УДК 342.951

АЛЕКСЕЄВА О.А., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-6629-3606.

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. *У статті висвітлено питання правового забезпечення кібербезпеки об'єктів критичної інфраструктури. Розглядається понятійний апарат у сфері забезпечення кібербезпеки об'єктів критичної інфраструктури. Міститься аналіз чинного законодавства України у сфері забезпечення кібербезпеки, а також зарубіжного досвіду у цій сфері. Аналізується проект Закону України "Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури" в контексті оптимізації законодавства України у сфері забезпечення кібербезпеки. Визначено доцільність застосування комплексного підходу до забезпечення кібербезпеки об'єктів інформаційної критичної інфраструктури. Внесені пропозиції щодо удосконалення системи забезпечення кібербезпеки об'єктів критичної інфраструктури.*

Ключові слова: *правове забезпечення, об'єкти критичної інфраструктури, об'єкти інформаційної критичної інфраструктури, кібербезпека.*

Summary. *The article highlights the issue of legal support of cyber security of critical infrastructure objects. The conceptual apparatus in this area is considered. It contains an analysis of the current legislation of Ukraine in the field of cyber security. The project of the Law of Ukraine "On Amendments to Some Laws of Ukraine Regarding Urgent Measures to Strengthen Cybersecurity Capacities of State Information Resources and Critical Information Infrastructure Objects" is analyzed in the context of optimizing Ukrainian legislation in the field of cyber security. The expediency of applying a comprehensive approach to ensuring cyber security of critical information infrastructure objects has been determined. A proposal has been introduced to improve the legislation of Ukraine in the field of cybersecurity.*

Keywords: *legal support, critical infrastructure, critical infrastructure objects, critical information infrastructure objects, cyber security.*

Постановка проблеми. З 14 січня 2022 року, коли відбулася кібератака росії на низку об'єктів критичної інфраструктури, Україна перебуває в стані першої в історії кібервійни з рф [1, с. 9]. Повномасштабне вторгнення військ рф на територію України, що триває із 24 лютого 2022 року, супроводжується численними актами агресії у кіберпросторі, який визнано одним з можливих театрів воєнних дій. Відповідно до оприлюднених Державною службою спеціального зв'язку та захисту інформації України даних, від 15 лютого Україна зазнала понад 3000 DDoS-атак; постійно розповсюджується шкідливе програмне забезпечення, здійснюються фішингові розсилки та інші прояви війни у кіберпросторі [2]. У зв'язку зі збільшенням кількості та масштабу кібернападів як одного із проявів агресії рф проти України, що спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України, а також на об'єкти критичної інформаційної інфраструктури, набуває необхідність вдосконалення нормативного

забезпечення у сфері захисту об'єктів критичної інформаційної інфраструктури. Проблемою є фактична відсутність дієвої узгодженої політики у сфері захисту таких об'єктів, що зумовлюється як відсутністю системного підходу на національному рівні, так і законодавчою невизначеністю форм взаємодії державних органів між собою. Незважаючи на низку законів та інших нормативно-правових актів, що визначають повноваження й компетенцію державних органів у цій сфері, в Україні досі бракує системного підходу до управління комплексом таких систем та об'єктів [3, с. 58]. Відсутні й будь-які узгоджені прояви здійснення державно-приватного партнерства у сфері взаємодії із забезпечення кібербезпеки, що є одним з пріоритетних напрямів з огляду на світовий досвід [3, с.58].

Результати аналізу наукових публікацій. Ще до великомасштабних атак в Україні наукові дослідження у сфері захисту критичних інфраструктур від кібератак проводились такими вченими, як П.Д. Рогов [4], І.П. Сініцин, П.П. Ігнатенко, О.О. Слабоспицька, О.В. Артеменко [5], Н.О. Ткачук [6], І. Субач [7] та ін.

