УДК 351.863

ЄРМЕНЧУК Олександр Петрович
ПАЛЬЧИК Максим Леонідович

ПРОБЛЕМНІ АСПЕКТИ ПРАВОВОГО РЕГУЛЮВАННЯ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Постановка проблеми. Захист критичної інфраструктури (КІ) безпосередньо впливає на національну безпеку та реалізацію однієї з основних функцій держави, яка полягає у забезпеченні суверенності влади, оскільки формує здатність державного апарату ефективно та з урахуванням національних інтересів вирішувати внутрішні та зовнішні справи.

Директивою Ради ЄС від 2008 № 2008/114/ЄС зобов'язано всіх членів ЄС на законодавчому рівні належно закріпити питання організації захисту критичної інфраструктури. Для України, яка визначила курс вступу до ЄС одним із пріоритетних, відповідність законодавства європейським стандартам теж є важливим аспектом.

Ефективний захист критичної інфраструктури можливий лише за умов досить глибокої інтегрованої взаємодії державного та приватного сектору, їх партнерства, заснованого на двосторонній вигоді у забезпеченні безпеки та стійкості критичної інфраструктури [1].

Аналіз останніх досліджень і публікацій. Проблеми захисту критичної інфраструктури висвітлено в роботах Д. С. Бірюкова, І. Д. Бондаренка, С. П. Іванюти, О. О. Климчука, С. І. Кондратова, І. В. Манжул, О. І. Насвіт, В. М. Панченко, В. В. Петрова, П. П. Скурського, О. М. Суходолі та інших. Дослідженню окремих аспектів державно-приватного партнерства (ДПП) приділяли увагу такі науковці, як О. М. Вінник, Р. Н. Джабраілов, М. Ю. Маісурадзе, П. П. Надолішній, В. М. Устименко та інші. Водночас проблеми правового регулювання державно-приватного партнерства (ДПП) у сфері захисту критичної інфраструктури до сьогодні не були окремим об'єктом наукового дослідження та потребують додаткового вивчення.

Метою статті є аналіз правових основ регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури та формування з урахуванням міжнародного досвіду рекомендацій щодо їх подальшого удосконалення.

Виклад основного матеріалу. Відсутність наукових робіт за визначеним напрямом, на наш погляд, пов'язана з деякою новизною як проблематики державно-приватного партнерства, так і сфери захисту критичної інфраструктури. І якщо відносини державно-приватного партнерства, як окремої сфери якісно однорідних суспільних відносин, на законодавчому рівні в основному унормовані та

відносно досліджені, то законодавство щодо правовідносин у сфері критичної інфраструктури та її захисту ще знаходиться на стадії формування.

Зауважимо, що на необхідності заохочення повноцінної участі приватного сектору до захисту критичної інфраструктури наголошено у базовій Директиві ЄС від 2008 року № 114 «Про ідентифікацію та позначення європейської критичної інфраструктури та оцінки необхідності підвищення рівня її захисту». Вказане, на думку авторів документу, зумовлено значною участю приватного сектору у здійсненні нагляду і управління ризиками, плануванні безперервності ділових процесів та оперативного відновлення функціонування після стихійних лих [2].

У відповідності до зазначених директив, на національних рівнях, у різних країнах відповідні норми закріплюються переважно у стратегіях національної безпеки, стратегіях захисту різних сфер та інших базових розпорядчих актах, що стосуються функціонування критичної інфраструктури та організації її захисту.

Так, у Німеччині положення щодо доцільності зміцнення державно-приватного партнерства закріплено ще у Стратегії кібербезпеки від 2011 року. З метою поглиблення державно-приватної співпраці у сфері захисту критичної інфраструктури та підтримки надання послуг операторами критичної інфраструктури (KRITIS) між ними, їх асоціаціями та відповідними державними установами, такими, як Федеральне відомство інформаційної безпеки (нім. Bundesamt für Sicherheit in Informationstechnik, BSI), у більшості секторів критичної інфраструктури запроваджено взаємодію UP KRITIS (державно-приватне партнерство). Іншим прикладом державно-приватного партнерства у сфері захисту КІ є CERT-Verbund, групи безпеки і команди реагування на комп'ютерні інциденти (CERT), які сприяють обміну інформацією (наприклад, про вразливість або інциденти) та співпраці щодо усунення загроз. Співпраця з ними базується на угодах про нерозголошення інформації та на кодексі поведінки.

