УДК 351.86:004:007](477)

О. В. Мельничук,
аспірант кафедри глобалістики, євроінтеграції та управління національною безпекою, Національна академія державного управління при Президентові України

ПРАВОВІ МЕХАНІЗМИ УПРАВЛІННЯ КРИТИЧНОЮ ІНФОРМАЦІЙНОЮ ІНФРАСТРУКТУРОЮ УКРАЇНИ

У статті проведено аналіз існуючих правових механізмів управління критичною інформаційною інфраструктурою в Україні. Зосереджено увагу на ролі правового регулювання суспільних відносин у сфері протидії загрозам порушення безпеки критичної інформаційної інфраструктури шляхом навмисного використання інформаційно-комунікаційних технологій проти об'єктів критичної інфраструктури. Досліджено основні складові правового забезпечення безпеки критичної інформаційної інфраструктури: національну та міжнародну. Визначено можливі інструменти для вдосконалення механізмів правового забезпечення безпеки критичної інформаційної інфраструктури, зокрема для національної складової правового забезпечення безпеки – розробка Порядку ідентифікації об'єктів критичної інформаційної інфраструктури та запровадження згідно з ним паспортизації об'єктів критичної інформаційної інфраструктури. Сформульовано проблеми вдосконалення міжнародної складової правового забезпечення безпеки та розвитку правового забезпечення безпеки критичної інформаційної інфраструктури в цілому.
Ключові слова: критична інформаційна інфраструктура, автоматизовані системи управління, кібербезпека, інцидент у кіберпросторі.

O. V. Melnichuk,
postgraduate of the Department of Globalistics European integration and national security management, National Academy for Public Administration under the President of Ukraine

LEGAL MECHANISMS OF CRITICAL INFORMATION INFRASTRUCTURE MANAGEMENT IN UKRAINE

The article analyzes the existing legal mechanisms for managing critical information infrastructure in Ukraine. Attention are focused on the role of legal regulation of public relations in the area of counteracting threats to the security of critical information infrastructure by intentional using information and communication technologies against objects of critical infrastructure. The main components of legal security of critical information infrastructure: national and international are investigating. The possible tools for improving the mechanisms of legal security of critical information infrastructure are identifying, in particular, for the national component of legal security, – the development of the Procedure for Identification of Critical Information Infrastructure objects and the introduction of critical information infrastructure objects under it. In addition, the problems of improving the international component of legal security and development of legal security of critical information infrastructure in general are formulating.
Key words: critical information infrastructure, automated control systems, cybersecurity, incident in cyberspace.

Постановка проблеми. Сучасні тенденції активного використання ресурсного потенціалу, його наявних матеріальних, технічних, трудових, інформаційних ресурсів спричинили феноменальну залежність людства від послуг, які надають різноманітні інфраструктурні галузі. Такий розвиток суспільства зумовлює необхідність формування механізмів публічного управління безпекою критичної інфраструктури. Суттєва роль у формуванні цієї умови належить правовому регулюванню суспільних відносин у сфері протидії загрозам порушення безпеки критичної інформаційної інфраструктури (КІІ) шляхом навмисного використання інформаційно-комунікаційних технологій проти об'єктів критичної інфраструктури.

Наразі забезпечення захисту та стабільного функціонування життєво важливих інфраструктурних об'єктів у складному зовнішньому та внутрішньому середовищах є найважливішою і обов'язковою складовою національної безпеки розвинутих держав.

У Стратегії національної безпеки України проблеми забезпечення інформаційної безпеки, кібербезпеки і безпеки інформаційних ресурсів та критичної інфраструктури визначаються пріоритетними до вирішення у сфері державної політики національної безпеки держави [1].

Зазначені чинники характеризують актуальність наукового дослідження механізмів публічного управління національною безпекою, та у межах цього напряму – правовому регулюванню критичної інформаційної інфраструктури, впровадження яких спроможне забезпечити адекватне реагування на виклики і загрози.

Аналіз останніх публікацій за проблематикою. Серед вітчизняних учених, які розглядали питання сутності управління безпекою та критичною інфраструктурою, можна назвати таких авторів: В.Абрамов, Д.Бірюков, О.Довгань, О.Іжак, Г.Ситник, А.Семенченко, О.Суходоля, В.Лядовська, С.Кондратов, С.Кулінська, В.Куйбіда, О.Насвіт. Крім того, дослідженню проблемних питань критичної інформаційної інфраструктури присвячені праці A.Wenger, V.Mauer & M.Cavelty, A. Di Giorgio, F.Liberati, G.Giannopoulos, R.Filippini & M.Schimmer, L.Muresan та ін.

