УДК 324:338.49:338.583
DOI https://doi.org/10.32782/39221400

Крикун В. В.,
доктор юридичних наук, доцент,
проректор Одеського державного університету внутрішніх справ

КОРУПЦІЙНІ РИЗИКИ ЗАКОНУ УКРАЇНИ «ПРО КРИТИЧНУ ІНФРАСТРУКТУРУ»

CORRUPTION RISKS OF THE LAW OF UKRAINE «ON CRITICAL INFRASTRUCTURE»

У статті зазначається, що протягом останнього десятиріччя об'єкти критичної інфраструктури стали предметом посягання з боку спеціальних служб російської федерації, як шляхом здійснення численних кібератак, так і шляхом їх знищення з використанням різних способів під час військової агресії. Вказане обумовило необхідність правового забезпечення впровадження державної системи захисту критичної інфраструктури, що знайшло своє відображення у прийнятому 16 листопада 2021 року Верховною Радою України Закону України «Про критичну інфраструктуру». Мета вказаного закону – створення умов для формування та ефективної реалізації державної політики у сфері захисту критичної інфраструктури. Підкреслюється, що вказаний вище Закон України є на сьогодні найбільш з актуальних законодавчих актів, адже до його прийняття в нашій державі не існувало навіть поняття «об'єкти критичної інфраструктури» та фактично були відсутні особливі вимог до забезпечення безпеки об'єктів критичного призначення. Здійснюючи аналіз положень Закону України «Про критичну інфраструктуру» акцентується увага на існуванні окремих положень, які характеризуються корупційними ризиками. Автором відмічено, що реалізація норм, пов'язаних з діяльністю Уповноваженого органу у сфері захисту об'єктів критичної інфраструктури України – новоствореної Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України, а також операторів критичної інфраструктури, в певних ситуаціях може привести до негативних наслідків, пов'язаних із вчиненням корупційних правопорушень або правопорушень, пов'язаних з корупцією. Звертається увага на інші недоліки положень Закону України «Про критичну інфраструктуру» у сфері реалізації державної політики у сфері захисту критичної інфраструктури, які містять корупційні ризики. Зазначається увага на необхідності більш прискіпливого розроблення відомчих нормативно-правових актів, які будуть регулювати правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури, з метою усунення корупційних ризиків.

Ключові слова: *критична інфраструктура, кібербезпека, оператор критичної інфраструктури, уповноважений орган у сфері захисту об'єктів критичної інфраструктури України, захист критичної інфраструктури.*

The article notes that over the last decade, critical infrastructure objects have become subject to encroachment by the special services of the Russian Federation, both by carrying out numerous cyber attacks and by destroying them using various methods during military aggression. The above determined the need for legal support for the implementation of the state system for the protection of critical infrastructure, which was reflected in the Law of Ukraine «On Critical Infrastructure» adopted by the Verkhovna Rada (Parliament) of Ukraine on November 16, 2021. The purpose of this law is to create conditions for the formation and effective implementation of state policy in the field of critical infrastructure protection. It is emphasized that the above-mentioned Law of Ukraine is currently the most relevant legislative act, because before its adoption in our country there was not even the concept of «critical infrastructure objects» and in fact there were no special requirements for ensuring the safety of critical objects. Analyzing the provisions of the Law of Ukraine «On Critical Infrastructure», author'sattention is focused on the existence of certain provisions that are characterized by corruption risks. The author noted that the implementation of norms related to the activities of the Authorized Body in the field of protection of critical infrastructure objects of Ukraine – the newly created State Service for the Protection of Critical Infrastructure and Ensuring the National Stability System of Ukraine, as well as operators of critical infrastructure, in certain situations can lead to negative consequences related to the commission of corruption offenses or offenses related to corruption. Attention is drawn to other shortcomings of the provisions of the Law of Ukraine «On Critical Infrastructure» in the sphere of implementation of state policy in the sphere of protection of critical infrastructure, which contain corruption risks. It is brought to the fore the need for more meticulous development of departmental legal acts, which will regulate the legal and organizational foundations of the creation and functioning of the national system for the protection of critical infrastructure, in order to eliminate corruption risks.

