DOI: 10.33498/louu-2024-04-089

Вікторія Рєзнікова

докторка юридичних наук, професорка,
завідувачка кафедри економічного права
та економічного судочинства
Навчально-наукового інституту права
Київського національного університету
імені Тараса Шевченка
(Київ, Україна)
ORCID ID: https://orcid.org/0000-0003-0149-0710
Researcher ID: O-4799-2018
reznikova.vv78@gmail.com

Ніно Пацурія

докторка юридичних наук, професорка,
професорка кафедри економічного права
та економічного судочинства
Навчально-наукового інституту права
Київського національного університету
імені Тараса Шевченка
(Київ, Україна)
ORCID ID: https://orcid.org/0000-0001-9974-3637
Researcher ID: T-8391-2019
patsuriianino@gmail.com

Анастасія Головачова

кандидатка юридичних наук,
асистентка кафедри економічного права
та економічного судочинства
Навчально-наукового інституту права
Київського національного університету
імені Тараса Шевченка
(Київ, Україна)
ORCID ID: https://orcid.org/0000-0002-2324-1371
Researcher ID: O-4307-2017
anastasiiagolovacheva@gmail.com

УДК: 342.1:351.865:004.056

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ І ОБОРОНОЗДАТНОСТІ В СУЧАСНИХ ЕКОНОМІКО-ПРАВОВИХ УМОВАХ

Анотація. Активізація трансформаційних явищ світового виміру, військові конфлікти, загострення міжнародної економічної конкуренції, міждержавницькі торгові конфлікти, невтішні економічні наслідки пандемії (COVID-19) тощо зумовлюють потребу постійного перегляду й коригування державних механізмів нормативного регулювання кібербезпекового напряму.

Для України питання забезпечення безпеки у кіберпросторі та мінімізації потенційних і реальних кіберзагроз і кіберризиків гостро постало з 2014 р., коли рф здійснила вторгнення на територію України та незаконно анексувала частину суверенної території, і активізувалося у 2022 р., з моменту повномасштабної військової агресії.

Метою дослідження є аналіз сучасних тенденцій у безпековій політиці ЄС і НАТО щодо кібербезпеки, на основі якого необхідним убачається визначення основних напрямів адаптації державної політики у сфері кібербезпеки до стандартів ЄС, а також напрямів співробітництва України з ЄС і НАТО на базі основоположних принципів функціонування НАТО і її місії. Крім того, важливим є виявлення ключових новітніх технологій, необхідних для забезпечення національної безпеки і захисту кіберпростору України.

На основі проведеного аналізу сучасних тенденцій у безпековій політиці ЄС і НАТО були визначені основні напрями адаптації державної політики до стандартів ЄС у сфері кібербезпеки. Постійний розвиток технологій і утворення нових цифрових систем у поєднанні з мотивацією ворога до захоплення національного кіберпростору створюють загрозу безперервності діяльності ключових державних інституцій, а також щодо їх спроможності захищати свої дані. Саме тому важливим аспектом в умовах війни є гармонізація національного законодавства до вимог ЄС у частині запровадження внутрішнього управління кіберризиками; встановлення особливих вимог кіберзахисту та до організацій критичної інфраструктури та інших важливих інституцій держави та визначення відповідних заходів контролю над такими ризиками.

Також були досліджені ключові новітні технології, необхідні для забезпечення національної безпеки і захисту кіберпростору України. Зокрема, встановлено, що таким є штучний інтелект, який може застосовуватись для створення систем розвідки і контролю, що надасть можливість виявляти загрози національній безпеці та вживати заходів щодо запобігання їм, для автоматизації й оптимізації військових операцій, використовуватись у військовій логістиці, військовій медицині, аеророзвідці, у використанні БПЛА тощо.

Ключові слова: безпека; національна безпека; кібербезпека; система національної кібербезпеки; ризик; інформаційний ризик; кіберризик; кіберзагроза; обороноздатність; державна політика; співпраця України з ЄС і НАТО; безпекові стандарти ЄС і НАТО; штучний інтелект.

Перехід глобальних соціополітичних комунікацій у "цифру" аспектує прояв негативних наслідків різного виду загроз і ризиків, основними із яких є кіберзагрози і кіберризики, реалізація яких від'ємно впливає як на загальну систему національної безпеки, так і на економіку будь-якої країни в сучасному світі. Для України питання забезпечення безпеки в кіберпросторі та мінімізації потенційних і реальних кіберзагроз і кіберризиків гостро постало з 2014 р., коли рф здійснила вторгнення на територію України та незаконно анексувала частину суверенної території, й активізувалося у 2022 р., з моменту повномасштабної військової агресії.

Усі означені процеси (як зовнішні, так і внутрішні) зумовили посилення уваги законодавця до нормативного удосконалення відносин у сфері забезпечення кібербезпеки та кіберзахисту.

Підґрунтям правового регулювання досліджуваних питань став Закон України "Про основні засади забезпечення кібербезпеки України" від 5 жовтня 2017 р. № 2163-VIII[1], потребою прийняття якого стало значне зростання кількості та розширення спектра кібератак з метою порушення конфіденцій-

[1] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 23.03.2024).

ності, цілісності й доступності державних інформаційних ресурсів, зокрема тих, що циркулюють на об'єктах критичної інформаційної інфраструктури.

Цей закон визначив базові поняття і спрямований на встановлення правових та організаційних основ забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб і громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

26 серпня 2021 р. Президент України Указом "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року 'Про Стратегію кібербезпеки України'" № 447/2021 (далі – Стратегія)[2] затвердив цей довгостроковий документ з метою забезпечення кібербезпеки як одного із пріоритетів у системі національної безпеки України. Цей нормативно-правовий акт виданий на зміну Указу Президента України від 15 березня 2016 р. № 96 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року 'Про Стратегію кібербезпеки України'"[3], що був першою спробою стратегування державної політики в означеній сфері і який було скасовано у зв'язку із затвердженням Стратегії. Стратегія кібербезпеки України базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 р. № 2824-IV. На виконання Стратегії та ст. 8 Закону України "Про основні засади забезпечення кібербезпеки України", з метою забезпечення функціонування національної системи кібербезпеки Кабінет Міністрів України затвердив постановою № 1426 від 29 грудня 2021 р. "Про затвердження Положення про організаційно-технічну модель кіберзахисту"[4].

Можемо констатувати, що національний досвід реалізації попереднього документа виявив низку нагальних проблем, які завадили її всеосяжній та амбітній реалізації. Унаочнені недоліки мають бути враховані, а проблеми вирішені при реалізації планів і завдань Стратегії кібербезпеки України 2021 р. та упровадження спеціального законодавства, яке приймається у цій сфері на розвиток наведених вище нормативно-правових актів і міжнародних документів, які ратифіковані Україною.

