

ABSTRACT

**Oleh Levin, Oleh Poplavskyu. Specifics of democratic transit in the newly created Baltic countries after the the USSR's collapse.** The article describes in difficulties in transformation of political systems in Lithuania, Latvia and Estonia in conditions of independence. Certain features of the single political region of Baltic states are being explored, which was created after the breakup of the Soviet Union.

A feature of the successful reform of the political systems of the Baltic States was the mass support for democratic change by various segments of the population. Given the specific features of the ethnic composition of each Baltic country, especially the number of Russian-speaking population and its influence on political decision-making, each of them chose its own path of certain transformations.

In Lithuania, where the number of ethnic Lithuanians was 87% of the total population, the so-called «zero citizenship option» was adopted. It was given to all who lived on its territory at the time of the collapse of the USSR.

In Latvia and Estonia, in contrast to Lithuania, almost half of the population was Russian-speaking, and the non-inclusive nature of citizenship became non-inclusive. Most of the Russian-speaking population living in these countries did not receive citizenship at all, and therefore no political rights (and the Estonian government generally introduced two versions of passports – «blue» and «gray», respectively, for different categories of residents). As a result, the formation of the legislative and political fields took place without the participation of the Russian-speaking majority, causing discrimination on the basis of nationality. By adopting citizenship legislation, the Latvian and Estonian parliaments ensured the formation of a consolidated electorate with a more or less similar vision of their own statehood. Also, in fact, due to the legislation, the electorate was selected, which in the future ensured the recruitment of the Latvian and Estonian elites and its consolidation.

The effectiveness of democratic transit in Latvia, Lithuania and Estonia, as well as the synchronicity of their integration into the European Union led to the creation of a single Baltic political space in the former Soviet Union. The peculiarities of such a space are the common geopolitical goals and interests, the identity of political systems, the standardization of legal institutions in the European environment. Compared to other republics of the former Soviet Union, Latvia, Lithuania and Estonia have become more and more integrated into the world, and in particular, European structures.

**Keywords:** Lithuania, Latvia, Estonia, democracy, transformation.

УДК 342.727+351.751

DOI: 10.31733/2078-3566-2022-1-195-203



**Андрій САМОТУГА** ©

кандидат юридичних наук, доцент  
(Дніпропетровський державний університет  
внутрішніх справ, м. Дніпро, Україна)

**ОРГАНІЗАЦІЙНО-ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ  
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ**

У сучасних умовах повномасштабної агресії РФ проти України інформаційна складова не втрачає свого значення, що покладає особливі повноваження на суб'єктів забезпечення інформаційної безпеки держави. За результатами аналізу положень Стратегії інформаційної безпеки України визначено функції та завдання її суб'єктів, визначено пріоритетні напрямки їх взаємодії, зокрема щодо здійснення проактивної зовнішньої інформаційної політики, спрямованої на нейтралізацію та запобігання загрозам суспільству й державі в інформаційній сфері, зокрема, та міжнародно-безпековій, взагалі.

**Ключові слова:** інформаційна політика, інформаційна безпека, суб'єкти, забезпечення.

**Постановка проблеми.** Стрімкий розвиток засобів створення, пошуку, накопичення й передачі інформації, в т. ч. й дезінформації, спричинив низку проблем правового характеру, що передбачає захист інформаційних прав особи, суспільства і держави. Науково-практичний інтерес, що постійно зростає до такої комплексної галузі

© А. Самотуга, 2022

ORCID iD: <https://orcid.org/0000-0001-9802-0226>

samotuga@ua.fm

права й законодавства, як інформаційне право, має одним із своїх напрямків вивчення проблем інформаційної безпеки. Вона, зі свого боку, також є комплексним поняттям з точки зору її забезпечення – не лише технічними (програмно-телекомунікаційними), а також правовими (нормативними й організаційно-інституційними) засобами. Останніми роками в Україні створено ґрунтовну нормативну базу з питань інформації взагалі та інформаційної безпеки, зокрема, як на рівні законів, так і кількох програмних документів – стратегій, концепцій, доктрин тощо. Втім свого розв'язання потребує проблема належного виконання зазначених актів, що ставить на порядок денний питання саме організаційно інституційного забезпечення цієї однієї з провідних функцій сучасної держави, зважаючи на внутрішні та зовнішні виклики й загрози, зокрема військовій агресії як спосіб вирішення міждержавних конфліктів та реалізації ментально-ідеологічно-цивілізаційних експансіоністських зазіхань, заснованих на вже апробованих століттями ідеологіях імперіалізму, шовінізму, комунізму та фашизму.

