УДК 342.951

ГУРЖІЙ С.В., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-7863-8456.

ЗАСАДИ ІНСТИТУЦІОНАЛЬНО-ФУНКЦІОНАЛЬНОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В СУЧАСНИХ УМОВАХ

Анотація. *Окреслено кіберзагрози в умовах поширення викликів сучасності. Регламентовано заходи з метою посилення спроможностей національної системи кібербезпеки. Деталізовано пріоритетні засади інституційно-функціонального забезпечення розвитку національної системи кібербезпеки. Проаналізовані заходи, які вживаються з метою інституціонального посилення безпеки у кіберпросторі у деяких зарубіжних країнах Висвітлено засади формування вертикалі контролю й координації заходів у сфері кібербезпеки. Окреслено повноваження Національного координаційного центру з кібербезпеки як робочого органу Ради національної безпеки і оборони України. Уточнено повноваження деяких суб'єктів національної системи кібербезпеки з метою уникнення дублювань. Визначено шляхи удосконалення пріоритетних засад інституційно-функціонального забезпечення кібербезпеки виходячи із загрозливих тенденцій сучасності.*

Ключові слова: *кібербезпека, кіберпростір, кіберзагрози, цифровізація, національна система, кібербезпека, оптимізація, інституціонально-функціональне забезпечення кібербезпеки, сектор безпеки і оборони, критична інформаційна інфраструктура.*

Summary. *Cyber threats in the context of the spread of modern challenges are outlined. The measures to strengthen the capacity of the national cybersecurity system are regulated. The priority principles of institutional and functional support for the development of the national cybersecurity system are detailed. The measures taken to institutionally strengthen security in cyberspace in some foreign countries are analyzed. The principles of forming the vertical of control and coordination of measures in the field of cybersecurity are highlighted. The powers of the National Coordination Center for Cyber Security as a working body of the National Security and Defense Council of Ukraine are outlined. The capacities of some actors in the national cybersecurity system have been clarified in order to avoid duplication. The directions of improvements of the priority principles of institutional and functional support of cybersecurity based on the threatening trends of today have been identified.*

Keywords: *cybersecurity, cyberspace, cyberthreats, digitalization, national cybersecurity system, optimization, institutional and functional support of cybersecurity, security and defense sector, critical information infrastructure.*

Аннотация. *Определены киберугрозы в условиях распространения вызовов современности. Регламентировано мероприятия с целью усиления возможностей национальной системы кибербезопасности. Детализированы приоритетные основы институционально-функционального обеспечения развития национальной системы кибербезопасности. Проанализированы меры, которые принимаются с целью институционального усиления безопасности в киберпространстве в некоторых зарубежных странах Освещены основы формирования вертикали контроля и координации мероприятий в сфере кибербезопасности. Очерчены полномочия Национального координационного центра по кибербезопасности как рабочего органа Совета национальной безопасности и обороны Украины. Уточнены полномочия некоторых субъектов национальной системы кибербезопасности во избежание дублирования. Определены пути совершенствования приоритетных основ институционально-функционального обеспечения кибербезопасности исходя из угрожающих тенденций современности.*

Ключевые слова: *кибербезопасность, киберпространство, киберугрозы, цифровизация, национальная система, кибербезопасность, оптимизация, институционально-функциональное обеспечение кибербезопасности, сектор безопасности и обороны, критическая информационная инфраструктура.*

Постановка проблеми. Інтенсивний розвиток інформаційно-комунікаційних технологій (далі – ІКТ), їх широке застосування в усіх сферах життєдіяльності людини створили передумови для формування глобальної інформаційної інфраструктури. У сучасному суспільстві інформаційно-комунікаційні технології є фактором, який визначає рівень соціально-економічного розвитку та стан національної безпеки. Саме тому забезпечення кібербезпеки безпосередньо впливає на розвиток та інформатизацію суспільства, певним чином стимулюючи економічне зростання держав світу. На сьогодні розвиток інформаційного суспільства, поширення інформаційних цифрових технологій в усі сфери життєдіяльності людини та суспільства стали нормою подальшої глобальної еволюції цивілізації. Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачати нові можливості для цифровізації всіх сфер суспільного життя.

Становлення та динамічний розвиток ІКТ, та, як наслідок, входження в нову інформаційну еру, формування сучасного інформаційного суспільства в провідних країнах світу, з одного боку, а також переосмислення ролі та значення людини, її прав і свобод щодо інтересів держави в ракурсі її пріоритету, з іншого, спричинили необхідність динамічного розвитку вітчизняного та міжнародного законодавства у сфері кібербезпеки, яке повинно відповідати сучасним викликам шляхом формування ефективних механізмів протидії можливим правопорушенням та загрозам у кіберпросторі, вироблення моделі адекватного реагування на їх поширення та суцільну ліквідацію.

