УДК 355/359:004.056:342(045)

Б. М. Тична,
старший науковий співробітник

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОСНОВА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЗБРОЙНИХ СИЛ УКРАЇНИ

Національний університет оборони України імені Івана Черняховського
проспект Повітрофлотський, 30, 03186, Київ, Україна
E-mail: bm_tychna@ukr.net

Мета: *у статті досліджено зміст інформаційної безпеки у взаємозв'язку з інформаційною діяльністю Збройних сил України.* ***Методи дослідження:*** *використані формально-юридичний та системний методи. Результати: на основі аналізу законодавства та науково обґрунтованих підходів до розуміння змісту інформаційної безпеки, існуючих (та можливих) інформаційних загроз у сфері оборони країни, узагальнено зміст інформаційної безпеки у діяльності Збройних сил України. На основі аналізу норм Конституції України сформульовані принципові засади, які детермінують інформаційну діяльність Збройних сил України щодо забезпечення інформаційної безпеки. Установлено, що інформаційну безпеку у сфері оборони держави забезпечує належним чином урегульована та дієва інформаційна діяльність Збройних сил України за конкретними спрямуваннями.* ***Обговорення:*** *динамічний характер інформаційних загроз і пошук засобів, способів їх протидії у сфері діяльності Збройних сил України зумовлюють потребу подальших наукових досліджень.*

Ключові слова: *інформаційна безпека; Збройні сили України; інформаційна діяльність; інформаційні загрози; негативний інформаційний вплив.*

Постановка проблеми та її актуальність. Зростання цінності інформації у сучасному суспільстві охоплює як приватно-правові, так і глобальні інтереси всього суспільства. Інформаційна безпека є трансформованою складовою національної безпеки України, ефективність проведення якої гарантує суспільству і кожному громадянину захист від загроз, у тому числі інформаційних. Дієвим інструментарієм у цьому контексті є сектор безпеки і оборони, у системі органів якого діють Збройні сили України (далі – ЗСУ) [1, п. 16 ст. 1].

Упровадження інформаційної безпеки набуває дієвості через інформаційну діяльність, яка у ЗСУ відображена у двох основних спрямуваннях: внутрішнє (задоволення інформаційних потреб у межах діяльності ЗСУ із виконання поставлених державою, суспільством завдань) та зовнішнє (реалізація прав громадян на інформацію у зв'язку із функціонуванням ЗСУ). Крім того, інформаційну безпеку необхідно аналізувати через безпеку збереження самої інформації і джерел фіксування (зберігання) ресурсів її обробки. У контексті забезпечення безпеки відкритої інформації Q. Eijkman, D. Weggemans, наголошують на необхідності адаптування держаних органів до онлайн-культури [2]. У зв'язку із цим, суттєве значення у забезпеченні інформаційної безпеки має урегульована та реалізована інформаційна діяльність ЗСУ, з урахування рівня розвиту інформаційного суспільства.

Актуальність дослідження інформаційної безпеки в контексті інформаційної діяльності ЗСУ зростає у зв'язку із наявністю та появою нових видів загроз у інформаційному просторі, зокрема й військового характеру (тимчасова окупація Російською Федерацією (далі – РФ) частини території України – Автономної Республіки Крим і міста Севастополя, розпалювання Росією збройного конфлікту у східних регіонах України та руйнування

системи світової та регіональної безпеки і принципів міжнародного права) [3], що підсилює вимогливість інформаційного суспільства до ЗСУ у протистоянні інформаційним загрозам.

Завдяки новітнім інформаційним технологіям заподіюється шкода національній безпеці держав і без застосування воєнного інструментарію, послаблюється або навіть руйнується конкуруюча держава, не застосовуючи сили, за умови, якщо ця держава не усвідомить реальних і потенційних загроз негативних інформаційних впливів і не створить дієвої системи захисту та протидії цим загрозам [4]. Реальною загрозою для України стало використання РФ найновіших інформаційних технологій, які негативно впливають на свідомість громадян, розпалюють національну і релігійну ворожнечу, пропагують агресивну війну, зміни конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності України [5], разом із тим недопустиме ігнорування й інших чинників негативного впливу на інформаційну безпеку. Саме тому наукового аналізу потребує інформаційна безпека з урахуванням інформаційної діяльності ЗСУ.

