УДК 342.9
DOI https://doi.org/10.32840/1813-338X-2023.2.31

А. І. Русакевич
аспірант кафедри цивільного, господарського та екологічного права
ННІ гуманітарних та соціальних наук Національного технічного університету
«Дніпровська політехніка»

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ У АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ГРОМАДЯН

У сучасній військовій реальності важко, навіть недоречно, заперечувати роль інформації як інструменту протистояння і, по суті, як зброї. Інформація дозволяє вигравати війни без жодного пострілу, створюючи та розпалюючи внутрішні протиріччя. Така тактика характерна для нової гібридної війни, в якій військовий елемент є лише однією зі складових цілого. Саме тому в умовах прямого військового конфлікту розвідка є стратегічним інструментом перемоги. Якісна національна розвідувальна політика сприяє тактичній, оперативній та стратегічній перемозі. Сьогодні, коли майже кожен є джерелом інформації і може керувати громадською думкою, інформація, що поширюється, не завжди відповідає потребам, які диктує національна безпека. Метою цієї статті є визначення аспектів забезпечення інформаційних прав і свобод з урахуванням захисту інформаційної безпеки держави в умовах воєнного стану. Автор визначає пріоритетні напрями захисту та їх вплив на права і свободи людини і громадянина. Автори наголошують на комплексному характері питання забезпечення інформаційної безпеки, яке включає три фундаментальні елементи: правовий, політичний та технічний. Важливим є також висновок про те, що забезпечення інформаційної безпеки – це питання одночасного створення механізмів, які дозволять максимально ефективно виконувати поставлені завдання в умовах інформаційних обмежень та сприятимуть захисту прав і свобод громадян. Забезпечення інформаційної безпеки в Україні є основним напрямом державної політики, від якого залежить національна безпека та соціально-економічний розвиток. Ефективні механізми захисту інформаційної безпеки в Україні полягають у створенні відповідної правової системи, що регулює відносини, які виникають в інформаційній сфері, та узгоджених діях суб'єктів на всіх рівнях щодо забезпечення інформаційної безпеки в Україні. У статті проаналізовано актуальні проблеми інформаційної безпеки, які перешкоджають сталому розвитку інформаційно-комунікаційних технологій в умовах воєнного стану та бойових дій на території України.

Ключові слова: *безпека, інформаційна безпека, інформаційний захист, загрози, інформаційна політика, тимчасове призупинення норм, кіберзагроза, технічні можливості, оборона, військовий стан, протидія ворожій інформації.*

Постановка проблеми. У сучасній реальності війна це більше про гібридність та інформацію, ніж про зброю, оперативно-тактичний конфлікт і перемогу. Гібридні конфлікти включають в себе різні елементи, в тому числі розвідку, яка іноді є більш важливою, ніж військові елементи. Володіння зброєю масового знищення не гарантує державі перемогу, якщо вона не має інформаційної переваги. Така перевага створюється системою заходів, яка переводить інформаційну безпеку держави у воєнний стан. Важливість безпеки у праві важко переоцінити. Зокрема, реалізація права на життя, безсумнівно, пов'язана з правом на безпеку. У саме поняття «безпека» ми вкладаємо захист державою нас самих і того, що нам належить, від посягань інших осіб. Сучасні технології, інтернет, мобільний зв'язок та використання різних систем комунікації не лише забезпечують зручність, але й роблять всю систему безпеки вразливою до атак. Створюються передумови для витоку інформації, з'являється можливість технологічного впливу для формування бажаної громадської думки, а також можливість фіксації та передачі стратегічної інформації противнику за допомогою незначних технологічних зусиль. Втрата юрисдикції над окремими частинами України та прямі загрози існуванню Української

держави та її народу часто унеможливлюють реалізацію прав, гарантованих Конституцією. Саме тому указом Президента України № 64/2022 тимчасово, на період дії правового режиму воєнного стану, можуть обмежуватися конституційні права і свободи людини і громадянина, передбачені статтями 30–34, 38, 39, 41–44, 53 Конституції України, а також вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану». Окрему і вагому групу у цих обмеженнях становлять інформаційні права та свободи людини і громадянина.

Стан наукової розробки проблеми. Права людини в умовах інформаційного суспільства та безпеки досліджували такі зарубіжні та вітчизняні вчені, як І. Браун, В. Дрейк, Р. Йоргенсен, Д. Лайон, Л. Лессіг, К. Расерока. Проблеми забезпечення інформаційної безпеки покладені в основу досліджень В. Гурковського, В. Копилова, Б. Кормича, В. Настюка, М. Швеця, А. Селіванова. Сутність, класифікація та ефективність застосування інформаційних прав в Україні є у сфері наукових інтересів також вітчизняних вчених серед яких І. В. Арістова, Р. А. Калюжний, Б. А. Кормич, Т. А. Костецька, А. І. Марущак та багато інших авторів. Отже забезпечення та розвиток прав людини в умовах інформаційного суспільства були і є найважливішим предметом дослідження як вітчизняних, так і закордонних науковців та авторів праць.

