УДК 004.056.5:355.45
DOI https://doi.org/10.32782/2524-0374/2024-12/104

ПРАВОВІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ІНФОРМАТИЗАЦІЇ ТА ЗВ'ЯЗКУ В ЕЛЕКТРОМАГНІТНОМУ СЕРЕДОВИЩІ ТА КІБЕРПРОСТОРІ ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ВИКОНАННЯ ЗАВДАНЬ ПІДРОЗДІЛАМИ СИЛ ОБОРОНИ І БЕЗПЕКИ УКРАЇНИ

LEGAL BASIS OF INFORMATION SECURITY, INFORMATIZATION AND COMMUNICATIONS IN THE ELECTROMAGNETIC ENVIRONMENT AND CYBERSPACE AS A COMPONENT OF ENSURING THE FULFILLMENT OF TASKS BY UNITS OF THE DEFENSE AND SECURITY FORCES OF UKRAINE

Пащенко Є.М., старший викладач кафедри військового права
Військово-юридичний інститут
Національного юридичного університету імені Ярослава Мудрого

Корольов С.С., к.і.н., доцент,
начальник кафедри загальновійськових дисциплін
Військово-юридичний інститут
Національного юридичного університету імені Ярослава Мудрого

Гашенко С.В., старший викладач кафедри загальновійськових дисциплін
Військово-юридичний інститут
Національного юридичного університету імені Ярослава Мудрого

Мороховський М.Л., доцент кафедри загальновійськових дисциплін
Військово-юридичний інститут
Національного юридичного університету імені Ярослава Мудрого

Прозванюк О.В., викладач кафедри забезпечення державної безпеки
Національна академія Національної гвардії України

У статті розглянуто правові аспекти забезпечення інформаційної безпеки, інформатизації та зв'язку в електромагнітному середовищі та кіберпросторі як невід'ємної складової виконання завдань підрозділами Сил оборони і безпеки України. Проаналізовано основні нормативно-правові документи, що регулюють функціонування системи інформаційної безпеки держави, зокрема у військовій сфері. Розкрито зміст та значення ключових законодавчих актів у сфері інформатизації, зв'язку і кібербезпеки, спрямованих на захист критичної інформаційної інфраструктури та протидію кіберзагрозам. Визначено роль і місце правового забезпечення інформаційної безпеки як важливого чинника виконання завдань Силами оборони і безпеки України в умовах гібридної війни. Окреслено напрями подальшого вдосконалення нормативно-правової бази у цій сфері з урахуванням сучасних викликів і загроз національній безпеці України в інформаційній сфері. Досліджено особливості імплементації міжнародних стандартів та передових практик у сфері інформаційної безпеки в національне законодавство України. Висвітлено механізми координації діяльності різних державних органів та установ у забезпеченні інформаційної безпеки та кіберзахисту. Проаналізовано специфіку організації системи управління інформаційною безпекою в умовах ведення бойових дій та протидії гібридним загрозам. Розглянуто питання технічного та організаційного забезпечення захисту інформації в інформаційно-телекомунікаційних системах військового призначення. Запропоновано комплекс заходів щодо підвищення ефективності правового регулювання у сфері забезпечення інформаційної безпеки та кіберзахисту об'єктів критичної інфраструктури. Обґрунтовано необхідність постійного оновлення та адаптації нормативно-правової бази відповідно до еволюції інформаційних загроз та розвитку технологій.

Ключові слова: інформаційна безпека, інформатизація, зв'язок, електромагнітне середовище, кіберпростір, кібербезпека, критична інформаційна інфраструктура, Сили оборони і безпеки України.

