DOI 10.52363/2414-5866-2021-1-12
УДК 351.517

Курило А.Г., *ад`юнкт ННВЦ НУЦЗУ, м. Харків, ORCID: 0000-0002-5139-0278*

Kurilo A., *adjunct candidate of Educational, Scientific and Production Center of the National University of Civil Defense of Ukraine, Kharkiv*

МІСЦЕ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

THE PLACE OF INFORMATION SECURITY IN THE NATIONAL SECURITY SYSTEM

Стаття присвячена дослідженню місця інформаційної безпеки в системі національної безпеки держави. Однією з головних проблем залишається відсутність чіткої сформульованої політики необхідної для виявлення та попередження інформаційних загроз національній безпеці. Реалізація державної інформаційної політики повинно забезпечуватися проведенням єдиних організаційно-технічних заходів на території України органами влади всіх рівнів влади, організаціями та підприємствами щодо забезпечення інформаційної безпеки від внутрішніх і зовнішніх загроз.

Ключові слова: *інформація, інформаційна безпека, державна інформаційна політика, загрози інформаційній безпеці, національна безпека, стратегія національної безпеки.*

This article is devoted to the analysis of the place of information (cyber) security in the system of national security of the state One of the main problems remains the lack of a clear formulated policy necessary to identify and prevent information threats to national security. The implementation of the state communications policy must be provided with conducting of joint organizational and technical measures on the territory of Ukraine by the authorities of all government levels, the organizations and enterprises responsible for internal and external cyber security.

Keywords: *information, cyber security, state communications policy, menace of information (cyber) security, national security, strategy of national security.*

Постановка проблеми. Світова спільнота визнала міжнародну інформаційну безпеку як глобальну проблему, як необхідну складову для існування суспільства. Виходячи з того, що інформаційна безпека в третьому тисячолітті займає перше місце в системі національної безпеки, формування й проведення єдиної державної політики в цій сфері вимагає пріоритетного напрямку. Сучасний розвиток соціально - економічних, політичних та інших процесів в державі супроводжується вдосконаленням інформаційно-правового забезпечення органів державної влади, спрямованого на забезпечення національної безпеки держави. Це відбувається на тлі непростої соціально-економічної обстановки все-

редині країни, продовженні озброєних конфліктів, серйозних терористичних загрозах і зростання злочинності.

Однією з основних загроз для України в інформаційній сфері як і раніше є відсутність чітко сформульованої політики, що відповідає національним цілям і інтересам. У зв'язку з цим потрібно формування загальних принципів і загального розуміння всього комплексу проблем, пов'язаних з інформаційною безпекою, починаючи з концептуального апарату, наукових і методичних концепцій і закінчуючи практичним вирішенням поставлених завдань.

Аналіз останніх досліджень і публікацій. Проблеми державного управління наукової й науково-технічної діяльності та механізмів формування державної політики в галузі наукової діяльності розглянуто в працях науковців і практиків, а саме: [9; 10; 11; 12].

Виклад основного матеріалу. Розвиток нових інформаційних технологій обумовлює збільшення технологічного розриву між постійно зростаючими вимогами до показників захищеності інформаційних ресурсів в суб'єктах держави. Сучасні процеси публічного управління є уразливими без належного рівня забезпечення інформаційної безпеки. Безперервний процес розвитку інформаційних технологій породжує нові виклики і загрози, які виходять з інформаційного простору, які можуть завдати значної шкоди процесам публічного управління. Основним показником отримання достовірної і повної інформації, яка необхідна для формування державної політики, є забезпечення її безпеки, тому в даний час механізми і способи забезпечення інформаційної безпеки стають особливо актуальними в процесі публічного управління. Таким чином, забезпечення інформаційної безпеки розглядається як одне з державних пріоритетних завдань, як важливий елемент забезпечення національної безпеки держави.

У руслі даних тенденцій за останнє десятиріччя було прийнято значну кількість нормативно-правових актів, спрямованих на регулювання відносин у сфері інформаційної безпеки. Насамперед, у Конституції України закріплені норми, згідно яких інформаційна безпека визначається, як найважливіша функція держави [1]. Документом, який являє собою сукупність офіційних поглядів в області забезпечення національної безпеки в інформаційному просторі, інформаційної безпеки України в світі, включає в себе основні інформаційні загрози, стратегічні цілі та напрямки, організаційні основи захисту інформації є Доктрина інформаційної безпеки України [2].

