УДК 351.862.4

Алексєєв М. М.

Національний університет оборони України імені Івана Черняховського, Київ

Протидія кібернетичним загрозам у Польщі: досвід для України

Резюме. У статті розглянуто кроки збройних сил Республіки Польща щодо формування захисту кіберпростору та ставлення керівництва Міністерства національної оборони Польщі до цієї проблеми. Розглянуто нормативно-правову базу, що визначає основи забезпечення захисту національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, а також повноваження державних органів у цій сфері, основні принципи координації їх діяльності щодо забезпечення кібербезпеки.

Ключові слова: кібернетичні загрози, кіберзахист, кібератака, стандарти НАТО, критична інформаційна інфраструктура.

Постановка проблеми. Вивчення досвіду реформування збройних сил Республіки Польща (РП) відповідно до стандартів НАТО є надзвичайно актуальним, зважаючи на шлях, що пройшла РП від розпаду Організації Варшавського Договору до її інтегрування в структури Північноатлантичного альянсу. Адже Україна теж намагається впроваджувати стандарти НАТО, а відповідно до Концепції розвитку сектору безпеки і оборони України виконання завдань реформування та розвитку Збройних Сил України передбачає:

формування підрозділів забезпечення кібербезпеки та кіберзахисту Збройних Сил України, здійснення міжвідомчої координації з цих питань в інтересах забезпечення обороноздатності держави;

створення необхідних матеріально-технічних запасів для адекватного реагування разом з іншими складовими сектору безпеки і оборони на усі виклики і загрози, забезпечення здатності протидіяти інформаційним, кібернетичним атакам, спецопераціям противника, а також активної участі у міжнародних заходах із підтримання миру і безпеки [1].

Проведене в рамках комплексного огляду сектору безпеки і оборони оцінювання стану воєнної безпеки держави, а також набутий досвід участі Збройних Сил України в антитерористичній операції виявили низку проблем функціонування сил оборони в умовах наявних і потенційних загроз, зокрема, неспроможність ефективно реагувати на зростаючу кількість і потужність кібератак та протистояти кіберзлочинності.

Оперативна ціль 1.5. Стратегічного оборонного бюлетеня передбачає удосконалення системи кібербезпеки та захисту інформації. Очікуваний результат: створено в Міністерстві оборони України, інших складових сектору оборони підрозділи з кіберзахисту, протидії технічним розвідкам, впровадження заходів із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC [2].

Метою статті є вивчення досвіду Республіки Польща (РП), щодо протидії кібернетичним загрозам, можливості використання цього досвіду в Україні.

Аналіз останніх досліджень і публікацій. Фахівцями з питань національної безпеки доволі широко вивчається досвід реформування ЗС Республіки Польща. Зокрема передумови та причини розроблення керівництвом РП нової редакції Стратегії національної безпеки досліджувалися О. С. Александровим [3]. Зміни викликів і загроз для Республіки Польща на межі тисячоліть, під час падіння комуністичного режиму, розпаду Організації Варшавського Договору, під час її інтегрування в структури Північноатлантичного альянсу та до сьогодні досліджуються Н. Андріяновою [4]. Досвід РП щодо реформування системи стратегічного керівництва обороною, а саме реформування системи управління збройних сил РП відповідно до стандартів НАТО, проблемні питання та шляхи їх вирішення досліджуються О. Устименком, Н. Андріяновою, В. Біликом і колишнім начальником Генерального штабу ЗС України генерал-полковником у відставці А. Лопатою [5-7].

Питання створення, розвитку та захисту кібернетичного простору воєнної сфери України досліджувалися В. Кацалапом, Ю. Саричевим, О. Устименком [8-10]. Модель

оцінювання вразливостей систем з критичною кібернетичною інфраструктурою досліджували В. Телелим, Ю. Даник та А. Зінченко [11].

Проте науковцями Центру воєнно-стратегічних досліджень під час розроблення військового стандарту "Інформаційна безпека держави у воєнній сфері. Терміни та визначення" визначено сутність понять "кібернетична загроза", кібернетична атака", "кібернетичний удар" [12].

Основна частина. Для протидії "кібернетичним загрозам" у національному і міжнародному масштабах істотним є заздалегідь набутий консенсус у питанні, які дії мають вважатися агресією, наприклад, під час можливої "кібернетичної атаки" чи "кібернетичного удару" по критичним об'єктам національної інфраструктури, визначення законних заходів протидії та спроможностей по протидії.

