UDC 659.4:327.88

Kniaziev S. O.

‘SECRECY REGIME’: CONSISTENCY OF THE LEGISLATIVE TERMINOLOGY DEFINITION

The article examines the consistency of the legislative terminological definition of the ‘secrecy regime’ concept.

Considering the results of the research of the national legislation, the author focuses upon the necessity to introduce a new definition to the term of ‘secrecy regime’ that denotes the ‘regime of state secrets protection’.

Legislative consolidation of the definition of the aforesaid term and its appropriate interpretation will facilitate its correct understanding and practical use that is of primary importance in the process of preventing offences, responding effectively to various threats and, in particular, ensuring comprehensive application of the necessary security measures.

Key words: *secrecy regime, state secret, protection of state secrets, restricted information.*

DOI 10.51369/2707-7276-2024-1(37)-9
УДК 341.23(045)

ТКАЧЕНКО Олексій Петрович

ОСОБЛИВОСТІ СПІВРОБІТНИЦТВА СУБ’ЄКТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ З ОБ’ЄДНАНИМ ЦЕНТРОМ СПІЛЬНОЇ КІБЕРОБОРОНИ НАТО CCDCOE

У статті розглядається проблематика організації міжнародного співробітництва суб’єктів забезпечення кібербезпеки та протидії кіберзагрозам. Визначаються особливості організації протидії кіберзагрозам у межах діяльності Північноатлантичного альянсу та роль НАТО в кіберпросторі, головні принципи співробітництва Альянсу з країнами-партнерами у сфері кіберзахисту.

Аналізується питання проведення та наслідків кібератак російських спецслужб і підконтрольних їм хакерських угруповань на державні електронні інформаційні ресурси й об’єкти критичної інформаційної інфраструктури України.

Розглядаються заходи, проведені Національним координаційним центром кібербезпеки при РНБО України задля підвищення ефективності міжнародного співробітництва та протидії кіберзагрозам, а також у межах співпраці України, зокрема й Служби безпеки України, з Об’єднаним центром передових технологій з кібероборони НАТО (CCDCOE).

Пропонуються шляхи покращання міжнародної взаємодії у сфері забезпечення кібербезпеки та протидії кіберзагрозам.

State policy of Ukraine in the field of ensuring information security of person, society and the state

Ключові слова: *Апарат РНБО України, кібербезпека, кіберзагрози, НАТО, Національний координаційний центр кібербезпеки України, Об'єднаний центр передових технологій з кібероборони НАТО, РНБО України.*

Постановка проблеми. Аналіз кібератак на критичну інформаційну інфраструктуру держави, підвищення їхньої складності та розширення відповідного інструментарію з початком широкомасштабного вторгнення російської федерації в Україну свідчать про те, що Україна фактично стала полігоном для апробації росією нових зразків кіберзброї та відповідних комбінаторних стратегій стосовно нашої держави [1].

Ураховуючи кіберагресію російської федерації проти України в кіберпросторі, глобальність сучасних кіберзагроз і пріоритетність євроатлантичного курсу нашої держави, однією з проблем, що потребує негайного вирішення, зокрема Національним координаційним центром кібербезпеки (НКЦК), стало налагодження дієвої взаємодії з міжнародними партнерами у протидії гібридній агресії рф проти України в кіберпросторі.

Аналіз останніх досліджень і публікацій. Проблематику організації міжнародного співробітництва у сфері кібербезпеки в межах діяльності міжнародних і регіональних організацій розглядали такі вітчизняні фахівці як О. Бакалинський, С. Бондаренко, Д. Дубов, О. Климчук, А. Марущак, Д. Мельник, М. Ожеван, В. Петрик, С. Петров, М. Присяжнюк, О. Ткаченко, Н. Ткачук, В. Хлевицький та інші [2–4]. Однак у їхніх дослідженнях не висвітлювалися особливості міжнародного співробітництва у сфері забезпечення кібербезпеки та протидії кіберзагрозам із відповідними центрами та структурами Північноатлантичного альянсу.

