НАЦІОНАЛЬНА БЕЗПЕКА

УДК 338.2(477):004.056.5

ЗАХИСТ КІБЕРПРОСТОРУ ЯК СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Головка А.А.
Національний інститут стратегічних досліджень
при Президентові України

Досліджено сучасний стан кібербезпеки України в умовах гібридної війни. Зокрема, проаналізовані основні проблеми української системи протидії кіберзагрозам на конкретних прикладах. Хронологічні рамки даного аналізу охоплюють 2013-2015 роки. В підсумку систематизовані основні шляхи покращення якості функціонування системи кібербезпеки України. Насамперед мова йде про посилення взаємодії між громадянським суспільством та державою, вдосконалення законодавчої бази, міжнародне співробітництво у сфері кібербезпеки.
Ключові слова: кібербезпека, інформаційна безпека, гібридна війна, інформація, кіберпростір, інформаційні загрози.

Постановка проблеми. Сучасне людство перебуває в умовах нестримного розвитку інформаційних технологій, які визначальним чином впливають на всі сфери життя соціуму. Цей процес є дуже неоднозначним: з одного боку, він забезпечує вдосконалення технологічного інструментарію, значно спрощує та пришвидшує роботу людини в різних сферах, надає вільний доступ до джерел інформації. Разом з тим, це робить суспільство, державу та індивіда вразливими перед зовнішніми загрозами, зокрема перед кіберзагрозами, які можуть нанести значну матеріальну шкоду, паралізувати діяльність органів державної влади, промислових об'єктів, соціальних установ. Дана проблема має особливе значення в українських реаліях, враховуючи факт воєнно-інформаційної агресії з боку Росії. Підрив основ інформаційної безпеки у цілому та кібербезпеки зокрема без сумніву є складовою частиною експансіоністських планів Кремля. Саме тому це питання є актуальним і потребує вивчення.

Аналіз останніх досліджень і публікацій. Дослідження питань кібербезпеки як складової інформаційного захисту держави в сучасних умовах знаходиться в фокусі уваги багатьох зарубіжних науковців: С. Морган, А. Клімбург, М. Шмідт, М. Гедекер, М. Лібіцкі, Дж. Най, І. Зубарєв, М. Безкоровайний. Неабиякий інтерес до даної проблематики проявляють і українські вчені, зокрема Д. Дубов, М. Ожеван, В. Фурашев, В. Л. Бурячок, В. Бутузов, В. Б. Толубко, О. Довгань, В. О. Хорошко, С. В. Толюпа та ін.

Виділення невирішених раніше частин загальної проблеми. Не дивлячись на велику кількість досліджень в даній сфері, питання забезпечення кібербезпеки як невід'ємного елементу системи інформаційної безпеки в умовах гібридної війни, зокрема на прикладі України, все ще залишається відкритим.

Метою даної статті є аналіз сучасного стану кібербезпеки України в контексті забезпечення інформаційної безпеки держави.

У відповідності з метою дослідження випливають наступні завдання:

1. визначення рівня ефективності кібербезпеки України та висвітлення ключових проблем у даній сфері;
2. систематизація основних шляхів вдосконалення системи кібербезпеки України.

Виклад основного матеріалу. Сьогодні, в науковій літературі можна знайти велику кількість різних визначень поняття «Кіберпростору». Причому строкатість розуміння даного поняття властива і нормативно-правовій сфері: практично кожна країна в своєму законодавстві дає власне визначення. Тому для узагальнення слід використовувати міжнародний стандарт, відповідно до якого, кіберпростір – це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі [2, с. 8].

