Адміністративне право і процес; фінансове право; інформаційне право
УДК 004.056.5

Жевелєва Ірина Сергіївна
старший викладач
Національна академія Служби безпеки України
Жевелева Ирина Сергеевна
старший преподаватель
Национальная академия Службы безопасности Украины
Zhevelieva Iryna
Senior Lecturer
National Academy of Security Service of Ukraine

ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ
ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ
LEGAL FRAMEWORKS FOR ENSURING THE INFORMATION SECURITY OF CRITICAL INFRASTRUCTURE FACILITIES

Анотація. *У статті проведений аналіз правових засад забезпечення захисту об'єктів критичної інфраструктури в Україні та провідних країнах світу. На основі проведеного аналізу, а також вивчення і узагальнення наукових публікацій вітчизняних фахівців щодо об'єктів критичної інфраструктури, запропоновані шляхи удосконалення забезпечення інформаційної безпеки об'єктів критичної інфраструктури України. Здійснено аналіз діючого законодавства України з питань захисту об'єктів критичної інфраструктури. Визначено основні проблеми у сфері побудови державної системи захисту критичної інфраструктури.*

Наведено визначення основних термінів, які містяться у законодавчих та підзаконних нормативних актах. Підкреслено, що термін «критична інфраструктура» законодавчо не закріплений і запропоноване його авторське визначення. Виокремлено складові національної інформаційної інфраструктури, які є першочерговими об'єктами кіберзахисту. Проаналізовано погляди науковців на основні завдання для забезпечення інформаційної безпеки об'єктів критичної інфраструктури. Наведено визначення критичної інфраструктури за законодавством зарубіжних країн на прикладі Сполучених Штатів Америки, Великобританії, країн Європейського Союзу. Доведено, що державно-приватне партнерство є ключовим елементом захисту критичної інфраструктури, визначено основні напрями його розвитку у сфері забезпечення інформаційної безпеки об'єктів критичної інфраструктури. Аргументовано необхідність взаємодії Служби безпеки України із об'єктами критичної інфраструктури, визначено основні умови для такої взаємодії, запропоновано повноваження СБ України з питань забезпечення інформаційної безпеки об'єктів критичної інфраструктури. Наведено пропозиції по удосконаленню законодавства України з питань забезпечення інформаційної безпеки об'єктів критичної інфраструктури.

Ключові слова: *критична інфраструктура, захист критичної інфраструктури, забезпечення інформаційної безпеки об'єктів критичної інфраструктури.*

Аннотация. *В статье проведен анализ правовых основ обеспечения защиты объектов критической инфраструктуры в Украине и ведущих странах мира. На основе проведенного анализа, а также изучения и обобщения научных публикаций отечественных специалистов по объектам критической инфраструктуры, предложены пути совершенствования обеспечения информационной безопасности объектов*

критической инфраструктуры Украины. Осуществлен анализ действующего законодательства Украины по вопросам защиты объектов критической инфраструктуры. Определены основные проблемы в сфере построения государственной системы защиты критической инфраструктуры. Приведены определения основных терминов, содержащихся в законодательных и подзаконных нормативных актах. Подчеркнуто, что термин «критическая инфраструктура» законодательно не закреплен и предложено его авторское определение. Выделены составляющие национальной информационной инфраструктуры, которые являются первоочередными объектами киберзащиты. Проанализированы взгляды ученых на основные задачи для обеспечения информационной безопасности объектов критической инфраструктуры. Приведены определения критической инфраструктуры в законодательстве зарубежных стран на примере Соединенных Штатов Америки, Великобритании, стран Европейского Союза. Доказано, что государственно-частное партнерство является ключевым элементом защиты критической инфраструктуры, определены основные направления его развития в сфере обеспечения информационной безопасности объектов критической инфраструктуры. Аргументировано необходимость взаимодействия Службы безопасности Украины с объектами критической инфраструктуры, определены основные условия для такого взаимодействия, предложено полномочия СБ Украины по вопросам обеспечения информационной безопасности объектов критической инфраструктуры. Приведены предложения по усовершенствованию законодательства Украины по вопросам обеспечения информационной безопасности объектов критической инфраструктуры.