Під час проведення зустрічі на вищому рівні глав держав і голів урядів країн - учасниць Північноатлантичного альянсу, яка проходила у 2016 році у Варшаві, було укладено перший в історії договір між ЄС та НАТО про співпрацю у сфері безпеки, зокрема в питаннях гібридних війн та кібератак. Кіберпростір, поряд із землею, повітрям, морем і космосом, визнано новим оперативним простором, а кібероперації - невід'ємною частиною гібридної війни. Найбільше уваги операціям у кіберпросторі приділяють такі провідні країни світу, як США, Великобританія, Китай та ін. У них в бюджеті закладено величезні кошти на розвиток кібернетичної складової збройних сил та постійно втілюються в життя програми для забезпечення національної безпеки і захисту об'єктів критичної інфраструктури від кібератак.

Міністерство національної оборони Польщі завершує роботу над проектом рішення про формування військ оборони кіберпростору. Для їх створення планується виділити два мільярди злотих.

Міністр національної оборони Польщі Antoni Macierewicz взяв участь у III Європейському форумі з кібербезпеки. У своєму виступі Antoni Macierewicz підкреслив, що в сучасному світі кіберпростір - це місце війни не менш важливе ніж суша, море, повітря і космічний простір. За його словами, Польща прийняла рішення про створення військ оборони кіберпростору, про збільшення спроможностей Національного центру криптології, про створення офісу для організації кібер-армій та повноважного представника Міністерства оборони для забезпечення безпеки кіберпростору.

Antoni Macierewicz зазначив, що в технологічній сфері існує постійна гонка озброєнь, яка породжує все більш складні загрози. Немає ні інституції, ні організації, які не піддаються нападам у кібернетичній сфері. Навіть функціонування всієї держави може опинитися під загрозою, підкреслив він. Якщо ми хочемо створити потенціал у кіберпросторі, нам потрібно визначити природу загроз, зазначив він [13].

Серед прикладів нападів у кіберпросторі міністр оборони нагадав: параліч веб-сайтів парламенту, міністерств та банківських установ в Естонії у 2007 році, хакерські атаки до та під час саміту НАТО у Варшаві, вірус "Пієта", який завдав шкоди Україні та діяльність російських хакерів під час нещодавнього референдуму в Каталонії.

Усі ці випадки не є окремими діями комп'ютерних хакерів. Це ті заходи, які потребують складного процесу організації, активної підтримки країн, які стоять за цими атаками, сказав Antoni Macierewicz. Він додав, що урядам все більше треба вживати заходи, пов'язані з їх безпекою у цій сфері. Як приклад він навів уряд США, який вирішив вилучити зі своїх комп'ютерних систем встановлене програмне забезпечення Лабораторії Касперського [14].

Міністр нагадав, що 5 грудня 2016 року Президент Росії Володимир Путін підписав нову доктрину безпеки, яка створює інформаційні армії, і що ми нещодавно спостерігали за тим, як через дезінформацію росіяни намагалися впливати на виборчі процеси в США, Франції, Німеччині та Каталонії.

"Будь-яка держава, щоб зберегти своє функціонування під час кризи або IT-атаки, має побудувати суверенний контроль над телекомунікаційними мережами", – сказав Macierewicz. Як він підкреслив, ця частина критично важливої інфраструктури є "не тільки мішенню потенційних нападів", але залишається "нервовим ядром, що дасть змогу вижити і відновити контроль над кіберпростором".

Після масштабних кібератак, які були здійснені минулого року на багато українських компаній і державні інституції, Україна серйозно замислилась над регулюванням сфери кіберзахисту. Так, у жовтні 2017 року Верховна Рада ухвалила відповідний закон "Про основні засади забезпечення кібербезпеки України" [15].

Документ визначає основи забезпечення захисту національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, а також повноваження державних органів у цій сфері, основні принципи координації їх діяльності щодо забезпечення кібербезпеки.

Саме прийняття цього нормативно-правового акту означає для України закріплення на законодавчому рівні понятійного апарату з приставкою "кібер" і початок регулювання цифрової економіки в цілому.

