УДК 004.7.056.5(477)(045)

Петров В.В.[*]

СПІВРОБІТНИЦТВО УКРАЇНИ З НАТО ЩОДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Анотація. *Розбудова національної системи кібербезпеки, здатної забезпечити належну протидію кіберзагрозам національній безпеці держави, є нагальним завданням, що постало сьогодні перед Україною. У цьому контексті, з урахуванням транснаціонального та транскордонного характеру кіберзагроз набуває особливого значення міжнародне співробітництво в ці сфері. Насамперед йдеться про співробітництво з Північноатлантичним Альянсом, який з самого початку агресії РФ надає нам практичну допомогу із зміцнення обороноздатності України. В статті теоретично обґрунтовані та проаналізовані перспективи співробітництва України з НАТО щодо протидії актуальним кіберзагрозам, розкриті практичні механізми реалізації Трастового фонду НАТО з питань забезпечення кібербезпеки.*

Ключові слова: *міжнародна безпека, національна безпека, кібербезпека, кіберзагрози, НАТО, трастовий фонд, євроатлантична інтеграція.*

Annotation. *One of crucial problems that Ukraine is facing now is the necessity of national cybersecurity system development. International cooperation is especially important it this domain taking into account transnational and transborder character of cyberthreats. First of all, we are talking about cooperation with NATO that since very beginning of Russian aggression against Ukraine delivers us practical assistance in strengthening our*

[*] кандидат політичних наук, доцент кафедри міжнародних медіакомунікацій та комунікативних технологій Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

defense capabilities. This article is devoted to theoretical and analytical research of NATO-Ukraine cooperation in countering actual cyberthreats. Practical implementations of NATO cybersecurity Trust fund are being examined.

Key words: *international security, national security, cybersecurity, cyberthreats NATO, Trust fund, euroatlantic integration.*

Аннотация. *Построение национальной системы кибербезопасности, способной обеспечить должное противодействие киберугрозам национальной безопасности государства, является актуальным заданием, которое стоит сегодня перед Украиной. В этой связи, с учетом транснационального и трансграничного характера киберугроз, международное сотрудничество в данной сфере приобретает особое значение. Прежде всего, речь идет о сотрудничестве с Североатлантическим Альянсом, который с самого начала агрессии РФ предоставляет нам практическую помощь по укреплению обороноспособности Украины. В статье теоретически обоснованы и проанализированы перспективы сотрудничества Украины с НАТО по вопросам противодействия актуальным киберугрозам, раскрыты практические механизмы реализации Трастового фонда по вопросам обеспечения кибербезопасности.*

Ключевые слова: *международная безопасность, кибербезопасность, киберугрозы, НАТО, трастовый фонд, евроатлантическая интеграция.*

Постановка проблеми. протидія загрозам національній безпеці, що надходять з кіберпростору, набула нового значення. У контексті військової агресії з боку Російської Федерації ця проблема є особливо актуальною для нашої держави. Зазначене корелюється з загальносвітовою тенденцією щодо перетворення кіберпростору на новітній вимір військового та політичного протистояння, а також інструмент реалізації злочинів проти

основ національної безпеки держави, який почали активно використовувати спецслужби іноземних країн та терористичні організації.

У зв'язку із глобальною актуалізацією кіберзагроз національній безпеці провідні держави світу активно реалізують заходи із підвищення ефективності власних кібербезпекових систем, що в першу чергу передбачає розширення повноважень та збільшення можливостей (удосконалення сил та засобів) відповідних державних органів, насамперед спеціальних служб та правоохоронних органів. Створюється й послідовно нарощується технологічний і інтелектуальний потенціал, направлений на розбудову спроможностей кіберзахисту, удосконалюються механізми координації та взаємодії суб'єктів забезпечення кібербезпеки.