Аналіз останніх досліджень і публікацій. Питання інформаційної безпеки досліджені в багатьох наукових працях, зокрема у дисертаційних і монографічних дослідженнях: Ю. П. Лісовської, А. І. Суббота, Т. В. Субіної, О. О. Тихомирова; у публікаціях: О. О. Безвершенко, І. О. Громика, В. М. Желіховського, О. М. Косогова, А. М. Кузьменко, В. А. Ліпкана, Ю. Є. Максименка, Ю. Є. Муравської (Якубівської), В. Р. Остроухова, В. А. Петрика, Т. І. Саханчук, С. В. Северини, та багатьох інших. Разом із тим інформаційна безпека не достатньо досліджена у взаємозв'язку із інформаційною діяльністю ЗСУ, що зумовило визначення **мети** нашого дослідження. Для досягнення цієї мети нами сформульовані завдання, які необхідно вирішити у межах даного дослідження, а саме: установити зміст інформаційної безпеки в межах функціонування ЗСУ; проаналізувати інформаційну діяльності ЗСУ у взаємозв'язку з інформаційною безпекою.

Виклад основного матеріалу. У законодавстві закріплено, що одним із напрямків державної інформаційної політики держави є інформаційна безпека [1, ч. 4 ст. 3; 6, ч. 1 ст. 3] та невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки [6].

Інформаційну безпеку можна розглядати у таких розуміннях: статичному, як захищеність особистості, суспільства та держави від деструктивних та інших негативних впливів в інформаційному просторі; динамічному, як сукупність практичних дій, сплямованих на захист даних від несанкціонованого доступу чи змін, як при їх зберіганні, так і при передачі [7].

О. М. Косогов, аналізуючи протидію інформаційним загрозам в особливий період, зокрема в інтересах ЗСУ та забезпечення інформаційної безпеки особи, суспільства, держави, зазначає, що всебічного захисту та реабілітації потребує цільова аудиторія, яка зазнає негативного інформаційного впливу, а також проведення упереджувальних заходів для його унеможливлення або зниження рівня ефективності [8, с. 42]. У такому контексті О. М. Косогов зводить інформаційні загрози лише до негативного інформаційного впливу, разом з тим існують і інші загрози.

Дійсно негативний інформаційний вплив становить сьогодні серйозну загрозу. Воєнна доктрина України визначає воєнно-політичні виклики, які можуть перерости в загрозу застосування воєнної сили проти України, а саме: цілеспрямований інформаційний (інформаційно-психологічний) вплив з використанням сучасних інформаційних технологій, спрямований на формування негативного міжнародного іміджу України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних і міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин [3, п. 10].

Інформатизація суспільства, електронне урядування, обмін інформацією ЗСУ зі взаємодіючими суб'єктами у сфері оборони засобами телекомунікаційних систем потребують створення додаткових умов у забезпеченні інформаційної безпеки. Розвиток

інформаційних технологій зумовив появу нових інформаційних загроз, кібератак та, відповідно, інформаційних воєн [9, с. 65], що потребує урахування їх у діяльності ЗСУ.

Інформаційна безпека реалізується у напрямку боротьби з витоком закритої (таємної) інформації, а також з розповсюдженням хибної та ворожої інформацій, що обумовлює необхідність здійснення переходу від принципу забезпечення безпеки інформації до принципу інформаційної безпеки, з урахуванням майбутнього розвитку інформатизації, проникнення інформаційних технологій у найважливіші сфери життя суспільства [4]. Безпечне інформаційне середовище детермінує нормальні умови функціонування конкретного органу державного управління, а також проведення моніторингу стану інформаційної безпеки для розроблення оптимальної моделі функціонування системи забезпечення інформаційної безпеки, чим відображається взаємозалежність ефективної діяльності ЗСУ щодо забезпечення інформаційної безпеки, а її належний стан дозволяє функціонувати у сприятливих умовах з'єднанням, військовим частинам і підрозділам ЗСУ.

Змістовними елементами інформаційної безпеки є: інформація з обмеженим доступом; системи і засоби передавання та зберігання інформації; інформаційний простір від поширення інформації, зміст якої через неповноту, недостовірність тощо суперечить національним інтересам держави [10, с. 319].