Key words: *critical infrastructure, cyber security, critical infrastructure operator, authorized body in the field of protection of critical infrastructure objects of Ukraine, protection of critical infrastructure.*

Останнє десятиріччя для незалежної України характеризується протистоянням найбільшим викликам у сфері забезпечення державної безпеки. Розпочати проти нашої держави так звана гібридна війна, яка супроводжувалася численними кібератаками на об'єкти критичної інфраструктури України, а у подальшому і військова агресія засвідчили про уразливість важливих об'єктів інфраструктури, призвели до порушення їх безперервності діяльності і стійкості, створили реальні чи потенційні загрози для населення, суспільства, соціально-економічного стану, національної безпеки і оборони України.

І в даному випадку можна погодитися з І.В. Солоповою, яка зазначила, що створення державної системи захисту критичної інфраструктури (як комплексу організаційних, нормативно-правових, інженерно-технічних, наукових та інших заходів, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури) потребує нормативно-правового врегулювання основоположних принципів її функціонування, запровадження єдиних підходів до організації управління об'єктами системи на державному й місцевому рівнях, визначення засад взаємодії залучених до захисту критичної інфраструктури державних органів та суб'єктів господарювання, суспільства і громадян [1, с. 120].

Саме тому, з метою реалізації Концепції створення державної системи захисту критичної інфраструктури [2] 16 листопада 2021 року Верховною Радою України був прийнятий Закон України «Про критичну інфраструктуру» [3], метою якого було створення умов для формування та ефективної реалізації державної політики у сфері захисту критичної інфраструктури.

Аналіз останніх досліджень публікацій. Дослідженню проблематики правового регулювання забезпечення безпеки критичної інфраструктури значну увагу приділяли у своїх працях такі вітчизняні вчені, як Д. Г. Бобро, Д. С. Бірюков, С. Ф. Гончар, О. П. Єрменчук, С. П. Іванюта, С. І. Кондратов, О. В. Копан, Г. П. Леоненко, Б. Д. Леонов,В. А. Ліпкан, М. Л. Пальчик, В. С. Серьогін, І. В. Солопова, О. М. Суходоля, С. С. Теленик, А. Г. Чубенко, О. Ю. Юдін та інші. Водночас з урахуванням складного та багатоаспектного характеру проблематики правового забезпечення безпеки об'єктів критичної інфраструктури, важливість безпекових відносин, на даний час залишається малодослідженою сфера наявних корупційних ризиків у Законі України «Про критичну інфраструктуру» [3], що і обумовлює актуальність даної статті.

Метою статті є аналіз положень Закону України «Про критичну інфраструктуру» для визначення існуючих норм, які становлять корупційні ризики.

Виклад основного матеріалу. Як зазначалося, 16 листопада 2021 року Верховною Радою України було прийнято Закон України «Про критичну інфраструктуру» [3], який визначає правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки. Важливими перевагами вказаного Закону є те, що у ньому на законодавчому рівні:

– надано визначення низки понять, серед яких необхідно відмітити такі, як «захист критичної інфраструктури», «інцидент безпеки критичної інфраструктури», «кризова ситуація», «об'єкти критичної інфраструктури», «несанкціоноване втручання», «паспорт безпеки», «реєстр об'єктів критичної інфраструктури», «рівень критичності об'єкта критичної інфраструктури», «стійкість критичної інфраструктури»;

– визначено засади державної політики у сфері захисту критичної інфраструктури та встановити мету державної політики у сфері захисту критичної інфраструктури, якою є забезпечення безпеки об'єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури;

– визначено основні принципи функціонування національної системи захисту критичної інфраструктури та рівні управління національною системою захисту критичної інфраструктури;

– сформульовано критерії віднесення об'єктів до критичної інфраструктури;

– визначено життєво важливі функції порушення яких призводить до негативних наслідків для національної безпеки України;

– запроваджено створення Реєстр об'єктів критичної інфраструктури;

– запроваджено інститут регулятора у цій сфері, яким стане Уповноважений орган у сфері захисту об'єктів критичної інфраструктури України (Державна служба захисту критичної інфраструктури та забезпечення національної системи стійкості України). Діяльність Уповноваженого органу буде спрямовувати, координувати та контролювати Міністр Кабінету Міністрів України [4].

