УДК 343.543

ЩОДО ФОРМУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ УКРАЇНИ

Петров Валентин Володимирович,
кандидат політичних наук

Проаналізовано стан і перспективи формування Національної системи кібербезпеки як одного з елементів системи забезпечення національної безпеки України.
Ключові слова: **кібернетична безпека, кіберпростір, національна система кібербезпеки, сектор безпеки і оборони.**

Аналіз сучасного стану забезпечення національної безпеки держави, зокрема інтересів України у сфері інформаційної безпеки, свідчить про актуальність загроз, пов'язаних із досить високим рівнем транснаціональної кіберзлочинності, а також активізацією спроб використання сучасних інформаційних технологій іноземними державними органами, організаціями, групами осіб та окремими особами на шкоду національним інтересам.

Метою даної статті є висвітлення актуальних проблем формування національної системи кібернетичної безпеки як одного з елементів забезпечення національної безпеки держави.

Завдання цієї статті – дослідити сучасний стан забезпечення національної безпеки в інформаційній (кібернетичній сфері), зокрема її нормативно-правове забезпечення в контексті триваючого процесу реформування сектору безпеки та оборони.

Різні аспекти забезпечення кібернетичної безпеки розглядались у працях відомих вітчизняних та іноземних науковців, зокрема В. Богдановича, Г. Броді, В. Бутузова, К. Гаджиєва, Д. Дубова, С. Гнатюка, У. Ліппмана, М. Ожевана, М. Присяжнюка, Д. Прудникова, В. Телелима, В. Толубка, Г. Семигіна, В. Шеломенцева, Л. Шеллі та ін. Проте у працях зазначених авторів недостатня увага приділялася вирішенню завдань методологічного та організаційного забезпечення створення Національної системи кібернетичної безпеки, оскільки це завдання є новим для сектору національної безпеки і оборони та для держави загалом.

Загальносвітовою є стійка тенденція зростання числа комп'ютерних атак на важливі об'єкти національних інфраструктур іноземних країн, що призводило й призводить до завдання шкоди державам через спотворення та витоки важливої для них інформації, блокування виробничих процесів на стратегічних об'єктах. Зазначене зумовило зміну зовнішньополітичних доктрин провідних ядерних країн світу, згідно з якими кібератаки прирівнюються до військових дій та передбачають можливість завдання воєнних ударів у відповідь.

Нова Стратегічна концепція Альянсу на 2011–2020 роки [1], ухвалена під час Лісабонського саміту країн-членів НАТО, фактично прирівняла загрозу кібертероризму до військових загроз, що своєю чергою передбачає можливість відповіді на масовані кібератаки із застосуванням національних збройних сил. Кіберзагрози стали одним із найбільш небезпечних викликів безпеці країн-членів Альянсу, а забезпечення інформаційної безпеки було визначене другим за значимістю пріоритетом. Доктрина НАТО з кібербезпеки [2] визначає співробітництво з державами-партнерами у сфері розбудови системи забезпечення кібернетичної безпеки Альянсу як ключовий механізм заходів із забезпечення кіберзахисту.

Вказана позиція була підтверджена в резолюції Чиказького саміту НАТО у травні 2012 р. [3]. Зокрема, у п. 49 резолюції йдеться про готовність Альянсу співпрацювати з іноземними партнерами для організації адекватних відповідей на кіберзагрози та забезпечення власної безпеки.

Справді, досвід останніх років свідчить, що об'єктами хакерських атак все частіше стають

інформаційні системи державних установ, життєзабезпечення та фінансової сфери, тому стрімко зростають суспільні небезпеки таких дій та непередбачувані за масштабами їхні шкідливі наслідки.

Україна не лишається осторонь світових тенденцій. Оновлена у 2012 р. Стратегія національної безпеки нашої держави, затверджена відповідним Указом Президента України [4], серед основних завдань у цій сфері визначила й створення національної системи кібербезпеки.