У Великобританії основи взаємодії державного та приватного секторів закладені Стратегією національної безпеки, Антитерористичною стратегією, (CONTEST – Counter terrorism strategy), Стратегією захисту кіберпростору (Cyber Security Strategy), а також в урядовому Плані розвитку національної інфраструктури.

Розвитку державно-приватного партнерства активно сприяє Національний центр кібербезпеки (англ. National Cybersecurity Center, NCSC). Ця організація Великобританії надає консультативну допомогу і підтримку державному і приватному секторам з питань протидії загрозам комп'ютерної безпеки [3]. До центру включені експерти у галузі безпеки з команди по реагуванню на комп'ютерні надзвичайні ситуації CERT-UK та MI5. Метою діяльності є покращення кіберзахисту об'єктів критичної інфраструктури, мереж державного та приватного секторів, надання консультацій операторам та громадянам для функціонування та ведення бізнесу з використанням інформаційних мереж та Інтернету [4].

В Іспанії при Національному центрі розвідки (ісп. Centro Nacional

de Inteligencia, CNI) діють одночасно орган сертифікації безпеки інформаційних систем та національна комп'ютерна команда криптологічного центру реагування на комп'ютерні інциденти (CCN-CERT) [5]. Центр реагування на комп'ютерні інциденти (ісп. Instituto Nacional de Ciberseguridad de España) займається збиранням інформації про інциденти у кіберпросторі, їх класифікацією та організацією протидії.

Загалом виникнення структури CERT тісно пов'язана з боротьбою проти комп'ютерних вірусів, так званих «мережевих черв'яків». Для протидії першому виявленому комп'ютерному вірусу у 1988 році на замовлення уряду США в університеті Карнегі – Меллон була сформована «комп'ютерна команда екстреної готовності – computer emergency response team» або «CERT». Після цього створення подібних організацій розпочалось в усьому світі [6]. На відміну від США, на території Європейського Союзу більшість груп CERT створювалися університетами і великими IT-компаніями. Загальноєвропейська організація носить назву «TF-CSIRT» (англ. Task force – collaboration security incident response teams).

Також досить активно співпраця в рамках ДПП розвивається і у сфері захисту критичної інфраструктури від надзвичайних ситуацій (аварії, катастрофи, стихійні лиха тощо).

Так, у деяких країнах, наприклад, у Данії, одним із основних координаторів роботи у сфері захисту критичної інфраструктури є Агентство з управління надзвичайними ситуаціями (датс. Beredskabsstyrelsen, DEMA). Саме цей орган і очолює контактну групу по захисту критичної інфраструктури, у межах якої організована міжгалузева співпраця, включаючи приватний сектор. Законодавчою основою організації партнерства в Данії є Акт керування діями (Інструкція) у випадку надзвичайної ситуації (англ. the Emergency Management Act). Він визначається як план функціонування суспільства за незвичайних умов. Його основною метою є забезпечення впорядкованого та скоординованого використання ресурсів громадянського суспільства.

Поряд із захистом від кіберзагроз та загроз від надзвичайних ситуацій захист критичної інфраструктури передбачає і захист від загроз у сфері державної безпеки (диверсії, розвіддіяльність іноземних спецслужб, тероризм, економічні експансії, економічне та промислове шпигунство, конкурентна розвідка), захист від внутрішніх загроз та фізичного знищення (хуліганство, підпали, загрози від діяльності організованих злочинних угруповань).

В Німеччині захист КІ та нових розробок є обов'язком операторів КІ, водночас Федеральне відомство Німеччини з охорони Конституції (нім. Bundesamt für Verfassungsschutz, BfV) надає операторам рекомендації щодо захисту КІ. Такі рекомендації, у першу чергу, включають протидію розвіддіяльності, організованій спецслужбами іноземних держав, та протидію іншим загрозам у цій сфері [7].

Обмін інформацією між BfV та бізнесом розпочато з 2008 року, цим займається підрозділ захисту економіки (нім. Arbeitsgemeinschaft für

Sicherheit der Wirtschaft). Крім того, у Німеччині діє цікавий механізм залучення до співпраці зі спецслужбою і цей процес активно заохочує держава. Так, особам, які сприяють діяльності BfV, надається право платити знижену податкову ставку на 10 відсотків за своїми доходами.

У межах реалізації державно-приватного партнерства у сфері захисту критичної інфраструктури в Німеччині існує спільна інтернет-платформа BSI та BBK (Федеральне управління цивільного захисту та ліквідації наслідків стихійних лих, нім. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe) щодо захисту критичної інфраструктури. Законодавчу основу для організації державно-приватного партнерства становлять Концепція основних заходів захисту критичної інфраструктури, Національна стратегія захисту критичної інфраструктури, Стратегія кібербезпеки Німеччини.