Разом з тим кількість публікацій, де розглянуто сутність правових механізмів публічного управління КІІ у вітчизняній та зарубіжній літературі, обмежена, тому означена тема дослідження є актуальною.

Формулювання цілей (мети) статті. Метою статті є аналіз існуючих правових механізмів управління критичною інформаційною інфраструктурою в Україні та дослідження інструментів для їх вдосконалення.

Виклад основного матеріалу дослідження. Сьогодні в Україні законодавчий акт, де сформульовані основи державної політики, спрямованої на розв'язання проблеми сфери критичної інфраструктури, перебувають на стадії розробки.

Відповідно до завдань Річної національної програми співробітництва Україна–НАТО в 2015 р. розроблено Зелену книгу з питань захисту критичної інфраструктури в Україні. У ній розглянуто питання створення в Україні системи захисту критичної інфраструктури та сформульовано стратегічні цілі, принципи й завдання системи державної політики у сфері захисту критичної інфраструктури в Україні (далі – Зелена книга).

У Зеленій книзі наводиться таке визначення: "Критична інфраструктура України – це системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєді-

яльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки" [2].

Важливим компонентом критичної інфраструктури є її інформаційна складова – критична інформаційна інфраструктура, концепцію захисту якої уперше розроблену в США, згодом було прийнято в більшості розвинених держав світу. Галузь захисту КІІ в Україні перебуває на початковому етапі формування. Чинним законодавством визначено лише окремі об'єкти соціально-економічної сфери, на яких надзвичайні події можуть призвести до суспільно небезпечних наслідків, які не систематизовані. Крім того, немає визначеного понятійно-категорійного апарату в цій галузі.

Відсутність поняття "критична інформаційна інфраструктура" у законодавстві деяких держав можна пояснити тим, що інформаційна складова входить до обсягу поняття інфраструктури взагалі (тобто критичної інфраструктури) і не виокремлюється як певна ланка. Однак слід зазначити, що в тлумаченні цього терміна в різних державах простежується чітка аналогія [3].

З огляду на те, що термін "критична інформаційна інфраструктура" не має сталого тлумачення в різних державах, на нашу думку, критична інформаційна інфраструктура – це система управління інформацією критично важливих об'єктів та інформаційно-комунікаційні мережі, що забезпечують обороноздатність і безпеку державних і приватних установ, функціонування яких може вплинути на національну безпеку України.

У складі КІІ можна виділити інформаційну та мережеву складові. Інформаційне середовище КІІ являє собою систему управління інформацією критично важливих об'єктів, у тому числі обчислювальні та інформаційні ресурси, що утворюють автоматизовані системи управління (АСУ). При цьому обчислювальні ресурси утворюються сукупністю локальних обчислювальних мереж, інших засобів обчислювальної техніки і програмних засобів, що описують методи і способи автоматизації обробки інформації і можуть бути використані для організації розподілених обчислень (наприклад для дешифрування зашифрованого коду, моделювання складних соціальних і фізичних процесів).

Мережева складова КІІ утворюється із сукупності: телекомунікаційних пристроїв; ліній зв'язку та мережевого обладнання;

систем відкритих протоколів обміну інформацією між телекомунікаційними пристроями; глобальної системи цифрових адрес і цифрових ідентифікаторів; програмного забезпечення, що реалізує методи, алгоритми і процеси телекомунікаційного зв'язку на базі протоколів взаємодії локальних обчислювальних мереж і надає доступ до локальних обчислювальних мереж та інших засобів автоматизованої обробки інформації.

Регулювання взаємоз'єднання телекомунікаційних мереж здійснювалося відповідно до Закону України "Про телекомунікації" та Правил взаємоз'єднання телекомунікаційних мереж загального користування. Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ), своїм рішенням від 31 березня 2015 р. № 174 затвердила нову редакцію Правил взаємоз'єднання телекомунікаційних мереж загального користування, за якими введені новації та встановлено, що:

– реалізація проектної пропускної спроможності точки взаємоз'єднання може відбуватись поетапно, за результатами вимірювань фактичного навантаження відповідно до договору про взаємоз'єднання;

– можлива оплата ініціатором тільки частки запроектованої пропускної спроможності точки взаємоз'єднання в обсязі, достатньому для реалізації відповідного етапу;

– одноразова плата за доступ до телекомунікаційної мережі може бути замінена на розрахункову таксу за доступ, яка сплачується ініціатором одночасно з оплатою за послуги пропуску трафіку;

– заборонено блокувати в точках взаємоз'єднання весь вхідний трафік, за винятком трафіку, який надходить із порушенням порядку маршрутизації трафіку, трафік, пропуск якого не передбачений договором, або у разі наявності заборгованості за пропуск такого трафіку.

