УДК 341.4

В. В. МАРКОВ,
кандидат юридичних наук, старший науковий співробітник,
начальник факультету підготовки фахівців для підрозділів боротьби
з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ;

О. В. КАРАЧЕНЦЕВ,
курсант
факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

НАПРЯМИ ДІЯЛЬНОСТІ НАТО У СПРАВІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Досліджено проблему протидії кіберзлочинності, що є загрозою міжнародній інформаційній безпеці, у рамках Організації Північноатлантичного договору (НАТО), проаналізовано напрями діяльності НАТО і організаційні форми співпраці з Україною у зазначеній сфері. Запропоновано шляхи вирішення окремих питань проблеми.

Ключові слова: *Організація Північноатлантичного договору, НАТО, кіберзлочинність, кіберпростір, міжнародна інформаційна безпека, хакери, кібератака, кіберзахист.*

XXI століття – час стрімкого розвитку цифрових технологій і масової комп'ютеризації. Вони максимально спростили людині всі технологічні та виробничі процеси, полегшили існування і змінили уявлення про роботу, кар'єру, дозвілля, фінанси та навіть особисте життя. Водночас це приховує і серйозні загрози.

Щодня системи інформаційної безпеки по всьому світу знешкоджують близько 250 тисяч кібератак. Кожен несанкціонований злам надає хакерам доступ до особистих даних сотень інтернет-користувачів. Тільки за минулий рік кількість хакерських атак по всьому світу зросла на 42 %. За цей період їм піддалися компанії та державні організації 27 країн світу. За даними компанії Symantec, близько 75 % атак здійснюють з метою збагачення. Крім них є і так звані «протестні» кібератаки – з політичним підґрунтям [1].

Актуальність теми цього наукового дослідження обумовлена тим, що зростання інформаційних технологій призводить не тільки до прогресивних змін в економіці, але і негативних тенденцій розвитку злочинного світу, до появи нових форм і видів злочинних посягань. Це проявляється у тому, що зловмисники активно використовують у своїй злочинній діяльності новітні комп'ютерні засоби і нові інформаційні технології. Розповсюдження комп'ютерних вірусів і дитячої порнографії, шахрайство з пластиковими платіжними картками, розкрадання грошових коштів із банківських рахунків, комп'ютерний тероризм – це далеко не повний перелік подібних злочинів, які отримали поширену назву «кіберзлочинність».

У сфері вирішення питань протистояння сучасним загрозам в інформаційній сфері продовжує залишатися актуальною тема налагодження і розвитку всебічної співпраці різних держав у рамках міжнародних міжурядових організацій (ООН, НАТО, Інтерпол, Європол).

Вивчення стану наукової розробленості проблематики співпраці і взаємодії держав у боротьбі з кіберзлочинністю показало, що на сучасному етапі спеціального дослідження з цих проблем не проводилося. Проте необхідно відзначити, що окремі аспекти такої співпраці розглядалися в наукових роботах Ю. М. Батуріна, П. Д. Біленчука, В. Б. Вєхова, В. О. Голубєва, М. Д. Діхтярєнко, Б. Х. Толеубекова, І. Л. Сафронова, А. В. Крутських, О. О. Смирнова та ін. Незважаючи на наявність значного обсягу наукових праць і досліджень, присвячених цій проблемі, окремі питання міжнародного співробітництва у боротьбі з кіберзлочинністю залишаються не повністю дослідженими.

Метою цієї статті є комплексне вивчення проблем, пов'язаних із налагодженням і здійсненням міжнародного співробітництва у боротьбі з кіберзлочинністю в рамках Організації Північноатлантичного договору (НАТО), і на базі цього розробка пропозицій, направлених на підвищення ефективності протистояння кібератакам.

Звичайно, викладені положення у цій науковій статті можуть бути використані практично, а саме в науково-дослідницькій сфері для подальших наукових досліджень цієї проблеми, в науково-освітній сфері під час викладання навчальних дисциплін, у науково-методичній сфері з метою вдосконалення, розробки навчальних

програм, підручників і навчально-методичних посібників, а також у правоохоронній діяльності різних держав.

У межах цього наукового дослідження насамперед потрібно зазначити, що кіберзлочинність – це злочинність у так званому «віртуальному просторі». Віртуальний простір (або кіберпростір) можна визначити як модельований за допомогою комп'ютера інформаційний простір, в якому знаходяться відомості про осіб, предмети, факти, події, явища і процеси, наведені в математичному, символьному або будь-якому іншому вигляді і що знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки і передачі [2].