Закон розширив і доповнив положення Стратегії кібербезпеки України, затвердженої Указом Президента у 2016 році [16]. Метою стратегії було створення умов для безпечного функціонування кіберпростору, його використання в інтересах особистості, суспільства і держави. До того ж основний масив положень стратегії стосується сфери національної оборони. Стратегія стала підтвердженням прийнятого Україною курсу на євроінтеграцію, початком якого було підписання і ратифікація Україною Конвенції про кібербезпеку. Держави – члени Ради Європи та деякі інші держави, які підписали конвенцію, взяли на себе зобов'язання вжити загальні та індивідуальні, для кожної країни, заходи щодо запобігання злочинів у цифровій сфері.

Основним досягненням закону "Про основні засади забезпечення кібербезпеки України" є імплементація в правове поле визначень, що стосуються кібербезпеки, кібератак і кіберзахисту. Закон про кібербезпеку – це перші важливі кроки держави у сфері регулювання кіберпростору. Крім того, у законі є і положення, які концептуально зачіпають не тільки питання національної безпеки, але стосуються і бізнесу. Вводиться поняття "об'єкт критичної інформаційної інфраструктури", які будуть зобов'язані проходити обов'язковий аудит з кібербезпеки.

Саме тому прийняття закону – важливий етап для України, адже це запускає комплексний процес регулювання кібербезпеки як окремої важливої галузі [17].

Наступним етапом має стати перелік об'єктів критичної інфраструктури від Кабміну (об'єкти, що мають життєво важливе значення для функціонування держави).

Аналогічний підхід був закріплений і в ЄС. Для систематизації та встановлення мінімальних вимог для всіх країн-членів ЄС була прийнята директива про загальні заходи безпеки мережевих та інформаційних систем у ЄС 2016/1148 [18]. Директива зобов'язує держав-членів визначити об'єкти критичної інфраструктури в різних сферах.

Влітку минулого року, а саме 27 червня, відбулась кібератака на державні установи, об'єкти, фінансового, енергетичного, транспортного секторів, а також приватні підприємства за допомогою шкідливого програмного продукту Petya. Ця кібератака завдала значних збитків державному сектору і бізнесу, фактично заморозивши бізнес-процеси в країні на декілька днів. З упевненістю можна констатувати, що від вірусу постраждало понад половини українських компаній, і йдеться не лише про невеликі збої в роботі мереж, а про втрату великих обсягів даних і фінансової звітності за кілька звітних періодів. Терміни відновлення компаній варіювали від декількох днів до місяця, а в окремих випадках і довше. Утім, як заявляють у Генштабі ЗС України, системи ЗС України не були заражені вірусом Petya [19]. Це може свідчити як про відмінну роботу підрозділів кіберзахисту, так і про недостатньо активне використання кіберпростору ЗС України.

Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану [15].

Нині Україна активно співпрацює з міжнародними партнерами у галузі розвитку систем захисту інформації та кібернетичної безпеки в інформаційно-телекомунікаційних системах Міноборони та ЗС України. До штаб-квартири НАТО подано 5 проектів щодо розвитку кібербезпеки ЗС України для їхнього впровадження у рамках Трастового фонду Україна-НАТО з кібербезпеки, головним розпорядником якого є СБ України. У рамках угоди USAI ITI Україна отримала допомогу з підвищення рівня кібербезпеки. Спільно з естонськими колегами розроблено проект зі створення кіберлабораторії на базі однієї з військових частин ЗС України. Безпосередньо зараз проводяться роботи з монтажу

обладнання та інсталяція програмного забезпечення у Центрі оперативного реагування на кіберінциденти [20].

Висновок. Оскільки ніхто не може з упевненістю стверджувати, що його мережі повністю захищені та можуть протистояти багатовекторним кібератакам, кібернетична безпека стала пріоритетом розвитку сучасної армії. Російська Федерація постійно збільшує кількість операцій з кібершпіонажу та все більше намагається вплинути на громадську думку в нашій країні, не гребуючи використанням фейкових новин та відвертої пропаганди. Основною метою цих операцій є розхитування ситуації всередині країни, створення хаосу та паніки як підґрунтя для просування власних інтересів.

