УДК 351.865

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ: ДЕРЖАВНІ ПРІОРИТЕТИ

Р. В. Лук'янчук,
здобувач Інституту законодавства Верховної Ради України

У статті визначено концептуальні засади міжнародного співробітництва у сфері забезпечення кібербезпеки за участі України та НАТО. Розкрито основні завдання держав-партнерів НАТО у сфері гарантування кібернетичного захисту. Окреслено перспективні напрями співробітництва між НАТО та Україною у сфері забезпечення кібербезпеки. Деталізовано пріоритети державної інформаційної політики в умовах зовнішньої агресії РФ у міжнародному кіберпросторі. Висвітлено етапи взаємодії між Україною та Альянсом у рамках функціонування Трастового фонду НАТО з кібербезпеки. На підставі аналізу чинного законодавства вказано напрями конструктивного діалогу з НАТО у сфері забезпечення кібернетичної безпеки в сучасних умовах. Визначено напрями діяльності РФ з метою посягання на державні інформаційні ресурси інших держав, у тому числі й на шкоду національним інтересам нашої держави. Деталізовано організаційно-правові засади співробітництва РФ та КНР у сфері міжнародної інформаційної безпеки. Обґрунтовано доцільність прискорення процесу приєднання України до НАТО з метою входження до системи колективної безпеки, у тому числі й у форматі забезпечення кібербезпеки.
Ключові слова: національна безпека, кібербезпека, кібератака, кіберпростір, інформаційні технології, НАТО, кіберзагрози, кібертероризм, кіберзлочинність, хакери, міжнародна інформаційна безпека, державна інформаційна політика, державні інформаційні ресурси, Трастовий фонд з кібербезпеки, промисловий шпіонаж, національна система кібербезпеки, об'єкти критичної інформаційної інфраструктури, національний центр кіберзахисту.

R. V. Lukianchuk,
Ph.D researcher, The Legislation Institute of the Verkhovna Rada of Ukraine

INTERNATIONAL COOPERATION IN SPHERE OF SUPPLY OF THE CYBER SECURITY: STATE PRIORITIES

In the article the concept principles of international cooperation in sphere of supply of the cyber security between Ukraine and NATO are considered. The main tasks of NATO partners in supporting of cyber defense are exposed. The perspective directions of cooperation between NATO and Ukraine in sphere of supply of the cyber security are outlined. The priorities of state information policy in situation of external aggression of Russian Federation in the international cyberspace are detailed. The stages of cooperation between Ukraine and Alliance in the framework of the NATO Trust Fund for *cyber security* are fixed. Due to the analysis of the legal resources the directions of constructive dialogue with NATO in sphere of supply of the cyber security nowadays are defined. The directions of Russian Federation with a view to attacks on government information resources of other countries, including to the detriment of the national interests of our country are determined. Organizational and legal framework of cooperation of Russia and China in the sphere of international information security are detailed. Consequently outlined the perspective of accelerate the accession process of Ukraine to NATO with the aim of joining the collective security system, including the format of supply of the cyber security.
Key words: national security, cyber security, cyber, cyberspace, information technology, NATO, cyber threats, cyberterrorism, cybercrime, hackers, international information security, public information policy, government information resources, trust fund on cyber security, industrial espionage, the national cybersecurity, objects of critical information infrastructure, national cyber center.

Р. В. Лукьянчук,
соискатель Института законодательства Верховного Совета Украины

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ ОБЕСПЕЧЕНИЯ КИБЕРНЕТИЧЕСКОЙ БЕЗОПАСНОСТИ: ГОСУДАРСТВЕННЫЕ ПРИОРИТЕТЫ

В статье определены концептуальные основы международного сотрудничества в сфере обеспечения кибербезопасности при участии Украины и НАТО. Раскрыты основные задачи государств-партнеров НАТО в сфере гарантирования кибернетической защиты. Обозначены перспективные направления сотрудничества между НАТО и Украиной в сфере обеспечения кибербезопасности. Детализированы приоритеты государственной информационной политики в условиях внешней агрессии РФ в международном киберпространстве. Освещены этапы взаимодействия между Украиной и Альянсом в рамках функционирования Трастового фонда НАТО по кибербезопасности. На основании анализа действующего законодательства указаны направления конструктивного диалога с НАТО в сфере обеспечения кибернетической безопасности в современных условиях. Освещены направления деятельности РФ с целью посягательства на государственные информационные ресурсы других стран, в том числе и во вред нацио-

