою та оціненою у межах звітного періоду. Наголошено на важливості, щоб над розробкою та впровадженням цього плану працювали усі зацікавлені суб'єкти, а щодо стратегічної основи уточнюється, що така має репрезентувати забезпечення безперервного покращення безпеки та реагування на загрози через співпрацю регуляторів, приватного сектору, державних установ та міжнародних партнерів. Завданнями при цьому мають бути: а) виявлення, запобігання, припинення та завчасна підготовка до загроз та небезпек; б) зменшення вразливостей; в) мінімізування потенційних наслідків від інцидентів або несприятливих подій, які можуть відбутися.

12. Доведена необхідність розробки та прийняття Концепції сприяння розвитку державно-приватного партнерства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України. Уточнено, що для цього необхідно здійснити ряд заходів, а саме: провести діалог з лідерами

юрисдикцій; встановити цілі щодо захисту об'єктів критичної інфраструктури фінансового сектору та роль кожного суб'єкта в цьому захисті; розробити стандарти очікуваних послуг та стабілізаційних цілей для систем життєзабезпечення, інфраструктури та ланцюгів постачання; сприяти діалогу для розуміння та інформування про фінансовий розвиток та пріоритети реагування і відновлення в разі настання кризових ситуацій; визначити внутрішні/зовнішні ресурси для розбудови/підвищення стійкості критичної інфраструктури у фінансовому секторі; впровадити та здійснювати моніторинг та оцінку ефективності проектів з пом'якшення наслідків кризових ситуацій; узгодити організаційні стратегії з юрисдикційними пріоритетами стійкості.

13. Наступним напрямком розвитку адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України названо адаптаційний, який передбачає подальшу імплементацію європейських стандартів, а також впровадження інших позитивних практик. Констатується, що загалом українське законодавство наближено до законодавства ЄС у сфері фінансових послуг, однак все ще актуально забезпечити належний розвиток державного внутрішнього фінансового контролю, привести цю сферу у відповідність до норм ЄС. Виявлено низку ключових вимог та рекомендацій щодо розвитку сфери захисту критичної інфраструктури загалом, у тому числі її об'єктів у межах фінансового сектору.

14. Останнім напрямком розвитку адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України названо функціональний, який має вирішити низку практичних проблем його здійснення. Окрім необхідності розвитку механізмів стимулювання державно-приватного партнерства та саморегулювання, які стимулюватимуть представників сектору об'єднуватись в асоціації, ради чи комітети для можливості таких бути учасниками розробки політики захисту об'єктів критичної інфраструктури у досліджуваній сфері, обґрунтовується

необхідність: 1) переглянути інституційну структуру системи цього захисту, тим самим вирішити питання наявного дисбалансу у сфері реалізації громадського нагляду, зокрема і проведення незалежного аудиту діяльності уповноважених представників; 2) збільшити фінансування для програм тестування об'єктів критичної інфраструктури на предмет вразливостей; 3) стандартизувати процедури, що забезпечують організаційну стійкість; 4) сформувати безпечні канали для обміну інформацією між різними представниками національної системи захисту критичних інфраструктур; 5) забезпечити розвиток платформ для публічного обговорення проблем функціональності об'єктів критичної інфраструктури фінансового сектору та сформувати ефективні механізми обміну досвідом з міжнародними партнерами; 6) системно здійснювати підвищення кваліфікації кадрового ресурсу через програми професійного розвитку та навчання.

15. Узагальнено, що оптимізаційні зміни вітчизняного адміністративного законодавства у сфері захисту об'єктів критичної інфраструктури фінансового сектору України мають трьох векторну структуру, що передбачає: 1) нормативний аспект (розробка та затвердження Плану захисту об'єктів критичної інфраструктури фінансового сектору України); 2) адаптаційний (подальша імплементація європейських стандартів, а також впровадження інших позитивних практик); 3) функціональний (вирішення низки практичних проблем його здійснення).

ВИСНОВКИ

У дисертації представлено результати проведеного комплексного аналізу особливостей здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, а також окреслено напрями його оптимізації. Основні з них такі:

1. Обґрунтовується, що правовий концепт «критична інфраструктура фінансового сектору України» позначає коло суспільних відносин виникнення яких обумовлено необхідністю забезпечення безперебійного функціонування окремих складових фінансового сектору, які є критично важливими в аспекті спроможності держави обслуговувати свої потреби і розвиватись у руслі автономності та самодостатності, а також утвердження як правової, демократичної, суверенної держави, яка належним чином виконує своє соціальне призначення з дискурсу гарантування кожному непорушності його прав та законних інтересів. Висунуто припущення, що така інтерпретація не зумовлює виникнення сумнівів чи дискусій щодо того, що держава має створити усі необхідні умови задля того, щоб усі критично важливі складові фінансового сектору перебували у стані захисту, тобто були забезпеченими можливістю здійснення адекватної, належної, допустимої, необхідної та ефективної реакції на фактори, чинники, обставини, події тощо, які потенційно чи реально здатні або завдають негативного впливу на функціональність їхньої роботи.

2. Узагальнено, що без адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України навряд чи вдасться забезпечити належний рівень безпеки та стабільності ринку фінансових послуг та пов'язаних з ними операцій в Україні, адже ризики та загрози є постійними, різноманітними, а недостатня увага та реагування на них можуть мати катастрофічні наслідки. Визначено, що адміністративно-правовий захист об'єктів критичної інфраструктури фінансового сектору України є системою заходів охоронного та захисного спрямування, реалізованих

уповноваженими суб'єктами національної системи захисту критичної інфраструктури задля забезпечення стійкості та безпеки сегментів ринку фінансових послуг та окремих фінансових операцій, що формують фінансовий сектор критичної інфраструктури України. Констатується, що у досліджуваній площині ризику мають два різновиди: ті, що пов'язані із виникненням загроз (неврахування ризику веде до загрози); ті, що існують паралельно з ймовірністю виникнення загроз (самостійні ризику, що наявними є постійно). Причому другий контекст є значно ширшим. Більшою мірою саме про нього йдеться у нормах чинного законодавства. Натомість загрозою, за таким баченням, є фізичний прояв небезпеки від наявності (виникнення) певного явища. З точки зору наукового суб'єктивізму визначається, що ризик має бути пов'язаним із загрозою, точніше зумовлювати наявність останніх.

3. Доведено, що механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України: а) є сукупним терміном, термінологічний аспект якого формується шляхом поєднання базових характерних ознак адміністративно-правових механізмів загалом та адміністративно-правового механізму захисту – зокрема; б) є репрезентацією практичного прояву дії охоронних та захисних заходів у цій сфері; в) має власну сферу об'єктивізації – суспільні відносини, породжені необхідністю забезпечення схоронності об'єктів критичної інфраструктури фінансового сектору України; г) як правове явище діяльнісного характеру має власну систему завдань, функцій та цілей; д) з внутрішньо організаційного дискурсу має свій структурний склад, відмінний від тих, що встановлені для інших правових механізмів забезпечення безпеки та стійкості об'єктів критичної інфраструктури фінансового сектору України.

4. Визначено, що нормативно-правовими основами адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України є сукупність правових документів різної юридичної сили, виданих (прийнятих) з метою врегулювання питань: а) кіберзахисту, інформаційної

безпеки, інституційної збалансованості цієї сфери загалом; б) реалізації міжвідомчих механізмів взаємодії між регуляторами та іншими суб'єктами національної системи її захисту; в) управління та моніторингу ризиків, пов'язаних із фінансовими операціями та діяльністю установ, які входять до переліку об'єктів критичної інфраструктури; г) контрольно-наглядової діяльності у цій сфері, включаючи імплементацію міжнародних стандартів та рекомендацій. Однак констатується, що досліджувані нормативно-правові основи перебувають на стадії формування своєї повноцінної правової структури, адже наразі продовжується процес оптимізації їх змісту. Виявлено, що основоположними з таких є акти секторальних органів, проте основна проблема полягає у відсутності їх публічності.

5. Доведено, що принципи адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, як правила організаційного та практико-реалізаційного характеру, мають подвійну юридичну спрямованість сфери розповсюдження своєї дії. З одного боку, уповноважені представники національної системи їхнього захисту мають дотримуватись встановлених загальноправових, галузевих та спеціальних орієнтирів, щоб ефективно та результативно виконувати своє функціональне призначення. З іншого боку, вони покладають на державу обов'язок забезпечити цим суб'єктам належні умови для реалізації задекларованих принципів, зокрема через створення правового, організаційного та ресурсного забезпечення. З'ясовано, що розвиток нової філософії забезпечення безпеки зумовив виникнення низки нових правил адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України, обумовлених необхідністю розвитку «культури управління ризиками». Серед таких ключовими є: 1) принцип комунікативної взаємодії між представниками держави та приватним сектором; 2) принцип системно здійснюваної співпраці між усіма суб'єктами та учасниками захисту об'єктів критичної інфраструктури фінансового сектору України;

3) принципом автономної стійкості; 4) принцип міжнародного співробітництва.

