УДК 007.51(477)

ОРГАНІЗАЦІЙНО-ПРАВОВІ МЕХАНІЗМИ РОЗВИТКУ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ: СТАН ТА ПЕРСПЕКТИВИ

Жиляєв Ігор Борисович,
доктор економічних наук, старший науковий співробітник
Семенченко Андрій Іванович,
доктор наук з державного управління, професор

У статті розглянуто стан і перспективи організаційно-правових механізмів розбудови національної системи кібербезпеки України, актуальність дослідження яких зумовлена збільшенням кількості кіберзагроз, їхньою складністю, масштабністю, комплексністю, розширенням кількості їх суб'єктів та об'єктів. Метою статті є аналіз тенденцій розвитку цих механізмів, їх відповідності сучасним загрозам та європейським підходам, а також пропозиції щодо їх удосконалення з урахуванням національного та міжнародного досвіду.

Проведений аналіз організаційно-правових механізмів розвитку національної системи кібербезпеки засвідчив їх недосконаліть насамперед щодо відповідності сучасним загрозам, європейським підходам, а також їх неповноту за складом, нечіткість і недостатню конкретність стосовно повноважень суб'єктів цієї системи. Запропоновано конкретні напрями вдосконалення цих механізмів, у т. ч. шляхом розширення кола основних суб'єктів з уточненням їхніх повноважень, застосування державно-приватного та державно-суспільного партнерства.

Ключові слова: кібербезпека, національна система кібербезпеки, організаційно-правові механізми кібербезпеки.

Zhylyaev Igor, Semenchenko Andrii

ORGANIZATIONAL AND LEGAL MECHANISMS OF THE DEVELOPMENT OF THE NATIONAL CYBER SECURITY SYSTEM OF UKRAINE: THE STATE AND PROSPECTS

The article examines the state and prospects of organizational and legal mechanisms for the development of the national cyber security system of Ukraine, the relevance of which is due to the increase in the number, complexity, scale, complexity of cyber threats, and the expansion of the number of their subjects and objects. The purpose of the article is to analyze trends in the development of these mechanisms, their compliance with modern threats and European approaches, as well as proposals for their improvement, taking into account national and international experience.

The analysis of organizational and legal mechanisms for the development of the national system of cyber security showed their imperfection; first of all, in relation to their compliance with the list of modern threats, European approaches, as well as their incompleteness in composition, lack of clarity and lack of specificity regarding the powers of the subjects of this system. Specific directions of their improvement are offered, including, by expanding the range of key actors with clarification of their powers, application of public-private and public-public partnerships.

Keywords: cybersecurity, national system of cyber security, organizational and legal mechanisms of cyber security.

Постановка проблеми. Питання формування сучасної національної системи кібербезпеки останнім часом усе більш актуалізуються. Розширюється сукупність суб'єктів, які стають безпосередніми та потенційними об'єктами кіберзагроз як на глобальному, регіональному, національному рівнях, так і на рівні окремих бізнес-структур та інституцій громадянського суспільства, людини і громадянина. Зростає кількість кіберзагроз, вони стають більш складними, масштабними та комплексними. У зв'язку з цим Європейський Союз оголосив про перегляд та актуалізацію в 2017 р. [1] Стратегії кібербезпеки ЄС 2013 року [2].

Не є виключенням й Україна, де останнім часом було видано низку нормативно-правових актів з питань кібербезпеки, у системі виконавчої влади створюються установи та організації, орієнтовані на виконання завдань, що стосуються кібербезпеки. Так, метою Стратегії кібербезпеки України визначено створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, для чого, зокрема, передбачено створення національної системи кібербезпеки.

Аналіз останніх досліджень і публікацій. Нормативно-правові аспекти системи кібернетичної безпеки розглядались у працях зарубіжних учених: Д. Аддікотта, К. Александера, Т. Вінгфілда, Дж. Ліпмана, А. Льюїса, В. Мазурова, Д. Крамера, Р. Олдрича, І. Соколова, Є. Старостіної, В. Шарпа, М. Шмітта, Б. Шнаєра, А. Щетилова. Можна назвати вітчизняні наукові праці за цією тематикою В. Бурячка, Р. Грищука, Ю. Даника, О. Довганя, Д. Дубова, В. Петрова, В. Пилипчука, Т. Тропініної, В. Шеломенцева та ін. Однак варто зазначити, що в Україні недостатньо досліджень з питань кібербезпеки взагалі та з розвитку національної системи кібербезпеки зокрема. Про це, наприклад, свідчать дані пошуку від 3.12.2017 р. в *Google*. За ключовими словами «кібербезпека» знайдено приблизно 144 тис. посилань; «кибербезопасность» – 606 тис.; «*cybersecurity*» – 52 300 тис.