Аналіз норм законодавства провідних країн світу у сфері державно-приватного партнерства під час захисту критичної інфраструктури свідчить, що партнерство є взаємовигідним фактором, який сприяє інтеграційним процесам та забезпеченню державної безпеки загалом.

Так, в Концепції основних заходів захисту критичної інфраструктури, розроблених німецьким Федеральним міністерством внутрішніх справ (нім. Bundesministerium des Innern) для власників та керівників підприємств передбачено економічне обґрунтування по забезпеченню безпеки. У обґрунтуванні серед переваг для операторів КІ зазначена така вигода: збільшення доходів; спрощення обмежень; захист сегмента ринку; ризик-менеджмент; захист технологій та товарних знаків [8].

У США згідно положень національного плану (англ. National Infrastructure Protection Plan, NIPP) у частині (партнерство для забезпечення безпеки та стійкості критично важливої інфраструктури) передбачена необхідність учасників-партнерів колективно визначати національні пріоритети та формулювати чіткі заходи задля пом'якшення ризиків, прогнозувати та аналізувати прогрес і вигоду та відслідковувати зворотний зв'язок [1]. У свою чергу, національний план є формою організації національних зусиль, він сприяє прогресу на основі залучення широкого кола учасників-партнерів з різних рівнів урядової гілки влади, приватних та некомерційних секторів, у тому числі й громадянського суспільства, до розуміння важливості забезпечення безпеки і стійкості критично важливої інфраструктури. Крім того, план слугує консолідуючим фактором, оскільки використовує спільні структури та механізми, що полегшують обмін інформацією та вирішення спільних проблем.

В Україні на загальнодержавному рівні за останній час прийнято низку документів стратегічного та доктринального характеру, що так чи інакше охоплюють питання захисту критичної інфраструктури. У цих документах приділено увагу як розвитку правового регулювання, так і державно-приватного партнерства у сфері захисту критичної інфраструктури.

Зокрема в п. 4.13 Стратегії національної безпеки України одним з основних пріоритетів забезпечення

безпеки критичної інфраструктури визначено комплексне вдосконалення правової основи захисту критичної інфраструктури та створення системи державного управління її безпекою. Також пріоритетним визнано налагодження співробітництва між суб'єктами захисту критичної інфраструктури та розвиток державно-приватного партнерства у сфері запобігання надзвичайним ситуаціям і реагування на них. Приділено увагу в Стратегії національної безпеки України й необхідності розробки та запровадження механізмів обміну інформацією між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту чутливої інформації у цій сфері [9].

У контексті нашого дослідження варто згадати положення Стратегії кібербезпеки України. Відповідно до п. 1 Стратегії державно-приватне партнерство та широка співпраця з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту визнані одним із ключових принципів забезпечення кібербезпеки України. Пунктом 4.3 аналізованого документу закріплено, що кіберзахист критичної інфраструктури має полягати у налагодженні співробітництва між суб'єктами забезпечення кіберзахисту критичної інфраструктури та розвитку ДПП у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема, в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період.

У Стратегії кібербезпеки України також наголошується на необхідності створення умов «для залучення підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інфраструктури, до забезпечення кібербезпеки України. Зокрема, мають бути врегульовані питання щодо обов'язковості вжиття ними заходів із забезпечення захисту інформації та кіберзахисту відповідно до вимог законодавства, а також щодо сприяння ними державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту» [10].

Як бачимо, розробниками Стратегії кібербезпеки України та Стратегії національної безпеки України наголошено на необхідності запровадження механізму обміну інформацією між державними органами, приватним сектором і громадянами стосовно загроз критичній інформаційній інфраструктурі.

Значну увагу проблемам державно-приватного партнерства у сфері захисту КІ приділено в Концепції створення державної системи захисту критичної інфраструктури. По-перше, визнано, що нерозвиненість державно-приватного партнерства у сфері захисту критичної інфраструктури є однією із основних проблем, що потребує розв'язання. По-друге, закріплено, що здійснення державно-приватного партнерства у сфері захисту критичної інфраструктури є одним із основних принципів. В межах створення державної системи захисту критичної інфраструктури на загальнодержавному рівні передбачено формування засад державно-приватного

партнерства у сфері захисту критичної інфраструктури. Які, у свою чергу, планується створювати на основі взаємної довіри, обміну інформацією, створення стимулів для інвестування у здійснення заходів, спрямованих на захист критичної інфраструктури, запровадження уніфікованих підходів щодо вимог до підвищення рівня захисту. Також документом визначено необхідність налагодження обміну інформацією між суб'єктами державної системи захисту критичної інфраструктури про загрози критичній інфраструктурі, характеристики систем захисту об'єктів критичної інфраструктури, механізми і процедури реагування на загрози [11].

