

**АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС;
ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО**

УДК 40; 342.1
DOI 10.36919/EIJ.1.2023.21

П. В. Цимбал,
доктор юридичних наук, професор,
заслужений юрист України, завідувач кафедри права
ПВНЗ «Європейський університет»
ORCID ID 0000-0002-7244-4669;

А.М. Лисеюк,
кандидат юридичних наук, доцент, доцент кафедри кримінального
розслідування Державного податкового університету,
ORCID ID 0000-0002-9026-1188

**ПОНЯТТЯ ТА СУТНІСТЬ ПУБЛІЧНО-ПРАВОВОЇ ОХОРОНИ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

Нові виклики і загрози, які ставлять світ на межу катастрофи: міжнародний тероризм; кібертероризм, організована злочинність; незаконний обіг наркотиків і зброї; расова нетерпимість; релігійний фанатизм; політичний екстремізм; агресивний сепаратизм. Виникають загрози і в такій важливій сфері міжнародного співробітництва, інтеграції всього світового співтовариства, як інформаційна.

Стаття присвячена питанням поняття, структури і змісту інформаційних відносин та інформаційної безпеки як об'єктів публічно-правової охорони, визначенню закономірностей розвитку в інформаційну епоху, вирішення актуальних проблем і розвитку національного законодавства у сфері інформаційної безпеки.

Результати розвитку інформаційних технологій дозволяють сподіватися на створення динамічної світової інформаційної моделі. Останні роки неймовірно зростала інтенсивність споживання інформації в усіх сферах життєдіяльності людини і суспільства: соціальній, науково-технічній, технологічній, статистичній, економічній та ін. Процеси збору, накопичення, переробки та розповсюдження інформації стають необхідною умовою існуючих структур політичного та іншого управління, здійснення ефективних політичних впливів, вирішення масштабних економічних завдань.

На сьогодні існує стан українського інформаційного законодавства та необхідність термінових заходів щодо його удосконалення. Однак єдності у шляхах якісної трансформації інформаційного законодавства України серед дослідників цієї проблематики не існує, що є логічним, зважаючи на складність, динаміку та масштабність сучасних інформаційних процесів, які відбуваються в умовах становлення національної правової системи.

Ключові слова: інформаційна безпека, публічно-правова охорона, захист інформації, публічно-правовий захист в інформаційному суспільстві.

Постановка проблеми та її актуальність. У сучасному світі на провадження зовнішньої та внутрішньої політики держави, а також загальний рівень розвитку і життєдіяльності суспільства країни чи не найголовніше впливає інформаційна політика, що здійснюється на державному рівні. Через постійне впровадження нових технологій і невідпинний розвиток цієї галузі увесь час з'являються нові загрози та виклики у сфері забезпечення особистих інтересів, суспільства і держави, а також національної безпеки.

Серед стратегічних завдань, які стоять на першому місці у кожній сучасній державі, можна виділити такі: подолання суперечностей в інформаційній сфері регіонального та гло-

бального масштабу, зменшення рівня негативного комунікативного впливу, необхідність забезпечення інформаційних ресурсів національного рівня, гарантування та забезпечення інформаційної безпеки країни й інформаційної незалежності тощо. Впровадження та забезпечення системи інформаційної безпеки, що протидіє загрозам і викликам, які постають у сфері інформаційного простору, підтримує належне функціонування інформаційної інфраструктури та захищає інформаційні ресурси держави, є основними завданнями інформаційної безпеки.

Питання забезпечення інформаційної безпеки є актуальним тому, що суспільство наразі формується під призмою розвитку інформації та інформаційних технологій, які викликають значні зміни та впливають на всі сфери державного і суспільного життя. Інформацію можна визначити як ресурс стратегічного значення у публічній сфері держави. Розвиток країни та суспільства прямопропорційно залежить від стану правового регулювання і державного управління сферою забезпечення інформаційної безпеки. Інформаційна безпека також значною мірою впливає на безпеку держави у сфері економіки, оборони, політики та суспільного життя, а також на охорону особистих, суспільних і державних інтересів в інформаційній сфері.

