УДК 35.078.3+004.056

ТКАЧУК Н.А., старший науковий співробітник НДІІП НАПрН України

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ ПЕРЕЛІКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Анотація. *У статті автор досліджує організаційно-правові засади, стан та проблемні питання формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави як важливого елемента системи заходів із забезпечення кіберзахисту та кібербезпеки України.*

Ключові слова*: інформаційно-телекомунікаційні системи, критична інформаційна інфраструктура, кібербезпека, кіберзагрози, кіберзахист.*

Summary. *The article examines the organizational and legal bases, the status and problems of formation of the national critical information and communication systems list as an important component of comprehensive measures to ensure cyber security and cyber protection of Ukraine.*

Keywords: *information and telecommunication systems, critical information infrastructure, cyber security, cyber threats, cyber protection.*

Аннотация. *В статье автор исследует организационно-правовые основы, состояние и проблемные вопросы формирования перечня информационно-телекоммуникационных систем объектов критической инфраструктуры государства как важного элемента системы мероприятий по обеспечению киберзащиты и кибербезопасности Украины.*

Ключевые слова: *информационно-телекоммуникационные системы, критическая информационная инфраструктура, кибербезопасность,киберугрозы, киберзащита.*

Постановка проблеми. Забезпечення надійного кіберзахисту об’єктів критичної інфраструктури є однією з ключових умов безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Наслідки масованих кібератак на комп’ютерні мережі банківського, енергетичного, транспортного секторів, галузі зв’язку, а також органів державної влади України, які відбулися у червні 2017 року, викликали значний резонанс у суспільстві та засвідчили невідповідність існуючого стану захисту критичної інформаційної інфраструктури держави актуальним та потенційним кіберзагрозам сьогодення.

Підвищення ефективності та удосконалення організаційно-правових засад забезпечення кіберзахисту об’єктів критичної інфраструктури, в тому числі тих, які перебувають у приватній власності, а також встановлення відповідних вимог у цій сфері до їх власників та операторів не можливі без визначення на загальнодержавному рівні безпосереднього переліку їх інформаційно-телекомунікаційних систем (далі – ІТС), що потребують пріоритетного захисту від кібератак та повинні належати до критичної інформаційної інфраструктури держави.

Водночас, незважаючи на ініціативи вищих органів влади щодо формування такого переліку, наразі, це питання в Україні залишається не вирішеним, що негативно впливає на подальший розвиток спроможностей держави з протидії кіберзагрозам.

Результати аналізу наукових публікацій. Теоретичні та нормативно-правові аспекти кіберзахисту об’єктів критичної інфраструктури держави розглядалися такими науковцями як Д. Бірюков, В. Бурячок, С. Гнатюк, О. Довгань, Ю. Дрейс, Д. Дубов, О. Корченко,

В. Панченко та ін. Проте, у науковій літературі відсутні публікації, присвячені вивченню проблематики формування переліку інформаційно-телекомунікаційних систем таких об’єктів, що є необхідним для подальшого розвитку організаційно-правових засад кіберзахисту та обумовлює актуальність теми статті.

Метою статті є визначення організаційно-правових засад, стану та проблемних питань формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури України як пріоритетної складової системи заходів із забезпечення кіберзахисту та кібербезпеки держави.

Виклад основного матеріалу. Інформаційна складова є важливим елементом критичної інфраструктури будь-якої країни. В умовах актуалізації кіберзагроз та перетворення кібератак на інструмент міждержавного протистояння, а також засіб реалізації гібридної агресії з боку Російської Федерації, перед нашою державою виникла нагальна потреба – забезпечити у контексті розбудови національної системи кібербезпеки належний захист інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури.

Вочевидь, одним із перших кроків у цьому напрямку визначається розроблення переліку об’єктів, що належать до критичної інформаційної інфраструктури держави, організація та проведення оцінки стану їх захищеності. Саме такі завдання, виконання яких повинно було завершитись до кінця 2016 року, були поставлені Урядом перед Державною службою спеціального зв’язку та захисту інформації України відповідно до п. 4 Плану заходів щодо захисту державних інформаційних ресурсів, затвердженому розпорядженням Кабінету Міністрів України від 5.11.14 р. № 1135-р [1].

