А. В. Войціховський
к.ю.н., професор кафедри конституційного і міжнародного права факультету № 4 Харківського національного університету внутрішніх справ, доцент

КІБЕРБЕЗПЕКА ЯК НАПРЯМ ЄВРОАТЛАНТИЧНОЇ ІНТЕГРАЦІЇ УКРАЇНИ

Стрімкий розвиток інформаційних технологій, комп'ютеризація, створення глобального комп'ютерного простору сформували принципово нові субстанції – інформаційне суспільство, кібернетичний простір, які мають невичерпний потенціал і відіграють головну роль в економічному і соціальному розвитку країн світу. Однак, створення інформаційного суспільства призвело до виникнення багатьох кібернетичних загроз, а одним із головних завдань сучасного інформаційного суспільства є забезпечення кібернетичної безпеки.

Протидія загрозам національній безпеці, що надходять з кіберпростору, сьогодні, набула нового значення. Кіберзагрози стають дедалі частішими, більш організованими і збитковішими для державних установ, підприємств, економіки та об'єктів критичної інфраструктури; вони можуть досягти критичного рівня, який загрожує національному і євроатлантичному процвітанню, безпеці і стабільності. Джерелом таких загроз можуть бути іноземні військові і розвідувальні служби, організовані злочинні угруповання, терористичні та екстремістські групи.

У цих умовах, головним завданням європейських, та й інших країн світу є вжиття заходів, що дозволять принципово зменшити (а подекуди – унеможливити повністю) негативні наслідки від кіберзагроз. Неабияку роль у виробленні єдиних підходів щодо забезпечення кібербезпеки як складової національної безпеки країн відіграє Організація Північноатлантичного договору (НАТО).

Розмаїття способів можливого застосування кіберзасобів ставить перед НАТО одне з основних завдань щодо розуміння її власної ролі в забезпеченні кібербезпеки країн-членів, так і країн-партнерів Альянсу. Враховуючи вразливість кібернетичної безпеки кіберзахист став одним із пріоритетних напрямів діяльності НАТО.

Нова Стратегічна концепція оборони та безпеки країн-членів НАТО, що була прийнята главами держав та урядів під час Лісабонського саміту країн-членів НАТО 19 листопада 2010 року, фактично прирівняла загрози кібератак до військових загроз, що, у свою чергу, передбачає можливість відповіді на масовані кібератаки із застосуванням національних збройних сил. Кібератаки стали одним з найбільш небезпечних викликів безпеці країн-членів Альянсу, а забезпечення кібернетичної безпеки було зазначено в якості другого за значимістю пріоритету НАТО. Доктрина НАТО з кібербезпеки, у свою чергу, відзначає співробітництво з країнами-партнерами у сфері розбудови системи забезпечення кібернетичної безпеки Альянсу в якості ключового механізму заходів НАТО із забезпечення кіберзахисту. [1]

Вказана позиція Альянсу була підтверджена в Декларації Чиказького саміту, схвалена главами країн та урядів, які брали участь у засіданні Північноатлантичної ради в м. Чикаго (США) 20 травня 2012 року. [2] Зокрема в п. 49 Декларації йдеться про готовність НАТО співпрацювати з іноземними партнерами для організації адекватних відповідей на кіберзагрози та забезпечення власної безпеки.

Остаточне визнання Альянсом кіберпростору в якості операційного простору для ведення бойових дій відбулось за результатом саміту країн-членів НАТО у м. Варшава (Польща), який проходив 8–9 липня 2016 року. [3]

Роль НАТО щодо забезпечення кібербезпеки можна розділити на дві великі складові. Першим пріоритетом є захист своїх власних мереж, про що країни-члени Альянсу домовилися на саміті НАТО в м. Ньюпорт (Уельс), який проходив 4–5 вересня 2014 року. Зважаючи на широку присутність Альянсу в Інтернет-мережі, це завдання є надто складним. Виконуючи цю частину своєї ролі в забезпеченні кібербезпеки, НАТО повинна забезпечити захист усіх інформаційно-комунікаційних систем, на які Альянс покладається у своїх операціях і місіях, від тих загроз, що походять з кіберпростору.

Другим пріоритетом НАТО є допомога своїм країнам-членам у сфері розвитку власних сил і засобів кіберзахисту. Ця діяльність здійснюється різними засобами, в тому числі через дворічний процес визначення колективних цілей кіберзахисту, які кожен член Альянсу має підтримати, наприклад, розроблення стратегії кіберзахисту. Процес досягнення цих спільно узгоджених цілей регулярно переглядається. На додаток НАТО пропонує широкий спектр освітніх, тренувальних і навчальних можли-

востей за допомогою різноманітних освітніх установ, серед яких школа НАТО в Обераммергау (Німеччина) і Кіберакадемія, створення якої заплановане в Португалії. Акредитований НАТО кооперативний Центр передового досвіду з кіберзахисту в м. Таллінн (Естонія) також відіграє важливу роль в цьому аспекті.

