УДК 342.7
DOI https://doi.org/10.32689/2617-9660-2022-6(24)-16-20

Капля Олександр Миколайович,
доктор юридичних наук, старший науковий співробітник, професор кафедри правових дисциплін Одеського інституту Міжрегіональної академії управління персоналом, вулиця Чорноморського Козацтва, 19, Одеса, Одеська область, 65000

ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ГРОМАДЯНИНА ПІД ЧАС ДІЇ ВОЄННОГО СТАНУ

Анотація. *У статті досліджено основні юридичні загрози та ризики інформаційної безпеки громадян. Встановлено нормативно-правові механізми управління рівнем інформаційної безпеки суспільства у період воєнного стану та в мирний час. Проведено порівняння дії відповідних механізмів, що дозволило провести порівняння адміністративно-правових ризиків в залежності від умов (воєнного, або мирного часу). Визначено суб'єктів забезпечення інформаційної безпеки громадянського суспільства, а також нормативно-правові положення, що регламентують їх діяльність. Проведено дослідження способів мінімізації негативних інформаційних впливів, зокрема: розглянуто юридичний захист прав і свобод використання інформації; адміністративно-правовий захист інформаційних потреб громадян та їх інтересів в інформаційному просторі територіальними та відомчими органами безпеки; адміністративно-правовий захист професійної, особистої та сімейної таємниці з використанням технічних засобів захисту. Дослідження проведено з метою вдосконалення чинних правових норм, спрямованих на захист прав громадянин на свободу слова, захист персональних даних, та власних інформаційних потреб, що визначені Законами України: «Про інформацію», «Про захист персональних даних», «Про захист інформації в інформаційно-комунікаційних системах», «Про звернення громадян», «Про доступ до публічної інформації» в умовах воєнного стану. Проведено дослідження ризиків та загроз у сфері інформаційної безпеки у кіберпросторі, що дозволило виявити важливі напрями вдосконалення діючих норм закону під час дії воєнного стану. Проаналізовано дію нормативних механізмів захисту персональних даних у військовий час.*

Ключові слова: *інформаційна безпека, громадяни, право, захист, закон, воєнний стан.*

Kaplia Oleksandr Mykolayovych,
Doctor of Legal Sciences, Senior Researcher, Professor of the Department of Legal Disciplines of the Odessa Institute of the Interregional Academy of Personnel Management, Chornomorskoho Kozatstva str., 19, Odesa, Odeska oblast, 65000

LEGAL REGULATION OF CITIZEN'S INFORMATION SECURITY DURING MARTIAL LAW

Abstract. *The article examines the main legal threats and risks of citizens' information security. Regulatory and legal mechanisms for managing the level of information security of society during martial law and peacetime have been established. A comparison of the action of the relevant mechanisms was carried out, which made it possible to compare the administrative and legal risks depending on the conditions (wartime or peacetime). The subjects of ensuring information security of civil society, as well as the normative and legal provisions regulating their activities, have been determined. A study of ways to minimize negative information impacts was conducted, in particular: legal protection of the rights and freedoms of information use was considered; administrative and legal protection of information needs of citizens and their interests in the information space by territorial and departmental security bodies; administrative and legal protection of professional, personal and family secrets using technical means of protection. The study was conducted with the aim of improving the current legal norms aimed at protecting the rights of citizens to freedom of speech, protection of personal data, and their own information needs, which are defined by the Laws of Ukraine: «On Information», «On Protection of Personal Data», «On Protection of Information in Information -communication systems», «On citizens' appeals», «On access to public information» under martial law. A study of risks and threats in the field of information security in cyberspace was conducted, which made it possible to identify important areas of improvement of the current legal norms during martial law. The effect of regulatory mechanisms of personal data protection in wartime is analyzed.*