нальным интересам нашего государства. Детализированы организационно-правовые основы сотрудничества РФ и КНР в сфере международной информационной безопасности. Также обоснована целесообразность ускорения процесса присоединения Украины к НАТО с целью вхождения в систему коллективной безопасности, в том числе и в формате обеспечения кибербезопасности.
Ключевые слова: национальная безопасность, кибербезопасность, кибератака, киберпространство, информационные технологии, НАТО, киберугрозы, кибертерроризм, киберпреступность, хакеры, международная информационная безопасность, государственная информационная политика, государственные информационные ресурсы, Трастовый фонд по кибербезопасности, промышленный шпионаж, национальная система кибербезопасности, объекты критической информационной инфраструктуры, национальный центр киберзащиты.

Постановка проблеми. Кіберпростір стає ареною конфліктів між державами, організаціями та приватними особами. За сучасних умов активізації міжнародних терористичних, екстремістських організацій та злочинних структур, які використовують інформаційні технології для реалізації своїх злочинних намірів, забезпечення інформаційної безпеки є однією з найважливіших складових системи забезпечення національної і міжнародної безпеки [1, с. 120].

Через збройний конфлікт на Сході України, воєнно-політичну нестабільність на Близькому Сході, боротьбу за вплив на світові фінансові та енергетичні потоки масштабно посилюється глобальна воєнно-політична нестабільність у світі. Політика позаблоковості, яку Україна в 2010 р. визначила основним курсом зовнішньої політики та воєнної доктрини, не створила надійних гарантій безпеки, а система забезпечення національної безпеки країни виявилася неспроможною ефективно протистояти російській агресії. 23 грудня 2014 р. Верховна Рада України прийняла рішення про відмову України від політики позаблоковості. Відтепер Україна здійснює формування нових кардинальних підходів до забезпечення національної безпеки, при цьому першочерговим завданням залишається безпосередня участь нашої країни в удосконаленні та розвитку євроатлантичної й європейської систем колективної безпеки. Обрано курс на динамічну інтеграцію до європейського політичного, економічного, правового простору з метою набуття членства в ЄС, а також вектор поглибленої співпраці з НАТО для досягнення критеріїв, необхідних для максимального прискорення набуття членства в цій організації.

Україна як європейська держава здійснює відкриту зовнішню політику і прагне рівноправного взаємовигідного співробітництва з усіма зацікавленими партнерами виходячи насамперед із пріоритетів гарантування безпеки, суверенітету та захисту територіальної цілісності [2]. Конструктивне партнерство з Організацією Північноатлантичного договору є одним із стратегічних напрямів безпекової політики України і спрямоване на взаємодію в подоланні традиційних та нових викликів і загроз, досягнення Українською державою провідних міжнародних стандартів розвитку та обороноздатності.

У сучасних умовах вітчизняний інформаційний простір залишається уразливим перед зовнішніми кіберзагрозами, особливо з боку РФ.

Джерелами зовнішніх кібернетичних загроз виступають міжнародні злочинні групи хакерів, окремі підготовлені кіберзлочинці, спецслужби іноземних держав, терористичні та екстремістські угруповання, транснаціональні корпорації та фінансово-промислові групи тощо [3, с. 160].

Як свідчить міжнародний досвід, забезпечення національної безпеки неможливо без реалізації конструктивних заходів щодо формування виваженої державної інформаційної політики, створення надійного захисту об'єктів критичної інформаційної інфраструктури та вітчизняного сегмента кіберпростору, інтеграції до світових систем колективної безпеки, що потребує чітко визначеного формату. За таких умов стратегічним завданням нашої держави залишається вдосконалення системи забезпечення кібербезпеки, яка б відповідала критеріям членства України в НАТО.

Викладене зумовлює необхідність на науковому рівні визначити напрями діяльності політичного керівництва держави щодо формування засад міжнародного співробітництва у сфері забезпечення кібербезпеки в умовах наявної агресивної політики країни-сусіда РФ, створення механізмів оперативного реагування на будь-які кіберзагрози в рамках колективної системи безпеки.