Актуальність тематики зумовлена деякими характерними особливостями.

По-перше, відбувається все масштабніше проникнення інформаційно-комунікаційних технологій (ІКТ) в політичне та соціально-економічне життя; різко зростає кількість інтернет-користувачів, пристроїв, підключених до мережі Інтернет, тощо. Безперечно, навіть просте збільшення кількості користувачів призводить до збільшення кіберінцидентів в Інтернеті (за деякими висновками, кількість кіберінцидентів щорічно зростає на декілька десятків відсотків).

По-друге, зростає ступінь вразливості економічних та суспільних суб'єктів через порушення їхньої діяльності в Інтернеті (прямий вплив) та широкомасштабні кібератаки/операції щодо суспільно-економічної діяльності (опосередкований), на що, зокрема, звертається увага в Стратегії кібербезпеки України.

По-третє, дії в кіберпросторі, спрямовані на політичні та соціально-економічні структури, є менш затратними та приносять більш вагомі результати, ніж проведення прямої військової чи економічної агресії. Вони також є менш ризикованими для кіберзлочинців з позицій кримінального права та значно ефективнішими з точки зору політичного чи соціально-економічного впливу, що досягається з меншими витратами.

Міжнародний валютний фонд (МВФ) у своїй доповіді 2017 р., присвяченій питанням глобальної фінансової стабільності, оцінив економічні втрати від глобальних кібератак у 53 млрд дол. США, у т. ч. 850 млн дол. США від кібератаки 2017 р., пов'язаної з вірусом *NotPetya*, що вразив український фінансовий та публічний сектор і створив проблеми в інших країнах [3].

У щорічному звіті компанія *Trend Micro* визначила 2016 р. роком програм-вимагачів (*ransomware*). Саме впродовж цього року кількість кібератак з вимогами оплати за деблокування вражених комп'ютерів досягла максимального рівня за всю історію спостереження, а збитки бізнесу становили 1 млрд дол. США у світовому масштабі. Кількість видів шкідливих програм-вимагачів із вимогами викупу, які стали популярними серед кіберзлочинців, за рік зросла майже у 8 разів [4].

За останні два роки на 23 % збільшилися збитки від кіберзлочинності, яка нині «коштує» кожній бізнес-організації в середньому 11,7 млн дол. США. Число успішних кібератак, здійснюваних щорічно, на одну компанію в середньому зросло зі 102 до 130 кібератак (більш ніж на 27 %). Окрім того, бізнес-організації несуть тягар збільшення витрат на кібербезпеку. В таких галузях, як фінансові та комунальні послуги, енергозбереження тощо, кожна компанія в середньому за рік витрачає понад 17 млн дол. США [5].

Україна також несе збитки від кібератак. Так, унаслідок кібератаки в грудні 2016 р. на державні фінансові установи протягом майже трьох днів було ускладнено сплату до бюджету податків та інших платежів, заблоковано електронну систему адміністрування ПДВ, порушено роботу митниці. У листопаді-грудні 2016 р. було здійснено близько 6,5 тис. кібератак на 5 відомств і 31 державний інформресурс.

За експертними оцінками, у результаті атаки вірусу *NotPetya* на комп'ютерні системи українських державних і комерційних установ України станом на 7 липня 2017 р. було виведено з ладу до 10 % приватних, урядових і корпоративних комп'ютерів [6].

Наостанок, через те, що дії у кіберпросторі перейшли на якісно новий рівень, в останні роки кіберінциденти все частіше:
1) ініціюються спеціально створеними державними структурами;
2) проводяться за завданнями державних структур іноземних країн спеціальними недержавними організаціями та групами підготовлених фахівців високої кваліфікації;
3) загрози набувають нових ознак – стали можливі кіберінциденти із людськими втратами, значними комплексними політичними, екологічними, технологічними та економічними ризиками;
4) використовуються як засіб зовнішнього втручання в політичні процеси, дезорганізації діяльності публічної адміністрації країн, проти яких здійснюються відповідні кібератаки.