Key words: *information security, citizens, law, protection, law, martial law.*

Постановка проблеми та її зв'язок з науковими та практичними завданнями. В умовах воєнного стану захист суспільства від деструктивного інформаційного впливу з боку держави агресора та ряду терористичних організацій, які задіяні в процесі дестабілізації нашої країни, а також від інших негативних інформаційних факторів, які руйнують вітчизняний інформаційний простір, необхідно уточнити форми та методи забезпечення інформаційної безпеки громадян. Значна кількість загроз інформаційної безпеки обумовлюють наступні ризики: ризик застосування інформаційних технологій та механізмів реалізації ворожих актів агресії проти громадян; незаконне застосування інформаційних ресурсів іншої держави; неправомірна діяльність в інформаційному просторі з метою дестабілізації суспільства; використання інформаційної інфраструктури для поширення інформації, що розпалює міжрасову та міжнаціональну ворожнечу, а також ідеї та теорії, що підбурюють до ненависті, дискримінації, або насильства; маніпулювання інформацією з метою спотворення сталих моральних, етичних та культурних цінностей. Відповідна проблема потребує нових шляхів вирішення, які пов'язані із розробкою потрібних організаційних, правових, а також технологічних засобів аналізу, пошуку, поширення, зберігання та використання інформації у всіх сферах життєдіяльності суспільства. Зокрема необхідність створення територіально-розподілених сховищ інформаційних ресурсів, які проходять низку державних перевірок, створення державних та комп'ютерних мереж, телекомунікаційних мереж та систем спеціального призначення та загального користування, окремих ліній зв'язку, захищених каналів передачі даних, спеціальних засобів управління інформаційними потоками. Такі заходи мають бути регламентовані та контролюватись на законодавчому рівні. Негативні явища інформаційного характеру у воєнний час, можна вважати такими, що ставлять під загрозу основні принци забезпечення безпеки громадян, в основі яких лежать чинні принципи та норми права на міжнародному рівні. Тому, основним завданням державної політики, пов'язаної із забезпеченням безпеки в інформаційній сфері є створення умов для надання кожному громадянину права на інформаційну безпеку.

Огляд літературних джерел. Під час дії воєнного стану, мета якого полягає в концентрації суспільства для головної мети подолання ворога, першочерговим завдання для суспільства є забезпечення безпеки країни на усіх її рівнях. Це пов'язано з тим, що саме поняття інформаційної безпеки громадянина можна розглядати в сукупності із національною, державно та суспільною інформаційної безпекою. Відповідну класифікацію запропоновано в роботі Золотар О.О. [1], де основоположну роль відіграє саме інформаційна безпека людини. Зміст ряду статей Конституції України (50, 31, 34, 32) вказує на гарантії права на поширення усної інформації, захисту від поширення не достовірної інформації, захист від втручання в приватне життя таємницю листування, кореспонденцію, можливість судового захисту права на спростовувати не досвідну інформацію, а також вимагати її вилучення, права на доступ до публічної інформації [2]. Зважаючи на те, що норми головного документа нашої країни гарантують належне забезпечення інформаційної безпеки громадянського суспільства, саме поняття інформаційної безпеки громадянина, або людини не знаходить належної уваги в інших нормативно правових документах, що спричинило безсистемність національного законодавства у сфері інформаційної безпеки людини, як особистості. Наразі, основні його положення належать до інформаційної безпеки держави та суспільства загалом. Вирішити проблему виокремлення категорії інформаційної безпеки громадянина намагався дослідник із Вінницького національного аграрного університету Правдюк Л.А., розкривши це поняття, як стан захищеності особистості від інформаційних загроз, ризиків та небезпек [3]. В деяких працях інформаційна безпека громадянина розглядається, в системі забезпечення інформаційної безпеки держави [4]. Існують спроби провести класифікацію видів інформаційної безпеки, де розділяють три класифікаційних види інформаційної безпеки: інформаційна безпека громадянина, інформаційна безпека суспільства, інформаційна безпека держави [1 5]. Значну кількість праць присвячено інформаційній безпеці держави під час воєнного стану [6, 7, 8], проте окремі питання забезпечення інформаційної безпеки громадянина в цей період висвітлено дуже мало.

Вимагає юридичного уточнення ступінь обмеження прав та законних інтересів громадян в інформаційній сфері під час воєнного стану, які передбачені ч. 1 ст. 8 Закону України «Про правовий режим воєнного стану» [2]. Також існує потреба в уточненні видів персональної інформації громадян в період воєнного стану, викликана необхідністю виявлення ворожих агентів. Усе це та багато інших, не врегульованих правових аспектів, пов'язаних із відсутністю чіт-

кого визначення проблем пов'язаних із інформаційною безпекою громадян в період воєнного стану, потребує деталізації як нормативної, так і законодавчої бази. Тому, відповідну проблему можна вирішити шляхом внесення змін до чинних законодавчих актів, які забезпечать конструктивну реалізацію конституційних засад інформаційної безпеки громадянського суспільства, як в мирний, так і в воєнний час.

Цілі дослідження. Дослідити можливості уточнення стану захищеності громадянина від загроз, ризиків та небезпек інформаційного характеру у воєнний час та визначити дієві нормативні-правові механізми мінімізації інформаційних загроз для громадян в цей період.