6. Визначено, що система суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України – це цілісне інституційне утворення, що має функціонувати на засадах єдності та диференціації, гармонійності та кооперації. Уточнено, що в умовах сучасності можна вести мову про її сформованість, однак не публічність. Йдеться зокрема про те, що переважна частина прийнятих рішень та реалізованих заходів є внутрішньоорганізаційним аспектом розвитку означеної сфери, а отже – широкий громадський загаль не має до неї доступу навіть в інформаційному аспекті. Яскраво це демонструється на прикладі Міністерства фінансів України, яке нормативно визначене як секторальний орган у сфері захисту критичної інфраструктури фінансового сектору України, що має низку необхідних повноважень, доступ до аналізу практичної реалізації яких фактично відсутній. Аналогічно й щодо рішень Національного банку України.

7. Обґрунтовано необхідність диференціації категорій «форми», «методи» та «інструменти» в контексті їх використання в управлінсько-організаційному, регуляторному чи іншому державно-владному процесі. Визначено, що інструментальний контекст адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України репрезентується через систему варіантів зовнішнього оформлення управлінського рішення та конкретного підходу, застосовного до досягнення поставлених у ньому цілей.

8. Доведено, що позитивний досвід США та ЄС у сфері захисту критичної інфраструктури фінансового сектору може стати корисним прикладом для України в контексті: 1) наявності спеціальних планів захисту критичної інфраструктури фінансового сектору, що визначають особливості її захисту від системних загроз і ризиків; 2) інституційної різноманітності, що має прояв широким колом суб'єктів захисту та чіткістю процедур обміну

інформацією між ними; 3) активної участі приватного сектору та ефективної координації між державними та приватними суб'єктами; 4) встановлення єдиних вимоги до кібербезпеки для критичних секторів, включно з фінансовим; 5) розвинутих систем партнерства між державними та приватними установами; 6) чіткого розподілу обов'язків та відповідальності суб'єктів реалізації такого захисту; 7) дієвості механізмів оцінки кіберстійкості об'єктів критичної інфраструктури фінансового сектору.

9. Висунуто припущення, що нині сформована інституційна система захисту критичної інфраструктури фінансового сектору потребує оптимізаційних змін у контексті розширення до загальнонаціонального рівня. Рада національної безпеки та оборони України має бути тим провідним органом, що контролює превентивність захисних дій, не обмежуючись функціями забезпечення стійкості, а від вертикалі якого функціонують інші інституції по горизонталі у тісній взаємодії між собою. Однак уточнено про важливість збереження за такими суб'єктами їхньої самостійності та зведення повноважень Ради національної безпеки та оборони України до мінімально необхідних повноважень. Це вимагає проведення уніфікації чинного законодавства, зокрема і в контексті ідентифікації обов'язків кожного з представників означеної системи, що будуть підкріплені мірами відповідальності за порушення законодавства у сфері захисту об'єктів критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністративне право України в сучасних умовах (виклики початку XXI століття): монографія. За заг. ред. Галунька В. В. «Херсонська міська друкарня», 2010. 378 с.
2. Адміністративне право України. Повний курс. За загальн. ред. Галунька В.. Херсон: Олді-Плюс, 2018. 446 с.
3. Адміністративне право України: навчальний посібник: у 2-х томах. За заг. ред. Галунька В. В. Херсон: ПАТ «Херсонська міська друкарня», 2011. Т. 1: Загальне Адміністративне право. 320 с.
4. Адміністративне право України. За заг. ред. Битяка Ю. П. К.: Юрінком Інтер, 2007. 544 с.
5. Албул С. Націоналізація «Сенс Банку»: холдинг російського олігарха Фрідмана подав позов на мільярд доларів проти України. LB.ua, 2024 URL: <http://surl.li/ronwdr>
6. Алфьоров, С. М. Адміністративно-правовий механізм протидії корупції в органах внутрішніх справ: автореф. дис. ... д-ра юрид. наук: 12.00.07; Харк. нац. ун-т внутр. справ. Харків, 2011. 38 с.
7. Арістова А., Мазур Г. Інструментарій державного антикризового управління в банківському секторі. *Вісник КНТЕУ*, 2010. № 2. С. 88–102.
8. Банки фіксують відновлення попиту на кредити та очікують на подальше зростання корпоративного і роздрібного портфельів – результати Опитування про умови банківського кредитування. Національний банк України, 2023. URL: <https://bank.gov.ua/ua/news/all/banki-fiksuyut-vidnovlennya-popitu-na-kredit-ta-ochikuyut-na-podalshe-zrostannya-korporativnogo-i-rozdribnogo-portfeliv--rezultati-opituvannya-pro-umovi-bankivskogo-kredituvannya>
9. Барчук В. О. Адміністративно-правовий механізм охорони лісового фонду в Україні: дис. ... доктора філософії: 081 «Право». Науково-дослідний інститут публічного права, Київ, 2021. 226 с.

10. Баштанник О. Концептуальні засади визначення феномену спроможності в сучасній методології дослідження державного управління. *Публічне управління та місцеве самоврядування*, 2023. № 2. С. 10–18.
11. Бенефіціарна власність юридичних осіб. Міністерство фінансів України, 2023. 66 с. URL: <http://surl.li/raayjk>
12. Белєвцева В. До питання класифікації адміністративно-правових режимів. *Вісник Академії правових наук України*, 2009. № 2 (57). С. 103–111.
13. Білий Д. О. Поняття та елементи механізму адміністративно-правового захисту прав пацієнтів. *Juris Europensis Scientia*, 2022. № 1. С. 62–66.
14. Бірюков Д. С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики. *Науково-інформаційний вісник Академії національної безпеки*, 2015. № 3-4. С. 155–170.
15. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні. К.: НІСД, 2012. 57 с.
16. Бірюков Д. С., Кондратов С. І., Насвіт О. І., Суходоля О. М. Зелена книга з питань захисту критичної інфраструктури в Україні: аналітична доповідь. К.: НІСД, 2015. 35 с.
17. Бірюков Д. С., Кондратов С. І. Актуальні питання захисту критично важливої для життєдіяльності держави інфраструктури. *Стратегічні пріоритети*, 2011. №4 (21). С. 113–117.
18. Богачова Л. Л. Принцип правової визначеності в європейському і національному праві (змістовна характеристика). *Теорія і практика правознавства*, 2013. Вип. 2.
19. Бондаренко К. В. До питання про форми й методи державного управління. *Вісник Запорізького національного університету. Юридичні науки*, 2015. № 4(1). С. 111–118.
20. Боняк В. О. Конституційно-правові засади, конституційно-правові основи та конституційно-правові принципи: співвідношення понять.

Науковий вісник Дніпропетровського державного університету внутрішніх справ, 2015. № 2. С. 64–76.

21. Булавіна С., Давидова Т. «Захист» та «охорона»: теоретичні аспекти юридичних термінів. *Історико-правовий часопис*, 2017. № 1. С. 27–31.

22. Бурятинська Н. І. Правові засоби: поняття та їх види. Шляхи активізації інноваційної діяльності в освіті, науці, економіці: матеріали Всеукр. наук.-практ. конф.: у 2-х т. орг. ком.: Крисоватий А. І., Задорожний М. В., Погріщук Б. В. та ін. Вінниця: ВННІЕ ТНЕУ, 2016. Т. 1. С. 190–192.

23. В Ощадбанку стався технічний збій: клієнти скаржаться на роботу сервісів. Мінфін, 2022. URL: <https://minfin.com.ua/ua/2022/09/01/91503987/>

24. Валькова Є. Зміст та структура механізму адміністративно-правового регулювання у сфері охорони права інтелектуальної власності. *Форум права*, 2012. № 3. С. 84–88.

25. Вархов А. Г. Адміністративно-правовий механізм взаємодії суб'єктів сектору безпеки й оборони щодо забезпечення національної безпеки: питання теорії та практики: дис. ... канд. юрид. наук: 12.00.07. Науково-дослідний інститут публічного права. Київ, 2023. 226 с.

26. Вархов А. Г. Організація та здійснення взаємодії суб'єктів сектору безпеки й оборони щодо забезпечення національної безпеки України: аспекти доцільності. *Науковий вісник публічного та приватного права*, 2022. Вип. 6. С. 78–81.

27. Вдарити по центру банківських операцій. Чи можуть російські терористи «покласти» банки? ЕП, 2022. URL: <https://www.epravda.com.ua/rus/publications/2022/12/15/695046/>

28. Великий тлумачний словник сучасної української мови (з дод., допов. та CD) уклад. і голов. ред. Бусел В. Т. Київ; Ірпінь: ВТФ «Перун», 2009. 1736 с.

29. Венгер В. М. Прозорість як принцип діяльності органів публічної влади. *Наукові записки НаУКМА. Юридичні науки*, 2017. Т. 200. С. 79–84.