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.

Досвід вірусу «Стакснет», який серйозно зашкодив ядерній програмі Ірану в 2010 році, вказує на перехід від кіберсвіту до фізичного світу. В сучасних умовах розвитку інформаційно-комунікаційних технологій існує багато інформаційних ресурсів, пошкодження яких може призвести до порушення роботи як окремих компаній, так і функціонування держав у цілому.

Враховуючи вразливість міжнародної інформаційної безпеки, кіберзахист став одним із пріоритетних напрямів діяльності НАТО. На думку експертів НАТО, всі майбутні політичні й військові конфлікти будуть відбуватися саме в кібернетичному просторі, а країни, які до них належним чином не підготуються, будуть надзвичайно вразливими. Істотно підвищити рівень безпеки кіберпростору можна тільки завдяки тісному співробітництву, використовуючи сучасні комп'ютерні технології [3].

Інформаційно-комунікаційна система НАТО і її окремих країн-членів потерпають сьогодні від численних кібератак. Задля протистояння кіберзлочинності НАТО повинна надавати допомогу у сфері кіберзахисту своїм членам, допомагаючи їм запобігати таким нападам, виявляти їх, а в разі нападу швидко реагувати заради зменшення шкоди.

З метою протидії різним проявам кіберзлочинності НАТО ще у 2011 році розпочала формулювати концепцію Групи швидкого реагування. Створення цієї групи стало результатом перегляду політики кіберзахисту НАТО, яка була переглянута міністрами оборони країн-членів Організації у червні 2011 року. Зазначені фахівці з кіберзахисту відповідальні за надання допомоги країнам-членам, які звертаються по допомогу в разі нападу національного значення.

Кібернапади такого типу, яких зазнали Естонія і Грузія, в майбутньому стануть найбільш поширеною формою хакерського нападу. Все частіше в суспільстві проявляється суміш протестів або звичайних воєнних дій із кібернетичним елементом. Тому групи швидкого реагування НАТО мають бути готовими до дій негайно в міру необхідності.

Технічний центр Сил реагування НАТО на комп'ютерні інциденти NCIRC (NATO Computer Incident Response Capability) став мозковим вузлом боротьби Альянсу проти кіберзлочинності. NCIRC відповідає за кіберзахист усіх інформаційних ресурсів НАТО, незалежно від того, належать вони постійним штабам, чи штабам розгорнутим на час операцій чи навчань [4].

На початку 2012 року НАТО підписала контракт вартістю 67 млн доларів США з італійською компанією Finmeccanica на розробку, впровадження й обслуговування програми кіберзахисту NCIRC. У рамках угоди італійська компанія, за підтримки американської Northrop Grumman, забезпечить інформаційну безпеку приблизно 30 важливим об'єктам і штабквартирам НАТО у 28 країнах світу [5].

NCIRC досяг цілковитої оперативної готовності на початку 2013 року. Були розроблені умови співробітництва, в тому числі між експертами, які користуються взаємною довірою і представляють країни, промисловість, академічні кола і НАТО. Ці домовленості зрештою відкрили доступ до спеціальних знань в усіх сферах кібербезпеки. Розроблені також вимоги до експертів, які беруть участь у місіях із надання допомоги, визначаються сфери їх компетенції.

Усі процедури Групи швидкого реагування НАТО і можливі дії визначено в посібнику, над яким надалі продовжують працювати експерти у галузі протидії кіберзлочинності і фахівці з планування на випадок надзвичайних ситуацій цивільного характеру. У цьому посібнику закріплено рекомендації щодо реагування НАТО на прохання країн Альянсу і партнерів про допомогу в захисті їхніх інформаційних і комунікаційних систем.

Маючи Групи швидкого реагування, НАТО зможе на запит запропонувати професійну і добре організовану допомогу своїм країнам-членам і партнерам, але передусім тим країнам, які поки що не мають ресурсів для створення такого роду оборонних сил. Це одна з версій військового принципу взаємодопомоги та колективної оборони.

Сили швидкого реагування складаються з постійного ядра з шести спеціалістів, які здатні координувати і виконувати місії Групи швидкого реагування. У певних сферах можуть бути задіяні національні експерти й експерти з НАТО. Їх кількість і характер залежатимуть від місії, яку необхідно буде виконувати.

