

Котерлін І. Б.,

*старший викладач кафедри суспільних наук**Івано-Франківського національного технічного університету нафти і газу*

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ У АСПЕКТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ТА СВОБОД

INFORMATION SECURITY IN MARTIAL LAW IN TERMS OF ENSURING INFORMATION RIGHTS AND FREEDOMS

В сучасних воєнних реаліях важко та навіть недоречно заперечувати роль інформації як інструменту протистояння, фактично – зброї. Інформація дозволяє вигравати у війні не зробивши жодного пострілу, шляхом формування і розпалювання внутрішніх протиріч. Така тактика є характерною для війн нового формату – гібридних, де безпосередньо військовий фактор є лише однією зі складових цілого.

Саме тому, в умовах безпосереднього воєнного зіткнення інформація є стратегічним інструментом перемоги. Якісна державна інформаційна політика здатна посприяти тактичним, оперативним і стратегічним перемогам. В час, коли джерелом інформації і лідером суспільної думки може стати практично кожен, поширювана інформація не завжди може відповідати потребам, які диктуються захистом національної безпеки.

Право, як регулятор суспільних відносин може і повинно бути використане для належного урегулювання питань, пов'язаних із забезпеченням інформаційної безпеки. При цьому введення повної, тотальної цензури, так званих «законів військового часу» однозначно не є хорошим виходом. В демократичній державі влада повинна відповідати на вимогу суспільства забезпечувати демократичні права і свободи там, де це можливо, навіть в умовах воєнного стану.

У статті розкриваються аспекти забезпечення інформаційних прав та свобод з врахуванням захисту інформаційної безпеки держави в умовах воєнного стану. Визначаються пріоритетні напрямки захисту та вплив на права свободи людини і громадянина. В роботі концентрується увага про важливість збереження правових принципів для подальшого відновлення держави на демократичних засадах. Робиться акцент на комплексному характері питання щодо забезпечення інформаційної безпеки, включно з трьома основоположними елементами – правовим, політичним, технічним. Також, важливим є висновок про те, що забезпечення інформаційної безпеки полягає у створенні механізму, який би водночас максимально ефективно виконував поставлені завдання в контексті інформаційних обмежень і сприяв захисту прав і свобод громадян.

Ключові слова: безпека, інформаційна безпека, інформаційний захист, загрози, інформаційна політика, тимчасове призупинення норм, кіберзагроза.

Information security in martial law in terms of ensuring information rights and freedoms English Abstract: In modern military realities, it is difficult and even inappropriate to deny the role of information as a tool of confrontation, and in fact – weapon. Information allows you to win the war without firing a single shot, by forming and inciting internal contradictions. This tactic is typical of wars of a new format – the so-called hybrid wars, where the military factor is only one component of the whole. That is why, in the face of direct military conflict, information is a strategic tool for victory. High-quality state information policy can contribute to tactical, operational and strategic victories. At a time when the source of information and the leader of public opinion can be almost anyone, the information disseminated may not always meet the needs dictated by the protection of national security.

Law, as a regulator of public relations, can and should be used to properly address issues related to information security. At the same time, the introduction of full, total censorship, the so-called «laws of war» is clearly not a good solution. In a democracy, the government must respond to society's demand for democratic rights and freedoms where possible, even in martial law.

The article reveals aspects of ensuring information rights and freedoms, taking into account the protection of information security of the state in martial law. Priority areas of protection and impact on human and civil rights are identified. The paper focuses on the importance of preserving legal principles for further restoration of the state on democratic principles. Emphasis is placed on the complex nature of the issue of information security, which includes three fundamental elements – legal, political, technical. Also, it is important to conclude that information security is to create a mechanism that would at the same time most effectively perform tasks in the context of information constraints and contribute to the protection of rights and freedoms of citizens.

Key words: security, information security, information protection, threats, information policy, temporary suspension of norms, cyber threat.

Вступ. В сучасних реаліях, війна – це все менше про зброю і оперативні й тактичні зіткнення та перемоги, а все більше – про гібридність. Гібридні конфлікти передбачають наявність різних складових, в тому числі й інформаційної, яка набуває подекуди більш важливого значення, аніж військова [1]. Наявність зброї масового знищення не гарантує державі можливість перемоги, якщо вона не забезпечена перевагою в інформаційній сфері. Така перевага створюється системою заходів щодо переведення інформаційної безпеки держави на рейки воєнного стану.