Доктрина, в першу чергу, містить основні положення, що визначають державну політику щодо забезпечення інформаційної безпеки України, головним завданням якої є захист інформаційних ресурсів, формування та оновлення системи забезпечення інформаційної безпеки.

Положення Доктрини націлені на досягнення ефективного функціонування системи публічного управління, а також спрямовані на організацію міжгалузевого та міжвідомчого взаємодії в частині, що стосується системи забезпечення інформаційної безпеки.

З огляду на те, що інформаційна безпека впливає на стан і розвиток всіх

складових національної безпеки, будучи її безпосередньою частиною, Доктрина закріпила основні національні інтереси в даній сфері.

У першу чергу, це життєво важливі інтереси особи, а саме: 1) забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; 2) забезпечення конституційних прав людини на захист приватного життя; 3) захищеність від руйнівних інформаційно-психологічних впливів;

По-друге, життєво важливі інтереси суспільства і держави:

- захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації;
- захист українського суспільства від агресивного інформаційного впливу РФ, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;
- всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації;
- забезпечення вільного обігу інформації, крім випадків, передбачених законом;
- розвиток та захист національної інформаційної інфраструктури;
- збереження і примноження духовних, культурних і моральних цінностей Українського народу;
- забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;
- вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;
- зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;
- розвиток медіа-культури суспільства та соціально відповідального медіа-середовища;
- формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;
- створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;
- розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;
- безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;
- розвиток системи стратегічних комунікацій України [2].

На нашу думку, особливої актуальності набуває процес прогнозування і аналізу всього спектра загроз національній безпеці в інформаційній сфері. Причини загроз необхідно виявляти, проводити їх політологічний аналіз для визначення їх системності впливу і виробляти шляхи, методи і засоби їх нейтраліза-

ції. Загрози, які виходять з інформаційного простору на даному етапі світового розвитку є найактуальнішими тому що впливати на об'єкт можливо за допомогою різних інформаційних заходів, інформаційних атак, які характеризуються високою швидкістю поширення інформації великого обсягу, можуть бути нанесені з будь-якої точки землі.

Г. Сащук наголошує, на великому значенні загроз інформаційної безпеки: «Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися світогляд і мораль як окремих осіб, так і суспільства загалом, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності й форм виявів сучасних методів прихованого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які суперечать інтересам національної безпеки» [3].

У науковій літературі розглядається велика кількість класифікацій загроз за різноманітними ознаками.

О. До́ренський провівши аналіз класифікацій виділяє три найбільш прийнятні різновиди класифікаційного поділу загроз безпеці інформації: 1) природні (об'єктивні) та штучні (суб'єктивні); 2) технічні, стихійні, антропогенні; 3) апаратні, програмні, стихійні (природні), антропогенні (людські) [4].

Але зважаючи на постійний розвиток інформаційних технологій і відповідно появи нових загроз перелік не може вважатися таким, який досяг своєї межі. В умовах сучасного швидко мінливого світу з'явилася велика кількість нових понять (інформаційний тероризм - кібертероризм, кібербезпека [5], дестабілізація державної управлінської інфраструктури, комп'ютерні атаки, атаки на віртуальні системи, психологічні операції, різні типи інформаційних війн нових високотехнологічних загроз (застосування інформаційної зброї, розробка високотехнологічних засобів розвідки та ін.) цим обумовлюється необхідність постійного розвитку, вдосконалення та оновлення нормативно-правової бази в інформаційній сфері, а також в галузі регулювання і контролю кіберпростору.

Відповідно до статистичних даних фахівців фінської компанії F-Secure, що працює в сфері інформаційної безпеки, відбувається постій зріст інформаційних атакі кібератак, де Україна є однією з найбільш часто атакованих країн.

Аналіз статистичних даних , щодо держав на які були направлено найбільше інформаційних атак в 2019 році наведено у рис. 1 [5].

На нашу думку, в тексті Доктрини не зазначено важливість забезпечення інформаційної безпеки об'єктів критичної інформаційної інфраструктури. Під об'єктами критичної інформаційної інфраструктури розуміється комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури. До об'єктів критичної інфраструктури відносяться підприємства та установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування держави та суспільс-

тва. Це визначення наведене в «Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» затверджений постановою кабінетів міністрів України від 23 серпня 2016 р. № 563, яка втратила чинність. В чинному порядку формування переліку об'єктів критичної інформаційної інфраструктури дане визначення відсутнє [6].