Закордонний досвід забезпечення захисту об'єктів критичних інфраструктур був предметом поглиблених досліджень таких науковців, як Батюк О.В. [8], Єрменчук О.П. [9], Гора І.В. [8], Кондратов С.І., Суходоля О.М. [3], Пядишев В.Г. [10] та ін.

Однак, не зважаючи на наявність значної кількості наукових праць щодо цієї теми, варто зазначити, що вони не вичерпують усіх аспектів проблеми правового забезпечення кіберзахисту об'єктів критичної інфраструктури. Крім того, залишаються не достатньо дослідженими результати зарубіжних наукових досліджень забезпечення кібербезпеки критичної інфраструктури. Водночас, євроатлантичні прагнення України однозначно передбачають надалі зближення нормативно-правової бази, програмних та інших технічних засобів та методів протидії кібератакам на критичні інфраструктури, а також забезпечення стійкості останніх [10, с. 230]. Проблематика забезпечення кібербезпеки критичної інфраструктури загострюються в умовах воєнного стану, що зумовлює актуальність цієї статті.

Метою статті є визначення шляхів та удосконалення правового забезпечення кібербезпеки об'єктів критичної інфраструктури на основі аналізу законодавства окремих зарубіжних країн а також нормативно-правової бази з питань захисту об'єктів критичної інфраструктури.

Виклад основного матеріалу. Сьогодні тематика кіберзахисту об'єктів інформаційної критичної інфраструктури дедалі частіше обговорюється під час наукових конференцій, семінарів, міжнародних форумів, присвячених питанням розвитку та захисту критичної інфраструктури. Термін "забезпечення кібербезпеки об'єктів критичної інфраструктури" дедалі частіше вживають журналісти в засобах масової інформації. Помітним кроком у забезпеченні кібербезпеки стало створення в Україні Національного координаційного центру кібербезпеки у 2016 році.

Проблематика критичної інфраструктури пов'язана із бурхливим розвитком нових підходів до забезпечення національної безпеки в розвинених країнах світу, що спричинено швидкими змінами, які відбуваються у безпековому середовищі у глобальному, регіональному та національному вимірах. Зрозуміло, що це знаходить відповідне відображення у розвитку національних законодавств, у т.ч. в термінологічному забезпеченні діяльності державних органів тієї чи тієї країни [3, с. 32].

Значне місце цьому безпековому напрямку відведене в нормах чинного законодавства України, де він визнаний пріоритетним у контексті політики національної безпеки. Нормативно-правову базу в цій сфері утворюють: Закон України "Про основи забезпечення кібербезпеки України"; Указ Президента України "Про затвердження

Стратегії кібербезпеки України" від 26.08.21 р. № 447; Постанова Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.19 р. № 518; Постанова Кабінету Міністрів України "Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимогу щодо захисту якої встановлено законом" від 11.11.20 р. № 11; Постанова Кабінету Міністрів України "Про затвердження Методичних рекомендацій щодо категоризації об'єктів критичної інфраструктури від 9.10.20 р. № 1109; Вимоги до функціонування системи кіберзахисту у банківській системі України (постанова Правління Національного банку України від 12.08.22 р. № 178). Також можна стверджувати, що сьогодні у процесі протидії кібератакам в умовах воєнного стану напрацьовується безцінний новий досвід.

В Україні під критичною інфраструктурою розуміється сукупність об'єктів такої інфраструктури до кола яких віднесено: 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 [11]. Відповідно до Закону України "Про критичну інфраструктуру" об'єкти критичної інфраструктури – це підприємства, установи й організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей. До критичної інфраструктури належать й особливо небезпечні виробництва, аварії на яких викликані будь-якими причинами (природними або техногенними надзвичайними ситуаціями), також можуть обернутися катастрофічними для певних територій і їх населення наслідками [12].

