Keywords: bank, determination of persons related to a bank, measures of influence, the National Bank of Ukraine, violation of banking legislation.

Петровська І.І.

ПРАВОВІ ЗАСАДИ ПУБЛІЧНОГО КОНТРОЛЮ ЗА ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УКРАЇНІ

УДК 342.95:004.056

Перед сучасною державою постає багато завдань, основними серед яких є вирішенням проблем національної безпеки, цивільного захисту, соціальних та економічних проблем. Ефективне прогнозування, планування (вироблення напрямків політичного розвитку) та реалізація правових норм є основою для правової, соціальної, демократичної держави в сучасному інформаційному суспільстві. Інформаційна діяльність публічних осіб є основою забезпечення національної безпеки та територіальної цілісності України. Тому розгляд законодавства, яке стосується інформаційній безпеки є актуальним і важливим.

Державний контроль, як інститут адміністративного права, досліджували В. Авер'янов, С.Алексєєв, О.Андрійко, Д.Бахрах, І. Бачило, Ю.Битяк, А.Васильєв, В.Гаращук, І.Голосніченко, С.Гончарук, Є.Додін, В.Олефір, В.Зуй, Р.Калюжний, Л.Коваль, В.Колпаков, А.Комзюк, О.Коренєв, Б.Лазарєв, І.Мартьянов, Н. Нижник, О.Остапенко, І.Пахомов, В.Пєтков, А.Селіванов, Ю.Тихомиров, М.Тищенко, В.Чиркін, В.Шкарупа та інші. Інформаційні правовідносини також аналізувались науковцями, зокрема: О. Бандурко, К. Беляков, Н. Бєляєв, А. Венгеров, В. Іванов, А. Куліш, О. Синєокий, М. Танчинець, Ю. Тихомиров тощо, проте на сьогодні питання інформаційної безпеки та правових засобів її забезпечення потребує детального вивчення та вдосконалення.

Метою даного дослідження є характеристика правових засад публічного контролю за інформаційною безпекою України.

Публічно-правова підсистема права України, що охоплює публічні галузі права, предметом регулювання яких є суспільні відносини публічної сфери та взаємодія суб'єктів приватного

права з суб'єктами публічного права, на сьогодні зазнає реформування та змін в наукових підходах щодо визначень основних категорій та їх місця в системі права. Дане положення стосується і публічного контролю, специфіка законодавчих визначень видів якого залежить від сфери правового застосування. Наприклад, Буханевич А. визначає публічний контроль як важливий інструмент демократичного суспільства, покликаний оптимізувати систему діяльності органів публічної влади в сучасних умовах суспільно-політичного розвитку [1, с. 31]. Кравчук В. зазначає, що по-перше, публічний контроль у державі – це система організаційно-правових форм забезпечення додержання законності у діяльності публічної адміністрації, прав і свобод людини, ефективного виконання повноважень і завдань органами державної влади, місцевого самоврядування, їх посадовими і службовими особами; по-друге, цілком обґрунтовано публічний контроль класифікувати за суб'єктами його реалізації на: державний, громадський, муніципальний та міжнародний [2]. Різновидом такого контролю за сферою здійснення є публічний контроль за інформаційною безпекою в державі. А інформаційна безпека є частиною національної безпеки. Загалом, інформаційну діяльність органів публічної влади можна визначити як сукупність дій щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації, що реалізуються органами державної влади, органами місцевого самоврядування, іншими суб'єктами, що здійснюють владні управлінські функції в межах їх компетенції, у тому числі на виконання делегованих повноважень, спрямованих на задоволення як власних інформаційних потреб та інформаційних потреб сторонніх осіб [3, с.35].