Також потребує аналізу й детального розгляду діяльність НКЦК, який зайняв проактивну позицію, виступаючи ініціатором нововведень у сфері регіональної та міжнародної кібербезпеки у відповідних організаціях, і з початком широкомасштабної агресії рф проти України активізував взаємодію із спецслужбами та правоохоронними органами країн Європи, насамперед Балтії, Польщі, Чехії, Великої Британії, Данії, США, а також ключовими міжнародними організаціями – НАТО, ЄС, Радою Європи, ООН, ОБСЄ тощо.

Метою статті є дослідження аспектів міжнародного співробітництва України у сфері забезпечення кібербезпеки в межах діяльності міжнародних і міжрегіональних організацій, особливостей організації протидії кіберзагрозам у межах діяльності Північноатлантичного альянсу, визначення шляхів покращання міжнародної взаємодії у сфері забезпечення кібербезпеки та протидії кіберзагрозам.

Виклад основного матеріалу. Кібератаки російських спецслужб і підконтрольних їм хакерських угруповань на державні електронні інформаційні ресурси, об'єкти критичної інформаційної інфраструктури України продовжують супроводжувати конвенційні атаки російської армії та дедалі набувають характеру спланованої глобальної кібервійни, яка є невід'ємною

частиною гібридної агресії рф як нової форми війни.

Після початку повномасштабного вторгнення рф стало цілком зрозуміло, кому вигідно і хто фінансує такі кібердиверсії. Більшість інцидентів, які детально розслідувала Служба безпеки України, потребували значного фінансування, але, окрім шкоди для України, вони не мали економічної доцільності ані для злочинців, ані для фінансово-промислових груп [5].

Серед основних ознак, які є характерними для початку здійснення кібератак на певні підприємства й об'єкти критичної інфраструктури, визначаються *іміджева, матеріальна* та *політична* позиції підприємства.

Практично всі кібератаки завдавали матеріальних та іміджевих втрат Україні, зокрема й психологічного тиску на українців. Вони проводилися за однаковими сценаріями, їхньою метою було блокування роботи інформаційних систем державних інституцій, а головне – досягнення негативного суспільного резонансу. У зловмисників є потенційні можливості спричиняти ще негативніші наслідки, однак перевага віддається загостренню соціальних проблем.

Характерною ознакою є й політично вмотивований вибір часу здійснення більшості кібератак, як-то: загострення бойових дій із боку збройних сил рф, значущі міжнародні, соціально-політичні події в Україні або напередодні прийняття на міжнародній арені важливих для українців політичних рішень.

У контексті розслідування таких кібератак із боку російської федерації активізація міжнародної співпраці у сфері їх ідентифікації та нейтралізації з представниками профільних структур, центрів країн – членів НАТО та інших міжнародних інституцій має вирішальне значення [5].

Кіберпростір уважається одним із найуразливіших місць для Північноатлантичного альянсу. Стрімкий розвиток інформаційних технологій значно ускладнює роботу спецслужб та інших уповноважених державних органів щодо захисту від кібератак, а також потребує постійного пошуку нових засобів захисту елементів критичної інфраструктури [4].

Особливістю організації протидії кіберзагрозам у межах діяльності НАТО є те, що кіберзахист став частиною основного завдання колективного захисту країн – членів Альянсу. Основна увага НАТО в кіберзахисті спрямована на захист власних мереж (включно з кіберопераціями та місіями) та підвищення стійкості критичної інфраструктури Альянсу, зокрема інформаційної. Також пріоритетним є застосування міжнародного права в кіберпросторі [4].

У результаті проведених досліджень було виокремлено *три ключові ролі* Північноатлантичного альянсу в кіберпросторі:

– просування ефективних заходів Альянсу щодо забезпечення кібероборони;

– створення умов для обміну інформацією, тренувань і досліджень у сфері кібербезпеки;

– здійснення кіберзахисту мереж Альянсу.

Тобто НАТО зосереджується на кіберзахисті власних мереж і посилен-

ні внутрішньої кіберстійкості країн – членів Альянсу.

