СТРАТЕГІЧНЕ УПРАВЛІННЯ РОЗВИТКОМ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

STRATEGIC MANAGEMENT DEVELOPMENT OF CYBERNETIC DEFENCE OF CRITICAL INFORMATIVE INFRASTRUCTURE OF UKRAINE

УДК 007.51 (477)

Жиляєв І.Б.
д. екон. наук, старшій науковий співробітник
Інститут підготовки кадрів державної служби зайнятості України
Семенченко А.І.
д. наук з держ. упр., професор
Інститут підготовки кадрів державної служби зайнятості України
Мялковський Д.В.
здобувач
Інститут підготовки кадрів державної служби зайнятості України
Станіславський Т.В.
здобувач
Інститут підготовки кадрів державної служби зайнятості України

У статті розглянуто організаційно-правові механізми стратегічного управління розвитком кіберзахисту критичної інформаційної інфраструктури України, актуальність дослідження яких обумовлена динамікою зростання кількості та рівня кіберзагроз, невідповідністю державної політики та державного управління вимогам надійного та оперативного реагування на ці загрози, розривом та неузгодженістю між сукупністю концептуальних документів та їх реальною імплементацією, відсутністю дієвої координації та взаємодії складників національної системи кібербезпеки щодо кіберзахисту критичної інформаційної інфраструктури.
Ключові слова: *кібербезпека, кіберзахист, критична інформаційна інфраструктура, стратегічне управління.*

В статье рассмотрены организационно-правовые механизмы стратегического управления развитием киберзащиты критической информационной инфраструктуры Украины, актуальность исследования которых обусловлена динамикой увеличения количества и уровня киберугроз, несоответствием государственной политики и государственного управления требованиям надежного и оперативного реагирования на эти угрозы, разрывом и несогласованностью между совокупностью концептуальных документов и их реальным внедрением, отсутствием действенной координации и взаимодействия составляющих национальной системы кибербезопасности и киберзащиты объектов критической информационной инфраструктуры.
Ключевые слова: *кибербезопасность, киберзащита, критическая информационная инфраструктура.*

The article deals with the organizational and legal mechanisms of strategic management of the development of the cybernetic defence of critical informative infrastructure in Ukraine, the relevance of which is due to the dynamics of quantitative and cyber threats growth, the incompatibility of state policy and public administration with the requirements for reliable and prompt response to these threats, the gap and inconsistency between the set of conceptual documents and their real implementation, lack of effective coordination and interaction of the components of the national cyber security system.
Key words: *cybersecurity, cybernetic defence, critical informative infrastruktura, strategic management.*

Постановка проблеми у загальному вигляді. Сучасні загальносвітові тренди з розвитку базуються на широкому, повсюдному та динамічному впровадженні й застосуванні інформаційно-комунікативних технологій (ІКТ). Однак вони одночасно актуалізують проблему інформаційної безпеки та кіберзахисту (особливо для об'єктів критичної інформаційної інфраструктури), обумовлену збільшенням кількості та підвищенням складності кіберінциндентів, що посилюють ризики природного та техногенного характеру, агресією Російської Федерації, насамперед в цій сфері [1]. З метою успішного розв'язання цієї проблеми з урахуванням міжнародного досвіду та законодавства, особливостей національного розвитку розробляється публічна політика та здійснюється публічне управління у сфері кібербезпеки [2; 3].

В Україні останнім часом прийнято низку концептуальних нормативно-правових актів [1; 4; 5]. Однак актуальною залишається проблема їх реального впровадження та взаємоузгодженості, прискорення імплементації сукупності міжнародних документів, насамперед ЄС та НАТО (кількість яких стрімко збільшується[1]), координованості дій та взаємодії основних об'єктів та суб'єктів кібербезпеки та кіберзахисту, відповідності їх вимогам надійного та оперативного реагування на комплекс загроз у цій сфері[2]. Окрім того, формування національної системи кібербезпеки здійснюється вкрай повільно, що не відповідає сучасній військово-політичній обстановці та соціально-економічному стану України, загрози збільшуються, в тому числі через недосконалість публічного управління та адміністрування, особливо на стратегічному рівні.

При цьому, як показує практика провідних країн світу, в умовах суттєвої невизначеності та непередбачуваності функціонування систем публічного управління та адміністрування переваги мають, насамперед, методи стратегічного планування та управління.