Прискорений розвиток та взаємопроникнення ІКТ поряд з потужними соціально значимими перевагами супроводжується масштабуванням кіберзагроз у всіх сферах життєдіяльності, їх еволюцією в бік високотехнологічних рішень та урізноманітненням інструментарію реалізації. Докорінно змінюючи світовий життєустрій, пандемія коронавірусу COVID-19 матиме довготривалий вплив на світовий порядок. Зростає залежність від цифрових комунікацій, що робить вразливим процес обміну інформацією, захисту інформації та персональних даних. Кіберзлочинці, максимально використовуючи тему пандемії, від її початку дедалі більше застосовують нові методи проведення кібератак, що змушує національні уряди впроваджувати додаткові механізми протидії, збереження доступу до необхідних пристроїв, належного функціонування всіх потрібних для життя та роботи важливих електронних ресурсів і відповідних систем. З огляду на це, висвітлення проблемних питань оптимізації інституційної системи забезпечення кібербезпеки залишається важливим та актуальним як з позиції фундаментальної базової теорії, так і практики її застосування.

Результати аналізу наукових публікацій. Питання організаційно-правового забезпечення кібербезпеки досліджували у своїх наукових працях такі фахівці: І. Діордиця [1], І. Доронін [2], Н. Ткачук [3], В. Шеломенцев [4] та інші. Проте деталізацію засад перспективного інституційно-функціонального забезпечення розвитку кібербезпеки жоден із вказаних авторів не здійснював, особливо в умовах масштабного поширення гібридних загроз та глобального інформаційного протистояння.

Метою статті є визначення перспективних засад інституційно-функціонального забезпечення кібербезпеки в умовах поширення гібридних загроз та викликів сучасності.

Виклад основного матеріалу. З 2014 року Росія активно використовує кіберпростір у гібридній агресії проти України шляхом здійснення деструктивного впливу на органи державної влади, системи управління військами, а також на об'єкти критичної інфраструктури. Держава-агресор невпинно нарощує арсенал кіберзброї наступального, розвідувального та підривного призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Зазначені чинники вимагають постійного нарощування можливостей забезпечення кібербезпеки органами сектору безпеки і оборони. Надзвичайно актуальною загрозою на сьогодні є розвідувально-підривна діяльність у кіберпросторі проти України, яка пов'язана з проведенням спецслужбами іноземних держав, насамперед РФ, розвідувальної діяльності з метою викрадення інформації (кібершпигунство) та підривних акцій з порушення штатного режиму функціонування об'єктів критичної інформаційної інфраструктури, передусім систем управління державою, об'єктів життєзабезпечення, електроенергетики, транспорту, ядерної і хімічної промисловості, банківської сфери (актів кібердиверсій).

За таких умов, активізація посилення спроможностей національної системи кібербезпеки здійснюється шляхом виконання стратегічних завдань на планових засадах, спрямованих на досягнення визначених цілей. Враховуючи викладене, для України актуальним залишається інституціональна розбудова національної системи кібербезпеки, оскільки як переконливо доводить набутий досвід, діяльність її суб'єктів залишається недостатньо скоординованою й такою, що спрямована на виконання лише поточних завдань. За результатами експертних оцінок, стан та ефективність реалізації Стратегії кібербезпеки України за визначеними показниками не перевищує 40 %. Невирішеними залишаються питання оперативного обміну інформацією про кіберзагрози, налагодження ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства.

Однією із виявлених сучасних проблем стала недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була не конкретною. Протягом 2014 – 2020 років повільно здійснювався розвиток спроможностей основних суб'єктів національної системи кібербезпеки, була зафіксована обмеженість ресурсного забезпечення функціонування цієї системи, відсутність належної державної підтримки розвитку її інституційного забезпечення. Таким чином, інституціоналізація сфери забезпечення кібербезпеки – це перманентний процес створення відповідних органів державного управління, належного правового регулювання відносин у кіберпросторі, які виникають між громадянами, суспільством, державою, з метою недопущення будь-яких проявів кібертероризму, запобігання кіберзагрозам і кібератакам, ефективності заходів боротьби з кіберзлочинністю. Кардинальні зусилля держави мають бути спрямовані та активізовані на створення потужної багаторівневої інституційної системи кібербезпеки, яка була би здатна захистити не тільки громадян і суспільство, а й державні органи, приватний сектор. Інституційна система кібербезпеки має включати сукупність компонентів, серед яких важливе місце посідають: цифрова грамотність та обізнаність населення, сучасні засоби захисту особистої інформації в кіберпросторі, кіберзахист державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, розроблення методів запобігання кібератакам та оприлюднення інформації про них, упровадження механізмів попередження та профілактики кіберзагроз тощо.

Поширення ландшафту загроз та ускладнення інструментарію їх реалізації спонукає уряди провідних країн удосконалювати архітектуру національних систем кібезбезпеки, змінювати стратегію і тактику протидії кіберзагрозам. Вносяться зміни до моделі протидії кіберзагрозам, які пов'язані з розумінням недостатньої можливості побудувати абсолютно невразливі системи захисту. Як демонструє практика, будь-які інформаційно-комунікаційні системи можуть бути уражені внаслідок кібератаки незалежно від рівня їх захисту. Тому набуває значимості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди.