Аналіз попередніх досліджень. Сучасні наукові розробки, присвячені проблемним питанням забезпечення кібербезпеки, здійснювали: В.Бурячок, В.Горовий, Д.Дубов, А.Мовчан, В.Петров, Л.Раєцька, С.Шапочка, В.Шеломенцев та інші науковці. Проте висвітлення особливостей міжнародного співробітництва у сфері забезпечення кібернетичної безпеки з Організацією Північноатлантичного договору (НАТО), як складової пріоритетних засад державної інформаційної політики, залишилося поза увагою вказаних авторів, що посилює актуальність теми обраного наукового дослідження.

Невирішені раніше частини загальної проблеми. Питання забезпечення кібербезпеки належать до сфери національної безпеки. Гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки залишаються одним із стратегічних завдань діяльності НАТО, оскільки більшість політичних і військових конфліктів відбуваються або віддзеркалюються саме у віртуальному просторі. 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.

В.Ю.Лук'янчикова слушно вказує, що країни, які залучені до ведення міжнародних відносин у кіберпросторі, нині активно розпочинають формувати структурні одиниці для протидії та запобігання кіберзагрозам [4].

За таких умов одним із ключових пріоритетів міжнародного співробітництва у сфері забезпечення кібербезпеки є стратегічне партнерство з Північноатлантичним Альянсом, при цьому основними завданнями співробітництва між НАТО та державами-партнерами у сфері забезпечення кібернетичного захисту залишаються: підтримання нормальної життєдіяльності об'єктів критичних інформаційно-комунікаційних інфраструктур; розробка дієвих заходів протидії кібернетичним атакам; надання допомоги країнам-членам у відновленні нормального функціонування відповідної інфраструктури внаслідок проведення зовнішніх кібернетичних атак, функціонування системи оперативного реагування на будь-які загрози в інформаційній сфері країн-членів.

Проте перспективні напрями співробітництва між НАТО та Україною у сфері забезпечення кібербезпеки, створення платформи захисту вітчизняного сегмента кіберпростору в умовах російської інформаційної експансії та «інформаційної війни» з боку РФ проти нашої країни потребують висвітлення з урахуванням процесів формування Національної системи кібербезпеки за стандартами, які запроваджені в країнах-членах НАТО.

Мета публікації – визначити концепти міжнародного співробітництва між Україною та НАТО у сфері забезпечення кібербезпеки як стратегічного напряму державної інформаційної політики в сучасних умовах.

Виклад основних результатів та їх обґрунтування. Загальновизнано, що міжнародна діяльність держав повинна сприяти соціальному та економічному розвитку і здійснюватись таким чином, щоб бути сумісною із завданнями підтримки миру та міжнародної безпеки, відповідати загальновизнаним принципам і нормам міжнародного права. Не менш важливими в умовах різноманітного і широкомасштабного використання ІКТ є принципи забезпечення міжнародної інформаційної безпеки. Так, державам необхідно враховувати у своїй міжнародній інформаційній діяльності принцип неподільності безпеки та принцип відповідальності за власний інформаційний простір [5].

Одним із базових аспектів безпекової політики України є розвиток конструктивного партнерства з НАТО, в основі якого міститься критерій протидії сучасним викликам та загрозам, досягнення Україною провідних стандартів у сфері обороноздатності. Позитивним залишається набутий досвід співпраці України та НАТО: у галузі оборони та безпеки за своїми результатами наша країна випереджає співпрацю Альянсу з будь-якою іншою країною-партнером. Відповідно до положень Хартії «Про особливе партнерство між Україною та НАТО» [6], підписаної в Мадриді у 1997 р., з 1998 р. була заснована Спільна робоча група Україна–НАТО з питань воєнної реформи, основним напрямом діяльності якої є допомога Україні в складанні плану дій щодо здійснення реформування у сфері оборони шляхом щорічного затвердження Національної програми співробітництва Україна–НАТО.