Наукову основу дослідження становлять доробки вітчизняних і зарубіжних науковців і практиків у сфері забезпечення національної та світової кібербезпеки і застосування передових технологій для підвищення обороноздатності України (зокрема, штучного інтелекту та інших). Так, цю тему досліджували вчені: Н. Ткачук, Ю. Даник, П. Воробієнко, В. Черне-

[2] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26 серпня 2021 р. № 447/2021 <https://zakon.rada.gov.ua/laws/show/447/2021#Text> (дата звернення: 23.03.2024).

[3] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15 березня 2016 р. № 96 <https://zakon.rada.gov.ua/laws/show/96/2016#Text> (дата звернення: 23.03.2024).

[4] Про затвердження Положення про організаційно-технічну модель кіберзахисту: постанова Кабінету Міністрів України від 29 грудня 2021 р. № 1426 <https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text> (дата звернення: 23.03.2024).

га, Г. Андрощук, Т. Кваша, А. Махнюк, О. Кириченко, А. Войцехівський, В. Хаустова, О. Решетняк, М. Хаустов, В. Зінченко та ін. Проте правовому регулюванню відносин у згаданих сферах присвячено доволі мало публікацій, які здебільшого аналізують окремі аспекти кібербезпеки чи новітніх технологій, що зумовлює проведення комплексного дослідження цієї тематики.

Метою дослідження є аналіз сучасних тенденцій у безпековій політиці ЄС і НАТО щодо кібербезпеки, на основі якого необхідним убачається визначення основних напрямів адаптації державної політики у сфері кібербезпеки до стандартів ЄС, а також напрямів співробітництва України з ЄС і НАТО на основі основоположних принципів функціонування НАТО та його місії. Крім того, важливим є виявлення ключових новітніх технологій, необхідних для забезпечення національної безпеки і захисту кіберпростору України.

Воєнна сфера зазнає на сьогодні чи не найдраматичніших змін унаслідок розбудови глобального кіберпростору. Більшість країн світу активно трансформують свої потенціали у сфері оборони в напрямі посилення кібернетичних можливостей ведення бойових дій і захисту від аналогічних дій з боку супротивника, оскільки дедалі актуальнішими стають нові типи загроз.

З урахуванням широкої інформатизації сектору безпеки і оборони, зокрема, створення Єдиної автоматизованої системи управління Збройних Сил України (ЄАСУ ЗСУ), оборонний потенціал нашої держави стає більш чутливим до кіберзагроз. Впровадження провідними країнами сучасних кіберозброєнь перетворює кіберпростір на окрему, поряд з традиційними "Земля", "Повітря", "Море", "Космос", сферу ведення бойових дій, а у найближчому майбутньому рівень обороноздатності країни визначатиметься, зокрема, наявністю у неї ефективних підрозділів для ведення бойових дій у кіберпросторі та здатності протистояти кіберзагрозам у сфері оборони[5].

Загрози кібербезпеці також актуалізуються через дію таких чинників, як: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам; недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз; безсистемність заходів кіберзахисту критичної інформаційної інфраструктури; недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інформаційної інфраструктури та державних електронних інформаційних ресурсів; недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру; недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки. При цьому, окреслюючи найбільш актуальні потреби перспективного нормативного забезпечення, однозначно слід враховувати найбільш помітні іннова-

[5] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. (н 2).

ційні тренди, які вже кардинально впливають на ландшафт можливостей оборонного сектору світу, Європи і, власне, України. Це, зокрема: 1) *штучний інтелект* (як створення та розвиток комп'ютерних систем або алгоритмів, здатних виконувати завдання, що зазвичай потребують людського інтелекту) у сфері оборони; 2) *кіберзахист.* З огляду на актуальність питання кіберзахисту в Україні слід сприяти розвитку дискусії між представниками науки, промисловості та Збройних Сил для проведення відповідних досліджень і формулювання нових тем для досліджень. Поточна і майбутня дослідницька діяльність має проводитись у напрямах боротьби зі складними кіберзагрозами, проєктування програмного забезпечення зворотної дії щодо шкідливих програм і проєктування зміцнення ситуаційної обізнаності в кіберпросторі серед багатьох інших; 3) *військовий інтернет речей;* 4) *аналіз великих масивів даних у сфері оборони;* 5) *технологія "блокчейн" у сфері оборони;* 6) *робототехніка.* Розробка і серійне виробництво роботизованої безпілотної техніки військового призначення в інтересах ЗСУ – завдання довгострокове. Його успішне вирішення можливе лише за системного підходу та спільних зусиль законодавця, уряду, органів державного управління у сфері оборонної, промислової та військово-технічної політики, Міністерства оборони України, а також підприємств державної та приватної форм власності; 7) *застосування 3D-виробництва у сфері оборони.* Адитивне виробництво (AM – Additive Manufacturing), добре відоме як 3D-друк, було визначено Європейською Комісією однією з ключових технологій, що здатна підвищити конкурентоспроможність промисловості у Європі завдяки її потенціалу до швидкого, делокалізованого та гнучкого виробництва; 8) *використання нових матеріалів для потреб оборони;* 9) *автономність у обороні:* від зброї до системи прийняття рішень; 10) *готовність до біологічних загроз*[6]. Мета – сприяти підвищенню можливостей України, її армії і громадян, вміло та результативно захищати свої інтереси у всіх сферах конкурентного протистояння – від інтелектуального до військового.

Належить визнати, що розвиток безпечного, стабільного й надійного кіберпростору має полягати насамперед у: виробленні й оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС і НАТО; створенні вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО; формуванні конкурентного середовища у сфері електронних комунікацій, наданні послуг із захисту інформації та кіберзахисту; залученні експертного потенціалу наукових установ, професійних і громадських об'єднань до підготовки проєктів концептуальних документів у сфері кібербезпеки; проведенні навчань щодо надзвичайних ситуацій та інцидентів у кіберпросторі; розвитку й удосконаленні системи державного контролю за станом захисту інформації, а також

[6] 10 трендів майбутнього, які армія України поки що ігнорує (Defence Express, 14.11.2020) <https://defence-ua.com/minds_and_ideas/10_trendiv_majbutnogo-2067.html> (дата звернення: 23.03.2024).

системи незалежного аудиту інформаційної безпеки, запровадженні кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту; розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, підтримці міжнародних ініціатив у сфері кібербезпеки, які відповідають національним інтересам України, поглибленні співпраці України з ЄС і НАТО для посилення спроможностей України у сфері кібербезпеки, участі у заходах зі зміцнення довіри в кіберпросторі, які проводяться під егідою ОБСЄ; створенні умов для впровадження в Україні сучасних технологій кіберзахисту тощо[7].