Робота у цьому напрямку тривала декілька років. Так, ще у 2010 р. Рада національної безпеки і оборони України своїм рішенням «Про виклики та загрози національній безпеці України у 2011 році» визначила необхідність створення єдиної загальнодержавної системи протидії кіберзлочинності [5]. Водночас при реалізації цього завдання стало зрозуміло, що питання забезпечення національної безпеки в інформаційній сфері потрібно вирішувати системно, беручи до уваги не тільки загрози суто кримінального характеру, а й весь комплекс загроз, з урахуванням джерел їх походження, інструментарію, що застосовується для їх реалізації, об'єктів, на які вони спрямовуються, та мети, яка переслідується. Саме тому виникла ідея щодо створення саме національної системи кібербезпеки, яка має поєднувати у собі як комплекс адміністративних, правових, технічних та організаційних заходів у сферах захисту інформації у воєнній, правоохоронній та спеціальних сферах, так і суто оперативних – розвідувальних і контррозвідувальних заходів.

При цьому можна виділити таку типологію кібернетичних загроз:

– кібервійна;
– кібертероризм;
– кібершпигунство;
– кіберзлочинність.

Характер загроз, на перший погляд, обумовлює необхідність формування в межах національної системи кібербезпеки декількох підсистем:

– система кібербезпеки у сфері оборони;
– система боротьби з кіберзлочинністю;
– система боротьби з кіберзагрозами у сфері державної безпеки (насамперед ідеться про загрози кібертероризму та кібершпигунство).

Водночас не можна нехтувати тими глибинними трансформаціями суспільних відносин, що відбуваються в результаті всеосяжної інформатизації та проникнення сучасних інформаційних технологій в усі без винятку сфери життєдіяльності. Інформаційна революція стирає державні кордони в їх класичному розумінні, розмиває межі між діями державних органів та недержавних акторів, формуючи нове безпекове середовище, у широкому сенсі протиставляє «мережу» як форму взаємодії елементів системи ієрархії традиційного суспільства.

Дійсно, один хакер, і багато сучасних прикладів це підтверджують, може одночасно працювати сам на себе, на транснаціональне злочинне угруповання, на екстремістську групу політично вмотивованих «хактивістів», а водночас ще й на одну або навіть декілька урядових структур. Якщо взяти інструментарій, то один і той самий вірус за незначної модифікації чи навіть без неї може застосовуватися для крадіжки банківської інформації, отримання доступу до державних інформаційних ресурсів, у яких циркулює інформація з обмеженим доступом, або для перехоплення сигналів дистанційного керування зброєю. Те саме можна говорити і про бот-мережі.

Якщо виходити від об'єкта, то тут теж неоднозначна ситуація. Наприклад, банківські системи можуть бути уражені як з метою звичайної крадіжки, так і з метою дестабілізації фінансової системи країни загалом, як це було у Південній Кореї, або з метою політичного тиску, як це було у випадку з кібератаками на платіжні системи *PayPal, Mastercard* та *Visa*, які заблокували рахунки Джуліана Асанжа у 2010 р. [6].

Таким чином, слід констатувати, що перед нами постає комплекс загроз принципово нового характеру, який вимагає й нових підходів до їх вирішення.

На нашу думку, **Національна система кібербезпеки** (*далі* – НСКБ) як насамперед система взаємодії суб'єктів кібербезпеки має об'єднати спецслужби, правоохоронні органи, державні органи, що здійснюють регулювання у сфері інформатизації, телекомунікацій та захисту інформації, для своєчасного виявлення, попередження та припинення кіберзагроз, усунення передумов до їх настання та мінімізації негативних наслідків від їх реалізації. Функціонування вказаної системи є неможливим без тісної співпраці з приватним сектором – операторами та провайдерами телекомунікації, власниками та розпорядниками критичних об'єктів інформаційної інфраструктури держави, компаній, діяльність яких пов'язана зі сферою інформаційної безпеки.

При цьому організація НСКБ має забезпечуватися не тільки за згаданим «галузевим» принципом, а й за функціональним, а її складниками мають бути такі підсистеми:

– консультативно-дорадча система – система здійснення загального керівництва, су-

проведження стратегічних рішень вищого керівництва держави у сфері кібернетичної безпеки, координації дій відповідних державних органів у цій сфері;