У січні 2008 р. НАТО затвердила концепти кібернетичної політики Альянсу, враховуючи наслідки скоєних кібератак проти Естонії в жовтні 2007 р., коли веб-сайти урядових установ й інші естонські інтернет-ресурси зазнали хакерських атак після рішення влади країни перенести пам'ятник радянським воїнам. Викладене спонукало до об'єднання зусиль країн-членів НАТО у сфері посилення кіберзахисту та забезпечення кібербезпеки, у зв'язку з чим у Брюсселі був підписаний меморандум про створення в Естонії (м. Таллінн) міжнародного Центру кібернетичного захисту НАТО. Того ж самого року Північноатлантична рада НАТО затвердила акредитацію новоствореного Центру кіберзахисту з розташуванням його штаб-квартири у Таллінні і надала йому статус міжнародної військової організації. Завдяки його потужностям Естонія стала однією з найбільш захищених від кібератак країною в ЄС. У сучасних умовах у роботі вказаного центру беруть участь 16 європейських країн.

У 2015 р. в Таллінні було створено Кібернетичний тренувальний центр НАТО – віртуальне середовище, що дає змогу проводити тренінги фахівців, відпрацьовувати індивідуальні та ко-

мандні навички, на базі якого в квітні поточного року було проведено навчання «Locked Shields» за участі 400 комп'ютерних фахівців.

У 2008 р. 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 р. штаб-квартира НАТО затвердила стратегічний документ «Рамки співробітництва у питаннях кібернетичного захисту між НАТО та державами-партнерами», яким було закладено політико-правове підґрунтя для налагодження комплексної взаємодії та співробітництва із зацікавленими країнами-партнерами, у тому числі з Україною.

Указом Президента України від 24 вересня 2014 р. № 744/2014 введено в дію рішення Ради національної безпеки і оборони України від 28 серпня 2014 р. «Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності», визначено, що пріоритетним національним інтересом України у сфері зовнішньополітичної діяльності є подальший розвиток відносин стратегічного партнерства України з США, ЄС та НАТО [7]. Стратегія національної безпеки України [8] декларує, що забезпечення інтеграції України до ЄС та формування умов для вступу в НАТО є пріоритетними цілями сучасної безпекової політики. На виконання зазначеного з 1 липня 2015 р. в Державній службі спеціального зв'язку та захисту інформації України на базі Державного центру захисту інформаційно-телекомунікаційних систем Держспецзв'язку розпочав свою роботу Національний центр кіберзахисту та протидії кіберзагрозам з метою забезпечення діяльності команди реагування на комп'ютерні надзвичайні події України (CERT-UA), а також проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах органів державної влади.

У рамках досягнутих між Україною та НАТО домовленостей було прийнято спільне рішення про створення п'яти трастових фондів для нашої держави, при цьому один із них спрямований на розвиток сучасних систем кіберзахисту відповідно до стандартів країн-членів НАТО, контрибуторами якого виступили Румунія, Естонія, Туреччина та Угорщина. Ідея створення Трастового фонду Україна–НАТО з кібербезпеки полягає в тому, що його можливості дозволять надати Україні необхідну підтримку виключно для розвитку оборонних технічних можливостей (таких як CSIRT-1), у тому числі створення лабораторій для розслідування інцидентів у кібернетичній сфері.

Основним завданням діяльності Трастового фонду є створення сприятливих умов для підвищення технічних можливостей України у сфері забезпечення кібербезпеки протягом 24 місяців, при цьому загальний обсяг фінансування становить 815 тис. євро. У квітні 2015 р. Естонія виділила на діяльність трастового фонду НАТО для підтримки кібербезпеки в Україні 100 тис. євро, решту – інші країни Альянсу.

Саме через систему цього Трастового фонду країни–члени НАТО надаватимуть підтримку Україні з метою розвитку її оборонних можливостей у галузі забезпечення кібернетичної безпеки, що передбачає постачання устаткування та обладнання, програмного забезпечення, технічної допомоги, консультативних послуг та проведення навчальних тренінгів.

На виконання зазначених ініціатив була розроблена Річна Національна програма співробітництва Україна–НАТО на 2015 рік [9], розд. IV якої присвячений питанням забезпечення безпеки, а п. 4.7 регулює проблематику забезпечення кібербезпеки. В її положеннях задекларовано, що забезпечення сучасної кібербезпеки передбачає створення за консультативної та дорадчої допомоги НАТО Національної системи кібербезпеки як складової системи забезпечення інформаційної безпеки, налагодження комплексної взаємодії з відповідними органами іноземних держав та міжнародних організацій у режимі реального часу.