Глобальне протистояння в кіберпросторі є небезпечною складовою гібридної війни, розв'язаної проти України, у зв'язку з чим Україні потрібно швидко, надійно та ефективно реагувати на будь-які кіберзагрози, що неможливо без інтегрування та чіткої взаємодії всіх наявних ресурсів суб'єктів забезпечення кібербезпеки. Таким чином, крім відпрацювання ефективного реагування на кібератаки та кіберінциденти, доцільно вибудувати активний захист кіберпростору, створюючи належні умови для інституційно-функціонального забезпечення кібербезпеки. Проте становлення інституційної системи кібербезпеки ускладнюється низкою поточних факторів, серед яких передусім виділяється невідповідний та неефективний механізм міжвідомчої координації, наявність широких дублювань у сфері їх функціональності та компетенції.

Розуміючи сучасний стан та актуальність проблеми забезпечення кібербезпеки, більшість країн світу вживають комплексних заходів щодо безпеки в кіберпросторі, які пов'язані передусім з розробкою та вдосконаленням нормативно-правової бази, що регулює питання сфери кібербезпеки, а також створюють відомчі та державні структури, що відповідають за забезпечення кібербезпеки. Спеціальні служби різних країн вивчають методи діяльності хакерських груп, а іноді навіть активно співпрацюють з ними, використовуючи їхні знання та навички при проведенні кібернетичних операцій, пропонуючи їм натомість лояльність та захист. У рамках посилення інституційних спроможностей забезпечення кібербезпеки на початку 2019 року керівники трьох американських спецслужб ЦРУ, АНБ і ФБР офіційно заявили, що смартфони Huawei та ZTE можуть стежити за користувачами та здійснювати шпигунську діяльність.

Можна констатувати, що переважна більшість країн світу на державному рівні опікується питаннями створення та ефективного функціонування парадигми кібербезпеки, яка має такі інституційні ознаки: формуються відповідні правові норми переважно у форматі стратегій кібербезпеки та спеціальних актів законодавства, розробляються пріоритетні засади державної політики у сфері забезпечення кібербезпеки, створюються уповноважені державні органи, які відповідають за стан забезпечення кібербезпеки, динамічно розвиваються нові інтерактивні сфери, що орієнтуються на запобігання кібератакам, системну боротьбу з кіберзлочинністю, кібертероризмом, розробляються та постійно вдосконалюються технології захисту інформації та апаратно-програмного забезпечення в інформаційно-комунікаційних мережах тощо.

У сучасному світі понад 65 держав мають власні національні стратегії кібербезпеки, в яких акцент робиться на зменшенні та усуненні факторів ризиків для суспільства і громадськості. При цьому кожна країна визначає найбільш важливі для неї загрози та вразливості в кіберпросторі, тому не існує однакових національних стратегій кібербезпеки. Аналіз переважної більшості стратегій кібербезпеки надає змогу визначити їх основні позиції: підтримка та гарантування безпечного та захищеного кіберпростору, створення довірчого середовища електронних комунікацій; усунення ризиків для ІКТ; посилення спроможностей і стійкості критичної інформаційної інфраструктури; підтримка та підвищення рівня економічного потенціалу, соціального

благополуччя населення. Наприклад, у квітні 2014 року Національний конгрес Бразилії затвердив т.зв. "Біль Марко", більш відомий як "Інтернет-Конституція Бразилії", яким задекларовано права та свободи особи й громадянина в Інтернет-просторі, а також механізми їх забезпечення й додержання. Цей закон став відправною точкою для створення власної, окремої від США, національної системи в кібернетичній сфері. Із набранням чинності цим законом державним службовцям та військовослужбовцям Бразилії нормативно заборонено використання в службовій діяльності послуг постачальників електронної пошти з США. У 2015 році в Бразилії розпочато реалізацію великомасштабного проекту щодо прокладання Інтернет-кабелю з Європи до Бразилії по дну Атлантичного океану в обхід США, а в перспективі очікується також створення аналогічних Інтернет-мереж між Бразилією та Африкою. У 2017 році Уряд Бразилії схвалив рішення про створення підрозділів кіберполіції та активізував інституціоналізацію співробітництва в цьому напрямі між Бразилією та Європолом.

Індія посідає одне з перших місць у світі за кількістю скоєних кіберзлочинів на душу населення та масштабами поширення шкідливого програмного забезпечення. У 2013 році в Індії створено Національний центр захисту об'єктів критичної інфраструктури та розпочала свою діяльність кіберполіція. У лютому 2017 року команда реагування на кіберінциденти (CERT-In) розпочала впровадження проекту "Cyber Swachha Kendra", який є частиною ініціативи Уряду "Цифрова Індія" під егідою Міністерства електроніки та інформаційних технологій щодо створення безпечного кіберпростору шляхом виявлення інфікованих ботнетів та аналізу шкідливих програм кінцевих користувачів.

