01.07.2013 р., відповідно до якого сучасні методи та інструменти (засоби) для сертифікації не є абсолютно адекватними для сертифікації КФС натепер через їх невідповідність вимогам сучасних КФС залежно від середовища КФС. Іншим питанням, на якому наголошується в рамковому документі Німеччини про КФС і у відповідному рамковому документі США, є питання прийняття та застосування уніфікованих стандартів КФС.

Для того, щоб дати універсальне повноцінне визначення КФС, варто проаналізувати аспекти створення КФС. Це було зроблено ґрунтовно в рамковому документі США Framework for Cyber-Physical Systems May 2016 Cyber Physical Systems Public Working Group.

Особливого значення набувають дослідження різних учених та наукових закладів у питанні аспекту вартості довіри (trustworthiness) КФС, який включає в себе конфіденційність, надійність, стійкість, безпеку.

Відбуваються періодичні Workshop на рівні ЄС за участю вчених, експертів, представників влади, бізнесу, які мають результатом важливі напрацювання та практичні висновки в сфері КФС.

Натепер численні зусилля різних міжнародних організацій в сфері створення стандартів кіберфізичних систем, зокрема ISO, ITU, Industrial Internet Consortium, IoT-A та ін., досі не забезпечили повну сумісність цих стандартів щодо різнорідних КФС.

Список використаних джерел:

1. German Agenda Cyber physical systems 2010, URL: www.acatech.de.
2. Framework for Cyber-Physical Systems Release 1.0 May 2016 Cyber Physical Systems Public Working Group, URL: www.nist.gov.
3. The UK Cyber Security Strategy 2011, URL: www.cabinetoffice.gov.uk.
4. Guidance “The key principles of vehicle cyber security for connected and automated vehicles” published 6 August 2017, URL: www.gov.uk..
5. Указ Президента України від 15.03.2016 року «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».
6. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р.

ЧОРНОУС А. Г.,
аспірант кафедри
адміністративного права
(Київський національний університет імені Тараса Шевченка)

УДК 342.951:351.82

ПЕРСПЕКТИВИ ВДОСКОНАЛЕННЯ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

У статті розглянуто проблемні питання сучасної інформаційної інфраструктури України. Встановлені та виокремлені наявні законодавчі прогалини та запропоновано дієві шляхи вирішення останніх, а також наведено власне визначення поняття критичної інфраструктури України, спираючись на об’єктивні фактори, що мають вплив на сучасну інформаційну інфраструктуру держави у цілому.

Ключові слова: *інформаційна інфраструктура, критична інформаційна інфраструктура, фактори впливу, об’єкти інфраструктури, суб’єкти відповідальності, чинники інформаційної інфраструктури.*

В статье рассмотрены проблемные вопросы современной информационной инфраструктуры Украины. Определены и выделены существующие законодательные пробелы и предложены действенные пути их решения, а также приведено собственное определение понятия критической инфраструктуры Украины, опираясь на объективные факторы, оказывающие влияние на современную информационную инфраструктуру государства в целом.

Ключевые слова: *информационная инфраструктура, критическая информационная инфраструктура, факторы влияния, объекты инфраструктуры, субъекты ответственности, факторы информационной инфраструктуры.*

The article examines the issues of the existing information infrastructure of Ukraine. The current legislative gaps identified and singled out, and the effective ways of filling thereof were proposed. Moreover, the author introduced his own definition of critical infrastructure of Ukraine, based on objective factors have influence on the existing state information infrastructure as a whole.