Крім того, встановлені технічні, організаційні та економічні умови взаємоз'єднання з телекомунікаційними мережами, що стосуються операторів телекомунікацій з істотною ринковою перевагою на ринках певних телекомунікаційних послуг та порядок визначення економічних умов взаємоз'єднання мереж [4].

Слід зазначити, що мережа Інтернет може розглядатися як технологічна надбудова над мережею електрозв'язку, що забез-

печує надання послуг передачі і обробки інформації (наприклад електронна пошта, телеконференції, передача файлів, доступ до обчислювальних і інформаційних систем у локальних обчислювальних мережах).

Надання послуг передачі й обробки інформації, інших інформаційних послуг у мережі Інтернет здійснюється в просторі цифрових адрес або доменних імен (різновиди цифрових ідентифікаторів об'єктів комунікації). Регулювання відносин у галузі розподілу цифрових ідентифікаторів і підтримання їх в актуальному стані здійснюється поза територією України. Відповідно використання цифрових ідентифікаторів об'єктів мережі Інтернет, а також забезпечення безпеки процесу їх використання здійснюється на основі міжнародного правового регулювання.

На нашу думку, основну загрозу безпеці АСУ критично важливих об'єктів інформаційної інфраструктури становлять цілеспрямовані дії на інформаційні системи та інформаційно-телекомунікаційні мережі програмно-технічними засобами. Тому правове забезпечення безпеки КІІ має включати дві основні складові – національну і міжнародну.

Національна складова правового забезпечення безпеки КІІ може бути утворена сукупністю принципів, правових інститутів і норм, закріплених національним законодавством, регулюючих публічні відносини в Україні у сфері протидії загрозам безпеки АСУ критично важливих об'єктів.

Суспільні відносини в галузі забезпечення безпеки АСУ критично важливих об'єктів інформаційної інфраструктури, що забезпечують взаємодію цих об'єктів, регулюються законодавством та регламентуючими документами. Українське законодавство щодо захисту об'єктів, які згідно зі світовою практикою відносять до критичної інфраструктури, є достатньо розгалуженим і включає численні нормативно-правові акти, які, проте, мають переважно відомчий характер.

Для забезпечення захисту найбільш важливих об'єктів КІІ необхідно насамперед ідентифікувати ці об'єкти. Чинне законодавство визначає такі категорії об'єктів, для яких встановлюються особливі умови забезпечення їх захисту та функціонування: підприємства, які мають стратегічне значення для економіки та безпе-

ки держави; особливо важливі об'єкти електроенергетики; особливо важливі об'єкти нафтогазової галузі; важливі державні об'єкти, у тому числі пункти управління органів державної влади та органів місцевого самоврядування; об'єкти можливих терористичних посягань; об'єкти, які підлягають охороні й обороні в умовах надзвичайних ситуацій і в особливий період; об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони за договорами; об'єкти підвищеної небезпеки (в тому числі Перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю громадян, майну, спорудам, навколишньому природному середовищу; об'єкти, які включені до Державного реєстру потенційно небезпечних об'єктів; радіаційні небезпечні об'єкти, для яких розробляється об'єктова проектна загроза; об'єкти, які віднесені до категорій із цивільного захисту; об'єкти, що належать суб'єктам господарювання, проектування яких здійснюється з урахуванням вимог інженерно-технічних заходів цивільного захисту; чергово-диспетчерська система екстреної допомоги населенню за єдиним безкоштовним телефонним номером виклику екстрених служб; аварійно-рятувальні служби; Національна система конфіденційного зв'язку; платіжні системи; нерухомі об'єкти культурної спадщини [2].

Деякі із зазначених категорій об'єктів, частково або повністю, можуть бути віднесеними до об'єктів критичної інфраструктури.

Специфіка забезпечення інформаційної безпеки знайшла відображення в законах України "Про основи національної безпеки України" [5], "Про концепцію національної програми інформатизації" [6], "Про національну програму інформатизації" [7], а також у Концепції розвитку сектору безпеки і оборони України [8], Стратегії національної безпеки України [1], Стратегії кібербезпеки України [9].