Актуальність тематики зумовлена ще й тим, що Україна вже кілька років перебуває в умовах гібридної війни, одним із невід'ємних елементів якої є гібридно-воєнні дії в інформаційно-комунікаційних системах. Вдаючись до їх активного застосування, «супротивник не припиняє своєї деструктивної діяльності, і кібератаки на державні органи та об'єкти критичної інфраструктури продовжуються й у 2017 р.» [6]. При цьому визнається, що Україна має значні проблеми з організацією системи кібербезпеки. Зокрема, у сфері захисту об'єктів, систем і ресурсів критичної інфраструктури відстає від європейських країн приблизно на 10–12 років.

Мета статті – проаналізувати стан розвитку організаційно-правових механізмів забезпечення національної системи кібербезпеки в Україні, їх відповідність сучасним загрозам та європейським підходам до створення та функціонування аналогічних систем, запропонувати конкретні напрями їх удосконалення.

Виклад основного матеріалу. Серед провідних завдань у сфері кібербезпеки України є формування національної політики кібербезпеки, що забезпечується низкою національних та міжнародних актів, насамперед:
1) актами загального спрямування, зокрема: Конституцією України та Стратегією національної безпеки України 2015 року; нормативно-правовими актами України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації тощо;
2) спеціалізованими актами щодо кібербезпеки, а саме: Конвенцією про кіберзлочинність, яка ратифікована Законом України від 7 вересня 2005 р. № 2824-IV; Стратегією кібербезпеки України [7]; Законом України «Про основні засади забезпечення кібербезпеки України» [8]; Рішенням Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»; Порядком формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затвердженим постановою Кабінету Міністрів України від 23 серпня 2016 р. № 563 тощо.

Однак сформована національна політика кібербезпеки має певні суттєві розбіжності за спрямуванням та змістом із європейською політикою, у т. ч. із Стратегією кібербезпеки ЄС 2013 року.

До основних недоліків чинного національного законодавства із розбудови національної системи кібербезпеки можна віднести:
1) недостатню сконцентрованість мети – незважаючи на декларування захисту людини та громадянина, їхніх основних прав, свободи слова, персональних даних та конфіденційності, цей розділ законодавства насамперед зосереджений на захисті інтересів органів державної влади (фактично не вирішена проблема системності кіберзахисту всіх об'єктів національної системи кібербезпеки: людини/громадянина; бізнесу; органів публічної влади; держави в цілому, зокрема в особливих сучасних умовах (війна/гібридна війна) тощо;
2) «пласку» (горизонтальну – в одній площині) та ієрархічну (не мережеву) побудову її структури;
3) неекономічність – не беруться до уваги як економічні наслідки кіберінцидентів, так і ефективність пропонованих заходів (витрати – результати);

4) недостатню обґрунтованість – не передбачено включення (немає посилань на роль і місце) науки та інновацій, у той час як Стратегія кібербезпеки ЄС 2013 року використовує Рамкову програму Європейського Союзу з досліджень та інновацій «Горизонт 2020» як невід'ємну частину;
5) відведення достатньо пасивної ролі бізнесу та інститутам громадянського суспільства, механізмам державно-приватного партнерства;
6) зосередженість на «злій волі» – діях зовнішніх кіберзлочинців, зовнішніх кібератаках, а не на комплексному захисті національного кіберпростору від усіх негативних впливів (зовнішніх і внутрішніх) тощо.

Недарма серед проблем функціонування сил оборони в умовах існуючих та потенційних загроз[1], зокрема, визначено «неспроможність ефективно реагувати на зростаючу кількість та потужність кібератак та протистояти кіберзлочинності» [9].

Розглянемо систему кібербезпеки України, яка організаційно має кілька складників.

I. Суб'єкти кібербезпеки, до яких, зокрема, належать:
1) *атакуюча сторона*: українські, іноземні й міжнародні особи та організації, які забезпечують організацію та здійснення (проведення) кіберінцидентів (зокрема кібератак) та вчиняють шкоду (або загрожують) кібербезпеці взагалі та конкретним об'єктам національної інфраструктури;
2) ті з них, що *забезпечують формування та здійснення національної політики (та участі в міжнародній політиці)*;
3) ті з них, *на яких впливають кіберінциденти*, а саме: органи публічної влади; власники об'єктів критичної інфраструктури приватної та державної форм власності; власники інформаційних систем та інформаційних ресурсів, які офіційно не визнано критичними, але які можуть бути об'єктами кіберінцидентів (зокрема кібератак); громадяни України, присутні в Мережі; іноземні та міжнародні особи та організації, які діють в українському сегменті Інтернету;
4) *системи протидії та захисту*: фізичних осіб, державних установ та приватних фірм, які працюють над створенням антивірусних програм, програмного та організаційно-технічного забезпечення кіберзахисту; закладів освіти та наукових організацій, що задіяні у виконанні завдань кібербезпеки; експертних, розвідувальних та контррозвідувальних органів; системи судочинства (судового розгляду шкідливих наслідків кібератак);
5) *системи ліквідації наслідків* кіберінцидентів (у першу чергу кібератак та кібердиверсій), у т. ч. тих, що завдали шкоди фізичним об'єктам (шляхом створення надзвичайних ситуацій);
6) *суб'єкти активної кібероборони*, що забезпечують запобігання кіберзлочинності та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, відсіч агресії;
7) *суб'єкти іноземних і міжнародних організацій, мереж та систем кібербезпеки*.