Так само важко дати єдину вичерпну дефініцію визначення «Кібербезпека». Разом з тим, більшість дефініцій зводяться до розуміння кібербезпеки як стану захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від зовнішніх впливів та ризиків, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й ней-

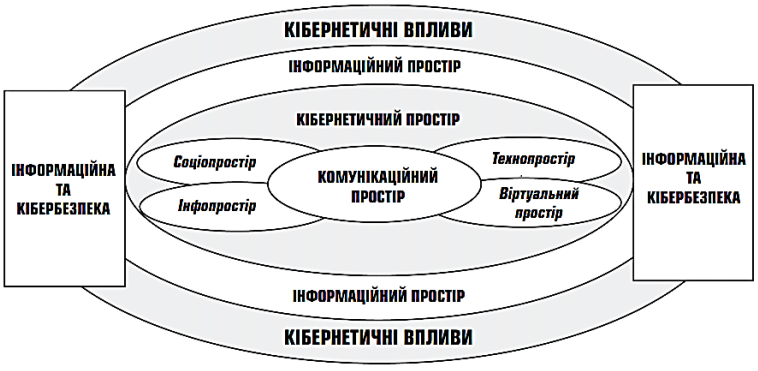

Рис. 1. Взаємозв'язок інформаційного та кіберпросторів [2, с. 8]

тралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам [2, с. 15].

Сьогодні ми можемо говорити про наявність фактично неприхованих спроб впливу протиборчих сторін на інформаційний і кіберпростори один одного за рахунок використання засобів сучасної обчислювальної і/або спеціальної техніки й відповідного програмного забезпечення – кібервтручань, а також інших проявів їхнього дестабілізуючого впливу на той чи інший об'єкт, здійснюваного за рахунок технологічних можливостей інформаційного і кіберпростору, зі створенням небезпеки – так званих кіберзагроз, як для цього простору, так і для свідомості кожної людини [2, с. 24].

На думку відомого українського вченого Дмитра Дубова, очільника відділу інформаційної безпеки та розвитку інформаційного суспільства НІСД при Президентові України, усі кіберзагрози, які на сьогоднішній день, в тій чи іншій мірі, використовуються для здійснення негативного впливу на кіберпростір України, можна поділити на дві умовні групи. До першої належать так звані «класичні» кіберзлочини – як абсолютно оригінальні, так і вже звичні для нас, для своєї реалізації вони потребують лише сучасних інформаційних технологій. Друга група об'єднує злочини, характерні для геополітичної боротьби (або такі злочини на місцевому рівні, які мають потенціал вплинути на політичне становище держави): хактивізм (використання комп'ютерних систем, соціальних мереж для просування певних політичних ідей, лозунгів, гасел тощо) кібершпигунство та кібердиверсії. Водночас техніки здійснення атак в обох випадках демонструють чимало спільного. Наприклад, фішингові техніки можуть бути використані як для заволодінням коштами громадян, так і з кібершпигунською метою. Хоча, звичайно, ціла низка кіберзлочинів має на меті й може скоюватися виключно для збагачення злочинців [4, с. 210].

Якщо говорити про кіберзагрози, які входять до другої групи, то у цілому можна констатувати, що наша держава вже активно залучається у протистояння хактивістів, в окремих випадках стає об'єктом кібершпигунських акцій, однак досі не було зареєстрованих випадків кібердиверсій (принаймні офіційно) [4, с. 212].

В історії України наявні часті приклади застосування тих чи інших інструментів для кібератак. Особливо часто застосовувались методи хактивізму. До прикладу можна згадати скандал навколо довкола закриття файлообмінного сервісу «@ex.ua.», коли населення здійснювало масовані DDoS-атаки на ресурси органів державної влади. Подібним чином розгортались події після рішення уряду Азарова про призупинення процесу підготування до підписання Угоди про асоціацію між Україною та Євросоюзом в листопаді 2013 року. І в першому і в другому випадку органи державної влади, безпекові та силові структури були безсильними перед кібератаками і не могли ефективно впоратись із інформаційними викликами [4, с. 212-213].