У Південно-Африканській Республіці (ПАР) ще у 2010 році вперше були створені спеціальні підрозділи кіберполіції, основним завданням яких стало відстеження та боротьба з кіберзлочинністю. У 2016 році Уряд ПАР оприлюднив регламент "Про кіберзлочинність", у положеннях якого першочерговим завданням визначено суцільну інформатизацію суспільства, органів державної влади та правоохоронних органів як складових забезпечення національної безпеки. На виконання положень цього програмного документа у 2017 році за сприяння Уряду країни було утворено Центр кібербезпеки при Національному університеті Йоганнесбурга, який здійснює підготовку кадрів, розробляє нормативно-правові основи регулювання інформаційного простору ПАР, забезпечує інформаційно-технічну підготовку кадрів для урядових структур та проводить науково-дослідницьку діяльність у сфері кібербезпеки.

Провідну роль у системі інформаційного захисту Фінляндії відіграє Стратегія кібербезпеки 2013 року, що стала першим самостійним документом у цій сфері. У Стратегії визначено ключові орієнтири стосовно забезпечення кібербезпеки, а також реальні для виконання положення щодо досягнення бажаного кінцевого результату захисту інформаційного простору та гарантування цифрового суверенітету. Так, відповідальними за розробку та реалізацію політики у сфері захисту національного кіберпростору у Фінляндії є урядові та неурядові структури, які здійснюють постійний нагляд і контроль за поточним станом інформаційного захисту. Із 2014 року у Фінляндії функціонує Національний центр з кібербезпеки, діяльність якого спрямована на забезпечення безпеки в кіберпросторі, надання гарантованого захисту та доступу користувачам (державним і приватним), які використовують інформаційно-комунікаційні мережі загального та спеціального зв'язку, долаючи при цьому всі можливі кіберзагрози, а також створення сприятливих умов для підтримки найважливіших соціальних функцій держави. У зв'язку з подальшим поширенням використання у злочинній діяльності ІКТ правоохоронним органам слід розробляти нові

методологічні підходи у боротьбі з новими видами злочинної діяльності та створювати відповідні організаційні структури.

Таким чином, інституційна система забезпечення кібербезпеки – сукупність організаційних структур, які забезпечують функціонування державного механізму забезпечення безпеки в кіберпросторі та дієвого кіберзахисту державних інформаційних ресурсів й об'єктів критичної інформаційної інфраструктури, а її оптимізація – один з аспектів організаційного розвитку. Метою оптимізації інституційної системи забезпечення кібербезпеки є визначення заходів та механізмів, завдяки яким гарантується безпека в кіберпросторі, що, у свою чергу, передбачає проведення у стислі терміни огляду наявних сил, засобів і можливостей нарощування потенціалу для реагування на кіберзагрози та кіберінциденти за участю усіх компетентних державних органів, впровадження в практичну площину механізмів взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки. З огляду на це важливим аспектом діяльності державного апарату в напрямі розбудови системи кібербезпеки залишається визначення алгоритму роботи різних національних структур для виконання покладених на них функцій відповідно до вимог сучасного вітчизняного законодавства.

Крім того, має бути побудована чітка вертикаль контролю і координації заходів у сфері кібербезпеки, впроваджені дієві механізми мобілізації ресурсів та оперативного реагування на кіберзагрози з використанням принципу асиметричної відповіді. Саме критична інформаційна інфраструктура є технологічним плацдармом життєдіяльності інформаційного суспільства, від сталого та надійного функціонування всіх її складових залежить стан забезпечення кібербезпеки, можливість управління державою, забезпечення потреб оборони та безпеки, функціонування промисловості, кредитно-фінансової та банківської систем, енергетичних, транспортних інфраструктур, комунального господарства, цивільного захисту, адже в державі ще й досі не сформовано повної та систематизованої бази даних про топологію і наявні ресурси телекомунікаційних мереж загального користування, що перебувають у приватній власності, а також відомчих телекомунікаційних мереж, побудованих за державні кошти.

Отже, кібербезпека відноситься до заходів безпеки та дій, які можуть використовуватися для захисту кіберпростору як у цивільній, так і військовій сферах, від таких загроз, які пов'язані або можуть пошкодити міжнародні інформаційно-комунікаційні мережі або об'єкти критичної інформаційної інфраструктури. Завдяки кібербезпеці забезпечується доступність і цілісність мереж та інфраструктури, а також конфіденційність інформації, яка в них циркулює. Проте ще й досі держава не володіє достовірними даними щодо сталості та надійності цих мереж, стану завантаженості, динаміки розвитку. Відсутні також достатні технічні вимоги до телекомунікаційних мереж щодо забезпечення сталості та живучості, у зв'язку з чим унеможливлюються: організація централізованого моніторингу стану мережевих та інформаційних ресурсів, моніторингу кібератак; контроль сталості кібербезпеки і ефективного використання ресурсів усіх мереж в умовах критичних ситуацій, надзвичайного або воєнного стану відповідно до чинного законодавства. Інакше кажучи, навіть, якщо захист державних інформаційних систем має регламентовані законодавством механізми, то, наприклад, налагодження комплексної взаємодії приватного сектору та держави щодо кіберзахисту об'єктів критичної інформаційної інфраструктури передбачає розробку нових методик з урахуванням інтересів IT-бізнес-середовища та відповідного стимулюючого ефекту, оскільки більшість таких об'єктів перебуває у віданні саме комерційних структур. Також необхідною є розробка методики оцінки та управління ризиками в вітчизняному сегменті кіберпростору.