Відповідно *головними принципами співробітництва НАТО з країнами-партнерами* у сфері кіберзахисту є [4]:

– надання Альянсом країнам-партнерам, у разі необхідності, експертної допомоги та потенційних спроможностей для захисту проти кібератак;

– можливість звернення країн-партнерів із пропозицією щодо співпраці у сфері кіберзахисту та отримання від НАТО підтримки у випадку кібератак національного значення;

– взаємовигідна співпраця між Альянсом та країною-партнером;

– уникнення дублювання заходів, що вживаються в рамках інших міжнародних організацій та залучаються до захисту інформаційних систем від кібератак, як НАТО, так і партнерами;

– підписання та дотримання угод про допомогу, інформаційний обмін та безпеку між НАТО та країнами-партнерами.

Варто зазначити, що з метою забезпечення безпеки кіберпростору в межах діяльності структур НАТО вживаються *такі заходи*:

– створені команди кіберреагування на кіберінциденти;

– підписано Меморандум про взаєморозуміння між Альянсом і його окремими країнами-членами щодо забезпечення захищених підключень для обміну та врегулювання криз;

– Центр передового досвіду з кіберзахисту НАТО активізував діяльність у напрямі розвитку спеціальних можливостей щодо протидії шкідливим програмам і підготовки фахівців відповідного рівня [5];

– налагоджується співпраця між Альянсом і малими та середніми компаніями-розробниками кібертехнологій, які часто найбільш інноваційні в цій сфері;

– країни-члени Альянсу підписали документ під назвою «Зобов'язання щодо кіберзахисту», згідно з яким усі члени НАТО підтвердили курс на розвиток необхідних сил і засобів із метою зміцнення загальної стійкості організації;

– у країнах – членах НАТО прийняті національні стратегії кібербезпеки та внесені зміни до законодавства щодо злочинів проти неї.

Однією з ключових інституцій Альянсу, яка визначає основні чинники, що на сьогодні сприяють підвищенню ефективності міжнародного співробітництва, є ***Об'єднаний центр передових технологій з кібероборони НАТО*** (Cooperative Cyber Defence Center of Excellence, NATO CCDCOE).

CCDCOE є акредитованим НАТО центром кібербезпеки й аналітичним центром, що спеціалізується на міждисциплінарних прикладних дослідженнях і розробках у сфері кіберзахисту, аналізу, обміну інформацією, а також на навчанні фахівців із кіберзахисту НАТО та проведенні командно-штабних навчань країн – членів Альянсу у сфері кіберзахисту.

Дослідивши роботу CCDCOE з моменту його створення у 2008 році, зрозуміло, що Об'єднаний центр передових технологій з кібероборони НАТО функціонує як центр компетенцій НАТО у сфері кібероборони. Основними напрямами співпраці та взаємо-

дії учасників є законодавство, операції в кіберпросторі, розробка стратегій кібербезпеки, технологій.

Також CCDCOE проводить важливі дослідження та розробки щодо виявлення й протидії сучасним кіберзагрозам, відпрацювання навичок спільного реагування на кібератаки, операції з оборони та стримування в кіберпросторі [6].

Крім того, Центр є організатором проведення щорічних масштабних кібернавчань на рівні НАТО на кшталт «Locked Shields», що спрямовані на відпрацювання навичок кібероборони, і «Crossed Swords», метою яких є відпрацювання активних кіберопераций, а також великої кількості професійних тренінгів із кібероборони та кібербезпеки.

Центр надає експертів із розробки сценаріїв і бере безпосередню участь у плануванні низки щорічних навчань НАТО, таких як «Trident Juncture», «Trident Jaguar», «Cyber Coalition», «CWIX» (Coalition Warrior Interoperability Exercise).

Вагомим результатом діяльності CCDCOE стало видання у 2013 році «Талліннського керівництва з міжнародного права щодо методів ведення кібернетичних операцій» (Tallinn Manual 2.0 on the international law applicable to Cyber Warfare).

