



UDC 35.01; 23.04.44

DOI: [https://doi.org/10.32689/2617-2224-2019-4\(19\)-228-241](https://doi.org/10.32689/2617-2224-2019-4(19)-228-241)

Прав Роман Юрійович,

аспірант, Міжрегіональна Академія управління персоналом, 04071, м. Київ, вул. Почайнинська, 25/49, кв. 14, тел.: +38 (067) 471 15 55, e-mail: romapprav@gmail.com

ORCID: 0000-0001-8064-2836

Прав Роман Юрьевич,

аспірант, Межрегиональная Академия управления персоналом, 04071, г. Киев, ул. Почайнинская, 25/49, кв. 14, тел.: +38 (067) 471 15 55, e-mail: romapprav@gmail.com

ORCID: 0000-0001-8064-2836

Прав Роман Yuriyovich,

postgraduate student, Interregional Academy of Personnel Management, 04071, Kyiv, Str. Pochainynska, 25/49, 14, tel.: +38 (067) 471 15 55, e-mail: romapprav@gmail.com

ORCID: 0000-0001-8064-2836

НОРМАТИВНО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ І РЕАЛІЗАЦІЇ ПОЛІТИКИ ДЕРЖАВНОЇ БЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Анотація. Акцентовано увагу на питанні інформаційної безпеки України, що ускладнене відсутністю відповідної стратегії.

До важливих стратегічних документів у сфері інформаційної політики та державної безпеки належать “Стратегія розвитку інформаційного суспільства в Україні” (2013), у якій визначено пріоритети діяльності в галузі забезпечення інформаційної безпеки, “Стратегія кібербезпеки України” (2016). Метою цієї стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Визначено загрози кібербезпеці, національну систему кібербезпеки, основних суб’єктів забезпечення кібербезпеки, пріоритети та напрями забезпечення кібербезпеки України тощо. Законодавчо-нормативні акти щодо державної безпеки в інформаційній сфері можна поділити на

чотири блоки за рівнем узагальнення та конкретизації. 1-й блок складають концептуальні, доктринальні, стратегічні акти, які є основою забезпечення інформаційної безпеки; 2-й блок — закони України, що безпосередньо або опосередковано стосуються безпеки в інформаційній сфері; 3-й блок — підзаконні нормативні акти Верховної Ради і Кабінету Міністрів України і нормативні акти міністерств, інших органів виконавчої влади щодо безпеки в інформаційній сфері; виділено 4-й блок нормативних актів, які стосуються окупованих українських територій. Це, насамперед, стратегії щодо інформаційної реінтеграції окупованих територій — Донецької і Луганської областей, Криму. Визначено необхідність формування окремої інформаційної політики для окупованих і прилеглих регіонів та для іншої території України.

До інформаційної складової належить також нормативно-правові акти щодо забезпечення прав, свобод населення окупованих територій: Закон України “Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України” (2014), постанова ВРУ “Про Заяву Верховної Ради України щодо гарантії прав кримськотатарського народу у складі Української Держави” (2014), рішення РНБО “Про невідкладні заходи щодо захисту національних інтересів на Півдні та Сході України, у Чорному та Азовському морях і Керченській протоці” (2018).

Порушено питання проблеми регулювання у сфері інформаційної безпеки України: декларативність багатьох норм, відсутність законодавчо наданих повноважень відповідальних органів і механізмів координації діяльності тощо.

Ключові слова: державна безпека в інформаційній сфері, правові засади інформаційної безпеки, Доктрина інформаційної безпеки, узагальнення і конкретизація засад державної інформаційної безпеки.

НОРМАТИВНО-ПРАВОВЫЕ ОСНОВЫ ФОРМИРОВАНИЯ И РЕАЛИЗАЦИИ ПОЛИТИКИ ГОСУДАРСТВЕННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОЙ СФЕРЕ

Аннотация. Акцентируется внимание на вопросе информационной безопасности Украины, что затруднено отсутствием соответствующей стратегии.