Групи швидкого реагування мають усе необхідне оснащення: комп'ютерне і телекомунікаційне обладнання, таке як супутникові телефони і обладнання для цифрового збирання свідчень, криптографії, цифрового судового аналізу, зниження вразливості, безпеки мереж тощо.

Будь-яка країна – член НАТО, яка постраждала від серйозного кібернападу, зможе звернутися до Альянсу по допомогу. Такий запит розгляне Комісія з менеджменту кіберзахисту (CDMB). Прохання про допомогу, які надходитимуть від країн – не членів НАТО, будуть затверджуватися Північноатлантичною радою.

У разі приведення в дію Групи швидкого реагування НАТО зможуть відреагувати на інцидент протягом 24 годин [4].

З метою вироблення спільної позиції у справі протидії кіберзлочинності під егідою НАТО проводяться різноманітні міжнародні науково-практичні конференції. Так, в м. Таллінні (Естонія) з 5 по 9 червня 2012 року відбулася міжнародна конференція, присвячена проблемам кіберзахисту «4rd International Conference on Cyber Conflict», організована Талліннським Центром НАТО з кіберзахисту. Традиційно в ній взяли участь понад 300 представників 37 країн – членів НАТО та держав – учасниць партнерських програм Альянсу. Головною метою обговорення були військова і воєнізована діяльність у кіберпросторі. Ця проблема розглядалася всебічно – з політичної, юридичної, технічної точок зору [5].

Враховуючи партнерські стосунки НАТО з Україною як активним учасником кіберпростору, у справі протидії різноманітним посяганням на комп'ютерні мережі Організація почала здійснювати відпрацювання зі Службою безпеки України спільних механізмів боротьби з кіберзлочинністю. Так, в м. Ялті 11–13 жовтня 2011 року відбулися міжнародні експертні консультації «Україна – НАТО». В обговоренні, організованому Радою національної безпеки і оборони України, взяли участь представники НАТО, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, Міністерства оборони України, Служби зовнішньої розвідки України, Міністерства внутрішніх справ України, Міністерства закордонних справ України; міністерства оборони Естонії, наукових інститутів Туреччини, Румунії, Франції та Польщі.

Експертні консультації у рамках роботи групи «Україна – НАТО» мали на меті відпрацювання механізмів міжнародного співробітництва та спільних програм із залученням представників гілки державного управління та приватного сектора у питаннях захисту інформаційної сфери держави. Вітчизняні та іноземні учасники робочих зустрічей обговорили найбільш актуальні питання розвитку систем захисту кіберпростору, зокрема особливості забезпечення кібернетичної безпеки за умов інформатизації; взаємодії державного та приватного секторів у питаннях захисту інформаційної сфери держави; особливості обробки персональних даних в контексті кібернетичного захисту; проблеми формування недержавного сектору безпеки України; сучасні загрози інтернет-простору. Представники Ради національної безпеки і оборони України розповіли про роботу над проектом Стратегії України у галузі кібернетичного захисту. Під час Консультацій сторони обмінялися досвідом із питань протистояння кібернетичним загрозам. Обговорювалися суто практичні аспекти – особливості правозастосовної діяльності, розслідування, попередження та протидії кіберзлочинності, шляхи розбудови системи реагування на кібернетичні атаки на національні інформаційні інфраструктури тощо.

На думку багатьох фахівців, відсутність міжвідомчої структури, яка координуватиме діяльність державних органів та спецслужб, гальмує роботу у справі протидії кіберзлочинності. Нині функції захисту інформації з обмеженим доступом покладено на різні структури (Держспецзв'язку, СБУ, МВС). Для більш тісного й ефективного співробітництва у справі протидії кіберзлочинності підкреслюється на необхідності створити Україною міжвідомчу структуру по боротьбі з кіберзлочинністю для координації дій державних органів у цій сфері [6].

Варто відзначити, що певна координаційна робота ведеться в межах діяльності Робочої підгрупи Спільної робочої групи Україна – НАТО високого рівня з питань кібернетичного захисту, створеної в Апараті Ради національної

безпеки і борони України. Цю групу створено в межах Спільної робочої групи з питань воєнної реформи. В межах роботи цієї Робочої групи було об'єднано зусилля основних відомств, що задіяні у сфері кібербезпеки держави (принаймні на рівні інституцій, що формують політику в цій сфері). З боку НАТО співголовою цієї групи до останнього часу був С. Аніл (Голова служби кіберзахисту та контрзаходів, Офісу з безпеки НАТО).