Аналіз останніх досліджень і публікацій. Значна кількість учених і науковців приділяла увагу у своїх дослідженнях питанню інформаційної безпеки. Проте постійні зміни та невинний розвиток, якими характеризується ця сфера, залишають потребу у постійному проведенні нових комплексних досліджень. Значний внесок у питання захисту інформаційної безпеки держави здійснили такі вчені, як В. Ю. Артемов (2016), А. Л. Баланда (2018), Д. О. Беззубов (2013), О. О. Богомолів (2018), В. М. Брижко (2013), М. В. Волошина (2010), М. Т. Гаврильців (2020), В. І. Гурковський (2004) тощо.

Мета статті полягає у формуванні теоретико-правових основ поняття та сутності публічно-правової охорони інформаційної безпеки, визначенні закономірностей її розвитку в інформаційну епоху та підготовці пропозицій щодо шляхів вирішення актуальних проблем і розвитку національного законодавства у цій сфері.

Виклад основного матеріалу дослідження. Сьогодні успішний розвиток демократичної, правової держави та громадянського суспільства може бути успішним лише за умови повного використання інформаційних ресурсів і формування чіткої національної політики щодо забезпечення високого рівня національної інформаційної безпеки. Насправді інформаційна безпека націй і національних суспільств постає як ключовий фактор трансформації внутрішньої демократії та появи рівнів конкуренції в регіональному та глобальному масштабі.

Публічно-правовий захист в інформаційному суспільстві — система врегульованої правовими нормами публічно-управлінської діяльності, спрямованої на попередження злочинів і відновлення порушених прав у сучасних мережах «Інтернет», яка здійснюється у формі адміністративного права та має такі можливості вжити заходів адміністративного примусу і притягнути до кримінальної відповідальності згідно із законом.

За адміністративною діяльністю публічної адміністрації (застосування заходів адміністративного примусу) зміст публічно-правового захисту поділяється на три рівні: перший рівень адміністративно-правового захисту реалізується публічною адміністрацією у процесі запобігання та порушення: вузьке розуміння адміністративно-превентивного захисту або адміністративно-правового захисту; другий рівень адміністративно-правового захисту здійснюється публічною адміністрацією у процесі відновлення порушених прав: адміністративно-правовий захист, або вузький адміністративно-правовий захист. Третій рівень — це перший і другий рівні поєднання адміністративно-правового захисту, тобто державне управління комплексно здійснює запобігання та відновлення порушень прав: адміністративно-правовий захист у широкому розумінні.

Основним напрямом впливу законів на суспільні відносини, що виникають у сфері публічно-правової охорони, з метою впорядкування є досягнення особливої правової функції: нормозахисної, у якій функція регулювання є функцією упорядкування, в певному діапазоні визначають лінії поведінки людей, наділяючи їх певними правами й обов'язками, а захист — функція встановлення і забезпечення правового захисту та юридичної відповідальності за допомогою державних заходів, спрямованих на заміну суспільно шкідливих відносин і захист позитивних.

Охоронна функція виражається у:

- 1) визначенні заборони протиправних дій;
- 2) правових санкцій за такі діяння (адміністративна відповідальність згідно із Кодексом про адміністративні правопорушення);

3) правових санкціях безпосередньо проти правопорушників. Охоронний вплив права, особливо в інформаційному суспільстві, передбачає існування широкого арсеналу норм, до яких належать як охоронні, так і регулятивні.

Публічно-правове регулювання інформаційної безпеки визначається потребами держави в управлінні формуванням і використаннім інформаційних ресурсів, створенням і застосуванням інформаційних систем, захистом інформаційної безпеки в соціальних системах. Значною мірою інформаційна безпека залежить від необхідності адміністративного регулювання інформаційних відносин у різних областях, які утворюють саму систему та підтримують її цілісність. Адміністративно-правові принципи інформаційної безпеки в соціальних системах повинні забезпечувати ідеальний стан діяльності суб'єктів, систем та їх моделей.