[1] Всього на сайті документів європейського права EUR-Lex (станом на 30.05.2018 р.) розміщено 405 актів, які врегульовували питання кібербезпеки, зокрема, лише за січень-травень 2018 року – 89 нових актів (у 2017 році – 138 актів). http://eur-lex.europa.eu/search.html?qid=1527708295257&text=cybersecurity&scope=EURLEX&type=quick&lang=en.

[2] Недарма у схваленому 7 лютого 2018 року Палатою представників Конгресу США та внесеного до Сенату проекті «Закону про співпрацю з Україною з питань кібербезпеки» (Ukraine Cybersecurity Cooperation Act), передбачено допомогу Україні в удосконаленні стратегії кібербезпеки, зокрема, щодо посилення захисту комп'ютерних мереж органів державної влади, зменшення залежності України від російських інформаційних та комунікаційних технологій, сприяння участі України в програмах обміну інформацією. Див.: S. 2455: Ukraine Cybersecurity Cooperation Act of 2018 https://www.congress.gov/bill/115th-congress/senate-bill/2455/text.

Аналіз останніх досліджень і публікацій. Нормативно-правові аспекти системи кібернетичної безпеки розглядалися в працях К. Александера (Alexander K.), Дж. Ліпмана (Liepman, J), В. Мазурова, Р. Олдрича (Aldrich R.), Є. Старостиної, М. Шмітта (Schmitt M.), А. Щетилова. Серед вітчизняних науковців необхідно відмітити праці В. Бурячка, Р. Грищука, Ю. Даника, О. Довганя, Д. Дубова, В. Петрова, Т. Тропініної та ін.

Але в Україні досліджень з питань кібербезпеки взагалі та зокрема щодо стратегічного управління розвитком національної системи кібербезпеки недостатньо.

Виділення невирішених раніше частин загальної проблеми. У загальній проблемі забезпечення кіберзахисту об'єктів критичної інфраструктури особливо актуальною є проблема розробки та впровадження організаційно-правових механізмів стратегічного управління розвитком кіберзахисту критичної інформаційної інфраструктури України з урахуванням міжнародного досвіду в цій сфері, насамперед країн НАТО та ЄС.

Метою статті є аналіз стану стратегічного управління розвитком кіберзахисту критичної інформаційної інфраструктури України, систематизація сукупності законодавчих актів з розвитку кібербезпеки та кіберзахисту, розробка методологічних підходів та пріоритетних напрямів щодо удосконалення стратегічного управління розвитком з урахуванням досвіду та вимог ЄС.

Виклад основного матеріалу. Відповідність системи кібербезпеки сучасним викликам та загрозам, її збалансованість на основі впровадження принципів мінімально необхідного регулювання (пропорційності та адекватності заходів кібербезпеки), максимально можливого застосування норм національного та міжнародного права, невтручання у приватне життя і захисту персональних даних, еквівалентності вимог до забезпечення кібербезпеки об'єктів критичної інфраструктури та інших є головним завданням публічної політики у сфері кібербезпеки та кіберзахисту.

У ст. 3 Закону України «Про основні засади забезпечення кібербезпеки» [5] визначена загальна ієрархія законодавчих актів, які формалізують публічну політику в цій сфері, а саме: «Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України», які за рівнем спеціалізації було запропоновано класифікувати [6] на акти загального спрямування та спеціалізовані акти щодо кібербезпеки. Але такий підхід потребує подальшої конкретизації та деталізації в залежності від рівня державно-управлінського впливу, в основу якого, наприклад, могла би бути покладена ієрархія структур функціонування державної системи захисту критичної інфраструктури: загальнодержавний, регіональний, галузевий, місцевий та об'єктовий рівні [1].

Закон України «Про основні засади забезпечення кібербезпеки» за своїм змістом та сутністю є концепцією розвитку сфери кібербезпеки та кіберзахисту. Він визначає категорійно-понятійний апарат, об'єкти, суб'єкти та принципи кібербезпеки, об'єкти кіберзахисту, структуру Національної системи кібербезпеки та завдання її основних складників, механізми державно-приватного та державно-суспільного партнерства тощо. За логікою формування системи стратегічних документів цей закон як концепція мав би передувати іншому законодавчому акту, а саме Стратегії кібербезпеки України [4]. Прийнята роком раніше Стратегія кібербезпеки України значною мірою дублює вищевказаний закон, насамперед у розкритті принципів, пріоритетів та напрямів Національної системи кібербезпеки, але при цьому не відповідає на низку принципових питань: у ній не визначені терміни та етапність її реалізації, не сформульовані варіанти розв'язання проблем у сфері кібербезпеки (песимістичний, оптимістичний та реалістичний), не обґрунтовані кількісно-якісні показники досягнення кінцевих цілей, відсутні механізм корегування та фінансове обґрунтування забезпечення реалізації Стратегії. Крім того, практика реалізації цього документу через механізм щорічних планів заходів з реалізації Стратегії, не підтриманих ресурсно, показав його декларативність та недієвість, що призвело до невиконання більшості із запланованих заходів і до суттєвої затримки чергового плану заходів на 2018 рік.