Однак, протягом 2014 – 2016 років ці завдання повною мірою реалізовані не були. Натомість, на виконання вказаного розпорядження, Держспецзв’язку спільно із зацікавленими державними органами було розроблено Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави (далі – Порядок), який визначав механізм, за яким відбуватиметься формування переліку таких систем, та повинен був стати “вагомим кроком у напряму підвищення рівня захисту інформації, що обробляється в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури держави” [2].

У серпні 2016 року Порядок було затверджено Постановою Кабінету Міністрів України “Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави” № 563 (далі – Постанова) [3], яка зобов’язувала органи державної влади у тримісячний строк подати Адміністрації Державної служби спеціального зв’язку та захисту інформації пропозиції до переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, попередньо погоджені з СБ України, на підставі яких Держспецзв’язку доручалося сформувати у шестимісячний строк перелік таких систем та подати його в установленому порядку Кабінету Міністрів України.

Однак, станом на лютий 2018 року, перелік ІТС об’єктів критичної інфраструктури в Україні (далі – Перелік) досі не сформовано. Основними чинниками негативного впливу на цей процес можна визначити наступні.

По-перше, формальне ставлення керівництва державних органів, у власності чи розпорядженні яких перебувають об’єкти критичної інфраструктури держави або до сфери управління яких вони належать, до задачі щодо своєчасного подання інформації стосовно ІТС таких об’єктів Держспецзв’язку для подальшого врахування у Переліку. Переважна більшість міністерств та відомств або взагалі не подало інформацію у встановлені терміни, або подана інформація була неповною.

За результатами розгляду цієї проблеми на засіданні Ради національної безпеки і оборони України рішенням РНБО України “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації” від 29.12.16 р. [4] було доручено Кабінету Міністрів України забезпечити у місячний строк виконання міністерствами, іншим центральним органам виконавчої влади завдання, передбаченого Постановою Кабінету Міністрів України “Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави” від 23.08.16 р. № 563, та вжити в установленому порядку заходів щодо притягнення до відповідальності осіб, які не забезпечили його виконання у визначений постановою строк.

Також, подання Адміністрацією Держспецзв’язку Кабінету Міністрів України переліку ІТС об’єктів критичної інфраструктури держави до кінця першого кварталу 2017 року з метою його затвердження було передбачене п. 5 Плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України, затвердженому Розпорядженням КМУ від 10.03.17 р. № 155-р. [5]

Хоча, фактично, формування та затвердження актом Уряду такого Переліку, на той час, не мало під собою достатніх юридичних підстав. Адже до прийняття у жовтні 2017 року Закону України “Про основні засади забезпечення кібербезпеки України” [6] Кабінет Міністрів жодним законодавчим актом не було уповноважено затверджувати критерії, порядок віднесення об’єктів до об’єктів критичної інфраструктури та їх перелік, в тому числі перелік їх інформаційно-телекомунікаційних систем.

Ще одним чинником, який унеможливлює подання уповноваженими державними органами повної інформації до Переліку є відсутність належної взаємодії з приватним сектором, до якого належить значна кількість об’єктів критичної інфраструктури держави, та які не зобов’язані подавати інформацію про їх інформаційно-телекомунікаційні системи в рамках виконання Постанови.

Більше того, у зв’язку з тим, що надання статусу критичної інформаційної інфраструктури передбачає збільшення зобов’язань та вимог із кіберзахисту власних систем (що в т. ч. потребуватиме збільшення фінансових витрат), а також запровадження відповідальності за їх порушення, значна кількість представників приватного сектору, наприклад, сфери телекомунікацій, фактично саботують діяльність із формування Переліку, аргументуючи, що це призведе до “надмірного та необґрунтованого навантаження” на бізнес [7].

Наступним проблемним питанням формування Переліку критичної інформаційної інфраструктури держави є відсутність нормативно закріплених критеріїв визначення оцінки негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему, з урахуванням яких і повинні формуватися пропозиції до Переліку. Зокрема, Постанова КМУ “Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави” зазначених критеріїв не містить.