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 практичної реалізації діяльності Трастового фонду НАТО в Україні 23 липня 2015 р. укладено Угоду між Службою безпеки України та Румунською службою інформації «Про реалізацію Трастового фонду Україна–НАТО з питань кібербезпеки» [10], оскільки керівництвом НАТО саме Румунію було визначено провідною країною зазначеного Трастового фонду, а його координаторами – Румунську спецслужбу та Державну румунську компанію «RASIROM RA», яка спеціалі-

зується на інтеграції та інжинірингу систем кібернетичної безпеки.

Предметом зазначеної Угоди є перспективний розвиток оборонного технічного потенціалу України у сфері кібернетичної безпеки шляхом: упровадження на об'єктах критичної інфраструктури передових технічних рішень, які забезпечуватимуть належний рівень кібернетичної безпеки; створення центральної та мережевої лабораторій комп'ютерно-технічних експертиз із фіксованими та мобільними компонентами; проведення тренінгів для персоналу, у тому числі для групи реагування на інциденти кібербезпеки (CERT) щодо експлуатації, ремонту й управління створеними інформаційними системами. Захист мереж об'єктів критичної інформаційної інфраструктури здійснюватиметься на основі потреб української сторони, проте з урахуванням румунського досвіду в указаній сфері.

В умовах проведення антитерористичної операції на Сході України, з метою формування концептуальних засад воєнної політики держави, сучасної системи військового реагування на зовнішню агресію та загрози національній безпеці України у вересні 2015 р. набула чинності Воєнна доктрина України [11]. Зокрема, її п. 59 задекларовано необхідність поглиблення кооперації та співробітництва з НАТО і ЄС у сфері розвідки щодо протидії агресивній політиці РФ, 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, держава спрямовує свою діяльність на консолідацію зусиль щодо прискорення запровадження стандартів НАТО у сфері приєднання до колективної системи забезпечення кіберзахисту у форматі Альянсу. 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.

У контексті зазначеного актуальною загрозою для нашої держави в умовах проведення антитерористичної операції залишається діяльність китайських «кібертерористів» на користь політичного керівництва РФ. Аналіз матеріалів періодичних видань та останніх публікацій в авторитетних виданнях «The Financial Times», «The Wall Street Journal», «Reuters» свідчить про те, що російські фахівці комп'ютерних атак здійснюють свої операції, у тому числі з використанням китайських хакерських організацій з метою завдання шкоди інформаційному забезпеченню діяльності НАТО та ОБСЄ. Саме до такого висновку дійшли американські експерти з питань кібербезпеки.

Американська компанія «FireEye», що спеціалізується у дослідженні проблем забезпечення міжнародної кібербезпеки, відкрито заявила, що група хакерів під кодовою назвою «APT28» тривалий час проводила інформаційні операції на замовлення російського уряду. Починаючи з 2007 р. «APT28» добувала інформацію з питань оборони та глобальної безпеки шляхом викрадення даних із комп'ютерних мереж державних і оборонних структур країн Східної Європи (у тому числі й України), європейських силових структур, а також НАТО. На це конкретно вказує характерна специфіка роботи «APT28», а саме: обрані цілі комп'ютерних атак, типи шкідливого програмного забезпечення.

Про злочинну діяльність «APT28» було проінформовано Уряд США та прийнято рішення щодо порушення кримінальних справ проти китайських хакерів. За переконанням американських кіберекспертів, серед перспективних цілей кібератак підрозділу «APT28» були: польський, угорський, український і грузинський вектори; командування НАТО; Організація з безпеки і співробітництва в Європі; військові аташе; офіційні особи, які працюють у США і Великобританії; офіцери військового командування Канади та Норвегії та ін. Характерною особливістю діяльності шпигунської команди «APT28» була вузька спеціалізація оборонної, військово-політичної, геополітичної спрямованості, при цьому хакери не прагнули збагатитися на зламуваннях банківських рахунків – їх цікавили тільки державні таємниці військово-політичного характеру [12]. Дослідивши діяльність спецпідрозділу «APT28», американські експерти констатують, що кібератаки проводилися з урахуванням геополітичних інтересів саме РФ з метою збирання інформації на користь російського уряду.