Key words: *information infrastructure, critical information infrastructure, factors of influence, infrastructure objects, subjects of responsibility, factors of information infrastructure.*

Вступ. Актуальність цієї теми зумовлена тим, що за останні кілька років розвитку соціально-економічного й політичного устрою нашої держави відбулося чимало змін. Водночас стагнаційні процеси, що спостерігаються й дотепер, не дають змоги говорити про позитивні результати, яких Україна мала досягти до цього часу. Дискусії, що тривають, і трансформаційні процеси на українській політичній арені стали приводом до міжусобиць як органів влади нашої держави, так і зовнішніх партнерів, довіра яких з кожним неправильно прийнятим рішенням стрімко згасає. Запровадження недієвих реформ у сфері забезпечення національної інформаційної інфраструктури України протягом кількох останніх років свідчить про їх недосконаліть та певну лояльність органів влади до цього питання. Програми національного забезпечення інформаційної інфраструктури як дієвого механізму захисту інформаційних ресурсів на національному рівні як такої немає. Є лише нариси того, що має бути. Враховуючи зазначене, варто детально проаналізувати ситуацію, що склалася нині, виявити законодавчі прогалини та наявні проблеми практичної реалізації реформ у сфері забезпечення національної інформаційної інфраструктури.

Метою запропонованого наукового дослідження є визначення наявних в України перспектив подальшого розвитку національної інформаційної інфраструктури з огляду на проаналізований автором та наведений у цій статті досвід зарубіжних країн. Окрім цього, під час написання статті автором досліджені наукові праці Д.С. Бірюкова, Н.В. Березняк, О.В. Бондаренко, С.О. Гнятюк, С.В. Гончар, Т.К. Кваші, В.М. Лядовської, Г.В. Новіцької, а також інших науковців, які вивчали методологічні та практичні питання становлення та розвитку національної інформаційної та критичної інфраструктури України.

Постановка завдання. Основним завданням цієї статті є системний аналіз наявних факторів, що впливають або можуть вплинути на подальший розвиток національної інформаційної інфраструктури України.

Виклад основного матеріалу дослідження. Для України, як країни з перехідною економікою, надзвичайно важливим чинником завершення ринкових перетворень і забезпечення стійкого розвитку є зміцнення всіх типів інфраструктури сучасного суспільства. Головним чинником такого завершення є виокремлення першочергових завдань та їх практична реалізація. Особливе місце в цій сфері належить саме національній інформаційній інфраструктурі (далі – НІІ), яка, насамперед, покликана забезпечити створення єдиного інформаційного простору України як цілісної держави, поглиблення процесів інтеграції та послідовного входження України в глобальну інформаційну інфраструктуру. Відтак, роз-

виток інформаційної інфраструктури України багато в чому визначається загальним рівнем розвитку вітчизняних інформаційних технологій та інформатизації.

Детальний аналіз сучасного стану інформаційної інфраструктури національного рівня дає змогу констатувати, що головними завданнями державної політики у сфері інформаційно-комунікаційних технологій є такі:

– створення сучасних інформаційних технологій на національному рівні та розвиток виробництва технічних засобів для їх реалізації;

– розвиток вітчизняного виробництва сучасних інформаційних систем та технічних засобів телекомунікацій;

сприяння впровадженню інформаційних технологій, що використовуються в зарубіжних інформаційних системах національного і транснаціонального масштабів, у діяльність органів публічної адміністрації;

– підготовка кваліфікованих кадрів для роботи із сучасними інформаційними системами та технічними засобами.

Досліджуючи питання інформаційної структури, варто також зазначити, що вітчизняна інформаційна індустрія має розвиватися саме з урахуванням світових досягнень у галузі інформаційних технологій та засобів телекомунікаційного обміну. Як підтверджує зарубіжний досвід, лише такий вектор розвитку інформаційної індустрії дозволить Україні вийти на світовий рівень технічного розвитку. Створення ефективного світового інформаційного простору потребує активного використання систем та мереж обміну інформацією, проведення широкомасштабної комп'ютеризації процесів оброблення інформації у всіх сферах діяльності, зокрема діяльності органів публічної адміністрації, та використання досвіду передових інформаційних технологій різних країн світу.

Важливим чинником на шляху формування та ефективного функціонування інформаційної інфраструктури будь-якої країни є конструктивна державна інформаційна політика, яка має стимулювати розвиток засобів інформаційної взаємодії та інформаційного простору країни в цілому.