К важным стратегическим документам в сфере информационной политики и государственной безопасности относятся “Стратегия развития информационного общества в Украине” (2013), в которой определены приоритеты деятельности в области обеспечения информационной безопасности, “Стратегия кибербезопасности Украины” (2016). Целью этой стратегии является создание условий для безопасного функционирования киберпространства, его использование в интересах личности, общества и государства. Определены угрозы кибербезопасности, национальная система кибербезопасности, основные субъекты обеспечения кибербезопасности, приоритеты и направления обеспечения кибербезопасности Украины и др. Законодательно-нормативные акты по государственной безопасности в информационной сфере

можно разделить на четыре блока по уровню обобщения и конкретизации. 1-й блок составляют концептуальные, доктринальные, стратегические акты, которые являются основой обеспечения информационной безопасности; 2-й блок — законы Украины, непосредственно или косвенно касающиеся безопасности в информационной сфере; 3-й блок составляют подзаконные нормативные акты Верховной Рады и Кабинета Министров Украины и нормативные акты министерств, других органов исполнительной власти, безопасности в информационной сфере; 4-й блок нормативных актов, которые касаются оккупированных украинских территорий. Это, в первую очередь, стратегии по информационной реинтеграции оккупированных территорий — Донецкой и Луганской областей, Крыма. Определена необходимость формирования отдельной информационной политики для оккупированных и прилегающих регионов, а также для другой территории Украины.

Информационной составляющей также являются нормативно-правовые акты по обеспечению прав, свобод населения оккупированных территорий: Закон Украины “Об обеспечении прав и свобод граждан и правовой режим на временно оккупированной территории Украины” (2014), постановление ВРУ “О Заявлении Верховной Рады Украины относительно гарантии прав крымскотатарского народа в составе Украинского государства” (2014), решение СНБО “О неотложных мерах по защите национальных интересов на Юге и Востоке Украины, в Черном и Азовском морях и Керченском проливе” (2018).

Затронут вопрос относительно проблем регулирования в сфере информационной безопасности Украины: декларативность многих норм, отсутствие законодательно предоставленных полномочий ответственных органов и механизмов координации деятельности и тому подобное.

Ключевые слова: государственная безопасность в информационной сфере, правовые основы информационной безопасности, Доктрина информационной безопасности, обобщение и конкретизация принципов государственной информационной безопасности.

REGULATORY AND LEGAL BASES FOR FORMATION AND IMPLEMENTATION OF THE STATE SECURITY POLICY IN THE INFORMATIONAL SPHERE

Abstract. The article emphasizes that the issue of information security of Ukraine is complicated by the lack of an appropriate strategy.

Important strategic documents in the field of information policy and state security also include: “Strategy for the development of the information society in Ukraine” (2013), which defines the priorities of activities in the field of information security; “Cyber security Strategy of Ukraine” (2016). The purpose of this strategy is to create conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state. The threats of cybersecurity, the national system of cybersecurity, the main subjects of cybersecurity, priorities and directions of ensuring cyber security of Ukraine and the like are defined.

Legislative and regulatory acts on state security in the information sphere can be divided into four blocks according to the level of generalization and concretization. The 1st block consists of conceptual, doctrinal, strategic acts, which are the basis of information security. The 2nd block consists of the laws of Ukraine, directly or indirectly related to security in the information sphere. The 3rd block consists of subordinate normative acts of the Verkhovna Rada and the Cabinet of Ministers of Ukraine and normative acts of ministries and other executive authorities on security in the information sphere. We have identified the 4th block of regulations; they relate to the occupied Ukrainian territories. It is, first and foremost, the strategy on the information the reintegration of occupied territories of Donetsk and Luhansk areas, the Crimea. We believe that it is necessary to form a separate information policy for the occupied and nearby regions, and for other territory of Ukraine.

The informational component also includes normative-legal acts on ensuring the rights and freedoms of the population of the occupied territories: the Law of Ukraine “On ensuring rights and freedoms of citizens and legal regime on the temporarily occupied territory of Ukraine” (2014), the decision of Parliament “On the Statement of the Verkhovna Rada of Ukraine on guarantees of the rights of the Crimean Tatar people within the Ukrainian State” (2014), the NSDC decision “On urgent measures for the protection of national interests in the South and East of Ukraine, in the Black and Azov seas and the Kerch Strait” (2018).

The article highlights the problems of regulation in the field of information security of Ukraine: the declarative nature of many rules, the lack of legislative authority of the responsible authorities and mechanisms of coordination of activities and the like.

Keywords: state security in the information sphere, the legal basis of information security, the Doctrine of information security, generalization and specification of the principles of state information security.

Постановка проблеми. В епоху постійного пришвидшення розвитку інформація, безумовно, вона є вирішальним фактором для досягнення успіху в усіх сферах діяльності.