Основною категорією, на основі якої виникають і змінюються відносини у сучасному суспільстві є інформація. Інформація є одним із найбільш загальних понять науки, що означає деякі відомості, сукупність певних даних та/або знань [4, с.24]. Інформаційною визнається виключно така діяльність, що спрямована на задоволення інформаційних потреб різноманітних суб'єктів, головний зміст якої полягає у збиранні, зберіганні, використанні та поширенні інформації [4, с.49]. Закон «Про інформацію»

[5] визначає її як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Цей ж закон [5], у статті 2, зазначає, що основними принципами інформаційних відносин є гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя. У законодавстві України визначено також основні напрямами державної інформаційної політики (буквально термін «політика» (від грец. politike) означає державну діяльність або державні, суспільні справи, з якими пов'язані загальні засади політичної культури [4 с.35]), а саме: забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України; сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору [5].

Один з напрямків інформаційної діяльності щодо забезпечення національної безпеки можна охарактеризувати як інформаційна війна (заходи та методи протидії інформаційній війні Росії). Мета інформаційної війни – послабити моральні і матеріальні сили супротивника або конкурента та зміцнити власні [6, с.136]. Горбань Ю. виділяє такі основні методи інформаційної агресії проти України: (1) дезінформування та маніпулювання; (2) пропаганда; (3) диверсифікація громадської думки; (4) психологічний та психотропний тиск; (5) поширення чуток [6, с.138]. Тому надзвичайно актуальними стають науково-практичні дослідження щодо розробки нових тактик, стратегій, доктрин державного

управління в царині захисту інформаційного простору держави [6, с.140]. Політика безпеки інформаційно-телекомунікаційних технологій включає правила, директиви та практику, що визначають засоби управління, захисту та розподілення активів, у тому числі критичної інформації, в інформаційних мережах [4, с.37].

Інформаційна діяльність органів влади – це специфічна професійна діяльність службовців державних органів влади, спрямована на забезпечення власної функціональної діяльності, інформаційну взаємодію з іншими органами влади, об'єднаннями громадян, юридичними та фізичними особами та організацію доступу до публічної інформації [7, с.81]. Для повноти характеристики доцільно додати до цього визначення також і охорону та захист інформації. При цьому, в сучасних умовах, варто охороняти й захищати на рівні держави не тільки інформацію з обмеженим доступом, а і масову інформацію, яка впливає на світогляд українців (зокрема щодо таких вимог до неї як достатність для об'єктивної істини та правдивість). В нормативних актах України закріплено поняття «офіційна інформація органів державної влади та органів місцевого самоврядування» [8]. Це офіційна документована інформація, створена в процесі діяльності органів державної влади та органів місцевого самоврядування, яка доводиться до відома населення в порядку, встановленому Конституцією України [9], законами України «Про інформацію» [5] та «Про доступ до публічної інформації» [10], Законом [8]. При здійсненні інформаційної діяльності учасники публічно-правових інформаційних відносин несуть відповідальність за порушення встановлених законодавством України правових режимів інформації, правил застосування інформаційно-комунікаційних технологій в діяльності органів публічної адміністрації, процедур захисту інформації з обмеженим доступом. Зокрема, адміністративні інформаційні правопорушення вчиняються через невиконання або неналежне виконання посадовими особами покладених на них обов'язків, у тому числі делегованих повноважень, що виключає можливість вчинення таких деліктів особами, які не мають спеціального статусу. Також, посадові особи як спеціальні суб'єкти адміністративних інформаційних правопорушень, визнаються такими, що вчи-

нили правопорушення, якщо не доведуть правомірність власних рішень, дій чи бездіяльності. Посадові особи органів публічної адміністрації можуть визнаватися суб'єктами адміністративних інформаційних правопорушень не лише за рішення, дії, вчинені на виконання посадових та службових обов'язків, а й за участь у прийнятті колегіальних рішень від імені органів публічної адміністрації [11, с.137].

