Інформаційна і національна безпека

УДК 342.951

МАНУІЛОВ Я.С., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-8149-2745.

ОГЛЯД НОВЕЛ ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ (НА ПРИКЛАДІ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ НА 2021 – 2025 РОКИ)

Анотація. *Проаналізовано положення оновленої Стратегії кібербезпеки України. Визначено результативність Стратегії кібербезпеки України 2016 року. Досліджено питання організаційно-правових засад забезпечення кібербезпеки. Розглянуто складові національної системи кібербезпеки. Деталізовано практичну складову Стратегії кібербезпеки України та пріоритетні завдання сектору безпеки і оборони. Висвітлено стратегічні засади забезпечення кібербезпеки в Японії. Узагальнено перспективи реалізації Стратегії кібербезпеки України в умовах сучасного геополітичного протиборства.*

Ключові слова: *національна система кібербезпеки, стратегічне планування, кіберзагроза, кіберпростір, сектор безпеки і оборони, кібератака.*

Summary. *The provisions of the updated Cyber Security Strategy of Ukraine are analyzed. The effectiveness of the Cyber Security Strategy of Ukraine in 2016 has been determined. The issue of organizational and legal bases of cyber security is studied. The components of the national cyber security system are considered. The practical component of the Cyber Security Strategy of Ukraine and the priority tasks of the security and defense sector are detailed. The strategic principles of cyber security in Japan are highlighted. The prospects of implementation of the Cyber Security Strategy of Ukraine in the conditions of modern geopolitical confrontation are generalized.*

Keywords: *national cyber security system, strategic planning, cyber threat, cyberspace, security and defense sector, cyber attack.*

Аннотация. *Проанализированы положения обновленной Стратегии кибербезопасности Украины. Определена результативность Стратегии кибербезопасности Украины 2016 года. Исследованы вопросы организационно-правовых основ обеспечения кибербезопасности. Рассмотрены составляющие национальной системы кибербезопасности. Детализирована практическая составляющая Стратегии кибербезопасности Украины и приоритетные задачи сектора безопасности и обороны. Освещены стратегические основы обеспечения кибербезопасности Японии. Обобщены перспективы реализации Стратегии кибербезопасности Украины в условиях современного геополитического противостояния.*

Ключевые слова: *национальная система кибербезопасности, стратегическое планирование, киберугроза, киберпространство, сектор безопасности и обороны, кибератака.*

Постановка проблеми. Світ активно входить в нову епоху цифровізації. XXI століття знаменується активним формуванням шостого технологічного укладу (біо-, нано-, інфо-, когнотехнологій, їх конвергенцією) та потенційними ризиками, з якими стикається світова спільнота внаслідок масштабного впровадження новітніх технологій, зокрема їх використання у кіберпросторі. Значення кіберпростору в розвитку цивілізації

повсякденно зростає і поступово перетворюється на одну зі сфер міждержавного протиборства. Кіберпростір разом з іншими фізичними просторами у світовому масштабі визнано одним з можливих театрів воєнних дій, тому спроможність держави захищати національні інтереси в ньому розглядається як важлива складова кібербезпеки. Сучасна геополітика постійно стимулює діяльність політичного керівництва країн, спрямовану на пошук ефективної моделі оперативного управління кібербезпекою, підвищення ролі і значення реалізації заходів щодо розбудови її національної системи.

За оцінками експертів у сфері кібербезпеки, у переважній більшості провідних країн світу спостерігається стійка тенденція до значного збільшення кількості та розширення спектру кібератак з метою порушення конфіденційності, цілісності і доступності державних інформаційних ресурсів, зокрема тих, що циркулюють на об'єктах критичної інформаційної інфраструктури. Загальновідомо, що основними цілями кібератак стають об'єкти стратегічної інфраструктури країн (ядерна, транспортна, хімічна чи будь-яка інша промисловість, системи життєзабезпечення великих мегаполісів, фінансова, продовольча, енергетична національні системи, транспортні мережі, діяльність уряду, правоохоронних органів, Збройних Сил тощо). Посягання здійснюються через інформаційно-телекомунікаційні системи, особливо автоматизовані системи управління, які необхідні для повсякденного життя людей, функціонування структур економіки, органів державної влади. З огляду на це, підвищення рівня забезпечення кібербезпеки неможливо уявити без чітко спланованих спільних дій та заходів відповідальних суб'єктів, які мають бути синхронізовані та здійснюватися за єдиним стратегічним вектором розвитку національної системи кібербезпеки.