II. Об'єкти кібербезпеки та об'єкти кіберзахисту [8].

III. Функціональні зв'язки, зокрема нормативно-правового та адміністративно-організаційного забезпечення.

Організаційне забезпечення. Стратегія кібербезпеки України визначає мету створення національної системи кібербезпеки, основних суб'єктів забезпечення кібербезпеки та їх загальні повноваження. Так, зазначено, що національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури [7].

У Стратегії визначено, що основу національної системи кібербезпеки становитимуть: Рада національної безпеки і оборони України (РНБОУ), Міністерство оборони України, Генеральний штаб Збройних Сил України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи [7].

---

[1] У Стратегічному оборонному бюлетені України також визначено загальні проблеми оборони, які теж стосуються кібербезпеки, зокрема: а) відсутність чіткого розподілу відповідальності за формування та застосування сил оборони, що негативно позначається на здатності керівництва держави здійснювати ефективне управління у сфері оборони; б) відсутність об'єднаного керівництва силами оборони, яке здійснювалося б відповідно до принципів і стандартів, прийнятих державами – членами НАТО; в) надмірність обсягів та неактуальність нормативно-правової бази у сфері оборони.

Закон України «Про основні засади забезпечення кібербезпеки України», що набере чинності у травні 2018 р., значно розширює перелік суб'єктів забезпечення кібербезпеки. Так, Законом (стаття 5) визначено, що Президент України здійснює забезпечення координації у сфері кібербезпеки через очолювану ним РНБО України; на Кабінет Міністрів України покладається обов'язок із формування та реалізації державної політики у сфері кібербезпеки та контроль і аудит за її виконанням тощо; всі органи державної влади, а саме: міністерства та інші центральні органи виконавчої влади, місцеві державні адміністрації та органи місцевого самоврядування здійснюють заходи із забезпечення кібербезпеки в межах своєї компетенції. Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, також є: правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства критичної інфраструктури тощо [8].

Крім того, у вирішенні питань щодо кібербезпеки бере участь Верховна Рада України (контроль), а також два парламентські комітети: національної безпеки і оборони та інформатизації та зв'язку. Сфера захисту персональних даних та доступ до публічної інформації у сфері кібербезпеки – царина діяльності Уповноваженого Верховної Ради України з прав людини.

Слід зазначити, що протягом останніх років формування архітектури системи кібербезпеки України відбувалось у першу чергу через створення нових державних установ та організацій: 1) Національного координаційного центру кібербезпеки РНБОУ; 2) Департаменту кіберполіції Національної поліції (шляхом перетворення підрозділів боротьби з кіберзлочинністю на новітній орган правозахисного призначення); 3) Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України та його спеціалізованого структурного підрозділу *CERT-UA* (*Computer Emergency Response Team of Ukraine*) – команда реагування на комп'ютерні надзвичайні події України; 4) Центру з розслідування злочинів в інформаційній сфері Служби безпеки України; 5) у Міноборони: відділу безпеки інформації та відділу кібернетичної безпеки в Головному управлінні зв'язку та інформаційних систем; Головного об'єднаного центру захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційній системі; регіональних центрів захисту інформації та кібернетичної безпеки (Вінниця, Чернігів, Миколаїв) [10]; військових частин і підрозділів інформаційних (кібер) операцій [11].

Процес розвитку організаційної системи у сфері кібербезпеки не завершено: існують пропозиції щодо створення спеціального державного органу з питань координації захисту критичної інфраструктури [6].

Формування національної системи кібербезпеки сьогодні перебуває на початковому етапі, коли формуються концептуальні рішення, розбудовується відповідна термінологічна система, узгоджуються функції та відповідальні за виконання певних функцій. Нині більшість норм, що встановлюють функції, права та обов'язки вищевказаних ЦОВВ, не закріплена у відповідних положеннях про ці органи.