30. Визначений перелік банків, що є об'єктами критичної інфраструктури в банківській системі України. Національний банк України, 2021. URL: <https://bank.gov.ua/ua/news/all/viznacheniy-perelik-bankiv-scho-ye-obyektami-kritichnoyi-infrastrukturi-v-bankivskiy-sistemi-ukrayini>

31. Визначення прозорості: які інструменти вимірювання існують в Україні. Інститут аналітики та адвокації, 2023. URL: <https://iaa.org.ua/articles/defining-transparency-what-measurement-tools-exist-in-ukraine/>

32. Визначено критерії віднесення об'єктів банківської системи до критичної інфраструктури. Національний банк України, 2020. URL: <https://bank.gov.ua/ua/news/all/viznacheno-kriteriyi-vidnesennya-obyektiv-bankivskoyi-sistemi-do-kritichnoyi-infrastrukturi>

33. Вільний рух капіталу без будь-яких валютних обмежень, кінцева мета НБУ. Дебет-Кредит, 2019. URL: <https://news.dtki.ua/finance/currency-and-securities/55155-vilnii-rux-kapitalu-bez-bud-iyakix-valiutnix-obmezen-kinceva-meta-nbu>

34. Гаєнко В. І., Литвинов О. М. Деякі міркування щодо організації взаємодії на досудовому слідстві. *Право і безпека*, 2003. № 2'3. С. 58–60.

35. Галай В. О., Яворська О. О. Основні принципи діяльності органів публічної адміністрації як запорука забезпечення прав і свобод людини. *Актуальні проблеми держави і права*, 2014. Вип. 72. С. 300–305.

36. Гапонюк О. І. Концептуальні передумови становлення та розвитку фінансового сектору України. *Правовий часопис Донбасу*, 2022. № 2 (79). URL: <https://ljd.dnuvs.in.ua/wp-content/uploads/2022/06/gaponuk.pdf>

37. Гарбар Ж. В., Гарбар В. А. Саморегулівні організації в системі функціонування фінансового ринку. *Науковий вісник Ужгородського національного університету*, 2017. Вип.15, Ч. 1. С. 76–79.

38. Гладкова В., Федотова Ю. Функції управлінської діяльності менеджера освітньої установи. *Витоки педагогічної майстерності. Серія: Педагогічні науки*, 2009. Вип. 6. С. 263–266.

39. Гладун З. Адміністративно-правове регулювання охорони здоров'я населення в Україні: монографія. Київ: «Юрінком Інтер», 2007. 720 с.

40. Глущенко Н. В. Поняття адміністративно-правового механізму захисту прав у медичній сфері. *Правові горизонти*, 2018. № 8 (21). С. 65–69.

41. Гончарук С. Адміністративне право України. Загальна та Особлива частини: навч. посібник. Київ: «Аванпост-прим», 2000. 240 с.

42. Горбась Д. В. Здійснення суб'єктивних цивільних прав фізичних осіб: поняття, способи, межі: дис. ... канд. юрид. наук: 12.00.03. Київ, 2008. 219 с.

43. Грохольський В. Л. Управління діяльністю спеціальних підрозділів МВС України по боротьбі з організованою злочинністю: дис. ... д-ра юрид. наук: 12.00.07. Харків, 2004. 427 с.

44. Група з розробки фінансових заходів боротьби з відмиванням грошей (FATF). Державна служба фінансового моніторингу України. gov.ua, 2019. URL: <https://fiu.gov.ua/pages/dijalnist/mizhnarodne-spivrobitnictvo/mizhnarodni-organizaci/grupa-z-rozrobki-finansovix-zaxodiv-borotbi-z-vidmivannyam-groshej-FATF.html>

45. Гудков Д. Адміністративно-правові засоби запобігання і протидії корупції: дис...канд. юрид. наук.: 12.00.07; Держ. ун-т. Суми, 2018. 249 с.

46. Гук А. С. Адміністративні форми та методи публічного врядування. *Актуальні проблеми державного управління*, 2013. № 1 (43). С. 78–83.

47. Даниленко А. О. Засади публічного адміністрування в Україні: дис. ... до-ра філософії 081 «Право». Науково-дослідний інститут публічного права, Київ, 2020. 215 с.

48. Данильян О. Г., Дзьобань О. П. Філософія: підручник. 2-ге вид., переробл. і допов. Харків: Право, 2018. 432 с.

49. Дворкін, Р. Серйозний погляд на права; пер. з англ. Фролкіна А. К.: Вид-во Соломії Павличко «Основи», 2000. 519 с.

50. Держспецзв'язку підготувала Методичні рекомендації для розробки місцевих програм забезпечення безпеки та стійкості критичної інфраструктури. Держспецзв'язку. gov.ua, 2023. URL: <https://cip.gov.ua/ua/news/derzhspetszv-yazku-pidgotuvala-metodichni-rekomendaciyi-dlya-rozrobki-miscevikh-program-zabezpechennya-bezpeki-ta-stiikosti-kritichnoyi-infrastrukturi>

51. Деякі питання запровадження в діяльність центральних органів виконавчої влади системи оцінки СОСТА Україна: Постанова Кабінету Міністрів України від 26.01.2022 р. № 59. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/59-2022-%D0%BF/ed20220126#n69>

52. Деякі питання об'єктів критичної інформаційної інфраструктури: постанова Кабінету Міністрів України від 09.10.2020 р. № 943. Урядовий кур'єр, 2020. № 205.

53. Деякі питання об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF>

54. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Міжнародний документ від 06.07.2016 р. № 2016/1148. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/984_013-16/ed20160706#n120

55. Директива Європейського Парламенту і Ради (ЄС) 2018/843 від 30 травня 2018 року про внесення змін до Директиви (ЄС) 2015/849 про запобігання використанню фінансової цілей відмивання грошей або фінансування тероризму та про внесення змін до директив 2009/138/ЄС і

2013/36/ЄС: Міжнародний документ від 30.05.2018 р. № 2018/843. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/984_010-18#Text

56. Директива Європейського Парламенту і Ради 2002/87/ЄС від 16 грудня 2002 року про додатковий нагляд за кредитними установами, страховими компаніями та інвестиційними фірмами, що належать до фінансового конгломерату, та про внесення змін до директив Ради 73/239/ЄЕС, 79/267/ЄЕС, 92/49/ЄЕС, 92/96/ЄЕС, 93/6/ЄЕС та 93/22/ЄЕС, а також до директив Європейського Парламенту і Ради 98/78/ЄС та 2000/12/ЄС. Міжнародний документ від 16.12.2002 р. № 2002\87\ЄС. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/984_012-02/ed20140101#n23

57. Директива Європейського Парламенту і Ради 2012/18/ЄС від 4 липня 2012 року про контроль загроз виникнення значних аварій, пов'язаних із використанням небезпечних речовин, та про внесення змін і подальше скасування Директиви Ради 96/82/ЄС: Міжнародний документ від 04.07.2012 р. № 2012/18/ЄС. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/984_011-12/ed20120704#n77

58. Директива Ради 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту: Міжнародний документ від 08.12.2008 р. № 2008/114/ЄС. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/984_002-08#Text

59. Дніпров О. Адміністративно-правові відносини в умовах трансформації предмета адміністративного права. *Підприємництво, господарство і право*, 2021. № 3. С. 175–179.

60. Дьомін І. Адміністративно-правові засади запобігання та протидії корупції міліцією України: автореф. дис. ... канд. юрид. наук: 12.00.07; Відкритий міжнар. ун-т «Україна». Київ, 2011. 19 с.

61. Дяченко Ю. Ю. Реструктуризація фінансового сектору в Україні: автореф. дис. ... канд. екон. наук: спец. 08.00.01. К., 2010. 19 с.
62. Єрменчук О. П., Пальчик М. Л. Проблемні аспекти правового регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури URL: <https://journals.urau.ua/ispss/article/download/196014/197927/441005>
63. Єщук О. М. Адміністративно-правова охорона: теорія, практика та перспективи розвитку: дис. ... д-ра юрид. наук: 12.00.07. Київ, 2017. 464 с.
64. Жук Т. Адміністративно-правові засади забезпечення взаємодії контрольно-наглядових органів з іншими суб'єктами сектору безпеки з метою охорони національних інтересів: дис. ... канд. юрид. наук: 12.00.07. НДПП. Київ, 2021. 230 с.
65. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки) (аналітична записка). Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/sites/default/files/2017-03/KI_-Ivanyuta-3a331.pdf
66. Закони управління ризиками. Запорізький національний університет. URL: <https://moodle.znu.edu.ua/mod/resource/view.php?id=116784>
67. Захист критичної інфраструктури від російських атак потребує спільної роботи всіх. Державна служба спеціального зв'язку та захисту інформації України, 2023. URL: <https://cip.gov.ua/ua/news/zakhist-kritichnoyi-infrastrukturi-vid-rosiiskikh-atak-potrebuye-spilnoyi-roboti-vsikh>
68. Звіт про діяльність Ради з фінансової стабільності серпень 2022 липень 2023. Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/FSB_Report%202022-2023.pdf?v=7
69. Зеленський ліквідував Нацкомфінпослуг. Укрінформ, 2020. URL: <https://www.ukrinform.ua/rubric-economy/3055705-zelenskij-likviduvav-nackomfinposlug.html>

70. Золотухіна Л. Адміністративно-правовий механізм забезпечення реалізації публічного інтересу. *In: Jurnalul juridic national: teorie și practică*, 2019, №. 4(38). С. 61–64.