Більше того, сучасні умови ведення РФ широкомасштабної не лише гібридної (економічної, інформаційно-гуманітарної), а переважно вже суто збройної війни проти України вимагають належного та своєчасного реагування (в тому числі санкційного (обмежувального) характеру) з боку компетентних органів держави на прояви ворожих інформаційних та дезінформаційних спецоперацій проти України, які передують та супроводжують військові, в чому держава-агресор за десятки останніх років активно й небезуспішно, на жаль, вправлялася, витрачаючи на «індустрію брехні», у т. ч. з інвестуванням закордон близько мільярда доларів щороку.

**Аналіз публікацій, в яких започатковано вирішення цієї проблеми.** Останніми роками науковий арсенал з інформаційного права України значно поповнився вагомими доробками різноманітної тематики, в т. ч. й в суміжних галузях права – кримінальному, цивільному тощо, а також у працях з філософських, філологічних, економічних та політичних наук, з державного управління та соціальних комунікацій. Безпосередньо інформаційну безпеку в різних науково-методологічних вимірах досліджували такі автори, як О. Литвиненко (1997), О. Андреева (2003), В. Гурковський (2004), Б. Кормич (2004), В. Козубський (2005), О. Логінов (2005), В. Конах (2005), Ю. Максименко (2007), Т. Тардаскіна (2007), А. Юричко (2007), Ю. Романчук (2009), В. Триняк (2009), О. Золотар (2010), В. Петров (2010), Т. Субіна (2010), Л. Євдоченко (2011), Г. Линник (2011), Д. Сулацький (2011), О. Тихомиров (2011), О. Шевчук (2011), Є. Архіпова (2012), І. Березовська (2012), Д. Красіков (2012), М. Танцюра (2012), О. Чувакова (2012), О. Боборишева (2013), М. Карчевський (2013), О. Олійник (2013), О. Стоєцький (2013), І. Колодій (2014), О. Довгань (2016), К. Дубняк (2016), А. Шапка (2016), В. Антонюк (2017), О. Грицун (2017), О. Зозуля (2017), Ю. Лісовська (2017), Л. Буга (2018), І. Валюшко (2018), А. Нашинець-Наумова (2018), С. Лисенко (2019), Т. Перун (2019), О. Топчій (2019), С. Шайхет (2019), А. Бевза (2020), А. Турчак (2020) та ін. І це лише дослідження з гуманітарних та суспільних наук, не враховуючи технічні.

Незважаючи на постійний інтерес до зазначеної проблематики, потребує свого постійного висвітлення питання суб'єктів забезпечення інформаційної безпеки, виходячи з перманентних змін законодавства, національної правозастосовчої практики та міжнародної комунікації.

**Метою** статті є аналіз організаційно-правового забезпечення діяльності суб'єктів інформаційної безпеки України з подальшим викладенням можливих напрямків їх взаємодії.

**Виклад основного матеріалу.** Передусім потребує свого з'ясування дефініція «інформаційна безпека». Законодавство України донедавна не містило визначення цього поняття, за винятком, лише умовно, Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007, оскільки його назва містить визначені межі реалізації цього акта. Згідно з ним інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Вирішення проблеми інформаційної безпеки має здійснюватися шляхом: створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і

прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань; вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері; розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація [9].

Дата прийняття цього закону пов'язана із загостренням внутрішньополітичної боротьби в Україні між владною коаліцією – прибічниками проєвропейської зовнішньополітичної орієнтації держави та проросійськими політичними угрупованнями, всіляко підтримуваними нинішньою державою-агресором, в т.ч. через власні й афілійовані в Україні ЗМІ, політичні партії та «громадські» організації, які прагнули реваншу після поразки (в т. ч. й після невдалої фальсифікації результатів через масові протестні акції) на президентських виборах 2004 р., досягнувши своєї мети на чергових президентських виборах 2010 р.