– система моніторингу кіберзагроз – вона має поєднувати як технічні засоби, інформацію мережі *CERT*-ів (*Computer Emergency Response Team of Ukraine* – команда реагування на комп'ютерні надзвичайні події, яка функціонує на базі Державного центру захисту інформаційних ресурсів Державної служби спеціального зв'язку та захисту інформації України), дані провайдерів, банківських установ, правоохоронних органів, антивірусних компаній та ін., так і оперативну інформацію, отриману під час здійснення розвідувальної або контррозвідувальної діяльності, фінансового моніторингу тощо. При цьому вказана інформація має зосереджуватись у єдиному місці у режимі реального часу для невідкладного прийняття відповідних рішень;

– система кіберзахисту критичних об'єктів інформаційної інфраструктури держави – вона має передбачати комплекс заходів із технічного захисту інформації, безпеки персоналу, а також контррозвідувальний захист зазначених об'єктів від розвідувальних, терористичних та інших протиправних посягань.

При цьому треба враховувати важливу умову належної ефективності НСКБ – оперативність оцінки ситуації та прийняття відповідних рішень. Так, відсутність єдиного координаційного центру з питань забезпечення кібербезпеки суттєво ускладнює, уповільнює, а в деяких випадках й унеможливлює вжиття необхідних заходів з реагування на кібератаки, особливо з урахуванням їх високого ступеня латентності.

Слід зазначити, що розгортання НСКБ має супроводжуватись відповідними корективами у процесі реформування сектору безпеки та оборони. Основними суб'єктами державного сектору у сфері забезпечення кібернетичної безпеки держави нині є наступні відомства: Міністерство оборони, Міністерство внутрішніх справ, Державна служба спеціального зв'язку та захисту інформації, Служба безпеки України.

Кабінетом Міністрів України у 2013 р. був розроблений Проект закону про внесення змін до Закону України «Про основи національної безпеки» щодо кібернетичної безпеки України [7]. Вказаний законопроект має остаточно ввести у вітчизняне законодавство термін «кібернетична безпека» та похідну термінологію, що використовує префікс «кібер». Планується, що одразу після ухвалення зазначених змін МВС України буде розроблений законопроект «Про кібернетичну злочинність» [8], який має суттєво підвищити інституційну спроможність вітчизняних правоохоронних органів, забезпечити остаточну імплементацію Конвенції Ради Європи «Про кіберзлочинність» [9].

Міністерством оборони України розроблено зміни до Закону України «Про оборону», які мають урегулювати зокрема й питання забезпечення кібернетичної безпеки у воєнній сфері.

Немає сумнівів, що одним з основних елементів національної системи кібербезпеки має стати Державна служба спеціального зв'язку та захисту інформації. Водночас нагальним є суттєвий перегляд функцій цього відомства, визначений відповідним Законом України [10], саме в напрямку здійснення державного нагляду та контролю у сфері кіберзахисту критичних об'єктів інформаційної інфраструктури. На жаль, нині у цього відомства відсутні як повноваження, так і інструментарій та важелі впливу в цій сфері. Разом із тим позитивним є той факт, що в системі Держспецзв'язку функціонує спеціалізований підрозділ, про який уже згадувалося, – команда реагування на комп'ютерні інциденти (*CERT-UA*) [11].

Звичайно ж, до цієї системи має увійти і Служба безпеки України, в якій нещодавно було створено новий функціональний підрозділ контррозвідувального захисту інтересів держави у сфері інформаційної безпеки [12].

Нині законодавство [13, 14, 15] дає СБУ достатні повноваження не тільки для участі в НСКБ, а й для того, щоб бути її системоутворюючим елементом. Так, Служба безпеки України є правоохоронним органом, головним органом у загальнодержавній системі боротьби з терористичною діяльністю, виконує завдання із захисту не тільки державного суверенітету, конституційного ладу, територіальної цілісності, а й економічного, науково-технічного та оборонного потенціалу, інтересів держави та прав громадян. Крім того, на СБ України покладені завдання із захисту інформаційного потенціалу та національної системи зв'язку. Зазначений державний орган також є спеціально уповноваженим органом у сфері контррозвідувальної діяльності, а завданням і метою такої діяльності є, в тому числі, розроблення та реалізація заходів щодо запобігання, усунення та нейтралізації загроз інтересам держави, суспільства та правам громадян. Такі законодавчі рамки вже зараз дозволяють СБУ вживати комплексні заходи у сфері забезпечення кібернетичної безпеки держави.