Підпунктом 2 п. 3 ст. 8 Закону України "Про основні засади забезпечення кібербезпеки України" унормовано, що функціонування національної системи кібербезпеки забезпечується шляхом створення нормативно-правової і термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу і НАТО.

Одним із проявів аналізованого напряму є питання розбудови системи *оборонного планування на основі спроможностей.* Питанню підвищення ефективності стратегічного планування у сфері забезпечення національної безпеки та обороноздатності України приділяється особлива увага науковців і практиків. Стратегічне планування безпеки держави є загальноприйнятою формою стратегічного управління, яка застосовується державами Європейського Союзу і НАТО. В українську практику державного управління у сфері національної безпеки та оборони впроваджуються підходи до стратегічного та *оборонного планування на основі спроможностей,* прийняті в країнах – членах НАТО[8].

Рішенням Ради національної безпеки і оборони України від 20 травня 2016 р. "Про Стратегічний оборонний бюлетень України"[9] визначена недосконалість процедур оборонного планування в Україні, а однією з цілей оборонної реформи визначено розвиток системи оборонного планування. Вихідними даними цього планування означені, зокрема, висновки за результатами аналізу досягнень воєнної науки та *новітніх технологій* військового призначення[10].

Науковці наголошують на тому, що обов'язковою умовою належного оборонного планування на основі спроможностей є реальне сприйняття і аналіз загроз, їх правильна класифікація та всеосяжна оцінка[11]. Це стає можливим

[7] Ю Даник, П Воробієнко, В Чернега, *Основи кібербезпеки та кібероборони: підручник* (ОНАЗ ім. О. С. Попова, 2019) 142.

[8] Н Ткачук, 'Стратегічне планування та стратегічний аналіз у сфері забезпечення національної безпеки' [2021] 3 Юридичний вісник 80.

[9] Про Стратегічний оборонний бюлетень України: Указ Президента України від 6 червня 2016 р. № 240/2016 <http://www.president.gov.ua/documents/2402016-20137> (дата звернення: 23.03.2024).

[10] Г Андрощук, Т Кваша, 'Патентний ландшафт як інструмент прогнозування світових технологічних трендів: сфера озброєння та військової техніки' [2019] 4(12) Наука, технології, інновації 29.

[11] А Махнюк, О Кириченко, 'Окремі підходи щодо стратегічного аналізу ризиків у сфері інтегрованого управління кордонами: розроблення паспортів загроз прикордонної безпеки' [2012] 1 Державне будівництво <http://nbuv.gov.ua/UJRN/DeBu_2012_1_32> (дата звернення: 23.03.2024).

за переведення системи оборонного планування на засади штучного інтелекту (далі – ШІ). Такий підхід забезпечить захист безпекових і оборонних інтересів України, запобігання та усунення впливу загроз і дестабілізуючих чинників на національні інтереси, стане пріоритетом інноваційного розвитку в системі оборонного планування України[12].

Отже, ШІ може стати важливим інструментом у сфері оборонного планування в повоєнний період, допомагаючи збільшити ефективність і швидкість виконання військових завдань, знизити ризик втрат, підвищити захищеність військових систем і зменшити витрати на оборону. Проте при розробці та використанні ШІ у сфері оборонного планування необхідно враховувати кіберзагрози та кіберризики, що можуть виникати при застосуванні такого інструменту у стратегічній сфері, та всебічно унормовувати та упроваджувати положення нормативних актів, що застосовуються державами Європейського Союзу і НАТО у цій сфері.

Україні, НАТО та ЄС важливо продовжувати співпрацю в кіберсфері. Подальше співробітництво ЄС – НАТО – Україна у сфері кібербезпеки доцільно зосередити на таких напрямах: завершити створення чіткої робочої системи координації у сфері кібербезпеки, залучити всіх національних гравців, включаючи неурядові організації, і зробити допомогу НАТО, ЄС та інших організацій більш адресною та ефективною; використати досвід і практики ЄС і НАТО для створення широкої національної схеми сертифікації з кібербезпеки, розробки плану, як відповідати на широкомасштабні інциденти і кризи, поглиблювати державно-приватне партнерство; ініціювати приєднання України до Центру передового досвіду НАТО з кібероборони, що допоможе Україні імплементувати кращі практики й поглибити співпрацю з Альянсом у цій сфері; нарощувати оборонний технічний потенціал України у сфері кібербезпеки за сприяння Трастового фонду НАТО з кібербезпеки; продовжувати діяльність з визначення критичної інфраструктури та її ключових операційних вразливостей; опрацювати загальнонаціональний План реагування на надзвичайні ситуації в кіберпросторі; розробити механізм розподілення ризиків через використання захищених хмарних сервісів задля мінімізації можливих втрат у випадку кібернападу на інформаційні бази органів державної влади; залучити кращі західні практики задля посилення міжвідомчого співробітництва та державно-приватного партнерства з виробленням конкретного дієвого механізму його практичного застосування; пропонувати з боку НАТО і ЄС та залучити з боку України більше зовнішньої експертної допомоги та ін.[13] Надзвичайно позитивним кроком у аспекті викладеного є те, що у березні 2022 р. Україні був наданий статус країни – учасниці CCDCOE NATO. З травня ж 2023 р. Україна офі-

[12] Н Пацурія, 'Штучний інтелект як необхідна складова інноваційного розвитку системи оборонного планування України', *Правове регулювання цифрової економіки та штучного інтелекту: національний та міжнародний виміри: матеріали міжнародної науково-практичної конференції (*16 листопада 2023 р.) (Науково-дослідний інститут інтелектуальної власності НАПрН України, Інтерсервіс,) 208.

[13] Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері (Center of Global Studies "Strategy XXI") <https://geostrategy.org.ua/analityka/analitychna-zapyska/spivrobitnyctvo-ukrayina-yes-nato-z-protydiyi-gibrydnym-zagrozam-u-kiber-sferi/pdf> (дата звернення: 23.03.2024).

ційно приєдналася до Центру НАТО з питань співробітництва в галузі кібербезпеки. Об'єднаний центр передових технологій з кібероборони НАТО (Cooperative Cyber Defence Centre of Excellence, NATO CCDCOE) – один із центрів передового досвіду НАТО. Він забезпечує боротьбу з кібератаками й кіберзахист інформаційних систем, а також навчання та підготовку фахівців з кіберзахисту НАТО.