У системі законодавчого забезпечення кібербезпеки поза увагою залишилися деякі органи державної влади, яким делеговано певні функції, зокрема ті, на які покладаються повноваження згідно з нормами Закону України «Про ратифікацію Конвенції про кіберзлочинність»: *Міністерство юстиції України* (щодо запитів судів та їх доручень); *Генеральна прокуратура України*[2] (щодо запитів органів досудового слідства та їх доручень) та *Міністерство внутрішніх справ України* (щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних із комп'ютерними системами й даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі) [12].

Недарма європейські експерти наприкінці 2016 р. зазначали: «Оскільки *відповідальність стосовно питань, пов'язаних із кіберзлочинністю та кібербезпекою, перебуває у компетенції різних органів влади, на центральному урядовому рівні відсутня координація* (курсив наш. – *Авт.*) щодо цього питання» [13].

Адаптація до норм європейського права у сфері кібербезпеки. Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність та Додатковий

[2] Участь Генеральної прокуратури України у боротьбі з кіберзлочинністю передбачена також Угодою про співробітництво з Федеральною прокуратурою Королівства Бельгія (2015) та Меморандумом про співробітництво з Національною прокуратурою Королівства Нідерланди (2009).

протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи; Угоду про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії та їхніми державами-членами, з іншої сторони, статтею 32 якої встановлено, що «сторони співробітничають у боротьбі з кримінальною та незаконною організованою чи іншою діяльністю, а також з метою її попередження для вирішення, зокрема, проблем кіберзлочинності» [14]. Крім того, було підписано Міжвідомчу декларацію про співробітництво України з країнами Організації Північноатлантичного договору у сфері кібербезпеки від 6 жовтня 2014 р. та Угоду про реалізацію Трастового фонду Україна – НАТО з питань кібербезпеки між Службою безпеки України та Румунською службою інформації (2015) тощо.

Однак адаптація вітчизняного законодавства до норм європейського права у сфері кібербезпеки здійснюється вкрай повільно. Ратифіковано лише два базових акти європейського права – Конвенцію про кіберзлочинність та Додатковий протокол до Конвенції, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Відставання в законодавчому забезпеченні сфери кібербезпеки України щодо адаптації до європейського права продовжує зростати[3].

Значна кількість норм Конвенції про кіберзлочинність не імплементована в українське законодавство, відтак деякі норми законів України не відповідають змісту норм Конвенції. Зокрема, не імплементовано статтю 18 Конвенції щодо впровадження спеціальних судових ордерів на представлення даних (глава 15 Кримінального процесуального кодексу (КПК)); статтю 19 – про надання повноважень компетентним органами: 1) здійснювати заходи обшуку або відповідного доступу; 2) застосувати аналогічні заходи до мережевих систем; 3) арештовувати комп'ютерні системи, носії або дані; 4) вимагати від будь-якої особи, що обізнана із функціонуванням комп'ютерної системи або захистом комп'ютерних даних, які містяться в цій системі, надавати, наскільки це можливо, необхідну інформацію для проведення обшуку; статтю 20 – щодо збирання комп'ютерних даних у реальному масштабі часу; статтю 21 – щодо перехоплення даних змісту інформації тощо [13].

Можна констатувати певне *зволікання із розробкою та впровадженням регуляторних рішень щодо національної політики у сфері кібербезпеки; певну фрагментарність рішень, що приймаються, їхню частковість; несистемність заходів органів державної влади.*

Європейські експерти, аналізуючи чинне українське законодавство і проекти законів, що пов'язані з кіберзлочинністю, зазначали: «Потрібно *чітко встановити відповідальних за проведення законодавчих реформ.* Іншими словами, належить *чітко визначити, яка саме установа відповідальна за реформу*, навіть попри те, що до цього процесу варто залучати широкий перелік зацікавлених сторін. У цьому контексті значною проблемою є той факт, що деякі проекти законів, які готували одночасно, торкаються однакових питань, і прикладом цього є внесення однакових змін до КПК. Виглядає на те, що *спільного розуміння практичних проблем і методів їхнього вирішення немає* (курсив наш. – *Авт.*)» [13].

До певної міри деякі правові рішення були достатньо кон'юнктурними, такими, що орієнтувалися на нагальні вимоги часу, зокрема кібер-інциденти, які відбувалися в інформаційному просторі країни або були ініційовані глобальними трендами.