Після Революції Гідності 2013-2014 рр. та початком військової агресії РФ проти України національне законодавство, яке почало переживати бурхливий розвиток, обійшло, на жаль, належною увагою зазначену категорію. Новий Закон України «Про Національну безпеку» від 21.06.2018, хоча й містить поняття «інформаційна безпека» як складову національної безпеки, але не надає його визначення, на відміну від таких понять, як «воєнна безпека», «громадська безпека», «державна безпека», «національна безпека». Також без визначення в цьому законі залишилися поняття економічної, зовнішньополітичної та екологічної безпеки [5]. Деяко подібне визначення містить Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017, але стосовно кібербезпеки, яка визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі – мережі Інтернет та інші глобальні мережі передачі даних [8] (напр., VPN-сервіси). А оскільки інформаційна діяльність поступово переходить із таких традиційних видів, як телебачення і радіо до мережі Інтернет та таких її підвидів, як соціальні мережі й мобільні додатки-месенджери для приватного та групового спілкування, то кібербезпеку за всіма підставами можна вважати різновидом інформаційної безпеки.

Більше того, цим законом визначено суб'єктів забезпечення кібербезпеки, а саме:

а) загальні:

1) Президент України, який через очолювану ним Раду національної безпеки і оборони України здійснює координацію діяльності у сфері кібербезпеки як складової національної безпеки України;

2) Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України – здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України;

3) Кабінет Міністрів України – забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури (крім об'єктів критичної інфраструктури у банківській системі України);

б) спеціальні:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури. При цьому до об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які: 1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах; 2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров'я; 3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню; 4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави; 5) є об'єктами потенційно небезпечних технологій і виробництв;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [8].

Другий блок суб'єктів містить, знов-таки, як органи загальної (місцеві державні адміністрації, органи місцевого самоврядування), так і органи спеціальної компетенції. Водночас, як зазначено в новій Стратегії кібербезпеки України, затвердженій Указом Президента України від 26.08.2021, діяльність суб'єктів національної системи кібербезпеки залишається недостатньо скоординованою і такою, що спрямована на виконання лише поточних завдань. За результатами експертних оцінок, стан реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.2016, за визначеними показниками не перевищує 40 відсотків. Невирішеними залишилися питання оперативного обміну інформацією про кіберзагрози, ефективної системи підготовки кадрів та дієвої моделі державно-приватного партнерства. Недостатніми є організації і проведення наукових досліджень у сфері кібербезпеки [16].

Про значення програмних документів держави у сфері інформаційної безпеки можна вести мову, звернувшись до іншого акта глави держави – Стратегії інформаційної безпеки (далі – Стратегія), затвердженій Указом Президента України від 28.12.2021. Стратегія, хоча й не є законодавчим актом, але містить, на відміну від деяких програмних документів, своєрідний блок визначення термінів. Так, інформаційну безпеку вона визначає як складову частину національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система 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 [15].

Отже, зазначена дефініція є ширшою, на відміну від, напр., визначення кібербезпеки, наданого в Стратегії кібербезпеки, оскільки акцентує, крім того, на забезпеченні фундаментальних інформаційних прав людини, проголошених Основним Законом – Конституцією України (ст. ст. 31, 32) та міжнародними актами з прав людини.

Більше того, Стратегія містить хоча й безпосередній перелік суб'єктів забезпечення інформаційної безпеки, але визначає механізм реалізації визначеної мети та завдань Стратегії, до якого включено широке коло суб'єктів із визначенням їхніх функцій та повноважень, яких, як вважаємо, слід розглянути детально.

1. *Рада національної безпеки і оборони України.* Відповідно до Конституції України (ст. 107) та у встановленому законом порядку [10] здійснює координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері, зокрема з використанням спроможностей Центру протидії дезінформації. Окрім нормотворчої діяльності, як от розробка та схвалення програмних

документів в інформаційній сфері (доктрини, стратегії), РНБО також вживає заходів цілеспрямованого індивідуального характеру з метою виявлення та своєчасної нейтралізації інформаційних загроз Україні.