Захист інформаційної безпеки – комплекс заходів, спрямованих на запобігання пошкодження інформації та інформаційної інфраструктури властивостей об'єктів захисту, засобів і суб'єктів цієї діяльності. Здійснювана державою у формі законів діяльність із захисту інформації становить сутність правового захисту інформаційної безпеки.

Водночас захист інформації – це вид інформаційної діяльності, під якою розуміється поведінка, яку здійснює певний суб'єкт у межах свого правового статусу щодо захисту й охорони інформаційних масивів і технологій, засобів і каналів зв'язку. Кампанія спрямована на запобігання загрозам безпеці об'єктів національного інтересу в регіоні та протидію незаконним посяганням різних суб'єктів, які можуть завдати шкоди конкретним об'єктам. Зрозуміло, що основним інструментом і найефективнішим регулятором вищезазначеної діяльності є сам закон.

Як зазначалося вище, різновидами інформаційної діяльності й інформаційних правовідносин переважна більшість фахівців вважає охорону і захист інформації та пов'язаних з нею ресурсів і пов'язаних з цим відносини. Продовжуючи логічний ланцюжок від загального «інформаційної безпеки» до окремого «інформаційного захисту», доходимо висновку, що забезпечення інформаційної безпеки як інформаційна діяльність має ширший обсяг, ніж захист інформації [1].

Захист інформаційної безпеки має включати діяльність із забезпечення безпеки людської, соціальної та національної інформації, захисту прав і свобод у сфері інформації. Відповідальність за забезпечення інформаційної безпеки покладається на всіх суб'єктів інформаційного поля, але ключову роль у реалізації інформаційної політики має відігравати держава в особі відповідних державних відомств. У зв'язку з цим питання про те, наскільки сучасні системи державного управління можуть впоратися із викликами, спричиненими глобальною цифровізацією та загостреними перебігом сучасних епідемій, стає все більш важливим.

До найважливіших теоретико-методологічних і суспільно-правових засад забезпечення інформаційної безпеки відносимо засоби. Вони не є вичерпними, але їх правова інтеграція та застосування сприятимуть формуванню й ефективній роботі систем захисту інформації. Публічно-правовий захист включає кримінально-правові, адміністративно-правові засоби, а також організаційні (організація веде єдину спеціалізовану систему зв'язку, проводить кадрову перевірку, створює системи ризиків тощо). Сутністю адміністративно-правових засобів правового регулювання та державного управління є сукупність правових механізмів, прийомів і способів встановлення та реалізації владних повноважень державними органами в різних державних структурах, спрямованих на забезпечення інформаційної безпеки особи і суспільства.

Серед адміністративно-правових засобів забезпечення інформаційної безпеки найбільш актуальним можна вважати метод колегіального контролю за дотриманням режимів секретності (конфіденційності). Застосування зазначеного методу передбачає проведення колегіальних (комісійних) перевірок дотримання режиму секретності (конфіденційності): на внутрішніх об'єктах, тобто в центральних апаратах державних органів, на підприємствах, в установах та організаціях, – у строки, визначені нормативними документами; у відомствах загальнодержавного рівня (здійснюється спеціально уповноваженим органом державної влади у сфері охорони державної таємниці) – у строк, визначений відповідним розпорядником [2, с. 107].

До методів забезпечення інформаційної безпеки належать сертифікація засобів захисту інформації, ліцензія на діяльність у сфері захисту інформації, що становить державну таємницю, сертифікація систем телекомунікаційного обладнання, відповідність програмного забезпечення автоматизованих систем обробки інформації вимогам безпеки інформації.

Також варто зазначити, що держава повинна здійснювати найсуворіший контроль за охороною відомостей, що становлять державну таємницю.