Ключевые слова: *критическая инфраструктура, защита критической инфраструктуры, обеспечение информационной безопасности объектов критической инфраструктуры.*

Summary. *The article analyzes the legal basis for ensuring the protection of critical infrastructure in Ukraine and leading countries. Based on the analysis, as well as the study and generalization of scientific publications of domestic experts on critical infrastructure, author proposed ways of improving of the information security of critical infrastructure of Ukraine. The current legislation of Ukraine on the protection of critical infrastructure is analyzed. The main problems in the field of building a state system of critical infrastructure protection are identified. The definition of the basic terms contained in legislative and by-laws is given. It is emphasized that the term "critical infrastructure" is not enshrined in law and its author's definition is proposed. The components of the national information infrastructure, which are the primary objects of cyber security, have been identified. The views of scientists on the main tasks for information security of critical infrastructure are analyzed. The definition of critical infrastructure according to the legislation of foreign countries is given on the example of the United States of America, Great Britain, the countries of the European Union. It is proved that public-private partnership is a key element of critical infrastructure protection, the main directions of its development in the field of information security of critical infrastructure are identified. The necessity of interaction of the Security Service of Ukraine with critical infrastructure facilities is argued, the main conditions for such interaction are determined, the powers of the Security Service of Ukraine on information security of critical infrastructure facilities are proposed. Suggestions for improving the legislation of Ukraine on information security of critical infrastructure are presented.*

Key words: *critical infrastructure, protection of critical infrastructure, information security of critical infrastructure facilities.*

Постановка проблеми. На необхідності та першочерговості захисту об’єктів критичної інфраструктури у своєму щорічному Посланні до Верховної Ради України «Про внутрішнє та зовнішнє становище в Україні» ще у 2017 році наголосив Президент України. Проте, наявного у держави законодавчого та інституційного інструментарію недостатньо щоб оперативно та якісно реагувати на проблеми, пов’язані із забезпеченням інформаційної безпеки об’єктів критичної інфраструктури. Наразі виникла ситуація, коли жоден орган державної влади комплексно не опікується цією проблематикою. Єдина державна система захисту критичної інфраструктури фактично відсутня. Відсутній і єдиний закон, який визначав би термінологію, критерії віднесення об’єктів до критичної інфраструктури та регулював би взаємовідносини у цій сфері.

Захист об'єктів критичної інфраструктури в Україні врегульований сегментарно та, переважно, у підзаконних нормативно-правових актах. Очевидно, що сектор безпеки та оборони України в частині захисту об’єктів критичної інфраструктури потребує реформування, в першу чергу шляхом прийняття відповідного закону та удосконалення діючих нормативно-правових актів в частині, що стосується.

Аналіз останніх досліджень і публікацій. Автором проаналізовано ряд наукових публікацій, статей, монографій, аналітичних доповідей про останні тенденції у підходах до проблем пов’язаних з правовими засадами забезпечення інформаційної безпеки об’єктів критичної інфраструктури. Проведено порівняльний аналіз вітчизняного та міжнародного досвіду у цій сфері.

Сучасні виклики та пріоритетні завдання сектору безпеки у процесі захисту критичної інфраструктури у своїх наукових працях досліджував

Суходоля О.М [1]. Проблеми, що стосуються захисту критичної інфраструктури та забезпечення інформаційної безпеки об'єктів критичної інфраструктури розглядались Гончаром С.Ф., Леоненком Г.П., Юдіним О.Ю. [2] Проблемні аспекти правового регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури досліджувались Єрменчуком О.П., Пальчиком М.Л. [3] Проблеми та перспективи впровадження захисту критичної інфраструктури в Україні були проаналізовані Бірюковим Д.С. [4], Кондратовим С.І., Насвітом О.І. [5].

Зазначені роботи частково висвітлюють шляхи вирішення проблематики та не дають єдиного уявлення про сучасні підходи до розуміння правових засад забезпечення інформаційної безпеки об'єктів критичної інфраструктури.

Формулювання цілей статті (постановка завдання). Автором у даній науковій статті за мету ставиться визначити окремі проблеми, пов'язані з недосконалістю правових засад забезпечення інформаційної безпеки об'єктів критичної інфраструктури в Україні та запропонувати шляхи їх вирішення.