При розгляді мети інформаційної діяльності публічних службовців щодо забезпечення інформаційної безпеки, яка є складовою національної безпеки, остання визначається як захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз [12]. Даний Закон «Про національну безпеку України», у статті 31, містить положення щодо стратегії кібербезпеки України. Кібербезпека є частиною інформаційної безпеки. Інформаційна безпека стосується інформації в цілому, а кібербезпека – інформації в ІТ системах. Зазначено, що ця стратегія є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб'єктів забезпечення кібербезпеки, насамперед суб'єктів сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів. Організація підготовки Стратегії кібербезпеки України здійснюється за дорученням Президента України Національним координаційним центром кібербезпеки після затвердження Стратегії національної безпеки України. Стратегія кібербезпеки України схвалюється рішенням Ради національної безпеки і оборони України та затверджується указом Президента України, є осно-

вою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України. Реалізація цієї стратегії здійснюється на основі національного оборонного, безпекового, економічного, інтелектуального потенціалу з використанням механізмів державно-приватного партнерства, а також із залученням міжнародної консультативної, фінансової, матеріально-технічної допомоги [12]. Стратегія кібербезпеки України - документ довгострокового планування, що визначає загрози кібербезпеці України, пріоритети та напрями забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави (ст.1 Закону «Про національну безпеку»). Про необхідність розробки стратегії інформаційної/кібербезпеки науковці говорили протягом тривалого часу. Тому передбачення таких положень у законодавстві є позитивним кроком. Варто якнайскоріше її розробити та почати впроваджувати.

Серед заходів кібербезпеки варто окрему увагу приділити з запобіганню правопорушенням у даній сфері, зокрема кіберзлочинам, оскільки вони є суспільно-небезпечними діяннями, які трансформуються із звичайних злочинів під впливом виникнення і розвитку ІТ, посягають на комунікації та інші суспільні відносини, які здійснюються при посередництві комунікацій і спрямовуються на комп'ютерні системи, завдають шкоди їм та інформаційним даним [13, с.251].

Загрози національній безпеці України нормативно визначено як явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України. А національні інтереси України – це життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян [12]. Серед спеціалізованих суб'єктів забезпечення інформаційної безпеки варто виділити Державну служба спеціального зв'язку та захисту інформації України, яка є державним органом, призначеним для забезпечення функціонування і роз-

витку державної системи урядового зв'язку, національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону (стаття 22 Закону «Про національну безпеку»).

Варто погодитись з твердженням, що розвиток технологій, зокрема телекомунікаційних систем та електроніки, привів до надзвичайно швидкого зростання комунікаційних можливостей. Це є викликом не тільки для підприємців, які дбають про свої власні інтереси, але й для держави, яка повинна побудувати ефективну правову систему для захисту від шпигунських дій [14, с.293].

У межах повноважень, наданих відповідно до законодавства України, сектор безпеки і оборони підлягає демократичному цивільному контролю. Система демократичного цивільного контролю складається з контролю, що здійснюється Президентом України; контролю, що здійснюється Верховною Радою України; контролю, що здійснюється Радою національної безпеки і оборони України; контролю, що здійснюється Кабінетом Міністрів України, органами виконавчої влади та органами місцевого самоврядування; судового контролю; громадського контролю [12]. Він здійснюється за принципами верховенства права, законності, підзвітності, прозорості, ефективності та результативності.

Предметом демократичного цивільного контролю є: (1) дотримання вимог Конституції і законів України у діяльності органів сектору безпеки і оборони, недопущення їх використання для узурпації влади, порушення прав і свобод людини і громадянина; (2) зміст і стан реалізації стратегій, доктрин, концепцій, державних програм та планів у сферах національної безпеки і оборони; (3) стан правопорядку в органах сектору безпеки і оборони, їх укомплектованість, оснащеність сучасним озброєнням, військовою і спеціальною технікою, забезпеченість необхідними запаса-

ми матеріальних засобів та готовність до виконання завдань за призначенням у мирний час та в особливий період; (4) ефективність використання ресурсів, зокрема бюджетних коштів, органами сектору безпеки і оборони [12].

Органи місцевого самоврядування та інші органи публічної влади здійснюють свої функції із забезпечення національної безпеки у взаємодії з органами, які входять до складу сектору безпеки і оборони.