Під час засідання міністрів оборони країн – членів НАТО, що відбулася 3 червня 2014 року в м. Брюсселі (Бельгія), представники країн – членів Організації і України намітили шляхи зміцнення партнерства між Альянсом і Україною. Високопосадовці НАТО обговорили шляхи надання Україні довгострокової допомоги, спрямованої на реформування її сил безпеки та оборони.

На додаток до пакету заходів НАТО окремі члени Альянсу добровільно надають Україні консультативну, технічну та матеріальну допомогу.

Для допомоги у проведенні української оборонної реформи НАТО створила трастові фонди. П'ятий фонд покликаний боротися з кіберзлочинністю і спрямований на розвиток систем кіберзахисту відповідно до найпрогресивніших стандартів країн – членів НАТО. Контрибуторами цього фонду стали Естонія, Румунія, Туреччина, Угорщина [7].

У межах цього дослідження слід зазначити, що на саміті НАТО, який відбувся у вересні 2014 року в Уельсі (Великобританія), представники 28 країн-членів висловили свої позиції стосовно офіційного застосування міжнародно-правових норм ведення війни щодо кібератак, що здійснюються у віртуальному просторі [8].

Вважаємо, що наслідки такого запровадження допоможуть і Україні протистояти у цих невидимих війнах, оскільки останнім часом ми зіткнулися із гібридом інформаційної війни та кібератак. Підготовка анексії українського півострову Крим та розв'язання збройного конфлікту на Донбасі планувалися та реалізовувалися на базі багатолітньої інформаційної війни. Війни, якій багато хто не надавав належного ступеня небезпеки. І особливий вплив тут відіграв Інтернет і засоби масової інформації, зокрема телебачення.

У **підсумку** цього наукового дослідження зазначимо, що Україна потребує адекватної системи інформаційної безпеки, що трансформується, де виклики національній безпеці все частіше набувають рис, відмінних від традиційних загроз. Питання захисту у кіберпросторі є питаннями національної безпеки. Найкращим варіантом для України є приєднання до НАТО і спільними зусиллями з іншими членами Альянсу розбудова та застосування систем колективної безпеки від кібератак та інформаційної війни, а не залишатися наодинці у цьому складному протистоянні.

До моменту вступу до НАТО Україна має стати активним учасником процесів під егідою ООН із вироблення єдиних підходів до міжнародної інформаційної безпеки та демілітаризації кіберпростору.

Список використаних джерел

1. Кіберзлочинність: глобальний масштаб : 14 жовт. 2013 р. [Електронний ресурс] // Голос Столиці. – Режим доступу: http://newsradio.com.ua/radio_broadcast/122868066/122873429.

2. Голубев В. А. «Кибертерроризм» – миф или реальность? [Електронний ресурс] / В. А. Голубев ; Центр исслед. компьютер. преступности. – Режим доступу: http://www.crime-research.org/library/terror3.htm.

3. Masssimoua. НАТО разом з Україною хоче боротися з кіберзлочинністю : [блог] : 12 лют. 2010 р. [Електронний ресурс] / masssimoua. – Режим доступу: http://masssimoua.blog.ru/86858499.html?attempt=1.

4. Група швидкого реагування НАТО для боротьби проти кібернападів : 13 берез. 2012 р. [Електронний ресурс] // Організація Північноатлантичного договору : [сайт]. – Режим доступу: http://www.nato.int/cps/uk/natohq/news_85161.htm?selectedLocale=uk.

5. Котух Є. Кіберзброя: проблеми та перспективи протидії кіберзлочинності : 24 квіт. 2012 р. [Електронний ресурс] / Євгеній Котух // З.С. : зовнішні справи : [сайт] / UA Foreign Affairs. – Режим доступу: http://www.uaforeignaffairs.com/en/expert-opinion/view/article/kiberzbroja-problemi-ta-perspektivi-protidiji-kiberzlo/.

6. У Ялті відбулися міжнародні експертні Консультації «Україна-НАТО» з питань кібернетичного захисту : 12 жовт. 2011 р. [Електронний ресурс] / Прес-центр СБ України // Служба безпеки України : офіц. вебсайт. – Режим доступу: http://www.sbu.gov.ua/sbu/control/uk/publish/article?art_id=108904. – Назва з екрана.