Оскільки державні органи та правоохоронні структури – суб'єкти забезпечення кібербезпеки фізично не мають можливості захистити комерційні підприємства та організації, вони повинні самостійно забезпечувати власну кібербезпеку, при цьому державні структури виконують координаційні та контрольні функції. За таких умов необхідно: законодавчо визначити, що відповідальність за забезпечення кіберзахисту об'єкта критичної інформаційної інфраструктури покладається на його власника, який зобов'язаний надавати суб'єктам забезпечення кібербезпеки відомості про об'єкт критичної інформаційної інфраструктури; утворювати у своїй структурі підрозділ забезпечення кібербезпеки або уповноважувати окремих осіб на виконання функцій такого підрозділу та забезпечувати їх функціонування; негайно інформувати Держспецзв'язку про будь-які спроби вчинення стосовно об'єкта критичної інформаційної інфраструктури кібератак та інших несанкціонованих дій, а також здійснювати заходи щодо блокування, усунення або локалізації їх негативних наслідків. Формування чіткої вертикалі контролю й координації заходів у сфері кібербезпеки передбачає ієрархічну побудову системи її компетентних органів, у межах якої відповідальними суб'єктами надається розпорядницька та звітна інформація в чітко встановлені строки про здобуті результати з метою подальшого інформування керівництва держави, а в разі необхідності – світової спільноти.

Водночас координування з питань забезпечення кібербезпеки має відбуватися на двох рівнях – стратегічному та оперативному. Стратегічне координування є сферою відповідальності РНБО України, а саме Національного координаційного центру кібербезпеки як робочого органу РНБО України, оперативне – Кабінету Міністрів України. Адже недостатня координація досить часто призводить до негативних явищ у сфері практичних дій суб`єктів забезпечення кібербезпеки. З огляду на це, завданням держави є розробка та впровадження ситуативної моделі управління ризиками в кіберпросторі, визначення алгоритму дій суб`єктів забезпечення кібербезпеки, порядку та умов їх комплексної взаємодії, здійснення поточної та перспективної оцінки стану забезпечення кібербезпеки, контролю за результатами виконання планово-звітної документації.

Актуальним та важливим напрямком стало посилення спроможностей Національного координаційного центру кібербезпеки як робочого органу РНБО України. У зв'язку з тим було змінено формат його діяльності, зокрема, до його роботи відповідно до Указу Президента України від 28.01.20 р. № 27 залучено фахівців з приватного сектору, які спеціалізуються на кіберзахисті. Одночасно було акцентовано увагу на головній меті діяльності Національного координаційного центру кібербезпеки: залучити технологічний та інженерний потенціал прямих виробників до співпраці з Центром; використати існуючу в Україні інсталяційну базу на об'єктах критичної інфраструктури; поглибити співпрацю із суб'єктами кібербезпеки та приватними компаніями у рамках державно-приватного партнерства. В даному контексті слід вказати, що ефективність системи забезпечення кібербезпеки безпосередньо залежить від можливостей її постійного вдосконалення на фоні щоденного виникнення нових загроз у кіберпросторі, оскільки результати успішних інцидентів у кіберпросторі обмежуються не лише тимчасовими незручностями, але й призводять до тяжких наслідків для держави в економічній та соціальній площинах.

Розбудову інституційної системи забезпечення кібербезпеки також неможливо уявити без створення оптимальної управлінської організаційної ланки та залучення професійного людського кадрового ресурсу. Така модернізація вимагає часу та достатніх як фінансових, так і технічних ресурсів, відповідного кадрового потенціалу. Адже побудова дієвої системи кіберзахисту без її поступової модернізації деградує, передусім, через те, що інформаційні системи досить швидко розвиваються, а процес

створення відповідних систем захисту іноді не встигає за динамічним ІТ-розвитком. Хоча існують й здобутки у цій сфері. Так, у Національному координаційному центрі кібербезпеки РНБО України було створено реєстр обміну інформацією щодо кіберінцидентів з метою вчасного реагування на них у режимі реального часу та прямого зв'язку. Подібні центри вже існують в усіх передових державах світу, а їх робота визнається ефективною та результативною. Ці структури повинні обмінюватися інформацією. Отже, Національний координаційний центр кібербезпеки РНБО України має тісно взаємодіяти з міжнародними партнерами для вчасного реагування на кіберзагрози. Однак, на жаль, з точки зору розвитку системи кібербезпеки можна констатувати, що для спільної протидії викликам та загрозам в кіберпросторі не вистачає координованості зусиль як між державними структурами, міжнародними партнерами, так і між державою та приватним сектором.