Метою наукової статті є дослідження формування правових засад інформаційної безпеки України в умовах війни у системі національної безпеки щодо їх впливу на інформаційні права людини та суспільства в цілому, а також протидія ворожій дезінформації в умовах військового стану.

Виклад основного матеріалу. Захист національної безпеки визначається Конституцією України як найважливіша функція держави (ст. 17). В Україні з 1997 року приймаються концепції (документи, які визначають стратегічний розвиток) національної безпеки, у яких приділяється увага інформаційній безпеці. Їх ключова мета спрямована на розбудову напрямків політики національної безпеки, протидію інформаційній експансії іноземних держав. Очевидно, одна з причин виключно формального характеру та практичного незастосування Концепцій полягала у відсутності конкретизацій джерел інформаційних загроз для України, оцінки геополітичної обстановки й формування засобів інформаційної протидії [2].

У 2020 році була прийнята нова редакція Стратегії національної безпеки України з підзаголовком «Безпека людини – національна безпека». Відповідно до неї, пріоритетами національної безпеки є захист особи, суспільства і держави від злочинів, у тому числі корупційних, поновлення порушених прав та забезпечення відшкодування завданих збитків; посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі; зміцнення дипломатичного та інформаційно-пропагандистського потенціалу держави. Одним з основних напрямів внутрішньополітичної діяльності є забезпечення національних інтересів і безпеки та доступ до повної і достовірної попередньої інформації [3].

У 2021 році прийнята нова Стратегія інформаційної безпеки (далі Стратегія), яка передбачає комплексну взаємодію на основі Конституції України, законодавства України, Стратегії національної безпеки України, затвердженої тако ж стратегії кібербезпеки України та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України. Було передбачено наступне інформування: потенційні інформаційні загрози вже визначені: «Інформаційна політика Російської Федерації є загрозою не лише для України, а й для інших демократичних держав».

Стратегія визначає поняття «інформаційна безпека» як невід'ємну складову національної безпеки України, тобто стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших життєво важливих інтересів особи, суспільства і держави, за якого забезпечуються конституційні права і свободи людини і громадянина на збирання, зберігання, використання та поширення інформації. Стратегія визначає як держава, яка належним чином забезпечує доступ до достовірної та об'єктивної інформації та існування ефективної системи захисту і протидії заподіянню шкоди правам і свободам людини і громадянина. Таким чином, згідно з визначенням, одним з елементів інформаційної безпеки є стан захищеності демократичного устрою, що сприяє забезпеченню конституційних прав і свобод особистості та людей у державі.

Стратегія визначає поняття «інформаційна загроза» як потенційне або реальне негативне явище, тенденція чи чинник інформаційного впливу на особу, суспільство і державу, що застосовується в інформаційній сфері з метою перешкоджання чи ускладнення реалізації національних інтересів України, утвердження національних цінностей і може завдати прямої чи опосередкованої шкоди державним інтересам, національній безпеці та обороні [4].

Очевидно, що у воєнний час акцент на виявленні загроз та реагуванні на них змістився з необхідності забезпечення впливу на потенційні та існуючі загрози до звуження прав людини заради збереження держави.

Так, у зв'язку із введенням в Україні воєнного стану тимчасово, на період дії правового режиму воєнного стану, вводяться тимчасові обмеження прав і законних інтересів юридичних осіб в межах та обсязі, що необхідні для забезпечення можливості запровадження та здійснення заходів правового режиму воєнного стану, які передбачені частиною першою статті 8 Закону України «Про правовий режим воєнного стану».

З моменту оголошення воєнного стану до регуляторних законів були внесені зміни, які враховують реалії війни. Вони стосуються регулювання окремих аспектів інформаційних відносин щодо заборони поширення певної інформації суспільно небезпечного характеру, врегулювання важливих аспектів технічної фіксації інформації в умовах воєнного стану та війни, встановлення або посилення відповідальності за поширення певної інформації та регулювання процесуальних заходів щодо вилучення розвідувальних даних [1].

Так, Верховна Рада ухвалила законопроєкт про кримінальну відповідальність за незаконну фото та відеозйомку переміщення ЗСУ та міжнародної військової допомоги під час воєнного стану.

У п'ятницю, 31 березня 2023 року, набув чинності Закон України «Про медіа», який Верховна Рада ухвалила 13 грудня 2022 року. Слід зауважити що прийняття закону про «Медіа» було однієї з вимог для вступу України до ЄС. Новий закон значно розширює повноваження Національної ради з питань телебачення і радіомовлення. Зокрема, регулятор реєструватиме онлайн-медіа та друковані ЗМІ. Цей закон також запроваджує новий тип відносин між ЗМІ та державним регулятором на українському медіаринку – співрегулювання. Метою співрегулювання є забезпечення участі суб'єктів медійної діяльності у формулюванні та визначенні вимог до змісту інформації, а також запобігання цензурі та зловживанню свободою слова.