Виклад основного матеріалу. Поняття критичної інфраструктури визначено в законодавстві багатьох країн світу. Ним оперують експерти, науковці, цей термін вживають журналісти в засобах масової інформації. В Україні на законодавчому рівні визначені окремі терміни та аспекти функціонування об'єктів критичної інфраструктури. Захист таких об'єктів розглядається, переважно, у відомчому форматі та регламентується підзаконними нормативно-правовими актами.

Вперше на небезпеці знищення або пошкодження об'єктів критичної інфраструктури наголошено у рішенні РНБО України від 01.03.2014 року «Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України» [6]. Важливість захисту критичної інфраструктури для забезпечення національної безпеки

визначена у Стратегії національної безпеки України та рішеннях РНБО України 2016-2017 років. Суттєві кроки у напрямі законодавчого регламентування критичної інфраструктури було зроблено із прийняттям Стратегії кібербезпеки України [7], Закону України «Про основні засади забезпечення кібербезпеки України» [8] та Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави [9].

На виконання Рішення РНБО України від 29 грудня 2016 р. «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» [10] та з метою упровадження низки суттєвих заходів на державному, галузевому й регіональному рівнях із правового й організаційно-методичного забезпечення, координації та консолідованого забезпечення ресурсами систем безпеки, спільного використання засобів безпеки, що знаходяться в підпорядкуванні окремих відомств Кабінетом Міністрів України було розроблено Концепцію створення державної системи захисту критичної інфраструктури України [11], яка визначила основні напрямки, механізми і строки комплексного правового врегулювання питання захисту критичної інфраструктури та створення системи державного управління в цій сфері, та План заходів з реалізації Концепції створення державної системи захисту критичної інфраструктури України [12]. Реалізація Концепції розрахована на десятирічний строк (з 2017 р. до 2027 р.) та передбачає короткострокові, середньострокові, довгострокові завдання.

Зокрема, у Концепції зазначається, що на теперішній момент основними проблемами у сфері побудови державної системи захисту критичної інфраструктури є:

- недостатність та неузгодженість нормативно-правового регулювання в Україні захисту систем і об'єктів, які відносять до критичної інфраструктури, зокрема, відсутність у національному

законодавстві профільного закону про критичну інфраструктуру та її захист;

- відсутність на національному рівні державного органу, відповідального за координацію дій у сфері захисту критичної інфраструктури існуючих державних систем захисту та кризового реагування;
- невизначеність функцій, повноважень та відповідальності центральних органів виконавчої влади та інших органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів об'єктів критичної інфраструктури;
- відсутність єдиної методології проведення оцінки загроз та ризиків критичній інфраструктурі, запобігання їх реалізації та реагування на них реалізовані загрози;
- відсутність єдиних критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації;
- нерозвиненість державно-приватного партнерства та невизначеність джерел фінансування заходів із захисту критичної інфраструктури;
- недостатній рівень міжнародного співробітництва у цій сфері [11].

Слід відзначити, що завдання щодо створення системи захисту критичної інфраструктури України та уточнення ролі сектору безпеки і оборони уже перейшло на етап практичного вирішення.

Міністерством економічного розвитку і торгівлі України, на виконання завдань поставлених Концепцією, спільно із відповідними центральними органами виконавчої влади, іншими державними органами і установами, підготовлено проект Закону України «Про критичну

інфраструктуру та її захист», в якому передбачається врегулювання вищевказаних проблем.

Проте, для забезпечення відповідності завдань та повноважень сектору безпеки новим викликам, разом із прийняттям Закону України «Про критичну інфраструктуру та її захист», треба внести зміни і до Законів України «Про Службу безпеки України», «Про національну безпеку України», «Про інформацію», «Про боротьбу з тероризмом».

У Зеленій книзі з питань захисту критичної інфраструктури в Україні критична інфраструктура України визначається, як система та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки. У свою чергу захист критичної інфраструктури України – це комплекс заходів, реалізований в нормативно-правових, організаційних, технологічних інструментах, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури [5, с. 8].

Незважаючи на те, що поняття критичної інфраструктури в нормативно-правових актах України вживалось і раніше, офіційне визначення цьому поняттю було дане лише в 2016 році Постановою Кабінету Міністрів України «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави» від 23 серпня 2016 р. № 563 [9] критична інфраструктура визначається як сукупність об’єктів інфраструктури 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 та людських жертв.