71. Зубко А. О. Адміністративно-правові механізми в контексті впровадження адміністративної політики України: проблематика теоретичного дискурсу. *Юридичний науковий електронний журнал*, 2024. № 3/2024. С. 296–299.

72. Імплементативний Регламент Комісії (ЄС) № 628/2013 від 28 червня 2013 року про методи роботи Європейського агентства з безпеки авіації при проведенні стандартизаційних інспектувань та при здійсненні моніторингу застосування правил Регламенту Європейського Парламенту і Ради (ЄС) № 216/2008 та про скасування Регламенту Комісії (ЄС) № 736/2006: Міжнародний документ від 28.06.2013 р. № 628/2013. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/984_024-13/ed20130628#n49

73. Кабмін затвердив трирічний план захисту критичної інфраструктури. *Ukrinform*, 2023. URL: <https://www.ukrinform.ua/rubric-economy/3763289-kabmin-zatverdiv-triricnij-plan-zahistu-kriticnoi-infrastrukturi.html>

74. Казміришин Е. О. Адміністративно-правові інструменти забезпечення реалізації державної політики у сфері європейської інтеграції України. *Актуальні проблеми вітчизняної юриспруденції*, 2019. № 5. С. 78–83.

75. Карабін Т. О. Проблеми визначення суб'єктного складу публічної адміністрації. *Прикарпатський юридичний вісник*, 2015. Вип. 3 (9). С. 164–169.

76. Керівництво із застосування ризик-орієнтованого нагляду. FATF, 2021. URL: www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html

77. Кібербезпека критично важливої інфраструктури України USAID. Грант Sense, 2024. URL: <https://www.grantsense.com.ua/grants2024/kiber-bezpeka-kriti-ch-no-va-zh-livo-yi-infrastrukturi-ukra-yi-ni-usaid>

78. Кобрусєва Є. Структура адміністративно-правового механізму забезпечення права на мирні зібрання в Україні. *Право та державне управління*, 2020. № 1. Т. 1. С. 262–269.

79. Ковальчук Я. Л. Генетичний аспект спеціальних принципів інформаційно-аналітичного забезпечення діяльності органів національної поліції України. *Держава та регіони. Серія: Право*, 2022. №2 (66). С. 205–209.

80. Кодекс цивільного захисту населення України: Закон України від 02.10.2012 р. № 5403-VI. Відомості Верховної Ради України, 2013. № 34-35. Ст. 458.

81. Кожура Л. О. Адміністративно-правовий захист та охорона: поняття та співвідношення. Гол. ред. Бисага Ю. М. Ужгород: Видавничий дім "Гельветика". *Науковий вісник Ужгородського Національного університету: Серія: Право*, 2015. Вип. 35. Ч. 1. Т. 2. С. 119–122.

82. Кожура Л. О. Принципи адміністративно-правового захисту бездомних осіб та безпритульних дітей. *Науковий вісник Академії муніципального управління. Серія: Право*, 2015. Вип. 2. С. 74–79.

83. Козюбра М. І. Принципи права: методологічні підходи до розуміння природи та класифікації в умовах сучасних глобалізаційних трансформацій. *Право України. Юридичний журнал*, 2017. Вип. 11. С. 142–164.

84. Колодій А. М. Принципи права: генеза, поняття, класифікація та реалізація. *Альманах права*, 2012. Вип. 3. С. 42–46.

85. Колпаков В. К. Адміністративне право України: К.: Юрінком Інтер, 1999. 736 с.

86. Комзюк А. Заходи адміністративного примусу в правоохоронній діяльності міліції: поняття, види та організаційно-правові питання реалізації: моногр. Х.: Вид-во Нац. ун-ту внутр. справ, 2002. 336 с.

87. Конопльов В. Поняття, зміст та основні напрями сучасної адміністративної діяльності органів внутрішніх справ. *Вісник Національної академії правових наук України*, 2013. № 3 (74). С. 135–150.

88. Косинський В. В. Адміністративно-правове забезпечення безпеки критичної інфраструктури в Україні: дис. ... до-ра філософії. 081 «Право». Науково-дослідний-інститут публічного права. Київ; Дніпропетровський державний університет внутрішніх справ, Дніпро, 2020. 215 с.

89. Кравчук М. Теорія держави і права (опорні конспекти): навч. посібник. Київ: «Атіка», 2003. 288 с.

90. Красногор О. В. Поняття та зміст механізму адміністративно-правового захисту прав і законних інтересів нотаріусів в Україні. *Прикарпатський юридичний вісник*, 2015. Вип. 3 (9). Т. 3. С. 216–220.

91. Кремень В. М., Семенов А. Ю. Науково-методичні засади забезпечення розвитку фінансового сектора України. *Вісник Університету банківської справи Національного банку України*, 2013. №2 (17). С. 29–33.

92. Крикун В. В. Адміністративно-правовий механізм захисту об'єктів критичної інфраструктури в Україні: дис. ... д-ра юрид. наук 12.00.07; Харківський національний університет внутрішніх справ. Харків, 2021. 453 с.

93. Крикун В. В. Поняття адміністративно-правового механізму захисту об'єктів критичної інфраструктури в Україні Актуальні проблеми реформування системи законодавства України: матеріали Міжнародної науково-практичної конференції Запоріжжя: Запорізька міська громадська організація «Істина», 2019. С. 91–94.

94. Крикун В. В. Сутність і структура адміністративно-правового механізму захисту об'єктів критичної інфраструктури в Україні. *Visegrad journal on human rights*, 2019. № 6/3. С. 192–197.

95. Кузьменко К. Е. Нормативно-правові гарантії забезпечення інституційної спроможності державних регуляторів діяльності з надання фінансових послуг. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Публічне управління та адміністрування*, 2024. № 2. Т. 35 (74) С. 79–83.

96. Кузьменко А. І. Треті особи в адміністративному процесі.: автореф. дис... канд. юрид. наук : 12.00.07. Київ: Національний університет біоресурсів і природокористування України, 2017.

97. Кукін І. В. Методи та інструменти забезпечення інформаційної безпеки особистості у сфері національної безпеки та її прикордонному секторі. *Право та державне управління: зб. наук. пр. Запоріжжя: Класичний приватний університет*, 2020. № 4. С. 233–240.

98. Кунєв Ю. Д. Принципи побудови та вдосконалення організаційної структури органів внутрішніх справ України: загальнотеоретичні аспекти державного управління: дис. ... канд.. юрид. наук: 12.00.07. Запоріжжя, 2001. 227 с.

99. Курило В. Адміністративні правовідносини у сільському господарстві України: автореф. дис. ... д-ра юрид. наук: 12.00.07. Київ, 2008. 39 с.

100. Лазаренко С. Аналіз законодавчо-правового регулювання запобігання та протидії корупції в сфері освіти в Україні. *Інвестиції: практика та досвід*, 2015. № 2. С. 97–100.

101. Лазур Я. Поняття, сутність та елементи адміністративно-правового механізму забезпечення прав і свобод громадян у державному управлінні. *Форум права*, 2009. № 3. С. 392–398.

102. Левчинський Д. Л. Сутність інституціональних моделей відносин учасників інвестиційного процесу відтворення житлового фонду. *Науковий вісник Ужгородського університету. Серія Економіка*, 2011. Вип. 2 (32). С. 93–97.

103. Літяга В. В. Образ України в дискурсі міжнародних відносин французьких ЗМІ: автореф. дис. ... канд. філолог. наук: 10.02.05. Київський національний університет імені Тараса Шевченка. Київ, 2019. 21 с.

104. Літяга В.В. Образ України в дискурсі міжнародних відносин французьких ЗМІ: дис. ... канд. філолог. наук: 10.02.05. Київський національний університет імені Тараса Шевченка. Київ, 2019. 239 с.

105. Макропруденційна політика. Національний банк України. URL: <http://surl.li/cvcgkk>

106. Малиновський В. Я. Державне управління: навчальний посібник. Київ: Атіка, 2009. 608 с.

107. Манжело А. Бути об'єктом критичної інфраструктури - це і великі переваги, і чіткі зобов'язання голова Держспецзв'язку. Interfax, 2023. URL: <https://interfax.com.ua/news/interview/947864.html>

108. Маркеєва О. Д., Розвадовський Б. Л. Актуальні проблеми правового забезпечення державно-приватного партнерства у сфері захисту критичної інфраструктури. Національний інститут стратегічних досліджень, 2020. URL: <https://niss.gov.ua/sites/default/files/2020-09/derzhavno-pryvatne-partnerstvo.pdf>

109. Матвєєва Ю. І. Поняття та розуміння принципу правової визначеності. *Наукові записки НаУКМА. Юридичні науки*, 2017. Т. 200. С. 93–97.