Використовуючи кіберпростір, хакери можуть зламувати захищені мережі та отримувати необхідну інформацію, тому необхідно спрямувати зусилля на захист своїх мереж і забезпечити їх безпеку, використовуючи різні рівні захисту інформації. Важливим кроком є впровадження сегментації мережі – логічного поділу мережі на різні сегменти залежно від ступеня важливості, користувачів, серверів тощо. У такому випадку у разі зараження шкідливим ПО будь-якої робочої станції загрозу можна локалізувати в межах одного сегмента й тим самим врятувати від зараження всю інфраструктуру сил оборони. Доступ до інформації та технології надається тільки для персоналу, який отримав допуск та має відповідні фахові навички.

Резервування даних забезпечить ефективне відновлення інформації. Виявлення шкідливого ПО дасть змогу забезпечити раннє виявлення злочинів і зловживань, навіть якщо механізми захисту були обійдені.

Висновок, який маємо зробити для себе, – це збільшення інвестування в кібербезпеку, щоб сили оборони мали спроможності протидіяти кібератакам і забезпечувати необхідний рівень кіберзахисту критичної інформаційної інфраструктури.

Напрями подальших досліджень. Надалі доцільно провести аналіз заходів із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану, як це передбачено законом “Про основні засади забезпечення кібербезпеки України” [15], які були здійсненні в період із 14 години 00 хвилин 26 листопада 2018 року до 14 години 00 хвилин 26 грудня 2018 року – тобто в час введення воєнного стану в Україні.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Указ Президента України від 14 березня 2016 року № 92 Про рішення РНБО України від 4 березня 2016 року “Про Концепцію розвитку сектору безпеки і оборони України” – Режим доступу : http://www.president.gov.ua/documents/922016-19832
2. Стратегічний оборонний бюлетень України: Указ Президента України від 06.06.2016 № 240 Про рішення РНБО України від 20 травня 2016 року “Про Стратегічний оборонний бюлетень України” // Офіційне інтернет-представництво Президента України. URL: http://www.president.gov.ua/ documents/2402016-20137 (дата звернення 03.09.2018).
3. Александров О. С. Нова Стратегія національної безпеки Польщі – відповідь на європейські виклики та загрози сьогодення / О. С. Александров // Стратегічні пріоритети – 2015. – № 1 (34). – С. 131–138.
4. Андріянова Н. Аналіз змін у безпековому просторі Республіки Польща в період до і після вступу в НАТО. Гілея: науковий вісник. Збірник наукових праць / Гол. ред. В. М. Вашкевич. – К. : «Видавництво «Гілея», 2017. – Вип. 122 (7). – С. 438–443.
5. Устименко О. В, Андріянова Н.М., Білик В. І. Реформування системи стратегічного керівництва силами оборони відповідно до стандартів НАТО (на основі досвіду Республіки Польща); Київ: Науковий часопис Академії національної безпеки, 2017. – № 1-2. – С. 81–97.
6. Устименко О. В Реформування системи стратегічного керівництва обороною Республіки Польща: досвід для України; НАДУ. Київ: Вісник НАДУ, 2017. – № 3. – С. 60–65.
7. Лопата А. В. Стратегічний оборонний бюлетень – прихована безпорадність Радбезу – Режим доступу : http://glavcom.ua/columns/lopata/strategichniy-oboronniy-byuleten-prihovana-bezporadnist-radbezu-358358.html
8. Кацалап В. О., Устименко О. В Створення, розвиток та захист кібернетичного простору воєнної сфери України / Гілея: науковий вісник. Збірник наукових праць / Гол. ред. В. М. Вашкевич. – К.: ВІР УАН, 2013. – Випуск 75 (№ 8). – С. 519–521.
9. Устименко А. В., Кацалап В. О., Сарычев Ю. А. Киберпространство военной сферы / «Информационная безопасность в свете Стратегии Казахстан-2050»: Сборник трудов I Международной научно-практической конференции (12 сентября 2013 г., Астана). – Астана, 2013. – С. 539–545.
10. Сніцаренко П. М, Саричев Ю. О., Рогов П. Д. Методика оцінки інформаційного впливу на елементи інформаційної інфраструктури держави / Збірник матеріалів VII науково-технічної