Можемо констатувати, що наведеними нормативними актами стратегічного та доктринального характеру саме державно-приватне партнерство визначено ключовим елементом захисту критичної інфраструктури. При цьому пріоритетними напрямами розвитку державно-приватного партнерства у сфері захисту критичної інфраструктури необхідно вважати:

– розвиток ДПП у сфері запобігання надзвичайним ситуаціям та реагування на них;

– розвиток державно-приватного партнерства у запобіганні кіберзагрозам, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема, в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

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

– сприяння приватними партнерами державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту.

Втім, на наш погляд, вказані напрями не є вичерпними та деталізуються щорічними планами заходів на відповідний рік. Зокрема, щорічні плани заходів із реалізації Стратегії кібербезпеки України на 2016 та 2018 роки містять положення, що стосуються окремих напрямів державно-приватної взаємодії. Серед них можемо виокремити такі, як:

– розробка галузевих стандартів кіберзахисту та впровадження системи незалежного аудиту інформаційної безпеки об'єктів критичної інфраструктури;

– створення на базі СБ України та Держспецзв'язку ситуаційних центрів з кібербезпеки, об'єднаних в єдину систему виявлення та попередження кіберзагроз на об'єктах КІ;

– створення національної телекомунікаційної мережі як єдиної платформи захищених електронних комунікацій органів державної влади;

– здійснення проектно-пошукових робіт зі створення резервного центру обробки даних Казначейства;

– опрацювання питання з розробки програми державно-приватного партнерства з питань кіберзахисту;

– організація та сприяння проведенню державної експертизи вітчизняного антивірусного програмного забезпечення;

– розробка правового механізму блокування електронних інформаційних ресурсів із забороненим законом

контентом та підготовка пропозицій з його організаційно-технічного забезпечення;

– розроблення пропозицій щодо механізму забезпечення кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури в умовах особливого періоду, правового режиму воєнного або надзвичайного стану та ін.

Водночас, незважаючи на широке закріплення напрямів державно-приватного партнерства, їх реалізація у сфері захисту критичної інфраструктури значно ускладнюється тим, що, не обмежуючись сферою захисту критичної інфраструктури, в Україні практично відсутній позитивний досвід реалізації проектів державно-приватного партнерства, незалежно від сфери впровадження.

Стримуючим фактором для розвитку державно-приватного партнерства в Україні, на думку дослідників, є складність, багаторівневість і забюрократизованість нормативно-правової бази регулювання державно-приватного партнерства, що створює ризики для ефективного використання цього механізму [12].

На сьогодні одним з основних нормативно-правових актів, яким унормовано правові та організаційні засади взаємодії державних та приватних партнерів, є Закон України «Про державно-приватне партнерство України». Законом сформовано поняття та ознаки державно-приватного партнерства, закріплено його основні принципи та форми, визначено основні сфери застосування державно-приватного партнерства та особливості договірно-правових відносин [13]. Відповідно до статті 1 вказаного закону державно-приватне партнерство – це співробітництво між державою Україна, Автономною Республікою Крим, територіальними громадами в особі відповідних державних органів та органів місцевого самоврядування (державними партнерами) та юридичними особами, крім державних та комунальних підприємств, або фізичними особами-підприємцями (приватними партнерами), що здійснюється на основі договору в порядку, встановленому цим законом та іншими законодавчими актами, і відповідає ознакам державно-приватного партнерства, визначеним законом.

Основними ознаками ДПП відповідно до ст. 1 закону є:

– надання прав управління (користування, експлуатації) об'єктом партнерства або придбання, створення (будівництво, реконструкція, модернізація) об'єкта державно-приватного партнерства з подальшим управлінням (користуванням, експлуатацією) за умови прийняття та виконання приватним партнером інвестиційних зобов'язань відповідно до договору, укладеного в рамках державно-приватного партнерства;

– довготривалість відносин (від 5 до 50 років);

– передача приватному партнеру частини ризиків у процесі здійснення державно-приватного партнерства;

– внесення приватним партнером інвестицій в об'єкти партнерства із джерел, незаборонених законодавством.