110. Мельник А. Ф., Оболенський О. Ю., Васіна А. Ю. Державне управління. Київ: Знання, 2009. 583 с.

111. Мельник Р. С. Загальне адміністративне право в питаннях і відповідях: навч. посіб. Київ: Юрінком Інтер, 2018. 308 с.

112. Миргород-Карпова В. Адміністративно-правовий механізм забезпечення контролю за міжнародними фінансами в Україні: дис. ... канд. юрид. наук: 12.00.07. Суми: СумДУ, 2018. 258 с.

113. Митяй О. Дослідження понять «державне управління» і «публічне адміністрування». *Держава та регіони. Сер. Держ. упр.*, 2018. Вип. 1. С. 124–128.

114. Міщенко С. В. Формування ефективної структури фінансового сектору України: дис. ... канд. екон. наук: 08.00.08. К., 2009. 246 с.

115. Надолішній П. Теорія та історія державного управління. навч. посіб. Одеса: ОРІДУ НАДУ, 2006. 126 с.

116. Наконечна І. В. Адміністративно-правовий механізм забезпечення національної безпеки в умовах євроінтеграції: питання теорії і практики: дис... д-ра юрид. наук: 12.00.07. Науково-дослідний інститут публічного права, Київ, 2023. 274 с.

117. Національний банк посилить роботу щодо захисту критичної інфраструктури фінансового сектору. Національний банк України, 2023. URL: <https://bank.gov.ua/ua/news/all/natsionalniy-bank-posilit-robotu-schodo-zahistu-kritichnoyi-infrastrukturi-finansovogo-sektoru>

118. Національний банк та Державний центр кіберзахисту співпрацюватимуть у сфері кібербезпеки. Національний банк України, 2019. URL: <https://bank.gov.ua/ua/news/all/natsionalniy-bank-ta-derjavniy-tsentr-kiberzahistu-spivpratsyuvatimut-u-sferi-kiberbezpeki>

119. НБУ розпочав процес націоналізації Сенс Банку (раніше - Альфа-Банк). Інтерфакс-Україна, 2023. URL: <https://interfax.com.ua/news/economic/924069.html>

120. Новіков В., Боровікова В. Про механізм реалізації прав і свобод людини. *Науковий вісник Львівського державного університету внутрішніх справ*, 2018. № 3. С. 45–56.

121. Огляд роботи делегації України в РБ ООН 13-19 лютого 2017 р. Постійне представництво України при ООН, 2017. URL: <https://ukraineun.org/press-center/254-oglyad-roboty-delegatsiy-ukrayny-v-rb-oon-13-19-lyutogo-2017-r/>

122. Огляд ССПД - ООКД: Національний банк України. Держстат України, 2024. URL: <https://ukrstat.gov.ua/imf/nbu.htm>

123. Оксін В. Місцевий розвиток в Україні: теорія та практика публічного адміністрування: монографія. Київ: ФОП Чалчинська Н. В., 2020. 428 с.

124. Олькіна О. Поняття та механізм реалізації права особи на захист та правову допомогу. *Актуальні проблеми держави і права*, 2017. Вип. 67. С. 242–248.

125. Омелян В. О. Принципи адміністративного розсаду в діяльності публічної адміністрації. *Актуальні проблеми вітчизняної юриспруденції*, 2017. Спецвип. Ч. 1. С. 150–155.

126. Оніщенко Н. М. Правова система: проблеми теорії: монографія. Київ: Інститут держави і права ім. В.М. Корецького НАН України, 2002. 352 с.

127. Оніщенко Н. М. Теоретико-методологічні засади формування та розвитку правової системи: дис. ... д-ра наук: 12.00.01. Київ, 2002. 424 с.

128. Осауленко О., Панько О. Зміцнення законності у правозастосовному процесі. *Право України*, 2004. № 12. С. 61–68.

129. Осіпов Ю. Сутність механізму реалізації права на звернення до адміністративного суду. *Наукові записки. Серія: Право*, 2020. Вип. 8. Спецвипуск. С. 262–266.

130. Основні принципи ефективного банківського нагляду (Основні Базельські принципи). Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/Basel_Core_principles_2012.pdf

131. Остапенко О. Наукові уявлення про механізм адміністративно-правового регулювання. Львів: *Наук. вісн. Львів. держ. ун-ту внутр. справ. Сер. юрид.*, 2010. Вип. 2. С. 142–149.

132. Патерило І. В. Проблеми сучасного розуміння інструментів діяльності публічної адміністрації. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*, 2014. Т. 1. С. 97–100.

133. Петров Є. В. Феноменологія адміністративно-господарського права України: монографія. Харків: Діса плюс, 2012. 392 с.

134. Петровський П. Проблема розуміння в контексті розвитку публічного управління в Україні. *Ефективність державного управління*, 2017. Вип. 1. С. 21–27.

135. Пітателєв В. Г. Адміністративно-правовий захист земель сільськогосподарського призначення в Україні: дис... канд. юрид. наук: 12.00.07. Науково-дослідний інститут публічного права. Київ, 2017. 150 с.

136. Плішкін В. М. Теорія управління органами внутрішніх справ: підручник за ред. канд. юрид. наук Кравченка Ю. Ф. Київ: Національна академія внутрішніх справ України, 1999. 702 с.

137. Плохута Є. П. Принципи адміністративно-правового регулювання діяльності з примусового виконання судових рішень і рішень інших органів. *Держава та регіони. Серія: Право*, 2022. № 2 (76). С. 47–53.

138. Плукар В. В. Принципи забезпечення адміністративно-правового захисту учасників виборів в Україні. *Наукові записки Львівського університету бізнесу та права*, 2010. Вип. 4. С. 141–145.

139. Погребняк С. П. Основоположні принципи права. монографія. Х.: Право, 2008. 240 с.

140. Положення про організацію кіберзахисту в банківській системі України. затверджене Постановою Правління Національного банку України від 12.08.2022 р. № 178. Національний банк України, 2022. URL: https://bank.gov.ua/ua/legislation/Resolution_12082022_178

141. Положення про порядок визначення Національним банком України юридичних осіб, що є критично важливими для функціонування економіки та забезпечення життєдіяльності населення в особливий період. затверджене Постановою Правління Національного банку України від 24.03.2023 р. № 32. Національний банк України, 2023. URL: https://bank.gov.ua/ua/legislation/Resolution_24032023_32

142. Полянничко А. О. Принципи права: сучасний загальнотеоретичний погляд. *Університетські наукові записки*, 2013. № 3. С. 55–60.

143. Постанова Великої Палати Верховного Суду від 13 лютого 2019 року (Справа № 810/2763/17 (К/9901/44258/18)). ЄДР судових рішень. URL: <https://reyestr.court.gov.ua/Review/79883398>

144. Потьомкін С. О. Мета і завдання правового механізму судового контролю за виконанням судових рішень у адміністративному судочинстві. *Часопис Київського університету права*, 2023. № 4. С. 108–115.

145. Пояснювальна записка до проекту Закону України про внесення змін до деяких законодавчих актів України щодо удосконалення процедури виведення з ринку банку в умовах воєнного стану. Верховна Рада України офіційний сайт. URL: <https://itd.rada.gov.ua/4e286507-1e13-4beb-854b-a5a0e55e7c60>

146. Прес-центру ПУМБ. ПУМБ, 2023. URL: <https://about.pumb.ua/presscenter/news/item/6965-vnasldok-ataki-rf-poshkodzheno-vddlennya-pumb-u-za>

147. Прийма С. В. Поняття принципу в аспекті співвідношення з суміжними категоріями. *Державне будівництво та місцеве самоврядування*, 2014. Вип. 28. С. 46–55.

148. Прийма С. В. Принцип своєчасності інтерпретації норм права. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*, 2019. № 6. Т. 30 (69). С. 30–34.

149. Присяжнюк А. Адміністративно-правовий механізм забезпечення економічної безпеки держави. *Форум права*, 2011. № 1. С. 808–813.

150. Приходько Х. В. Представницька функція Верховної Ради-парламенту України: дис.... канд. юрид. наук: спец. 12.00.02. Інститут законодавства Верховної Ради України. Київ, 2004. 197 с.

151. Пришляк М. І. Механізм адміністративно-правового забезпечення медичного обстеження наречених в Україні: поняття та загальний аналіз складових елементів. *Держава та регіони*, 2017. №3 (57). С. 46–52.