Останнім часом Україна залишається мішенню для російських та проросійських кіберзлочинців. Кібератаки, також фіксувалися і проти інших держав, зокрема під час попередньої президентської кампанії у США та голосувань у країнах Європи (Великобританія, Нідерланди, Франція). Наведемо кілька останніх прикладів: Британія звинуватила хакерів, підконтрольних СЗР РФ, у втручанні в парламентські вибори 2019 року. Крім того, Лондон, Вашингтон та Оттава звинуватили Кремль у спробі вкрасти дані про вакцину від COVID-19. Також, нещодавно ЄС застосував санкції до російських хакерів, які були причетні до атаки "NotPetya", яка, зокрема, була встановлена за допомогою українських правоохоронців.

Загалом кібератаки завдали мільярдних збитків. Вони дали зрозуміти, наскільки ефективна кіберзброя в руках противника аби паралізувати будь-яку країну. Важливим завданням українського політичного істеблішменту є також залучення фахівців до кола суб'єктів забезпечення кібербезпеки, використання сучасних технічних засобів, апаратно-програмних комплексів, високоякісної ІТ-продукції. Забезпечення кібербезпеки неможливо уявити без людських ресурсів. Однак рівень кадрового забезпечення відомств відповідними фахівцями у сфері кібербезпеки все ще є незадовільним.

Оскільки структурно забезпечення кібербезпеки здійснюється у двох стратегічних напрямах: цивільному та військовому секторах, то важливим завданням держави в умовах оптимізації інституційної системи забезпечення кібербезпеки залишається дієвість і контрольованість заходів, спрямованих на підтримку зазначених векторів, які повинні розвиватися комплексно та системно.

У контексті військового сектору необхідно вказати, що спеціальні завдання, які здатна виконувати ворожа кіберзброя, мають переважно чітко виражений військовий характер. Тому для України доцільним є запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони. Йдеться про утворення у складі Збройних Сил України окремого роду військ – "Сили кібероборони" ("MilCert"), їх забезпечення належними фінансовими, кадровими і технічними ресурсами для стримування збройної агресії у кіберпросторі та надання відсічі агресору. З цією метою слід розробити загальнодержавний план кібероборони в контексті забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів та оглядів у сфері кібербезпеки тощо.

Актуальним напрямом діяльності держави щодо оптимізації інституційної системи забезпечення кібербезпеки також залишається інформаційно-роз'яснювальна робота з метою профілактичного впливу на свідомість суспільства щодо негативних наслідків і масштабів збитків від кіберзагроз, кіберзлочинності та кібертероризму. У зв'язку із цим

необхідними є проведення просвітницької роботи з населенням з питань забезпечення кібербезпеки, роз'яснення методів протидії сучасним кіберзагрозам, надання консультативної допомоги в питаннях протидії злочинній діяльності в кіберпросторі, створення вітчизняних експертних інформаційно-аналітичних центрів, які б спеціалізувалися на питаннях кіберзахисту.

З огляду на це, слід зазначити, що незалежно від політичного курсу будь-якої країни світу Інтернет став технологічною інновацією, що наразі потребує інноваційного підходу до інституційної та регуляторної сфери. Надмірна політизація питання управління Інтернетом та нормативних засад розвитку кіберпростору знижують ефективність інституційних платформ, що сьогодні діють у цій сфері. У зв'язку з цим невирішеними залишаються питання протидії кібершпигунству, ідентифікації суб'єктів у кіберпросторі, мережевої нейтральності, юрисдикції в мережі Інтернеті тощо. Крім того, множинність інституційних механізмів може зрештою призвести до небажаної фрагментації екосистеми Інтернету.

Гібридна війна, розгорнута державою-агресором проти України, поряд з класичними воєнними діями та інформаційно-психологічними операціями, включає в себе й проведення кібероперацій. Державне управління процесами забезпечення сфери кібербезпеки має бути спрямоване на вирішення таких функціональних завдань щодо:

планування та контролю – оцінка ризиків та заходи щодо їх усунення, координація діяльності суб'єктів її забезпечення;

забезпечення кіберзахисту – проектування та практична реалізація заходів захисту критичної інформаційної інфраструктури, розроблення вимог щодо захисту державних інформаційних ресурсів та контроль за їх виконанням, розроблення вимог щодо безпечного використання Інтернету та електронних послуг;

оперативного реагування – оперативне реагування на кіберінциденти, розроблення методики попередження кіберінцидентів;

науково-методологічної підтримки – проведення наукових досліджень у сфері кібербезпеки, розроблення відповідних галузевих стандартів;

розслідування та попередження кіберзлочинів – розслідування кіберзлочинів, запровадження особливостей щодо судового провадження у сфері кіберзлочинів.

За таких умов для України прискорення оптимізації інституційної системи забезпечення кібербезпеки є дієвим інструментом, який передбачає два ключових напрями: правовий та організаційний.

Правовий полягає в ініціативній розробці необхідної нормативної бази та її постійному удосконаленні з метою формування відповідних правових норм, які знаходять відображення в Стратегії кібербезпеки та Законі України "Про основні засади забезпечення кібербезпеки України".