The article considers the legal aspects of ensuring information security, informatization and communications in the electromagnetic environment and cyberspace as an integral component of the fulfillment of tasks by units of the Defense and Security Forces of Ukraine. The main regulatory and legal documents regulating the functioning of the state information security system, in particular in the military sphere, are analyzed. The content and significance of key legislative acts in the field of informatization, communications and cybersecurity aimed at protecting critical information infrastructure and countering cyber threats are revealed. The role and place of legal support of information security as an important factor in the fulfillment of tasks by the Defense and Security Forces of Ukraine in the conditions of a hybrid war are determined. The directions of further improvement of the regulatory and legal framework in this area are outlined, taking into account modern challenges and threats to the national security of Ukraine in the information sphere. The peculiarities of implementing international standards and best practices in the field of information security into the national legislation of Ukraine are studied. The mechanisms of coordinating the activities of various state bodies and institutions in ensuring information security and cyber defense are highlighted. The specifics of organizing the information security management system in the conditions of combat operations and countering hybrid threats are analyzed. Issues of technical and organizational support for information protection in military information and telecommunications systems are considered. A set of measures is proposed to improve the effectiveness of legal regulation in the field of information security and cyber protection of critical infrastructure facilities. The necessity of constant updating and adaptation of the regulatory framework in accordance with the evolution of information threats and technology development is substantiated.

Key words: information security, informatization, communications, electromagnetic environment, cyberspace, cybersecurity, critical information infrastructure, Defense and Security Forces of Ukraine.

В сучасних умовах розвитку інформаційного суспільства та глобалізаційних процесів, питання забезпечення інформаційної безпеки держави набувають особливої актуальності. В умовах гібридної війни, яку російська федерація веде проти України, інформаційна сфера стала одним з основних театрів бойових дій. Агресор активно використовує методи інформаційно-психологічного впливу, кібератаки та інші деструктивні технології для досягнення своїх геополітичних цілей.

У зв'язку з цим надзвичайно важливим є створення надійної та ефективної системи інформаційної безпеки держави, зокрема у військовій сфері. Ключову роль у цьому відіграє розробка та вдосконалення правових основ функціонування такої системи, адже саме нормативно-правова база визначає засади державної політики у сфері інформаційної безпеки, повноваження та взаємодію суб'єктів забезпечення інформаційної безпеки, механізми протидії інформаційним загрозам тощо.

Особливого значення набуває правове регулювання інформаційної безпеки, інформатизації та зв'язку в електромагнітному середовищі та кіберпросторі, адже саме ці сфери є найбільш вразливими до кіберзагроз. Від надійності функціонування систем зв'язку та інформаційних систем, стійкості їх до кібератак значною мірою залежить ефективність виконання завдань підрозділами Сил оборони і безпеки України.

Відтак, метою даної статті є аналіз правових основ інформаційної безпеки, інформатизації та зв'язку в електромагнітному середовищі та кіберпросторі як складової забезпечення виконання завдань підрозділами Сил оборони і безпеки України, визначення ролі та значення відповідної нормативно-правової бази, а також окреслення напрямів її подальшого вдосконалення з урахуванням сучасних викликів і загроз.

Конституція України визначає, що забезпечення інформаційної безпеки є однією з найважливіших функцій держави, справою всього Українського народу (ст. 17) [1]. Саме на реалізацію цього конституційного положення спрямована вся система законодавства у сфері інформаційної безпеки.

Основними нормативно-правовими актами, що регулюють питання інформаційної безпеки в Україні, є закони України «Про Концепцію Національної програми інформатизації» [4], «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [5], «Про захист інформації в інформаційно-телекомунікаційних системах» [6], «Про основні засади забезпечення кібербезпеки України» [7] та ін.

Закон України «Про національну безпеку України» [2] відносить інформаційну безпеку до фундаментальних національних інтересів України. Загрози інформаційній безпеці визначаються серед актуальних загроз національній безпеці України. Суб'єктами сектору безпеки і оборони забезпечується, у межах визначених законодавством, інформаційна безпека, кібербезпека та безпека інформаційних ресурсів.

Доктрина інформаційної безпеки України [3], затверджена Указом Президента України від 25 лютого 2017 року № 47/2017, є основним концептуальним документом, що визначає засади державної інформаційної політики та напрямки розвитку системи інформаційної безпеки держави. Доктрина окреслює національні інтереси України в інформаційній сфері, наявні загрози їх реалізації, а також пріоритети та напрями державної політики в інформаційній сфері.