152. Про встановлення вимог з безпеки та захисту інформації до кваліфікованих надавачів електронних довірчих послуг та їхніх відокремлених пунктів реєстрації: Наказ Адміністрації Держспецзв'язку від 14.05.2020 р. № 269. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/z0668-20/ed20200514#n25>

153. Про Загальнодержавну програму адаптації законодавства України до законодавства Європейського Союзу: Закон України від 18.03.2004 р. № 1629-IV. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/1629-15#Text>

154. Про застосування спеціальних заходів щодо імпорту в Україну: Закон України від 22.12.1998 р. № 332-XIV. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/332-14/ed20181004#n15>

155. Про затвердження Інструкції з проведення аналізу ризиків у Державній прикордонній службі України: Наказ МВС України від 11.12.2017 р. № 1007. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/z0091-18/ed20171211#n20>

156. Про затвердження Комплексної програми розвитку фінансового сектору України до 2020 року: Постанова Правління Національного банку України від 18.06. 2015 р. № 391. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/v0391500-15#Text>

157. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури: Розпорядження Кабінету Міністрів України від 19.09.2023 № 825-р. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text>

158. Про затвердження Положення про нагляд за безпекою польотів у системі організації повітряного руху та змін до деяких нормативно-правових актів: Наказ Міністерства транспорту та зв'язку України від 31.05.2010 р. № 320. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/z0446-10/ed20100716/find?text=%D0%E8%E7%E8%EA#w1_5

159. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Постанова Національного банку України від 28.09.2017 р. № 95. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/v0095500-17#Text>

160. Про затвердження Порядку технічного розслідування дорожньо-транспортних пригод, катастроф, аварій на автомобільному та міському електричному (трамвай, тролейбус) транспорті. Наказ Міністерства інфраструктури України від 23.06.2015 р. № 231. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/z0818-15/ed20150623#n27>

161. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: Постанова Кабінету Міністрів України від 23.08.2016 р. № 563. *Офіційний вісник України*, 2016. № 69. Ст. 2332.

162. Про затвердження Порядку функціонування державної системи фізичного захисту: Постанова Кабінету Міністрів України від 21.12.2011 р. № 1337. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/1337-2011-%D0%BF#Text>

163. Про затвердження Правил сертифікації суб'єктів, що надають послуги з аеронавігаційного обслуговування: Наказ Міністерства транспорту та зв'язку України від 01.2007 р. № 42. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/z0104-07/ed20111229/find?text=%D0%E8%E7%E8%EA#Text>

164. Про затвердження Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури: Постанова Кабінету Міністрів України від 14.10.2022 р. № 1174. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/1174-2022-%D0%BF#Text>

165. Про карантин рослин: Закон України від 30.06.1993 р. № 3348-XII. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/3348-12#Text>

166. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>

167. Про Національний банк України: Закон України від 20.05.1999 р. № 679-XIV. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/679-14#n109>

168. Про об'єкти підвищеної небезпеки: Закон України від 18.01.2001 р. № 2245-III. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/2245-14#Text>

169. Про основні засади державного нагляду (контролю) у сфері господарської діяльності: Закон України від 05.04.2007 р. № 877-V. Верховна Рада України офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/877-16?find=1&text=%D1%80%D0%B8%D0%B7%D0%B8%D0%BA#w1_1

170. Про основні принципи та вимоги до безпечності та якості харчових продуктів: Закон України від 23.12.1997 р. № 771/97-ВР. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/771/97-%D0%B2%D1%80#Text>

171. Про Раду з фінансової стабільності: Указ Президента України від 24.03.2015 р. № 170/2015. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/170/2015#Text>

172. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 р. № 183/98-ВР. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text>

173. Про рішення Ради національної безпеки і оборони України від 20.08.2021 р. «Про запровадження національної системи стійкості»: Указ Президента України від 27.09.2021 р. №479/2021. Офіційне інтернет-

представництво Президента України. URL: <https://www.president.gov.ua/documents/4792021-40181>

174. Про роботу банківської системи в період запровадження воєнного стану: Постанова Національного банку України від 24.02.2022 р. № 18. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/v0018500-22#Text>

175. Про технічні регламенти та оцінку відповідності: Закон України від 15.01.2015 р. № 124-VIII. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/124-19#Text>

176. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України: Постанова Кабінету Міністрів України від 12.07.2022 р. № 787. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text>

177. Проєкт USAID «Кібербезпека критично важливої інфраструктури України». Національний університет «Запорізька політехніка». URL: <https://zp.edu.ua/proyekt-usaid-kiberbezpeka-krytychno-vazhlyvoyi-infrastruktury-ukrayiny>

178. Публічне управління: термінол. слов. уклад.: Куйбіда В. С., Білинська М. М., Петроє О. М. та ін.; Київ: НАДУ, 2018. 224 с.

179. Пухтецька А. Європейські принципи адміністративного права: поняття і система. *Право України*. 2006, № 10. С. 15–19.

180. Рада з фінансової стабільності погодила концепцію створення в Україні системи страхування воєнних ризиків. Міністерство Фінансів України. URL: https://mof.gov.ua/uk/news/rada_z_finansovoi_stabilnosti_pogodila_kontseptsiuu_stvorennia_v_ukraini_sistemi_strakhuvannia_voiennikh_rizikiv-4424

181. Рада з фінансової стабільності. Національний банк України. URL: <https://bank.gov.ua/ua/stability/radafinstab>

182. Резнік О. Сутність та структура адміністративно-правового механізму забезпечення фінансово-економічної безпеки України. *Jurnalul juridic national: teorie și practică*, 2018. № 2-2(30). С. 69–72.

183. Річний звіт 2022. Power Banking: Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2022.pdf

184. Рішення Конституційного Суду України у справі за конституційним поданням Верховного Суду України щодо відповідності Конституції України (конституційності) положень статті 69 Кримінального кодексу України (справа про призначення судом більш м'якого покарання) від 02.11.2004 р. № 15-рп/2004. Верховна Рада України офіційний сайт. URL: <https://zakon.rada.gov.ua/laws/show/v015p710-04#Text>

185. Романчик Т. В. Небезпека, загроза, ризик: аналіз термінологічного апарату теорії економічної безпеки. *Економічний вісник НТУУ «КПІ»*, 2020. С. 257–267.

186. Русецький А. А. Поняття адміністративно-правового механізму взаємодії та координації діяльності правоохоронних органів на регіональному рівні. *Науковий вісник публічного та приватного права*, 2018. Вип. 5. С. 107–111.

187. Савчин М. В. Порівняльне правознавство. Загальна частина: навч. посіб. К.: Центр навчальної літератури, 2005. 288 с.

188. Садовнікова Г. В. Співвідношення категорій концепт, поняття і значення у когнітивному термінознавстві. *Вісник Київського національного лінгвістичного університету*, 2014. Т. 17. № 1. С. 156–164.

189. Світові фінансово-економічні кризи. Finance UA, 2023. URL: <https://finance.ua/ua/goodtoknow/finansovo-ekonomiczni-kryzy>

190. Сервіси Csirt-NBU. Національний банк України. URL: <https://csirt.bank.gov.ua/bankam>

191. Скакун О.Ф. Теорія держави і права: підручник Харків: Консул, 2006. 656 с.

192. Словник синонімів української мови: у 2 т. Бурячок А. А., Гнатюк Г. М., Головащук С. І. та ін. К.: Наук. думка, 1999. Т. 1. 1040 с.

193. Собакарь А. О. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки України. Російсько-українська війна: право, безпека, світ: матеріали VI міжнародної науково-практичної конференції. Тернопіль, 2022. С. 264–267.

194. Сокіран М. Стан наукової розробленості проблем адміністративно-правового забезпечення безпеки та стійкості критичної інформаційної інфраструктури. *Юридичний науковий електронний журнал*, 2023. №12. С. 287–291.

195. Солових В. П. Good Governanse як одна із сучасних моделей державного управління. *Науковий вісник академії муніципального управління. зб. наук. праць. Серія Управління*. К.: АМУ, 2010. Вип. 1. С. 112–120.

196. Сорока Л. В. Щодо доцільності використання терміно-поняття «концепт» у адміністративно-правовій науці. Інноваційні технології публічного управління та адміністрування: теорія і кращі практики 21 століття: матеріали Всеукраїнської науково-практичної конференції Мелітополь: ФОП Однорог Т.В., 2020. С. 183–185.

197. Соціально-економічні наслідки політичної нестабільності, що виникла після підписання Указу Президента України про дострокове припинення повноважень Верховної Ради було обговорено на розширеному засіданні Комітету з питань економічної політики. Верховна Рада України офіційний сайт. URL: <https://www.rada.gov.ua/news/Povidomlennya/10355.html>

198. Стан фінансового сектору України та заходи НБУ з підтримки його безперебійного функціонування в умовах воєнного стану. Національний банк України, 2022. URL: <https://bank.gov.ua/ua/news/all/stan-finansovogo-sektoru-ukrayini-ta-zahodi-nbu-z-pidtrimki-yogo-bezperedbiynogo-funktsionuvannya-v-umovah-voyennogo-stanu>

199. Старчук О. Щодо поняття принципів права. *Часопис Київського університету права. Теорія та історія держави і права. Філософія права*, 2012. №2. С. 40–43.