У Законі України "Про основи національної безпеки України" вперше дано офіційну оцінку значущості й системної сутності інформаційної безпеки як невід'ємної складової національної безпеки України.

Стратегією національної безпеки визначено актуальні загрози національній безпеці та зазначено пріоритети для забезпе-

чення інформаційної безпеки, кібербезпеки і безпеки інформаційних ресурсів та критичної інфраструктури.

Із зазначених пріоритетних напрямів наразі розроблено та затверджено лише Стратегію кібербезпеки України, якою визначено суб'єкти кібербезпеки та заходи забезпечення кібербезпеки України.

Принципи, на яких має базуватися забезпечення кібербезпеки України: верховенства права і поваги до прав та свобод людини і громадянина; забезпечення національних інтересів України; відкритості, доступності, стабільності та захищеності кіберпростору; державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту; пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам; пріоритетності запобіжних заходів; невідворотності покарання за вчинення кіберзлочинів; пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу; міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях; забезпечення демократичного цивільного контролю над утвореними відповідно до законів України військовими формуваннями і правоохоронними органами держави, що діють у сфері кібербезпеки [9].

З метою реалізації Стратегії кібербезпеки України Кабінетом Міністрів затверджено план заходів на 2017 р. із реалізації цієї Стратегії [10]. Цим планом передбачено подання в установленому порядку Кабінетові Міністрів України переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави з метою його затвердження.

Фактично це перший крок до законодавчого визначення об'єктів критичної інфраструктури. Водночас реалізація положень державної політики в галузі забезпечення безпеки КІІ вимагає подальшого розвитку правових принципів і норм, що регулюють відповідні суспільні відносини, тобто національної складової правового забезпечення безпеки КІІ. Україна має забезпечити формування загальнодержавної системи оцінки ризиків та загроз критичній

інфраструктурі, належну координацію органів державної влади та узгодження дій різних залучених осіб. Це також може потребувати визначення або створення відповідального державного органу та надання йому відповідних повноважень.

Вважаємо, що наступним кроком щодо забезпечення правового регулювання захисту критичної інфраструктури після законодавчого визначення основних термінів повинно були запровадження Порядку ідентифікації об'єктів критичної інформаційної інфраструктури.

Ідентифікація об'єктів КІІ в подальшому може бути здійснена шляхом запровадження паспортизації об'єктів критичної інформаційної інфраструктури. Такі паспорти мають містити загальні дані про об'єкт, дані щодо основних джерел небезпеки, дані про небезпечні природні умови, технологічні процеси та реагування на загрози тощо.

Міжнародна складова правового забезпечення безпеки КІІ передбачає регламентування сукупності принципів і норм, визначених міжнародними договорами і визнаних державою, що регулюють питання міжнародного співробітництва в цій сфері.

Підписання Угоди про асоціацію та подальша її ратифікація Україною і низкою країн-членів ЄС зумовлюють необхідність визначення першочергових кроків, які повинна зробити Україна у сфері захисту критичної інфраструктури з метою приведення своїх підходів у відповідність із підходами, які застосовуються в ЄС.

У 2004 р. ЄК оприлюднила офіційне повідомлення, в якому містився як огляд дій ЄК у цій сфері, так і пропозиції щодо додаткових заходів заради вдосконалення європейської системи запобігання, готовності та реагування стосовно терористичних атак, спрямованих проти елементів критичної інфраструктури ЄС. У повідомленні наголошується, що підхід до захисту критичної інфраструктури в усіх країнах ЄС повинен бути методологічно близьким. Забезпечити впровадження та реалізацію такого загального підходу мають Європейська програма захисту критичної інфраструктури (ЄПЗКІ) та Європейська інформаційна мережа попередження загроз критичній інфраструктурі [2].

Україна разом із державами-членами Ради Європи та іншими державами підписала Конвенцію про кіберзлочинність (яку ра-

тифіковано), що набрала чинності в 2006 р. Конвенція спрямована на зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними шляхом установлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для боротьби з кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого та надійного міжнародного співробітництва.

Крім того, планом заходів на 2017 р. із реалізації Стратегії кібербезпеки України передбачено Імплементація Директиви 2008/114/ЄК щодо захисту критичної інфраструктури, зокрема з питань кібербезпеки та кіберзахисту об'єктів критичної інфраструктури.