Важливість безпеки у праві важко переоцінити. Так, зокрема, реалізація права на життя безперечно пов'язана з правом на безпеку [2]. У саме поняття «безпека» ми вкладаємо стан захисту нас чи того, що нам належить від посягань інших. Сучасне використання технологій, Інтернету, мобільного зв'язку, різноманітних телекомунікаційних систем окрім зручностей роблять загальну систему безпеки вразливою щодо посягань на неї. Створюються передумови витоку інформації, можливості технічного впливу на неї з метою формування потрібної суспільної думки та створення можливості фіксувати і передавати стратегічну інформацію ворогу незначними з технічної точки зору зусиллями.

Реалії нецивілізованих атак російської федерації вимагають активних дій щодо забезпечення національної безпеки України, які повинні бути збалансовані прагненням суспільства в Україні зберегти правовий характер держави. Аналіз існуючих та потенційних інформаційних загроз національній безпеці та протидія цим загрозам потребують негайної реакції, виходячи з нових викликів, спричинених війною. Гостроти проблематиці інформаційної безпеки додає спроможність ворога маніпулювати інформацією, прописувати власні наративи, відповідно, впливати на свідомість людей та формувати зручний для себе інформаційний простір. З іншого боку, сучасні технічні можливості дозволяють практично в прямому етері слідкувати за розвитком воєнних дій і, відповідно, викривати злочинні дії агресора, що є визначальним у перевазі на інформаційному фронті.

Правовий режим воєнного стану де-юре і де-факто впливає на загальний обсяг прав людини та громадянина. Інформаційна безпека

держави, яка зазнає збройної агресії, стає уразливою і потребує комплексних дій щодо її захисту, у тому числі, через звуження прав та свобод суб'єктів на її території. Гарантовані Конституцією права часто неможливо забезпечити через втрату юрисдикційних спроможностей у частині областей України та внаслідок інших безпосередніх загроз, направлених проти існування самої держави Україна та її громадян. 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 вагомую групу у цих обмеженнях становлять інформаційні права та свободи людини і громадянина.

Стан дослідження. Права людини в умовах інформаційного суспільства досліджували такі зарубіжні 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 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 важливим предметом дослідження як вітчизняних, так і закордонних науковців.

Відповідно, **мета цієї статті** – дослідження формування правових засад інформаційної безпеки України в умовах війни у системі національної безпеки щодо їх впливу на інформаційні права людини та суспільства.

Виклад основного матеріалу. Захист національної безпеки визначається Конституцією України як найважливіша функція держави (ст. 17) [3]. 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 із 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.

2020 року у новій редакції приймається «Стратегія національної безпеки України» Підзаголовком до якої є «Безпека людини – безпека країни». Відповідно до неї, пріоритетами забезпечення національної безпеки є захист особи, суспільства та держави від правопорушень, зокрема корупційних, забезпечення відновлення порушених прав, відшкодування заподіяної шкоди; посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі; а одним із основних напрямків зовнішньополітичної та внутрішньополітичної діяльності держави є забезпечення національних інтересів і безпеки, отримання повної і достовірної упереджувальної інформації про ситуацію в Україні та світі, протидія зовнішнім загрозам національній безпеці України, сприяння реалізації національних інтересів України [4].

2021 року прийнята нова Стратегія інформаційної безпеки (далі Стратегія), що передбачає комплексну взаємодію на основі Конституції України, законів України, Стратегії національної безпеки України, Стратегією кібербезпеки України, затвердженою, а також міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України. У ній вже конкретизуються потенційні інформаційні загрози: «інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав» [5].

У Стратегії дається визначення поняттю «інформаційна безпека України» як складової частини національної безпеки України, стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належ-

ним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існування ефективної системи захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом. Як бачимо, відповідно до визначення, одним із елементів інформаційної безпеки є стан захищеності демократичного ладу, що сприяє забезпеченню конституційних прав і свобод людини.