Відповідно до п 16 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» дано визначення критично важливих об'єктів інфраструктури – це підприємства, установи та 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 [8].

Отже, об'єктами критичної інфраструктури можуть виступати не тільки підприємства пріоритетних галузей, але і інші об'єкти, наприклад, транспортні системи, науково-дослідні установи та ін.

Б. В. Хлевицький пропонує виокремити першочерговими об'єктами кіберзахисту такі складові національної інформаційної інфраструктури:

– державні електронні інформаційні ресурси, автоматизовані системи керування, а також електронні інформаційні ресурси, у яких обробляється (зберігається) інформація, що є власністю держави або інша інформація, несанкціоновані дії стосовно якої можуть створювати погрозу національній безпеці й обороноздатності країни;

– автоматизовані системи керування, що функціонують в інтересах суб'єктів військової організації країни;

– телекомунікаційні системи загального користування;

– інформаційно-телекомунікаційні системи й автоматизовані системи керування, несанкціоноване втручання в роботу яких може загрожувати економічній безпеці, соціальній стабільності держави тощо [13, с. 31-32].

Д. С. Бірюков в аналітичній доповіді «Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні»

наводить у якості можливого прикладу для застосування в Україні досвіду деяких зарубіжних держав в цій сфері. Зокрема, науковець на підставі аналізу міжнародного досвіду визначає, що основою забезпечення захищеності й безпеки критичної інфраструктури є вирішення низки питань, з-поміж яких основними виділяє такі: координація і взаємодія органів державної влади та обмін інформацією про загрози; організація державно-приватного партнерства у сфері безпеки; використання ризик-орієнтованого підходу при попередженні загроз критичній інфраструктурі [4 , с. 5].

При всій близькості визначень цього терміну в законодавстві іноземних країн, існують відмінності у цьому понятті. Під критичною інфраструктурою в США розуміють «комплекс фізичних та віртуальних активів, систем і мереж, що мають життєво важливе значення для держави, руйнування або недієздатність яких, в тому числі і окремих їх елементів, матиме згубні наслідки для національної безпеки, економіки, безпеки і здоров'я населення, чи матиме будь-яку комбінацію з перелічених наслідків» [14]. У законодавстві Великобританії критична інфраструктура визначена як: «найважливіші елементи інфраструктури, а саме активи, об'єкти, системи, мережі, процеси і ключові посадови особи, втрата яких може привести до згубного впливу на: 1) доступність, цілісність або надання основних послуг, в тому числі тих, порушення цілісності яких може привести до втрати життя або виникнення нещасних випадків з урахуванням значних економічних і соціальних наслідків; 2) національну безпеку, національну оборону або функціонування держави» [15]. В окремих державах ЄС критична інфраструктура – це активи, системи або їх частини, що розташовані в державах-членах Європейського Союзу, які мають важливе значення для основних життєво важливих соціальних функцій, здоров'я, безпеки, економічного або соціального благополуччя

людей, а також порушення або руйнування яких матиме значний вплив на спроможність держави виконувати свої функції [16].

З наведених визначень видно, що відмінності у терміні «критична інфраструктура» в різних країнах світу не суттєві. Терміни покликані відобразити національну, організаційну особливість унікальності сфери його застосування, відмінності нормативно правових систем.

Окремі країни, об'єднання держав здійснюють захист національних та колективних інтересів, не обмежуючись своїми кордонами. Крім національних об'єктів критичної інфраструктури, розглядаються і зарубіжні об'єкти, безпека яких має стратегічне значення для тієї чи іншої держави. У законодавстві ЄС, європейська критична інфраструктура – це критична інфраструктура, що розташована в державах членах Європейського Союзу, недієздатність або руйнування якої матиме істотний згубний вплив на принаймні дві держави Союзу.

Акцентуємо увагу на необхідності законодавчого регламентування забезпечення інформаційної безпеки об'єктів критичної інфраструктури, розробки організаційних форм захисту інформації з обмеженим доступом, державно-приватного партнерства у цій сфері.