Зокрема, одним із пріоритетів державної політики в інформаційній сфері згідно Доктрини є забезпечення надійного функціонування та всебічного розвитку національної інформаційної інфраструктури, зокрема в умовах цифровізації. Серед основних напрямів реалізації пріоритетів державної політики в інформаційній сфері визначено вдосконалення правових та організаційних механізмів забезпечення інформаційної безпеки, зокрема захисту державних інформаційних ресурсів, протидії поширенню негативного інформаційного впливу.

Правові засади функціонування системи зв'язку в Україні, в тому числі в інтересах оборони та безпеки держави, визначені Законом України «Про телекомунікації» [8]. Зокрема, ст. 8 вказаного Закону встановлює, що центральні органи виконавчої влади в межах своїх повноважень забезпечують функціонування і розвиток телекомунікацій спеціального призначення для потреб національної безпеки та оборони України. Згідно ст. 25 наведеного Закону оператори зобов'язані надавати на договірних засадах ресурси своїх мереж на потреби національної безпеки та оборони, ліквідації надзвичайних ситуацій, забезпечення правопорядку, а також зобов'язані забезпечувати і фінансувати створення та функціонування системи захисту інформації в телекомунікаційних мережах.

Закон України «Про радіочастотний ресурс України» [9] регулює використання радіочастот як обмеженого ресурсу, в тому числі для потреб національної безпеки і оборони. Згідно ст. 23 Закону виділення радіочастотного ресурсу України для потреб оборони здійснюється з урахуванням пріоритетності таких потреб та забезпечення радіочастотним ресурсом функціонування телекомунікаційних мереж спеціального призначення.

Особлива увага у законодавстві приділяється питанням кібербезпеки як невід'ємної складової інформаційної безпеки. Закон України «Про основні засади забезпечення кібербезпеки України» [7] визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі. Закон визначає національну систему кібербезпеки, об'єкти кіберзахисту, основні суб'єкти забезпечення кібербезпеки та їх завдання, а також принципи та засади забезпечення кібербезпеки України.

Одним із ключових понять Закону є критична інформаційна інфраструктура (надалі – КІІ) – сукупність об'єктів інфраструктури держави у інформаційній сфері, кібератака на які може створити негативний вплив на стан національної безпеки, економічної та соціальної сфери. КІІ підлягає обов'язковому захисту від кіберзагроз.

Стратегія кібербезпеки України [10], затверджена Указом Президента України від 15 березня 2016 року № 96/2016, визначає загальний погляд на проблематику забезпечення кібербезпеки держави та визначає ключові напрями державної політики у цій сфері. Зокрема, Стратегія передбачає вдосконалення нормативно-правової бази з питань кібербезпеки, формування системи підготовки кадрів у цій сфері, забезпечення захисту КІІ та державних електронних інформаційних ресурсів, розвиток міжнародного співробітництва у галузі кібербезпеки.

Окрему увагу законодавець приділяє питанням захисту інформації в інформаційно-телекомунікаційних системах. Відповідні норми містяться у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» [6], який регулює відносини у сфері захисту відомостей, що обробляються в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Захист інформації забезпечується шляхом використання комплексу правових, організаційних і технічних заходів.

Слід відзначити також роль міжнародного права у сфері інформаційної безпеки. На сьогодні існує низка міжнародних договорів, які регламентують питання співробітництва держав щодо протидії кіберзлочинності та захисту критичної інформаційної інфраструктури. Зокрема, це Конвенція про кіберзлочинність [11], Додатковий протокол до неї [12], Угода про співробітництво

держав-учасниць СНД у боротьбі зі злочинами у сфері комп'ютерної інформації [13]. Україна є учасницею цих договорів, відтак їх положення є частиною національного законодавства.