Особливістю сфери кібербезпеки є висока динаміка змін, які відбуваються в ній і які значною мірою обумовлені динамікою розвитку ІКТ, збільшенням кількості та рівня складності кіберзагроз, способів, методів і інструментів протидії їм. Ця особливість обмежує терміни дії стратегічних документів з кібер-

безпеки та кіберзахисту, які з часом швидко втрачають свою актуальність і тому не повинні розроблятись на термін більш ніж 3–5 років. Враховуючи вищезазначені недоліки Стратегії, а також прийняття Закону України «Про основні засади забезпечення кібербезпеки», Концепції створення державної системи захисту критичної інфраструктури, стан розробки таких проектів законів України, як «Про національну безпеку України», «Про критичну інформаційну інфраструктуру та її захист», «Про електронні комунікації» тощо, нагальною є проблема актуалізації чинної Стратегії та механізму її імплементації.

Водночас серед позитивних результатів прийняття Стратегії необхідно відмітити те, що її основні ідеї та підходи були враховані під час розробки Закону України «Про основні засади забезпечення кібербезпеки», в ній достатньо конкретно та обґрунтовано сформульовано перелік сучасних загроз кібербезпеці, документ включено в систему стратегічних документів, що визначають розвиток сектору безпеки та оборони, насамперед у проект Закону України «Про національну безпеку України», постановляючою частиною документу визначено необхідність створення Національного координаційного центру кібербезпеки, якій має забезпечити координацію діяльності суб'єктів національної безпеки й оборони України, підвищити ефективність системи державного управління у формуванні та реалізації державної політики у сфері кібербезпеки тощо. Загальним недоліком і Закону, і Стратегії є також їх недостатня узгодженість з міжнародними документами, насамперед законодавством ЄС і НАТО у сфері кібербезпеки.

У Стратегії національної безпеки України, Програмі діяльності Кабінету Міністрів України та Середньостроковому плані пріоритетних дій Уряду до 2020 року «забезпечення кібербезпеки» визначено як окремий напрям державної політики у сфері національної безпеки та оборони. Так, наприклад, у Стратегії національної безпеки України вперше чітко виокремлено сферу «забезпечення кібербезпеки і безпеки інформаційних ресурсів» від «забезпечення інформаційної безпеки» та визначено такі її пріоритети, як [7]:

– розвиток інформаційної інфраструктури держави;

– створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT);

– моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам та їх нейтралізації;

– розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів;

– забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого в Російській Федерації;

– реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС;

– створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони;

– розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Схема нормативно-правового забезпечення розбудови національної системи кібербезпеки та кіберзахисту України (далі – Схема) може бути представлена у вигляді ієрархічної структури сукупності таких основних документів (рис. 1).

Вкрай актуальною з точки зору повноти та системності законодавчого забезпечення кібербезпеки є прийняття таких законопроектів, як «Про національну безпеку України» та «Про критичну інфраструктуру та її захист», що займають відповідно другу та третю ланку в запропонованій ієрархічній моделі нормативно-правових актів. У першому з вищевказаних документів надається визначення Стратегії кібербезпеки України, вказується її місце в системі довгострокових документів з питань національної безпеки і оборони, розкривається узагальнена структура змісту, а також визначені головні суб'єкти, що відповідають за кібербезпеку та кіберзахист.