Стратегічна концепція НАТО 2022 р.[14] підтвердила її відданість основоположним принципам НАТО та її основній місії – колективній обороні і безпеці в євроатлантичній зоні, безперечно, "не в мирний час". У ній також відображена думка про те, що за кіберпростір, глобальну сферу взаємозв'язаних інформаційних технологій і даних "весь час ведеться змагання" між низкою держав і недержавних гравців. Зважаючи на широкомасштабну конкуренцію в кіберпросторі між військовими і розвідувальними відомствами, фірмами, криміналітетом, хакерами, хактивістами і різноманітними авантюристами, з таким висновком важко сперечатись[15]. В аспекті кібероборони численні ініціативи з розбудови потенціалу НАТО допомагають зміцнити стабільність Альянсу, серед них: навчальні й освітні програми, навчання і військові тренування, спільні доктрина і стратегія, у результаті об'єднання яких виробляється чітко сформульоване бачення, як, наприклад Зобов'язання щодо кібероборони[16]. Варто зазначити також визначення НАТО кіберпростору як сфери операцій[17], на Центр кібероперацій НАТО (CyOC)[18] і інтеграцію наступальних кіберзасобів при плануванні місій і операцій за допомогою SCEPVA – структури[19] суверенних кіберефектів, наданих союзниками на добровільній основі.

У Стратегічній концепції 2022 р.[20] НАТО відверто визнається необхідність у тіснішому партнерстві між НАТО і ЄС в обороні та безпеці, так само, як і у Стратегії кібербезпеки ЄС (2020)[21]. Є домовленості про обмін розвідданими про кіберзагрози і передовим досвідом, а також співробітництво в сфері підготовки і досліджень, але потрібно ще більше спільної роботи. НАТО може допомогти не лише з розробкою і запровадженням заходів з кібероборони і кіберстійкості, які покращили б загальну стабільність кіберпростору, а також і з посиленням нормативних аспектів цих

[14] NATO's Strategic Concept (NATO 2022 Strategic Concept) <https://www.nato.int/strategic-concept> (accessed: 23.03.2024).

[15] Т Стівенс, Д Бертон, 'НАТО і стратегічна конкуренція в кіберпросторі' (NATO Review, 06 червня 2023 р.) <https://www.nato.int/docu/review/uk/articles/2023/06/06/nato-strategchna-konkurentsya-v-kberprostor/index.html> (дата звернення: 23.03.2024).

[16] Cyber Defence Pledge (NATO, 08 July 2016) <https://www.nato.int/cps/en/natohq/official_texts_133177.htm> (accessed: 23.03.2024).

[17] T Minárik, 'NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit' (CCDCOE) <https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit> (accessed: 23.03.2024).

[18] R Emmott, 'NATO cyber command to be fully operational in 2023' (Reuters, 16 October 2018) <https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9> (accessed: 23.03.2024).

[19] W Goździewicz, 'Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)' (Cyber Defense Magazine, 11 November 2019) <https://www.cyberdefensemagazine.com/sovereign-cyber> (accessed: 23.03.2024).

[20] NATO's Strategic Concept (n 14).

[21] The Cybersecurity Strategy (European Commission) <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy> (accessed: 23.03.2024).

форм регулювання і врядування, у такий спосіб демонструючи важливість спільних цінностей і підходів до поліпшення кіберстабільності поза вузькими військовими межами, що стосуються лише НАТО. НАТО також береться за покращення взаємодії з промисловістю і академічними колами за допомогою Кіберпартнерства НАТО – промисловість (NICP)[22]. Це головним чином механізм обміну інформацією, несекретними розвідданими про кіберзагрози між Альянсом і фірмами в країнах НАТО. Аналітична група НАТО 2030 рекомендувала[23] НАТО пошукати поза межами своїх "класичних" партнерів з оборонної промисловості, щоб скористатись навичками і досвідом представників широкого приватного сектору, академічних кіл і неурядових організацій. Тобто партнерства такого типу не повинні обмежуватись відносинами між клієнтом і постачальником, а необхідно шукати нові джерела креативності й відповідного досвіду. Залишається невизначеним, як це допоможе стабільності кіберпростору, але з'являються вікна для посилення обміну розвідувальною інформацією про кіберзагрози, кіберстійкості, для технічної допомоги, розроблення політики та інших форм продуктивної взаємодії, які покращать стабільність цієї сфери. Війна в Україні продемонструвала вплив недержавних гравців на кібербезпеку і важливість цивільно-військової співпраці; від технічної допомоги, яку надають такі фірми, як Мендіант українським інженерам[24], і ініціатив Майкрософт[25] та інших, які забезпечують доступність і продовження функціонування своїх платформ перед російською кіберагресією. Очевидно, що кібероборона НАТО значною мірою зазнаватиме впливу нових технологій, таких як хмарне обчислення, штучний розум і здатність машин до навчання, військовий інтернет речей і гібридні системи "людина – машина"[26]. Оперативна гнучкість і стратегічна вага залежать від засвоєння цих нових технологій, але вони всі мають вплив на кібербезпеку як щодо їхнього захисту і стійкості до зовнішнього втручання, так і в можливих наслідках для стабільності кіберпростору, стабільності Альянсу і міжнародної системи загалом. НАТО працює над інтеграцією цих технологій у свої процеси планування і операції, зокрема, створивши Прискорювач оборонних інновацій для Північної Атлантики (DIANA)[27] і розробивши стратегію НАТО щодо штучного розуму[28].

[22] NATO Industry Cyber Partnership (NCIA-NATO Communications and Information Agency) <https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html> (accessed: 23.03.2024).
[23] NATO 2030: United for a New Area. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General Islands under the jurisdiction of any of the Parties in the North (NATO, 25 November 2020) <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf> (accessed: 23.03.2024).
[24] K Proska, J Wolfram, J Wilson, D Black, K Lunden, D Kapellmann Zafra, N Brubaker, T Mclellan, Ch Sistrunk, 'Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology' (Mandiant Advantage, 9 November 2023) <https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology> (accessed: 23.03.2024).
[25] B Smith, 'Microsoft suspends new sales in Russia' (Microsoft, 4 March 2022) <https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict> (accessed: 23.03.2024).
[26] Стівенс, Бертон (н 15).
[27] Defence Innovation Accelerator for the North Atlantic (DIANA) (accessed: 23.03.2024).
[28] Summary of the NATO Artificial Intelligence Strategy (NATO, 22 October 2021) <https://www.nato.int/cps/en/natohq/official_texts_187617.htm> (accessed: 23.03.2024).