Термін "критична інфраструктура" з'явився порівняно недавно і ввійшов до обігу ділового, наукового та дипломатичного спілкування із середини 1990-х рр. і спершу був пов'язаний з інформаційною інфраструктурою [13, с. 151]. Критично важливі об'єкти інфраструктури діють як система життєзабезпечення повсякденного існування людей, співтовариство яких підтримується доволі комплексною і складною мережею інфраструктурних систем. Виведення з ладу, серйозні і дрібні збої, постійні недоліки в роботі та функціонуванні певної інфраструктури чи її елементів можуть створювати загрозливі, а іноді й критичні для нормальної життєдіяльності ситуації [8, с. 134].

Цілісна концепція критичної інфраструктури вперше була сформована та розроблена у США і саме цю країну вважають піонером у розробленні й запровадженні концепції критичної інфраструктури та її захисту, оскільки саме у 1996 р. уперше дано визначення терміну "критична інфраструктура", до якого вносилися зміни й він набув сучасного розуміння [13, с. 4; 14]. Натомість посилений розвиток відповідного безпекового напряму розпочався як наслідок уроків, винесених із терактів 11 вересня 2001 р., коли було усвідомлено рівень загроз міжнародного тероризму [3, с. 31].

Під критичною інфраструктурою законодавство США розуміє "системи та засоби, фізичні чи віртуальні, настільки важливі для Сполучених Штатів, що недієздатність або знищення таких систем та активів підривало би національну безпеку, національну економіку, загрожувало би здоров'ю чи безпеці населення, чи мало би результатом будь-яку комбінацію із переліченого" [15].

Директива Президента США (PPD-21) визначає безпеку "як зменшення ризиків для критичної інфраструктури шляхом вжиття фізичних заходів чи захисних кіберзаходів стосовно вторгнень, нападів або дії природних лих чи техногенних аварій" [16].

Відповідно до директиви Президента США № 63 "Стратегія спільних зусиль адміністрації США і приватного сектору у сфері захисту критичної інфраструктури" головне завдання досліджень у цій сфері полягає у виявленні ключових об'єктів (або їх сукупності), вплив на які може спричинити найбільш негативний ефект на галузь економіки, ключовий ресурс або всю інфраструктуру, а також в оцінці прогнозованих наслідків подібного впливу й розробці механізмів зниження таких ризиків [17]. США сьогодні є лідером у запровадженні інноваційних підходів, мають розвинуту, добре розгалужену національну державну систему забезпечення безпеки об'єктів критичної інфраструктури, яка спрямована на посилення безпеки та стійкості критичної інфраструктури стосовно фізичних і кіберзагроз. З цією метою Федеральний уряд цієї країни співпрацює із власниками та операторами відповідних об'єктів і систем, державними органами всіх рівнів, місцевими органами влади з тим, щоб вживати активних заходів з управління ризиками, враховуючи при цьому всі види загроз, реалізація яких може призвести до тяжких наслідків для національної безпеки, стабільності економіки, здоров'я та безпеки населення чи будь-якої комбінації з переліченого. При цьому зусилля спрямовуються на зменшення уразливостей, мінімізацію наслідків, ідентифікацію та ліквідацію загроз, прискорення реагування та застосування відновлювальних заходів, пов'язаних з такою інфраструктурою. Уряд ураховує міжнародний контекст проблем, пов'язаних із безпекою та стійкістю такої інфраструктури, та взаємодіє з міжнародними партнерами у цій сфері [3, с. 34]. Крім цього, плідною і ефективною визнається діяльність кібервійськ США, які проводять операції в кіберпросторі.

У США серед актів, що становлять нормативно-правову основу у цій сфері, слід виокремити: Національну стратегію внутрішньої безпеки (жовтень 2007 р.); Національну стратегію фізичного захисту критичної інфраструктури та ключових активів (лютий 2003 р.); Національну стратегію захисту кіберпростору (лютий 2003 р.); Закон про внутрішню безпеку (листопад 2002 р.).