Аналіз положень Закону України «Про критичну інфраструктуру» [3] засвідчує, що низка його норм все ж таки містять певні корупційні ризики, визначимо деякі з них.

Так, відповідно до статті 5 вказаного Закону передбачається створення нового регуляторного органу – Уповноваженого органу у сфері захисту об'єктів критичної інфраструктури України, який має створити та вести реєстр об'єктів, розробляти нормативно-правову базу та проводити перевірки та регулювання у сфері захисту об'єктів критичної інфраструктури, а саме Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України, положення про яку було затверджено постановою Кабінетом Міністрів України від 12 липня 2022 року № 787 [5].

Разом з тим сфера діяльності та повноваження Уповноваженого органу у сфері захисту об'єктів критичної інфраструктури України (Державна служба захисту критичної інфраструктури та забезпечення національної системи стійкості України) відповідно до Закону України «Про захист критичної інфраструктури» [3] настільки різнопланові та широкі, що відразу проявляються корупційні ризики в його функціонуванні, особливо з огляду на те, що запровадження заходів безпеки критичної інфраструктури завжди були, є і залишаються особливо зараз досить коштовними і на сьогодні нормативно неврегульованими, що знайти недоліки в їх реалізації представнику вказаного вище державного регулятору в разі необхідності у майбутньому не складе великої проблеми.

Виходячи з вищесказаного, новий державний регулятор, посилаючись на необхідність дотримання національної безпеки, недопущення інцидентів безпеки критичної інфраструктури може встановлювати будь-які вимоги, що стосуються захисту об'єкта критичної інфраструктури (енергетичні, фінансові, страхові, кібербезпека, захищеність приміщень, режимні заходи, безпека повітряного простору тощо), які без належного фінансування, а в окремих випадках і без перебудови самого об'єкта, практично не можна бути виконати за короткий період часу. І в подальшому Уповноважений орган у сфері захисту об'єктів критичної інфраструктури України на вибір може здійснювати аудит дотримання встановлених вимог серед значної кількості підприємств, установ та організацій. Звідти виникає вже проблеми у суб'єкта господарювання, який був внесений у Реєстр об'єктів критичної інфраструктури, яким шляхом і з ким вирішувати проблеми фінансового та організаційного характеру, що може з часом перетворити новостворену службу у корупційного монстра.

Наступним важливий корупційний ризик може проявитися під час здійснення фінансування заходів у сфері захисту об'єктів критичної інфраструктури. Так, у статті 30, закону, який обговорюється, зазначається, що «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.». Проте із норм законодавства не визначено, які саме об'єкти критичної інфраструктури будуть фінансуватися в першу чергу, а які – за залишковим принципом. Жоден державний бюджет та бюджети органів місцевого самоврядування не силах забезпечити фінансування всіх виявлених заходів, які повинні бути забезпечити безпеку об'єктів критичної інфраструктури, а використання власних коштів може стати просто непосильним фінансовим тягарем для суб'єкта господарювання, який був віднесений у Реєстр об'єктів критичної інфраструктури і якому визначили перелік заходів виконання яких повинно забезпечити повну безпеку такого об'єкта. При цьому необхідно підкреслити важливу деталь, що в разі не вжиття відповідних заходів, керівники таких суб'єктів господарювання, також самі юридичні особи можуть бути притягнуті

до відповідальності згідно із законом. З наведеного вбачається, що кошти на вказані заходу будуть виділятися тільки для «обраних» об'єктів або за умов надання неправомірної вигоди посадовим особам органів державної влади чи місцевого самоврядування, які причетні до розподілу таких коштів.

Однією з важливих новел Закону України «Про критичну інфраструктуру» [3] щодо створення національної системи захисту критичної інфраструктури є визначення суб'єктів національної системи захисту критичної інфраструктури – 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 буде покладено завдання з формування та/або реалізація державної політики у сфері захисту критичної інфраструктури, а також підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки та стійкості критичної інфраструктури.

Серед системи захисту критичної інфраструктури необхідно відмітити запровадження нових суб'єктів національної системи захисту критичної інфраструктури – операторів критичної інфраструктури – юридичних осіб будь-якої форми власності та/або фізичної особи – підприємця, що на правах власності, оренди або на інших законних підставах здійснює управління об'єктом критичної інфраструктури та відповідає за його поточне функціонування.