Варто зазначити, що фактично формування Концепції національної системи кібербезпеки характеризується:
1) галузевим (несистемним) підходом (кібербезпека: авіаційна, банківська, електромереж та електровиробників тощо)[4];
2) прагненням виокремити питання кібербезпеки в окреме завдання, без органічного включення її в цілісну систему національної безпеки[5].

---

[3] Усього на сайті документів європейського права *EUR-Lex* лише в 2017 р. (станом на 4.12.2017 р.) було розміщено 110 нових документів з питань кібербезпеки (див.: http://eur-lex.europa.eu/search.html?qid=1512390007458&text=cybersecurity&scope=EURLEX&type=quick&lang=en&DD_YEAR=2017).

[4] В Аналітичній доповіді до Щорічного Послання Президента України 2017 р. зазначено: «Існуючі в Україні державні системи та відповідні процедури реагування на безпекові інциденти реалізовані переважно на основі відомчих підходів, незважаючи на їх загальнодержавний статус. Інструменти забезпечення координації дій, взаємодії та обміну інформацією між суб'єктами цих систем є недостатньо розвинутими, неперевіреними під час тренувань у ситуаціях комплексного характеру, національного рівня» [6].

[5] Прикладом є проект Закону про внесення змін до деяких законодавчих актів України щодо боротьби з тероризмом (реєстр. № 6438 від 12 травня 2017 р., поданий Кабінетом Міністрів України), у якому пропонується внормувати діяльність із боротьби з актами ядерного тероризму без урахування загроз кібератак.

Ураховуючи, що значну загрозу в сучасних умовах становлять кібератаки, спрямовані на дезорганізацію економічних і технологічних процесів на об'єктах критичних інфраструктур, що можуть призвести до технологічних та екологічних катастроф, варто «вбудувати» політику з кібербезпеки у загальну політику національної безпеки як її невід'ємну складову (зокрема, прив'язати до політики у сфері надзвичайних ситуацій). Так, у Класифікаційних ознаках надзвичайних ситуацій надано перелік 152 надзвичайних ситуацій, зокрема: 78 – техногенного характеру; 49 – природного; 25 – соціального (однак у класифікаторі не визначено, котрі з них можуть бути викликані кібератаками) [15];

3) намаганням здійснювати побудову *ієрархічної структури* управління кібербезпекою країни, якій протидіють *мережеві структури* кіберзлочинців, перш за все – міжнародні та іноземні (протистояння за принципом «ієрархія проти мережі»);

4) опорою на державні структури, які мають адміністративно-командно забезпечувати діяльність усіх суб'єктів кібербезпеки в країні (більша частина об'єктів національної системи критичної інфраструктури є у приватній, а не у державній власності) через директивні акти, а не шляхом рекомендаційних актів; відсутністю формування чіткої, відповідальної системи кібербезпеки рівноправних суб'єктів усіх форм власності; несформованістю системи державно-приватного партнерства у цій сфері;

5) відсутністю централізованого фінансування комплексних проектів кібербезпеки, організації розробки та впровадження типових рішень (процедур і заходів) забезпечення кібербезпеки;

6) формуванням спрощеної «пласкої» системи кібербезпеки, не багаторівневої, системної, зокрема з урахуванням *різних режимів безпеки*: 1) повсякденного функціонування; 2) підвищеної готовності; 3) надзвичайної ситуації; 4) надзвичайного стану); рівнів терористичних загроз (наприклад, «сірий» (можлива загроза); «синій» (потенційна загроза); «жовтий» (імовірна загроза); «червоний» (реальна загроза)) [16];

7) відсутністю цілісної національної політики з побудови системи кібербезпеки, що призводить до невизначеності щодо її ресурсного забезпечення (кадри, технічне, програмне та організаційно-методичне забезпечення тощо).

Висновки

1. Проведений аналіз стану організаційно-правових механізмів забезпечення національної системи кібербезпеки засвідчив їх недосконаліть, насамперед щодо її відповідності переліку сучасних загроз, європейським підходам до створення та функціонування аналогічних систем, а також її неповноту за складом, нечіткість та недостатню конкретність стосовно повноважень суб'єктів цієї системи, відсутність централізованого фінансування тощо.

2. Запропоновано конкретні напрями вдосконалення організаційно-правових механізмів забезпечення національної системи кібербезпеки, у т. ч. стосовно включення до складу основних суб'єктів національної системи кібербезпеки Генеральної прокуратури України, Міністерства юстиції та Міністерства внутрішньої політики з уточненням їх повноважень у цій сфері.