У проекті закону «Про критичну інфраструктуру та її захист», основним призначенням якого є визначення повноважень, завдань і відповідальності суб'єктів державної системи захисту критичної інфраструктури, передбачено врегулювання комплексу питань, більшість з яких відносяться до стратегічного планування та управління в цій сфері / 1/:

– створення державної системи захисту критичної інфраструктури;

– визначення повноважень складників сектору безпеки й оборони, які повинні передбачати забезпечення оборони, провадження правоохоронної, розвідувальної, контрроз-

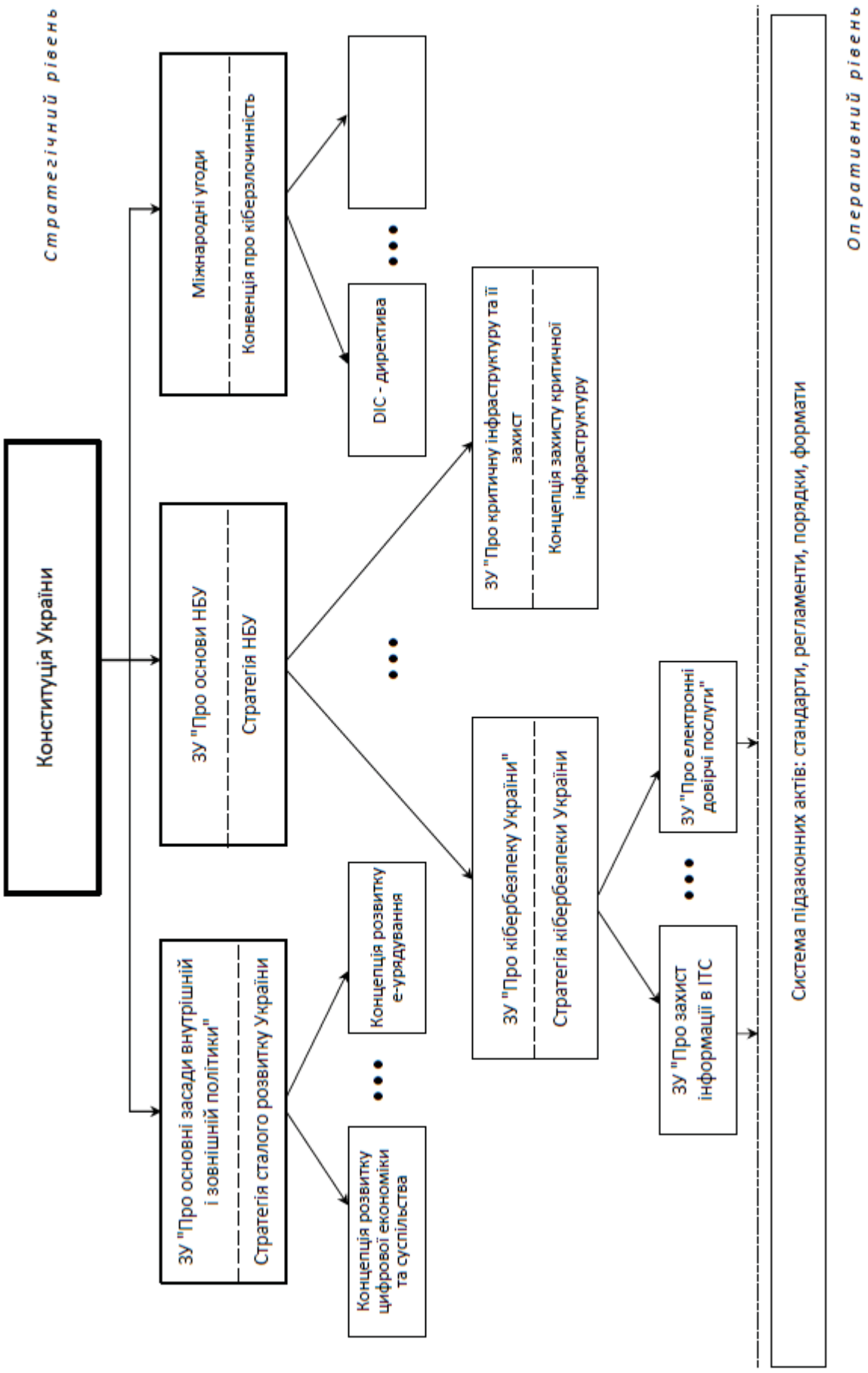

Рис. 1. Схема нормативно-правового забезпечення розбудови національної системи кібербезпеки України

відувальної діяльності, контртерористичний захист та кіберзахист критичної інфраструктури, захист економічного та науково-технічного потенціалу держави, обмін інформацією з питань оцінки загроз та реагування на загрози та кризові ситуації, а також ліквідації їхніх наслідків у взаємодії з іншими суб'єктами державної системи захисту критичної інфраструктури;

– запровадження єдиної методології проведення оцінки загроз критичній інфраструктурі та реагування на них, зокрема щодо аварій і технічних збоїв, небезпечних природних явищ, протиправних дій;

– визначення критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації;

– визначення засад державно-приватного партнерства та ресурсного забезпечення у сфері захисту критичної інфраструктури;

– здійснення міжнародного співробітництва у сфері захисту критичної інфраструктури.