Розбудова національної системи кібербезпеки, здатної забезпечити належну протидію кіберзагрозам національній безпеці держави, є нагальним завданням, що постало сьогодні перед Україною. У цьому контексті, з урахуванням транснаціонального та транскордонного характеру кіберзагроз набуває особливого значення міжнародне співробітництво в ці сфері. Насамперед йдеться про співробітництво з Північноатлантичним Альянсом, який з самого початку агресії РФ надає нам практичну допомогу із зміцнення обороноздатності України.

Актуальність даної роботи обумовлена передусім якісно новими викликами та загрозами кіберпростору, які постали перед Україною у сфері національної безпеки. На тлі сучасної інформаційної революції та розвитку інформаційно-комунікаційних застосування можливостей кіберпростору перетворилося на елемент міждержавного протиборства, що використовується спецслужбами іноземних держав для здійснення розвідувально-підривної діяльності, організації спеціальних операцій, акцій кибершпигунства, встановлення віддаленого доступу та контролю над об'єктами критичної інформаційної інфраструктури тощо направлених на отримання інформаційних переваг та забезпечення інтересів власної держави у військовій, економічній, політичній та інших сферах.

Вдала реалізація кібератак на об’єкти галузі енергетики, транспорту, фінансової сфери України протягом 2015-2017 років засвідчила вразливість критичної інфраструктури держави до кіберзагроз та актуалізацію загрози кібертероризму.

Аналіз останніх публікацій. Дослідженню сутності кібербезпеки як нового явища глобального безпекового середовища присвячені роботи іноземних дослідників: К. Александера, Л. Вентца, Т. Вінгфілда, Д. Іванченка, Ф. Крамера, М. Лібіцкі, Дж. Ліпмана, Дж. Льюіса, А. Нестерова, Р. Олдріча, Є. Роговського, А. Соловйова, Д. Стаблі, В. Шарпа, Дж. Франселли та інш. Серед вітчизняних учених відзначимо передусім дослідження С. Бондаренка, В. Бутузова, В. Бурячка, С. Гнатюка, О. Довганя, Д. Дубова, О. Климчука, М. Ожевана, В. Панченко, В. Пилипчука, В. Фурашева, В Шеломенцева, В. Толубка, О. Хорошка, І. Храбана.

Теоретичні засади проблематики забезпечення кібербезпеки України викладено в роботах вітчизняних учених В.Бутузова, В. Горбуліна, Ю. Даника, О. Дзьобаня, Д. Дубова, О. Корченка, Р. Лук’янчука, О. Мандзюка, О. Манжая, М. Ожевана, В. Пилипчука, М. Погорецького, І. Рязанцевої, В. Тихомирова, В. Харченка, В. Шеломенцева та ін.

Серед вітчизняних наукових розробок слід відмітити монографію Д. Дубова [1], який розглядає кібербезпеку через призму міжнародної безпеки, а кіберпростір як новий вимір геополітичного протистояння, який, у тому числі, безпосередньо пливає на воєнно-політичну обстановку у світі.

Виділення невирішених раніше частин загальної проблеми. У вітчизняній науковій літературі на сьогодні бракує досліджень щодо практичної взаємодії України з НАТО з питань забезпечення кібербезпеки.

Формулювання цілей статті. В статті теоретично обґрунтовані та проаналізовані перспективи співробітництва України з НАТО щодо

протидії актуальним кіберзагрозам, розкриті практичні механізми реалізації Трастового фонду НАТО з питань забезпечення кібербезпеки.

На наших очах сформовано принципово нове середовище, яке безпосередньо впливає на безпеку в її міжнародному, регіональному та національних вимірах. Вказана трансформація знайшла своє відображення в формуванні політики НАТО. Так, нова Стратегічна концепція Альянсу на 2011–2020 роки [2], ухвалена під час Лісабонського саміту країн-членів НАТО, фактично прирівняла загрози кібертероризму до військових загроз, що, у свою чергу, передбачає можливість відповіді на масовані кібератаки із застосуванням національних збройних сил. Кіберзагрози стали одним з найбільш небезпечних викликів безпеці країн-членів Альянсу, а забезпечення інформаційної безпеки було зазначено в якості другого за значимістю пріоритету НАТО. Доктрина НАТО з кібербезпеки, у свою чергу, відзначає співробітництво з державами-партнерами у сфері розбудови системи забезпечення кібернетичної безпеки Альянсу в якості ключового механізму заходів НАТО із забезпечення кіберзахисту.