Саме тому кібербезпека визнана у більшості країн світу важливою складовою національної безпеки, забезпечення якої неможливе без формування і функціонування загальнодержавної системи та скоординованої й виваженої державної політики у сфері кібербезпеки, що ґрунтується на таких засадах, як повага до норм і принципів міжнародного права, захист фундаментальних цінностей, визначених чинним законодавством, забезпечення національних пріоритетних інтересів у кіберпросторі. За таких умов, загальною усталеною практикою країн світу стає чітке доктринальне визначення концептуальних засад державної політики у сфері забезпечення безпеки у кіберпросторі у форматі документів стратегічного планування та змісту. Будь-який стратегічний документ кібербезпекової тематики державного рівня має враховувати не тільки внутрішньополітичні аспекти, але й сучасні світові тренди в глобальному кіберсередовищі як вагомі фактори впливу на розбудову національної системи кібербезпеки будь-якої держави світу.

Загальноприйнятим світовим трендом є той факт, що схвалені національні стратегії кібербезпеки відображають політичну волю та свідоме прагнення країн світу максимально забезпечити власну кібербезпеку, попередити кіберзлочинність як на національному так і міжнародному рівнях, максимально запобігти несанкціонованому витоку даних та конфіденційної інформації. Прогнозування розвитку безпекового середовища навколо України на період до 2025 року свідчить про те, що суб'єктам забезпечення національної безпеки держави необхідно терміново вжити запобіжних заходів для захисту національних інтересів в інформаційному просторі, невід'ємною частиною якого є саме кіберпростір. За таких умов огляд новел вітчизняного законодавства і зокрема Стратегії кібербезпеки України на 2021 – 2025 роки, є актуальним та доцільним як з позиції теорії, так і практики.

Результати аналізу наукових публікацій. Розгляд актуальних питань розбудови національної системи кібербезпеки та дослідження базових положень Стратегії

кібербезпеки України здійснювали у своїх наукових працях: І. Діордиця [1], К. Галинська [2], І. Доронін [3], В. Петров [4], Н. Ткачук [5], В. Шеломенцев [6]. Проте аналіз положень оновленої Стратегії кібербезпеки України, схваленої Указом Президента України від 26 серпня 2021 року [7] не здійснювався, що дозволяє констатувати практичну значущість та актуальність тематичного спрямування цієї наукової публікації.

Метою статті є висвітлення на підставі аналізу основних позицій оновленої Стратегії кібербезпеки України та заходів щодо її практичної реалізації в умовах поширення гібридних загроз, переважно російського походження.

Виклад основного матеріалу. Як правило, у стратегіях викладаються базові принципи, на яких ґрунтується стратегія, деталізовані державні інтереси, які мають бути захищені, визначаються інструменти, що використовуються з метою посування або захисту цих інтересів, окреслюються загрози та проблеми, регламентуються пріоритетні завдання державної політики та обсяг ресурсів, які виділяються для її реалізації. Оновлена Стратегія кібербезпеки України, яка схвалена 26 серпня 2021 року [7], не стала виключенням.

Це вже друга Стратегія кібербезпеки, яка схвалена за останні п’ять років. Уперше на національному рівні Стратегія кібербезпеки як фундаментальний документ держави була схвалена ще у березні 2016 року, проте вона була розрахована на поточних п’ять років та стала першим етапом розвитку національної системи кібербезпеки держави. Схвалення на державному рівні у 2016 році Стратегії кібербезпеки України стало важливим та революційним кроком у запровадженні нових підходів довгострокового планування в цій сфері. Отже, сам факт її прийняття однозначно є позитивним результатом. Проте, враховуючи позитивні здобутки та тенденції, аналіз виконання положень Стратегії кібербезпеки України 2016 року щодо результативності діяльності суб’єктів національної системи кібербезпеки засвідчує недостатню скоординованість таких дій. За результатами експертних оцінок задекларовано, що стан реалізації Стратегії кібербезпеки 2016 року за визначеними показниками не перевищує 40 %. Невирішеними залишилися низка питань оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства. У положеннях Стратегії кібербезпеки 2016 року знайшли своє відображення засади створення національної системи кібербезпеки, потужним поштовхом для чого стало перетворення кіберпростору ще на одне поле протистояння і боротьби за незалежність держави, враховуючи сценарії скерованого хаосу, які намагається реалізувати політичне керівництво РФ.