Окремі аспекти правового забезпечення інформаційної безпеки у військовій сфері регулюються низкою підзаконних нормативно-правових актів. Зокрема, це Указ Президента України від 20 травня 2016 року № 216/2016 «Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України» [4], Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави» [5] та ін.

Значну роль відіграють також норми спеціальних законів, що регулюють діяльність правоохоронних органів та спецслужб у сфері забезпечення інформаційної безпеки. Так, в Законі України «Про Службу безпеки України» [6] визначено, що до завдань наведеного органу належить здійснення інформаційно-аналітичної роботи в інтересах ефективного проведення органами державної влади внутрішньої і зовнішньої діяльності, протидія зовнішнім загрозам національній безпеці України у інформаційній сфері. Згідно із Законом України «Про контррозвідувальну діяльність» [7] здійснення контррозвідувального забезпечення інформаційної безпеки є складовою контррозвідувальної діяльності.

Варто зауважити, що існуюча нормативно-правова база з питань інформаційної безпеки певно мірою не встигає за реальним розвитком інформаційних технологій та появою нових викликів і загроз. У зв'язку з цим актуальним завданням є постійне вдосконалення законодавства в даній сфері, його адаптація до сучасних реалій.

Зокрема, потребують подальшого розвитку правові механізми протидії гібридним загрозам в інформаційній сфері, забезпечення стійкості критичної інформаційної інфраструктури, підвищення спроможностей правоохоронних органів та спецслужб щодо виявлення, запобігання та нейтралізації кіберзагроз. Важливим також є вдосконалення правових засад міжнародного співробітництва у сфері забезпечення кібербезпеки, особливо в умовах транскордонного характеру сучасних інформаційних загроз.

Окремої уваги заслуговує питання правового забезпечення інформаційної безпеки Збройних Сил України та інших військових формувань. В умовах триваючої російської агресії надзвичайно важливим є надійне функціонування систем управління та зв'язку військ, захист інформаційних ресурсів оборонного значення від кібератак противника. Це вимагає подальшого розвитку нормативно-правової бази у цій специфічній сфері.

Зокрема, доцільним є розроблення окремого законодавчого акту, який би комплексно врегулював питання забезпечення інформаційної безпеки Збройних Сил України, визначив повноваження Міністерства оборони, Генерального штабу та інших органів військового управління щодо захисту інформації та протидії кіберзагрозам у військовій сфері. Потребує вдосконалення й підзаконна нормативна база, що регламентує порядок функціонування систем зв'язку та інформаційних систем військового призначення, забезпечення їх кіберзахисту.

Також необхідним є налагодження ефективної взаємодії між суб'єктами забезпечення кібербезпеки України – як на рівні нормативно-правового регулювання, так і в практичній площині. Йдеться про чіткий розподіл завдань та повноважень, узгодження планів і порядку спільних дій на випадок кібератак та інцидентів, проведення спільних навчань і тренувань. Це дозволить суттєво підвищити загальний рівень захищеності держави в кіберпросторі, мінімізувати ризики для систем управління та критичної інформаційної інфраструктури.

Проведений аналіз засвідчив вагому роль правового забезпечення інформаційної безпеки, інформатизації та зв'язку в електромагнітному середовищі та кіберпросторі як важливої складової виконання завдань підрозділами Сил оборони і безпеки України. Ефективна нормативно-правова база у цій сфері є необхідною передумовою забезпечення стійкості держави до інформаційних загроз, безперебійного функціонування систем управління та зв'язку в умовах протидії гібридній агресії.

Водночас існуюче законодавство потребує постійного вдосконалення з урахуванням стрімкого розвитку інформаційних технологій та появи нових викликів і загроз. Подальші зусилля мають бути спрямовані на розвиток правових механізмів протидії гібридним загрозам, забезпечення надійного захисту критичної інформаційної інфраструктури та інформаційних систем військового призначення, вдосконалення міжнародно-правової бази співробітництва у сфері забезпечення кібербезпеки.