З урахуванням розвитку системи міжнародної інформаційної безпеки можна виділити такі основні групи міжнародних відносин, що вимагають нормативного правового регулювання в рамках правового забезпечення безпеки КІІ: визначення меж національної КІІ в глобальній інформаційно-комунікаційній інфраструктурі та закріплення ознак комп'ютерних інцидентів в АСУ об'єктів критичної інформаційної інфраструктури.

Необхідність визначення меж національної частини глобальної інформаційно-комунікаційної інфраструктури зумовлена неможливістю встановлення стійкої прив'язки цифрових ідентифікаторів об'єктів інформаційної інфраструктури до національної території. Однак державний суверенітет країни передбачає закріплення загальновизнаних міжнародних національних меж, у тому числі в просторі об'єктів інформаційної інфраструктури.

Відсутність загальновизнаних кордонів державного суверенітету держав в цьому просторі є суттєвою перешкодою для застосування норм міжнародного права до дій інших держав. Зокрема, це перешкоджає встановленню меж відповідальності держав за порушення безпеки КІІ та організації міжнародного співробітництва у сфері протидії комп'ютерній злочинності і т. ін.

Як відомо, виділення цифрових ідентифікаторів об'єктів мережі Інтернет національним провайдерам, а також підтримка в ак-

туальному стані відповідних інформаційних систем IP-адрес і доменних імен здійснюється американською некомерційною організацією ICANN і некомерційними організаціями RIP, зареєстрованими в різних державах світу. Дані організації не є суб'єктами міжнародного права і не володіють міжнародною правоздатністю, дієздатністю та не несуть юридичну відповідальність за шкоду, заподіяну її протиправними діями.

З цієї точки зору вони не можуть гарантувати стійкість виконання виділених функцій в умовах значної динаміки міжнародних відносин. Жодна держава або міжнародна організація не взяли на себе міжнародних правових зобов'язань щодо забезпечення стійкості і безпеки функціонування системи цифрових ідентифікаторів глобальної інформаційної інфраструктури. Усе це разом створює певні ризики порушення стійкості функціонування глобальної інформаційної інфраструктури.

Так, Група урядових експертів ООН вважає, що: державний суверенітет і повноваження держави давати правову оцінку фактам, розв'язувати ті чи інші правові питання є основою системи захисту національних інтересів, забезпечення національної безпеки, протидії загрозі зловмисного використання об'єктів КІІ проти прав і свобод громадян, інтересів суспільства та держави, порушення міжнародного миру й безпеки. Усі держави несуть головну відповідальність за забезпечення державної безпеки і безпеки своїх громадян, у тому числі в інформаційному середовищі [11].

Без встановлення просторових меж державного суверенітету в інформаційному середовищі взагалі і в мережі Інтернет зокрема, покладання такої відповідальності на держави не представляється можливим.

Про актуальності законодавчого закріплення ознак комп'ютерних інцидентів в АСУ об'єктів критичної інформаційної інфраструктури говорить широке застосування поняття "інцидент" в міжнародному праві. Так, поняття "міжнародний інцидент" зазвичай розкривається як невеликі, або обмежені дії чи аварія, результатом яких став широкий обмін думками між двома або більше національними державами.

Інцидент у кіберпросторі, зазвичай пов'язаний із порушенням функціонування складових кіберпростору – електронного

середовища збирання й автоматизованої обробки інформації, що визначають процеси здійснення даних операцій, а також інформаційних систем і систем автоматизованого управління.

Сутність загального визначення "міжнародного інциденту" у сфері КІІ буде визначатися, насамперед, характером міжнародних відносин між державами, порушеними "інцидентом". Ця подія може бути результатом непередбачених дій держави, у тому числі дій, що завдають шкоди інтересам публічних органів однієї чи більше держав, або, навпаки, бути одним із багатьох навмисних, але незначних провокацій, здійснюваних агентами однієї держави проти іншої держави. Наразі така політика проводиться Російською Федерацією.

З огляду на те, що міжнародні відносини в галузі інцидентів у сфері КІІ не регулюються міжнародними договорами, основним і, по суті, єдиним джерелом міжнародного права в даному випадку служить міжнародний звичай, однак, його застосування до сфери КІІ супроводжується значними складнощами.

Для України можливе запровадження позитивного досвіду інших держав у сфері безпеки КІІ, зокрема проблема забезпечення безпеки інформаційних технологій, була закріплена в міжнародному стандарті ISO/IEC 15408 "Загальні критерії оцінки безпеки інформаційних технологій".