Заслуговує на увагу прийнятий у 2002 р. в США Акт щодо інформації з критичної інфраструктури (Critical Infrastructure Information Act ("CIIA") [5], в якому регулювалися положення стосовно обміну інформацією з питань оцінки вразливості та загроз інфраструктурі, також і пов'язаних із терористичними загрозами [18]. Цей Акт запровадив термін "інформація щодо критичної інфраструктури" і розуміння інформації, яка зазвичай не перебуває в полі зору суспільства та належить до безпеки функціонування критичної інфраструктури чи захищених систем [8, с. 134].

Нині в більшості розвинених країн широко використовують досвід і напрацювання з питань кіберзахисту критичної інфраструктури, які отримали й продовжують отримувати фахівці з США.

Водночас розуміння критичної інфраструктури та її об'єктів у окремих європейських країнах за спільних до їх визначення підходів може дещо різнитись, що зумовлене національними традиціями, розуміннями національних цінностей, безпеки країни, добробуту населення тощо [8, с. 135].

Ще у 2004 р. на рівні ЄС та Європейської Комісії розпочали створення проекту захисту критичної інфраструктури "European Programme for Critical Infrastructure Protection" ("EPCIP"), в рамках якого важливу увагу приділено захисту від терористичних загроз. Тоді під критичною інфраструктурою розуміли "обладнання,

служби й інформаційні системи, життєво важливі для держави, знищення чи відмова від яких призведе до послаблення суспільства, національного господарства, системи охорони здоров'я, безпеки ефективного функціонування державного устрою" [8, с. 135].

У законодавстві Євросоюзу з питань захисту від кібератак на себе звертає увагу Директива (ЄС) 2016/1148 Європейського Парламенту та Ради "Про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем на території Союзу" від 6 липня 2016 р. [19], яка приймалася з урахуванням 75-ти визначальних факторів. Ця Директива встановлює заходи, спрямовані на досягнення високого рівня безпеки мережевих та інформаційних систем у Євросоюзі [10, с. 232]. З цією метою Директива: (a) встановлює зобов'язання для всіх держав-членів прийняти національну стратегію безпеки мереж та інформаційних систем; (b) створює групу співробітництва для підтримки та сприяння стратегічній співпраці та обміну інформацією між державами-членами, а також для розвитку довіри між ними; (c) створює мережу груп реагування на інциденти комп'ютерної безпеки ("мережа CSIRT"), щоб сприяти розвитку довіри між державами-членами та сприяти швидкому та ефективному оперативному співробітництву; (d) встановлює вимоги безпеки та сповіщення для операторів основних послуг та постачальників цифрових послуг; (e) встановлює зобов'язання для держав-членів щодо призначення національних компетентних органів, єдиних контактних осіб та CSIRT із завданнями, пов'язаними з безпекою мереж та інформаційних систем [19; 10, с. 232]. Для посилення протидії проявам кіберзлочинності у 2013 році в структурі Європолу був створений Європейський центр боротьби з кіберзлочинністю [8; 10].

У червні 2023 року депутати Європарламенту ухвалили нові правила обміну електронними доказами між правоохоронними органами з метою підвищення ефективності транскордонних розслідувань.

За висновками зарубіжних експертів [20; 21], критична інфраструктура являє собою складну систему, яка характеризується атрибутами, серед яких виділяється: 1) необмежена кількість варійованих об'єктів та параметрів системи; 2) важко прогнозована поведінка об'єктів, для яких характерна велика кількість взаємозв'язків, які класифіковано по різних секторах [22]. Вбачається, що складовою цієї системи є й чітко визначені правові засади захисту об'єктів критичної інфраструктури від кіберзагроз.