Виклад основного матеріалу.

Під системою інформаційної безпеки країни зазвичай розуміють об'єднання органів державної влади, які виконують свої задачі на основі закону, в умовах постійного контролю судової влади. Метою відповідної системи є: діагностика та прогнозування інформаційних загроз та ризиків, що впливають на стан життєво важливих інтересів суспільства; реалізація ряду довготривалих заходів, які спрямовані на попередження відповідних загроз; підтримка готовності до забезпечення інформаційної безпеки.

Виокремлення інформаційної безпеки громадянина із цієї системи у відповідності до норм конституції, та низки нормативних документів, вимагає більш деталізованих підходів. Так, у відповідності до Закону України «Про основи національної безпеки України» запропоновано безпеку усіх трьох складових інформації безпеки: держави, українського суспільства та окремих його членів. Це зазначено в нормах ст. 3 відповідного закону, де визначено основних об'єктів інформаційної безпеки. До таких віднесено громадян, державу та суспільство. В таблиці 1 приведено їх детальна класифікація.

З огляду на норми конституції та ряду законодавчих актів, інформаційна безпека громадянина розглядається в широкому розумінні і охоплює практично всі аспекти діяльності держави. Тому й залишається відкритою проблема юридичної конкретизації інформаційної безпеки громадянина. Зважаючи на те, що основною конституційної нормою є захист національної безпеки держави(ст. 17), деталізація цього поняття була встановлена у 2021 р., під час розробки «Стратегії національної безпеки України», де було введено поняття «інформаційна загроза», що визначається, як потенційне, або реально негативне явище, що впливає на людину, суспільство та державу [10]. Загалом закон передбачає шляхи деталізації окремої юридичної категорії, що описує стан інформаційної захищеності громадян. Для цього потрібно на законодавчому рівні урівноважити баланс інтересів особистості, суспільства та держави. За умови взаємної відповідальності цих суб'єктів, можна говорити про окремі принципи забезпечення інформаційної безпеки громадянина не лише в мирний час, а й під час військового стану. Такий підхід дозволить сформувати комплексну систему нормативних, соціальних, організаційних, економічних та політичних механізмів захисту громадян в інформаційній сфері, спрямованих на подолання існуючих розмитих категорій інформаційної безпеки окремої людини, як явища що характеризує її стан інформаційної захищеності.

Разом з тим, застосування конституційних норм в інформаційній сфері громадянина не можуть діяти повною мірою у воєнний час, оскільки пріоритети в протидії загроз схиляються до захисту саме держави, її територіальної цілісності, незалежності та забезпечення інтересів. Таким чином, інформаційна безпека громадянина у воєнний час обумовлена специфічними обставинами. З одного боку громадянам надається право захищати країну у будь-який спосіб, але при цьому здійснюються заходи правового режиму воєнного стану, що регламентує ст. 8 Закону України «Про правовий режим воєнного стану». Окремі норми цього закону можуть обмежувати конституційні права, пов'язані із інформаційною безпекою громадян. Так, наприклад ст. 31 Конституції України передба-

Таблиця 1

Класифікація об'єктів інформаційної безпеки у відповідності до ст. 3 Закону України «Про основи національної безпеки України»

Об'єкти інформаційної безпеки	Елементи
громадяни	права та свободи, що гарантуються Конституцією;
суспільство	природні ресурси, матеріальні цінності, інтелектуальні здобутки, культурні та історичні надбання, інформаційне, а також навколишнє середовище
держава	територіальна цілісність, конституційний лад, суверенітет та недоторканність

Джерело: розроблено автором на основі [1]