В Україні “право на інформацію охороняється законом. Держава гарантує всім суб’єктам інформаційних відносин рівні права і можливості доступу до інформації. Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків,

передбачених законом”. “Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів” (закон “Про інформацію”) [1]. Також у законі “Про інформацію” містяться положення про неприпустимість зловживання правом на інформацію: “Інформація не може бути використана для закликів до повалення конституцій-

ного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини” [1].

Отже, інформація є вигодою, яка має бути захищена певним чином, особливо коли йдеться про інформацію в обороні держави або інших її сферах, де розкриття відомостей загрожувало б стратегічним інтересам. Узгодження цих двох аспектів (вільного доступу до інформації та її захисту) не є однозначним, оскільки концепція безпеки в інформаційній сфері однаково стосується держави як інституції, суспільства та окремих громадян, які їх формують.

Наша країна не має стратегії державної інформаційної безпеки, водночас її елементи можна знайти в різних джерелах. Актуальним завданням є аналіз масиву нормативно-правових актів у цій сфері.

Державну безпеку в інформаційній сфері можна розглядати з кількох сторін, а саме: як забезпечення захисту прав громадян на вільний доступ до інформації і свободу слова; як захист громадян від впливу спотвореної, неповної, хибної інформації, маніпулятивного інформаційного впливу; як захист приватної чи державної значущої інформації від неправомірних посягань з боку людей, державних чи приватних структур, у тому числі іноземних.

Аналіз останніх досліджень і публікацій. Серед останніх досліджень відмітимо публікацію Я. Малик (2015), в якій автор розглядає стан та перспективи розвитку інформа-

ційної безпеки України [2]. В. Савицький (2017) досліджує інформаційну безпеку в системі національної безпеки України [3].

Мета статті — проаналізувати правові основи формування і реалізації політики державної безпеки України в інформаційній сфері, спробувати структурувати нормативно-правові акти цієї сфери у певну систему, виокремили недоліки та проблеми.

Виклад основного матеріалу. У розвитку людства інформація завжди відігравала важливу роль, але останнім часом її значення зросло неймовірно. Саме доступ до інформації та здатність її використовувати нині визначає можливості досягнення успіху в багатьох галузях. Сьогодні інформаційні ресурси розглядаються як не менш важливі, ніж демографічні, сировинні або енергетичні ресурси, є основою функціонування багатьох видів людської діяльності, таких як управління, економіка, політика, соціальна і культурна сфери, національна безпека, оборона та міжнародні відносини.

Однак інформація перестає бути цінністю, якщо вона не може бути збережена, вибрана, виділена, передана, розповсюджена і зрозуміла. Саме тому інформація стає цінною лише тоді, коли вона доступна для людей, яким потрібна і в потрібному місці. В іншому випадку вона може бути не тільки марною, але й небезпечною.

Цінною є корисна інформація, тобто яка об'єктивно або суб'єктивно підвищує рівень знань людини у певній сфері (збільшує знання). Також фактичну корисність інфор-

мації визначає її точність, повнота і вчасність, тобто надходження її до одержувача в потрібний час і в потрібних обсягах, що дозволить йому прийняти правильне рішення. Крім того, інформація повинна бути реальною (надійною), доступною, позбавленою спотворень та невизначеності.

Право доступу до інформації, її збір та розповсюдження в даний час розглядаються як одне з основних прав людини і громадянина, є її невід'ємним атрибутом, підтверджує гідність людської особи як суб'єкта громадянського суспільства і становить основу демократії. Можна навіть стверджувати, що держава, яка не гарантує своїм громадянам вільний доступ до інформації, рано чи пізно зазнає деградації, це приведе до відмови від засад плюралізму, толерантності та відкритості, без яких неможливо уявити демократичне суспільство.

Право на інформацію було сформульовано вже в 1948 році у Декларації прав людини, прийнятій Генеральною Асамблеєю ООН. Дещо ширша ідея права на комунікацію, що впливає з інших прав людини, вперше була сформульована разом з Концепцією громадянського суспільства. Її творцем був Жан д'Арсі, директор інформаційного офісу ООН. Міжнародний пакт про громадянські та політичні права, ратифікований Україною в 1973 р., також включає право мати і висловлювати власні погляди, а також збирати, отримувати і поширювати інформацію. Це право може бути обмежене лише законом. Положення про доступ до інформації також можна знайти в

інших актах міжнародного права, таких як Європейська конвенція з прав людини або Хартія основних прав Європейського Союзу. У 1990-х роках принципи відкритості, прозорості та доступу до документів були включені до існуючих рішень ЄС.