Так, Законом України «Про санкції» санкції можуть застосовуватися з боку України по відношенню до іноземної держави, іноземної юридичної особи, юридичної особи, яка знаходиться під контролем іноземної юридичної особи чи фізичної особи-нерезидента, іноземців, осіб без громадянства, а також суб'єктів, які здійснюють терористичну діяльність. Рішення щодо застосування, скасування та внесення змін до санкцій приймається Радою національної безпеки та оборони України, вводиться в дію указом Президента України та затверджується протягом 48 годин з дня видання указу Президента України постановою Верховної Ради України. Відповідне рішення набирає чинності з моменту прийняття постанови Верховної Ради України і є обов'язковим до виконання [13].

На виконання зазначеного закону починаючи з 2015 року РНБО було прийнято понад 50 рішень про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій) до фізичних та юридичних осіб, діяльність яких становить небезпеку для України, зокрема в інформаційній сфері. Наприклад, рішенням РНБО від 02.02.2021 застосовано обмежувальні заходи (санкції) до таких юридичних осіб: ТОВ «Аріадна ТВ», ТОВ «Новий Формат ТВ», ТОВ «ТВ Вибір», ТОВ «Телерадіокомпанія «112-ТВ», ТОВ «Лідер ТВ», ТОВ «Партнер ТВ», «Новини 24 години», ТОВ «Нові комунікації»; рішенням РНБО від 16.02.2022 нею було застосовано обмежувальні заходи до 16-и фізичних та юридичних осіб, зокрема щодо А. Шарія та ТОВ «Інформаційне агентство «Шарій.нет» [11-12].

Отже, РНБО своїми рішеннями більш оперативно реагує на інформаційні загрози Україні, вживаючи заборонні та обмежувальні санкції, оминаючи при цьому звернення до суду, як це передбачено стосовно повноважень іншого конституційного органу – Національної ради України з питань телебачення і радіомовлення, діяльність якої буде розглянута далі.

2. *Кабінет Міністрів України* – проводить державну політику у сфері інформатизації, сприяє становленню єдиного інформаційного простору на території України [4]; забезпечує формування та реалізацію інформаційної політики держави, забезпечує інформаційний суверенітет, фінансування програм, пов'язаних з інформаційною безпекою, спрямовує і координує роботу міністерств, інших органів виконавчої влади у цій сфері. Кабінет Міністрів України розробляє та затверджує план заходів з реалізації Стратегії, на основі якого відповідні органи виконавчої влади реалізують заходи щодо забезпечення інформаційної безпеки. Органи державної влади у взаємодії з органами місцевого самоврядування, Центром протидії дезінформації та інститутами громадянського суспільства забезпечують реалізацію Стратегії згідно з планом заходів, який затверджується Кабінетом Міністрів України.

3. *Центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері:*

- здійснює в межах компетенції нормативно-правове регулювання у сфері інформаційної безпеки України;
- визначає перспективи та пріоритетні напрями розвитку у сфері інформаційної безпеки України;
- разом із Міністерством закордонних справ України сприяє популяризації та формуванню позитивного іміджу України у світових інформаційних ресурсах та національних інформаційних ресурсах іноземних держав з метою захисту її політичних, економічних та соціально-культурних інтересів, зміцнення національної безпеки і відновлення територіальної цілісності України.

На сьогодні таким органом є Міністерство культури та інформаційної політики України (МКІП), утворене у 2019 р. в результаті об'єднання Міністерства культури і мистецтв України з ліквідованим Міністерством інформаційної політики України, створеним у 2014 р. Відповідним положенням зазначено, що МКІП є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах культури, державної мовної політики, популяризації України у світі, державного іномовлення, інформаційного суверенітету України (у частині повноважень з управління цілісними майновими комплексами державного підприємства “Мультимедійна платформа іномовлення України” та Українського національного інформаційного агентства “Укрінформ”) та інформаційної безпеки, а

також забезпечує формування та реалізацію державної політики у сферах відновлення та збереження національної пам'яті, міжнародних відносин, релігії та захисту прав національних меншин в Україні, мистецтв, охорони культурної спадщини, музейної справи, вивезення, ввезення і повернення культурних цінностей [2].