Одним з найважливіших нововведень є створення національного регулятора медіаринку їм стає Національна рада України з питань телебачення і радіомовлення (Нацрада). Згідно з новим законом, Національна рада тепер контролює радіо і телебачення, а також друковані та інтернет-ЗМІ. Відтепер Нацрада матиме право накладати санкції на ЗМІ і навіть втручатися в їхню діяльність, що раніше можна було зробити лише через суд.

Новий закон також передбачає накопичувальну систему правопорушень проти певних ЗМІ. За словами Микити Потураєва, голови Комітету Верховної Ради з питань гуманітарної та інформаційної політики, запроваджено механізм припису. Це означає, що Нацрада повідомляє ЗМІ про виявлені в його роботі порушення і просить їх виправити. Приписи не фіксуються в особових справах, але фіксується кількість порушень [5].

Висновки. Сьогоднішня військова реальність чітко демонструє, що інформація є «зброєю масового знищення». Тому існує потреба у забезпеченні національної інформаційної безпеки та дотриманні прав людини, водночас створюючи ефективні механізми, які дозволять людям уникнути наслідків порушень їх свободи та демократії. Найбільша цінність українців полягає в розумінні та сприйнятті понять свободи та справедливості. Це те, за що вони зараз ризикують своїм життям і за що платять велику ціну. Для того, щоб побудувати ефективну систему інформаційної безпеки, важливо, щоб вона базувалася на трьох логічних елементах, які складають механізми системи:

1) технічна, тобто створення і функціонування всіх необхідних технічних складових систем;

2) політична державна політика повинна бути спрямована на забезпечення інформаційної безпеки;

3) правова оформлення всіх пов'язаних елементів у якісні нормативно-правові акти.

Слід розуміти, що у воєнний час держави часто об'єктивно не в змозі гарантувати права людини в повному обсязі. Однак, захищаючи базові принципи через політико-правову взаємодію механізмів інформаційної безпеки,

основи демократії та система загальних принципів права захищені від руйнування спонтанними рішеннями. Якщо стіни конституційної батьківщини будуть зруйновані війною, міцний демократичний фундамент дозволить їх відремонтувати і відбудувати знову та прокласти шлях до Європейського майбутнього.

Список використаної літератури:

1. Боднар О. Б. Поняття та зміст права людини на безпеку та його співвідношення з суміжними правами. *Актуальні проблеми юридичної науки*. фрм. прв … канд. юрид. наук. Київ, 2011. С. 88–93.
2. Конституція України; *Верховна Рада України* від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/1818-20?lang=en#Text
3. «Про Стратегію національної безпеки України» Указ Президента України : Стратегія від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text
4. «Про Стратегія інформаційної безпеки України» Указ Президента України : Стратегія від 28.12.2021 № 685/202. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
5. Закон України про «Медіа» від 13.12.2022 № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

Rusakevych A. I. Information security under martial law in terms of ensuring the information rights of citizens

In today's military reality, it is difficult, even inappropriate, to deny the role of information as a tool of confrontation and, in fact, as a weapon. Information allows wars to be won without a single shot being fired, creating and fueling internal contradictions. Such tactics are characteristic of the new hybrid war, in which the military element is only one component of the whole. That is why in the conditions of a direct military conflict, intelligence is a strategic tool for victory. A quality national intelligence policy contributes to tactical, operational and strategic victory. Today, when almost everyone is a source of information and can manipulate public opinion, the information that is disseminated does not always correspond to the needs dictated by national security. The purpose of this article is to determine the aspects of ensuring information rights and freedoms, taking into account the protection of information security of the state in the conditions of martial law. The author defines the priority areas of protection and their impact on the rights and freedoms of a person and a citizen. The authors emphasize the complex nature of the issue of ensuring information security, which includes three fundamental elements: legal, political and technical. It is also important to conclude that ensuring information security is a matter of simultaneously creating mechanisms that will allow to perform tasks as efficiently as possible in conditions of information restrictions and will contribute to the protection of the rights and freedoms of citizens. Ensuring information security in Ukraine is the main direction of state policy, on which national security and socio-economic development depend. Effective mechanisms for the protection of information security in Ukraine consist in the creation of an appropriate legal system that regulates relations that arise in the information sphere, and coordinated actions of subjects at all levels to ensure information security in Ukraine. The article analyzes the current problems of information security, which prevent the sustainable development of information and communication technologies in the conditions of martial law and hostilities on the territory of Ukraine.

Key words: *security, information security, information protection, threats, information policy, temporary suspension of norms, cyber threat, technical capabilities, defense, martial law, countering hostile information.*