Попри наявність загальновизнаних принципів та підходів щодо забезпечення безпеки об'єктів інформаційної інфраструктури кожна національна система є по суті унікальною і неминуче несе на собі відбиток національної специфіки, тому слід уникати механічного копіювання зарубіжного досвіду на українських теренах [3, с. 54]. Україна перебуває на початковому етапі створення державної системи забезпечення безпеки таких об'єктів, тому при розгляді зарубіжного досвіду в цій слід пам'ятати, що механічне перенесення навіть передового досвіду без належного урахування специфіки та реалій українського сьогодення може лише підірвати зусилля на цьому напрямі, скомпрометувати його та в такий спосіб суттєво затримати його розвиток у нашій країні [3, с. 32].

В Україні ще за радянських часів існувала збалансована система управління техногенною безпекою об'єктів підвищеної небезпеки, в основу якої покладено методологічний підхід аналізу ризиків, які обумовлювалися надійністю функціонування елементів, складових, об'єктів тощо. Іншими словами, ризик виникнення надзвичайної ситуації визначався вірогідністю відмов природнього характеру, аварій, інших

надзвичайних подій (ймовірність виникнення та розвитку подій внаслідок умисного пошкодження елементів не враховувався та не розглядався взагалі) [23, с. 92].

Проте, комплексне забезпечення об'єктів критичної інфраструктури, у т.ч. об'єктів інформаційної інфраструктури, передбачає інший підхід, в основу якого має бути покладено: удосконалення механізмів та процедури взаємодії та обміну інформацією на всіх рівнях управління, функціонування на основі ризик-орієнтованих підходів, чіткого розподілу повноважень і відповідальності щодо критичної інфраструктури (для цього зазвичай визначають відповідальний державний орган або органи); розвиток взаємодії з іншими суб'єктами системи з метою ефективного залучення населення, суспільства, бізнесу та державних установ і організацій до розв'язання проблем забезпечення безпеки та стійкості критичної інфраструктури; налагодження ефективного обміну інформацією між усіма суб'єктами процесу забезпечення безпеки та стійкості критичної інфраструктури; забезпечення виконання функцій інтегрування та аналізу даних для підтримки процесів планування та прийняття рішень стосовно критичної інфраструктури; проведення підготовки кадрів і населення для забезпечення безпеки та стійкості критичної інфраструктури; постійна перевірка готовності сил і засобів, планів і процедур взаємодії та обміну інформацією під час регулярних навчань на всіх рівнях управління [3, с. 54-55].

Відповідно до положень Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.21 р. № 447, забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Серед передумов та чинників, що формують загрози кібербезпеці України, Стратегія кібербезпеки України називає: недосконаліть нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації; відсутність у значної частини державних органів відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом, здійснення фінансування робіт із кіберзахисту за залишковим принципом; відсутність механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності держави; невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі; незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки; недостатню захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури; невідповідність вимогам законодавства стану захисту інформаційно-комунікаційних систем державних органів та суб'єктів господарювання, в яких обробляється значна частина інформації з обмеженим доступом [24].

Беручи до уваги вищеназвані чинники, усунення яких є необхідним для зменшення загроз кібербезпеці України, а також нагальну потребу у посиленні спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, було розроблено проект Закону України "Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури" (реєстр. №8087 від 29.09.22 р.), впровадження якого, на думку розробників, створить належну правову основу для стримування збройної агресії рф у кіберпросторі та надання відсічі агресору. Цим проектом, зокрема, передбачено: створення та забезпечення функціонування національної системи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози щодо інформаційних, електронних комунікаційних та інформаційно-

комунікаційних систем; визначення завдань, функцій та повноважень суб'єктів національної системи реагування: Національного координаційного центру з кібербезпеки, галузевих та регіональних команд реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, уповноважених представників Національної поліції України і Служби безпеки України, Об'єднаної групи реагування на інциденти кібербезпеки, кібератаки, кіберзагрози, приватних команд реагування; створення та забезпечення функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки: закріплення обов'язку власників та розпорядників інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури, повідомляти про всі інциденти кібербезпеки, кібератаки; закріплення обов'язку операторів критичної інфраструктури повідомляти про всі значні інциденти кібербезпеки, кібератаки щодо об'єктів критичної інформаційної інфраструктури; впровадження системи державного контролю за станом технічного захисту інформації та кіберзахисту. За результатами громадських слухань щодо цього законопроекту підприємці, юристи, експерти дійшли згоди, що він потребує суттєвого серйозного доопрацювання через невідповідність сучасним європейським стандартам у сфері кібербезпеки та створення загроз для бізнесу [26].