Водночас варто пам'ятати, що розвиток інформаційної інфраструктури неможливий без належної законодавчої підтримки. Відтак, наявне нормативно-правове регулювання інформаційної сфери України однозначно потребує додаткового вдосконалення та суттєвої адаптації до світових та міжнародних стандартів. Варто відзначити, що в різних діючих законодавчих актах зафіксовані прагнення держави до інтегрування у світовий та європейський інформаційні простори. Йдеться про Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [1], Розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» [2], Концепцію розвитку Державної інформаційної системи реєстраційного обліку фізичних осіб та їх документування, затверджену Розпорядженням Кабінету Міністрів України від 17 червня 2009 року № 711-р [3], та Концепцію Національної інформаційної політики України [4].

Що стосується доктринального вивчення можливостей вдосконалення та розвитку національної інформаційної інфраструктури, то, як зазначає О.В. Бондаренко, інформаційна інфраструктура являє собою сукупність таких елементів:

– електронних інформаційних ресурсів;

– автоматизованих інформаційних систем (далі – АІС) як засобів для збору, оброблення, збереження та розповсюдження отриманої інформації;

– засобів доставки електронних інформаційних ресурсів безпосередньо до користувачів із сталим забезпеченням функціонування інформаційного обміну (лінії та засоби зв'язку, мережі телекомунікацій);

– відповідних існуючих складників в інститутах (обчислювальні центри, оператори та провайдери, інформаційні агенції тощо);

– системи забезпечення національної інформаційної інфраструктури, що включає в себе засоби економічного й нормативно-правового забезпечення, а також певні стандарти, документацію та інструктивні матеріали;

– системи підготовки кадрів і людини як активного фактора впливу на інформаційний простір [5, с. 261].

У зазначеному переліку загальноприйнятих складників інформаційної інфраструктури доцільно виокремити головні компоненти, які безпосередньо визначають рівень формування та розвитку національної інформаційної інфраструктури та, відштовхуючись від цього, запропонувати дієві шляхи удосконалення правового регулювання механізму забезпечення національної інформаційної інфраструктури в Україні.

В умовах стрімкого розвитку інформаційних технологій, насамперед, варто виділити питання, що стосуються захисту автоматизованих систем та систем телекомунікацій, враховуючи те, що саме ці дві категорії є ключовим фактором функціонування та розвитку інформаційної інфраструктури. Вектор дій щодо підвищення рівня захищеності національних автоматизованих систем та систем телекомунікацій має бути спрямований не лише на забезпечення внутрішньо-національних баз даних, а й на глобальний, світовий рівень забезпечення безпеки інформаційної інфраструктури. Різні міжнародні дослідницькі агенції під час проведення ранжирування електронної готовності (e-readiness, з англ. – електронна готовність) країн світу на перше місце ставлять саме рівень зв'язності та розвитку технологічної інфраструктури (Connectivity and technology infrastructure, з англ. – підключення та технологічна інфраструктура) [5, с. 261].

Таким чином, для формування чіткого уявлення про те, які заходи потрібно провести, аби забезпечити достатній рівень захищеності національної інформаційної інфраструктури, варто провести аналіз діяльності й дієвості аналогічних зарубіжних систем. Очевидно, подібне дослідження дасть змогу підвищити рівень національного захисту такої важливої категорії як інформаційна інфраструктура. Водночас створення національної інформаційної інфраструктури, яка б відповідала європейським та світовим стандартам, є досить тривалим та трудомістким процесом, який, своєю чергою, потребує значних фінансових та трудових ресурсів та має здійснюватися завдяки узгодженим рішенням та діям органів державної влади, організацій та посадових осіб щодо організації, формування, захисту всіх інформаційних ресурсів та їх використання в інтересах держави і суспільства. При цьому ключовим орієнтиром зовнішньої інформаційної політики України виступатиме забезпечення національного інформаційного суверенітету та інформаційної безпеки.