Проведений аналіз тенденцій у безпековій політиці НАТО щодо кібернетичної безпеки, зважаючи на посилення кібербезпекової компоненти в євроатлантичній інтеграції України, на думку А. Войцехівського[29], дає змогу зробити ряд висновків: 1) Україна потребує адекватної системи кібернетичної безпеки, що трансформується, де виклики національній безпеці дедалі частіше набувають рис, відмінних від традиційних загроз. Питання захисту у кіберпросторі є невід'ємною складовою реалізації державної політики у сфері забезпечення національної безпеки; 2) поглиблення співробітництва України із НАТО суттєво посилює спроможності нашої держави у протидії кіберзагрозам. З одного боку, Україна за рахунок використання ресурсів Трастового фонду НАТО з кібербезпеки зміцнює власний кіберзахист, з другого – така співпраця вигідна й Альянсу, оскільки уможливлює в реальних умовах випробувати технічні та організаційні рішення; 3) зважаючи на значний прогрес і досвід НАТО у виробленні й удосконаленні механізму забезпечення кібербезпеки країн-членів, Україна повинна стати активним учасником цих безпекових процесів. З одного боку, враховуючи євроатлантичні прагнення України, це сприятиме поліпшенню іміджу держави, а з другого – впливатиме на формування організаційно-правової основи національної кібербезпеки України, її інтеграцію до НАТО і створення оптимальної моделі надійного захисту вітчизняного кіберпростору; 4) в умовах розробки Україною національної системи кібернетичної безпеки дієвим фактором вважається запозичення досвіду НАТО і відповідних органів країн-членів щодо організації протидії кіберзагрозам, упровадження інформаційно-комунікаційних і технологічних стандартів НАТО в Україні, а також розвиток технічних можливостей груп реагування (CERT) на кіберінциденти. В умовах гібридної війни та запровадження практик електронного врядування питання кібербезпеки для України повинні бути в центрі уваги державної політики. Загалом же, на тлі розширення та поглиблення різнобічної співпраці між Україною та НАТО, Україною та ЄС, зміцнення кіберстійкості України в контексті посилення її загального потенціалу опірності у різних сферах означатиме закриття ще однієї зони вразливості європейського кіберпростору та появу додаткового щита, що прикриватиме Європу зі Сходу.

Водночас окремим викликом для України залишатиметься на найближчу перспективу адаптація національного законодавства до вимог ЄС. Так, наприклад, у ЄС 7 січня цього року набула чинності постанова про кібербезпеку, в якій окреслено заходи для зміцнення кібербезпеки європейських інституцій, органів та організацій[30]. У постанові перелічено кроки для запровадження внутрішнього управління з кіберризиків і рамки врядування та контролю для кожної структури ЄС. Документ також передбачає створення нової Міжвідомчої ради з кібербезпеки (ІІСВ), яка наглядатиме й підтри-

[29] А Войцехівський, 'Кібербезпека як напрям євроатлантичної інтеграції України', *Право і безпека у контексті європейської та євроатлантичної інтеграції: зб. ст. та тез наук. повідомл. за матеріалами дискус. панелі II Харків. міжнар. юрид. форуму* (Харків, 28 вересня 2018 р.) (Право, 2018) 42–8.

[30] New rules to boost cybersecurity of the EU institutions enter into force (European Commission, 08 January 2024) <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6782> (accessed: 23.03.2024).

муватиме реалізацію постанови в структурах ЄС. Крім того, постанова надає розширені повноваження команді реагування на комп'ютерні надзвичайні події в інституціях, органах, офісах і агентствах ЄС (CERT-EU), яка діятиме як хаб для розвідки можливих загроз, обміну інформацією й реагування на інциденти, а також центральний дорадчий орган і центр надання послуг. З огляду на ці повноваження CERT-EU буде перейменована на Сервіс кібербезпеки для інституцій, органів, офісів і агентств ЄС, але абревіатура CERT-EU залишиться чинною. Структури ЄС розроблять внутрішні процеси управління кібербезпекою в межах періоду, визначеного в постанові, і проводитимуть оцінювання ризиків. ІІСВ буде створена й уведена в дію щонайшвидше для стратегічного виконання розпоряджень CERT-EU в межах її розширеного мандата, надання рекомендацій і підтримки структурам ЄС та нагляду за реалізацією постанови.

Нагадаємо також, що Європейська рада у березні 2021 р. визнала необхідність зміцнення кібербезпеки на рівні ЄС і надала політичні рекомендації із забезпечення належного рівня захисту у цій сфері для персоналу, баз даних, комунікаційних мереж, інформаційних систем і для процесу прийняття рішення. У березні 2022 р. Єврокомісія представила відповідні законодавчі пропозиції, які були погоджені на рівні Ради ЄС та Європарламенту у червні 2023 р. Відтак ЄС затвердила директиву про підтримку високого рівня кібербезпеки 'для подальшого підвищення стійкості та потенціалу реагування на інциденти як державного та приватного секторів, так і ЄС загалом'[31]. Нова директива ЄС під назвою NIS2 замінила директиву з безпеки мереж та інформаційних систем (директиву NIS[32]). NIS2 набула чинності 16 січня 2023 р. та повністю замінить чинну Директиву про безпеку мереж та інформаційних систем (NIS) 17 жовтня 2024 р. NIS2 призначена встановити базовий рівень для заходів контролю над ризиками кібербезпеки у всіх секторах, на які поширюється дія директиви, таких як енергетика, транспорт, охорона здоров'я та цифрова інфраструктура. Директива спрямована на гармонізацію вимог кібербезпеки та реалізацію заходів кібербезпеки у різних державах-членах. Встановлено мінімальні правила для нормативно-правової бази та започатковані механізми ефективної співпраці між відповідними органами в кожній державі ЄС. Тоді як у старій директиві NIS держави-члени несли відповідальність за визначення того, які організації мають кваліфікуватися як оператори основних послуг, нова директива NIS2 запровадила загальне правило для ідентифікації організацій, що підпадають під відповідне регулювання. При цьому в тексті уточнюється, що директива не застосовуватиметься до організацій, які провадять діяльність у таких галузях, як оборона чи національна безпека, громадська безпека та правоохоронні органи. Судова система, парламенти та центральні банки також виключені зі

[31] The NIS2 Directive: A high common level of cybersecurity in the EU (European Parliament, 08 February 2024) <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333> (accessed: 23.03.2024).

[32] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) <https://eur-lex.europa.eu/eli/dir/2022/2555/oj> (accessed: 23.03.2024).

сфери дії. NIS2 застосовується до державних адміністрацій на центральному та регіональному рівнях. Держави-члени можуть вирішувати, що це стосується й адміністрацій на місцевому рівні. Крім того, нова директива приведена у відповідність до галузевого законодавства, зокрема, з положенням про цифрову операційну стійкість для фінансового сектору та директивою про стійкість критично важливих об'єктів, щоб забезпечити юридичну ясність та узгодженість між NIS2 та цими актами.