Отже, для виконання завдань з розвідки та інформаційного впливу в комп'ютерних мережах Кремль залучає китайські кіберресурси. Нова тактика дає можливість основному замовнику – РФ – проводити незаконні вторгнення в комп'ютерні мережі своїх визначених цілей, використовуючи китайську програмно-комп'ютерну платформу для посягань на основи національної безпеки будь-якої країни, скоєння актів промислового шпіонажу, блокування та локалізацію діяльності банківських і кредитно-фінансових установ, масштабне поширення шкідливого програмного забезпечення на замовлення російської сторони.

З метою запровадження легітимних засад спільної діяльності у міжнародному кіберпросторі за участі РФ та КНР 8 травня 2015 р. між урядами

РФ та КНР було підписано Угоду «Про співробітництво у сфері забезпечення міжнародної інформаційної безпеки», яка затверджена розпорядженням Уряду РФ від 30 квітня 2015 р. № 788-р [13].

Угодою передбачається створення організаційно-правових засад співробітництва РФ та КНР у сфері забезпечення міжнародної інформаційної безпеки. КНР та РФ спільно реагуватимуть на будь-які прояви та загрози міжнародній інформаційній безпеці, до яких належать, зокрема: використання інформаційно-комунікаційних технологій для здійснення актів агресії, спрямованих на порушення суверенітету, безпеки, територіальної цілісності держав; для завдання економічних та інших збитків, у тому числі шляхом деструктивного впливу на об'єкти інформаційної інфраструктури, з терористичною метою, для пропаганди тероризму та залучення до терористичної діяльності нових прихильників тощо.

Основні напрями двостороннього співробітництва передбачають: створення каналів зв'язку та контактів щодо спільного реагування на загрози у сфері міжнародної інформаційної безпеки; обмін інформацією та співробітництво у правоохоронній сфері з метою розслідування справ, пов'язаних із використанням ІКТ у терористичних та кримінальних цілях; створення механізму співробітництва між уповноваженими органами держав щодо оперативного обміну інформацією та спільного її використання про реальні та потенційні ризики, загрози у сфері інформаційної безпеки; взаємний обмін технологіями для забезпечення безпеки функціонування критичної інформаційної інфраструктури.

Викладене дає підстави сформулювати висновок, що РФ створює технологічний плацдарм для здійснення агресивної зовнішньої інформаційної політики, підготовку до ведення кібернетичних війн з метою посилення впливу в міжнародному кіберпросторі. Реалізується експансійна політика РФ щодо обізнаності про сучасні розробки та передові технічні досягнення зарубіжних країн, особливо держав-членів НАТО.

Висновки. Активна фаза протистояння між полярними системами колективної безпеки (об'єднаннями) в міжнародному кіберпросторі ще й досі триває, що стимулює НАТО та ЄС розробляти новий стратегічний підхід до запобігання інформаційно-психологічній агресії з боку РФ. На жаль, сьогодні для України відсутні реальні ефективні зовнішні гарантії безпеки, у тому числі й у кіберпросторі. Військово-технічне співробітництво з іноземними державами, прискорення процесу приєднання України до НАТО з метою входження до системи колективної безпеки, у тому числі й у форматі забезпечення кібербезпеки України, залишаються пріоритетами зовнішньої політики нашої держави [14].

Український вектор зовнішньої політики має бути спрямований на активізацію міжнародного співробітництва у сфері забезпечення кібернетичної безпеки, продовження взаємодії з питань кібербезпеки за участі органів державної влади України і відповідних органів НАТО шляхом співпраці на двосторонній основі, упровадження інформаційно-комунікаційних та технологічних стандартів НАТО в Україні, розвиток технічних можливостей спільних груп реагування (CERT) на кіберінциденти.

У сучасних реаліях перед політичним керівництвом нашої держави постає важливе та відповідальне завдання: запозичуючи передовий зарубіжний досвід, разом зі світовим співтовариством спільними зусиллями активізувати реалізацію дієвих заходів щодо боротьби з міжнародною кіберзлочинністю, кібертероризмом, що передбачає насамперед побудову ефективної моделі Національної системи кібербезпеки, її інтеграцію до ЄС та НАТО, дієвого захисту національних та комерційних інформаційно-комунікаційних ресурсів та їх критичної інфраструктури, затвердження офіційної акредитації з боку НАТО Національного центру кіберзахисту та протидії кіберзагрозам з метою розвитку конструктивної співпраці з Альянсом у цій галузі, блокування будь-яких посягань на національну інформаційну сферу, створення оптимальної моделі надійного захисту вітчизняного кіберпростору, формування засад для розробки методів і принципів здійснення «електронної оборони».