Наразі НАТО намагається імплементувати висновки Талліннського керівництва в документи, що визначають процес прийняття рішень із створення та бойового управління кібервійськами Альянсу.

Історія стосунків України та CCDCOE починається з 2021 року. Зокрема в серпні 2021 року з ініціативи Національного координаційного центру кібербезпеки та за сприяння Уряду Республіки Естонії делегація від України на чолі із Секретарем НКЦК Н. Ткачук вручила лист Секретаря РНБО України О. Данілова на ім'я директора Керівного комітету НАТО CCDCOE як запит на вступ до центру.

Для *підвищення ефективності міжнародного співробітництва Національний координаційний центр кібербезпеки при РНБО України провів такі заходи*:

1) з метою підтримання руху України до членства в Національному координаційному центрі кібербезпеки при Апараті РНБО України було засновано Робочу групу з питань членства України в Центрі НАТО CCDCOE. До складу групи ввійшли представники всіх суб'єктів забезпечення кібербезпеки України.

4–5 листопада 2021 року в Таллінні (Естонія) відбулося засідання Керівного комітету CCDCOE, під час якого було поставлено питання щодо членства України в Центрі. З огляду на політичні розбіжності Румунія, Угорщина та Нідерланди утрималися від підтримки заявки України на вступ до CCDCOE. Пізніше завдяки активній взаємодії суб'єктів забезпечення кібербезпеки України та допомозі міжнародних партнерів серед країн, які були проти участі України в Центрі, залишилася лише Угорщина;

2) після початку широкомасштабної агресії російської федерації проти України, зокрема в кіберпросторі, у березні 2022 року Керівний комітет одностайно ухвалив рішення

щодо прийняття України до країн – членів Центру.

З цього моменту розпочато узгодження тексту Технічної угоди про співробітництво з Об'єднаним центром передових технологій з кібероборони НАТО. Підписанти Угоди з української сторони – Національний координаційний центр кібербезпеки. Зі сторони Альянсу угоду мали підписати всі країни – члени НАТО.

Паралельно з відпрацюванням тексту угоди відбувалося напрацювання напрямків практичного співробітництва України та центру НАТО CCDCOE;

3) за ініціативи НКЦК було досягнуто домовленості, що Україну в Центрі на ротаційній основі представлятимуть представники Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України й Міністерства оборони України;

4) з осені 2022 року до складу Керівного комітету Центру на постійній основі ввійшли представники Національного координаційного центру кібербезпеки;

5) наприкінці жовтня – на початку листопада 2022 року вперше новообраний директор Об'єднаного центру передових технологій з кібероборони НАТО Мартін Ноорм (естонець за національністю) відвідав Україну.

Під час візиту відбулися зустрічі М. Ноорма з керівництвом НКЦК, Мінооборони, СБ України, Держспецзв'язку, Мінцифри, заступником секретаря РНБО тощо. Під час зустрічей директора Центру НАТО було ознайомлено з реальним станом російської кіберагресії проти України, станом забезпечення кібербезпеки України, досвідом України в протиборстві з рф у кіберпросторі. Наприкінці візиту М. Ноорм наголосив на необхідності якомога скоріше направити представника України на роботу до центру НАТО CCDCOE. Також із керівником Центру було погоджено можливість участі представників суб'єктів забезпечення кібербезпеки України в тренінгах і навчальних курсах, які проводяться Центром або під його егідою;

6) наприкінці січня 2023 року Секретар Ради національної безпеки і оборони України О. Данілов підписав Технічну угоду про приєднання України до Об'єднаного центру передових технологій з кібероборони НАТО. Завдяки підписаній угоді в лютому перший представник України взяв участь у курсі, який проводить центр НАТО CCDCOE з питань застосування положень міжнародного законодавства для протидії кіберзагрозам, зокрема військового характеру, у кіберпросторі;

7) у квітні Кабінет Міністрів України ухвалив постанову, завдяки якій забезпечуються правові, організаційні та фінансові підстави роботи представника України в CCDCOE;

8) у травні 2023 року з ініціативи НКЦК та за сприяння Консультативної місії ЄС в Україні вперше група представників суб'єктів забезпечення кібербезпеки України взяла участь у тренінгу з питань захисту об'єктів критичної інфраструктури від кібератак, який відбувся в центрі НАТО CCDCOE в Таллінні;

9) 16 травня 2023 року в штабквартирі Об'єднаного центру передових технологій з кібероборони НАТО

офіційно піднято Державний прапор України, що відзначило офіційне приєднання України до CCDCOE.