Іншим центральним органом виконавчої влади, але вже зі спеціальним статусом, діяльність якого спрямовується і координується Кабінетом Міністрів України через Міністра культури та інформаційної політики, є Державний комітет телебачення і радіомовлення України (Держкомтелерадіо). Цей орган виконує за дорученням Міністра культури та інформаційної політики за участю інших державних органів завдання, зокрема, щодо забезпечення інформаційної безпеки, вживає заходів з підвищення захорожної якості вітчизняних телерадіопрограм, із захисту суспільства від негативного впливу аудіо- і відеопродукції, яка становить загрозу суспільній моралі [1]. Серед пріоритетних завдань цього органу на 2022 рік визначено, зокрема, реалізацію заходів з формування медіаграмотності та протидії дезінформації, недопущення на український ринок іноземної видавничої продукції антиукраїнського змісту [3].

4. *Міністерство оборони України, а також сили оборони* в межах компетенції забезпечують:

- моніторинг інформаційного простору, прогнозування та виявлення інформаційних загроз національній безпеці держави у воєнній сфері;
- підготовку та проведення інформаційних заходів оборони держави, координацію залучення до них суб'єктів забезпечення національної безпеки держави;
- розвиток та функціонування системи стратегічних комунікацій сил оборони;
- здійснення правових, організаційних, технічних, інформаційних та інших дій щодо забезпечення власної інформаційної безпеки, у тому числі захисту єдиного інформаційного середовища сил оборони, зокрема в місцях дислокації, розгортання та застосування угруповань, військових частин та підрозділів Збройних Сил України, інших військових формувань, утворених відповідно до законів України;
- зв'язки з українськими та іноземними засобами масової інформації щодо висвітлення ситуації у районах здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії РФ;
- протидію інформаційним операціям та іншим заходам інформаційного впливу, спрямованим проти Збройних Сил України та інших військових формувань, утворених відповідно до законів України;
- донесення достовірної інформації до військовослужбовців Збройних Сил України, інших складових сил оборони.

Підготовка держави до оборони в мирний час включає, зокрема: проведення розвідувальної та інформаційно-аналітичної діяльності в інтересах підготовки держави до оборони; захист інформаційного простору України та її входження у світовий інформаційний простір, створення розвинутої інфраструктури в інформаційній сфері. Відсіч збройній агресії проти України передбачає на підставі відповідного рішення Президента України здійснення Збройними Силами України разом з іншими військовими формуваннями воєнних дій, у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі [7].

5. *Служба безпеки України* у межах компетенції здійснює:

- моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та Інтернету з метою виявлення загроз національній безпеці України в інформаційній сфері;
- протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на піддрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації.

6. *Розвідувальні органи України* у процесі провадження розвідувальної діяльності мають сприяти реалізації та захисту національних інтересів України в інформаційній сфері за кордоном, здійснювати виявлення та протидію зовнішнім інформаційним загрозам у сфері безпеки та оборони держави.

7. *Національна рада України з питань телебачення і радіомовлення* (далі – Нацрада), відповідно до компетенції, бере участь у забезпеченні захисту українського інформаційного простору від пропагандистської аудіовізуальної продукції держави-агресора, сприяє розповсюдженню українського телерадіомовлення на тимчасово окупованих територіях України. Основними її повноваженнями, відповідно до закону, є

контроль і нагляд за дотриманням законодавства у сфері телерадіомовлення, його ліцензування та державна реєстрація телерадіоорганізацій та провайдерів програмної послуги [6]. Стосовно санкцій, що застосовує Нацрада, то спеціальний закон відсилає до іншого профільного закону, в якому зазначено, що санкції за порушення законодавства про телебачення і радіомовлення застосовуються за рішенням суду або, у встановлених цим Законом випадках, за рішенням Нацради. Вона може застосовувати до телерадіоорганізацій та провайдерів програмної послуги такі санкції: оголошення попередження; стягнення штрафу; анулювання ліцензії на підставі рішення суду за позовом Національної ради. При цьому рішення про оголошення попередження приймається у разі першого порушення законодавства чи умов ліцензії телерадіоорганізацією або першого порушення законодавства провайдером програмної послуги [14]. Як впливає з наведеного, ускладнений, ступеневий порядок застосування зазначених інформаційно-правових санкцій є важливою гарантією дотримання свободи слова як ключового принципу демократичної, правової держави.

До реалізації Стратегії відповідальними державними органами можуть залучатися наукові та науково-дослідні установи, які забезпечують науково-аналітичне та експертне супроводження процесу формування та реалізації державної інформаційної політики.