Спосіб реєстрації, безумовно, займає важливе місце в системі адміністративно-правових засобів. В існуючій системі адміністративної влади реєстраційні функції поділяються на контрольні та наглядові. Реєстрація ЗМІ є необхідною умовою для виробництва і розповсюдження ЗМІ. Так, враховуючи вимоги ст. 4 Закону України «Про друковані засоби масової інформації (пресу) в Україні», визначено, що друковані засоби масової інформації України видаються державною мовою та іншими мовами, зареєстрованими засобами масової інформації [3].

Сам процес реєстрації не являє собою особливої складності. Заявки розглядаються впродовж одного місяця з дня їх надходження. За результатами розгляду заяви приймається одне із чотирьох можливих рішень.

Не менш важливу роль в адміністративно-правових засобах забезпечення інформаційної безпеки України відіграє адміністративний примус, який є одним із засобів державного управління. У системі механізмів забезпечення громадської та національної безпеки він являє собою особливу діяльність із застосуванням засобів і методів правового впливу на фізичних та юридичних осіб, які становлять загрозу національній безпеці. Основним критерієм класифікації заходів адміністративного примусу є безпосередня мета вжиття певних заходів.

Кримінально-правову охорону інформаційних правовідносин можна визначити як систему кримінально-правових засобів, яка повинна включати кримінально-правові норми (забона, тлумачення, заохочення й обмеження) та методи кримінально-правової політики (криміналізація і декриміналізація, покарання та декриміналізація), засобами яких нормативність права трансформується в упорядкованість суспільних відносин.

Інформаційна безпека як окремий кримінально-правовий об'єкт кримінальним правом не розглядається, тому її кримінально-правова охорона здійснюється через відповідні кримінально-правові норми, які законодавець розміщує в різних частинах Особливої частини Кримінального кодексу України [4]. Не вдаючись до доказів, пошлемося на склад злочину, передбачений стст. 111, 114, 328, 329, 330, 333 розділу XVI Особливої частини КК України. Водночас якщо провести детальний науковий аналіз іншої частини статті, то в частині норми також передбачена кримінальна відповідальність за явне порушення національної інформаційної безпеки.

Враховуючи таку ситуацію, насамперед необхідно переглянути перелік загальних об'єктів, які охороняються кримінальним законом згідно зі ст. 1 КК України, а також визначають вертикальну роль і положення державного рівня інформаційної безпеки, наприклад конкретних об'єктів та їх різноманітних складових – безпосередньо. На підставі отриманих висновків доцільно створити відповідний кримінальний орган, відповідальний за загрозу національній інформаційній безпеці, доповнивши новими нормами, які передбачають кримінальну відповідальність за порушення національної інформаційної безпеки (наприклад, інформаційної інфраструктури на об'єктах критичної інфраструктури).

Як згадувалося раніше, інформація, середовище та інфраструктура, яку вона створює, набір суб'єктів, пов'язаних з нею, і соціальні відносини, що впливають з цього, складають інформаційну сферу індивідуального, соціального та національного життя. Для забезпечення безпеки у цій сфері держава має розробляти і здійснювати єдину цілеспрямовану політику. У складних умовах сьогодення Українською державою сформовано інформаційну доктрину та стратегію кібербезпеки, формується й удосконалюється відповідне законодавство, спрямоване на захист національних інтересів України у цій сфері. Наразі є всі підстави стверджувати, що в країні діє система, яка досить чітко регулює відносини щодо забезпечення безпеки національної інформації [5].

Окремі аспекти цих відносин регулюються конституційною, адміністративною та іншими «фундаментальними» галузями правової системи країни. Однак окрема юридична особа із власною структурою (комплексне агентство, субагентство тощо) та внутрішньою організацією повинна поєднувати всі ці положення і регулювати таку діяльність. Отже, до комплексних інститутів, передбачених законом про національну інформаційну безпеку, належать: інститути конфіденційності (державні, комерційні, медичні тощо), інститути захисту інформації, зокрема суб'єкти ліцензованої діяльності в цій сфері, суб'єкти захисту персональних даних, відповідальність за злочини в інформаційній сфері. Під національною інформаційною політикою варто розуміти політику, яка створює та гарантує правове регулювання інформаційних

відносин, захищає права й основні свободи людини, збалансовує інтереси всіх сторін через державну (політичну) владу [6].