Перспективи подальших досліджень. Актуальними та своєчасними як з позиції фундаментальної теорії, так і практичної складової залишаються подальші наукові розробки й дослідження проблем формування базових концептів виваженої державної інформаційної політики в сучасних умовах, поглиблення міжнародного співробітництва та конструктивної співпраці з НАТО та ЄС з метою запозичення передового досвіду забезпечення кібербезпеки, результативності функціонування інституцій, які опікуються питаннями кіберзахисту (Трастовий фонд з кібербезпеки, Міжнародний центр кіберзахисту НАТО тощо).

Список використаних джерел

1. Марков В. В. Напрями діяльності НАТО у справі протидії кіберзлочинності / В. В. Марков, О. В. Караченцев // Право і безпека. – 2014. – № 4 (55). – С. 119–123.
2. Про засади внутрішньої і зовнішньої політики : Закон України від 1 лип. 2010 р. № 2411 // Відом. Верхов. Ради України. – 2010. – № 40. – Ст. 527.
3. Мовчан А. В. Кібернетична безпека України в умовах глобальної нестабільності / А. В. Мовчан // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2015. – № 1 (34). – С. 159–163.
4. Лук'янчикова В. Ю. Кіберпростір: загрози для міжнародних відносин та глобальної безпеки [Електронний ресурс] / В. Ю. Лук'янчикова // Гілея: наук. вісн. – 2013. – № 72. – С. 793–796. – Режим доступу : http://nbuv.gov.ua/j-pdf/gileya_2013_72_153.pdf
5. Забара І. М. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві [Електронний ресурс] / І. М. Забара // Теорія і практика правознавства. – 2013. – Вип. № 2. – Режим доступу : http://nbuv.gov.ua/j-pdf/tipp_2013_2_77.pdf
6. Про особливе партнерство між Україною та Організацією Північно-Атлантичного договору : Хартія від 9 лип. 1997 р. № 994 // Офіц. вісн. України. – 2006. – № 34.
7. Про рішення Ради національної безпеки і оборони України від 28 серпня 2014 року «Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності» : Указ Президента України від 24 верес. 2014 р. № 744/2014 // Офіц. вісн. Президента України. – 2014. – № 40.
8. Стратегія національної безпеки України : затверджена Указом Президента України від 26 трав. 2015 р. № 287/2015 // Офіц. вісн. України. – 2015. – № 43.
9. Про затвердження Річної Національної програми співробітництва Україна–НАТО на 2015 рік : Указ Президента України від 23 квіт. 2015 р. № 238/201 // Офіц. вісн. України. – 2015. – № 34.
10. Угода про реалізацію Трастового фонду Україна–НАТО з питань кібербезпеки між Службою безпеки України та Румунською службою інформації від 23 лип. 2015 р. // Офіц. вісн. України. – 2015. – № 79.
11. Воєнна доктрина України, затверджена Указом Президента України від 24 верес. 2015 р. № 555/2015 // Офіц. вісн. України. – 2015. – № 78.
12. В FireEye привели доказательства связи хакеров из АТР28 с Кремлем [Электронный ресурс]. – Режим доступа : http://www.osp.ru/news/2014/1028/13026314/
13. О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] : распоряжение Правительства Российской Федерации от 30 апреля 2015 г. № 788-р. – Режим доступа : http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf
14. Про Рекомендації парламентських слухань на тему: «Обороноздатність України у XXI столітті: виклики, загрози та шляхи їх подолання» : Постанова Верхов. Ради України від 12 серп. 2014 р. № 1639 // Відом. Верхов. Ради України. – 2014. – № 36. – Ст. 2003.