**Висновки.** З урахуванням викладеного можна констатувати, що наведений перелік суб'єктів (державних) забезпечення інформаційної безпеки буде неповним, якщо не спрямувати їхню діяльність на взаємодію з інститутами громадянського суспільства, зокрема незалежними спілками журналістів та інших творчих працівників медійної сфери, які як ніхто інший найбільше заінтересовані у прозорості та виваженості державної інформаційної політики зі створенням рівних умов для діяльності в цій сфері, що буде тематикою окремої публікації.

Більше того, нинішній стан інформаційної політики в умовах воєнної агресії РФ щодо України вимагає нових, нестандартних підходів до налагодження співпраці з військовими адміністраціями в регіонах, складовою чого також є інформаційна безпека.

Зрештою, на створенні нормативної та інституційної бази формування цілісної системи забезпечення інформаційної безпеки не завершується. Воно вимагає надто більшого – людських, фахових та матеріально-технічних ресурсів, зокрема для здійснення цілеспрямованої зовнішньої інформаційної політики, чим, на жаль, не володіє ще достатньо Україна, на відміну від держави-агресора, яка роками вибудовувала одночасно з озброєнням свою пропагандистську імперію, в т. ч. за кордоном.

#### **Список використаних джерел**

1. Положення про Державний комітет телебачення і радіомовлення України : затв. постановою Кабінету Міністрів України від 13.08.2014 № 341. URL : [http://comin.kmu.gov.ua/control/uk/publish/article?art\\_id=170429&cat\\_id=32820](http://comin.kmu.gov.ua/control/uk/publish/article?art_id=170429&cat_id=32820).
2. Положення про Міністерство культури та інформаційної політики України : затв. постановою Кабінету Міністрів України від 16.10.2019 № 885. URL : <https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text>.
3. Пріоритетні завдання Держкомтелерадіо у 2022 році. URL : [http://comin.kmu.gov.ua/control/uk/publish/article?art\\_id=182262&cat\\_id=68691](http://comin.kmu.gov.ua/control/uk/publish/article?art_id=182262&cat_id=68691).
4. Про Кабінет Міністрів України : Закон України від 27.02.2014. *Відомості Верховної Ради України*. 2014. № 13. Ст. 222.
5. Про національну безпеку України : Закон України від 21.06.2018. *Відомості Верховної Ради*. 2018. № 31. Ст. 241.
6. Про Національну раду України з питань телебачення і радіомовлення : Закон України від 23.09.1997. *Відомості Верховної Ради України*. 1997. № 48. Ст. 296.
7. Про оборону України : Закон України від 06.12.1991. *Відомості Верховної Ради України*. 1992. № 9. Ст. 106.
8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.
9. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : затв. Законом України від 09.01.2007. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.
10. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998. *Відомості Верховної Ради України*. 1998. № 35. Ст. 237.
11. Про рішення Ради національної безпеки і оборони України від 02.02.2021 «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» : введено в дію Указом Президента України від 02.02.2021 № 43/2021. URL : <https://www.rnbo.gov.ua/ua/Ukazy/4801.html>.
12. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про внесення змін до персональних спеціальних економічних та інших обмежувальних заходів

(санкцій)» : введено в дію Указом Президента України від 16 лютого 2022 року № 57/2022. URL : <https://www.rnbo.gov.ua/ua/Ukazy/5265.html>.

13. Про санкції : Закон України від 14.08.2014. *Відомості Верховної Ради України*. 2014. № 40. Ст. 2018.

14. Про телебачення і радіомовлення : Закон України від 21.12.1993. *Відомості Верховної Ради України*. 1994. № 10. Ст. 43.

15. Стратегія інформаційної безпеки : затв. Указом Президента України від 28.12.2021 № 685/2021. URL : <https://www.president.gov.ua/documents/6852021-41069>.

16. Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» : затв. Указом Президента України від 26.08.2021 № 447/2021. *Офіційний вісник Президента України*. 2021. № 22. Ст. 1055.