Отже, директива встановлює вимоги до організацій, що надають найважливіші послуги у сфері енергетики, логістики, фінансів, охорони здоров'я, комунальних служб, цифрової інфраструктури, промисловості, державного управління та досліджень. Компанії, в яких працюють менше ніж 50 осіб, і річний оборот яких не перевищує 10 мільйонів євро, або річний підсумковий баланс не перевищує 10 мільйонів євро, вважаються невеликими, і тому не підпадають під дію директиви NIS2. Однак є винятки – під дію директиви потрапляють такі компанії, незалежно від їхнього розміру: провайдери трастових послуг; оператори загальнодоступних мереж електронного зв'язку або постачальники загальнодоступних послуг електронного зв'язку; реєстри імен TLD і постачальники послуг DNS, за винятком операторів кореневих серверів імен; компанії, які є єдиним постачальником послуг у державі – члені ЄС, необхідних для підтримки критично важливої соціальної або економічної діяльності[33]. Відтак NIS 2 поширюється не тільки на великі організації, а й на деякі підприємства малого бізнесу[34], які своєю чергою повинні дотримуватися вимог директиви для забезпечення високого загального рівня кібербезпеки на всій території ЄС. Директива також офіційно заснувала Європейську мережу організацій у зв'язку з випадком кіберкриз – EU-CyCLONe – яка підтримуватиме скоординоване управління великомасштабними інцидентами кібербезпеки.

13 березня 2024 р. Європарламент схвалив закон про штучний інтелект, який забезпечує безпеку і дотримання основних прав громадян, а також стимулювання інновацій[35]. Закон спрямований на захист фундаментальних прав, демократії, верховенства права та стійкості навколишнього середовища від ШІ з високим ризиком, водночас стимулюючи інновації та утверджуючи Європу як лідера в цій галузі. Він встановлює зобов'язання для ШІ на основі його потенційних ризиків і рівня впливу. Нові правила забороняють певні додатки ШІ, які загрожують правам громадян, включно із системами біометричної категоризації на основі конфіденційних характеристик і нецільового збирання зображень обличчя з інтернету або записів камер відеоспостереження для створення баз даних розпізнавання облич. '*Розпізнаван-*

[33] Нові правила посиленої кібербезпеки в Євросоюзі (H-X Technologies) <https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua> (дата звернення: 23.03.2024).

[34] Директива ЄС NIS2: як компаніям найкраще підготуватися? (B2B Cyber Security, 25 вересня 2023 р.) <https://b2b-cyber-security.de/uk/директива-eu-nis2-як-компанії-можуть-найкраще-підготуватися> (дата звернення: 23.03.2024).

[35] Artificial Intelligence Act: MEPs adopt landmark law (European Parliament, 13 March 2024) <https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law> (accessed: 23.03.2024).

ня емоцій на робочому місці та в школах, соціальна оцінка, інтелектуальна поліція (якщо вона ґрунтується виключно на профілюванні особи чи оцінці її характеристик), а також штучний інтелект, який маніпулює людською поведінкою або використовує вразливі місця людей, також буде заборонено"[36]. Заборонено використання біометричних систем ідентифікації правоохоронними органами за вузько визначеними винятками. RBI в реальному часі може бути розгорнуто лише за умови дотримання суворих заходів безпеки і підлягатиме спеціальному попередньому судовому або адміністративному дозволу. Такі види використання можуть охоплювати, наприклад, цілеспрямований пошук зниклої особи або запобігання терористичному нападу. Використання таких систем постфактум (після віддаленого RBI) вважається випадком використання з високим ризиком, який потребує судового дозволу, пов'язаного з кримінальним злочином. Чіткі зобов'язання також передбачені для інших систем штучного інтелекту з високим ризиком (через їх значну потенційну шкоду для здоров'я, безпеки, основних прав, навколишнього середовища, демократії та верховенства права). Приклади використання штучного інтелекту з високим ризиком охоплюють критичну інфраструктуру, освіту та професійну підготовку, працевлаштування, основні приватні та державні послуги (наприклад, охорону здоров'я, банки), певні системи правоохоронних органів, управління міграцією та кордонами, правосуддя та демократичні процеси (наприклад, вплив на вибори). Громадяни матимуть право подавати скарги на системи штучного інтелекту та отримувати пояснення щодо рішень, заснованих на системах високого ризику штучного інтелекту, які впливають на їхні права. Системи штучного інтелекту загального призначення (GPAI) і моделі GPAI, на яких вони базуються, мають відповідати певним вимогам щодо прозорості, включаючи дотримання законодавства ЄС про авторське право та публікацію детальних резюме вмісту, який використовується для навчання. Потужніші моделі GPAI, які можуть створювати системні ризики, стикаються з додатковими вимогами, включаючи виконання оцінки моделі, оцінку та пом'якшення системних ризиків, а також звітування про інциденти. Крім того, штучні або підроблені зображення, аудіо- чи відеоконтент (дипфейки) повинні бути чітко позначені.

Досвід зарубіжних країн доводить, що швидке, ефективне й гнучке забезпечення потреб суспільства у воєнній безпеці та обороноздатності держави в повоєнний період досягається шляхом впровадження новітніх технологій, зокрема застосування ШІ та *BigData,* як пріоритету подальшого розвитку оборонно-промислового комплексу повоєнної України. На сьогодні ШІ належить до таких технологічних сфер суспільного розвитку, які стрімко розвиваються та мають великий потенціал у багатьох галузях, включаючи: національну безпеку, оборону, військову медицину, військову логістику, розвідку і контррозвідку, аеророзвідку тощо.

[36] Євродепутати ухвалили закон про штучний інтелект (*Юридична практика,* 13 березня 2024 р.) <https://pravo.ua/ievrodeputaty-ukhvalyly-zakon-pro-shtuchnyi-intelekt> (дата звернення: 23.03.2024).

Оборонно-промисловий комплекс (далі – ОПК) стратегічно був, є і має стати джерелом запровадження новітніх технологій, зокрема окремих інформаційно-комунікаційних технологій (далі – ІКТ). Виникнення, розвиток і стрімке поширення ІКТ, зокрема ШІ, надають поштовху інноваційним перетворенням ОПК і стають драйвером перетворень інших галузей економіки через інструмент трансферу технологій у різних країнах світу[37].

Підтвердженням важливості використання ШІ для забезпечення національної безпеки є результати досліджень Науково-технічної організації НАТО, що визначають найбільш суттєві з них для розвитку технологій, згідно з яким ключовими технологіями є: ШІ, *BigData*, автономні транспортні засоби, космос, гіперзвукові літальні апарати, квантові технології, біотехнології, нові матеріали тощо[38].