Немає сумнівів, що нині відбуваються формування та інституалізація Національної системи кібербезпеки, створюється її нормативно-правове забезпечення. Важливим кроком у цьому напрямку має стати ухвалення Стратегії кібернетичної безпеки, презентованої під час цьогорічних експертних консультацій Україна-НАТО з питань кіберзахисту [16]. Водночас на Україну чекає процес перегляду та ревізії власних можливостей у сфері забезпечення кібернетичної безпеки, насамперед ідеться про сектор національної безпеки та оборони. У цьому контексті може бути корисним досвід оборонного огляду, проведеного свого часу Міністерством оборони України.

Список використаних джерел

1. *Strategic* Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization // NATO HQ, 2010 [Електронний ресурс]. – Режим доступу: www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf
2. *Шариков П.* Киберком займется конфликтом Google и Китая / П. Шариков // Новое военное обозрение, 7.10.2011 [Електронний ресурс]. – Режим доступу: http://nvo.ng.ru/forces/2011–10–07/11_cybercom.html
3. *Chicago* Summit Declaration // NATO HQ, 2012 [Електронний ресурс]. – Режим доступу: http://www.nato.int/cps/en/natolive/official_texts_87593.htm?mode= pressrelease
4. *Про рішення* Ради національної безпеки і оборони України від 8 червня 2012 року «Про нову редакцію Стратегії національної безпеки України» : указ Президента України від 08.06.2012 р. № 389/2012 // Урядовий кур'єр від 26.06.2012 р. № 113.
5. *Про рішення* Ради національної безпеки і оборони України від 17 листопада 2010 року «Про виклики та загрози національній безпеці України у 2011 році» : указ Президента України від 10.12.2010 р. № 1119/2010 // Урядовий кур'єр від 15.12.2010 р. № 235.
6. *Mulligan D.* Doctrine for Cybersecurity / D. Mulligan, K. Deirdre ; Schneider, B. Fred // Daedalus. – 2011, Vol. 140 Issue 4, p. 70–92.
7. *Про внесення* змін до Закону України «Про основи національної безпеки» щодо кібернетичної безпеки України : проект закону // Офіційний сайт Верховної Ради України [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1? pf3511=45998.
8. *Про імплементацію* у 2013 році порядку денного асоціації Україна ЄС : інформація // Офіційний сайт КМДА [Електронний ресурс]. – Режим доступу: http://darn.kievcity.gov.ua/done_img/f/2171_1299959528.pdf.
9. *Про ратифікацію* Конвенції про кіберзлочинність : закон України від 07.09.2005 р. № 2824-IV // Відомості Верховної Ради. – 2006. – № 5–6. – Ст. 71.
10. *Про Державну* службу спеціального зв'язку та захисту інформації : закон України від 23.02.2006 р. № 3475-IV // Відомості Верховної Ради України. – 2006. – № 30. – С. 258.
11. *О CERT-UA* / Офіційний сайт CERT-UA [Електронний ресурс]. – Режим доступу: http://www.cert.gov.ua/?page_id=17.
12. *Рада* передбачила створення в СБУ підрозділу контррозвідки у сфері інформаційної безпеки // Журналистское расследование, 10.12.2011 [Електронний ресурс]. – Режим доступу: http://analitica.kiev.ua/info/5729-rada-peredbachila-stvorennya-v-sbu-pidrozdilu-kontrrozvidki-u-sferi-informacijnoyi-bezpeki.html
13. *Про Службу* безпеки України : закон України від 25.03.1992 р. № 2229-XII // Відомості Верховної Ради. – 1992. – № 27. – Ст. 382.
14. *Про контррозвідувальну* діяльність : закон України від 26.12.2002 р. № 374-IV // Відомості Верховної Ради. – 2003. – № 12. – Ст. 89.
15. *Про боротьбу* з тероризмом : закон України від 20.03.2003 р. № 638-IV // Відомості Верховної Ради України (ВВР). – 2003. – № 25. – Ст. 180.
16. *Експертні* консультації Україна-НАТО з питань кіберзахисту // Офіційний сайт Служби безпеки України [Електронний ресурс]. – Режим доступу: http://www.ssu.gov.ua/sbu/control/uk/publish/article ;jsessionid =A8275DD122930F3D16F12100B9EADAC.app1? art_id=120650&cat_id=80518.