Беручи до уваги досвід зарубіжних країн, особливу увагу варто звернути на програму розвитку національної інформаційної інфраструктури Сполучених Штатів Америки (далі – США). Як зазначає Н.В. Березняк у співавторстві з Т.К. Квашею Т. К. та Г.В. Новіцькою, державна політика США в галузі побудови інформаційної інфраструктури спрямована на значну підтримку цього процесу за такими чотирма напрямами:

1) формування економіки, що ґрунтується на знаннях;

2) розвиток електронної торгівлі;

3) підвищення ефективності системи освіти і перепідготовки кадрів;

4) удосконалення діяльності органів державної влади, відповідальних за розвиток цієї сфери.

Досвід США щодо інноваційного розвитку країни переконує, що інвестування в розвиток інформаційної інфраструктури є важливим чинником економічного зростання [6, с. 14]. Одним із головних напрямів державних витрат американський уряд вбачає саме розвиток інформаційної інфраструктури шляхом розширення мережі Інтернет як платформи для економічних інновацій і науково-технічного прогресу. Державним органам США заборонено конкурувати з приватним сектором у сфері надання будь-яких інформаційних послуг. Це завдяки подібній державній політиці сфера інформаційних послуг США постійно перебуває в умовах відкритої конкуренції, що постійно стимулює розвиток інформаційних відносин.

Також варто зазначити, що згідно з програмою «Національна інформаційна інфраструктура: план дій» 1993 року інформаційна інфраструктура створюється в основному приватним сектором та складається з трьох частин:

– перша – ініціатива Information Super Highway (з англ. – інформаційна супер-магістраль) – націлена на об'єднання університетів, шкіл, громадських організацій і ділових центрів, бібліотек, лікарень та міністерств;

– друга – програма High Performance Computing and Networking (з англ. – висока продуктивність обчислень та мереж) – зосереджена на розробленні напрямів застосування у таких галузях, як медицина, управління і контроль руху транспорту, освіта;

– третя – це програма модернізації діяльності державної адміністрації і державного доступу до інформації [6, с. 19].

Отже, американська програма забезпечення національної інформаційної інфраструктури не обмежується лише інвестиціями у фізичну інфраструктуру, але й передбачає розроблення нових технологій на більш високих рівнях. Таким чином, розвиток національної й глобальної інформаційної інфраструктури в США визначений пріоритетом державної політики. Вважаємо, що саме американський досвід є прийнятним для України в аспекті запозичення базових принципів становлення і функціонування інформаційної інфраструктури на базі інформаційно-комунікаційних технологій та державного регулювання розвитку інноваційної сфери з обов'язковим урахуванням пріоритетних напрямів економічного і науково-технічного розвитку держави.

Варто також зазначити, що в низці розвинених країн світу існує таке поняття як «критичний рівень забезпечення інформаційної інфраструктури». Зазначене поняття слугує класифікатором обов'язкового рівня захисту інформаційної інфраструктури, зменшення якісних показників якого може призвести до незворотних негативних наслідків та значних соціально-економічних потрясінь, здатних підірвати стабільність у суспільстві і призвести до реалізації загроз національній безпеці країни. Натепер важливим елементом критичної інфраструктури є її інформаційний складник, тобто критична інформаційна інфраструктура, концепцію захисту якої вперше розроблено в Сполучених Штатах Америки, а згодом запроваджено в більшості розвинених країн світу [7, с. 3].

У сучасній науковій літературі та законодавстві не існує єдиного визначення поняття критичного рівня забезпечення інформаційної інфраструктури. Насамперед, це пояснюється тим, що національні потреби й проблеми держав істотно відрізняються між собою залежно від рівня розвитку країни та інших специфічних чинників. Власне, саме ці чинники і є основною перешкодою на шляху до стандартизації (на міжнародному рівні) у галузі захисту критичної інфраструктури. Проте у наявному розмаїтті дефініцій простежується спільна риса критичної інфраструктури різних держав світу: її ключове значення для безпеки громадян, суспільства й держави. Вважається, що відсутність поняття «критична інформаційна інфраструктура» у законодавстві деяких держав можна пояснити тим, що інформаційний складник уже входить до обсягу поняття інфраструктури (тобто критичної інфраструктури) і не виділяється в окрему категорію.