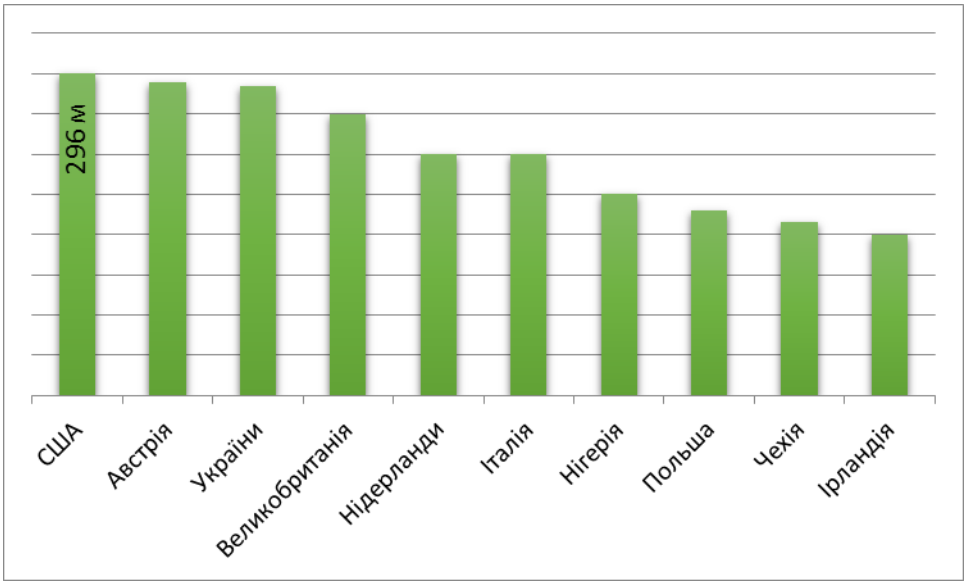

Рис. 1. Перелік держав з найбільшою кількістю кібератак

Відповідно до Оперативної інформації Державної служба спеціального зв'язку та захисту інформації України щодо захисту державних інформаційних ресурсів за період з 30 грудня 2020 по 05 січня 2021 року.

Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 5 055 047 підозрілих подій, що на 17% більше, ніж попереднього тижня. Переважна більшість зафіксованих підозрілих подій стосується спроб викрадення інформації (38%), мережевого сканування (27%), спроб отримання прав користувача (13%) та спроб отримання прав адміністратора (12%) [7]. Відповідно до наведених статистичних даних приходимо к висновку, що кількість інформаційних атак постійно зростає й сучасні складні часи вимагають застосування надійних технологій безпеки. Розрізнених інструментів і одноріневого захисту окремих компонентів інформаційної системи компаній вже недостатньо. Тільки багаторівневі рішення можуть забезпечити комбінований захист від багатокомпонентних і багатоплатформених загроз електронної пошти, призначених для користувача пристроїв, серверів, мережевої та хмарної інфраструктури.

Реалізація державної інформаційної політики забезпечується проведенням єдиних організаційно-технічних заходів на території України органами влади всіх рівнів влади, організаціями та підприємствами щодо забезпечення інформаційної безпеки від внутрішніх і зовнішніх загроз.

Інформаційне забезпечення органів публічної влади є основною умовою

для сталого розвитку та ефективного функціонування державних механізмів, а також проведення процесу публічного управління, яке відповідає сучасним міжнародним реаліям, а також внутрішньодержавним потребам. Щодо пріоритетних напрямків державної політики в інформаційній сфері, то відповідно до Доктрини інформаційної безпеки України до них відносяться: 1) щодо забезпечення інформаційної безпеки; 2) щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію; 3) щодо відкритості та прозорості держави перед громадянами [2].

Висновки. Таким чином, можна відзначити, що формування і оновлення державної політики повинно здійснюватися послідовно з урахуванням національних інтересів держави, постійно мінливих умов і появі нових загроз інформаційної безпеки, які виходять як із зовнішнього інформаційного простору, так і обумовлені внутрішньодержавними змінами. Тільки за умови державного підходу до вирішення проблеми захисту інформації в інформаційних системах, телекомунікаційних мережах Держави можуть бути створені умови для адекватної протидії постійно зростаючим загрозам в інформаційній сфері, в першу чергу, це передбачає вдосконалення національної інформаційної інфраструктури, що включає електронні ЗМІ, банківські системи, системи зв'язку, транспорту, енергетики, промисловості і сфери послуг.

2. На основі проведеного аналізу можна сказати, що рівень захисту інформації не відповідає сучасним процесам, потребам держави і суспільства.