Формування національної системи кібербезпеки передбачало результативність процесів державного управління як сукупності безперервних взаємопов’язаних дій та функцій, здійснюваних органами державної влади, які спрямовані на забезпечення безпеки в кіберпросторі. Тому розбудова національної системи кібербезпеки спрямована передусім на повномасштабне забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, яка досягається шляхом комплексного застосування сукупності організаційно-правових, інформаційних, технічних заходів, що визначаються відповідно до концептів державної політики, а саме: створення захищеного національного сегмента кіберпростору; запобігання втручанню у внутрішні справи України і нейтралізація посягань на її інформаційні ресурси з боку інших держав; посилення обороноздатності держави в кіберпросторі; боротьба з кіберзлочинністю та кібертероризмом; зниження рівня вразливості об’єктів кіберзахисту; гарантування повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки; дотримання міжнародних зобов’язань щодо боротьби з кіберзлочинністю та кібертероризмом.

Зрозуміло, що Стратегія кібербезпеки України 2016 року не була позбавлена недоліків та проблемних аспектів.

В контексті порівняння, аналіз положень Стратегії кібербезпеки України 2016 року та досвід її практичного впровадження дав змогу сформулювати проблемні питання, які або ускладнювали, або унеможливлювали її ефективну її реалізацію. Однією з виявлених проблем стала недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети або було не конкретною. Незадовільним був рівень планування заходів з реалізації Стратегії, заплановані заходи не завжди корелювались із завданнями Стратегії. Об'єктивно реалізація Стратегії кібербезпеки України 2016 року була ускладнена відсутністю цілісного бачення (програми) розвитку спроможностей основних суб'єктів національної системи кібербезпеки, обмеженістю ресурсного забезпечення функціонування цієї системи, відсутністю належної державної підтримки розвитку її інституційного забезпечення. На жаль, не були розроблені критерії оцінки стану кібербезпеки – індикатори виконання Стратегії, що ускладнило процес моніторингу її результативності та виокремлення незавершених завдань. Участь у реалізації Стратегії переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучались інші міністерства і відомства, наукові установи, а також громадськість. До виконання завдань із розвитку наукового потенціалу та поширення кіберграмотності недостатньо залучались освітні установи та наукові заклади. Надзвичайно важливі для розвитку національної системи кібербезпеки завдання Стратегії не були виконані: не сформовано перелік критичної інформаційної інфраструктури; не створено модель державно-приватного партнерства [8, с. 117-118].

Стратегія кібербезпеки України на 2021 – 2025 роки як фундаментальний документ національного значення регламентує вектор щодо: подальших кроків розбудови національної системи кібербезпеки в нашій державі; системних заходів щодо надійного захисту національного сегменту кіберпростору; зовнішньополітичної діяльності у сфері посилення кібербезпеки тощо. Загалом Стратегія кібербезпеки України складається з 9 взамопов`язаних розділів та детально визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення передумов задля побудови безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Нова Стратегія кібербезпеки України враховує попередній досвід і проблеми, поточний та перспективний стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО.

У положеннях оновленої Стратегії кібербезпеки України знайшли своє відображення концептуальні методологічні підходи до подальшого розвитку й удосконалення національної системи кібербезпеки, які базуються на таких пріоритетах: всеохоплюючому розумінні та аналізі цифрового середовища, глобальних трендів кібербезпекового середовища (з одночасним урахуванням особливостей нашої країни), неухильному захисті національних інтересів України; перманентності заходів з удосконалення законодавства у сфері кібербезпеки; орієнтованості на економічне і соціальне зростання суспільства; збалансованому забезпеченні потреб держави і прав громадян, дотриманні законності, процесуальних гарантій та засобів правового захисту; визначенні чітких ролей, потреб, зобов'язань під час розв'язання завдань кібербезпеки різного ступеня складності; ризик-орієнтованому підході щодо заходів забезпечення кібербезпеки та кіберзахисту; запровадженні механізмів державно-приватного партнерства у сфері кібербезпеки; проактивному підході, що передбачає здійснення випереджувальних

заходів; забезпеченні демократичного цивільного контролю за функціонуванням національної системи кібербезпеки.

Нова Стратегія кібербезпеки України деталізує перспективні напрями посилення спроможностей національної системи кібербезпеки. Оскільки забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України, то реалізація цього пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Також пріоритетами забезпечення кібербезпеки України визначені: убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки. Формування нової якості національної системи кібербезпеки потребує чіткого та зрозумілого визначення стратегічних цілей, які мають бути досягнуті протягом періоду реалізації Стратегії.