Значно поширена думка, що демократії повинні прагнути зробити свою політику і дії прозорими для громадян та інших націй. Керуючись цією філософією, органи, що виробляють політику, мають сформулювати політику у сфері інформаційної безпеки з метою створення суспільства відкритого доступу, де інформація доступна, а урядові процеси прозорі. Відстоюючи переваги цього підходу та підзвітність політичних діячів виборцям, деякі прихильники цієї точки зору визнають, що навіть у демократичних суспільствах можуть знадобитися більш суворі форми інформаційної безпеки для захисту життєво важливих національних інтересів, але цей контроль має бути обмеженим. Обмеження цього аргументу полягає в тому, що він не стосується перехідного періоду між нормою та політикою. Навіть якщо припустити, що демократичні норми підтримують повну або майже повну прозорість і протистоятимуть державній таємниці, залишається питання: як норми через політичний процес переходять у закон, що має силу. Незважаючи на те, що виконавча влада може бути зацікавлена в секретності, цей аргумент ігнорує той факт, що в демократичних державах у процесі прийняття рішень беруть участь численні суб'єкти.

Ефективне управління сучасним інформаційним суспільством неодмінно передбачає формування національної інформаційної політики та створення умов для її реалізації, а метою цієї діяльності має стати координація функцій системи й інформаційних складових в умовах швидкого поширення інформації та цифрового процесу. Це свідчить про те, що забезпечення інформаційної безпеки стало одним із найважливіших і пріоритетних завдань, а вирішення цієї проблеми необхідне для існування та подальшого розвитку нашого суспільства. Інформаційна безпека важлива, тому що захищаємо наш інформаційний простір, а відтак і наші інформаційні ресурси, свою національну культуру.

Висновки. Без провадження забезпечення і захисту національної інформаційної безпеки Україна не може успішно розвиватися як суверенна держава. У світі інформатизації та глобалізації значно зростає значення особистої, соціальної та національної інформаційної безпеки, і її норми повинні займати належне місце в національній політиці. Інформаційна безпека є важливою складовою національної безпеки, і завдяки послідовній реалізації продуманої інформаційної стратегії держави вона значною мірою сприятиме успішному вирішенню завдань у таких сферах національної діяльності, як політика, економіка, соціальне забезпечення тощо.

Інформаційна безпека є важливою частиною національної безпеки і позиціонується як основна функція країни. З одного боку, інформаційна безпека має на меті забезпечити громадянам доступ до якісної вичерпної інформації та необмежений доступ до різноманітних джерел інформації. З іншого — забезпечує контроль за недопущенням поширення неправдивої інформації, сприяє соціальній доброчесності, захищає інформаційний суверенітет, протидіє впливу пропаганди і негативної інформації психологічного характеру, захищає національний інформаційний простір від різноманітних маніпуляцій та інформаційної війни.

Вирішення складних питань інформаційної безпеки, по-перше, може захистити суспільні та національні інтереси, по-друге, захистити право громадян на користування повною, об'єктивною та якісною інформацією. Якщо розглядати поняття інформаційної безпеки в контексті національної безпеки, то, з одного боку, інформаційна безпека трактується як самостійна складова національної безпеки будь-якої країни, а з іншого — інформаційна безпека є невід'ємною частиною будь-якої іншої безпеки (військової, економічної, політичної тощо).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гурковський В. І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки : автореф. дис. на здобуття наук. ступеня канд. наук з держ. управ. : спец. 25.00.02 / Нац. акад. держ. управ. при Президентові України. Київ, 2004. 23 с.
2. Олійник О. В. Методологічні засади забезпечення системи інформаційної безпеки та її складової — захисту інформаційних ресурсів. Право і безпека. 2014. № 1(52). С. 103–109.
3. Про друковані засоби масової інформації (пресу) в Україні / Верховна Рада України. Відомості Верховної Ради України. 1992. URL : <https://zakon.rada.gov.ua/laws/show/2782-12>
4. Кримінальний кодекс України / Верховна Рада України. Відомості Верховної Ради України. 2001. URL : <http://zakon.rada.gov.ua/laws/show/4651-17>

