ТИЧНА Б. М.,
старший науковий співробітник
науково-дослідного відділу проблем
військового законодавства
Центру воєнно-стратегічних досліджень
*(Національний університет оборони
України імені Івана Черняховського)*

УДК 355/359:004.056
DOI https://doi.org/10.32842/2078-3736/2020.2-2.35

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОСНОВА ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЗБРОЙНИХ СИЛ УКРАЇНИ

Варто зазначити, що Збройні Сили України є сьогодні активним учасником інформаційних відносин, що зумовлено вимогами часу: потребами більшої відкритості перед суспільством, формуванням таких цивільно-військових відносин, які мають слугувати інтересам усього суспільства. У спеціальних військових виданнях і засобах масової інформації систематично висвітлюються питання повсякденної діяльності військових, ситуація в районі проведення операції Об'єднаних сил, соціально-правового захисту військовослужбовців, реформування ЗСУ, боротьби з корупцією у військовій сфері тощо.

Але ця багатогранна інформаційна діяльність здійснюється, як правило, не системно, інколи стихійно, як відповідь на ті чи інші гострі проблеми або ситуації, які виникають у ЗСУ, а отже, не завжди об'єктивно висвітлює ті проблеми, які супроводжують життєдіяльність військових. Виникла необхідність узагальнення напрацьованого досвіду з метою вироблення на цій основі головних регулятивних чинників – принципів і постановки практичних завдань подальшого нарощування інформаційної діяльності.

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

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

Tychna B. M. Information security as the basis of information activity of the armed forces of Ukraine

It should be noted that presently the Armed Forces of Ukraine is an active participant of information relations, which is dictated by the time: requirements to be more open to the society, establishment of such civil-military relations that should serve the interests

of the whole society. Specialized military publications and media provide information about routine activities of the military, situation in the area of Joint Forces Operation, social and legal protection of military personnel, reforms of the Armed Forces, fighting corruption in the military domain and other on the regular basis.

Meanwhile, these multifaceted information activities are carried out, as a rule, not in a systematic fashion, sometimes as a response to certain acute problems or situations, which emerge in the Armed Forces of Ukraine, thus not always objectively cover the issues, which follow the routine activities of the military. All that resulted into the necessity to conduct lessons learned in order to develop major regulatory factors – the principles and define the tasks to further enhance information activities.

Objective: the article explores the contents of information security in close relation with the information activities of the Armed Forces of Ukraine. Research methods: formal-legal and system methods. Results: the content of the information security within the Armed Forces of Ukraine activities has been generalized based on the analysis of the legislation and scientifically justified approaches for understanding the content of information security, current (and potential) information threats in the area of the national defense. The foundations, which define information activities of the Armed Forces of Ukraine to ensure information security, have been established based on the Constitution of Ukraine provisions' analysis. It has been established that information security in the area of national defense is provided by the properly regulated and efficient information activities of the Armed Forces of Ukraine in certain directions. Discussion: dynamic nature of information threats and search of methods and ways to address them within the Armed Forces of Ukraine activities, require further scientific research.

Key words: *information security, Armed Forces of Ukraine, information activities, information threats, negative information influence.*

Вступ. Зростання цінності інформації в сучасному суспільстві охоплює як приватноправові, так і глобальні інтереси всього суспільства. Інформаційна безпека є трансформованим складником національної безпеки України, ефективність проведення якої гарантує суспільству й 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 в ЗСУ відображена у двох основних спрямуваннях: внутрішньому (задоволення інформаційних потреб у межах діяльності ЗСУ з виконання поставлених державою, суспільством завдань) і зовнішньому (реалізація прав громадян на інформацію у зв'язку з функціонуванням ЗСУ). Крім того, інформаційну безпеку необхідно аналізувати через безпеку збереження самої інформації й джерел фіксування (зберігання) ресурсів її обробки. Але суттєве значення в забезпеченні інформаційної безпеки має урегульована та реалізована інформаційна діяльність ЗСУ.