У вітчизняному законодавстві право на інформацію, особливо про діяльність органів державної влади, як і будь-яку іншу, закріплено в Конституції. Так, ч. 1 ст. 34 Основного закону "Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань". У ч. 2 ст. 34 передбачено право кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб [4]. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [4].

Також ст. 32 Конституції передбачає право громадян знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною таємницею або іншою захищеною законом інформацією [4].

Розвиток цих прав міститься в законодавчих актах України, зокрема в законі "Про доступ до публічної інформації", що регулює суб'єктивний і об'єктивний обсяг і спосіб от-

римання інформації про діяльність державних органів (2011, нова редакція 2015 р.) [5], та новій редакції Закону “Про інформацію”, що закріпив “право кожного на інформацію”, “забезпечення доступу кожного до інформації”, принцип максимальної відкритості інформації, крім інформації з обмеженим доступом [1]. Окрім того, в Законі “Про інформацію” містяться інші положення, важливі для реалізації права на доступ до інформації, а саме: 1) дозвіл на поширення інформації з обмеженим доступом, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу; 2) право громадськості знати цю інформацію переважає потенційну шкоду від її поширення (ч. 1. ст. 29) [1]. У цих законах, відповідно до змін, вже не встановлюється, як раніше, помилкова концепція права власності на інформацію в цілому і права власності держави на інформацію зокрема.

Міжнародні норми щодо свободи слова і преси відображені у ст. 15 Конституції України – “Цензура заборонена” [4]. У свою чергу, ми знаходимо розширення конституційного принципу свободи слова і висловлювань в законі “Про друковані засоби масової інформації (преса) в Україні” [5].

Хоча право на інформацію вважається одним з основних прав людини, можливе його обмеження, наприклад, з метою забезпечення громадського порядку, безпеки, дотримання моральності, протидії наклепам, шахрайству, маніпуляції, захисту інших прав. Незалежно від того, які причини ці обмеження завжди викликають суперечки або й опір,

тому що багато людей сприймає це як втручання в основні громадянські права і свободи.

Обмеження права на інформацію виникає в першу чергу через ризики, пов’язані з неправильним використанням інформації або її використанням сторонніми особами. Беручи до уваги важливість інформації для сучасних людей, суспільств, держав і міжнародної спільноти, безперечно, що на додаток до очевидних переваг, які можуть бути досягнуті завдяки інформації, вона також може піддаватися загрозам, які виникають під впливом різних факторів.

Загрози в інформаційній сфері: несанкціоноване розкриття, асиметрія в міжнародному обміні інформацією, шпигунство, кіберпосягання, кіберзлочинність, нестача інформації, “інформаційний хаос”, дезінформація, інформаційна боротьба (війна), маніпулювання інформацією. Маніпулювання інформацією – це і надання неправдивої інформації, і зменшення важливості інформації, заангажована вибірковість інформації, її неоднозначність і надлишок, що викликає “інформаційний хаос”.

З точки зору безпеки держави найбільшою загрозою у сфері інформації вважаються інформаційні війни. Ми їх сприймаємо як загрози, конфлікти, в яких інформація є як ресурсом, об’єктом нападу, так і зброєю, не виключене і фізичне знищення інформаційної інфраструктури, що здійснюється супротивником. Ця боротьба може мати дві мети: знищення інформаційних ресурсів противника і забезпечення власної безпеки. Зазвичай це здійснюється за допомогою таких інструментів:

вплив на політичні чи культурні процеси; інформаційно-психологічні кампанії; дезінформація та вплив на ЗМІ; дипломатія; проникнення у комп'ютерні мережі і бази даних.