конференції НТТУ ДУТ “Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”, м. Київ, 23–24 жовтня 2014 р. – К.: ВІТІ ДУТ, 2014. – С. 88-96.
11. Телелим В. М, Даник Ю. Г., Зінченко А. О. Модель оцінювання вразливостей систем з критичною кібернетичною інфраструктурою / Зб. наук. пр. Центру воєнно-стратегічних досліджень Національного університету оборони України ім. Івана Черняховського. – 2018. – № 2 (63). – С. 63–67.
12. Інформаційна безпека держави у воєнній сфері. Терміни та визначення : ВСТ 01.004.004 – 2014 (01). – [Чинний від 2014-02-27] – (Військовий стандарт)
13. Powstają wojska do walki w cyberprzestrzeni. Kosztują 2 mld zł Сайт Polsatnews. Дата оновлення 09.10.2017. URL: http://www.polsatnews.pl/ wiadomosc/ 2017-10-09/powstaja-wojska-cybernetyczne-do-walki-w-cyberprzestrzeni-beda-kosztowac-2-mld-zl/ (дата звернення: 12.11.2018).
14. Oprogramowanie firmy Kaspersky Lab ma być usunięte z systemów rządowych USA. Дата оновлення 13.09.2017. URL: http://www.polsatnews.pl/wiadomosc/2017-09-13/oprogramowanie-firmy-kaspersky-lab-ma-byc-usuniete-z-systemow-rzadowych-usa/?ref=wyszukiwarka (дата звернення: 12.11.2018).
15. Закон України від 5 жовтня 2017 року № 2163-VIII “Про основні засади забезпечення кібербезпеки України” // Законодавство України. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 03.12.2018).
16. Стратегія кібербезпеки України: Указ Президента України від 15.03.2016 № 96 Про рішення РНБО України від 27 січня 2016 року “Про Стратегію кібербезпеки України” // Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua/documents/ 962016-19836 (дата звернення 03.12.2018).
17. Безпека в мережі: як Україна регулюватиме кіберпростір // Сайт Mind. URL: https://mind.ua/openmind/20184620-bezpeka-v-merezhi-yak-ukrayina-regulyuvatime-kiberprostir (дата звернення 12.12.2018).
18. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу // Законодавство України. URL: http://zakon.rada.gov.ua/laws/show/984_013-16/sp:max10 (дата звернення 12.12.2018).
19. У Генштабі заявляють, що системи ЗСУ не були заражені вірусом Petya / Сайт УНІАН. URL: https://www.unian.ua/politics/2071049-u-genshtabi-zayavlyut-scho-sistemi-zsu-ne-buli-zarajeni-virusom-petya.html (дата звернення 12.12.2018).
20. Створять кіберлабораторію на базі однієї з військових частин ЗСУ. Дата оновлення 05.11.2018. Сайт Gazeta.ua. URL: https://gazeta.ua/articles/science/ _stvoryat-kiberlaboratoriyu-na-bazi-odniyeyi-z-vijskovih-chastin-zsu/867780 (дата звернення: 05.11.2018).

Стаття надійшла до редакційної колегії 17.12.2018

Алексеев М. Н.
Национальный университет обороны Украины имени Ивана Черняховского, Киев

Противодействие кибернетическим угрозам в Польше: опыт для Украины

Резюме. В статье рассмотрены шаги вооруженных сил Республики Польша по формированию защиты киберпространства и отношение руководства Министерства национальной обороны Польши к этой проблеме. Рассмотрена нормативно-правовая база, которая определяет основы обеспечения защиты национальных интересов Украины в киберпространстве, основные цели, направления и принципы государственной политики в сфере кибербезопасности, а также полномочия государственных органов в этой сфере, основные принципы координации их деятельности по обеспечению кибербезопасности.

Ключевые слова: кибернетические угрозы, киберзащита, кибератака, стандарты НАТО, критическая информационная инфраструктура.

M. Alekseev
The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv

Countering cyber threats in Poland: experience for Ukraine

Resume. The article discusses the steps of the Armed Forces of the Republic of Poland in shaping the protection of cyberspace and the attitude of the leadership of the Ministry of National Defense of Poland to this problem. The regulatory framework that defines the basis for ensuring the protection of national interests of Ukraine in cyberspace, the main objectives, directions and principles of state policy in the field of cybersecurity, as well as the powers of state bodies in this area, the basic principles of coordinating their cybersecurity activities are considered.

Keywords: cyber threats, cyber defense, cyber attack, NATO standards, critical information infrastructure.