Слово «загроза» в інформаційній безпеці означає, що будь-хто або будь-що підпадає під небезпеку будь-яких негативних впливів у сфері інформаційної діяльності. Загрози можуть бути внутрішніми, спричиненими суб'єктом інформаційних відносин через недостатню кваліфікованість, розуміння процесів і наслідків чи злочинним умислом, так і зовнішнім. Загрози включають в себе впливи, до яких можна віднести хакерство і бездіяльність уповноважених органів щодо виявлення та реакції на загрози; помилки у стратегії політичного курсу щодо системи прийняття законів та їх реалізації; рівень інформаційної культури суспільства та владного істеблішменту; соціально-економічний стан суспільства та держави.

У Стратегії поняття «інформаційна загроза» пояснюється як потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні.

Очікуваними результатами реалізації Стратегії визначено захищений інформаційний простір України, ефективне функціонування системи стратегічних комунікацій, здійснення ефективної протидії поширенню незаконного контенту, забезпечення сталого процесу інформаційної реінтеграції громадян України, які проживають на тимчасово окупованих територіях України,

та поширення українського телерадіомовлення на територіях України, прилеглих до тимчасово окупованих територій, суттєве підвищення рівня медіа-культури та медіа-грамотності населення, дотримання конституційних прав особи на вільне вираження своїх поглядів і переконань, захист приватного життя, забезпечення захисту прав журналістів, формування української громадянської ідентичності.

Очевидно, в умовах війни акценти на виявлення загроз і реакцію змінюються у напрямку звуження прав людини, керуючись необхідністю забезпечення впливу на потенційні та існуючі загрози.

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» [6].

Серед конституційних норм, щодо яких можливі обмеження їх дії є і ті, що безпосередньо стосуються інформаційних прав. Зокрема:

- стаття 31 («Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції»);
- стаття 32 («Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України»);
- стаття 34 («Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань»);
- стаття 41 («Кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності»).

Ці обмеження обумовлені неможливістю захистити осіб на території України від свавілля ворога, Україна не може нести відповідальність за порушення цих прав на непідконтрольних, внаслідок окупації, територіях та місцях ведення бойових дій. Інше їх значення полягає у можливості прийняття нормативно правових актів, направлених у першу чергу на захист інформаційної безпеки держави. Такі пріоритети можуть іти в розріз із розумінням гарантій прав людини,

однак, в час війни перевага інтересів держави означає можливість збереження основоположних прав багатьох людей через забезпечення життєздатності самої держави. Завершення воєнного стану автоматично активує тимчасово призупинену дію норм вищеназваних норм.

Важливо зауважити: воєнний стан не став приводом для свавільного владного трактування права обов'язків суб'єктів із хаотичним встановленням обмежень і заборон. Послідовно, виходячи з актуальності і потреб приймаються закони, якими регламентуються правила поведінки.

З моменту оголошення воєнного стану, приймаються зміни до нормативно правових актів з врахуванням реалій війни. Вони стосуються врегулювання деяких аспектів інформаційних правовідносин щодо заборони поширювати певну інформацію, враховуючи її суспільно-небезпечний характер; врегулювання важливих моментів щодо технічного фіксування інформації в умовах воєнного стану; встановлення чи посилення відповідальності за поширення певної інформації; врегулювання процесуальних дій щодо вилучення інформаційних даних.

Так, Верховна Рада ухвалила законопроект про кримінальну відповідальність за незаконну фото- та відеозйомку переміщення ЗСУ та міжнародної військової допомоги під час воєнного стану [6].

22 березня 2022 р. набув чинності Закон, яким спрощено проведення слідчих дій та тимчасових доступів до речей і документів, слідчий може здійснити фіксацію комп'ютерних даних на місці обшуку, навіть якщо про це не сказано в дозволі: зміни до КПК [7].

Посилено кримінальну відповідальність за виготовлення та поширення забороненої інформаційної продукції відповідно до Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції» [8].