Інформаційна війна не обов'язково означає перебування держави в стані фактичної війни, така діяльність відбувається і в мирні часи. Дії вживаються не тільки для отримання інформації, але й для спричинення заворушень, урядових криз. Будучи заміною відкритої агресії, вони можуть скомпрометувати державу або її владу на міжнародній арені, підірвати її політичний авторитет або дискредитувати в економічній сфері. Ця боротьба стосується не тільки військової сфери, а й цивільної. Вона ведеться відкритим або таємним шляхом, це збройна боротьба, але в крайніх випадках вона може привести до фізичного знищення об'єкта. Це універсальна боротьба тому, що вона здійснюється у всіх сферах діяльності держави, а не тільки у військовій. Вона може мати форму політичного, військового та економічного тиску, а також залякування. Вона проводиться не тільки в сфері кібернетичного впливу на бази цифрових зашифрованих даних, а й, насамперед, шляхом поширення негативної реальної або помилкової інформації, наприклад, для створення конкретних соціальних настроїв. У цих заходах, часто несвідомо, беруть участь засоби масової комунікації, які оприлюднюючи сенсації, є в даний час найбільш ефективним інструментом в інформаційній боротьбі. Весь перелічений арсенал використовує Росія у війні проти України.

Ст. 17 Конституції проголошує: “Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу” [4]. Таким чином, держава вважає не лише можливістю, але й своїм обов'язком захистити громадян України від інформаційних загроз.

Зважаючи на сучасний воєнно-політичний стан України, яка перебуває в умовах гібридної війни з Росією, передбачаючи також майбутні загрози з боку агресора, важливо створити таку систему державної безпеки в інформаційній сфері, яка б забезпечила надійний захист держави і народу.

Затверджена “Доктрина інформаційної безпеки України” є відповіддю на сучасні загрози національній безпеці. “Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни” [5]. У Доктрині означено національні інтереси України (особи, суспільства і держави) в інформаційній сфері, актуальні загрози національним інтересам та національній безпеці України, пріоритети державної політики в інформаційній сфері та механізм реалізації Доктрини.

Як бачимо, у Доктрині викладено лише концептуальні засади інформаційної безпеки. Питання реалізації інформаційної безпеки України ускладнене відсутністю відповідної стратегії. Стратегія безпеки в інфор-

маційній сфері розглядається в рамках Стратегії національної безпеки України [5]. Зважаючи на те, що прямого визначення поняття безпеки в інформаційній сфері у законодавчих актах України немає, її можна сприймати як стан, який досягається після виконання певних умов. Ці умови визначено у Стратегії національної безпеки України. Отже, стан інформаційної безпеки слід розглядати як стан, коли:

- забезпечено наступальність заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і виявів інформаційної агресії;

- створено інтегровану систему оцінки інформаційних загроз та оперативного реагування на них;

- існує протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства;

- розроблена і реалізується скоординована інформаційна політика органів державної влади;

- виявлено суб'єктів українського інформаційного простору, що використовуються Росією для ведення інформаційної війни проти України, та унеможливлено їхню підривну діяльність тощо [5].

До важливих стратегічних документів у сфері інформаційної політики та державної безпеки належать також: “Стратегія розвитку інформаційного суспільства в Україні” (2013), у якій визначено пріоритети діяльності в галузі забезпечення інформаційної безпеки; “Стратегія

кібербезпеки України” (2016). Метою цієї стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Визначено загрози кібербезпеці, національну систему кібербезпеки, основних суб'єктів забезпечення кібербезпеки, пріоритети та напрями забезпечення кібербезпеки України тощо [5].

Загалом законодавчо-нормативні акти щодо державної безпеки в інформаційній сфері за рівнем узагальнення і конкретизації визначених у них засад можна поділити на чотири блоки (рисунок).

1-й блок складають концептуальні, доктринальні, стратегічні акти, які є основою забезпечення інформаційної безпеки. Це “Стратегія національної безпеки України”, “Доктрина інформаційної безпеки України”, “Стратегія кібербезпеки України”, “Стратегія розвитку інформаційного суспільства в Україні”, “Національна стратегія у сфері прав людини” (2015), також “Концепція Національної програми інформатизації” (остання редакція 2013 року), “Воєнна доктрина України” (нова редакція 2015 року) [5].