Сьогодні в умовах воєнно-інформаційного протистояння із Росією кібератаки стають набагато більш небезпечними і переслідують в першу чергу політичні цілі. Останні найбільш «гучні» кібератаки проросійських сил відбулися протягом 2014-2015 років. Перші серйозні напади були здійснені під час проведення виборів президента України. 27.05.2014. служба безпеки України (СБУ) встановила, що більшість хакерських атак, які здійснювалися проти сервера ЦВК у день виборів президента, організовували з території Росії. За інформацією прес-служби СБУ, атаки на сервер ЦВК здійснювались безперервно зі змінною динамікою потужності, а переважна кількість атак проводилася з території Російської Федерації з використанням бот-мереж.

Також СБУшники затримали групу хакерів у Києві. Вони збиралися вивести з ладу низку інформаційних ресурсів ЦВК та поставити під сумнів результати голосування. Два уражених вірусами сервери були заблоковані у Вінниці. Там зловмисники згенерували потужну DDOS-атаку на інформаційні ресурси ЦВК. Також було виявлене та завчасно знешкоджено шкідливе програмне забезпечення, яке було впроваджено до електронної системи обробки даних. За його допомогою російська сторона намагалася дискредитувати результати українських виборів, зокрема, лідером президентських перегонів з результатом у 37% збиралися оголосити Дмитра Яроша. Відповідну провокацію розповсюдив російський телеканал ОРТ [7].

28 липня 2015 року Міністерство закордонних справ України повідомило, що акаунт в Twitter Постійного представника України при ООН Юрія Сергеєва зламано. Хакерська атака носила провокаційний характер, оскільки відбулась напередодні розгляду в Раді Безпеки ООН резолюції стосовно катастрофи рейсу МН17 [1].

19 серпня 2015 року офіційний сайт Львівської обласної державної адміністрації зламали хакери і наповнили ресурс фотографіями президента Росії Володимира Путіна та його поплічників. (львів'яни та відвідувачі сайту встигли зробити скріншот сайту Львівської ОДА і викласти його в мережу інтернет) [6].

Через два дні, 21 серпня того ж року, хакери зламали сайт Івано-Франківської облдержадміністрації. На головній сторінці сайту з'явилися фотографії Путіна та Лаврова, а також численні провокативні світлини. Крім того були створені рубрики антиукраїнського характеру: «Рагулюція», «МВФ піможі нам», «Рагулізм Прикарпаття» і т. д. Через це роботу сайту довелося призупинити. Сьогодні не відкидається версія причетності російських спец-служб до даного нападу. Разом з тим жодна організація, терористична група чи політична партія не взяла на себе відповідальність за цей вчинок [5].

Всі вищеназвані приклади свідчать про недостатню ефективність сучасної системи кібербезпеки України і про нагальну потребу її удосконалення та модернізації. Від реалізації цих процесів залежить не тільки безпека в інформаційній сфері, але й сталий розвиток української держави в сучасному глобалізованому світі.

Саме тому з метою підвищення якості захисту кіберпростору України доцільно виділити чіткі способи досягнення даної цілі. Якщо говорити про конкретні рекомендації щодо підвищення якості функціонування вітчизняної системи кі-

бербезпеки, то слід акцентувати увагу на наступних елементах:

1. Варто розширити процес залучення інститутів громадянського суспільства до забезпечення ефективного захисту кіберпростору України та протидії кіберзагрозам. Зважаючи на досвід західних демократій (США, Великобританія, Німеччина) особливий акцент державні структури мають зробити на взаємодію із неурядовими аналітичними центрами (далі НАЦ). В умовах наявності зовнішніх загроз, що зачіпають національні інтереси країни в інформаційній сфері і цим наносять відчутний удар по національній безпеці у цілому, уряд потребує своєчасного надходження достовірної та об'єктивної інформації, її аналітики та фахової експертної оцінки того чи іншого явища.