Узгодженню різних підходів сприятиме обговорення цього проекту з громадськістю та широким колом науковців та практичних фахівців, а його реалізація допоможе якісному удосконаленню законодавства України у сфері кібербезпеки та захисту інформації.

Висновки.

У багатьох розвинутих країнах світу забезпечення кібербезпеки об'єктів критичної інфраструктури визнано пріоритетним напрямом політики національної безпеки, в рамках якого активно розбудовуються національні системи із забезпечення кіберзахисту (безпеки) таких об'єктів, ухвалюються законодавчі акти для регламентації діяльності учасників системи, готуються відповідні кадри, налагоджуються партнерські відносини з приватним сектором, здійснюються освітні заходи серед населення тощо [3, с. 7].

На підставі аналізу законодавства окремих зарубіжних країн, а також нормативно-правової бази з питань захисту об'єктів критичної інфраструктури, можна вважати, що система забезпечення кібербезпеки об'єктів критичної інфраструктури нашої держави потребує:

створення та забезпечення функціонування єдиної національної системи реагування на інциденти кібербезпеки, кібератаки, кібертероризм;

створення та забезпечення функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кібертероризм;

удосконалення державно-приватної взаємодії у сфері кібербезпеки;

законодавчого визначення повноважень уповноваженого органу з питань захисту критичної інфраструктури України з науково-технічного забезпечення процедур захисту об'єктів інформаційної критичної інфраструктури (у т.ч. реалізації функцій з координації, здійснення контролю та нагляду, експертної оцінки, організації заходів компенсаційного та превентивного характеру тощо);

створення науково-дослідних установ, які будуть забезпечувати наукове супроводження функціонування єдиної національної системи реагування на кіберінциденти;

розробки та впровадження необхідного методичного та нормативного забезпечення аналізу та прогнозування наслідків кібердиверсії або кібертероризму на об'єктах інформаційної критичної інфраструктури [23, с. 92].

Використана література

1. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа "Інститут інформації, безпеки і права НАПрН України"; Національна бібліотека України ім. В.І.Вернадського. Київ, 2023. № 6. 153 с. URL: https://ippi.org.ua/sites/default/files/2023-6.pdf (дата звернення: 14.10.2023).

2. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: пояснювальна записка до проєкту закону України. URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1490885 (дата звернення: 14.10.2023 р.).

3. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України: аналіт. доп. / Бобро Д.Г., Іванюта С. П., Кондратов С.І., Суходоля О.М. / за заг. ред. О.М. Суходолі. Київ: НІСД, 2019. 224 с. URL:https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf

4. Рогов П.Д. Ворович Б.О., Ткаченко В.А. Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері: збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2017. № 1. С. 64-72. URL: http:// nbuv.gov.ua/UJRN/Znpcvsd_2017 _1_13 (дата звернення: 06.01.2023).

5. Сініцин І.П., Ігнатенко П.П., Слабоспицька О.О., Артеменко О. В. Комплексний підхід до побудови системи кіберзахисту критичної інформаційної інфраструктури держави. *Проблеми програмування*. 2017. № 3. С. 128-148. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/144499/08-Sinitsyn.pdf?sequence=1 (дата звернення: 06.01.2023).

6. Ткачук Н.А. Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. *Інформація і право.* № 1(24)/2018. С. 133-138. URL: http://ippi.org.ua/sites/default/files/16_4.pdf (дата звернення: 06.01.2023).