Отже, в правових актах України визначено напрямки державної політики, публічних посадовців, основні методи забезпечення національної безпеки та її виду – інформаційної безпеки. Державна політика з національної безпеки спрямовується на забезпечення державної, економічної, інформаційної, воєнної, зовнішньополітичної, екологічної безпеки, кібербезпеки України на основі реалізації відповідних стратегій, правових актів інформаційної сфери. За правозастосовчою діяльністю в сфері інформаційної безпеки (як і національної безпеки) здійснюється демократичний цивільний контроль (який є видом публічного контролю).

1. *Буханевич А.І. Публічний контроль у контексті сучасних дослідницьких підходів. Вісник Національної академії державного управління, 2009.№1(5). С. 26-32. URL: http://visnyk.academy.gov.ua/wp-content/uploads/2013/11/2009-1-5.pdf (дата звернення: 15.05.2019).*
2. *Кравчук В.М. Поняття та зміст публічного контролю в сучасній державі. Актуальна юриспруденція: юридичні науково-практичні Інтернет конференції. 08.10.14. URL: http://legalactivity.com.ua/index.php?option=com_content&view=article&id=930%3A131014-13&catid=108%3A6-1014&Itemid=133&lang=ru (дата звернення: 15.05.2019)*
3. *Танчинець М.М. Поняття, зміст та види інформаційної діяльності органів публічної влади України. Науковий вісник Ужгородського національного університету. Серія право. Випуск 39. Том 2. 2016. С.31-35. URL: http://www.visnyk-juris.uzhnu.uz.ua/file/No.39/part_2/8.pdf (дата звернення: 11.04.2019).*
4. *Синєокий О.В. Інформаційне право України та електронне право високих технологій: електронний курс лекцій українською мовою. Запоріжжя : ЗНУ, 2010. 215 ел. с http://www.kul-lib.narod.ru/bibl.files/ILaw/10sovipu.pdf (дата звернення: 11.04.2019).*

5. *Про інформацію: Закон України від 2 жовтня 1992 року №2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 11.04.2019).*
6. *Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. Вісник Національної академії державного управління при Президентові України. №1. 2015. С. 136-141. URL: http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Vnadu_2015_1_21.pdf (дата звернення: 11.04.2019).*
7. *Дорогих С.О. Сутність та визначення понять «інформаційна діяльність» та «інформаційна діяльність органів влади». Інформація і право. №3(9). 2013. С.74-82*
8. *Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації: Закон України від 23.09.97 р. № 539/97-ВР. URL: https://zakon.rada.gov.ua/laws/show/539/97-%D0%B2%D1%80 (дата звернення: 11.04.2019).*
9. *Конституція України від 28 червня 1996 року. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 11.04.2019).*
10. *Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 11.04.2019).*
11. *Заярний О. Посадова особа органу публічної адміністрації як суб'єкт адміністративного інформаційного правопорушення: сучасне розуміння та проблеми удосконалення законодавчих підходів. Публічна служба і адміністративне судочинство: здобутки і виклики: Збірник матеріалів І Міжнародної науково-практичної конференції (м. Київ, 5–6 липня 2018 року). К.: ВД «Дакор», 2018.С.134-138.*
12. *Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 11.04.2019).*
13. *Савінова Н.А. Кіберзлочинність: витоки та тенденції детермінації в умовах розвитку глобального інформаційного суспільства. Актуальні проблеми вдосконалення чинного законодавства України: збірник наукових статей. Випуск 28. Івано-Франківськ. 2012. С.248-254. URL: http://lib.pnu.edu.ua/files/zbirnyky/zb28-2012.pdf*

14. Муравська (Якубівська) Ю.Є. Інформаційна безпека суспільства: концептуальний аналіз. Економіка та управління національним господарством №9. 2017. С. 289-294. URL: http://economyandsociety.in.ua/journal/9_ukr/50.pdf (дата звернення: 11.04.2019).