References

1. Markov V. V. Napryamy' diyal'nosti NATO u spravi proty'diyi kiberzlochy'nnosti / V. V. Markov, O. V. Karachencev // Pravo i bezpeka. – 2014. – #4 (55). – S. 119–123.
2. Pro zasady' vnutrishn'oyi i zovnishn'oyi polity'ky': Zakon Ukrayiny' vid 01 ly'pnya 2010 roku #2411 // Vidomosti Verxovnoyi Rady' Ukrayiny'. – 2010. – #40. – St. 527.
3. Movchan A. V. Kibernety'chna bezpeka Ukrayiny' v umovax global'noyi nestabil'nosti / A. V. Movchan // Borot'ba z organizovanoyu zlochy'nnistyu i korupciyeyu (teoriya i prakty'ka). – 2015. – # 1 (34). – S. 159–163.
4. Luk'yanchy'kova V. Yu. Kiberprostir: zagrozy' dlya mizhnarodny'x vidnosy'n ta global'noyi bezpeky' / V. Yu. Luk'yanchy'kova // Gileya: naukovy'j visny'k. – 2013. – #72. – S. 793–796. – Rezhy'm dostupu: http://nbuv.gov.ua/j-pdf/gileya_2013_72_153.pdf
5. Zabara I. M. Mizhnarodna informacijna bezpeka: suchasni koncepciyi v mizhnarodnomu pravi / I. M. Zabara // Teoriya i prakty'ka pravoznavstva. – 2013. – Vy'p. #2. – Rezhy'm dostupu : http://nbuv.gov.ua/j-pdf/tipp_2013_2_77.pdf
6. Pro osobly've partnerstvo mizh Ukrayinoyu ta Organizaciyeyu Pivnichno-Atlanty'chnogo dogovoru: Xartiya vid 09 ly'pnya 1997 roku #994 // Oficijny'j visny'k Ukrayiny'. – 2006. – #34.
7. Pro rishennya Rady' nacional'noyi bezpeky' i oborony' Ukrayiny' vid 28 serpnya 2014 roku «Pro nevidkladni zaxody' shhodo zaxy'stu Ukrayiny' ta zmicznennya yiyi oboronozdatnosti»: Ukaz Prezy'denta Ukrayiny' vid 24 veresnya 2014 roku #744/2014 // Oficijny'j visny'k Prezy'denta Ukrayiny'. – 2014. – #40.
8. Strategiya nacional'noyi bezpeky' Ukrayiny': zatverdzhena Ukazom Prezy'denta Ukrayiny' vid 26 travnya 2015 roku #287/2015 // Oficijny'j visny'k Ukrayiny'. – 2015. – #43.
9. Pro zatverdzhennya Richnoyi Nacional'noyi programy' spivrobitny'cztva Ukrayina – NATO na 2015 rik: Ukaz Prezy'denta Ukrayiny' vid 23 kvitnya 2015 roku #238/201 // Oficijny'j visny'k Ukrayiny'. – 2015. – #34.
10. Ugoda pro realizaciyu Trastovogo fondu Ukrayina – NATO z py'tan' kiberbezpeky' mizh Sluzhboyu bezpeky' Ukrayiny' ta Rumuns'koyu sluzhboyu informaciyi vid 23 ly'pnya 2015 roku // Oficijny'j visny'k Ukrayiny'. – 2015. – #79.
11. Voyenna doktry'na Ukrayiny', zatverdzhena Ukazom Prezy'denta Ukrayiny' vid 24 veresnya 2015 roku #555/2015 // Oficijny'j visny'k Ukrayiny'. – 2015. – #78.
12. V FireEye pry'vely' dokazatel'stva svyazy' xakerov y'z ATP28 s Kremlem. [Elektronny'j resurs]. Rezhy'm dostupu : http://www.osp.ru/news/2014/1028/13026314/.
13. O podpy'sany'y' Soglasheny'ya mezhdu Pravy'tel'stvom Rossy'jskoj Federacy'y' y' Pravy'tel'stvom Ky'tajskoj Narodnoj Respubly'ky' o sotrudny'chestve v oblasty' obespecheny'ya mezhdunarodnoj y'nformacy'onnoj bezopasnosty': Rasporyazheny'e Pravy'tel'stva Rossy'jskoj Federacy'y' ot 30 aprelya 2015 goda #788-r [Elektronny'j resurs]. – Rezhy'm dostupu : http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf
14. Pro Rekomendaciyi parlaments'ky'x sluxan' na temu: «Oboronozdatnist' Ukrayiny' u XXI stolitti: vy'kly'ky', zagrozy' ta shlyaxy' yix podolannya»: Postanova Verxovnoyi Rady' Ukrayiny' vid 12 serpnya 2014 roku #1639 // Vidomosti Verxovnoyi Rady' Ukrayiny'. – 2014. – # 36. – St. 2003.