чає гарантії таємниці листування, телефонних розмов та інших комунікацій, ст. 32 стосується невтручання в особисте і сімейне життя, крім випадків, передбачених Конституцією України, ст. 34 стосується права на свободу думки і слова, на вільне вираження своїх поглядів і переконань, ст. 41, гарантує право на розпорядження власністю, результатами інтелектуальної та творчої діяльності. Можна перераховувати й інші конституційні права, що стосуються інформаційної безпеки громадян, які у воєнний час можуть не діяти, оскільки під час війни надання переваги інтересам держави дозволить краще забезпечити основоположні права усіх громадян шляхом підтримання безпеки держави. Окремим питанням слід виділити загрози кібербезпеки громадян у воєнний час, оскільки сучасні війни проходять не лише на землі та в повітрі, а й в інформаційній сфері, зокрема у кіберпросторі. В той час, коли бойові дії точаться на полі бою і основні атаки ворога приймають на себе військові та силові структури, питання кібербезпеки безпосередньо стосується кожного громадянина, який має доступ до цифрових технологій, які під'єднані до глобальної мережі. Так, 24 лютого 2022 року в Україні об'єктами атак стали також цивільні ресурси та звичайні громадяни. Агресор шляхом дестабілізації населення, використовуючи різні інформаційні засоби намагався посіяти штучну паніку. Шляхом створення підробних сторінок в мережі, кібератак провідних українських сервісів онлайн – телебачення, створення штучного навантаження на мережі мобільних операторів, здійснення спроб отримати доступ до поштових сервісів державних служб з метою розповсюдження інформації дискредитуючого характеру та інших протиправних дій ворог створив загрозу для інформаційної безпеки громадян. З огляду на ряд нормативних положень, що регламентують безпеку громадян у кіберпросторі [11], [12],слід звернути увагу та те, що вони були розроблені в період мирного часу. Крім того, в період воєнного часу кіберзлочинці, що знаходяться на території нашої країни, можуть нанести шкоду набагато більшу, а ніж у мирний час, дестабілізувавши мирне населення, спричинивши збитки економіці, яка працює на перемогу у війні. У зв'язку з цим у перші місяці війни в Україні було оптимізовано кримінально-процесуальне законодавство, шляхом вдосконалення механізмів притягнення до відповідальності кіберзлочинців. Загалом після 2014 р. ситуація в галузі кібербезпеки зазнала значних зрушень. Так, у 2019 р. було представлено законодавчу базу у сфері кібербезпеки [13] в рамках якої розроблено Доктрину інформаційної безпеки України, яка була ведена в дію Законом України «Про основні засади забезпечення кібербезпеки України». Закон дозволяє уточнити основні об'єкти кіберзахисту. До таких віднесено критичну інфраструктуру країни, органи державної влади та громадян. Законом визначено відповідальність за порушення законодавства у цій сфері, а також засоби контролю законності заходів щодо забезпечення кібербезпеки. Дія даного закону у військовий час значно розширює повноваження органів державної влади та збільшує відповідальність за його порушення. Це пов'язано з тим, що закон спрямований на забезпечення ефективного застосування Збройних Сил України для належної відповіді кіберзагрозам в системі державної безпеки. Так, інформаційна безпека громадянина у воєнний час може розглядатися, як такий стан захищеності, при якому основні кібернетичні загрози та ризики спрямовані на державні інституції зокрема та національну безпеку загалом. Роль особистої інформаційної безпеки, яка виражена рядом конституційних норм, таких, як свобода пересування, право на отримання інформації, свобода висловлювань, обмежуються в цей період. Отже, інформаційна безпека громадян не зникає, а лише змінює правила поведінки органів державного управління з урахуванням воєнних реалій. Переважна більшість таких реалій стосується окремих інформаційних правовідносин щодо заборони поширення певної інформації, яка носить суспільно-небезпечних характер. Інша частина обмежує доступ до певних інформаційних ресурсів, деякі права на інформаційну діяльність в галузі обробки інформації також обмежуються. В таких умовах інформаційна безпека громадянина значною мірою трансформується, вона спрямована більше не на захищеність окремих його прав, як особистості, а на загальний захист інтересів суспільства.

Висновок. Інформаційна безпека громадянин закріплена в низці нормативних документів та є конституційною нормою. Проте, це поняття не достатньо деталізовано та законодавчо врегульовано та потребує його виокремлення із таких категорій, як інформаційна безпека держави, інформаційна безпека суспільства, національна безпека. Для вирішення цієї проблеми потрібні зміни в деяких законодавчих актах, з метою забезпечення ефективної реалізації конституційних засад інформаційної безпеки держави, суспільства та громадянина, як окремих категорій. Стан інформаційної безпеки громадянина