У статті 21 Закону України «Про критичну інфраструктуру» [3] визначено завдання, права та обов'язки операторів критичної інфраструктури. Зупинимося на окремих з них. Так, до завдань оператор критичної інфраструктури, зокрема, віднесено:

– забезпечення захисту об'єктів критичної інфраструктури, зокрема створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки;

– розроблення, оновлення та забезпечення виконання об'єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, правил управління ризиками безпеки, планів локалізації та ліквідації наслідків аварій, а також заходів кіберзахисту;

– проведення оцінки ризиків на об'єктах критичної інфраструктури та обмін інформацією про ризики та загрози з іншими суб'єктами національної системи захисту критичної інфраструктури, а також створення умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури;

– створення окремого структурного підрозділу або визначення відповідальної особи за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб'єктами національної системи захисту критичної інфраструктури;

– організація заходів з реагування на інциденти, кризові ситуації, а також ліквідації їх наслідків на об'єктах критичної інфраструктури у взаємодії з іншими суб'єктами національної системи захисту критичної інфраструктури;

– участь у заходах із захисту повітряного простору над визначеними об'єктами критичної інфраструктури;

– створення і використання необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків;

– захист інформації про системи управління, зв'язку, фізичну безпеку та кібербезпеку, забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про об'єкти критичної інфраструктури;

– забезпечення захисту персоналу об'єктів критичної інфраструктури, організація та здійснення евакуаційних заходів у разі виникнення надзвичайних ситуацій.

До прав операторів критичної інфраструктури віднесено, зокрема, самостійно розробляти заходи щодо забезпечення безпеки об'єктів критичної інфраструктури, що не суперечать вимогам цього Закону та прийнятих відповідно до нього нормативно-правових актів.

Також оператори критичної інфраструктури забезпечують розроблення та затвердження у встановленому законодавством порядку вимог щодо організації захисту об'єктів критичної

інфраструктури та паспортів безпеки об'єктів критичної інфраструктури, також страхування ризику настання кризової ситуації.

З наведеного, тобто напрямів діяльності оператора критичної інфраструктури, можна визначити наступні корупційні ризики.

По-перше, різноплановість обов'язків оператора критичної інфраструктури (наприклад, створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки; участь у заходах із захисту повітряного простору; створення і використання необхідних резервів фінансових та матеріальних ресурсів; забезпечити страхування ризику настання кризової ситуації) вимагає наявності певного штату фахівців у оператора критичної інфраструктури та відповідних фінансових, матеріально-технічних можливостей, що може призвести до того, що в державі можуть сформулюватися оператора критичної інфраструктури, які будуть мати монопольне становище на ринку. Або, як варіант, суб'єкт господарювання, який був внесений до Реєстру об'єктів критичної інфраструктури, повинен заключати угоди з декількома операторами критичної інфраструктури в залежності від напрямів забезпечення захисту об'єкта критичної інфраструктури, що може створювати певні труднощі, які визначені нижче.

По-друге, відсутність належної конкуренції на ринку серед операторів критичної інфраструктури може призвести до того, що вони можуть зловживати своїм монопольним становищем, і своїми рекомендаціями по забезпеченню діяльності об'єкта критичної інфраструктури, перелік і зміст яких нормативно не визначено, можуть поставити об'єкт критичної інфраструктури у складне фінансове становище [6]. Наприклад, оператор критичної інфраструктури запропонує надто складний пропускний режим на об'єкт критичної інфраструктури або придбати надто коштовне програмне забезпечення чи комп'ютерне обладнання для забезпечення кібербезпеки цього суб'єкта господарювання тощо [7].

Як наслідок, керівництво об'єкту критичної інфраструктури повинно «домовлятися» з оператором критичної інфраструктури щодо зменшення фінансових витрат для забезпечення захисту об'єкта критичної інфраструктури. Не виключено, що таких операторів може бути декілька і з кожним треба вирішувати питання.