200. Стійкість критичної інфраструктури ЄС: посилення політики та координації. національний Інститут стратегічних досліджень, 2024. URL: <https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/stiykist-krytychnoyi-infrastruktury-yes-posylennya-polityky-ta>

201. Стратегія розвитку фінансового сектору України до 2015 року (проект). Інформаційно-аналітичний портал Українського агентства фінансового розвитку, 2008. URL: <https://ufin.com.ua/konceptia/002.doc>

202. Стратегія розвитку фінансового сектору України до 2025 року (припинена у 2023 році). Національний банк України. URL: <https://bank.gov.ua/ua/about/develop-strategy/develop-strategy2023>

203. Стратегія розвитку фінансового сектору України до 2025 року. Національний банк України за підтримки USAID. URL: https://bank.gov.ua/admin_uploads/article/Strategy_finsector_NBU.pdf?v=7

204. Страхніцький Я. О. Особливості сучасної державної політики у сфері захисту критичної інфраструктури в умовах війни в Україні. URL: <https://doi.org/10.30525/978-9934-26-279-1-5>

205. Сухенко В. В. Особливості функціонування політико-адміністративних систем сучасних європейських країн: досвід для України: дис. ... канд. з держ. управління: 25.00.01. Національна академія державного управління при Президентові України, Київ, 2018. 199 с.

206. Суходоля О. М. Система захисту критичної енергетичної інфраструктури України: стан та проблеми формування. *Науково-інформаційний вісник Академії національної безпеки*, 2015. № 1-2. С. 134–146.

207. Тарахович Т. Механізм дії права, механізм правового регулювання, механізм реалізації права: особливості взаємодії. *Держава і право*, 2010. Вип. 50. С. 12–18.

208. Теленик С. С. Правовий зміст поняття «критична інфраструктура». *Jurnalul juridic national: teorie și practică*, 2019. № 6(40). С. 34–38.

209. Ткаченко О. Адміністративно-правові засади протидії корупції в органах внутрішніх справ: автореф. дис. ... канд. юрид. наук: 12.00.07. Ін-т з-ва Верховної Ради України. Київ, 2008. 22 с.

210. Тодика Ю. М. Конституція України. Основний Закон держави і суспільства. Харків, 2001. 382 с.

211. Толкованов В. Розвиток і впровадження інструментів політики державного управління: вітчизняний та зарубіжний досвід. Демократичне врядування. *Науковий вісник*, 2013. Вип. 12.

212. Тоцький Б. А. Принцип пропорційності: історичний аспект і теоретичні складові. *Часопис Київського університету права*, 2013. № 3. С. 70–74.

213. Троцюк Н. В., Петрина Н. О. Адміністративно-правовий захист авторського права та суміжних прав: теоретико-правовий аспект. *Порівняльно-аналітичне право*, 2015. №2. С. 115–118.

214. Трушкіна Н. В., Жукова І. В. Державно-приватне партнерство як ключовий принцип функціонування національної системи захисту критичної інфраструктури в Україні. *Наукові інновації та передові технології. Серія «Управління та адміністрування»*, 2023. № 7 (21). С. 11–26.

215. У Чернігові підірвали відділення банку «Південний». Мінфін, 2024. URL: <https://minfin.com.ua/ua/2024/05/06/126367313/>

216. Україна починає будувати систему захисту критичної інфраструктури відповідно до найкращих світових практик та чинних вимог європейського законодавства. Держспецзв'язку, 2023. URL: <https://cip.gov.ua/ua/news/ukrayina-pochinaye-buduvati-sistemu-zakhistu-kritichnoyi-infrastrukturi-vidpovidno-do-naikrashikh-svitovikh-praktik-ta-chinnikh-vimog-yevropeiskogo-zakonodavstva>

217. Фінансова фортеця України. Річний звіт 2023. Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/annual_report_2023.pdf?v=9

218. Фінансовий моніторинг. Національний банк України. URL: <https://bank.gov.ua/ua/supervision/monitoring>

219. Харитонов Є. О., Харитонova О. І. Приватне право як концепт: постановка питання. *Вісник Південного регіонального центру Національної академії правових наук України*, 2014. № 1. С. 68–77.

220. Цвих В. Ф. Профспілки у громадянському суспільстві: теорія, методологія, практика: монографія. Київ: ВПЦ «Київський університет», 2002. 376 с.

221. Центр кіберзахисту Національного банку України. Національний банк України, 2024. URL: <https://cyber.bank.gov.ua/>

222. Цілі сталого розвитку та Україна. Урядовий портал, 2024. URL: <https://www.kmu.gov.ua/diyalnist/cili-stalogo-rozvitku-ta-ukrayina>

223. Чаплюк О. І. Загальні та спеціальні принципи національної правотворчості: поняття, значення та види. *Часопис Київського університету права*, 2010. № 1. С. 87–93.

224. Чернишова О., Чорновол А., Мирончук В. Функціонування фінансового сектору України в умовах воєнного стану. *Економіка та суспільство*, 2022. Вип. 38. С. 38-49.

225. Чернов С., Гайдученко С. Текст лекцій з дисципліни «Публічне адміністрування» (для студентів всіх форм навчання за спеціальністю 7.03060101, 8.03060101 «Менеджмент організацій і адміністрування (за видами економічної діяльності)»; Харк. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Х.: ХНУМГ, 2014. 97 с.

226. Чи буде в Україні попит на онлайн кредити в 2023 році? Думки експертів. ЕП, 2022. URL: <https://www.epravda.com.ua/press/2022/12/15/694676/>

227. Шарук О. Г. Механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України: термінологічні аспекти. *Науковий вісник публічного та приватного права*, 2024. Вип. 2. С. 139–143.

228. Шарук О. Г. Основні загрози для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України. *Науковий вісник публічного та приватного права*, 2024. Вип. 3. С. 177–182.

229. Шарук О. Г. Система суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. *Kel'm*, 2024. № 3 (63). С. 89–96.

230. Шарук О. Г. Структура механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. Проблемні питання юридичної науки в контексті реформування правової системи України: матеріали міжнародної науково-практичної конференції. Київ: Науково-дослідний інститут публічного права, 2022. С. 221–223.

231. Школьник І. О., Семенов А. Ю. Фінансовий сектор України: теоретичний аналіз економічної дефініції. *Вісник Української академії банківської справи*, 2013. № 1 (213). С. 31–36.

232. Шпак Н. О., Романишин М. І. Основні принципи формування стратегії забезпечення економічної стабільності підприємства. *Vědecko-pokrok na rozmezí tisíciletí – 2010: materiály VI mezinárodní vědecko-praktická konference. Díl 10. Ekonomické vědy. Praha. Publishing "Education and Science" s.r.o. S. 7–10.*

233. Шпарага Ю. І. Нормативні засади діяльності регіонального департаменту соціального захисту населення: порівняльно-правовий аналіз. *Прикарпатський юридичний вісник*, 2019. Випуск 3(28). Том 2. С. 134–138.

234. Щодо розроблення планів забезпечення організаційної стійкості. НІСД. URL: https://niss.gov.ua/sites/default/files/2023-02/az_planuvannya-org-stiykosti_24022023.pdf

235. Юхимюк О. Принципи права як ефективний регулятор суспільних відносин. Державотворення та правотворення в період реформ: питання теорії та практики: матер. щорічної Всеукр. наук.-практ. конф. У 2-х ч. за заг. ред. Коваленка В. В. К.: НАВС, 2012. Ч .1. С. 134–137.

236. Як захистити свої гроші від шахраїв в інтернеті: спільний проект Держспецзв'язку, НБУ та Кіберполіції. Державна служба спеціального зв'язку та захисту інформації України, 2022. URL: https://cip.gov.ua/ua/news/yak-zakhistiti-svoyi-groshi-vid-shakhrayiv-v-interneti-spilnii-proyekt-derzhspeczv-yazku-nbu-ta-kiberpoliciyi?fbclid=IwAR3lL4E6n_cTjH2Ld0KEkdgAO-DLTf7KERthkIFNrIVdam8Jtw3JIWC0soA

237. About the FSB, 2024. URL: <https://www.fsb.org/about/>

238. Berman, Noah. What is the Dodd-Frank Act? Council on Foreign Relations, 2023. URL: <https://www.cfr.org/backgrounder/what-dodd-frank-act>

239. Building PrivatePublic Partnerships. FEMA, 2021. URL: https://www.fema.gov/sites/default/files/documents/fema_building-private-public-partnerships.pdf

240. Council Directive 2008/114/EC of 08.12.2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32008L0114>

241. Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure (Text with EEA relevance) 2023/C 20/01. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023H0120%2801%29>

242. Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts, 2020. URL: <https://www.gao.gov/products/gao-20-631>

243. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive). European Commission, 2024. URL: <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

244. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance). European Commission, 2022. URL: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>

245. European Critical Infrastructure. TEPSA, 2023. URL: <https://tepsa.eu/analysis/european-critical-infrastructure/>

246. FATF Recommendations. FATF, 2024. URL: <https://www.fatf-gafi.org/en/topics/fatf-recommendations.html>

247. Financial and Banking Information Infrastructure Committee. FBIIC, 2024. URL: <https://www.fbiic.gov/mission-history.html>

248. Financial Protection of Critical Infrastructure Services. World Bank, 2021. URL: <https://doi.org/10.1596/36902>

249. Financial Sector. Cleartax, 2023. URL: <https://cleartax.in/glossary/financial-sector/>

250. Financial Services Sector Coordinating Council. FSSCC, 2024. URL: <https://fsscc.org/>

251. Financial Services Sector. Cisa.gov., 2024. URL: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/financial-services-sector>

252. Financial Services Sector-Specific Plan 2015. Cisa.gov, 2015. URL: <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf>

253. FSARC: US Treasuries (UST) Initiative Highlights Treasury Market Practices Group (TMPG) October 23, 2018. URL: https://www.newyorkfed.org/medialibrary/Microsites/tmpg/files/FSARC_TMPG_Presentation.pdf

254. General Data Protection Regulation. GDPR, 2024. URL: <https://gdpr-info.eu/>

255. Good Governance for Critical Infrastructure Resilience. OECD, 2019. URL: <https://doi.org/10.1787/02f0e5a0-en>.

256. Hladkyi V. V. Signs of the legal mechanism of ensuring anti-corruption security. Modern views on reforming legislation: materials of the International of science conf. (Poltava, October 25-26, 2018). Kherson: Young Scientist, 2018. C. 62–66.