У 2-му блоці – закони України – можна виділити їх чотири групи:

- Закони, що безпосередньо стосуються безпеки в інформаційній сфері: “Про інформаційну безпеку України”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про основні засади забезпечення кібербезпеки України”, також закони “Про основи національної безпеки України”, “Про недержавне забезпечення національної

безпеки України”. Вважаємо що до цього блоку з повним правом можна віднести закон “Про забезпечення функціонування української мови як державної”, ухвалений 25 квітня 2019 р. Верховною Радою України;

- Закони що стосуються свободи інформації й інформатизації суспільства: “Про інформацію”, “Про доступ до публічної інформації”, “Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки”, “Про Суспільне телебачення і радіомовлення України”

(2014), “Про друковані засоби масової інформації (пресу) в Україні”, “Про Національну програму інформатизації” (остання редакція 2016 року);

- Закони про статус і засади діяльності державних органів по захисту та протидії інформаційній небезпеці: “Про службу безпеки України”, “Про Раду національної безпеки і оборони України”, “Про Державну службу спеціального зв’язку та захисту інформації України” (2015), “Про розвідувальні органи України”,

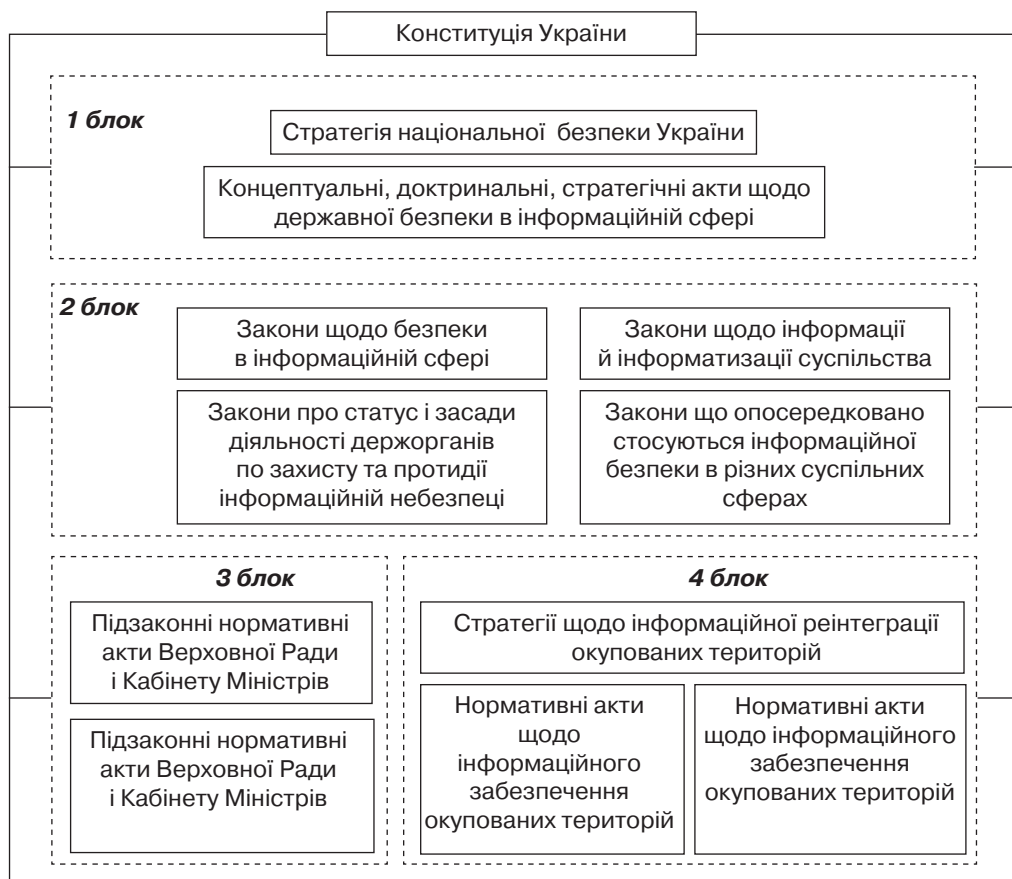


Рис. Структурування законодавчо-нормативних актів за рівнем узагальнення і конкретизації визначених у них засад щодо державної безпеки в інформаційній сфері

“Про Національну поліцію” (2015). Сюди ж віднесемо “Положення про Міністерство оборони України”, затверджене Постановою Кабінету Міністрів (2014);

- Закони що опосередковано стосуються інформаційної безпеки в різних суспільних сферах: “Про засади внутрішньої і зовнішньої політики” (2010), “Про державну таємницю”, “Про санкції” (2014), “Про боротьбу з тероризмом”, “Про контррозвідувальну діяльність”, “Про оборону України”, “Про державну охорону органів державної влади України та посадових осіб” (1998). Кримінальний, Цивільний, інші кодекси України, які мають відношення до регулювання відносин у сфері національної безпеки, отже, й інформаційної.