Слід погодитись з Єрменчуком О.П. та Пальчиком М.Л, які вважають державно-приватне партнерство ключовим елементом захисту критичної інфраструктури. При цьому, пріоритетними напрямами розвитку державно-приватного партнерства у сфері забезпечення інформаційної безпеки об'єктів критичної інфраструктури необхідно вважати:

– 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 і приватним сектором стосовно загроз критичній інфраструктурі та захисту інформації з обмеженим доступом у цій сфері;

– сприяння приватними партнерами державним органам у виконанні завдань із забезпечення кібербезпеки та кіберзахисту [3, с. 45].

Зважаючи на процес реформування Служби безпеки України у частині переходу від боротьби з економічною злочинністю до зосередження уваги на захисті об'єктів критичної інфраструктури, державно-приватне партнерство у сфері забезпечення, у тому числі, інформаційної безпеки об'єктів критичної інфраструктури доцільно здійснювати через Службу безпеки України. Для цього необхідно: по-перше, чітко визначити поняття та види об'єктів критичної інфраструктури на законодавчому рівні; по-друге, визначити інформацію, яка потребує особливого захисту у контексті забезпечення нормального функціонування об'єктів критичної інфраструктури; по-третє, визначити повноваження СБ України у сфері захисту інформаційної безпеки об'єктів критичної інфраструктури.

До таких повноважень, зокрема, слід віднести: участь у розробці поточних та перспективних планів, а також систем забезпечення інформаційної безпеки об'єктів критичної інфраструктури; обмін інформацією із суб'єктами, у віданні яких перебувають об'єкти критичної інфраструктури, щодо виникнення загроз інформаційної безпеки; оцінка загроз інформаційної безпеки для діяльності об'єктів критичної інфраструктури тощо. Для реалізації відповідних повноважень в структурі СБ України доцільно утворити спеціальний підрозділ та затвердити положення про нього.

Погодимось з О.М. Суходолею, який з метою удосконалення законодавства у сфері захисту об'єктів критичної інфраструктури, пропонує внести такі доповнення до Закону України «Про Службу безпеки

України»: ст. 2 – щодо «захисту критичної інфраструктури»; ст. 10 – щодо створення функціонального підрозділу «захисту критичної інфраструктури» (можливо замість слів «боротьби з корупцією і організованою злочинною діяльністю»); ст. 11 — щодо створення підрозділів на окремих «об'єктах критичної інфраструктури» (замість слів «державних стратегічних об'єктах»); підпункт 6 ст. 24 — щодо контррозвідувального забезпечення «критичної інфраструктури» (замість слів «енергетики, транспорту, зв'язку, а також важливих об'єктів інших галузей господарства») [1, с. 71-72].

Висновки і перспективи подальших досліджень у даному напрямку. Проведене дослідження підтверджує, що в Україні на сьогоднішній день законодавчо не визначено єдине поняття критичної інфраструктури та не унормований уніфікований перелік її об'єктів. Разом з тим, відсутній і єдиний закон, який би комплексно регламентував діяльність об'єктів критичної інфраструктури. Окремі аспекти її захисту регулюються різними, переважно, підзаконними нормативно-правовими актами. Законодавче регулювання забезпечення інформаційної безпеки об'єктів критичної інфраструктури зводиться лише до кіберзахисту і не охоплює інші організаційно-правові форми захисту інформації з обмеженим доступом.

Зважаючи на відсутність законодавчого визначення терміну «критична інфраструктура», ми пропонуємо ст. 1 Закону України «Про національну безпеку України» доповнити визначенням понять:

– критична інфраструктура – це об'єкти, які є стратегічно важливими для економіки і національної безпеки, виведення з ладу або руйнування яких може мати вплив на національну безпеку і оборону, природне середовище, призвести до значних фінансових збитків та людських жертв.

– об’єкти критичної інформаційної інфраструктури – це сукупність інформаційно-телекомунікаційних систем державного та приватного сектору, що забезпечують функціонування та безпеку стратегічних інститутів, систем і об’єктів держави (органів центрального та місцевого управління, систем управління енергетикою, транспортом, зв’язком, банківським сектором, підприємств, під час діяльності яких використовуються та/або виробляються небезпечні речовини тощо) і безпеку громадян (системи управління правоохоронних структур й оборонного сектору тощо), несанкціоноване втручання в роботу яких може загрожувати економічній, екологічній, соціальній та іншим видам безпеки або завдати шкоди міжнародному іміджу держави.