Окрім обнадійливих факторів тримання оборони демократичних засад ми можемо бачити і певні негативні антидемократичні передвісники, що виправдовуються воєнним станом. Зокрема рішенням Ради Національної безпеки і оборони від 8 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» встановлено, що в умовах

воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні «Єдині новини #UAразом»». З огляду на це рекомендовано Національній раді України з питань телебачення і радіомовлення вжити заходів щодо реалізації цього рішення[9]. Відповідно до цього Рішення декілька каналів, опозиційних до влади однак завжди з проукраїнською позицією, було відімкнено в цифровій мережі T2. При цьому жоден уповноважений орган як от Національна рада України з питань телебачення і радіомовлення, Міністерство оборони України, яке відповідно до закону регулює режим воєнного стану, РНБО України чи суд не приймали жодних рішень щодо відключення даних телеканалів[10]. У той самий час канал «Інтер», що був рупором російської пропаганди, майданчиком для антиукраїнських сил став частиною проєкту «Єдині новини #UAразом» [11].

Висновки. Сьогоднішні воєнні реалії чітко демонструють, що інформація є зброєю «масового ураження». Тому необхідно створити ефективний механізм, який би забезпечив державну інформаційну безпеку і дотримання прав людини та водночас дозволив би людям не відчувати ефекту посягань на свободи та демократію. Найбільша цінність українців полягає у їх розумінні

та сприйнятті понять свобода і справедливість. Саме це вони зараз відстоюють, і розплачуються за них власним життям. Для побудови ефективної системи інформаційної безпеки важливо покласти в його основу три логічні складові механізму цієї 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.

Таким чином, формування інформаційної безпеки в умовах війни є комплексною технічною та політико-правовою діяльністю уповноважених органів, спрямованою на захист держави, суспільства і людини. У воєнний час захист інформаційної безпеки держави є пріоритетним оскільки безпосередньо від нього залежить безпека суспільства і людини. У час війни публічно-правовий захист виходить за межі традиційного регулювання і поглинає приватно-правові відносини.

Необхідно розуміти, що за умов воєнних дій держава часто об'єктивно неспроможна гарантувати права людини в повному об'ємі. Однак збереження фундаментальних засад на основі політичної та правової взаємодії механізмів забезпечення інформаційної безпеки оберігає підвалини демократії та систему загальних принципів права від руйнування волонтаристськими рішеннями. Якщо війна валить стіни нашої конституційної оселі – міцний фундамент демократизму дасть змогу їх відновити і відбудувати.

ЛІТЕРАТУРА:

1. Боднар О. Б. Поняття та зміст права людини на безпеку та його співвідношення з суміжними правами. *Форум права*. 2011. № 1. С. 88-93. URL: http://nbuv.gov.ua/UJRN/FP_index.htm_2011_1_18 (дата звернення 20.04.2022)
2. Конституція України від 28 червня 1996 р. URL: <http://zakon5.rada.gov.ua/laws/show/254к/96-вр>. (дата звернення 20.04.2022)
3. 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 20.04.2022)
4. Стратегія інформаційної безпеки. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n14> (дата звернення 20.04.2022)
5. Про введення воєнного стану в Україні. URL: <https://www.president.gov.ua/documents/642022-41397> (дата звернення 20.04.2022)
6. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану. URL: <https://zakon.rada.gov.ua/laws/show/2160-20#n10> (дата звернення 20.04.2022)

7. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам. URL: <https://zakon.rada.gov.ua/laws/show/2137-20#Text> (дата звернення 20.04.2022)
8. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції. Закон України. URL: <https://zakon.rada.gov.ua/laws/show/2110-20#Text> (дата звернення 20.04.2022)
9. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану. Рішення РНБО. URL: <https://zakon.rada.gov.ua/laws/show/n0004525-22#Text> (дата звернення 20.04.2022)
10. Концерн РРТ вимкнув мовлення «Еспресо» в цифровій мережі T2: відкритий лист телеканалу до президента, РНБО, СБУ, Міноборони, Нацради. *Еспресо*. URL: <https://espresso.tv/kontsern-rrt-vimknuv-movlennya-espresso-v-tsifroviy-merezhi-t2-vidkritiy-list-telekanalu-do-prezidenta-rnbo-sbu-minoboroni-natsradi> (дата звернення 20.04.2022)
11. Детектор медіа. URL: <https://detector.media/infospace/article/198490/2022-04-18-opzzh-ne-pratsyuie-shcho-bude-z-interom/> (дата звернення 20.04.2022)