До 3-го блоку відносимо підзаконні нормативні акти Верховної Ради і Кабінету Міністрів (постанови, укази, розпорядження). Щодо безпеки в інформаційній сфері це: постанови ВРУ “Рекомендації парламентських слухань на тему: “Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України” (2016), “Рекомендації парламентських слухань на тему: “Законодавче забезпечення розвитку інформаційного суспільства в Україні” (2014); укази Президента України “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України (2014), “Про сприяння розвитку громадянського суспільства в Україні” (2016), “Концепція розвитку сектору безпеки і оборони України” (2016), “Про заходи щодо розвитку національної складової глобальної інформаційної

мережі Інтернет та забезпечення” (2000); Постанови КМУ “Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів” (2018), “Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави” (2016).

Також до 3-го блоку відносимо нормативно-правові акти міністерств, інших органів виконавчої влади, які на основі чинного законодавства й у межах своєї компетенції видають відомчі нормативні акти щодо безпеки в інформаційній сфері (накази, рішення, інструкції, положення, постанови, програми тощо). Наприклад, рішення Ради національної безпеки і оборони України “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” (2014) і “Про удосконалення заходів забезпечення захисту об’єктів критичної інфраструктури” (2016), наказ Служби безпеки України “Про затвердження Зводу відомостей, що становлять державну таємницю” (2005), рішення Нацради телерадіомовлення “Про затвердження Плану розвитку національного теле-радіо-інформаційного простору” (2010, в редакції 2018), накази Міністерства оборони “Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України” (2017) і “Реєстр електронних інформаційних ресурсів Міністерства оборони України” (2015).

Виділено 4-й блок нормативно-правових актів, які стосуються

окупованих українських територій. Це, в першу чергу, стратегії щодо інформаційної реінтеграції окупованих територій. У липні 2018 р. була затверджена “Стратегія інформаційної реінтеграції Донецької та Луганської областей”. Метою Стратегії є: реалізація інформаційних прав і свобод людини і громадянина, підвищення рівня підтримки громадянами України державної політики у сфері інформаційної реінтеграції тимчасово окупованих територій у Донецькій та Луганській областях; впровадження ефективного механізму для забезпечення доступу громадян України, які проживають на тимчасово окупованих територіях у Донецькій та Луганській областях, а також прилеглих до них територіях, до загальноукраїнського інформаційного простору [5].

Реалізація Стратегії розрахована на період до 2020 р. Досягнення мети Стратегії потребує виконання таких завдань: протидія використанню Російською Федерацією інформаційних технологій, спрямованих на розпалювання національної та релігійної ворожнечі, пропаганду війни, насильницьку зміну конституційного ладу України, порушення територіальної цілісності та суверенітету України; зміцнення почуття спільності між громадянами України, які проживають на тимчасово окупованих територіях у Донецькій та Луганській областях, прилеглих до них територіях, а також громадянами України, які проживають в інших регіонах України; створення умов для задоволення потреб населення тимчасово окупованих територій в об’єктивній, оперативній і достовірній інформації тощо [5].

У грудні 2018 р. була схвалена “Стратегія інформаційної реінтеграції Автономної Республіки Крим та м. Севастополя”. Метою цієї Стратегії є забезпечення інформаційної реінтеграції окупованої території України (Автономної Республіки Крим та м. Севастополя), створення інформаційними інструментами передумов для відновлення територіальної цілісності та суверенітету України. Реалізація Стратегії передбачає виконання таких завдань: реалізація державної інформаційної політики щодо АР Крим та м. Севастополя за принципом “єдиного голосу”; утвердження в українському та міжнародному інформаційному просторі стратегічних наративів обов’язкового відновлення територіальної цілісності України; здійснення постійного моніторингу інформаційного простору окупованої території України, збору, накопичення, систематизації, аналізу, оцінки отриманої інформації та обміну нею з метою оперативного реагування відповідними органами державної влади на дії Російської Федерації; інформування громадян України, іноземців про ситуацію в АР Крим; спростування ідеологем російської пропаганди щодо минулого та сучасного Криму, які поширюються в українських та іноземних засобах масової інформації; мобілізація інформаційними інструментами міжнародної підтримки відновлення територіальної цілісності України та інші [5].