Вказана позиція Альянсу була підтверджена в резолюції Чиказького саміту НАТО в травні 2012р. [3]. Зокрема в п.49 резолюції йдеться про готовність Альянсу 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 НАТО у Варшаві в липні 2016 року [4].

Рішення стосовно започаткування Трастового фонду Україна – НАТО з кібербезпеки (далі – Трастовий фонд, ТФ КБ) було прийняте Північноатлантичним Альянсом під час Уельського саміту Альянсу 4 вересня 2014 року [5].

Цьому рішенню передувала злагоджена робота багатьох інституцій та установ на міждержавному і національному рівнях, що потребувала

залучення великої кількості провідних фахівців з боку всіх сторін, зацікавлених в успіху цього проекту.

Особливий внесок у забезпечення реалізації цього проекту зробили представники штаб-квартири Альянсу, Міжнародного секретаріату НАТО, Офісу НАТО в Україні, Місії України при НАТО та Румунії як провідної країни ТФ КБ НАТО.

Необхідно нагадати певні чинники, що обумовили доцільність започаткування ТФ КБ та на сьогодні визначають необхідність його подальшого розвитку.

Стан кібербезпеки в Україні у 2014 році свідчив та продовжує вказувати сьогодні про те, що кіберпростір залишається критично слабкою складовою державної 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.

Відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287, однією з основних загроз кібербезпеці і безпеці державних інформаційних ресурсів визначено вразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів України [6].

Стратегією кібербезпеки України, затвердженою Указом Президента України від 15 березня 2016 року № 96, визначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури [7].

Для забезпечення належних умов безпечного функціонування кіберпростору Стратегією кібербезпеки України передбачено створення

Національної системи кібербезпеки. Зазначене завдання, насамперед, спрямовано на посилення спроможностей суб'єктів сектору безпеки і оборони для ефективної боротьби з кіберзагрозами та кібертероризмом та забезпечення кіберзахисту критичної інформаційної інфраструктури держави.

Одним з дієвих механізмів, що має сприяти виконанню цього завдання, є проект Трастового фонду Україна – НАТО з кібербезпеки, який за своїм основним призначенням спрямовано на підвищення технічних можливостей України у сфері кібербезпеки.

Головним виконавцем заходів з реалізації проектів Трастового фонду є Служба безпеки України.

Принциповим організаційним та технічним задумом проекту першого етапу Трастового фонду є розбудова мережі ситуаційних центрів кібербезпеки, базовими з яких стали центри СБУ та Держспецзв'язку. Фактично на першому етапі реалізації Трастового фонду створено центральну складову національної системи кібербезпеки, організаційно-технологічним фундаментом для якої є ресурси Ситуаційного центру забезпечення кібербезпеки СБУ і Державного центру кіберзахисту та протидії кіберзагрозам Адміністрації Держспецзв'язку України (CERT-UA).

Станом на поточний час відповідно до умов Угоди про реалізацію першого етапу Трастового фонду Україна – НАТО з питань кібербезпеки між Службою безпеки України та Румунською службою інформації в Україну поставлено технічне обладнання та програмне забезпечення, практичне використання якого спрямоване на розширення можливостей із захисту критичної інфраструктури України від кібернетичних атак.

Отримане комп'ютерне обладнання призначене для аналізу великих обсягів даних (ідентифікаторів) про підготовку та здійснення кібератак на інформаційно-телекомунікаційні системи державних органів України.

На сьогодні СБУ спільно з Держспецзв'язку завершує заходи з інтеграції вказаного обладнання у загальну інфраструктуру Національної системи кібербезпеки (далі – НСК), зокрема на майданчику МЗС України.