5. Чистоклетов Л. Г., Хитра О. Л. Адміністративно-правові засоби у забезпеченні інформаційної безпеки Україні. IT-право: проблеми та перспективи розвитку в Україні : зб. матеріалів II-ї Міжнар. наук.-практ. конф., м. Львів, 17 листоп. 2017 р. Львів, 2017. С. 212–217.

6. Політанський В. С. Світові моделі та фундаментальні принципи інформаційного суспільства. Науковий вісник Ужгородського національного університету. Серія «Право». 2017. Випуск 43, том 1. С. 34–39.

REFERENCES

1. Gurkovsky V. I. (2004). Organizational and legal issues of interaction of state authorities in the field of national information security : author's review. thesis Ph.D. sciences from state management : special 25.00.02 / National Acad. state management under the President of Ukraine. Kyiv. 23 p.

2. Oliynyk O. V. (2014). Methodological principles of ensuring the information security system and its component – protection of information resources. Law and Security. 2014. No. 1(52). Pp. 103–109.

3. About printed media (press) in Ukraine / Verkhovna Rada of Ukraine. Information of the Verkhovna Rada of Ukraine. 1992. URL : <https://zakon.rada.gov.ua/laws/show/2782-12>

4. Criminal Code of Ukraine / Verkhovna Rada of Ukraine. Information of the Verkhovna Rada of Ukraine. 2001. URL : <http://zakon.rada.gov.ua/laws/show/4651-17>

5. Chistokletov L. G., Khytra O. L. (2017). Administrative and legal means of ensuring information security in Ukraine. IT law: problems and prospects of development in Ukraine : Collection. materials of the II International science and practice conf, Lviv, November 17, 2017. Lviv, 2017. Pp. 212–217.

6. Politsansky V. S. World models and fundamental principles of the information society. Scientific Bulletin of the Uzhhorod National University. "Law" series. 2017. Issue 43. Volume 1. Pp. 34–39.

P. V. Tsymbal, A. M. Lyseiuk. CONCEPT AND ESSENCE OF PUBLIC-LEGAL PROTECTION OF INFORMATION SECURITY

New challenges and threats that put the world on the brink of disaster: international terrorism; cyber terrorism, organized crime; illegal trafficking of drugs and weapons; racial intolerance; religious fanaticism; political extremism; aggressive separatism. Threats also arise in such an important field of international cooperation, integration of the entire world community, as information.

The article is devoted to the issues of the concept, structure and content of information relations and information security as objects of public and legal protection, determining the patterns of development in the information age, solving current problems and developing national legislation in the field of information security.

The results of the development of information technologies allow us to hope for the creation of a dynamic global information model. In recent years, the intensity of information consumption in all spheres of human life and society – social, scientific and technical, technological, statistical, economic, etc. – has grown incredibly. The processes of collection, accumulation, processing and dissemination of information become a necessary condition for the existing structures of political and other management, the implementation of effective political influence, and the solution of large-scale economic problems.

Today, the state of Ukrainian information legislation and the need for urgent measures to improve it. However, there is no unity in the ways of qualitative transformation of the information legislation of Ukraine among researchers of this issue, which is logical, considering the complexity, dynamics and scale of modern information processes that take place in the conditions of the formation of the national legal system.

Key words: *information security, public legal protection, information protection, public legal protection in the information society.*