Закон України не встановлює вичерпного переліку форм державно-приватного партнерства, а лише

визначає, що основною формою ДПП є цивільно-правовий договір, зокрема про концесію; управління майном (виключно за умови передбачення у договорі, укладеному в рамках державно-приватного партнерства, інвестиційних зобов'язань приватного партнера); спільну діяльність та інші договори.

Відносини у сфері державно-приватного партнерства врегульовано також цілою низкою підзаконних актів, яких мають дотримуватись приватні та державні партнери. Серед них можемо назвати Постанову Кабінету Міністрів України від 11 квітня 2011 року № 384 «Деякі питання організації здійснення державно-приватного партнерства», якою затверджено Порядок проведення конкурсу з визначення приватного партнера для здійснення державно-приватного партнерства щодо об'єктів державної, комунальної власності та об'єктів, які належать Автономній Республіці Крим, а також Порядок проведення аналізу ефективності здійснення державно-приватного партнерства [14]; Постанову Кабінету Міністрів України від 16 лютого 2011 року № 232 «Про затвердження Методики виявлення ризиків здійснення державно-приватного партнерства, їх оцінки та визначення форми управління ними» [15].

У контексті обміну інформацією між державними та приватними партнерами, що визначений одним із пріоритетних напрямів розвитку ДПП, варто згадати Постанову Кабінету Міністрів України «Про затвердження Порядку надання приватним партнером державному партнеру інформації про виконання договору, укладеного в рамках державно-приватного партнерства». Порядок визначає процедуру надання приватним партнером державному партнеру інформації про виконання договору, укладеного в рамках державно-приватного партнерства, встановлює строки подання такої інформації у формі звіту та визначає уповноваженого суб'єкта, який проводить моніторинг, узагальнює та оприлюднює результати здійснення державно-приватного партнерства від імені державного партнера, яким є Мінекономрозвитку [16].

Зауважимо, що розробниками проекту Закону України «Про критичну інфраструктуру та її захист» [17], який наразі досить активно обговорюється, замість поняття «державно-приватне партнерство» запропоновано поняття «державно-приватна взаємодія» та відповідні способи її реалізації, що, на нашу думку, потребує додаткового наукового обґрунтування та подальшого унормування з визначенням конкретних форм такої взаємодії, адже вказані поняття не є тотожними.

Висновки. У межах підготовленої роботи нами досліджено досвід правового регулювання та організації захисту КІ з використанням елементів державно-приватного партнерства у таких іноземних юрисдикціях, як Німеччина, Іспанія, США та Данія. Встановлено, що на національних рівнях у різних країнах норми щодо захисту критичної інфраструктури закріплюються переважно у стратегіях національної безпеки, стратегіях захисту різних сфер та у розпорядчих актах, що стосуються функціонування критичної інфраструктури та організації її захисту.

При цьому найбільш поширеною організаційною формою взаємодії є групи безпеки та реагування на комп'ютерні інциденти, що складаються з представників державного та приватного сектору, основна діяльність яких спрямована на обмін інформацією та взаємодію у межах усунення загроз об'єктам критичної інформаційної інфраструктури.

Розбудова національної системи захисту критичної інфраструктури України на сьогодні передбачена документами стратегічного характеру, якими, серед іншого, визнано необхідність розвитку державно-приватного партнерства та окреслено основні його напрями. Також для громадського обговорення представлено проект Закону України «Про критичну інфраструктуру та її захист», яким також охоплено питання відносин державного і приватного сектору. Водночас, на наш погляд, запропонована в проекті закону дефініція «державно-приватна взаємодія» потребуватиме подальшого наукового дослідження та обґрунтування.

Аналіз існуючих підходів до захисту критичної інфраструктури у світі дозволив виокремити напрями, в яких доцільно розвивати партнерство. Поряд із захистом від кіберзагроз, захист критичної інфраструктури вважаємо передбачає і захист від загроз у сфері державної безпеки (диверсії, розвіддіяльність іноземних спецслужб, тероризм, економічні експансії, економічне та промислове шпигунство, конкурентна розвідка), захист від внутрішніх загроз та фізичного знищення (хуліганство, підпали, загрози від діяльності організованих злочинних угруповань), захист від надзвичайних ситуацій (аварій, катастроф, стихійних лих). Удосконалення державно-приватного партнерства у кожній із цих сфер потребує подальшого розвитку та детального наукового вивчення.