Організаційний – у підвищенні ефективності діяльності відповідальних інституційних структур – суб'єктів забезпечення кібербезпеки, міністерств, інших центральних органів виконавчої влади та інституцій громадянського суспільства завдяки підвищенню їх спроможностей, усуненню дублювань під час реалізації своїх повноважень, об'єднання зусиль під егідою робочого органу РНБО України – Національного координаційного центру кібербезпеки з урахуванням кращих практик міжнародного та європейського досвіду в цій площині.

Відповідно до компетенції РНБО України відповідає за координацію діяльності у сфері забезпечення кібербезпеки як важливої складової національної безпеки України. На жаль, в Україні відсутній комплексний звіт на національному рівні про процеси, пов'язані із поширенням та оцінкою стану кіберзлочинності, в якому можуть бути

окреслені загрози та визначені рекомендації щодо їх подолання та недопущення, в тому числі й транснаціонального характеру. Як переконливо демонструє провідний зарубіжний досвід, інституційно-функціональне забезпечення кібербезпеки передбачає два основних напрями: утворення підрозділів кіберполіції, розширення їх компетенції та утворення Національних центрів з кібербезпеки. В Україні актуальним залишається питання динамічної розбудови національної системи кібербезпеки. Важливим здобутком стало відкриття створеного Держспецзв'язку Центру реагування на кіберзагрози ("Cyber Threat Response Centre" – CRC) як центрального компоненту та ядра національної системи кіберзахисту. У своїй діяльності Центр реагування на кіберзагрози використовує кращі світові аналоги сучасних технологічних та аналітичних систем. Головним завданням вказаної структури стало запобігання кібератакам та максимальна локалізація можливих та потенційних уражень.

Ретельний аналіз положень Закону України "Про основні засади забезпечення кібербезпеки України" [5] надає змогу констатувати, що в його положеннях чітко розмежовуються функції між правоохоронними органами та вітчизняною спецслужбою. За стратегічне управління та координацію діяльності відомств, що забезпечують кібербезпеку, відповідає РНБО, якій підпорядкована Держспецзв'язку. Остання має розробляти комплексну систему кіберзахисту стратегічних об'єктів і контролює діяльність компаній, які проводять аудит таких стратегічних об'єктів. Держспецзв'язку підпорядкований Державний центр реагування на кібератаки, підрозділ якого – CERT-UA проводить моніторинг і виявляє потенційні кіберзагрози. Кіберполіція України відповідає за стан запобігання та розслідування кіберзлочинів. Міноборони та Генштаб забезпечують охорону військових об'єктів та об'єктів критичної інфраструктури під час війни та надзвичайного стану. СБУ здійснює запобігання терористичним атакам в кіберпросторі та має право перевіряти об'єкти критичної інфраструктури. Перелік об'єктів, що належать до критичної інфраструктури, визначає Кабінет Міністрів України, а кібербезпекою в банківській сфері опікується Національний банк України.

Однак законодавчо не визначено сфер відповідальності між різними державними та правоохоронними органами. Іншими словами, Закон України "Про основні засади забезпечення кібербезпеки України" [5] визначає базові поняття та передбачає, з одного боку, відповідальність керівників підприємств, установ та організацій за можливі кіберінциденти, з іншого боку, за кібербезпеку відповідають усі державні структури: Кабінет Міністрів України, Нацполіція, СБУ, Держспецзв'язку та Міноборони, НБУ, але виключно абстрактно.

Отже, якщо Україну раптом знову вразить вірус на військових об'єктах, то відповідальність мають нести Міноборони чи Генштаб і СБУ, якщо кібератака розцінюється як терористичний акт. Проте практично впровадити систему кіберзахисту, передбачену вказаним законом, навіть у державних органах досить складно. У рамках розбудови інституційного забезпечення кібербезпеки необхідно врегулювати організаційно-правові засади, на яких має бути побудована архітектура кібербезпеки об'єктів критичної інфраструктури, оскільки в Законі України "Про основні засади забезпечення кібербезпеки України" не визначено переліку об'єктів, що належать до такої інфраструктури, а також ще й досі не розроблені підзаконні акти, які мають регулювати нормативи кібербезпеки на таких об'єктах. Ураховуючи викладене, потребує удосконалення механізм співпраці та комплексної взаємодії між суб'єктами забезпечення кібербезпеки шляхом створення єдиної інтерактивної бази даних про кіберінциденти для ключових потреб Міноборони, Держспецзв'язку, СБУ, НПУ, НБУ, розвідувальних органів. Доцільним є також прискорення імплементації у вітчизняне

законодавство Директиви (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року щодо заходів із підвищення загального рівня безпеки мереж та інформаційних систем.