За результатами практичної реалізації Стратегії кібербезпеки у співпраці з приватним сектором та із залученням міжнародних партнерів очікується забезпечення: стійкості до кіберзагроз; підвищення здатності державних інституцій, бізнесу і громадян захищати себе та реагувати на кіберзагрози; спроможності до ефективної протидії злочинним діям у кіберпросторі, забезпечення їх швидкого виявлення та розслідування, створення ефективної системи превентивних заходів щодо недопущення таких дій, а також можливість проведення наступальних операцій у кіберпросторі; розвиток кадрового потенціалу та інноваційного ринку кібербезпеки, що сприятиме створенню національних розробок на рівні кращих світових практик для забезпечення можливості протидіяти майбутнім кіберзагрозам.

Своїм супротивником у кіберпросторі Україні слід вважати будь-які державні чи наддержавні утворення, недержавні суб'єкти, дії яких кваліфікуються законами України та/або міжнародно-правовими актами як підготовка або здійснення воєнної агресії та інших протиправних дій в кіберпросторі та через кіберпростір. Основним ворогом для України виступає держава-агресор, яка у кіберпросторі застосовує проти нашої держави весь наявний арсенал сучасних сил та засобів. Антиукраїнська діяльність з боку Російської Федерації проводиться у вигляді інформаційної кампанії, яка включає сукупність комплексних та окремих інформаційних операцій, інформаційних акцій та інших заходів, більшість з яких здійснюється з використанням кіберпростору і містить в собі складову безпосередніх дій в кіберпросторі.

З метою досягнення рівня максимального втручання, РФ використовуються внутрішні чинники, які обмежують потенційні можливості держави з протидії негативному впливу у кіберпросторі, основні з яких наступні: нерозвиненість, моральна і фізична застарілість; уразливість від протиправного впливу існуючої інформаційної інфраструктури (в першу чергу інформаційно-телекомунікаційних мереж та систем) держави, яка використовується в інтересах функціонування критичної інфраструктури, забезпечення безпеки та оборони держави; активне впровадження та використання в державі інформаційних технологій (систем, продуктів) іноземного походження, які не гарантують належного рівня безпеки використання і складно контролюються; ускладненість щодо розмежування військових і цивільних об'єктів критичної інфраструктури держави в кіберпросторі; можливість недержавних суб'єктів та неавторизованих (індивідуальних) користувачів здійснювати протиправні дії у кіберпросторі та проблематичність з їх виявленням; порушення встановленого національним законодавством порядку обміну інформацією з обмеженим доступом у сфері оборони; зниження науково-технічного потенціалу України; недостатнє нормативно-правове регулювання діяльності суб'єктів забезпечення кібербезпеки держави;

недостатність з огляду на зростаючий обсяг завдань як кількісно-якісного складу сил суб'єктів забезпечення кібербезпеки держави, так і кваліфікованих фахівців тощо.

Знайшли своє відображення у положеннях оновленої Стратегії кібербезпеки України такі завдання, як: створення сучасної національної системи забезпечення кібербезпеки держави; організації і забезпечення її розвитку та функціонування в інтересах національної безпеки держави; підготовки до відсічі воєнній агресії в кіберпросторі (підготовки та ведення кібероборони). Основними результатами реалізації Стратегії кібербезпеки має бути створення сприятливих умов для: захисту інтересів України в кіберпросторі; створення відповідних умов для розвитку інформаційного суспільства та розвитку "цифрової" України; підготовки та застосування структур сектору безпеки та оборони в кіберпросторі до виконання завдань за призначенням та безпечного використання ними кіберпросторі.

Практична складова Стратегії кібербезпеки передбачатиме: створення ефективної національної системи кібербезпеки з урахуванням тенденцій зміни безпекового середовища та кращих практик у сфері кібербезпеки провідних країн світу; набуття суб'єктами забезпечення кібербезпеки необхідних спроможностей для виконання завдань за призначенням, створення та розвиток відповідних організаційних структур, їх комплектування, підготовку та всебічне забезпечення; створення передумов для опанування сучасних форм та способів підготовки та проведення заходів забезпечення кібербезпеки; адекватного та завчасного нарощування потужностей щодо підготовки та ведення кібербезпеки (у т. ч. кіберзахисту, кібероборони) відповідно до зростання рівня загроз, особливо в контексті підготовки та здійснення супротивником воєнної агресії в кіберпросторі; вчасного реагування на поточні загрози кібербезпеки шляхом запобігання, завчасного виявлення, випереджувального реагування на них, усунення (мінімізації, ліквідації наслідків) їх впливу; створення системи управління забезпеченням кібербезпеки, її інтеграцію в систему державного управління; налагодження співпраці у межах повноважень з суб'єктами забезпечення національної безпеки держави, а також з НАТО, ЄС, державами-партнерами в частині спільного виконання завдань кібербезпеки.