3. Потребує більш конкретного та детального обґрунтування застосування державно-приватних та державно-громадських механізмів у національній системі кібербезпеки, при цьому мають ураховуватися процеси децентралізації та деконцентрації влади, а також фінансово-економічні механізми.

Список використаних джерел

1. The European Union is updating its cybersecurity strategy [Електронний ресурс]. – Режим доступу : https://www.eu2017.ee/news/press-releases/european-union-updating-its-cybersecurity-strategy
2. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 07.02.2013 JOIN (2013) 1 [Електронний ресурс]. – Режим доступу : final http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
3. International Monetary Fund: Global Financial Stability Report October 2017: Is Growth at Risk? [Електронний ресурс]. – Режим доступу : https://www.imf.org/en/Publications/GFSR/Issues/2017/09/27/global-financial-stability-report-october-2017
4. 2016 Security Roundup: A Record Year for Enterprise Threats [Електронний ресурс]. – Режим доступу : https://documents.trendmicro.com/assets/rpt/rpt-2016-annual-security-roundup-a-record-year-for-enterprise-threats.pdf
5. 2017 Ponemon Institute. Cost of cyber crime study: Insights on the Security Investments that make a Difference [Електронний ресурс]. – Режим доступу : https://www.accenture.com/t20171006T095146Z_w_/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50

6. Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України «Про внутрішнє та зовнішнє становище України в 2017 році». – К. : НІСД, 2017. – 928 с.
7. Стратегія кібербезпеки України, схвалена Указом Президента України від 15 березня 2016 р. № 96/2016 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/96/2016
8. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2163–19
9. Стратегічний оборонний бюлетень України [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/240/2016/paran10#n10
10. Додаток 1 до Стратегічного оборонного бюлетеня України [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/240/2016
11. Річна національна програма під егідою Комісії Україна – НАТО на 2017 рік, затверджена Указом Президента України від 8 квітня 2017 р. № 103/2017 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/103/2017
12. Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 р. № 2824-IV [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/994_575
13. Звіт щодо України 2016/DGI/JP/3608 «Про чинне законодавство і проекти законів, що доповнюють різні питання, пов'язані з кіберзлочинністю та електронними доказами, та вносять зміни до них» [Електронний ресурс]. – 2016. – 3 листоп. – Режим доступу : https://rm.coe.int/16806f3743
14. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/984_011/page
15. Класифікаційні ознаки надзвичайних ситуацій, затверджені Наказом Міністерства надзвичайних ситуацій України від 12 грудня 2012 р. № 1400 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/z0040–13/paran13#n13
16. Положення про єдину державну систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, затверджене Постановою Кабінету Міністрів України від 18 лютого 2016 р. № 92 [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/92–2016-%D0 %BF

References

1. The European Union is updating its cybersecurity strategy. (n. d.). *eu2017.ee*. Retrieved from https://www.eu2017.ee/news/press-releases/european-union-updating-its-cybersecurity-strategy [in English].
2. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 07.02.2013 JOIN (2013) 1. (n. d.). *eeas.europa.eu*. Retrieved from final http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf [in English].
3. International Monetary Fund: Global Financial Stability Report October 2017: Is Growth at Risk? (2017, 27 Sept.). *imf.org*. Retrieved from https://www.imf.org/en/Publications/GFSR/Issues/2017/09/27/global-financial-stability-report-october-2017 [in English].
4. 2016 Security Roundup: A Record Year for Enterprise Threats. (n. d.). *documents.trendmicro.com*. Retrieved from https://documents.trendmicro.com/assets/rpt/rpt-2016-annual-security-roundup-a-record-year-for-enterprise-threats.pdf [in English].
5. 2017 Ponemon Institute. Cost of cyber crime study: Insights on the Security Investments that make a Difference. (n. d.). *accenture.com*. Retrieved from https://www.accenture.com/t20171006T095146Z_w_/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50 [in English].
6. *Analitychna dopovid do Shchorichnoho poslannia Prezydenta Ukrainy do Verhovnoi Rady Ukrainy «Pro vnutrishnie ta zovnishnie stanovyshche v 2017 rotsi». [Analytical lecture to the Annual Message of the President of Ukraine in the Verkhovna Rada of Ukraine «About the internal and external position of Ukraine in 2017»].* (2017). Kyiv, NISD [in Ukrainian].
7. Stratehia kiberbezpeky Ukrainy, shvalena Ukazom Prezydenta Ukrainy vid 15 bereznia 2016 r. № 96/2016 [Cybersecurity Strategy of Ukraine, approved by Decree of the President of Ukraine dated March 15, 2016 No. 96/2016]. (n. d.). *zakon3.rada.gov.ua*. Retrieved from http://zakon3.rada.gov.ua/laws/show/96/2016 [in Ukrainian].
8. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky v Ukraini» vid 5 zhovtnia 2017 p. № 2163-VIII [Law of Ukraine "On the Basic Principles of Providing Cybersecurity of Ukraine" from 2017, Oct. 5 No. 2163-VIII]. (n. d.). *zakon3.rada.gov.ua*. Retrieved from http://zakon3.rada.gov.ua/laws/show/2163–19 [in Ukrainian].
9. Stratehichnyi oboronnyi buleten Ukrainy [Strategic Defense Bulletin of Ukraine]. (2016). *zakon.rada.gov.ua*. Retrieved from http://zakon3.rada.gov.ua/laws/show/240/2016/paran10#n10[in Ukrainian].
10. Dodatok 1 do Stratehichnoho oboronnoho buletenia Ukrainy [Annex 1 to the Strategic Defense Bulletin of Ukraine]. (2016). *zakon3.rada.gov.ua*. Retrieved from http://zakon3.rada.gov.ua/laws/show/240/2016 [in Ukrainian].