У зазначеному контексті важливим кроком має стати розбудова національної системи кібербезпеки, що передбачає: координацію дій та заходів, які вживаються державними органами, іншими суб'єктами забезпечення кібербезпеки, посилення спроможностей сектору безпеки і оборони, консолідацію зусиль та об'єднання знань, досвіду, потенціалу та ситуативної інформованості державного і приватного секторів. Також посилення спроможностей національної системи кібербезпеки неможливе без урегулювання питання щодо заборони державним органам, підприємствам, установам і організаціям державної форми власності закуповувати послуги (укладати договори) з доступу до мережі Інтернет в операторів (провайдерів) телекомунікацій, у яких відсутні документи про підтвердження відповідності системи захисту інформації встановленим вимогам захисту інформації; щорічного збільшення видатків на фінансування з метою модернізації ситуаційних центрів з кібербезпеки СБУ та Держспецзв'язку; забезпечення суцільної модернізації та розширення функціональних можливостей системи інформаційного обміну про кіберзагрози між відповідальними суб'єктами; активізації співпраці між СБУ та Держспецзв'язку із зарубіжними партнерами щодо протидії кібератакам на критичну інформаційну інфраструктуру, проведення спільних розслідувань таких кібератак, установлення причин і умов, що сприяли їх вчиненню, а також щодо залучення міжнародної технічної допомоги для забезпечення кіберзахисту державних електронних інформаційних ресурсів.

Висновки.

З метою покращення координації діяльності суб'єктів забезпечення кібербезпеки в Україні у 2016 році було утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки на правах робочого органу, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері. На цьому фоні Україна має необхідний потенціал для нарощування спроможностей у сфері кібербезпеки для адекватної протидії сучасним викликам і загрозам.

Проте, на жаль, в сучасних умовах зберігається загрозлива тенденція активного застосування й поєднання традиційних та нетрадиційних стратегій і тактик з використанням цифрових інформаційних технологій. Зокрема, держава-агресор активно впроваджує концепцію інформаційного протиборства, яка базується на симбіозі бойових дій у кіберпросторі та інформаційних операцій, механізми якої активно застосовуються в процесі гібридної війни проти України.

Провідні держави ЄС, держави-члени альянсу НАТО, провідні міжнародні корпорації та експерти одностайно визнають РФ та її дії у кіберпросторі головною загрозою міжнародній кібербезпеці. Її активна розвідувально-підривна діяльність у кіберпросторі є частиною гібридної війни, яку вона веде проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури. Прогнозується зростання інтенсивності міждержавного протиборства і розвідувально-підривної діяльності у кіберпросторі, яке проявлятиметься, насамперед, у розширенні кола держав, які намагатимуться сформувати власну кіберрозвідку, оволодіти сучасними технологіями розвідувально-підривної діяльності у кіберпросторі. Очікується розроблення інструментарію, що передбачає накопичення великих масивів даних та інформації щодо оцінки відомостей про людину, соціальних груп та використовує їх у сфері штучного інтелекту.

Важливим компонентом розвитку інституціонального забезпечення кібербезпеки для України є обов'язкове щорічне оприлюднення публічного звіту про стан реалізації та виконання Стратегії кібербезпеки за загальними оцінками. Саме Національний координаційний центр кібербезпеки у визначених законодавством формах має забезпечувати планування та забезпечення виконання заходів з реалізації Стратегії кібербезпеки, координує їх проведення і контролює стан виконання та ефективність. У рамках посилення інституціонального забезпечення кібербезпеки доцільно розширити мережі обміну інформацією про кібератаки, кіберінциденти та індикатори кіберзагроз на базі технологічної платформи Національного координаційного центру кібербезпеки, охопивши всі державні органи та об'єкти критичної інфраструктури, уніфікації форматів обміну інформацією; запровадити за досвідом держав-членів ЄС скоординованого виявлення та розкриття вразливостей інформаційно-комунікаційних систем під егідою Національного координаційного центру кібербезпеки, запровадити механізми заохочення приватного сектору, наукового співтовариства, громадських організацій та окремих громадян до участі у формуванні та реалізації заходів із забезпечення кібербезпеки держави. Також актуальним є запровадження обов'язкового надання в режимі реального часу інформації про кібератаки та кіберінциденти всіма відомчими та галузевими (секторальними) центрами до Національного координаційного центру кібербезпеки.

Важливим та ефективним напрямом має стати розробка нових національних стандартів у сфері кібербезпеки, зокрема впровадження міжнародного стандарту ISO 27001, розвиток організаційно-технічної моделі кіберзахисту, впровадження механізмів своєчасної ідентифікації кіберзагроз, виявлення кібератак з метою оперативного й адекватного реагування на них та швидкого відновлення стабільної роботи за їх наслідками; запровадження загальнонаціональної програми виявлення уразливостей інформаційно-комунікаційних систем, проведення на регулярній основі аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість тощо.

Використана література

1. Діордіца І.В. Поняття та зміст національної системи кібербезпеки. *Jurnalul juridic naţional: teorie şi practică.* 2016. № 6(22). С. 33-38.

2. Доронін І.М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави. *Інформація і право.* № 1(20)/2017. С. 104-111.

3. Ткачук Н. Стан та проблемні питання реалізації стратегії кібербезпеки України. *Інформація і право.* № 1(28)/2019. С. 129-134.

4. Шеломенцев В.П. Основні проблеми побудови системи кібернетичної безпеки України *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. № 2. С. 183-186. URL: http://nbuv.gov.ua/UJRN/ boz_2014_2_44

5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

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