З метою формування чіткого уявлення про те, що закладено в зміст поняття критичної інформаційної інфраструктури загалом та критичної інформаційної інфраструктури України зокрема, варто проаналізувати досвід деяких розвинених держав. Так, згаданий термін можна розглядати з таких точок зору:

сукупність інфраструктури об'єктів, які безперебійно та цілісно функціонують з метою запобігання загрозам, наявним ризикам, а також для нейтралізації їх негативних наслідків і швидкого оновлення інфраструктури в разі порушення їх роботи, а також для інших випадків, що виникають або можуть виникати стосовно об'єктів критичної інфраструктури, що порушують її належне функціонування (законодавство Польщі) [8];

– концепція, яка стосується готовності та реагування на ймовірні виникнення серйозних інцидентів, пов'язаних з критичною інфраструктурою окремого регіону або нації (С.Ф. Гончар) [9];

– захист інформаційних чи комунікаційних послуг, надійність, стійкість і доступність яких мають важливе значення для функціонування сучасної (національної) економіки, безпеки та інших важливих соціальних цінностей (законодавство США) [10];

– можливість підготовки до захисту, реагування і відновлення критичної інфраструктури в разі виникнення перебоїв або їх усунення (законодавство ЄС) [11].

Таким чином, з огляду на вищезазначене, критичний рівень інформаційної інфраструктури України варто розглядати як один з етапів забезпечення концепції національної інформаційної інфраструктури.

Відтак, критичним рівнем інформаційної інфраструктури України є такий, за якого в наявності нормально функціонуючі інформаційні об'єкти, а порушення чи припинення нормального функціонування яких призводить до втрати управління ними, і, як наслідок, до руйнування інфраструктури, незворотних негативних змін або руйнування економіки країни в цілому, або ж до тривалого та значного погіршення інформаційної захищеності життя населення, яке проживає на цих територіях.

Вважаємо, що саме таку норму-дефініцію варто передбачити в наявній нині національній Концепції створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів [12]. Подібна законодавча новела уможливить подальше запровадження дієвої системи захисту інформаційної інфраструктури України із визначенням її критичного (граничнодопустимого) рівня як на національному рівні, так і на рівні окремих організацій, що, своєю чергою, мінімізує, а подекуди й унеможливить злочинні посягання на національну інформаційну безпеку нашої держави.

Варто також зазначити, що в національній системі захисту інформаційної інфраструктури України натепер уже спостерігаються певні позитивні зміни. Так, 9 травня 2018 року набирає чинності Закон України «Про основні засади забезпечення кібербезпеки України» (далі – Закон), прийнятий 5 жовтня 2017 року. Суть цього законопроекту полягає в узаконенні значного спектра термінології з префіксом «кібер» (-простір, -злочин, -атака, -розвідка, -шпіонаж, -тероризм тощо). Після прийняття зазначеного законопроекту порушення, здійснені у віртуальному просторі (наприклад, незаконний переказ чи зняття коштів з чужого карткового чи банківського рахунку), будуть розцінюватися як кіберзлочини, а їх кваліфікація та відповідальність за них будуть аналогічні до злочинів, пов'язаних з більш стандартними складами злочинів (наприклад, шахрайство або фінансування тероризму).

Згідно з інформацією, зазначеною в пояснювальній записці до вказаного законопроекту, останнім визначаються основні об'єкти кіберзахисту, які у своїй сукупності складатимуть критичну інформаційну інфраструктуру країни та, як наслідок, підлягатимуть наступному внесенню до спеціального державного реєстру. Визначається також, що Президент має здійснювати загальне керівництво у сфері кібербезпеки України, визначати головну стратегію кібербезпеки, основні пріоритети та напрями її подальшого забезпечення. Рада Національної безпеки і оборони України має проводити моніторинг, координацію і контроль за діяльністю суб'єктів сектору безпеки й оборони, які, своєю чергою, забезпечують кібербезпеку, а також з цією метою має створити Національний координаційний центр кібербезпеки України.