Список використаних джерел

1. NIPP 2013 Partnering for Critical Infrastructure. Security and Resilience [Електронний ресурс]. – Режим доступу : https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

2. Council Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (CD 2008/ 114/EC) [Електронний ресурс]. – Режим доступу : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG.

3. Национальный центр кибербезопасности Великобритании [Електронний ресурс]. – Режим доступу : https://ru.wikipedia.org/wiki/Центр_национальной_компьютерной_безопасности_Великобритании.

4. About the NCSC [Електронний ресурс]. – Режим доступу: https://www.ncsc.gov.uk/information/about-ncsc.

5. Centro Nacional de Inteligencia [Електронний ресурс]. – Режим доступу : https://es.wikipedia.org/wiki/Centro_Nacional_de_Inteligencia.

6. El Instituto Nacional de Ciberseguridad (INCIBE) [Електронний ресурс].

– Режим доступу : https://www.incibe.es/que-es-incibe/como-trabajamos.

7. Bundesamt für Verfassungsschutz [Електронний ресурс]. – Режим доступу : https://www.verfassungsschutz.de.

8. Защита критической инфраструктуры. Концепция основных мер защиты. Рекомендация для предприятий. – Bundesministerium des Innern, 2006 [Електронний ресурс]. – Режим доступу : www.bmi.bund.de.

9. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : Указ Президента України від 26 травня 2015 року № 287/ 2015 // Офіційний вісник України. – 2015. – № 43. – Ст. 14.

10. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 року № 96/2016 // Офіційний вісник України. – К., 2016. – № 23. – Ст. 899.

11. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : Розпорядження Кабінету Міністрів України від 6 грудня 2017 року № 1009-р [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/ show/1009-2017-%D1%80.

12. Щодо розвитку державно-приватного партнерства як механізму активізації інвестиційної діяльності в Україні : аналітична записка / Національний інститут стратегічних досліджень [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/816.

13. Про Державно-приватне партнерство : Закон України від 1 вересня 2010 року № 2404-VI // Відомості Верховної Ради України. – 2010. – № 40. – Ст. 1436.

14. Деякі питання організації здійснення державно-приватного партнерства : Постанова Кабінету Міністрів України від 11 квітня 2011 року № 384 // Офіційний вісник України. – 2011. – № 28. – Ст. 1168.

15. Про затвердження Методики виявлення ризиків здійснення державно-приватного партнерства, їх оцінки та визначення форми управління ними : Постанова Кабінету Міністрів України від 16 лютого 2011 року № 232 // Офіційний вісник України. – 2011. – № 18. – Ст. 769.

16. Про затвердження Порядку надання приватним партнером державному партнеру інформації про виконання договору, укладеного в рамках державно-приватного партнерства : Постанова Кабінету Міністрів України від 9 лютого 2011 року № 81 // Офіційний вісник України. – 2011. – № 10. – Ст. 458.

17. Про критичну інфраструктуру та її захист : проект Закону України [Електронний ресурс]. – Режим доступу : http://me.gov.ua/.

Рецензенти:
доктор юридичних наук,
старший науковий співробітник
І. Авдошин,
кандидат юридичних наук,
М. Давиденко

Аннотация. Статья посвящена изучению правовых основ сотрудничества государства и частого сектора в сфере защиты критической инфраструктуры. Проанализирован международный опыт правового регулирования защиты критической инфраструктуры и развития государственно-частного партнерства в иностранных юрисдикциях. Предложены основные направления, по которым необходимо развивать государственно-частное партнерство в сфере защиты критической инфраструктуры Украины.

Ключевые слова: государственно-частное партнерство, правовое регулирование, критическая инфраструктура, защита критической инфраструктуры, международный опыт.

Abstract. The article is concerned with the study of legal basis of public and private partnership in the sphere of critical infrastructure protection. International experience of critical infrastructure protection and public-private partnership legal regulation in foreign jurisdictions was analyzed. The main directions for developing public-private partnership in the field of critical infrastructure protection in Ukraine have been proposed.

Key words: public-private partnership, legal regulation, critical infrastructure, critical infrastructure protection, international experience.

УДК 347.734

ІВАНОВ Юрій Анатолійович

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

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

Аналіз останніх досліджень і публікацій. Різні аспекти правового регулювання діяльності банків та банківської системи досліджують у своїх працях Ю. В. Ващенко, Д. О. Гетьманцев, А. І. Марущак, О. П. Орлюк та багато інших науковців. Безпосередньо на проблемах банківської безпеки зосередили свій науковий пошук