Такі дії НАТО повинні сукупно підсилювати одне одного. Безпека Альянсу і його здатність виконувати узгоджені завдання колективної оборони великою мірою залежить від здатності до кіберзахисту і спроможності кожної країни-члена НАТО. [4]

Розбудова національної системи кібербезпеки, здатної забезпечити належну протидію кіберзагрозам національній безпеці держави, є нагальним завданням, що постало сьогодні й перед Україною. Стан кібернетичної безпеки в Україні вказує про те, що кіберпростір залишається критично слабкою складовою національної безпеки та зберігає високий ступінь уразливості перед кіберзагрозами. Об'єктами кібератак і кіберзлочинів дедалі частіше стають інформаційні ресурси фінансових установ, підприємств транспорту та енергозабезпечення, державних органів, які гарантують безпеку, оборону, захист від надзвичайних ситуацій.

Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами і спеціальними службами, а також із міжнародними організаціями. За таких умов одним із ключових пріоритетів міжнародного співробітництва у сфері кібербезпеки є стратегічне партнерство України з Організацією Північноатлантичного договору.

У січні 2008 року НАТО затвердила концепти кібернетичної політики Альянсу, враховуючи наслідки скоєних кібератак проти Естонії в жовтні 2007 року, коли веб-сайти урядових установ й інші естонські інтернет-ресурси зазнали хакерських атак. Викладене спонукало до об'єднання зусиль країн-членів НАТО у сфері посилення кіберзахисту та кібербезпеки, у зв'язку з чим у м. Брюссель (Бельгія) був підписаний меморандум про створення в м. Таллінн (Естонія) міжнародного Центру кібернетичного захисту НАТО.

У 2008 році в рамках Спільної робочої групи України-НАТО з питань воєнної реформи за ініціативи Служби безпеки України було започатковано створення Робочої підгрупи з питань кібернетичного захисту, що стало поштовхом для розробки концептуальних засад взаємодії між Україною та Північноатлантичним Альянсом у вказаній сфері, запровадження

механізму консультацій та оперативного обміну інформацією в разі скоєння кібернетичних атак національного масштабу, розробки критеріїв оцінки кібернетичних загроз. У 2009 році Альянс затвердив стратегічний документ «Рамки співробітництва у питаннях кібернетичного захисту між НАТО та країнами-партнерами», яким було закладено політико-правове підґрунтя для налагодження комплексної взаємодії та співробітництва із зацікавленими країнами-партнерами, у тому числі з Україною.

Основними завданнями співробітництва між НАТО та країнами-партнерами у сфері забезпечення кібернетичного захисту визначено: підтримання нормальної життєдіяльності об'єктів критичних інформаційно-комунікаційних інфраструктур; розробка дієвих заходів з протидії кібернетичним атакам; надання допомоги країнам у відновленні нормального функціонування відповідної інфраструктури внаслідок вчинення зовнішніх кібернетичних атак, функціонування системи оперативного реагування на будь-які загрози в інформаційній сфері країн.

Указом Президента України від 24 вересня 2014 року № 744/2014 введено в дію рішення Ради національної безпеки і оборони України від 28 серпня 2014 року «Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності», в якому визначено, що пріоритетним національним інтересом України у сфері зовнішньополітичної діяльності є подальший розвиток відносин стратегічного партнерства України з США, ЄС та НАТО. [5]

Відповідно до Рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» від 6 травня 2015 року, введеного в дію Указом Президента України від 26 травня 2015 року № 287/2015, забезпечення інтеграції України до ЄС та формування умов для вступу в НАТО є пріоритетними цілями сучасної безпекової політики. [6] Однією з основних загроз національній кібербезпеці визначено вразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів України.

На виконання зазначеного з 1 липня 2015 року в Україні розпочав свою роботу Національний центр кіберзахисту та протидії кіберзагрозам з метою забезпечення діяльності команди реагування на комп'ютерні надзвичайні події України (CERT-UA). Центр виконує роль технічного координатора державних органів, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності з питань запобігання, виявлення та усунення наслідків кіберінцидентів.

Розвиток безпечного, стабільного і надійного кіберпростору і поглиблення співробітництва України з НАТО для посилення спроможностей України у сфері кібербезпеки, підтверджується рішенням Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 26 січня 2016 року, введеного в дію Указом Президента України від 15 березня 2016 року № 96/2016. [7]

У рамках досягнутих між Україною та НАТО домовленостей було прийнято спільне рішення про створення п'яти трастових фондів для нашої держави, при цьому п'ятий фонд покликаний протидіяти кіберзлочинності і спрямований на розвиток систем кіберзахисту відповідно до найпрогресивніших стандартів країн-членів НАТО. Контрибуторами цього фонду стали Естонія, Румунія, Туреччина, Угорщина.