11. Richna natsionalna prohrama pid ehidoiu Komisii Ukraina – NATO na 2017 rik, zatverdzhena Ukazom Prezydenta Ukrainy 8 kvitnia 2017 r. № 103/2017 [Annual National Program under the auspices of the Ukraine-NATO Commission for 2017, approved by the Decree of the President of Ukraine dated April 8, 2017 No. 103/2017]. (n. d.). *zakon3.rada.gov.ua*. Retrieved from http://zakon3.rada.gov.ua/laws/show/103/2017 [in Ukrainian].
12. Zakon Ukrainy «Pro ratyfikatsiiu Konventsii pro kiberzlochynnist» [Law of Ukraine "On Ratification of the Convention on Cybercrime"]. (n. d.). *zakon3.rada.gov.ua*. Retrieved from http://zakon3.rada.gov.ua/laws/show/994_575 [in Ukrainian].
13. Zvit shchodo Ukainy 2016/DGI/JP/3608 «Pro chynne zakonodavstvo i proekty zakoniv, shcho dopovniuiut rizni pytannia, poviazani z kiberzlochynnistiu ta elektronnymy dokazamy, ta vnosiat zminy do nyh» [Report on Ukraine 2016/DGI/JP/3608 "On Current Laws and Draft Laws Adding Various Issues Related to Cybercrime and Electronic Evidence" and amend them]. (2016, Nov. 3). *rm.coe.int*. Retrieved from https://rm.coe.int/16806f3743[in Ukrainian].
14. Uhoda pro Asotsiatsiu mizh Ukrainoiu ta Yevropeiskym Soiuzom, z odnoho boku, ta z Yevropeiskoiu Komisiieiu, Yevropeiskym spivtovarystvom z atomnoi enerhii ta ihnimy derzhavamy-chlenamy [Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their Member States]. (n. d.). *zakon2.rada.gov.ua*. Retrieved from http://zakon2.rada.gov.ua/laws/show/984_011/page [in Ukrainian].
15. Klasyfikatsiini oznaky nadzvychainyh sytuatsii, zatverdzheni nakazom Ministra nadzvychainyh sytuatsii Ukrainy vid 12 hrudnia 2012 r. № 1400 [Classification signs of emergencies, approved by the Order of the Ministry of Emergency Situations of Ukraine dated December 12, 2012 No. 1400]. (n. d.). *zakon3.rada.gov.ua*. Retrieved from http://zakon3.rada.gov.ua/laws/show/z0040–13/paran13#n13[in Ukrainian].
16. Polozhennia pro yedynu derzhavnu systemu zapobihannia, reahuvannia i prypynennia terorystychnyh aktiv ta minimizatsii naslidkiv, zatverdgenyh Postanovou Kabinetu Ministriv Ukrainy vid 18 liutoho 2016 r. № 92 [Regulations on a unified state system of prevention, response and termination of terrorist acts and minimization of their consequences, approved by the Resolution of the Cabinet of Ministers of Ukraine dated Feb. 18, 2016]. (n. d.). *zakon3.rada.gov.ua*. Retrieved from http://zakon3.rada.gov.ua/laws/show/92–2016-%D0 %BF [in Ukrainian].