Особлива увага має бути приділена питанням правового забезпечення інформаційної безпеки Збройних Сил України та інших складових сектору безпеки і оборони України. Доцільною є розробка спеціального законодавства в цій сфері та удосконалення механізмів міжвідомчої взаємодії щодо протидії інформаційним та кіберзагрозам. Це дозволить суттєво підвищити загальний рівень обороноздатності держави в умовах триваючої «гібридної» війни.

Водночас вдосконалення правової бази повинно поєднуватися з розвитком організаційного та ресурсного забезпечення системи інформаційної безпеки, підвищенням кваліфікації особового складу, проведенням активної роз'яснювальної роботи серед громадян щодо безпечної поведінки в інформаційному просторі. Лише комплексний підхід дозволить забезпечити надійну інформаційну безпеку України як важливу складову її національної безпеки.

ЛІТЕРАТУРА

1. Баран М.В. Адміністративно-правове забезпечення інформаційної безпеки в Україні: дисертація на здобуття ступеня доктора філософії за спеціальністю 081 «Право» / Львівський державний університет внутрішніх справ. Львів. 2022. 242 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/5076/1/baran_d.pdf.

2. Бєлов Д., Громовчук М. Правовий простір держави: конституційно-правовий аспект. *Науковий вісник Ужгородського національного університету. Серія Право*. 2021. Випуск 66. С. 46–50.

3. Бєлов Д.М., Белова М.В. Система захисту прав і свобод людини і громадянина: доктринальні та нормативні основи. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2022. Вип. 74. С. 85–90.

4. Денисюк Ж.З., Яковлєв О.В. Формування інформаційної культури суспільства в умовах цифровізації. *Вісник Національної академії керівних кадрів культури і мистецтв*. № 2. 2021. С. 18–22.

5. Дзьобань О., Данильян О. Права і свободи людини: інформаційний вимір. *Вісник Національного юридичного університету імені Ярослава Мудрого*. № 3 (58). *Серія: філософія, філософія права, політологія, соціологія*. 2023. С. 6–22.

6. Захаренко К.В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири: дисертація на здобуття наукового ступеня доктора політичних наук за спеціальністю 23.00.02 «Політичні інститути та процеси» / Національний педагогічний університет імені М. Драгоманова, Львівський національний університет імені Івана Франка. Львів. 2021. 423 с. URL: https://lnu.edu.ua/wp-content/uploads/2021/04/dis_zakharenko.pdf.

7. Квіткін П.В., Дятлова І.В., Петрова Л.О. Інформаційна безпека особистості: теоретико-методологічний аналіз. *Вісник Національного юридичного університету імені Ярослава Мудрого*. № 4 (51). *Серія: філософія, філософія права, політологія, соціологія*. 2021. С. 46–62.

8. Мельничук В., Горохова Л. Критичне мислення як складова інформаційної безпеки. *Вісник* Львівського університету. Випуск 29. Серія філософські науки. 2022. С. 7–13.

9. Тихомиров О. Ідея інформаційної гігієни в контексті інформаційної безпеки і захисту інформаційних прав людини. *Науковий юридичний журнал «Правові новели»*. № 20. 2023. С. 59–65. URL: http://legalnovels.in.ua/journal/20_2023/8.pdf.

10. Хитра О.Л. Інформаційна безпека людини як базова аксіологічна константа. *Modern information technologies and their implementation in the processes of social and technical project management.* Abstracts of IV International Scientific and Practical Conference. Boston. USA. 17–18 February 2020. P. 150–153. URL: https://isg-konf.com/wp-content/uploads/2020/02/IV-Conference-BostonUSA.pdf#page=151.

11. Byelov D., Novak O. Communal property disposal: actual issues. *Visegrad Journal on Human Rights.* Issue 1. 2022. P. 33–39.

12. Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science*, Engineering and Technology. 2022. P. 1–7.

13. Yuchong Li, Qinghui Liu. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 7. 2021. P. 1–11.