Також корупційні ризики вбачаються у разі, коли власник об'єкта критичної інфраструктури вирішив продати такий об'єкт чи його частину, змінити цільове призначення об'єкта, режим його функціонування чи передати права на цей об'єкт чи частину об'єкта іншим особам. Так, у підпункті 3) пункту 4 статті 21 Закону України «Про критичну інфраструктуру» [3] зазначається, що оператори критичної інфраструктури зобов'язані «завчасно, але не менше ніж за 30 календарних днів до дати зміни стану об'єкта критичної інфраструктури або його частини, інформувати уповноважений орган у сфері захисту критичної інфраструктури України про наміри змінити цільове призначення, режим функціонування чи намір передати права на об'єкт критичної інфраструктури та виконувати надані їм висновки та рекомендації.». Таким чином, відсутність нормативно врегульованих положень, у яких буде закріплено порядок, форми та зміст висновку (рекомендацій), які повинен надати оператора критичної інфраструктури,може призвести до того, що оператор критичної інфраструктури на власний розсуд може їх складати, що на практиці стане певним фінансовим чи організаційним тягарем для їх виконання власником об'єкта критичної інфраструктури і, відповідно, можуть бути однією з підстав для блокування реалізації комерційної угоди. І для реалізації комерційної угоди у власника об'єкта критичної інфраструктури можуть вимагати неправомірну вигоду або навпаки, власник об'єкта критичної інфраструктури буде зацікавлений у наданні неправомірної вигоди оператору критичної інфраструктури або посадовим особам уповноваженого органу з метою надання «позитивного» висновку чи рекомендації.

Неналежна реалізація у певних випадках вказаних у підпункті 3) пункту 4 статті 21 норм може сприяти порушенню прав суб'єктів господарювання, обмежувати їх можливості вільно розпоряджатися майном, яке перебуває у них на законних підставах, зокрема на праві приватної власності, що гарантується статтею 41 Конституції України [8] та статтею 319 Цивільного кодексу України [9].

Висновки. Враховуючи, що прийняття Верховною Радою України Закону України «Про критичну інфраструктуру» є на сьогодні найбільш з актуальних законодавчих актів, адже до його прийняття в нашій державі не існувало навіть поняття «об'єкти критичної інфраструктури» та фактично були відсутні особливі вимог до забезпечення безпеки об'єктів критичного призначення. Разом з тим аналіз вказаного закону засвідчує про існування великої кількості корупційних ризиків під час діяльності Уповноваженого органу у сфері захисту об'єктів критичної інфраструктури України – новоствореної Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України, операторів критичної інфраструктури, а також під час реалізації окремих його норм. Вказане вимагає у подальшому більш прискіпливого розроблення нормативно-правових актів, які будуть регулювати забезпечення безпеки об'єктів критичної інфраструктури.

ЛІТЕРАТУРА:

1. Солопова І. В. Правові умови захисту об'єктів критичної інфраструктури в Україні: проблеми та перспективи. *Південноукраїнський правничий часопис*. 2021. № 2. С. 119–125. DOI: https://doi.org/10.32850/sulj.2021.2.20

2. Концепція створення державної системи захисту критичної інфраструктури: схвалено розпорядженням Кабінету Міністрів України від 6 груд. 2017 р. № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80?find=1&text=%D0%97%D0%90%D0%9A%D0%9E%D0%9D#w1_1

3. Про критичну інфраструктуру: Закон України від 16 лист. 2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

4. Порядок віднесення об'єктів до критичної інфраструктури: затв. постановою Кабінету Міністрів України від 9 жовт. 2020 р. № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

5. Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України: постанова Кабінету Міністрів України від 12 липн. 2022 р. № 787. URL: https://zakon.rada.gov.ua/laws/show/787-2022-%D0%BF#Text

6. Приватна власність, але не до кінця. Які сюрпризи чекають на бізнес після ухвалення закону про критичну інфраструктуру? URL: https://www.epravda.com.ua/columns/2021/11/22/680007/

7. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури: затв. постановою Кабінету Міністрів України від 19 черв. 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

8. Конституція України, прийнята на п'ятій сесії Верховної Ради України 28 черв. 1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

9. Цивільний кодекс України від 16 січн. 2003 р. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15/ru/ed20131011#Text