Крім того, варто зазначити, що забезпечення кібербезпеки країни покладено також на Збройні сили України, Національний банк України, підприємства різних форм власності та громадян, які працюють у сфері державних інформаційних ресурсів, інформаційних електронних послуг, а також на підприємства, які відносяться до об'єктів критичної інфраструктури. Спільним обов'язком згаданих суб'єктів має бути забезпечення кібербезпеки шляхом всебічного недопущення використання кіберпростору у терористичних, військових чи інших незаконних цілях.

У зазначеному проекті Закону передбачено поняття «критичної інформаційної інфраструктури», згідно з яким критична інформаційна інфраструктура – це певна сукупність визначених об'єктів критичної інформаційної інфраструктури (пункт 15 статті 1 Закону). Вважаємо, що запропонована вище норма-дефініція є кращою за наявну, адже таке визначення є більш доступним та прийнятним. У Законі також визначено, що об'єкт критичної інформаційної інфраструктури – це технологічна (чи комунікаційна) система наявного об'єкта критичної інфраструктури.

Висновки. Вищезазначене свідчить про те, що рівень національного законодавства в частині забезпечення безпеки національної інформаційної інфраструктури нині є досить низьким, адже ми перебуваємо ще на етапі законодавчого визначення базових понять та їх структурних елементів. Разом з тим, збільшення кількості наукових робіт, присвячених дослідженню цього питання, безумовно, свідчить про очевидно виражену зацікавленість наукових кіл та суспільства у запровадженні зарубіжного досвіду з питань формування, впровадження і забезпечення національної інформаційної інфраструктури.

Список використаних джерел:

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України. Офіційне видання від 09 січня 2007 року./ Відомості Верховної Ради України (ВВР), 2007. № 12. Ст. 102. URL: http://zakon5.rada.gov.ua/laws/show/537-16.

2. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15 травня 2013 року. № 386-р. URL: http://zakon5.rada.gov.ua/laws/show/386-2013-р.

3. Про схвалення Концепції розвитку Державної інформаційної системи реєстраційного обліку фізичних осіб та їх документування: Розпорядження Кабінету Міністрів України від 17 червня 2009 року № 711-р. URL: http://zakon3.rada.gov.ua/laws/show/711-2009-р.

4. Про Концепцію національної інформаційної політики: Постанова Верховної Ради України від 03 квітня 2003 року. URL: http://zakon3.rada.gov.ua/laws/show/687-15.

5. Бондаренко О.В. Стан і перспективи розвитку національної інформаційної інфраструктури. Науковий вісник НЛТУ України. 2013. Вип. 23.18. С. 260–264.

6. Березняк Н.В. Досвід розбудови інформаційної інфраструктури інноваційної сфери у США / Березняк Н.В., Кваша Т.К., Новіцька Г.В. «Науково-технічна інформація». № 2. 2012. С. 14–19.

7. Гнатюк С.О. Визначення критичної інформаційної інфраструктури та її захисту: аналіз підходів / Гнатюк С.О., Рябий М.О., Лядовська В.М. Державний університет телекомунікацій. К.: «Зв'язок». С. 3–7.

8. Бірюков Д.С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Бірюков Д.С., Кондратов С.І. К. НІСД, 2012. 96 с.

9. Гончар С.Ф. Забезпечення інформаційної безпеки об'єктів критичної інфраструктури України / Гончар С.Ф., Леоненко Г.П., Юдін О.Ю. Information Technology and Security. 2013. Вип. 1(3). С. 44.

10. A Critical Information Infrastructure Protection Approach to Multinational Cyber Security Events. URL: http://www.enisa.europa.eu/activities/cert/events/files/ENISA_best_practices_for_ciip_Willke.pdf.

11. Green paper on a European programme for critical infrastructure protection (COM/2005/576 final). URL: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf.

12. Про схвалення Концепції створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів: Розпорядження Кабінету Міністрів України від 05 вересня 2012 року № 634-р. URL: http://zakon2.rada.gov.ua/laws/show/634-2012-р.