Таким чином, в умовах російської експансійної агресії найвищим національним пріоритетом є подальше зміцнення складових сектору безпеки і оборони. Тільки успішна і послідовна державна політика, що виходить із максимально ефективного використання власних людських, фінансових, матеріально-технічних та інформаційних ресурсів, неухильне просування у напрямі європейської і євроатлантичної інтеграції, а також всебічний розвиток взаємодії зі стратегічними союзниками, у тому числі з НАТО надасть змогу захистити інтереси України і створити синергетичний ефект національної єдності та міжнародної співпраці. За таких умов модель сектору безпеки і оборони України має бути суттєво змінена, що передбачає уточнення повноважень, взаємоузгодження функцій та завдань суб'єктів сектору безпеки і оборони з метою унеможливлення виконання ними дублюючих або невластивих їм функцій, розпорошення сил та засобів.

Зважаючи позитивний досвід розвинених країн, вирішення завдань у сфері кібербезпеки слід реалізовувати через посилення стратегічних функцій національної системи кібербезпеки. Вважається логічним, щоб вони (за досвідом США) корелювалися з функціями, які використовуються у сфері забезпечення національної стійкості, а саме: запобігання (англ. "Prevention") – заходи з завчасного виявлення, уникнення, стримування, запобігання можливих (потенційних) кіберзагроз чи кібератак, припинення підготовки до них; захисту (англ. "Protection") – заходи з забезпечення випереджувального захисту (в першу чергу кіберзахисту) від можливих кібератак (кібервпливу); запобігання та мінімізація загроз (англ. "Mitigation") – заходи з безпосереднього виявлення, відвернення

загрози, зменшення можливих втрат (збитків, пошкоджень) в разі безпосередньої загрози проведення кібератак. За певних умов в межах зазначеного можуть вживатися завчасні (зустрічні) заходи активного кіберзахисту; реагування (англ. "Response") – заходи комплексного реагування на факти загрози (кібератаки тощо) з боку супротивника та відповідне виконання суб'єктами забезпечення кібербезпеки держави впливу на супротивника, у т. ч. шляхом активного кіберзахисту в умовах безпосереднього проведення ним кібератак з одночасним вжиттям заходів з захисту власної інфраструктури, особового складу, ресурсів тощо від впливу ворога; відновлення (англ. "Recovery") – заходи, спрямовані на відновлення інформаційної та іншої інфраструктури, які стали об'єктом кібератак, стабілізацію ситуації та ліквідацію інших негативних наслідків.

Ретельний аналіз положень Стратегії кібербезпеки України на 2021 – 2025 роки дає змогу констатувати, що складовими державного стратегічного планування у сфері забезпечення кібербезпеки є: стратегічний прогноз, стратегічний аналіз, ситуаційне моделювання, оцінка стану забезпечення кібербезпеки. Державне прогнозування – функція державного управління, спрямована на визначення прогнозних показників розвитку держави. Державний стратегічний прогноз у сфері забезпечення кібербезпеки являє собою систему уявлень та знань про можливі кіберзагрози та кіберінциденти. Він дає змогу визначити роль і місце національної системи кібербезпеки в міжнародному кіберпросторі. Як правило, стратегічний прогноз передбачає визначення періодів (етапів) у сфері реалізації запланованих заходів. Стратегічний аналіз, який складає основу системи інформаційно-аналітичного забезпечення суб'єктів забезпечення кібербезпеки, використовується як ефективний засіб для визначення умов та факторів, які сприятимуть підвищенню результативності заходів державної політики у сфері забезпечення кібербезпеки. Оцінка стану забезпечення кібербезпеки в рамках державного стратегічного планування передбачає проведення періодичного огляду національної системи кібербезпеки на підставі розроблених критеріїв та показників, зокрема галузевих індикаторів кібербезпеки, моніторингу потенційних і реальних кіберзагроз та кібератак, визначення поточного й перспективного стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, аудиту кібербезпеки.