Існує підхід, за яким інформаційна безпека розглядається як певна сукупність складових чинників, яким може бути заподіяна шкода з точки зору інформаційних відносин, зокрема: охорона і захист інформації; недопущення негативного інформаційного впливу на діяльність органів влади; забезпечення реалізації конституційних прав, свобод і законних інтересів людини, громадянина, підприємств, установ, закладів усіх форм власності у відповідній сфері [11, с. 12].

Інформаційна безпека є багатовимірною категорією, що відображає рівень захищеності інформаційного середовища, реалізацію прав та обов'язків суб'єктів інформаційних правовідносин, інформаційну діяльність, інформаційні процеси з використанням наявних інформаційних ресурсів, нормальне функціонування інформаційних систем; збереження та цілісність інформації, розпорядником якої є ЗСУ (авт.); управління загрозами за допомогою здійснення аналізу ризиків шляхом обробки інформації для визначення наявних і потенційно можливих ризиків у сфері оборони країни (авт.), урахування як зовнішніх, так і внутрішніх загрозливих факторів [12, с. 83].

Цілеспрямований вплив на забезпечення інформаційної безпеки відбувається через інформаційну діяльність ЗСУ, втілену в конкретних її видах створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Правове підґрунтя інформаційної діяльності, а саме: урегульовані правила її здійснення, процедури що формують стан безпечного створення, використання, обробки, поширення інформації, недопущення іншого негативного впливу на інформаційні відносини створюють:

– закони України «Про інформацію», «Про державну таємницю», «Про Національну програму інформатизації», «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про науково-технічну інформацію», «Про доступ до публічної інформації», «Про звернення громадян» «Про захист персональних даних» тощо;

– укази Президента України «Питання забезпечення органами виконавчої влади доступу до публічної інформації», «Про першочергові заходи щодо забезпечення реалізації та гарантування конституційного права на звернення громадян до органів державної влади та органів місцевого самоврядування»;

– наказ Уповноваженого Верховної Ради України з прав людини «Типовий порядок обробки персональних даних»;

– постанови та розпорядження Кабінету Міністрів України «Про затвердження Типової

інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію», «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах»; «Про затвердження плану заходів з реалізації Концепції розвитку електронного урядування в Україні»;

– наказ Міністерства оборони України «Про затвердження Порядку обробки і захисту персональних даних у Міністерстві оборони України» тощо.

Основні положення інформаційної діяльності щодо забезпечення інформаційної безпеки закріплені в Конституції України, принципи яких деталізовані у законах і підзаконних нормативно-правових актах нашої держави [13, с. 113], а саме:

– інформаційна діяльність повинна здійснюватись з урахуванням забезпечення інформаційної безпеки України, яка є пріоритетом у діяльності ЗСУ [14, ст. 17];

– дотримуватись меж дозволеного та забороненого під час збирання інформації [14, ч. 2 ст. 32];

– урахування захисту приватності, дотримання інформаційних прав інших суб'єктів інформаційних правовідносин, зокрема фізичних осіб: свобода особистого і сімейного життя [14, ч. 1 ст. 32];

– дотримуватись таємниці листування, телефонних переговорів, телеграфної та іншої кореспонденції [14, ст. 31];

– надавати можливість особі знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відомостями про себе, якщо такі відомості не належать до державної або іншої захищеної законом таємниці [14, ч. 3 ст. 32];

– не перешкоджати праву громадян вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [14, ст. 34].

Окрему ланку у забезпеченні інформаційної безпеки посідає дієвість застосування відповідальність за управління у сфері інформаційної діяльності [15, с. 76], за порушення норм інформаційного законодавства, порядку, підстав надання та отримання інформації (обігу інформації) тощо.

Висновки. Отже, проаналізоване дозволяє установити, що інформаційну безпеку у сфері оборони держави забезпечує належним чином урегульована та дієва інформаційна діяльність ЗСУ, яка спрямована на створення нормальних умов функціонування з'єднань, військових частин і підрозділів, чим підкреслюється подвійний взаємозв'язок і залежність між діяльністю ЗСУ та інформаційною безпекою; недопущення витоку державної таємниці, розповсюдження службової інформації, персональних даних, а також неправдивої інформації у сфері оборони країни; недопущення деструктивного інформаційного впливу на особовий склад підрозділів та населення України у сфері функціонування ЗСУ; недопущення кібератак на інформаційні системи відомчого та міжвідомчого характеру. Загалом інформаційна безпека у сфері діяльності ЗСУ орієнтована на недопущення існуючих, можливих (прогнозованих) загроз проти безпечного функціонування ЗСУ та сфери їх відповідальності й залежить безпосередньо від планування та здійснення інформаційної діяльності спрямованої на недопущення втілення інформаційних загроз у реальність та чіткого дотримання законодавства під час реалізації окремих видів інформаційної діяльності ЗСУ.