В Законі України «Про основні засади забезпечення кібербезпеки» [5] визначені як суб'єкти забезпечення кібербезпеки взагалі, так і основні суб'єкти національної системи кібербезпеки зокрема з їхніми конкретними завданнями, а також система органів, що здійснює їх координацію. З метою якісного формування переліку об'єктів критичної інформаційної інфраструктури (комунікаційні й технологічні системи об'єктів критичної інфраструктури, технологічна інформація) та їх внесення до Державного реєстру об'єктів критичної інформаційної інфраструктури, з урахуванням секторального підходу та міжнародного досвіду до системи державних органів, що мають надавати Держспецзв'язку за встановленою формою галузеві переліки об'єктів критичної інформаційної інфраструктури, пропонується включити:

1) Міністерство енергетики та вугільної промисловості України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги в галузі енергетики;

2) Міністерство інфраструктури України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги в галузі транспорту;

3) Міністерство економічного розвитку і торгівлі України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги в галузі хімічної промисловості, або які включені до переліку підприємств, що мають стратегічне значення для економіки і національної безпеки держави (або безпеки населення та держави);

4) Міністерство регіонального розвитку, будівництва та житлово-комунального господарства України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, є комунальними службами;

5) Міністерство аграрної політики та продовольства України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги у сферах життєзабезпечення населення, зокрема у сферах виробництва продуктів харчування, сільського господарства, топографо-геодезичної та картографічної діяльності, ведення Державного земельного кадастру;

6) Міністерство охорони здоров'я України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги у сферах життєзабезпечення населення, зокрема у сфері охорони здоров'я;

7) Міністерство внутрішніх справ України – щодо підприємств, установ і організацій незалежно від форми власності, які є об'єктами потенційно небезпечних технологій і виробництв, є аварійними та рятувальними службами;

8) Міністерство юстиції України – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги щодо технічного, технологічного забезпечення створення та супроводження програмного забезпечення ведення автоматизованих систем Єдиних та Державних реєстрів, здійснення заходів із супроводження програмного забезпечення системи реалізації майна, технологічного забезпечення, збереження та захисту даних, що містяться в ній, на організацію та проведення електронних торгів, торгів за фіксованою ціною та на виконання інших функцій, передбачених Порядком реалізації арештованого майна;

9) Національний банк України – щодо підприємств, установ і організацій банківської системи незалежно від форми власності;

10) Державне агентство з питань електронного урядування України – щодо системи електронної взаємодії органів виконавчої влади, системи електронної взаємодії державних електронних інформаційних ресурсів, а також підприємств, установ і організацій

незалежно від форми власності, які забезпечують функціонування державних електронних інформаційних ресурсів;

11) Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації – щодо підприємств, установ і організацій незалежно від форми власності, які провадять діяльність і надають послуги в галузі електронних комунікацій.

При цьому необхідно підкреслити, що формування та забезпечення функціонування Державного реєстру об'єктів критичної інформаційної інфраструктури в банківській системі України здійснюються Національним банком України незалежно від органів виконавчої влади.

Два останніх державних органи із запропонованого вище списку відповідно до їх повноважень мають бути основними джерелами інформації про перелік об'єктів критичної інфраструктури сектору телекомунікації та зв'язку і включати :

– операторів та провайдерів телекомунікацій, які мають важливе значення для 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, зокрема ті, які надають послуги доступу до мережі Інтернет власникам (розпорядникам) ІТС ОКІ;

– державні електронні реєстри та їхні технологічні складники, інформаційно-телекомунікаційні системи, кадастри, державні інформаційні системи, незалежно від технології їх побудови, системи електронних торгів, системи державних тендерних закупівель;

– адміністраторів адресного простору мережі Інтернет у домені UA;

– адміністраторів доменів другого рівня, зокрема домену gov.ua;

– операторів цифрових послуг;

– операторів доступу до систем з використанням технологій «хмарних» обчислень;

– операторів доступу до систем пошуку в Інтернеті;

– операторів послуг пропуску трафіка тощо.