З цієї ж дати розпочав роботу в Центрі НАТО представник України, співробітник Державної служби спеціального зв'язку та захисту інформації України. Передбачається, що він перебуватиме в CCDCOE 1,5–2 роки. Наразі в Україні відпрацьовується механізм його заміни на ротаційній основі представником Служби безпеки України або Міноборони України;

10) наприкінці червня – на початку липня 2023 року делегація України на чолі із заступником секретаря РНБО України С. Демедюком узяла участь у засіданні керівного комітету центру НАТО CCDCOE, а також у міжнародній щорічній конференції CyCon 2023, яка проводиться під його егідою. За результатами участі представників України в комітеті досягнуто домовленості щодо участі експертів суб'єктів забезпечення кібербезпеки України в кібернавчаннях «Crossed Swords 2023» та «Locked Shields 2024» Північноатлантичного альянсу, які проводить Центр;

11) у серпні 2023 року на базі НКЦК створено постійно діючу робочу групу співробітництва України з Об'єднаним центром передових технологій з кібероборони НАТО. За результатами першого засідання робочої групи було погоджено Дорожню карту співробітництва.

Аналіз чинників, що на сьогодні сприяють співробітництву, показав, що всі вказані заходи є першими та дуже важливими кроками, що зробив Національний координаційний центр кібербезпеки при РНБО України для підвищення ефективності міжнародного співробітництва.

Висновки. За результатами проведеного дослідження проблематики співробітництва суб'єктів забезпечення кібербезпеки та протидії кіберзагрозам Україні можна визначити такі шляхи покращання міжнародної взаємодії:

– залучення фахівців, суб'єктів забезпечення кібербезпеки України до участі в роботі центру НАТО CCDCOE на постійній основі за чотирма ключовими напрямами, а саме: у роботі Technology Branch, Stratregy Branch, Operations Branch, Law Branch;

– залучення технічних фахівців, суб'єктів забезпечення кібербезпеки України до спеціалізованих навчань Альянсу «Crossed Swords» і «Locked Shields», які проводяться під егідою Центру, що разом з іншим передбачає розроблення сценаріїв, проєктування системних архітектур, надання зразків шкідливого програмного забезпечення, розроблення стратегій захисту / нападу тощо;

– забезпечення участі представників, суб'єктів забезпечення кібербезпеки України в тренінгах і курсах, які проводяться CCDCOE на постійній основі, зокрема в підготовці навчальних матеріалів курсів, тренінгів за напрямом кібербезпеки, які проводяться та розробляються цим Центром;

– залучення представників, суб'єктів забезпечення кібербезпеки України та наукових установ, котрі належать до їхньої сфери управління, до участі в щорічній конференції CyCon, яку проводить CCDCOE;

– залучення компетентних фахівців, суб'єктів забезпечення кібербезпеки України до процесу розроблення стратегічних документів Центру, зокрема таких як Доктрина НАТО із проведення операцій у кіберпросторі, «Tallinn manual 3.0» тощо;

– проведення спільних науково-дослідницьких робіт із CCDCOE у сфері забезпечення кібербезпеки, кіберзахисту та кібероборони;

– організація спільних із Центром НАТО й міждержавних командно-штабних навчань із питань кіберзахисту, кібербезпеки та кібероборони із залученням керівників державних органів, зокрема основних суб'єктів національної системи кібербезпеки;

– проведення в Україні конференцій, воркшопів, тренінгів і семінарів із питань кіберзахисту, кібербезпеки та кібероборони під егідою та із залученням CCDCOE;