Аналіз сучасних інформаційних загроз та засоби їх протидії у сфері діяльності ЗСУ можуть становити перспективний напрямок для подальших наукових досліджень.

Література

1. Про національну безпеку України: Закон України від 21 чер. 2018 р. *Голос України*. 2018. № 22.

2. Open source intelligence and privacy dilemmas. *Security and Human Rights*. 2012. № 4. P. 286–287.

3. Воєнна доктрина України: Указ Президента України від 24 вер. 2015 р. № 555/2015. *Урядовий кур'єр*. 2015. № 178.

4. Безвершенко О.О. Інформаційна безпека України в системі забезпечення національної безпеки. URL: http://www.rusnauka.com/ 13_NPN_2010/ Pravo/ 66151.doc.htm

5. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лют. 2017 р. № 47/2017. *Офіційний вісник Президента України*. 2017. № 5. Ст. 102.

6. Про Концепцію Національної програми інформатизації: Закон України від 04 лют. 1998 р. *Відомості Верховної Ради України*. 1998. № 27. Ст. 182.

7. Fruhlinger J. What is information security? Definition, principles, and jobs. URL: https:// www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html.

8. Косогов О.М. Підхід до побудови державної системи протидії інформаційним загрозам в особливий період. *Збірник наукових праць Харківського університету Повітряних сил*. 2015. № 4. С. 40–43.

9. Сопілко І.М. Становлення інформаційного суспільства та інформаційні загрози в мережі Інтернет. *Юридичний вісник «Повітряне і космічне право»*. Київ: НАУ, 2017. № 3 (44). С. 61–69. DOI: 10.18372/2307-9061.44.12068

10. Кузьменко А.М. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протиборства. *Часопис Київського університету права*. 2010. № 4. С. 317–321.

11. Субіна Т.В. Адміністративно-правове забезпечення інформаційної безпеки в органах Державної податкової служби України: автореф. дис. ... канд. юрид. наук: 12.00.07. Ірпінь, 2010. 19 с.

12. Кушнір І.П. Співвідношення понять «інформаційна безпека» та «захист інформації» в діяльності Державної прикордонної служби України. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція.* 2018. № 35. Т. 1. С. 81–84.

13. Селезньова О.М. Теоретико-методологічні основи інформаційного права України: монографія. Чернівці: Місто, 2014. 408 с.

14. Конституція України від 28 чер. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141. URL: http://zakon0.rada.gov.ua/ laws/254 %D0 %BA/96-%D0 %B2 %D1 %80.

15. Bohumil Pikna Evropská pohraniční a pobřežní stráž – «nová» agentura FRONTEX Časopis Policajná teória a prax 4-2017 p. 75-84.

References

1. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.2018. *Holos Ukriny*. 2018. № 22.

2. Open source intelligence and privacy dilemmas. Security and Human Rights. 2012. № 4. P. 286–287.

3. Voienna doktryna Ukrainy: Ukaz Prezydenta Ukrainy vid 24.09.2015. № 555/2015. *Uriadovyi kurier*. 2015. № 178.

4. Bezvershenko O.O. Informatsiina bezpeka Ukrainy v systemi zabezpechennia natsionalnoi bezpeky. URL: http://www.rusnauka.com/ 13_NPN_2010/Pravo/66151.doc.htm

5. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29.12.2016. «Pro Doktrynu informatsiinoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 25.02.2017 № 47/2017. *Ofitsiinyi visnyk Prezydenta Ukrainy*. 2017. № 5. St. 102.

6. Pro Kontseptsiiu Natsionalnoi prohramy informatyzatsii: Zakon Ukrainy vid 04.021998. *Vidomosti Verkhovnoi Rady Ukrainy*. 1998. № 27. St. 182.

7. Fruhlinger J. What is information security? Definition, principles, and jobs. URL: https:// www.csoonline.com/article/3513899/what-is-information-security-definition-principles-and-jobs.html.