Крім того, запропоновано ст.15 Закону України «Про інформацію» доповнити положенням про те, що інформація про об’єкти критичної інформаційної інфраструктури – це необхідна, для забезпечення кіберзахисту даних об’єктів державного та приватного секторів, інформація про стан захищеності та дотримання заходів кібернетичної безпеки, включаючи фактори або елементи, що впливають або можуть впливати на складові кібернетичного захисту систем критичної інформаційної інфраструктури.

Перспективи подальшого вивчення заявленої проблеми вбачаємо у дослідженні критеріїв віднесення підприємств, установ і організацій до об’єктів критичної інфраструктури.

Література

1. Суходоля О. М. Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки. Науковий часопис, 2017. Вип. 1-2 (13-14). С. 50-80.
2. Гончар С. Ф., Леоненко Г. П., Юдін О. Ю. Теоретико-методологічний аспект забезпечення інформаційної безпеки об'єктів критичної

інфраструктури. Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі, 2014. № 806. С. 34-39: веб-сайт. URL: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_8 (дата звернення 20.05.2020).

3. Єрменчук О.П., Пальчик М.Л. Проблемні аспекти правового регулювання державно-приватного партнерства у сфері захисту критичної інфраструктури. Інформаційна безпека людини, суспільства, держави. 2019. № 2 (26). С. 40-49.
4. Бірюков Д.С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: Аналітична доповідь. К.: ПП «Видавництво «ФЕНІКС», 2012. 92 с.
5. Зелена книга з питань захисту критичної інфраструктури в Україні / Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М. К.: Національний інститут стратегічних досліджень, 2015. 35 с.
6. Про невідкладні заходи щодо забезпечення національної безпеки, суверенітету і територіальної цілісності України: Рішення Ради національної безпеки і оборони України від 1.03.2014: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/n0001525-14 (дата звернення 15.05.2020).
7. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 № 96/2016: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення 15.05.2020).
8. Про основні засади забезпечення кібербезпеки: Закон України від 5.10.2017 № 2163-VIII: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 15.05.2020).
9. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури

держави: Постанова Кабінету Міністрів України від 23.09.2016 № 563: веб-сайт. URL: http://zakon5.rada.gov.ua/laws/show/563-2016-%D0%BF. (дата звернення 15.05.2020).

10. Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури: Рішення Ради національної безпеки і оборони України від 29.12.2016: веб-сайт. URL: http://zakon3.rada.gov.ua/laws/show/en/n0014525-16/paran2#n2 (дата звернення 15.05.2020).
11. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України від 6.12.2017 № 1009-р: веб-сайт. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80 (дата звернення 15.05.2020).
12. Про затвердження Плану заходів з реалізації Концепції створення державної системи захисту критичної інфраструктури України: Розпорядження Кабінету Міністрів України, 2017 р: веб-сайт. URL:http://www.kmu.gov.ua (дата звернення 15.05.2020).
13. Хлевицький В. Б. Захист критичної інформаційної інфраструктури в контексті контррозвідувального забезпечення інформаційної безпеки держави : Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., 30 березня 2012 р. Київ: Наук-вид. відділ НА СБ України, 2012. 301 с.
14. USA Patriot Act of 2001: веб-сайт. URL: https://www.gpo.gov/fdsys/pkg/BILLS107hr3162enr/pdf/BILLS107hr3162enr.pdf (дата звернення 05.05.2020).
15. The national infrastructure: веб-сайт. URL: http://www.cpni.gov. uk (дата звернення 05.05.2020).
16. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the

assessment of the need to improve their protection: веб-сайт. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L: 2008:345:0075:0082:EN:PDF (дата звернення 05.05.2020).