– надання визначеним представникам суб'єктів забезпечення кібербезпеки України за сприяння Центру НАТО доступу до матеріалів і баз даних NATO та CCDCOE;

– розроблення та впровадження за участі фахівців CCDCOE проєктно-технічних рішень для потреб суб'єктів забезпечення кібербезпеки України, об'єктів критичної інфраструктури України у сфері кібербезпеки, кіберзахисту та кібероборони;

– проведення спільного з центром НАТО CCDCOE дослідження існуючих у країнах – членах НАТО механізмів залучення державного та приватного секторів, приватних підприємств, громадських об'єднань, волонтерських організацій до проведення кібероперацій;

– дослідження за сприяння об'єднаного центру НАТО питання організації державно-приватної взаємодії під час реагування на кіберінциденти та кібератаки, запровадження страхування ризиків інформаційної та кібербезпеки з метою вжиття заходів щодо вирішення зазначеної проблеми;

– залучення фахівців центру НАТО CCDCOE до процесу створення та розбудови Кіберсил ЗС України, проведення фахової експертизи відповідних законопроєктів та інших нормативно-правових актів, надання консультативної допомоги тощо.

Усі вказані вище шляхи сприятимуть ефективному міжнародному співробітництву України.

Список використаних джерел

1. Секретар РНБО України Олексій Данілов підписав Технічну Угоду про приєднання України до НАТО CCDCOE. URL: https://estonia.mfa.gov.ua/news/sekretar-rnbo-ukrayini-oleksij-danilov-pidpisav-tehnichnu-ugodu-pro-priyednannya-ukrayini-do-nato-ccdcoe (дата звернення: 04.02.2024).

2. Петрик В. М., Мельник Д. С., Бакалинський О. О. та ін. Забезпечення інформаційної безпеки у провідних країнах світу : навчальний посібник / за заг. ред. Петрика В. М. Київ : Вид-во ІСЗЗІ НТУУ «КПІ», 2014. 260 с. URL: http://www.president.gov.ua/documents/4472021-40013 (дата звернення: 04.02.2024).

3. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України: аналітична доповідь. Київ : НІСД, 2017. 30 с.

4. Присяжнюк М. М., Марущак А. І., Ткаченко О. П., Мельник Д. С. Організаційно-правові основи забезпечення кібербезпеки : підручник. Київ, 2023. 47 с.

5. Ткаченко О. П. Особливості співробітництва з іноземними Інтернет-провайдерами та ІТ компаніями у сфері кіберпростору : практичний порадник. Київ : НА СБУ, 2023. 56 с.

6. Про Стратегію кібербезпеки України : Указ Президента України від 14.05.2021 № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 05.02.2024).

Стаття надійшла до редакції 22.02.2024

UDC 341.23(045)

Tkachenko O. P.

PECULIARITIES OF COOPERATION OF UKRAINE'S CYBERSECURITY ENTITIES WITH THE NATO COOPERATIVE CYBER DEFENSE CENTRE OF EXCELLENCE (CCDCOE)

The article considers the issues of organizing international cooperation of cybersecurity actors and countering cyber threats. The author identifies the peculiarities of organizing counteraction to cyber threats within the framework of the North Atlantic Alliance and the role of NATO in cyberspace, as well as the main principles of cooperation between the Alliance and partner countries in the field of cyber defense.

The author as well analyses the conduct and consequences of cyber attacks by Russian special services and hacker groups under their control on state electronic information resources and critical information infrastructure of Ukraine.

The article focuses upon the measures carried out by the National Coordination Centre for Cybersecurity under the National Security and Defense Council of Ukraine to improve the effectiveness of international cooperation and countering cyber threats, as well as within the framework of cooperation between Ukraine, including the Security Service of Ukraine, and the NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE).

The author suggests ways to improve international cooperation in the field of cybersecurity and countering cyber threats.

Key words: *National Security and Defense Council of Ukraine, cyber security, cyber threats, NATO, National Coordination Centre for Cybersecurity of Ukraine, NATO Cooperative Cyber Defense Centre of Excellence, NSDC of Ukraine.*