Враховуючи те, що ресурсів та кадрового потенціалу держави недостатньо для виконання таких завдань, вищому керівництву країни слід звертатися за допомогою до різного роду аналітичних центрів, які в свою чергу мають змогу надавати свою інформаційну допомогу. Британські (Королівський інститут міжнародних справ, Міжнародний Інститут Стратегічних Досліджень), американські (Центр стратегічних і міжнародних досліджень / «Chatham House»), європейські (Королівський інститут міжнародних і стратегічних досліджень / «Elcano», «Брейгель») НАЦ грають вагому роль у забезпеченні кібербезпеки і виступають у якості надійних союзників держави надаючи їй необхідну експертну, аналітичну та інформаційну підтримку. Спираючись на зарубіжний досвід і враховуючи українські реалії слід посилити взаємодію на лінії «Держава-НАЦ» у кібербезпеки шляхом створення при безпекових та силових структурах відповідних комітетів (мова йде в першу чергу про МВС, Міноборони, СБУ);

2. Необхідним кроком також є вдосконалення законодавчої бази України. Насамперед мова йде про розширення понятійно-категорійного апарату, оскільки у сучасному вітчизняному законодавстві часто можна спостерігати оперування великою кількістю термінів, що так чи і інакше стосуються питань кібербезпеки, але при цьому не мають конкретного визначення в нормативних документах. Наприклад, Закон України «Про основи національної безпеки України» містить статті де прописані так категорії, як «компютерна злочинність» та «компютерний тероризм», але тим не менш закон не містить їх визначення. Більше того жоден інший нормативно правовий акт не містить дефініцію даних категорій. Інший нормативно-правовий акт, а саме Закон «Боротьбу з тероризмом» не використовує терміни «компютерний тероризм» чи «кібертероризм», замість нього наявний термін «технологічний тероризм» [3].

У «Доктрині інформаційної безпеки України» теж згадуються такі поняття як «комп'ютерна злочинність», «кібератака», «комп'ютерний тероризм», але без жодних пояснень чи посилань (відсилань) до таких пояснень. Це ж саме стосується Законів «Про інформацію», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», стратегічного документу «Стратегії національної безпеки України». Тобто можна зробити висновок, що нормативно-правова база потребує перегляду та вдосконалення [4, с. 257].

3. Міжнародне співробітництво у сфері кібербезпеки так само допоможе підвищити обороноздатність України в даній сфері. Крім того, враховуючи сучасний рівень розвитку інформаційної зброї, наявності небезпечних терористичних та бандитських угрупувань, широкий спектр кіберзагроз, безумовно можна говорити про те, що жодна країна світу не здатна самостійно протистояти подібним викликам. Для посилення кібербезпеки як на міжнародному рівні так і на рівні національних держав необхідною є співпраця між різними країнами. Тому подальша співпраця в секторі безпеки, а також її розширення є перспективним кроком і для України і для її міжнародних партнерів. В першу чергу мова йде про співробітництво з НАТО, ЄС, ОБСЄ. Яскравим прикладом тут є програма співробітництва Україна-НАТО.

Висновки і пропозиції. Отже, сьогодні стан кібербезпеки України далекий від оптимального. Про це свідчить насамперед нездатність держави адекватно відповідати на зовнішні інформаційні ризики, що підтверджується на практиці (зокрема численними успішними кібератаками з боку проросійських угрупувань). Від правильного та своєчасного вирішення актуальних проблем в секторі кібербезпеки залежить ефективність функціонування усієї системи національної безпеки.

Якщо говорити про конкретні шляхи вирішення наявних проблем то слід акцентувати увагу на трьох основних факторах. По-перше, важливим є залучення інститутів громадянського суспільства до процесу конструювання системи кібербезпеки. Особливу роль тут грають неурядові аналітичні центри, які зможуть надавати безпековим структурам необхідну експертну, аналітичну та інформаційну допомогу. По-друге, необхідними є зміни в нормативній базі, а саме розширення понятійно-категорійного апарату, формування чіткого правового розуміння сутності та складових елементів кібербезпеки. По-третє, суттєво підвищує обороноздатність України в інформаційній сфері міжнародне співробітництво, зокрема з країнами ЄС, блоком НАТО, ОБСЄ.