8. Kosohov O.M. Pidkhid do pobudovy derzhavnoi systemy protydii informatsiinym zahrozam v osoblyvyi period. *Zbirnyk naukovykh prats Kharkivskoho universytetu Povitrianykh syl*. 2015. № 4. S. 40–43.

9. Sopilko I.M. Stanovlennia informatsiinoho suspilstva ta informatsiini zahrozy v merezhi Internet. *Yurydychnyi visnyk «Povitriane i kosmichne pravo»*. Kyiv: NAU, 2017. № 3 (44). S. 61–69.

10. Kuzmenko A.M. Osoblyvosti problem zakonodavchoho zabezpechennia informatsiinoi bezpeky derzhavy, suspilstva i hromadianyna v umovakh informatsiino-psykholohichnoho

protyborstva. *Chasopys Kyivskoho universytetu prava*. 2010. № 4. S. 317–321.

11. Subina T.V. Administratyvno-pravove zabezpechennia informatsiinoi bezpeky v orhanakh Derzhavnoi podatkovoi sluzhby Ukrainy: avtoref. dys. ... kand. yuryd. nauk: 12.00.07. Irpin, 2010. 19 s.

12. Kushnir I.P. Spivvidnoshennia poniat «informatsiina bezpeka» ta «zakhyst informatsii» v diialnosti Derzhavnoi prykordonnoi sluzhby Ukrainy. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia: Yurysprudentsiia*. 2018. № 35. T. 1. S. 81–84.

13. Selezniova O.M. Teoretyko-metodolohichni osnovy informatsiinoho prava Ukrainy: monohrafiia. Chernivtsi: Misto, 2014. 408 s.

14. Konstytutsiia Ukrainy: Zakon Ukrainy vid 28.06.1996. № 254k/96-VR. *Vidomosti Verkhovnoi Rady Ukrainy*. 1996. № 30. St. 141. URL: http://zakon0. rada. gov.ua/laws/254 %D0 %BA/96-%D0 %B2 %D1 %80.

15. Bohumil Pikna Evropská pohraniční a pobřežní stráž – «nová» agentura FRONTEX Časopis Policajná teória a prax 4-2017 p. 75-84.

B. Tychna

INFORMATION SECURITY AS THE BASIS OF INFORMATION ACTIVITY OF THE ARMED FORCES OF UKRAINE

The National Defense University of Ukraine named after Ivan Cherniakhovskyi
Povitroflotskyi Avenue, 30, 03186, Kyiv, Ukraine
E-mail: bm_tychna@ukr.net

***Purpose**: the article deals with the research of the content of information security in relation to the information activities of the Armed Forces of Ukraine. **Research methods:** formal legal and systemic methods are used. **Results**: based on the analysis of legislation and science-based approaches to understanding the content of information security, existing (and possible) information threats in the country's defence sphere, the content of information security in the Armed Forces activities is generalized. Based on the analysis of the norms of the Constitution of Ukraine, the principles that determine the information activity of the Armed Forces on information security are formulated. It is defined that information security in the country's defence sphere is provided by properly adjusted and effective information activities of the Armed Forces in specific areas. **Discussion**: the dynamic nature of information threats and the search for means and ways of counteracting them in the sphere of activity of the Armed Forces of Ukraine determine the need for further scientific research.*

It is defined that the main provisions of information activities on ensuring information security are enshrined in the Constitution of Ukraine, the principles of which are detailed in the laws and by-laws of our state adjusting the procedure of creating normal conditions of functioning of military formations, detachments and units, establishing legal regimes of information, including sensitive information, preventing the dissemination of false information in the field of defence of the country, preventing destructive information influence on the personnel of units and population of Ukraine in the sphere of the Armed Forces functioning, cyberattack on departmental and interdepartmental information systems.

It is summarized that information security in the Armed Forces activity is focused on the prevention of existing, possible (predicted) threats against the safe functioning of the Armed Forces of Ukraine and their sphere of responsibility and depends directly on the planning, implementation of information activities aimed at preventing the implementation of information threats into reality and clearly respecting the legislation during the implementation of certain types of information activities of the Armed Forces of Ukraine.

***Keywords:** information security; the Armed Forces of Ukraine; information activity; information threats; negative information impact.*