3. Розробка державної політики в сфері забезпечення інформаційної безпеки України, відповідно внутрішньої й зовнішньополітичної ситуації, а також організація процесів державного регулювання представляється актуальною комплексним завданням для сучасного публічного управління.

Список використаних джерел:

1. Конституція України від 28 червня 1996 р. URL: http://zakon5.rada.gov.ua/laws/show/254к/96-вр.

2. Доктрина інформаційної безпеки України: Затверджена указом Президента України від 25 лютого 2017 року №47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#.

3. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки / Г. Сащук. URL: http:// journ. univ.kiev.ua/trk/publikacii/satshuk_publ.php.

4. До́ренський О.П. Дослідження потенційних загроз безпеці інформації інформаційної системи та аналіз їх класифікаційного поділу // Збірник наукових праць Кіровоградського національного технічного університету. Вип. 19, 2007. С. 55-61.

5. https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/.

6. Основні засади забезпечення кібербезпеки України: затверджено Законом України від 05 жовтня 2017 року 2163-VIII https://zakon.rada.gov.ua/laws/show/2163-19.

7. Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури : затверджено Постановою кабінетів міністрів України від 19 червня 2019 р. № 518 https://zakon.rada.gov.ua/laws/show/518-2019.

8. https://cip.gov.ua/ua/news/operativna-informaciya-derzhspeczv-yazku-shodo-zakhistu-

derzhavnikh-informaciinikh-resursiv-za-period-z-30-grudnya-2020-po-05-sichnya-2021-roku.

9. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки. http://visnyk-nanu.org.ua/archive/2014_5.

10. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006.

11. Ткачук П.П., Гула Р.В., Сивак О.І., Щурко О.М., Шемчук В.В. Інформаційна війна і національна безпека: монографія. Л.: НАСВ, 2015.

12. Кормич Б. А. Інформаційна безпека: організаційно-правові основи: навч. посіб. К.: Кондор, 2008.

References:

1. Constitution of Ukraine - 1996 [Konstytutsiia Ukrainy - 1996]. Available to : http://zakon5.rada.gov.ua/laws/show/254k/96-vr Accessed: 28 June 1996.

2. Doctrine of information security of Ukraine [Doktryna informatsiinoi bezpeky Ukrainy]. Available to : https://zakon.rada.gov.ua/laws/show/47/2017
Accessed: 25 February 2017.

3. Sashchuk H. Information security in the system of national security [Informatsiina bezpeka v systemi zabezpechennia natsionalnoi bezpeky] Available to : http:// journ. univ.kiev.ua/trk/publikacii/satshuk_publ.php.

4. Dórenskyi O.P. Research of potential threats to information system information security and analysis of their classification division [Doslidzhennia potentsiinykh zahroz bezpetsi informatsii informatsiinoi systemy ta analiz yikh klasyfikatsiinoho podilu] Kirovohrad, 2007. Print.

5. Available to: https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/.

6. Basic principles of cyber security of Ukraine: approved by the Law of Ukraine [Osnovni zasady zabezpechennia kiberbezpeky Ukrainy] Available to://zakon.rada.gov.ua/laws/show/2163-19 : 05 October 2017.

7. General requirements for cyber security of critical infrastructure [Zahalni vymohy do kiberzakhystu ob'iektiv krytychnoi infrastruktury] Available to://zakon.rada.gov.ua/laws/show/518-2019:19 June 2019.

8. Available to://cip.gov.ua/ua/news/operativna-informaciya-derzhspeczv-yazku-shodo-zakhistu-derzhavnikh-informaciinikh-resursiv-za-period-z-30-grudnya-2020-po-05-sichnya-2021-roku.

9. Zadiraka V.K. Modern methods of solving information security problems[Suchasni metody rozv'iazannia zadach informatsiinoi bezpeky]. Available to://visnyk-nanu.org.ua/archive/2014_5.

10. Lipkan V. A., Maksymenko Yu. Ye., Zhelikhovskyi V. M. Information security of Ukraine in the conditions of European integration [Informatsiina bezpeka Ukrainy v umovakh yevrointehratsii] K.: KNT, 2006. Print.

11. Tkachuk P.P., Hula R.V., Syvak O.I., Shchurko O.M., Shemchuk V.V. Information warfare and national security [Informatsiina viina i natsionalna bezpeka] L.: NASV, 2015. Print.

12. Kormych B. A. Information security: organizational and legal bases [Informatsiina bezpeka: orhanizatsiino-pravovi osnovy] K.: Kondor, 2008. Print.