Аналіз міжнародного досвіду свідчить, що до таких критеріїв, як правило, належать: сума фінансових збитків державі, кількість жертв, площа території ураження, можливість виведення з ладу інших секторів критичної інфраструктури тощо [8].

Також, у разі циркуляції в ІТС об’єктів критичної інфраструктури інформації з обмеженим доступом, при формуванні критеріїв необхідно враховувати можливі негативні наслідки для національних інтересів держави у разі витоку такої інформації та/або розголошення державної таємниці.

Виникає цілком закономірне питання – чи можливо взагалі визначити перелік ІТС об’єктів критичної інфраструктури за умови відсутності в державі безпосередньо переліку таких об’єктів?

Відповідно до чинного законодавства, об’єктами критичної інфраструктури є підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей [6].

На сьогодні єдиний перелік зазначених об’єктів в Україні відсутній, а захист об’єктів, які згідно із світовою практикою відносять до категорії “критичної інфраструктури” регламентується численними нормативно-правовими актами, що носять переважно відомчий характер [9].

Загрози критичній інфраструктурі, зазвичай, розподіляють на три групи, що включають аварії й технічні збої, природні лиха та небезпечні природні явища, зловмисні дії (груп або окремих осіб, таких як терористи, злочинці й диверсанти, промислове шпигунство, а також бойові дії) [10]. протидія кіберзагрозам та заходи з кіберзахисту ІТС об’єктів критичної інфраструктури повинні реалізовуватись, перш за все, у рамках комплексної системи захисту критичної інфраструктури держави як один із її елементів.

Наразі в країні відбувається активний процес розбудови такої системи. Згідно із Законом України “Про основні засади забезпечення кібербезпеки України” [6], а також Концепцією створення державної системи захисту критичної інфраструктури, затвердженій розпорядженням Кабінету Міністрів України від 6.12.17 р. № 1009-р [11], передбачено розроблення переліку об’єктів критичної інфраструктури, методології та визначення критеріїв віднесення таких об’єктів до критичної інфраструктури, порядку їх паспортизації та категоризації.

Таким чином, формування переліку об’єктів критичної інфраструктури держави є першочерговим кроком, необхідним для визначення інформаційно-телекомунікаційних систем таких об’єктів, які потребуватимуть пріоритетного захисту від кібератак.

Також, як свідчить досвід провідних країн, центральним компонентом у визначенні критичної інфраструктури є інформаційна складова [8; 12]. Тож поняття “критична інформаційна інфраструктура” не повинно включати лише ІТС об’єктів критичної інфраструктури, як це передбачено Законом України “Про основні засади забезпечення кібербезпеки України”, відповідно до якого, “об’єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об’єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об’єкта критичної інфраструктури” [6].

Це поняття повинно охоплювати також інші інформаційні системи, зокрема, національні електронні інформаційні ресурси, кібератака на які може призвести до значних негативних наслідків та суттєвої шкоди життєво важливим інтересам держави. Наприклад, Єдині та державні реєстри (Єдиний реєстр нотаріусів України, Державний реєстр речових прав на нерухоме майно, Державний реєстр актів цивільного стану громадян тощо), які за формальними ознаками не є інформаційно-телекомунікаційними системами об’єктів критичної інфраструктури, водночас, з урахуванням потенційних негативних наслідків для держави, до яких може призвести протиправний кібервплив на такі ресурси, повинні належати до критичної інформаційної інфраструктури та забезпечуватись підвищеним рівнем кіберзахисту.

Висновки.

1. Існуючі організаційно-правові засади формування переліку інформаційно-телекомунікаційних об’єктів критичної інфраструктури держави, на сьогодні, не можуть забезпечити дійсне формування і затвердження такого переліку та потребують удосконалення.

2. Основними проблемними питаннями формування переліку ІТС об’єктів критичної інфраструктури є:

– відсутність у державі переліку об’єктів критичної інфраструктури, який повинен бути основою при подальшому формуванні переліку інформаційно-телекомунікаційних систем таких об’єктів;

– відсутність чітких, нормативно-закріплених критеріїв щодо оцінки негативних наслідків, до яких може призвести кібератака на інформаційно-телекомунікаційну систему, що визначатиме належність ІТС до критичної інформаційної інфраструктури держави та обумовлюватиме необхідність включення до Переліку;

– низький рівень співпраці з приватним сектором та небажання власників і операторів об’єктів критичної інфраструктури брати на себе додаткові зобов’язання у сфері кіберзахисту;

– формальний підхід відповідальних посадових осіб центральних органів виконавчої влади до формування Переліку.