Актуальність дослідження інформаційної безпеки в контексті інформаційної діяльності ЗСУ зростає у зв'язку з наявністю та появою нових видів загроз в 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 в східних регіонах України та руйнування системи світової й регіональної безпеки та принципів міжнародного права) [2], що підсилює вимогливість інформаційного суспільства до ЗСУ в протистоянні інформаційним загрозам.

В умовах «гібридної війни» одним із основних засобів є інформаційне протистояння, де «вже не фізичний, а віртуальний простір став стратегічним полем бою, докорінно змінивши геополітичні та військово-політичні пріоритети» [3, с. 189]. Завдяки новітнім

інформаційним технологіям заподіюється шкода національній безпеці держав і без застосування воєнного інструментарію, послаблюється або навіть руйнується конкуруюча держава без застосування сили за умови, що 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 й релігійну ворожнечу, пропагують агресивну війну, зміни конституційного ладу насильницьким шляхом, порушення суверенітету й 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.

Постановка завдання. Питання інформаційної безпеки досліджені в багатьох наукових працях, зокрема в 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 й багатьох інших. Разом із тим інформаційна безпека недостатньо досліджена у взаємозв'язку з інформаційною діяльністю ЗСУ, що зумовило визначення мети дослідження. Для досягнення цієї мети нами сформульовані завдання, які необхідно вирішити в межах дослідження, а саме: установити зміст інформаційної безпеки в межах функціонування ЗСУ; проаналізувати інформаційну діяльності ЗСУ у взаємозв'язку з інформаційною безпекою.

Результати дослідження. У законодавстві закріплено, що одним із напрямів державної інформаційної політики держави є інформаційна безпека [1, ч. 4 ст. 3; 6, ч. 1 ст. 3], що є невід'ємною частиною політичного, економічного, оборонного й інших складників національної безпеки [6].

Під інформаційною безпекою розуміють захищеність особистості, суспільства та держави від деструктивних та інших негативних впливів в інформаційному просторі [7, с. 26].

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 й 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 із тим існують й 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 [2, п. 10]. А.І. Суббот, окрім інформаційного впливу, пропонує розглядати ще один напрям інформаційної безпеки – захист і збереження особистої, корпоративної та державної інформації [9, с. 29].

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 і, відповідно, інформаційних воєн [10, с. 65], що потребує урахування їх у діяльності ЗСУ.

Інформаційна безпека реалізується в напрямі боротьби з витоком закритої (таємної) інформації, а також із розповсюдженням хибної та ворожої інформації, що зумовлює 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 дає змогу функціонувати в сприятливих умовах з'єднанням, військовим частинам і підрозділам ЗСУ.

Змістовими елементами інформаційної безпеки є інформація з обмеженим доступом; системи й засоби передавання та зберігання інформації; інформаційний простір від поширення інформації, зміст якої через неповноту, недостовірність тощо суперечить національним інтересам держави [11, с. 319].

Існує підхід, за яким інформаційна безпека розглядається як певна сукупність складових чинників, яким може бути заподіяна шкода з погляду інформаційних відносин, а саме: охорона й 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 [12, 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 [13, с. 83].

Цілеспрямований вплив на забезпечення інформаційної безпеки відбувається через інформаційну діяльність ЗСУ, утілену в конкретних її видах, таких як створення, збирання, одержання, зберігання, використання, поширення, охорона й захист інформації [14].

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 й 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 в законах і підзаконних нормативно-правових актах нашої держави [15, с. 113], а саме:

– інформаційна діяльність повинна здійснюватися з урахуванням забезпечення інформаційної безпеки України, яка є пріоритетом у діяльності ЗСУ;

– дотримуватися меж дозволеного та забороненого під час збирання інформації [16, ч. 2 ст. 32];

– урахування захисту приватності, дотримання інформаційних прав інших суб'єктів інформаційних правовідносин, зокрема фізичних осіб: свобода особистого й сімейного життя [16, ч. 1 ст. 32];

– дотримуватися таємниці листування, телефонних переговорів, телеграфної та іншої кореспонденції [16, 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 [16, ч. 3 ст. 32];

– не перешкоджати праву громадян вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [16, ст. 34].