*Надійшла до редакції 04.03.2022*

### **References**

1. Polozhennya pro Derzhavnyy komitet telebachennya i radiomovlennya Ukrayiny [Regulations on the State Committee for Television and Radio Broadcasting of Ukraine] : zatv. postanovoyu Kabinetu Ministriv Ukrayiny vid 13.08.2014 № 341. URL : [http://comin.kmu.gov.ua/control/uk/publish/article?art\\_id=170429&cat\\_id=32820](http://comin.kmu.gov.ua/control/uk/publish/article?art_id=170429&cat_id=32820). [in Ukr.].

2. Polozhennya pro Ministerstvo kul'tury ta informatsiyoi polityky Ukrayiny [Regulations on the Ministry of Culture and Information Policy of Ukraine] : zatv. postanovoyu Kabinetu Ministriv Ukrayiny vid 16.10.2019 № 885. URL : <https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text>. [in Ukr.].

3. Priorityetni zavdannya Derzhkomtelradio u 2022 rotsi [Priorities of the State Committee for Television and Radio Broadcasting in 2022]. URL : [http://comin.kmu.gov.ua/control/uk/publish/article?art\\_id=182262&cat\\_id=68691](http://comin.kmu.gov.ua/control/uk/publish/article?art_id=182262&cat_id=68691). [in Ukr.].

4. Pro Kabinet Ministriv Ukrayiny [On the Cabinet of Ministers of Ukraine] : Zakon Ukrayiny vid 27.02.2014. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 2014. № 13. Art. 222. [in Ukr.].

5. Pro natsional'nu bezpeku Ukrayiny [On National Security of Ukraine] : Zakon Ukrayiny vid 21.06.2018. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 2018. № 31. Art. 241. [in Ukr.].

6. Pro Natsional'nu radu Ukrayiny z pytan' telebachennya i radiomovlennya [On the National Council of Ukraine on Television and Radio Broadcasting] : Zakon Ukrayiny vid 23.09.1997. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 1997. № 48. Art. 296. [in Ukr.].

7. Pro oboronu Ukrayiny [On the Defense of Ukraine] : Zakon Ukrayiny vid 06.12.1991. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 1992. № 9. Art. 106. [in Ukr.].

8. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny [On the Basic Principles of Cybersecurity of Ukraine] : Zakon Ukrayiny vid 05.10.2017. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 2017. № 45. Art. 403. [in Ukr.].

9. Pro Osnovni zasady rozvytku informatsiyoho suspil'stva v Ukrayini na 2007-2015 roky [On the Basic Principles of Information Society Development in Ukraine for 2007-2015] : zatv. Zakonom Ukrayiny vid 09.01.2007. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 2007. № 12. Art. 102. [in Ukr.].

10. Pro Radu natsional'noyi bezpeky yi oborony Ukrayiny [On the National Security and Defense Council of Ukraine] : Zakon Ukrayiny vid 05.03.1998. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 1998. № 35. Art. 237. [in Ukr.].

11. Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 02.02.2021 «Pro zastosuvannya personal'nykh spetsial'nykh ekonomichnykh ta inshykh обмежувальних заходів (санкцій)» [On the decision of the National Security and Defense Council of Ukraine of 02.02.2021 «On the application of personal special economic and other restrictive measures (sanctions)»] : vvedeno v diyu Ukazom Prezydenta Ukrayiny vid 02.02.2021 № 43/2021. URL : <https://www.rnbo.gov.ua/ua/Ukazy/4801.html>. [in Ukr.].

12. Pro rishennya Rady natsional'noyi bezpeky i oborony Ukrayiny vid 30 hrudnya 2021 roku «Pro vnesennya zmin do personal'nykh spetsial'nykh ekonomichnykh ta inshykh обмежувальних заходів (санкцій)» [On the decision of the National Security and Defense Council of Ukraine of December 30, 2021 «On amendments to personal special economic and other restrictive measures (sanctions)»] : vvedeno v diyu Ukazom Prezydenta Ukrayiny vid 16 lyutoho 2022 roku № 57/2022. URL : <https://www.rnbo.gov.ua/ua/Ukazy/5265.html>. [in Ukr.].

13. Pro sanktsiyi [On sanctions] : Zakon Ukrayiny vid 14.08.2014. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 2014. № 40. Art. 2018. [in Ukr.].