Ідея створення Трастового фонду Україна-НАТО з кібербезпеки полягає в тому, що його інтелектуальні і матеріальні можливості дозволять надати Україні необхідну підтримку виключно для розвитку оборонних технічних можливостей, у тому числі створення лабораторій для розслідування інцидентів у кібернетичній сфері. Саме через систему цього Трастового фонду країни-члени НАТО надаватимуть підтримку Україні з метою розвитку її оборонних можливостей у сфері забезпечення кібернетичної безпеки, що передбачає постачання устаткування та обладнання, програмного забезпечення, технічної допомоги, консультативних послуг та проведення навчальних тренінгів.

Із використанням можливостей Трастового фонду НАТО до основних заходів, реалізація яких дасть змогу посилити кібербезпеку в нашій державі, відносять: проведення консультацій експертів з питань кіберзахисту, активізацію діяльності фонду в напрямі формування базових концептів Національної системи кібербезпеки; проведення переговорів у форматі експертних консультацій Україна-НАТО з питань кібербезпеки тощо.

З метою формування концептуальних засад воєнної політики держави, сучасної системи реагування на загрози національній безпеці України, Указом Президента України від 24 вересня 2015 року № 555/2015 було затверджено рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» [8]. Зокрема, в п. 59 Воєнної доктрини задекларовано необхідність поглиблення кооперації та співробітництва з НАТО і ЄС у сфері боротьби з кіберзлочинністю, що передбачає отримання доступу до інформаційних мереж, які поповнюються за рахунок розвідувальної інформації з різних джерел, у тому числі від держав-членів НАТО і ЄС.

Таким чином, Україна спрямовує свою діяльність на консолідацію зусиль щодо прискорення запровадження стандартів НАТО у сфері приєднання до колективної системи забезпечення кіберзахисту. Проте процес приєднання до колективної системи безпеки все ще залишається повільним, що свідчить про недосконалість існуючої системи протидії загрозам у кіберпросторі та зовнішнім кібератакам у сучасних умовах. [9, с.53–54]

Проведений аналіз тенденцій у безпековій політиці НАТО щодо кібернетичної безпеки, зважаючи на посилення кібербезпекової компоненти в євроатлантичній інтеграції України, дозволив зробити наступні висновки:

− Україна потребує адекватної системи кібернетичної безпеки, що трансформується, де виклики національній безпеці все частіше набувають рис, відмінних від традиційних загроз. Питання захисту у кіберпросторі є невід'ємною складовою реалізації державної політики у сфері забезпечення національної безпеки.

− 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 іншого, така співпраця вигідна й Альянсу, оскільки дозволяє в реальних умовах випробувати технічні та організаційні рішення.

− 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 буде сприяти поліпшенню іміджу держави, а з іншого – впливати на формування організаційно-правової основи національної кібербезпеки України, її інтеграцію до НАТО і створення оптимальної моделі надійного захисту вітчизняного кіберпростору.

− 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 та 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.

Література:

1. Стратегічна концепція оборони та безпеки членів Організації Північноатлантичного договору від 19.11.2010 р. // Офіційний сайт Організації Північноатлантичного договору / Організація Північноатлантичного договору. URL: https://www.nato.int/cps/uk/natohq/official_texts_68580.htm
2. Декларації Чиказького саміту від 20.05.2012 р. // Офіційний сайт Організації Північноатлантичного договору / Організація Північноатлантичного договору. URL: https://www.nato.int/cps/uk/natohq/official_texts_87593.htm?selectedLocale=uk
3. Cyber defence / Офіційний сайт Організації Північноатлантичного договору / Організація Північноатлантичного договору. URL: http://www.nato.int/cps/en/natohq/topics_78170.htm.
4. Зміна підходів до кіберзахисту // Офіційний сайт Організації Північноатлантичного договору / НАТО РЕВЮ. 2016 р. URL: https://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/UK/index.htm
5. Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності: Указ Президента України від 24.09.2014 № 744/2014 // Офіційне інтернет-представництво Президента України / Укази Президента України. URL: http://www.president.gov.ua/documents/7442014–17689
6. Про стратегію Національної безпеки України: Указ Президента України від 26.05.2015 № 287/2015 // Офіційне інтернет-представництво Президента України / Укази Президента України. URL: http: https://www.president.gov.ua/documents/2872015–19070
7. Про стратегію кібербезпеки України: Указ Президента України від 15.03.2016 № 96/2016 // Офіційне інтернет-представництво Президента України / Укази Президента України. URL: https://www.president.gov.ua/documents/962016–19836
8. Про нову редакцію Воєнної доктрини України: Указ Президента України від 24.09.2015 № 555/2015 // Офіційне інтернет-представництво Президента України / Укази Президента України. URL: https://www.president.gov.ua/documents/5552015–19443
9. Лук'янчук Р. В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети // Вісник національної академії державного управління при Президентові України. Серія «Державне управління». 2015. № 4. С. 50–56.