7. НАТО запустив трастові фонди для допомоги Україні : 2 груд. 2014 р. [Електронний ресурс] / за матеріалами: Интерфакс-Украина // Forbes Україна : [сайт] / Укр. Медіа Холдинг ; Forbes Media LLC™. – Режим доступу: http://www.forbes.ua/ua/news/1384031-nato-zapustiv-trastovi-fondi-dlya-dopomogi-ukrayini.

8. Богомазов П. Інформаційна війна та кіберзлочинність в Україні у 2014 році : [блог] : 21 лип. 2014 р. [Електронний ресурс] / Павло Богомазов. – Режим доступу: http://www.blog.liga.net/user/pbogomazov/article/15158.aspx.

Надійшла до редколегії 17.12.2014

МАРКОВ В. В., КАРАЧЕНЦЕВ А. В. НАПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТИ НАТО В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Исследована проблема противодействия киберпреступности, являющейся угрозой международной информационной безопасности в рамках Организации Североатлантического договора (НАТО), проанализированы направления деятельности НАТО и организационные формы сотрудничества с Украиной в указанной сфере. Предложены пути решения отдельных вопросов проблемы.

Ключевые слова: *Организация Североатлантического договора, НАТО, киберпреступность, киберпространство, международная информационная безопасность, хакеры, кибератака, киберзащита.*

MARKOV V. V., KARACHENTSEV O. V. THE DIRECTION OF NATO ACTIVITIES IN COMBATING OF THE CYBERNETIC CRIME

The purpose of this paper is the comprehensive study of the problems related to the implementation of international partnership in the fight against the cybernetic crime in the framework of NATO, as well as the proposals aimed at improving the efficiency of the combating cybernetic attacks that has been developed on this study.

The cybernetic protection has become one of the priorities of NATO activities because of the international information security vulnerability. For this purpose NATO was established NCIRC (NATO Computer Incident Response Capability) as the technical center of the Rapid Reaction Forces and this center is responsible for the cybernetic protection of all information resources of the Alliance.

To develop the common position in the fight against the cybernetic crime the international conferences operate under NATO auspices; military and paramilitary activities in cyberspace are discussed at these conferences.

According to the partnership between Ukraine and NATO the Organization began to work out common mechanisms to combat the cybernetic crime with the Security Service of Ukraine. For this purpose the expert consultations take place within the framework of the group «Ukraine – NATO».

The coordinating work carried out in the framework of the Sub-Working Group of the high-level General working group Ukraine – NATO which was established in the Office of National Security and Defense Council of Ukraine.

The individual members of the Alliance provide Ukraine the advisory, technical and material assistance. For example, for Ukrainian defense reform, NATO has created the trust funds. The fifth fund is designed to combat the cybernetic crime; it also aimed to develop the systems of cybernetic protection in accordance to the standards of NATO member countries.

In conclusion, we note that Ukraine requires an adequate system of information security. The best option for Ukraine would be joining NATO and then the creation by the joint efforts the collective security system against cybernetic attacks and information warfare for its joint usage.

Until the entry into NATO Ukraine has to become under the auspices of the UN the active participant in the process of elaboration of common approaches in the field of international information security and demilitarization of cyberspace.

Keywords: *North Atlantic Treaty Organization, NATO, cybercrime, cyberspace, international information security, hackers, cyber attacks, cyber defense.*

УДК 343.985

А. М. МЕДЕНЦЕВ,
здобувач кафедри кримінального права, процесу та криміналістики Міжнародного гуманітарного університету (м. Одеса)

СЛІДЧІ СИТУАЦІЇ ПОЧАТКОВОГО ЕТАПУ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ ДЕРЖАВНИХ ЗАКУПІВЕЛЬ

Наведено типові слідчі ситуації початкового етапу розслідування злочинів у сфері державних закупівель. Визначено роль та зміст матеріалів ревізій (перевірок), проведених державними органами, які здійснюють контроль у сфері держаних закупівель.

Ключові слова: *злочини у сфері державних закупівель, бюджетні кошти, початковий етап розслідування, типова слідча ситуація.*

Одним із проблемних питань сьогодення для правоохоронних органів є питання протидії економічним злочинам, зокрема у сфері державних закупівель. Неефективне використання бюджетних коштів та їх розкрадання є одним із найбільш прихованих і небезпечних різновидів