Інформація про стан об'єктів інформаційної критичної інфраструктури збирається вищевказаними державними органами та використовується як під час формування (корегування) Стратегії кібербезпеки України та інших стратегічних документів, так і для оперативного реагування системою кібербезпеки на кіберінциденти та кібератаки. Організаційно питання координації з розробки, прийняття та виконання стратегічних рішень з питань кібербезпеки та кіберзахисту визначено в Законі України «Про основні засади забезпечення кібербезпеки»: координація діяльності у сфері кібербезпеки як складової частини національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України; Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України; Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки. Але невизначеним залишається питання забезпечення взаємодії між Національним координаційним центром кібербезпеки, Державним центром кіберзахисту та протидії кіберзагрозам (ДЦКЗ) Держспецзв'язку, Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA та іншими командами реагування на комп'ютерні надзвичайні події, а також їх взаємодія з міжнародними центрами кіберзахисту. Виокремлюючи операційну та стратегічну діяльність вищевказаних суб'єктів кібербезпеки та кіберзахисту, пропонується такий координаційний механізм: координацію операційної діяльності команд реагування, їх облік та опублікування на загальнодоступних ресурсах усіх контактних даних для зв'язку з ними, інформування уповноважених з питань обміну інформацією про кіберінциденти органів інших країн, НАТО та ЄС здійснює Державний центр кіберзахисту та протидії кіберзагрозам (ДЦКЗ) Державної служби спеціального зв'язку та захисту інформації України.

У разі виявлення кіберінцидентів та кібератак, що можуть становити загрозу національній безпеці або обороноздатності держави, Державний центр кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України у встановленому порядку інформує Національний координаційний центр кібербезпеки, а також надає необхідну інформацію з Державного реєстру об'єктів критичної інфраструктури, для формування (коригування) Стратегії кібербезпеки України та інших стратегічних рішень у цій сфері.

Висновки:

1. Проаналізовано основні акти законодавства, що визначають розвиток наці-

ональної системи кібербезпеки в стратегічній перспективі та сформульовано напрями щодо їх удосконалення.

2. Для стратегічного рівня публічного управління запропонована схема нормативно-правового забезпечення розбудови національної системи кібербезпеки, запровадження якої сприятиме систематизації законодавства в цій сфері.

3. З метою якісного формування переліку об'єктів критичної інформаційної інфраструктури та їх внесення до Державного реєстру об'єктів критичної інформаційної інфраструктури, з урахуванням секторального підходу та міжнародного досвіду визначено систему державних органів, що мають надавати Держспецзв'язку за встановленою формою та погодженням із СБУ галузеві переліки об'єктів критичної інформаційної інфраструктури, а для сектору телекомунікацій та зв'язку сформовано орієнтовний перелік таких об'єктів критичної інфраструктури.

4. Запропоновано механізм взаємодії між Національним координаційним центром кібербезпеки та Державним центром кіберзахисту та протидії кіберзагрозам, а також взаємодію останнього з командами реагування на комп'ютерні надзвичайні події та з відповідними центрами інших країн ЄС та НАТО.

Подальшими перспективами розвитку даної проблеми передбачається розробка публічних механізмів аудиту об'єктів критичної інформаційної інфраструктури, державно-приватного та державно-суспільного партнерства з питань кібербезпеки та кіберзахисту.

ЛІТЕРАТУРА:

1. Концепція створення державної системи захисту критичної інфраструктури, схвалена розпорядженням Кабінету Міністрів України від 6 грудня 2017 р. № 1009-р. URL: http://zakon2.rada.gov.ua/laws/show/1009-2017-р.

2. The European Union is updating its cybersecurity strategy. URL: https://www.eu2017.ee/news/press-releases/european-union-updating-its-cybersecurity-strategy.

3. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 07.02.2013 JOIN(2013) 1. URL: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

4. Стратегія кібербезпеки України, схвалена Указом Президента України від 15.03.2016 р. № 96/2016. URL: http://zakon3.rada.gov.ua/laws/show/96/2016.

5. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII (Набрання чинності відбудеться 09.05.2018). URL: http://zakon3.rada.gov.ua/laws/show/2163-19.

6. Жиляєв І.Б., Семенченко А.І. Організаційно-правові механізми розвитку національної системи кібербезпеки України: стан та перспективи. Стратегічні пріоритети. Серія «Економіка». 2017. № 4(45). С. 55–63.

7. Стратегія національної безпеки України, схвалена Указом Президента України від 26.05.2015 року № 287/2015.