Крім того, були прийняті інші нормативні акти щодо інформаційного забезпечення окупованих територій. Це, зокрема, рішення Національної ради телерадіомовлення

“Про мовлення телерадіоорганізацій на території проведення антитерористичної операції” (2014), наказ Держкомтелерадіо України “Про заходи щодо збереження державними телерадіокомпаніями мовлення для задоволення інформаційних потреб національних меншин та осіб, які проживають на тимчасово окупованих територіях” (2015).

Інформаційну складову включають також нормативно-правові акти щодо забезпечення прав, свобод населення окупованих територій: Закон України “Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України” (2014), постанова ВРУ “Про Заяву Верховної Ради України щодо гарантії прав кримськотатарського народу у складі Української Держави” (2014), рішення РНБО “Про невідкладні заходи щодо захисту національних інтересів на Півдні та Сході України, у Чорному та Азовському морях і Керченській протоці” (2018).

Отже, слід на державному рівні формувати особливу інформаційну політику для окупованих та прилеглих регіонів, і для іншої території України. Відштовхуватися потрібно від тих акцентів, які важливі для населення конкретних територій. Для жителів Донбасу це один акцент, для кримчан — інший. Потрібно сформулювати цілі, завдання, ресурси й інструментарій для реалізації цих завдань і досягнення цілей.

Висновки і перспективи подальших досліджень. Проведений аналіз показав, що нормативно-правова база сфери державної інформаційної безпеки досить значна і розгалужена, але не позбавлена значних проблем.

Проблемою регулювання у сфері інформаційної безпеки України, втім, як й інших сфер державного регулювання, є невідповідність між нормативно-правовим забезпеченням та практичною реалізацією визначених кроків, декларативність багатьох норм. Органи, які визначені відповідальними за реалізацію політики державної безпеки в інформаційній сфері, мають ще й отримати законодавчо визначені повноваження і механізми координації. Це стосується, в першу чергу, Ради національної безпеки та оборони України й Міністерства інформаційної політики, а також інших органів.

Ще одним аспектом, який потребує додаткового дослідження, є доцільність відокремлення кібернетичної безпеки від інформаційної у нормативно-правових актах. Необхідне також нормативне узгодження діяльності державних і громадських структур у сфері інформаційної безпеки України, особливо тих, що вже діють (“Академія національної безпеки”, “Стоп-фейк”, “Інформаційний опір”, “Інформанапалм”, “Разом” тощо).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про інформацію. Закон України від 02.10.1992 № 2657-XII, поточна редакція від 01.01.2017. URL : <https://zakon.rada.gov.ua/laws/main/2657-12>
2. *Малик Я.* Інформаційна безпека України: стан та перспективи розвитку // Збірник наукових праць. 2015. Вип. 44 “Ефективність державного управління”. С. 13–20.
3. *Савицький В. Т.* Інформаційна безпека в системі національної безпеки

- України // Університетські наук. записки. 2017. № 62. С. 195–207.
4. Конституція України: від 28.06.1996 № 254к/96-ВР. URL : <https://zakon.rada.gov.ua/laws/main/254к/96-вр>
 5. Законодавство України. Верховна Рада України. URL : <https://zakon.rada.gov.ua/laws/>

REFERENCES

1. VRU (1992) Pro informaciju. [About the information], *Zakon Ukrainy* 02.10.1992 № 2657-XII, redakcija 01.01.2017 URL: <https://zakon.rada.gov.ua/laws/main/2657-12>
2. Malyk Ja. (2015). Informacijna bezpeka Ukrainy: stan ta perspektyvy rozvytku [Information security of Ukraine: the state and prospects of development]. *Zbirnyk naukovykh pracj "Efektyvnistj derzhavnogho upravlinnja"* – *Collection of scientific works "Efficiency of Public Administration"*, 44, 13–20 [in Ukrainian].
3. Savycjkyj V. T. (2017). Informacijna bezpeka v systemi nacionaljnoji bezpeky Ukrainy [Information security in the system of national security of Ukraine]. *Universytetsjki naukovy zapysky – University scientific notes*, 62, 195–207 [in Ukrainian].
4. Konstytucija Ukrainy [Constitution of Ukraine] 28.06.1996 № 254к/96-ВР. URL : <https://zakon.rada.gov.ua/laws/main/254к/96-вр>
5. Zakonodavstvo Ukrainy. Verkhovna Rada Ukrainy [Legislation of Ukraine. Verkhovna Rada of Ukraine]. URL : <https://zakon.rada.gov.ua/laws/>