References

1. Sukhodolja O. M. Zakhyst krytychnoji infrastruktury: suchasni vyklyky ta priorytetni zavdannja sektoru bezpeky. Naukovyj chasopys, 2017. Vyp. 1-2 (13-14). S. 50-80.
2. Ghonchar S. F., Leonenko Gh. P., Judin O. Ju. Teoretyko-metodologhichnyj aspekt zabezpechennja informacijnoji bezpeky ob'jektiv krytychnoji infrastruktury. Visnyk Nacionaljnogho universytetu «Ljvivsjka politekhnika». Komp'juterni systemy ta merezhi, 2014. # 806. S. 34-39: veb-sajt. URL: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_8 (data zvernennja 20.05.2020).
3. Jermenchuk O.P., Paljchyk M.L. Problemni aspekty pravovogho reghuljuvannja derzhavno-pryvatnogho partnerstva u sferi zakhystu krytychnoji infrastruktury. Informacijna bezpeka ljudyny, suspiljstva, derzhavy. 2019. # 2 (26). S. 40-49.
4. Birjukov D.S. Zakhyst krytychnoji infrastruktury: problemy ta perspektyvy vprovadzhennja v Ukrajini: Analitychna dopovidj. K.: PP «Vydavnyctvo «FENIKS», 2012. 92 s.
5. Zelena knygha z pytanj zakhystu krytychnoji infrastruktury v Ukrajini / Birjukov D.S., Kondratov S.I., Nasvit O.I., Sukhodolja O.M. K.: Nacionaljnyj instytut strateghichnykh doslidzhenj, 2015. 35 s.
6. Pro nevidkladni zakhody shhodo zabezpechennja nacionaljnoji bezpeky, suverenitetu i terytorialjnoji cilisnosti Ukrajiny: Rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 1.03.2014: veb-sajt. URL:

https://zakon.rada.gov.ua/laws/show/n0001525-14 (data zvernennja 15.05.2020).

7. Strateghija kiberbezpeky Ukrajiny: Ukaz Prezydenta Ukrajiny vid 15.03.2016 # 96/2016: veb-sajt. URL: https://zakon.rada.gov.ua/laws/show/96/2016 (data zvernennja 15.05.2020).
8. Pro osnovni zasady zabezpechennja kiberbezpeky: Zakon Ukrajiny vid 5.10.2017 # 2163-VIII: veb-sajt. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (data zvernennja 15.05.2020).
9. Pro zatverdzhennja Porjadku formuvannja pereliku informacijno-telekomunikacijnykh system ob'jektiv krytychnoji infrastruktury derzhavy: Postanova Kabinetu Ministriv Ukrajiny vid 23.09.2016 # 563: veb-sajt. URL: http://zakon5.rada.gov.ua/laws/show/563-2016-%D0%BF. (data zvernennja 15.05.2020).
10. Pro udoskonalennja zakhodiv zabezpechennja zakhystu ob'jektiv krytychnoji infrastruktury: Rishennja Rady nacionaljnoji bezpeky i oborony Ukrajiny vid 29.12.2016: veb-sajt. URL: http://zakon3.rada.gov.ua/laws/show/en/n0014525-16/paran2#n2 (data zvernennja 15.05.2020).
11. Pro skhvalennja Koncepciji stvorennja derzhavnoji systemy zakhystu krytychnoji infrastruktury: Rozporjadzhennja Kabinetu Ministriv Ukrajiny vid 6.12.2017 # 1009-r: veb-sajt. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80 (data zvernennja 15.05.2020).
12. Pro zatverdzhennja Planu zakhodiv z realizaciji Koncepciji stvorennja derzhavnoji systemy zakhystu krytychnoji infrastruktury Ukrajiny: Rozporjadzhennja Kabinetu Ministriv Ukrajiny, 2017 r: veb-sajt. URL:http://www.kmu.gov.ua (data zvernennja 15.05.2020).

13. Khlevycjkyj V. B. Zakhyst krytychnoji informacijnoji infrastruktury v konteksti kontrrozviduvaljnogho zabezpechennja informacijnoji bezpeky derzhavy: Aktualjni problemy upravlinnja informacijnoju bezpekoju derzhavy : zb. mater. nauk.-prakt. konf., 30 bereznja 2012 r. Kyjiv: Nauk-vyd. viddil NA SB Ukrajiny, 2012. 301 s
14. USA Patriot Act of 2001: veb-sajt. URL: https://www.gpo.gov/fdsys/pkg/BILLS107hr3162enr/pdf/BILLS107hr3162enr.pdf (data zvernennja 05.05.2020).
15. The national infrastructure: veb-sajt. URL: http://www.cpni.gov. uk (data zvernennja 05.05.2020).
16. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection: veb-sajt. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (data zvernennja 05.05.2020).