3. З метою удосконалення організаційно-правових засад формування Переліку запропоновано:

- реалізовувати завдання із формування переліку ІТС об’єктів критичної інфраструктури та їх кіберзахист в рамках системи комплексного захисту критичної інформаційної інфраструктури держави та на підставі попередньо сформованого переліку таких об’єктів, а також визначеної методики щодо оцінки потенційних негативних наслідків кібератак на їх інформаційно-телекомунікаційні системи;

- уточнити на законодавчому рівні поняття “критична інформаційна інфраструктура”, яке повинно включати не лише інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури, але й національні електронні інформаційні ресурси (державні реєстри, бази даних тощо) кібератака на які може призвести до завдання суттєвої шкоди національним інтересам;

- налагодити ефективний механізм державно-приватного партнерства та взаємодії із власниками та операторами об’єктів критичної інфраструктури у напряму забезпечення включення до Переліку інформації щодо об’єктів критичної інфраструктури, які перебувають у приватній власності, та організації належного рівня її кіберзахисту;

- підвищити контроль з боку компетентних держаних органів, зокрема Національного координаційного центру кібербезпеки при РНБО України, за станом виконання відповідальними посадовими особами органів державної влади завдань, передбачених чинними нормативно-правовими актами, щодо реалізації заходів з розбудови ефективної системи кіберзахисту ІТС об’єктів критичної інфраструктури держави, у тому числі щодо формування Переліку, та вжити в установленому порядку заходів щодо притягнення до відповідальності осіб, які не забезпечили своєчасне виконання зазначених завдань.

Використана література

1. Про затвердження плану заходів щодо захисту державних інформаційних ресурсів : Розпорядження Кабінету Міністрів України від 5.11.14 р. № 1135-р. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/1135-2014-%D1%80

2. Кабмін затвердив Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, який був розроблений за сприяння Адміністрації Держспецзв’язку. – Режим доступу : http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article%3Bjsessionid=2A9C287BFE0D1CA5AB75C3EFEC060867.app1?art_id=261878&cat_id=240232

3. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави : Постанова Кабінету Міністрів України від 23.08.16 р. № 563. – Режим доступу : https://www.kmu.gov.ua/ua/npas/249267402

4. Про рішення Ради національної безпеки і оборони України від 29.12.16 р. “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації” : Указ Президента України від 13.02.17 р. № 32/2017. – Режим доступу : http://www.president.gov.ua/ documents/322017-21282

5. Про затвердження Плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України : Розпорядженням Кабінету Міністрів України від 10.03.17 р. № 155-р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/155-2017-%D1%80

6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.17 р. № 2163-19. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2163-19

7. Відкритий лист Інтернет Асоціації України від 28.02.17 р. № 32 Президенту України щодо Рішення РНБО від 29.12.16 р. “Про загрози кібербезпеці держави та невідкладні заходи їх нейтралізації”. – Режим доступу : http://inau.ua/document/lyst-no32-vid-28022017-prezydentu-ukrayiny-shchodo-rishennya-rnbo-vid-29122016-pro-zagrozy

8. Гнатюк С.О. Визначення критичної інформаційної інфраструктури та її захисту : аналіз підходів / Зв’язок. – № 4 (2014). – С. 3-7.

9. Щодо створення державної системи захисту критичної інфраструктури : аналітична записка Національного інституту стратегічних досліджень. – Режим доступу : http://www.niss.gov.ua/articles/ 2490

10. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки : аналітична записка. – (Національний інститут стратегічних досліджень). – Режим доступу : http://www.niss.gov.ua/articles/2532

11. Про схвалення Концепції створення державної системи захисту критичної інфраструктури : Розпорядження Кабінету Міністрів України від 6.12.17 р. № 1009-р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/1009-2017-%D1%80

12. Дрейс Ю.О. Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави // Захист інформації. – Т. 19. – № 3 (2017). – С. 214-222.

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