Для обговорення на міжнародному рівні та вироблення стандартів у галузі управління та контролю інформаційними технологіями в 1998 р. засновано Інститут управління інформаційними технологіями (IT Governance Institute, ITGI). Ним видано стандарт "Цілі контролю для інформаційних та суміжних технологій" (CobiT®), яким надано хороші практики управління та контролю інформаційних технологій. Ці хороші практики являють собою сукупність дій, викладених у вигляді керованої та логічної структури. Передові практики, викладені в CobiT®, являють собою узгоджене бачення багатьох експертів, які брали участь у розробці цієї методології, є загальнодоступними для використання при розробці нормативно-правових актів України.

Висновки і перспективи подальших досліджень. Суспільні відносини в галузі забезпечення безпеки КІІ в Україні на даний час не врегульовані законодавством. Доцільним, на нашу думку, є

спрямування розвитку правового забезпечення безпеки КІІ в рамках реалізації положень Стратегій та Концепцій в цій сфері.

Запропоновані в статті інструменти вдосконалення механізмів правового забезпечення безпеки КІІ враховують розподіл правового забезпечення безпеки КІІ на національну та міжнародну складові. Зокрема, для національної складової правового забезпечення безпеки КІІ таким інструментом може бути Порядок ідентифікації об'єктів критичної інформаційної інфраструктури та запровадження, відповідно до нього, паспортизації об'єктів критичної інформаційної інфраструктури. Для міжнародної складової правового забезпечення безпеки КІІ – визначення меж національної КІІ в глобальній інформаційно-комунікаційній інфраструктурі та закріплення ознак комп'ютерних інцидентів в АСУ об'єктів КІІ, запровадження принципів і норм, що регулюють відповідні міжнародні стандарти.

У подальших дослідженнях, з урахуванням сформованого визначення КІІ та результатів цієї роботи, планується провести аналіз нормативно-правової бази розвинених держав світу та думки науковців щодо різних варіацій понятійно-категорійного апарату критичної інфраструктури та розглянути розподіл об'єктів критичної інфраструктури на сектори для наукової розробки методики віднесення певних об'єктів до критичної інформаційної інфраструктури.

Список використаних джерел

1. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. "Про Стратегію національної безпеки України" [Електронний ресурс] : Указ Президента України від 26 трав. 2015 р. № 287/2015. – Режим доступу: www.prezident.gov.ua.

2. Зелена книга з питань захисту критичної інфраструктури в Україні [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/public/ File/2015_table/ Green%20Paper%20on%20CIP_ua.pdf.

3. Лядовська В. М. Визначення критичної інформаційної інфраструктури та її захист: аналіз підходів / В. М. Лядовська, М. О. Рябий, С. О. Гнатюк // Зв'язок. – 2014. – № 4. – С. 3–7.

4. Про затвердження Правил взаємоз'єднання телекомунікаційних мереж загального користування [Електронний ресурс] :

Рішення Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 31 берез. 2015 р. № 174. – Режим доступу: http://www.nkrzi.gov.ua.

5. Про основи національної безпеки України [Електронний ресурс] : Закон України від 19 черв. 2003 р. № 964-IV. – Режим доступу: http://www.zakon.gov.ua.

6. Про концепцію національної програми інформатизації [Електронний ресурс] : Закон України від 04 лют. 1998 р. № 75/98-ВР. – Режим доступу: http://www.zakon.gov.ua.

7. Про національну програму інформатизації [Електронний ресурс] : Закон України від 04 лют. 1998 р. № 74/98-ВР. – Режим доступу: http://www.zakon.gov.ua.

8. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 р. "Про Концепцію розвитку сектору безпеки і оборони України" [Електронний ресурс] : Указ Президента України від 14 берез. 2016 р. № 92/2016. – Режим доступу: http://www.zakon.gov.ua.

9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. "Про Стратегію кібербезпеки України" [Електронний ресурс] : Указ Президента України від 15 берез. 2016 р. № 96/2016. – Режим доступу: www.prezident.gov.ua.

10. Про затвердження Плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України [Електронний ресурс] : розпорядження Кабінету Міністрів України від 10 берез. 2017 р. № 155-р. – Режим доступу: www.kmu.gov.ua.

11. Итоговое коммюнике саммита G20 от 16 декаб. 2015 г. [Электронный ресурс]. – Режим доступа: http://www.2000.ua/spectemy/sammit-g-20-v-antalii/itogovoe-kommyunike-sammita-g20-.htm.

12. Документ, перекладений на українську мову Київським відділенням ISACA® з дозволу ITGI® та відповідно до Англійського оригіналу CobiT® 4.1. – Б.м., б.р.