На його базі започатковано створення розгалуженої мережі автоматизованих датчиків подій, якими будуть оснащені інформаційно-телекомунікаційні системи (далі – ІТС) МЗС України, що підлягають захисту у реальному часі. Управління мережею та реагування на комп'ютерні інциденти планується здійснювати ситуаційними центрами кібербезпеки СБУ та Держспецзв'язку.

Про успішне завершення першого етапу Трастового фонду Україна – НАТО з питань кібербезпеки свідчить спільна заява Голови СБУ В. Грицака, заступника Генерального секретаря НАТО С. Дукару та заступника директора Румунської служби інформації К. Бізадя, зроблена 4 липня 2017 року [8].

При цьому сторонами досягнуто домовленостей щодо започаткування другого етапу Трастового фонду Україна – НАТО з питань кібербезпеки, оскільки розроблення та вдосконалення механізмів захисту об'єктів критичної інфраструктури від зовнішніх посягань є критично важливим питанням в умовах сьогодення. У подальшому до спільного контуру безпеки планується включити всі важливі для держави і суспільства об'єкти сектору безпеки та оборони, охорони правопорядку та галузеві об'єкти критичної інформаційної інфраструктури держави.

Одним з основних напрямів підвищення технічних можливостей України у сфері кібербезпеки в рамках реалізації другого етапу Трастового фонду Україна – НАТО з питань кібербезпеки є впровадження системних технологічних рішень, спрямованих на забезпечення захищеності державних інформаційних ресурсів та автоматизованих систем на об'єктах критичної інфраструктури держави від окремих кібернетичних інцидентів та цільових кібернетичних атак. Указані рішення мають реалізовувати основні функціональні складові технологічної інфраструктури НСК, що

призначені для ефективного вирішення завдань із своєчасного виявлення та реагування на комп'ютерні інциденти, прийняття управлінських рішень щодо усунення їх наслідків, попередження та протидії цільовим кібернетичним атакам, спрямованим на порушення сталого функціонування електронних інформаційних ресурсів та автоматизованих систем на об'єктах критичної інфраструктури держави.

Ефективна розбудова технологічної інфраструктури НСК вимагає розподілу всього спектра діяльності щодо забезпечення захищеності на два види: діяльність із кіберзахисту та кібербезпеки, які, попри єдину мету (забезпечення стану захищеності), мають різні функціональні завдання:

- суб'єкти кіберзахисту концентрують свої зусилля на об'єкті захисту – їх головне функціональне завдання полягає у створенні умов найкращого захисту, який унеможливить реалізацію кібератак та рецидивне відтворення кіберінцидентів;
- суб'єкти кібербезпеки концентрують свої зусилля на суб'єкті атаки – їх головне функціональне завдання полягає у протидії та нейтралізації підривної діяльності спеціальних служб іноземних держав, організацій, окремих груп та осіб, що готують або вчиняють кібератаки, організовують, замовляють чи фінансують їх вчинення.

Зазначений розподіл є принциповим і враховує наявні законодавчо закріплені повноваження суб'єктів силового блоку та органів державної влади, які реалізують політику кіберзахисту, а також дає змогу виокремити основні функціональні складові технологічної інфраструктури НСК.

Основою такої інфраструктури має стати система розподілених за адміністративно-територіальним та галузевим принципами функціонально споріднених автоматизованих інформаційних систем, що створюють мережу ситуаційних центрів швидкого реагування та забезпечують збалансоване застосування сил і засобів забезпечення кіберзахисту та кібербезпеки на конкретному об'єкті відповідно до визначеного типу (моделі) реальних або потенційних кіберзагроз.

Обрання подальших підходів до побудови центрів залежить від наявної структури галузей, сформованих реальним сектором економіки, розподілом сфер державного управління або відповідним адміністративно-територіальним розподілом. Таким чином, ситуаційні центри кіберзахисту та кібербезпеки можуть бути: галузевими або міжгалузевими, відомчими або міжвідомчими, загальнодержавними або регіональними чи територіальними.