14. Pro telebachennya i radiomovlennya [On Television and Radio Broadcasting] : Zakon Ukrayiny vid 21.12.1993. *Vidomosti Verkhovnoyi Rady Ukrayiny*. 1994. № 10. Art. 43. [in Ukr.].

15. Stratehiya informatsiyoi bezpeky [Information Security Strategy] : zatv. Ukazom Prezydenta Ukrayiny vid 28.12.2021 № 685/2021. URL : <https://www.president.gov.ua/documents/6852021-41069>. [in Ukr.].

16. Stratehiya kiberbezpeky Ukrayiny «Bezpechnyy kiberprostir – zaporuka uspishnoho rozvytku krayiny» [Cybersecurity Strategy of Ukraine «Safe Cyberspace – the key to successful development of the country»] : zatv. Ukazom Prezydenta Ukrayiny vid 26.08.2021 № 447/2021. *Ofitsiyyny visnyk Prezydenta Ukrayiny*. 2021. № 22. Art. 1055. [in Ukr.].



#### ABSTRACT

**Andriy Samotuha. Organizational and institutional support of information security of Ukraine.** In the current conditions of full-scale aggression of the Russian Federation against Ukraine, the information component does not lose its significance, which imposes special powers on actors of information security of the state. Based on the analysis of the provisions of the Information Security Strategy of Ukraine of 2021 (hereinafter – the Strategy), the functions and tasks of its actors have been identified, priority areas of their cooperation have been defined, in particular the implementation of proactive foreign information policy aimed at neutralizing and preventing threats to society and the state in the information area in general.

The article deals with the analysis of the legislative definition of the term «information security», on the basis of which the author has concluded that the solution to this issue is insufficient, except for the Strategy.

Based on the Strategy, the author has identified the place and role of information security actors, which include primarily public authorities, namely: the National Security and Defense Council of Ukraine, the Cabinet of Ministers of Ukraine, the Ministry of Culture and Information Policy of Ukraine and its subordinate body – the State Committee on Television and Radio Broadcasting of Ukraine, the Ministry of Defense of Ukraine, the Security Service of Ukraine, intelligence bodies of Ukraine, National Council of Ukraine on Television and Radio Broadcasting.

The conclusion is that the above list of actors (governmental) of information security will be incomplete if their activities are not aimed at cooperation with civil society institutions, including independent unions of journalists and other creative media workers, who, like no other, are most interested in the transparency and balance of state information policy with the creation of equal conditions for activities in this area.

*Keywords: information policy, information security, subjects, provision.*

УДК 343.73

DOI: 10.31733/2078-3566-2022-1-203-212



**Ельвіра СИДОРОВА**®

кандидат юридичних наук

(Дніпропетровський державний університет  
внутрішніх справ, м. Дніпро, Україна)

#### ХАРАКТЕРИСТИКА ПОВНОВАЖЕНЬ ВЕРХОВНОЇ РАДИ УКРАЇНИ ЩОДО ПОДАТКІВ І ЗБОРІВ

Розкрито особливості характеристики повноважень Верховної Ради України, що стосуються податкової сфери, можна безперечно констатувати її провідну роль в урегулюванні податкових відносин, що закріплено у відповідних конституційних положеннях і в окремих статтях Податкового кодексу України. Податкові повноваження вищого представницького органу державної влади відбиваються насамперед у його повноваженні законодавчо встановлювати систему оподаткування, податки і збори, що належить тільки йому й не може делегуватися іншим органам публічної влади або вирішуватись у порядку всенародного референдуму.

*Ключові слова: Верховна Рада України, податки, збори, суверенітет, податкові правовідносини, податкові повноваження, податкова компетенція.*

**Постановка проблеми.** Найвищим за своїм положенням у ієрархічній структурі органів публічної влади в Україні, законодавчим органом влади, первинним органом державної влади, що виражає волю всіх громадян України, є Верховна Рада України. Саме такій своїй природі парламент, найвищий представницький орган держави, зобов'язаний закріпленням за собою основоположної податкової компетенції будь-якого публічного територіального утворення, що полягає в його суверенному праві визначати правові механізми й установлювати податки і збори на всій території країни.

Як визначається у багатьох наукових роботах, право встановлювати податки і збори

© Е. Сидорова, 2022

ORCID iD: <https://orcid.org/0000-0002-1761-1583>

anelasidorova@ukr.net