у воєнний час, суттєво відрізняється від мирного часу, оскільки пріоритети в протидії загроз більше спрямовані до захисту саме держави, її територіальної цілісності та незалежності в цей період.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Золотар О.О. Класифікація інформаційної безпеки. *Інформація і право*. 2011. № 2(2). С. 109-113.
2. Конституція України. Верховна Рада України. Офіційний сайт. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 04.10.2022).
3. Правдюк А. Л. Конституційні гарантії інформаційної безпеки людини і громадянина. Юридичний науковий електронний журнал. 2021.№ 12. С. 303-305.
4. Сащук, Г. Інформаційна безпека в системі забезпечення національної безпеки. Режим доступу: http://journ. univ. kiev. ua/trk/publikacii/satshuk_publ. php, 2014.
5. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
6. Богданович, В. Ю.; воровиич, Б. О.; марко, Є. І. Інформаційна безпека як основа воєнної безпеки держави та суспільства. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, 2018, 3: 44-48.
6. Залєвська І.І., Удренас Г.І. Інформаційна безпека України в умовах російської військової агресії. Південноукраїнський правничий часопис. 2022. № 1-2. С. 20 – 26.
7. Запорожець, С. А. Стан забезпечення інформаційної безпеки України у воєнній сфері в умовах гібридної війни. Politology bulletin, 2019, 83: 16-25.
8. ЗАКОН УКРАЇНИ Про основи національної безпеки України (Відомості Верховної Ради України (ВВР), 2003, № 39, ст.351), режим доступу: https://zakon.rada.gov.ua/laws/show/964-15#Text
9. Стратегія національної безпеки України. URL: https://zakon.rada.gov.ua/laws/show/392/2020?find=1&text=%D0%BE%D1%82%D1%80%D0%B8%D0%BC%D0%B0%D0%BD%D0%BD%D1%8F+%D1%83%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B6%D1%83#w2_1 (дата звернення 10.10.2022)
10. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», url: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 18.10.22)
11. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403), url: https://zakon.rada.gov.ua/laws/show/2163-19#Text
12. О.Г. Трофименко Законодавча база забезпечення кібербезпеки держави. Кібербезпека в Україні: правові та організаційні питання: матер. II всеукр. наук.-практ. конф., 17 листопада 2017 р., Одеса: ОДУВС, С. 55–56.

REFERENCES:

1. Zolotar O.O. Klasyfikatsiia informatsiinoi bezpeky. Informatsiia i pravo. 2011. № 2(2). S. 109-113.
2. Konstytutsiia Ukrainy. Verkhovna Rada Ukrainy. Ofitsiinyi sait. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (data zvernennia: 04.10.2022).
3. Pravdiuk A. L. Konstytutsiini harantii informatsiinoi bezpeky liudyny i hromadianyna. Yurydychnyi naukovyi elektronnyi zhurnal. 2021.№ 12. S. 303-305.
4. Sashchuk, H. Informatsiina bezpeka v systemi zabezpechennia natsionalnoi bezpeky. Rezhym dostupu: http://journ. univ. kiev. ua/trk/publikacii/satshuk_publ. php, 2014.
5. Zolotar O.O. Informatsiina bezpeka liudyny: teoriia i praktyka: monohrafiia. Kyiv : TOV «Vydavnychyi dim «ArtEk», 2018. 446 s.
6. Bohdanovych, V. Yu.; vorovyych, B. O.; marko, Ye. I. Informatsiina bezpeka yak osnova voiennoi bezpeky derzhavy ta suspilstva. Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy imeni Ivana Cherniakhovskoho, 2018, 3: 44-48.
6. Zalievska I.I., Udrenas H.I. Informatsiina bezpeka Ukrainy v umovakh rosiiskoi viiskovoi ahresii. Pivdennoukrainskyi pravnychyi chasopys. 2022. № 1-2. S. 20 – 26.
7. Zaporozhets, S. A. Stan zabezpechennia informatsiinoi bezpeky Ukrainy u voiennii sferi v umovakh hibrydnoi viiny. Politology bulletin, 2019, 83: 16-25.
8. ZAKON UKRAINY Pro osnovy natsionalnoi bezpeky Ukrainy (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 2003, № 39, st.351), rezhym dostupu: https://zakon.rada.gov.ua/laws/show/964-15#Text
9. Stratehiia natsionalnoi bezpeky Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/392/2020?find=1&text=%D0%BE%D1%82%D1%80%D0%B8%D0%BC%D0%B0%D0%BD%D0%BD%D1%8F+%D1%83%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B6%D1%83#w2_1 (data zvernennia 10.10.2022)
10. Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku “Pro Stratehiiu kiberbezpeky Ukrainy”, url: https://zakon.rada.gov.ua/laws/show/447/2021#Text (data zvernennia 18.10.22)
11. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» (Vidomosti Verkhovnoi Rady (VVR), 2017, № 45, st.403), url: https://zakon.rada.gov.ua/laws/show/2163-19#Text
12. O.H. Trofymenko Zakonodavcha baza zabezpechennia kiberbezpeky derzhavy. Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia: mater. II vseukr. nauk.-prakt. konf., 17 lystopada 2017 r., Odesa: ODUVS, S. 55–56.