Основними елементами, що створюють інфраструктуру НСК, є об'єднані в єдину мережу за допомогою функціонально споріднених автоматизованих інформаційних систем:

1) ІТС об'єктів критичної інфраструктури;
2) ситуаційні центри кіберзахисту;
3) ситуаційні центри кібербезпеки.

Центри, що створюються на вищому функціональному рівні ієрархічної структури НСК, становлять мережу загальнодержавних центрів та враховують:

– розподіл за видами діяльності на суб'єкти забезпечення кіберзахисту та кібербезпеки;

– специфіку системних кіберзагроз, які включають потенційні та реальні кіберзагрози у різних сферах: національної безпеки, воєнній, фінансово-економічній тощо;

– наявну структуру галузей, сформованих реальним сектором економіки, розподілом сфер державного управління або відповідним адміністративно-територіальним розподілом.

Отже, мережу загальнодержавних центрів створюють: ситуаційні центри кіберзахисту Держспецзв'язку, МВС, Міноборони, а також ситуаційні центри кібербезпеки СБУ, Генерального штабу Збройних Сил, Національної поліції, Головного управління розвідки Міноборони, Служби зовнішньої розвідки.

Подальше масштабування інфраструктури НСК щодо створення відомчих, галузевих або регіональних ситуаційних центрів доцільно спланувати на наступних етапах залежно від потенціалу можливостей загальнодержавних центрів, який буде напрацьовано під час підключення та обслуговування відповідних об'єктів критичної інфраструктури.

Основними функціональними напрямами масштабування ІТС об'єктів критичної інфраструктури насамперед є:

захист ПЕОМ користувачів від шкідливого програмного забезпечення, несанкціонованого втручання з використанням уразливостей операційних систем та прикладного програмного забезпечення, а також шкідливих дій інсайдера;

захист від порушень цілісності, правил маршрутизації або витоку даних з локальних мереж, у тому числі під час обміну даними з іншими закритими мережами;

захист прикладних інформаційних ресурсів (обмін файлами, документообіг, бази даних), спільних для всіх користувачів або окремих груп, зокрема їх резервування та відновлення;

захист службових або публічних бездротових мереж (Wi-Fi);

захист DNS-трафіка;

захист публічних веб-ресурсів, зокрема їх доступності;

захист ресурсів електронної пошти, інших внутрішніх засобів електронної комунікації;

захист внутрішніх засобів, що забезпечують інтернет-доступ користувачів;

створення належних умов для функціонування засобів моніторингу шляхом установлення сенсорів подій, аналіз у реальному часі подій кібербезпеки (SIEM) та автоматизації використання ідентифікаторів компрометації (IOK).

Основні функціональні напрями масштабування ситуаційних центрів кіберзахисту:

розгортання мережі сенсорів подій на підпорядкованих Держспецзв'язку, МВС, Міноборони України об'єктах, забезпечення їх сталого функціонування, моніторингу та технічного захисту даних про кіберінциденти;

автоматизований аналіз у реальному часі подій кібербезпеки (SIEM);

автоматизація використання ідентифікаторів компрометації (IOK), які надходитимуть від ситуаційних центрів кібербезпеки;

забезпечення швидкого реагування на кіберінциденти шляхом організації взаємодії з Ситуаційним центром кіберзахисту Держспецзв'язку;

обстеження та оцінка стану захищеності об'єктів, надання відповідних рекомендацій у частині вдосконалення засобів захисту.