Зважаючи на сучасні суспільно-політичні та інформаційні виклики (насамперед стан неоголошеної гібридної війни Росії проти України) варто відмітити актуальність наукових досліджень такого роду. Насамперед перспективними з точки зору наукового інтересу та соціальної значимості є дослідження варіантів співпраці між бізнесом та державою в сфері інформаційної безпеки, шляхів залучення інститутів громадянського суспільства (зокрема громадських організацій, спілок, неурядових аналітичних центрів і т. д.) до процесу забезпечення кібербезпеки, використання інноваційних методів та технологій для конструювання ефективної системи кіберзахисту та інші.

Список літератури:

1. Аккаунты посла Украины при ООН Сергеева в Twitter и Facebook взломали [Електронний ресурс]. – сайт новин «Гордон». – Режим доступу: http://gordonua.com/news/politics/akkaunty-posla-ukrainy-pri-oon-sergeeva-v-twitter-i-facebook-vzlomali-91677.html
2. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.
3. Войтенко Ю. А. Кібербезпека проблема століття [Електронний ресурс] / Юлія Артурівна Войтенко // офіційний сайт «Єдиної служби правової допомоги 3222». – Режим доступу: http://3222.ua/article/kberbezpeka-problema_stolttya.htm
4. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія / Дмитро Володимирович Дубов. – К.: НІСД, 2014. – 328 с.
5. Хакери зламали сайт Івано-Франківської ОДА [Електронний ресурс]. – сайт інформаційного агентства «УНІАН». – Режим доступу: http://www.unian.ua/society/1114396-hakeri-zlamali-sayt-ivano-frankivskoji-oda.html
6. Хакери зламали сайт Львівської облдержадміністрації й розмістили на ньому фотографії Путіна та Лаврова [Електронний ресурс]. – сайт новин «Щоденний Львів». – Режим доступу: http://dailylviv.com/news/kryminal/khakery-zlamaly-sait-lvivskoyi-oda-i-rozmistyly-na-nomu-foto-putina-ta-lavrova-22073
7. Хакерські атаки на сервер ЦВК здійснювали з території Росії [Електронний ресурс]. – Офіційний сайт «ТСН». – Режим доступу: http://tsn.ua/politika/hakerski-ataki-na-sayt-cvk-zdiysnyuvali-z-teritoriyi-rosiyi-351769.html

Головка А.А.
Национальный институт стратегических исследований
при Президенте Украины

ЗАЩИТА КИБЕРПРОСТРАНСТВА КАК СОСТАВЛЯЮЩАЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УКРАИНЫ В УСЛОВИЯХ ГИБРИДНОЙ ВОЙНЫ

Аннотация
Исследовано современное состояние кибербезопасности Украины в условиях гибридной войны. В частности, проанализированы основные проблемы украинской системы противодействия киберугрозам на конкретных примерах. Хронологические рамки данного анализа охватывают 2013-2015 года. В итоге систематизированы основные пути улучшения качества функционирования системы кибербезопасности Украины. Прежде всего речь идет о усилении взаимодействия между гражданским обществом и государством, усовершенствования законодательной базы, международное сотрудничество в области кибербезопасности.
Ключевые слова: кибербезопасность, информационная безопасность, гибридная война, информация, киберпространство, информационные угрозы.

Holovka A.A.
National Institute for Strategic Studies under the President of Ukraine

PROTECTING CYBERSPACE AS A COMPONENT OF INFORMATION SECURITY OF UKRAINE IN CONDITIONS OF HYBRID WARFARE

Summary
Investigated the current state of cybersecurity Ukraine in conditions of hybrid warfare. In particular, analyzed the main problems of the Ukrainian system of combating cyberthreads specific examples. The chronological scope of this analysis covers 2013-2015. As a result, major systematic ways to improve the quality of the system cybersecurity Ukraine. First of all, it is about strengthening cooperation between civil society and government, improving the legal framework, international cooperation in cybersecurity.
Keywords: cyber security, information security, hybrid warfare, information, cyberspace, information threats.