13. Конвенція про кіберзлочинність [Електронний ресурс] : ратифіковано Законом України від 07 верес. 2005 р. № 2824-IV (2824-15). – Режим доступу: http://www.zakon.gov.ua.

References

1. Pro rìšennâ Radi nacìonal′noï bezpeki ì oboroni Ukraïni vìd 6 travnâ 2015 roku "Pro Strategìû nacìonal′noï bezpeki Ukraïni" [Tekst]: Ukaz Prezidenta Ukraïni vìd 26 travnâ 2015 roku # 287/2015.

2. Zelena kniga z pitan′ zahistu kritičnoï ìnfrastrukturi v Ukraïnì [Elektronnij resurs]. – Režim dostupu: http://www.niss.gov.ua/public/File/2015_table/ Green%20Paper%20on%20CIP_ua.pdf. – Nazva z ekranu.

3. Lâdovs′ka V.M. Viznačennâ kritičnoï ìnformacìjnoï ìnfrastrukturi ta ïï zahist: analìz pìdhodìv / V.M. Lâdovs′ka, M.O. Râbij, S.O. Gnatûk // Zv'âzok. – 2014. – #4.-S. 3–7.

4. Pro zatverdžennâ Pravil vzaêmoz'êdnannâ telekomunìkacìjnih merež zagal′nogo koristuvannâ [Tekst]: Rìšennâ Nacìonal′noï komìsìï, ŝo zdìjsnûê deržavne regulûvannâ u sferì zv'âzku ta ìnformatizacìï vìd 31 bereznâ 2015 roku # 174.

5. Pro osnovi nacìonal′noï bezpeki Ukraïni [Tekst]: Zakon Ukraïni vìd 19 červnâ 2003 roku # 964-IV.

6. Pro koncepcìû nacìonal′noï programi ìnformatizacìï [Tekst]: Zakon Ukraïni vìd 04 lûtogo 1998 roku # 75/98-VR.

7. Pro nacìonal′nu programu ìnformatizacìï [Tekst]: Zakon Ukraïni vìd 04 lûtogo 1998 roku # 74/98-VR.

8. Pro rìšennâ Radi nacìonal′noï bezpeki ì oboroni Ukraïni vìd 4 bereznâ 2016 roku "Pro Koncepcìû rozvitku sektoru bezpeki ì oboroni Ukraïni" [Tekst]: Ukaz Prezidenta Ukraïni vìd 14 bereznâ 2016 roku # 92/2016.

9. Pro rìšennâ Radi nacìonal′noï bezpeki ì oboroni Ukraïni vìd 27 sìčnâ 2016 roku "Pro Strategìû kìberbezpeki Ukraïni" [Tekst]: Ukaz Prezidenta Ukraïni vìd 15 bereznâ 2016 roku # 96/2016.

10. Pro zatverdžennâ Planu zahodìv na 2017 rìk z realìzacìï Strategìï kìberbezpeki Ukraïni [Tekst]: rozporâdžennâ Kabìnetu Mìnìstrìv Ukraïni vìd 10 bereznâ 2017 roku # 155-r.

11. Itogovoe kommûnike sammita G20 vìd 16 grudnâ 2015 roku [Elektronnij resurs]. – Režim dostupu: http://www.2000.ua/spectemy/sammit-g-20-v-antalii/itogovoe-kommyunike-sammita-g20-.htm. – Nazva z ekranu.

12. Dokument perekladenij na Ukraïns′ku movu Kiïvs′kim vìddìlennâm ISACA® z dozvolu ITGI® ta u vìdpovìdnostì z Anglìjs′kim origìnalom CobiT® 4.1.

13. Konvencìâ pro kìberzločinnìst′ [Tekst]: ratifìkovano Zakonom Ukraïni vìd 07 veresnâ 2005 roku # 2824-IV (2824-15).

Summary

The article analyzes the existing legal mechanisms for managing critical information infrastructure in Ukraine. The instruments for their improvement are proposing in this article.

An important component of critical infrastructure is its information component – a critical information infrastructure. The sphere of protection of critical information infrastructure in Ukraine is at the initial stage of formation. The current legislation defines only certain objects of socio-economic sphere, in which extraordinary events can lead to socially dangerous consequences.

In view of the fact, that the term "critical information infrastructure" does not having a consistent interpretation in different countries, we propose our opinion. "Critical information infrastructure is a system of information management of critical facilities and information and communication networks that provide defense capabilities and security of public and private institutions, whose operation may flow to the national security of Ukraine" (KII).