Петровська І.І. Правові засади публічного контролю за інформаційною безпекою в Україні

Автор аналізує правові засади забезпечення національної безпеки та її виду – інформаційної безпеки в Україні. У дослідженні розкрито засади державної політики безпеки. В статті розглянуто реалізацію ідеї соборності України через забезпечення національної безпеки в інформаційній діяльності (зокрема щодо одержання, використання, поширення, перетворення, спростування й охорони інформації, її достатності та правдивості).

Окремо аналізуються загрози національній безпеці та питання інформування про діяльність публічних осіб, методи ведення інформаційної війни.

Ключові слова: інформація, інформаційне суспільство, інформаційна діяльність, національна безпека, інформаційна безпека, охорона інформації, інформаційна війна.

Петровская И.И. Правовые основы публичного контроля за информационной безопасностью в Украине

Автор анализирует правовые основы обеспечения национальной безопасности и ее вида - информационной безопасности в Украине. В исследовании раскрыто основы государственной политики безопасности. В статье рассмотрены реализацию идеи соборности Украины путем обеспечения национальной безопасности в информационной деятельности (в частности по получению, использованию, распространению, преобразования, опровержения и охраны информации, ее достаточности и достоверности).

Отдельно анализируются угрозы национальной безопасности и вопросы информирования о деятельности публичных лиц, методы ведения информационной войны.

Ключевые слова: информация, информационное общество, информационная деятельность, национальная безопасность, информационная безопасность, охрана информации, информационная война.

Petrovska I.I. Legal aspects of public control for information safety in Ukraine

The author analyzes the legal principles of ensuring national safety and its type - information safety in Ukraine. The study reveals the principles of state security policy. The article deals with the implementation of the idea of the unity of Ukraine through the provision of national safety in information activities (in particular regarding the receipt, use, dissemination, transformation, refutation and protection of information, its sufficiency and truthfulness).

Separate analysis of the threats to national safety and the issue of informing about the activities of public figures, individual methods of information war.

Consequently, the legal acts of Ukraine define the directions of the state policy, public officials, the basic methods of ensuring national safety and its type - information safety.

The state policy on national safety is aimed at ensuring state, economic, information, military, foreign policy, ecological safety, cyber safety of Ukraine on the basis of implementation of relevant strategies, legal acts of the information sphere. For law enforcement activities in the field of information safety is carried out democratic civilian control (which is a kind of public control).

Keywords: information, information society, information activity, national safety, information safety, protection of information, information war.

Федорончук А.В.

ПРИВОДИ, ПІДСТАВИ ТА ПІДСУМКИ ВВЕДЕННЯ ВОЄННОГО СТАНУ В УКРАЇНІ

УДК 342.514

Постановка проблеми. Російська збройна агресія проти України триває з 2014 року і по сьогоднішній день. Складовими збройної агресії є окупація військовими Російської Федерації Автономної Республіки Крим та неоголошена Війна на сході України.

Втрати України в цій війні досі не пораховано офіційно. Держава повідомляє лише про втрату 7 % території та 13 % населення, яке на цій території проживало. За даними міністерства з питань окупованих територій, кількість внутрішніх біженців – тимчасово переміщених осіб – трохи не дотягує до мільйона 400 тисяч. Та навіть це, більше однієї Естонії. Зараз кількість загиблих на сході перетнула позначку в 13 тисяч. Від 4 до 5 тисяч з них, за різними цифрами, українські військові [1]. Але на жаль, це не кінцеві цифри цієї сумної статистики, адже війна ще не завершилася і від збройної агресії Російської Федерації практично щодня продовжують гинути громадяни нашої держави.

За цей період, внаслідок агресивних дій Російської Федерації ситуація в Україні неодноразово загострювалася, хоча до 26 листопада 2018 року воєнний стан так і не було введено. Тому, є актуальним питання щодо аналізу приводів, підстав, своєчасності запровадження та підсумків воєнного стану.