Основні функціональні напрями масштабування ситуаційних центрів кібербезпеки:

автоматизований аналіз у реальному часі подій кібербезпеки (SIEM) для з'ясування механізму та встановлення суб'єктів атаки;

автоматизація аналітичної діяльності з обробки масивів даних про кіберінциденти з урахуванням криміналістичної, оперативної та технологічної інформації;

автоматизація створення ідентифікаторів компрометації (IOK) за кіберінцидентами, які розслідуються в рамках кримінальних проваджень у сфері кіберзлочинності;

забезпечення криміналістичного дослідження даних, отриманих у рамках кримінальних проваджень у сфері кіберзлочинності;

автоматизація пошуку (збору) даних з відкритих джерел та їх кореляції з наявними масивами даних про кіберінциденти, які розслідуються в рамках кримінальних проваджень у сфері кіберзлочинності;

автоматизація обміну інформацією між територіально розосередженими оперативно-слідчими групами, які розслідують справи про кіберзлочини;

автоматизація процесів моделювання та прогнозування розвитку подій для забезпечення прийняття рішень в умовах кризових або надзвичайних ситуацій, пов'язаних з кіберінцидентами.

Крім того, в рамках подальшої реалізації проектів Трастового фонду передбачається створення на базі Головного об'єднаного центру захисту інформації та кібернетичної безпеки в ІТС Збройних Сил України міжвідомчого Центр ситуаційного моделювання систем кіберзахисту у сфері безпеки та оборони з такими функціями:

моделювання мережевої інфраструктури об'єктів кіберзахисту, їх захисних механізмів, інформаційних потоків тощо;

моделювання інформаційних процесів, що відбуваються на об'єктах кіберзахисту в ході кібератак, відпрацювання ефективних практик кіберзахисту та процедур реагування на інциденти з метою оцінки захищеності об'єктів, перевірки версій розвитку подій, створення прогнозів, з'ясування можливостей усунення негативних наслідків, вразливостей тощо;

міжвідомчої платформи для проведення навчань та тренінгів, у тому числі за участю іноземних партнерів.

Технологічну основу Центру моделювання має становити комплекс програмно-апаратних засобів обробки даних та типових засобів забезпечення кіберзахисту та кібербезпеки, які можуть бути штучно об'єднані за допомогою засобів віртуалізації, хмарних технологій та сучасних телекомунікаційних засобів в єдину топологічно гнучку мережу.

Висновки. Забезпечення кібербезпеки є невід'ємною складовою заходів з реалізації державної політики у сфері забезпечення національної безпеки. Водночас міжнародне співробітництво, насамперед, співробітництво України із НАТО суттєво посилює спроможності України щодо протидії усьому спектру кіберзагроз. З одного боку, наша держава за рахунок використання інтелектуальних та матеріальних ресурсів Трастового фонду НАТО з питань кібербезпеки зміцнює власний кіберзахист, з іншого, таке співробітництво вигідне й Альянсу, оскільки дозволяє в реальних умовах

випробувати технічні та організаційні рішення. Крім того Україна стає країною- контрибутором кібербезпеки на усьому євроатлантичному просторі, що підвищує її значущість для забезпечення колективної оборони Альянсу та, у кінцевому підсумку, сприяє розвитку партнерських та союзницьких стосунків України з НАТО.

Список використаних джерел

1. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва / Д.В. Дубов. – К. : НІСД, 2014. – 328 с.
2. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization [Electronic resource]. - Access mode: www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf.
3. Chicago Summit Declaration [Electronic resource]. - Access mode: http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode= pressrelease.
4. Cyber defence [Electronic resource]. - Access mode: http://www.nato.int/cps/en/natohq/topics_78170.htm.
5. Підтримка України з боку НАТО [Електронний ресурс]. - Режим доступу: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-nato-ukraine-support-ukr.pdf.
6. Указ Президента України № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про стратегію кібербезпеки України»» [Електронний ресурс]. – Режим доступу http://www.rnbo.gov.ua/documents/417.html.
7. У СБУ відбулася церемонія завершення першого етапу Трастового фонду НАТО зі сприяння Україні в зміцненні кіберзахисту [Електронний ресурс]. - Режим доступу: https://www.ssu.gov.ua/ua/news/1/category/2/view/3668#.dnBn8P1V.dpbs