In the KII we can identified information and network components. Information environment of KII is a system for information management of critical objects, including computing and information resources that form automated control systems (ACS). The network component of KII consists of a set of telecommunication devices, communication lines and network equipment, systems of open protocols for the exchange of information between telecommunication devices, global system of digital addresses and digital identifiers, software. The Internet network can be considered as a technological add-on over a telecommunication network that provides the provision of data transmission and processing services (e-mail, teleconferencing, file transfer, access to computing and information systems in local area networks).

The main threat to the safety of ACS of critical information infrastructure objects is targeted actions on information systems, informa-

tion and telecommunication networks by software and hardware. KII legal security include two main components – national and international. The national component may be forming by a set of principles, legal institutions and norms, which are enshrined in the national legislation regulating public relations in Ukraine in the area of counteracting the security threats of the ACS of critical objects.

In order to protect the most important objects of KII, it is necessary to identify these objects. The current legislation defines such categories of objects, for which special conditions for ensuring their protection and functioning are established. Some of them, in whole or in part, may be classifying as objects of critical infrastructure.

The specificity of providing information security was reflecting in such Ukraine laws like "On the Fundamentals of National Security of Ukraine", "On the Concept of the National Program of Informatization", "On the National Program of Informatization". As well as the Concept of Development of the Security and Defense Sector of Ukraine, the National Security Strategy of Ukraine, the Strategy of Cybersecurity Of Ukraine.

The National Security Strategy identifies actual threats to national security and sets priorities for information security, cyber security and security of information resources and critical infrastructure.

At the same time, the implementation of the state policy in the field of security of KII requires the further development of legal principles and norms governing the relevant social relations, that is, the national component of the legal security of KII. Ukraine should ensure the establishment of a nationwide system for assessing risks and threats to critical infrastructure, and after the legislative definition of the main terms, the implementation of the Identification of Critical Information Infrastructure objects. Identification of objects of critical information infrastructure can be accomplishing by introducing the certification of objects of critical information infrastructure. Such passports must contain general data about the facility, data on the main sources of danger, data on hazardous natural conditions, technological processes and response to threats.

The international component of the legal security of KII provides for the regulation of a set of principles and norms defined by interna-

tional treaties and recognized by the state, regulating issues of international cooperation in this area.

Ukraine has signed the Convention on Cybercrime together with the member states of the Council of Europe and other States. It is aiming at stopping actions against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as abusing such systems, networks and data by installing the criminal responsibility for such behavior, the provision of powers sufficient to combat criminal offenses, and the conclusion of agreements on rapid and reliable international cooperation.

In addition, the plan of measures for 2017 on implementation of the Cybersecurity Strategy of Ukraine provides for the implementation of Directive 2008/114/EC on the protection of critical infrastructure, in particular on cybersecurity and cyber defense of critical infrastructure objects.

Development of the system of international information security, the following main groups of international relations that require normative legal regulation within the framework of the legal security of KII: definition of the boundaries of the national KII in the global information and communication infrastructure and fixing signs of computer incidents in the control system of critical objects information infrastructure.

The absence of generally recognized borders of state sovereignty of States in this space is a significant obstacle to the application of international law to the actions of other states. In particular, this impedes the establishment of limits of responsibility of states for violating the security of the KII and organizing international cooperation in the field of countering computer crime.

The urgency of the legislative consolidation of signs of computer incidents in the automated control system of critical information infrastructure objects suggests the widespread use of the concept of "incident" in international law. An incident in cyberspace usually associated with a violation of the functioning of the components of cyberspace – an electronic collection environment and automated processing of information that determines the processes of the implementation of these operations, as well as information systems and automated control systems.

The essence of the general definition of the "international incident" in the field of KII will be determining, firstly, by the nature of international relations between states that are violating by the "incident". This event may be the result of unforeseen actions of the state, including actions that harm the interests of public bodies of one or more states, or, conversely, be one of many intentional but minor provocations carried out by agents of one state against another state.

Given that international relations in the field of incidents in the field of KII are not regulating by international treaties, the main and, in fact, the only source of international law in this case serves as an international custom, however, its application to the sphere of KII is accompanying by considerable difficulties.

For Ukraine, it is possible to introduce the positive experience of other states in the security of the KII. In particular, the problem of security of information technologies has been enshrined in the international standard ISO / IEC 15408 "General criteria for assessing the safety of information technology".