Таким чином, у вітчизняній Стратегії кібербезпеки актуалізуються такі тематичні питання, як: побудова ефективної державної моделі, направленої на забезпечення кібербезпеки; визначення дієвого механізму забезпечення кібербезпеки; визначення переліку заходів, яких доцільно вжити з метою розбудови національної системи кібербезпеки; розробка системного та інтегрованого підходу до державного управління ризиками у сфері кібербезпеки, посилення державно-приватного співробітництва у цій площині тощо. Метою Стратегії кібербезпеки є визначення та деталізація пріоритетів, засад, завдань та заходів, які доцільно впроваджувати у практичну площину складовими сектору безпеки й оборони, та іншими відповідальними суб'єктами.

Також слід вказати, що у вересні 2021 року було презентовано трирічну оновлену Стратегію кібербезпеки Японії. Уперше в положеннях Стратегії кібербезпеки Японії визначено, що суттєву загрозу для національного сегменту кіберпростору становлять РФ та КНР. Існує вірогідність, що КНР на системній основі здійснює викрадення конфіденційної інформації щодо стратегічних оборонних та передових технологічних підприємств Японії, а РФ у той час проводить кібератаки з метою досягнення військових та політичних цілей у кіберпросторі.

Висновки.

Розроблення документів державного стратегічного планування – процедура державного стратегічного планування, що включає аналіз, моделювання, формування

бачення та визначення цілей, напрямів, пріоритетів, завдань та заходів, ресурсного забезпечення, а також показників досягнення цілей та виконання завдань.

Саме тому від ефективної реалізації державної політики у сфері кібербезпеки, і зокрема положень Стратегії кібербезпеки, особливо в частині щодо створення Україною власного потенціалу кіберзахисту та активного кібервпливу, безпосередньо залежать подальший розвиток ситуації навколо агресії РФ проти України, тимчасової окупації нею частини української території, проведення операції Об'єднаних сил на території Донецької та Луганської областей, суспільно-політична обстановка в державі та особливо на Донбасі. Саме стратегічне планування у сфері забезпечення кібербезпеки надає змогу підвищити ефективність та якість державного управління кібербезпекою.

Стратегія кібербезпеки України повинна розглядатися усіма органами державної влади та управління, відповідальними складовими сектору безпеки і оборони України як універсальний інструмент, завдяки якому можливо забезпечити реалізацію актуальних державних завдань у сфері забезпечення кібербезпеки, у тому числі й з використанням механізму державно-приватного партнерства. Більш того, як демонструє практика, відмова від державного стратегічного планування у важливих сферах життєдіяльності держави має ризики кризових проявів та негативних наслідків для розвитку суспільства та державних інституцій. Підвищення стратегічних спроможностей та відповідальних за забезпечення кібербезпеки правоохоронних органів потребують координацію запровадження інституційних засад і стандартів системи стратегічного управління у сфері забезпечення кібербезпеки. Виходячи з аналізу положень Стратегії кібербезпеки України, реалізація заходів, спрямованих на її забезпечення, має здійснюватися чітко на планових засадах та в обмежений час. Остання тенденція схвалених сучасних стратегій кібербезпеки – визначення чіткого переліку країн, які становлять загрозу для кібербезпеки тієї чи іншої держави. Так для України у кіберпросторі ворог № 1 – це РФ, для Японії – РФ та КНР.

Використана література

1. Діордіца І.В. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право*. 2017. № 7. С. 109-116.

2. Галинська К.Ю. Стратегія кібербезпеки як основа інформаційного правопорядку в Україні. *Форум права*. 2016. № 1. С. 37-41

3. Доронін І.М. Правові проблеми координації у секторі національної безпеки й оборони України. *Актуальні проблеми вітчизняної юриспруденції*. 2019. № 1. С. 117-121.

4. Петров В.В. Щодо формування національної системи кібербезпеки України. *Стратегічні пріоритети*. – (Нац. ін-т стратег. дослідж.). Київ: НІСД, 2013. № 4(29). С. 127-131.

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

6. Шеломенцев В.П. Основні проблеми побудови системи кібернетичної безпеки України. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2014. № 2. С. 183-186.

7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

8. Грибоєдов С.М. Удосконалення державного планування у сфері забезпечення кібербезпеки в умовах гібридних загроз. *Інформація і право*. № 1(36)/2021. С. 114-122.

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