Висновки. Отже, проаналізоване дає змогу встановити, 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 і 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 наявних, можливих (прогнозованих) загроз проти безпечного функціонування ЗСУ та сфери їх відповідальності й залежить безпосередньо від планування, здійснення інформаційної діяльності, спрямованої на недопущення втілення інформаційних загроз у реальність, і чіткого дотримання законодавства під час реалізації окремих видів інформаційної діяльності ЗСУ.

Аналіз сучасних інформаційних загроз і засобів протидії їм у сфері діяльності ЗСУ можуть становити перспективний напрям для подальших наукових досліджень.

Список використаних джерел:

1. Про національну безпеку України : Закон України від 21.06.2018. *Голос України*. 2018. № 22.

2. Воєнна доктрина України : Указ Президента України від 24.09.2015 № 555/2015. *Урядовий кур'єр*. 2015. № 178.

3. Трофименко О.Г., Дубовий Я.В. Еволюція поглядів на інформаційні війни в епоху інформаційного суспільства. *Порівняльно-аналітичне право*. 2017. № 1. С. 189–192.

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 29.12.2016 «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017. *Офіційний вісник Президента України*. 2017. № 5. Ст. 102.

6. Про Концепцію Національної програми інформатизації : Закон України від 04.021998. *Відомості Верховної Ради України*. 1998. № 27. Ст. 182.

7. Гапеєва О.Л. Актуальні проблеми інформаційної безпеки: досвід ОДКБ. *Інформаційний вимір гібридної війни: досвід України:* матеріали Міжнародної науково-практичної конференції. Київ : НУОУ, 2017. С. 25–28.

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. Суббот А. Інформаційна безпека суспільства. *Віче*. 2015. № 8. С. 29–31

10. 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.

11. 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-

ШЕВЧЕНКО А. В.,
кандидат юридичних наук, суддя
(Київський окружний адміністративний суд)

УДК 342.9
DOI https://doi.org/10.32842/2078-3736/2020.2-2.36

ФУНКЦІЇ КАДРОВОЇ РОБОТИ В СУДОВІЙ СИСТЕМІ

У статті проведено аналіз поняття та видів функцій кадрової роботи в судових органах України.

Серед основних функцій у системі кадрового менеджменту в судових органах визначено: мотиваційну, професійного зростання, облікового забезпечення, визначення та прогнозування штату суддів та персоналу, дисциплінарну, соціально-правову, нормалізації навантаження тощо.

Функції кадрової роботи в судових органах – це зовнішні прояви та напрями реалізації кадрових завдань, що визначені метою кадрового менеджменту, здійснення яких суб'єктами кадрової діяльності закріплено законодавчими та підзаконними актами у сфері судового адміністрування та державної служби.

Закріплення загальних та спеціальних функцій кадрової роботи в судових органах має знайти свій нормативний прояв у Типовому положенні про кадрову роботу в судових органах, яке слід розробити в напрямі удосконалення правового забезпечення судового адміністрування.

Мета роботи кадрових інституцій в органах правосуддя є квінтесенцією визначення функцій кадрової діяльності. Зміст мети розкривається у формуванні високопрофесійного корпусу суддів та персоналу судів, забезпечення стабільного фахового зростання, високої дисципліни та авторитету системи правосуддя.

Прояви мотивації у роботі судді полягають не тільки у ефективному здійсненні судових функцій, дотриманні процедур, а й в ухваленні судових рішень із зрозумілим обґрунтуванням (мотивацією).

Низка спеціальних функцій для кадрової роботи випливають із законодавчого та підзаконного нормативного регулювання правосуддя та судового адміністрування.

Дисциплінарна функція полягає у забезпеченні суддею дотримання норм суддівської етики та поведінки. Хибними є думки, що дисциплінарна діяльність