7. Субач І., Микитюк А., Кубрак В. Архітектура та функціональна модель перспективної проактивної інтелектуальної SIEM-системи для кіберзахисту об'єктів критичної інфраструктури. *Information Technology and Security*. 2019. Vol. 7, Iss. 2 (13). Pp. 208-215.

8. Гора І.В., Батюк О.В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії.* 2021. Вип. 1 (11). С. 132-139. URL: https://dspace. lvduvs.edu.ua/bitstream/1234567890/3709/1/18-.pdf (дата звернення: 14.10.2023).

9. Єрменчук О.П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: ДДУ ВС, 2018. 180 с.

10. Пядишев В.Г. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. *Південноукраїнський правничий часопис.* 2022. № 4. Ч. 3. С. 229-234. URL: http://www.sulj. oduvs.od.ua/archive/2022/4/part_3/38.pdf (дата звернення: 14.10.2023).

11. Про критичну інфраструктуру: Закон України від 16.11.21 р. № 1882-IX. URL: https://zakon. rada.gov.ua/laws/show/1882-20#n80 (дата звернення: 14.10.2023 р.).

12. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA PATRIOT Act) ACT OF 2001. URL: http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW107publ56.htm (дата звернення: 14.10.2023).

13. Курбанов Я.Л. Забезпечення природно-техногенної безпеки в Україні і проблема визначення поняття "критична інфраструктура". *Південноукраїнський правничий часопис.* 2016. № 2. С. 150-154.

14. On July 15, 1996, President Clinton signed Executive Order 13010 establishing President's Commission on Critical Infrastructure Protection (PCCIP). Critical Infrastructure Protection. Federal Register. July 17, 1996. Vol. 61. No. 138.

15. USA PATRIOT ACT (2001) defined critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". URL: https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

16. Presidential Policy Directive 21 (PPD-21). Critical Infrastructure Security and Resilience. (2013, February 12). URL: https://obamawhitehouse.archives.gov/the-press-office/2013/ 02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (дата звернення: 14.10.2023).

17. Executive Order. 13010. Critical Infrastructure Protection. Federal Register. Vol. 61, № 138. July 17. 1996. P. 3747-3750.

18. Critical Infrastructure Information Act of 2002 ("CIIA"). URL: https:// www.fas.org/sgp/crs/RL31762.pdf

19. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high overall level of security for network and information systems within the Union territory. Site. URL: https:// eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:O J.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата звернення: 06.01.2023).

20. Keating C, Rogers, R., Dryer D., Sousa-Poza A., Safford R., Peterson W., Rabadi G. System of Systems Engineering. *Engineering Management Journal*. 2003. Vol. 15. № 3.

21. Jackson, M. Systems Methodology for the Management Sciences. New York. Plenum, 1991. 298 p.

22. Congressional Research Service Report for Congress. Critical Infrastructures: Background, Policy and Implementation. 2002. URL: https://fas.org/sgp/crs/homesec/RL30153.pdf (дата звернення: 19.06.2023).

23. Леонов Б.Д., Шостак Р.М., Серьогін В.С. Розвиток методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури (на прикладі США). *Інформація і право*. № 3(34)/2020. С. 88-95. URL: https://ippi.org.ua/sites/default/files/12_18.pdf (дата звернення: 19.09.2023).

24. Стратегія кібербезпеки України: Указ Президента України від 26.08.21 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 19.09.2023).

25. Про внесення змін до деяких законів України щодо невідкладних заходів посилення спроможностей із кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури: проєкт закону України (реєстр. № 8087 від 29.09.22 р.). URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1490881 (дата звернення: 19.09.2023).

26. Депутати готуються проголосувати за законопроект про кібербезбеку, проти поточної редакції якого виступив бізнес, юристи, Міноборони та експерти. URL: https://racurs.ua/ua/n184973-vlada-proignoruvala-golos-biznesu-schododoopracuvannya-zakonoproektu-pro-kiberbezpeku.html (дата звернення: 10.07.2023).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~