Зазначене зумовлює підвищення наукового інтересу і наукових дискусій до впровадження технологій ШІ у сферу забезпечення національної безпеки та обороноздатності України в повоєнний період, напрямів їх застосування, впливу технологій ШІ на ОПК і забезпечення обороноздатності країн світу і трансферу технологій ШІ через оборонну та безпекову сфери в інші галузі економіки. Однак поточна ситуація привела до усвідомлення необхідності перегляду як існуючих (оперативних і тактичних) підходів до організації економіки воєнного часу, так і загальних (стратегічних) принципів подальшого, повоєнного розвитку економіки України за умов наявності потенційної майбутньої загрози[39].

Отже, світовий досвід запровадження ШІ у сферу національної безпеки та обороноздатності вказує на те, що сьогодні жодний збройний конфлікт не може бути вирішений без використання новітніх видів озброєння та військових дій, заснованих на інформації, отриманій у ході ідентифікації об'єктів і цілей засобами сучасного обладнання розвідки[40], та характеризується трансфером технологій ШІ через оборонну та безпекову сфери в інші галузі економіки.

Наведене вище вказує напрям формування перспективного національного законодавства в частині застосування ШІ у сфері забезпечення національної безпеки та обороноздатності України в повоєнний період та доводить ефективність застосування ШІ при збройних конфліктах різної локалізації. Отже, більшість напрямів технологічного розвитку військового потенціалу та обороноздатності пов'язані із розвитком ШІ. Цей вплив відбуватиметься переважно завдяки використанню вбудованого ШІ в інші супутні технології, такі як віртуальна / доповнена реальність; квантові обчислення; авто-

[37] Н Пацурія, 'Упровадження технологій штучного інтелекту в забезпечення національної безпеки та обороноздатності України: правові проблеми і перспективи повоєнного періоду' [2023] 3 Теорія і практика інтелектуальної власності 68–78.

[38] В Хаустова, О Решетняк, М Хаустов, В Зінченко, 'Напрямки розвитку технологій штучного інтелекту в забезпеченні обороноздатності країни' [2022] 3 БІЗНЕСІНФОРМ 18.

[39] Пацурія (н 37).

[40] З Гбур, 'Можливість адаптації ізраїльського досвіду використання штучного інтелекту у бойових діях на Сході' [2021] 12 Інвестиції: практика та досвід 54.

номність, моделювання; дослідження матеріалів; виробництво, логістика, стратегічне управління; аналітика великих, малих і широких даних[41].

ШІ матиме трансформаційний вплив на ядерні, аерокосмічні, кібернетичні технології, технології розробки нових матеріалів та біотехнології. Так, практики зазначають, що ці наслідки матимуть такий самий стратегічний вплив на зміну у військових технологіях, що й впровадження ядерної зброї[42].

Однак поряд з перевагами ШІ також може становити загрозу національній безпеці. Наприклад, країна-агресор може використовувати ШІ для здійснення кібератак та інших злочинів, що можуть негативно впливати на національну безпеку. Також існує ризик, що інші держави можуть використовувати ШІ для проведення кібершпигунства та кібератак на інфраструктуру країни[43]. Україна має відтак вдосконалювати та розвивати надалі національне законодавство у сфері кібербезпеки з урахуванням останніх напрацювань та актів ЄС і НАТО.

Висновки. На основі проведеного аналізу сучасних тенденцій у безпековій політиці ЄС і НАТО були визначені основні напрями адаптації державної політики до стандартів ЄС у сфері кібербезпеки. Постійний розвиток технологій і утворення нових цифрових систем у поєднанні з мотивацією ворога до захоплення національного кіберпростору створюють загрозу безперервності діяльності ключових державних інституцій, а також щодо їх спроможності захищати свої дані. Саме тому важливим аспектом в умовах війни є гармонізація національного законодавства до вимог ЄС у частині запровадження внутрішнього управління кіберризиками; встановлення особливих вимог кіберзахисту та до організацій критичної інфраструктури, інших важливих інституцій держави та визначення відповідних заходів контролю над такими ризиками.

Також були досліджені ключові новітні технології, необхідні для забезпечення національної безпеки і захисту кіберпростору України, зокрема, встановлено, що таким є штучний інтелект, який може застосовуватись для створення систем розвідки та контролю, що надасть можливість виявляти загрози національній безпеці та вживати заходів щодо запобігання їм, для автоматизації та оптимізації військових операцій, використовуватись у військовій логістиці, військовій медицині, аєророзвідці, у використанні БПЛА тощо.

REFERENCES

Bibliography

Authored books

1. Danyk Yu, Vorobiienko P, Cherneha V, *Osnovy kiberbezpeky ta kiberoborony: pidruchnyk* (ONAZ im. O. S. Popova 2019).

[41] Пацурія (н 37).
[42] Хаустова, Решетняк, Хаустов, Зінченко (н 38) 22.
[43] Пацурія (н 37).

Journal articles

2. Androshchuk H, Kvasha T, 'Patentnyi landshaft yak instrument prohnozuvannia svitovykh tekhnolohichnykh trendiv: sfera ozbroiennia ta viiskovoi tekhniky' [2019] 4 Nauka, tekhnolohii, innovatsii 28–40.
3. Hbur Z V, 'Mozhlyvist adaptatsii Izrailskoho dosvidu vykorystannia shtuchnoho intelektu u boiovykh diiakh na Skhodi' [2021] 12 Investytsii: praktyka ta dosvid 54–61.
4. Khaustova V, Reshetniak O, Khaustov M, Zinchenko V, 'Napriamky rozvytku tekhnolohii shtuchnoho intelektu v zabezpechenni oboronozdatnosti krainy' [2022] 3 BIZNESINFORM 17–26.
5. Makhniuk A, Kyrychenko O, 'Okremi pidkhody shchodo stratehichnoho analizu ryzykiv u sferi intehrovanoho upravlinnia kordonamy: rozroblennia pasportiv zahroz prykordonnoi bezpeky' [2012] 1 Derzhavne budivnytstvo <http://nbuv.gov.ua/UJRN/DeBu_2012_1_32> (accessed: 23.03.2024).
6. Patsuriia N, 'Uprovadzhennia tekhnolohii shtuchnoho intelektu v zabezpechennia natsionalnoi bezpeky ta oboronozdatnosti Ukrainy: pravovi problemy i perspektyvy povoiennoho periodu' [2023] 3 Teoriia i praktyka intelektualnoi vlasnosti 68–78.
7. Tkachuk N, 'Stratehichne planuvannia ta stratehichnyi analiz u sferi zabezpechennia natsionalnoi bezpeky' [2021] 4 Yurydychnyi visnyk 80–6.