257. International Monetary Fund. Monetary and Capital Markets Department. Chapter 3 Cyber Risk: A Growing Concern for Macroeconomic Stability. Elibrary, 2024. URL: <https://www.elibrary.imf.org/display/book/9798400257704/CH003.xml?tabs=fulltext>

258. ISO 31000. Global standards for trusted goods and services. 256. ISO, 2024. URL: <https://www.iso.org/ru/iso-31000-risk-management.html>

259. ISO/IEC 27001:2022. Global standards for trusted goods and services. ISO, 2022. URL: <https://www.iso.org/ru/standard/27001>

260. Krüger, Philipp S. and Jan-Philipp Brauchle .The European Union, Cybersecurity, and the Financial Sector: A Primer. URL: <https://carnegieendowment.org/research/2021/03/the-european-union-cybersecurity-and-the-financial-sector-a-primer?lang=en>

261. Luijff, E., Nieuwenhuijs A., Klaver M., Van Eeten M., Cruz E. Empirical findings on critical infrastructure dependencies in Europe. In: Setola R, Geretshuber S (eds) CRITIS, 2009. LNCS 5508, pp. 302–310.

262. Maurer T., and Arthur Nelson The Global Cyber Threat. Spring, 2021. URL: <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm>

263. National Infrastructure Protection Plan and Resources. CISA.gov., 2013. URL: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources>

264. National Strategy for Critical Infrastructure Protection (CIP Strategy). BBK, 2024. URL: <https://www.kritis.bund.de>

265. National Strategy for Critical Infrastructure. Her Majesty the Queen in Right of Canada, 2009. URL: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx>

266. NIPP 2013 Partnering for Critical Infrastructure Security and Resilience. CISA.gov., 2013. URL: <https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf>

267. Opinion Of The European Central BANK of 13 May, 2024 on cybersecurity (CON/2024/14). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52024AB0014>

268. Presidential Policy Directive - Critical Infrastructure Security and Resilience. The White House, 2013. URL: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

269. Pursiainenata, Christer, Eero Kytömaa. From European critical infrastructure protection to the resilience of European critical entities: what does it mean? Sustainable and Resilient Infrastructure, 2023. Volume 8. Pages 85–101. <https://doi.org/10.1080/23789689.2022.2128562>

270. Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN>

271. Proposal for a directive of the council on identification and designation of European critical infrastructure and the assessment of the need to improve their protection. Commission of the European Communities. COM(2006) 787 final. Brussels, 12 December.

272. Proposal for a directive of the European parliament and of the Council on the resilience of critical entities. COM(2020) 829 final. 2020/0365 (COD). Brussels, 16 December. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829>

273. Protecting Critical Financial Infrastructure. FSSCC, 2024. URL: <https://fsscc.org/about-fsscc-13/>

274. Gandhi, R. Targeted attacks - protection of critical infrastructure of the country and capacity building. BIS, 2016. URL: <https://www.bis.org/review/r160810c.htm>

275. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December, 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554>

276. Regulation (EU) 2021/23 of the European Parliament and of the Council of 16 December 2020 on a framework for the recovery and resolution of central counterparties and amending Regulations (EU) No 1095/2010, (EU) No 648/2012, (EU) No 600/2014, (EU) No 806/2014 and (EU) 2015/2365 and Directives 2002/47/EC, 2004/25/EC, 2007/36/EC, 2014/59/EU and (EU) 2017/1132 (Text with EEA relevance). URL: <https://eur-lex.europa.eu/eli/reg/2021/23/oj>

277. Sharuk, O. «Critical infrastructure of the financial sector of Ukraine»: identification of content and essence as a legal concept. *Entrepreneurship, Economy and Law*, 2023. No 7. Pp. 99–104.

278. Sharuk O. Essence of administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine. *Entrepreneurship, Economy and Law*, 2023. No 8. pp. 76–80.

279. Sokiran, Maksym. Analysis of Terminology for Identifying the Risks of Ensuring Security and Sustainability of Critical Information Infrastructure in Ukraine. *Visegrad Journal on Human Rights*, 2023. No 5. Pp. 96–104.

280. Technical Brief on Resilient Infrastructure Public-Private Partnerships: Policy, Contracting, and Finance. The World Bank, 2023. URL: <https://documents1.worldbank.org/curated/en/925691571416771609/pdf/Technical-Brief-on-Resilient-Infrastructure-Public-Private-Partnerships-Policy-Contracting-and-Finance.pdf>

281. The Ministers of the Financial Action Task Force. FATF, 2024. URL: <https://www.fatf-gafi.org/en/the-fatf/ministerial-declarations.html>

282. Tim Maurer and Arthur Nelson. International Strategy to Better Protect the Financial System Against Cyber Threats. URL: <https://carnegieendowment.org/research/2020/11/international-strategy-to-better-protect-the-financial-system-against-cyber-threats?lang=en>

283. To, Jump. Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts. U.S. Government Accountability Office, 2020. URL: <https://www.gao.gov/products/gao-20-631>

284. U.S. Department of the Treasury. Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector. U.S. Department of the Treasury, 2024. URL: <https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf>

285. What is early intervention? Early Intervention Foundation. Early Intervention Foundation, 2023. URL: <https://www.eif.org.uk/why-it-matters/what-is-early-intervention>

286. Working at FS-ISAC. FS-ISAC, 2024. URL: <https://www.fsisac.com/careers>

287. Zubko A. Public policy of Ukraine: concept and essence. *Entrepreneurship, Economy and Law*, 2022. № 3. P. 91–95. <https://doi.org/10.32849/2663-5313/2022.3.13>

288. Zubko, O., Levchenko, D., Sokiran, M., Danylenko, A., & Zubko, A. Philosophical and legal interpretations of modern theory of public administration in Ukraine. *Amazonia Investiga*, 2023. № 12(72). P. 59–68. <https://doi.org/10.34069/AI/2023.72.12.5>

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Sharuk O. «Critical infrastructure of the financial sector of Ukraine»: identification of content and essence as a legal concept. *Entrepreneurship, Economy and Law*. 2023. № 7. P. 99–104.

2. Sharuk O. Essence of administrative and legal protection of critical infrastructure facilities of the financial sector of Ukraine. *Entrepreneurship, Economy and Law*. 2023. № 8. P. 76–80.

3. Шарук О.Г. Механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України: термінологічні аспекти. *Науковий вісник публічного та приватного права*. 2024. Вип. 2. С. 139–143.

4. Шарук О.Г. Основні загрози для стійкості функціонування об'єктів критичної інфраструктури фінансового сектору України. *Науковий вісник публічного та приватного права*. 2024. Вип. 3. С. 177–182.

5. Шарук О.Г. Система суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. *KELM*. 2024. № 3 (63). С. 89–96 (Республіка Польща).

які засвідчують апробацію матеріалів дисертації:

6. Шарук О.Г. Структура механізму адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. *Проблемні питання юридичної науки в контексті реформування правової системи України*: матеріали міжнародної науково-практичної конференції (м. Київ, 19–20 жовтня 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 221–223.

7. Шарук О.Г. До необхідності забезпечення міжвідомчих механізмів реалізації адміністративно-правового забезпечення захисту об'єктів

критичної інфраструктури фінансового сектору України. *Науково-практичні засади розвитку юридичної науки на сучасному етапі державотворення: матеріали міжнародної науково-практичної конференції* (м. Київ, 15–16 лютого 2023 р.). Київ: Науково-дослідний інститут публічного права, 2023. С. 117–120.

8. Шарук О.Г. Варіації класифікації суб'єктів здійснення адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України. *Реформування українського законодавства: проблемні питання та шляхи їх вирішення: матеріали міжнародної науково-практичної конференції* (м. Київ, 7–8 лютого 2024 р.). Київ: Науково-дослідний інститут публічного права, 2024. С. 171–173.