Conference papers

8. Patsuriia N, 'Shtuchnyi intelekt yak neobkhidna skladova innovatsiinoho rozvytku systemy oboronnoho planuvannia Ukrainy', *Pravove rehuliuvannia tsyfrovoi ekonomiky ta shtuchnoho intelektu: natsionalnyi ta mizhnarodnyi vymiry: materialy mizhnarodnoi naukovo-praktychnoi konferentsii 16 lystopada 2023 r.* (Naukovo-doslidnyi instytut intelektualnoi vlasnosti NAPrN Ukrainy 2023) 208–13.
9. Voitsekhivskyi A, 'Kiberbezpeka yak napriam yevroatlantychnoi intehratsii Ukrainy', *Pravo i bezpeka u konteksti yevropeiskoi ta yevroatlantychnoi intehratsii: zb. st. ta tez nauk. povidoml. za materialamy dyskus. paneli II Kharkiv. mizhnar. yuryd. forumu* (m. Kharkiv, 28 veres. 2018 r.) (Pravo 2018).

Newspaper articles

10. Emmott R, 'NATO cyber command to be fully operational in 2023' (Reuters, 16 October 2018) <https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9> (accessed: 23.03.2024).
11. Goździewicz W, 'Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)' (Cyber Defense Magazine, 11 November 2019) <https://www.cyberdefensemagazine.com/sovereign-cyber> (accessed: 23.03.2024).
12. Minárik Tomáš, 'NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit' (CCDCOE) <https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit> (accessed: 23.03.2024).
13. 10 trendiv maibutnoho, yaki armiia Ukrainy poky shcho ihnoruie (Defence Express 14 lystopada 2020) <https://defence-ua.com/minds_and_ideas/10_trendiv_majbutnogo-2067.html> (accessed: 23.03.2024).
14. Dyrektyva YeS NIS2: yak kompaniiam naikrashche pidhotuvatysia? (B2B Cyber Security, 25 veresnia 2023) <https://b2b-cyber-security.de/uk/директива-eu-nis2-як-компанії-можуть-найкраще-підготуватися> (accessed: 23.03.2024).
15. Stivens T, Berton D, 'NATO i stratehichna konkurentsiia v kiberprostori' (NATO Review, 06 chervnia 2023 roku) <https://www.nato.int/docu/review/uk/articles/2023/06/06/nato-strategchna-konkurentsya-v-kberprostor/index.html> (accessed: 23.03.2024).
16. Yevrodeputaty ukhvalyly zakon pro shtuchnyi intelekt (Yurydychna praktyka, 13 bereznia 2024 roku) <https://pravo.ua/ievrodeputaty-ukhvalyly-zakon-pro-shtuchnyi-intelekt/> (accessed: 23.03.2024).

Websites

17. Artificial Intelligence Act: MEPs adopt landmark law (*European Parliament,* 13 March 2024) <https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law> (accessed: 23.03.2024).
18. NATO 2030: United for a New Area. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General Islands under the jurisdiction of any of the Parties in the North (NATO, 25 November 2020) <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf> (accessed: 23.03.2024).
19. New rules to boost cybersecurity of the EU institutions enter into force (European Commission, 08 January 2024) <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_6782> (accessed: 23.03.2024).
20. Proska K, Wolfram J, Wilson J, Black D, Lunden K, Kapellmann Zafra D, Brubaker N, Mclellan T, Sistrunk Ch, 'Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology' (*Mandiant Advantage,* 9 November 2023) <https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology> (accessed: 23.03.2024).
21. Smith B, 'Microsoft suspends new sales in Russia' (*Microsoft,* 4 March 2022) <https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict> (accessed: 23.03.2024).
22. The NIS2 Directive: A high common level of cybersecurity in the EU (*European Parliament,* 08 February 2024) <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333> (accessed: 23.03.2024).
23. Novi pravyla posylenoi kiberbezpeky v Yevrosoiuzi (H-X Technologies) <https://www.h-x.technology/ua/services/nis-2-cybersecurity-directive-ua> (accessed: 23.03.2024).
24. Spivrobitnytstvo Ukraina – YeS – NATO z protydii hibrydnym zahrozam u kibersferi' (Center of Global Studies "Strategy XXI") <https://geostrategy.org.ua/analityka/analitychna-zapyska/spivrobitnyctvo-ukrayina-yes-nato-z-protydiyi-gibrydnym-zagrozam-u-kiber-sferi/pdf> (accessed: 23.03.2024).

Viktoriia Rieznikova
Nino Patsuriia
Anastasiia Holovachova

LEGAL SUPPORT OF THE NATIONAL CYBERSECURITY AND DEFENCE SYSTEM IN THE CURRENT ECONOMIC AND LEGAL ENVIRONMENT

Abstract. The intensification of global transformational phenomena, military conflicts, intensification of international economic competition, interstate trade conflicts, disappointing economic consequences of the pandemic (COVID-19), etc. necessitate constant review and adjustment of state mechanisms for regulating cybersecurity.

For Ukraine, the issue of ensuring security in cyberspace and minimizing potential and real cyber threats and cyber risks has been acute since 2014, when Russia invaded Ukraine and illegally annexed part of its sovereign territory, and intensified in 2022, with the outbreak of full-scale military aggression.

The purpose of the study is to analyse current trends in the EU and NATO security policy on cybersecurity, based on which it is necessary to identify the main directions of adaptation of the state policy in the field of cybersecurity to EU standards, as well as the directions of cooperation between Ukraine and the EU and NATO based on the fundamental principles of NATO and its mission. In addition, it is important to identify key new technologies needed to ensure national security and protect Ukraine's cyberspace.

ПРАВО УКРАЇНИ • 2024 • № 4 • 89-106

Based on the analysis of current trends in the EU and NATO security policy, the main directions of adaptation of the state policy to the EU standards in the field of cybersecurity were identified. The constant development of technology and the creation of new digital systems, combined with the enemy's motivation to seize national cyberspace, threaten the continuity of key government institutions and their ability to protect their data. That is why an important aspect in times of war is the harmonization of national legislation with EU requirements in terms of introducing internal cyber risk management; establishing special cyber defence requirements for critical infrastructure organizations and other important state institutions and identifying appropriate control measures for such risks.

The author also examines the key new technologies necessary to ensure national security and protection of Ukraine's cyberspace, in particular, it is established that such technologies include artificial intelligence, which can be used to create intelligence and control systems that will enable the identification of threats to national security and take measures to prevent them, to automate and optimize military operations, to be used in military logistics, military medicine, aerial reconnaissance, UAVs, etc.

Keywords: security; national security; cybersecurity; national cybersecurity system; risk; information risk; cyber risk; cyber threat; defense capability; state policy; Ukraine's cooperation with the EU and NATO; EU and NATO security standards; artificial intelligence.