

УДК 1:004.056–027.511

Костянтин Захаренко*Кандидат наук, здобувач НПУ імені М. П. Драгоманова*

ДЕРЖАВА ЯК СУБ'ЄКТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУСПІЛЬСТВА

Держава розглядається як основний суб'єкт інформаційної безпеки суспільства.

Ключові слова: людина, культура, інформація, держава, інформаційна сфера, інформаційний суверенітет, інформаційна безпека.

Згідно з чинним законодавством держава забезпечує безпеку кожного громадянина не тільки на території України, але й за її межами. З цією метою для підтримки належного рівня захисту національних інтересів, а також об'єктів національної безпеки України розробляється система правових норм, які регулюють суспільні відносини у сфері національної безпеки, визначаються основні напрями діяльності органів державної влади та управління, створюються або трансформуються органи і сили забезпечення національної безпеки, формується стратегія взаємодії суб'єктів забезпечення національної безпеки, розробляється механізм демократичного громадянського контролю за системою управління національною безпекою [1].

Однак жорсткі методи захисту з боку держави хоча й є найпростішими і найзрозумілішими, однак далеко не завжди влаштовують громадськість та відповідають демократичним засадам. Як правило, вирізняються дві основні форми державного контролю (цензури): безпосередній та опосередкований. Безпосередній контроль (цензура), своєю чергою, поділяється на попередній і наступний контроль. Попередній контроль був здебільшого поширений до початку нашого століття в усіх країнах світу, але зараз здійснюється лише у диктатурах та під час надзвичайного чи воєнного стану. Його суть полягає у тому, що відповідний урядовець (цензор) переглядає інформацію до її виходу у світ та дозволяє чи не дозволяє її розповсюдження. Прямий наступний контроль з використанням засобів судового переслідування (і не тільки) застосовується у багатьох сучасних державах. Журналіст в авторитарному суспільстві перетворюється на джерело небезпеки та потребує постійного контролю

з боку правлячої влади (еліти, ідеології тощо), звісно ж, в інтересах забезпечення існуючого статус-кво, тобто авторитаризму. Опосередкований контроль передбачає застосування економічних важелів щодо ЗМІ з метою коригування їхньої політичної лінії. Зрозуміло, що ця форма контролю найпоширеніша у сучасних демократичних суспільствах. Цей вид контролю здійснює цілеспрямований економічний вплив на ЗМІ [2, с. 78].

У Законі України «Про основи національної безпеки України» визначені основні напрями державної політики з питань національної безпеки в інформаційній сфері:—забезпечення інформаційного суверенітету України;—вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;—активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України;—забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;—життя комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [3].

Можна визначити такі функції системи забезпечення державної інформаційної безпеки: розроблення та прийняття законодавчих і нормативно-правових актів щодо забезпечення системи управління національними інформаційними ресурсами; розроблення та реалізація фінансово-економічних засад регулювання процесів формування і використання інформаційних ресурсів; здійснення державної реєстрації інформаційних ресурсів, забезпечення повноти створення первинних і похідних інформаційних ресурсів; забезпечення ефективного використання інформаційних ресурсів у діяльності органів державного управління; оптимізація державної політики інформатизації щодо забезпечення науково-технічних, виробничо-технологічних й організаційно-економічних умов створення та застосування інформаційних технологій, інших елементів інформаційної інфраструктури для

формування, розвитку й ефективного використання інформаційних ресурсів; забезпечення розробки та застосування правових, організаційних й економічних механізмів стосовно форм і засобів обігу інформаційних ресурсів держави; регулювання інформаційного співробітництва, спрямованого на забезпечення рівноправного та взаємовигідного використання національних інформаційних ресурсів у процесі міжнародного обміну, здійснення єдиної державної політики наукової підтримки системи державного управління формуванням, розвитком і використанням національних інформаційних ресурсів; кадрове забезпечення функціонування системи державного управління національними інформаційними ресурсами; інформаційно-аналітичне забезпечення прийняття управлінських рішень у сфері управління інформаційними ресурсами [4, с. 183].

Відповідно до своїх видів інформаційна безпека може включати в себе такі вектори [5, с. 16]:

1. Глобальна інформаційна безпека: 1) безпека розвитку міжнародної інформаційної сфери; 2) захист міжнародного інформаційного ринку від незаконних посягань акторів міжнародних інформаційних відносин; 3) захист та обмеження обігу інформації в цілях глобальної інформаційної безпеки; 4) захист міжнародної інформаційної інфраструктури; 5) захист міжнародних інформаційних ресурсів; 6) побудова глобального інформаційного суспільства тощо.

2. Інформаційна безпека окремих держав у міжнародному інформаційному просторі: 1) безпека інформаційного простору держави від інформаційних загроз, інформаційних операцій, інформаційного тиску та інформаційних війн з боку інших акторів міжнародних інформаційних відносин; 2) захист державного інформаційного ринку від незаконних посягань акторів міжнародних інформаційних відносин; 3) захист та обмеження міжнародного обігу інформації в цілях державної інформаційної безпеки; 4) побудова та забезпечення належного функціонування інформаційного суспільства; 5) захист своїх приватних осіб від незаконних посягань акторів міжнародних інформаційних відносин тощо.

3. Інформаційна безпека установ у міжнародному інформаційному просторі: 1) захист інформації з обмеженим доступом, яка належить установі, від несанкціонованих дій з боку інших акторів міжнародної інформаційної сфери; 2) доступ до загальнодоступної інформації та інформації, доступ до якої не може бути обмежено; 3) захист від випадкового чи навмисного втручання в нормальний процес функціо-

нування автоматизованої інформаційної системи організації (установи) з боку інших акторів міжнародної інформаційної сфери тощо.

4. Інформаційна безпека людини в міжнародному інформаційному просторі: 1) захист інформаційної і комунікаційної приватності (особливо персональних даних); 2) вільний доступ до масової та суспільно-значущої інформації; 3) захист від негативного інформаційного впливу; 4) захист інформаційних і комунікаційних прав на міжнародному рівні тощо.

Для держави розрізняють внутрішні та зовнішні джерела інформаційної безпеки. Внутрішніми джерелами називають відсутність історичного, політичного та соціального досвіду життя у правовій державі, що торкається процесу практичної реалізації конституційних прав та свобод громадян, зокрема в інформаційній сфері. Науковці вважають внутрішнім джерелом інформаційної безпеки посилення організованої злочинності та збільшення кількості комп'ютерних злочинів, зниження рівня освіченості громадян, що суттєво ускладнює підготовку трудових ресурсів для використання новітніх технологій, зокрема інформаційних. Водночас, науковці вважають таким джерелом недостатню координацію діяльності вищого державного керівництва, органів влади та військових формувань, а також відставання України від розвинутих країн за рівнем інформатизації органів державної влади, юридично-фінансової сфери, промисловості та побуту громадян.

До зовнішніх джерел інформаційної безпеки належить діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері; політика домінування деяких країн в інформаційній сфері; діяльність міжнародних терористичних груп; розробка концепцій інформаційних війн будь-якими структурами; культурна експансія у відношенні до конкретної країни [6, с. 25].

Суперечливі тенденції світових інтеграційних процесів, вибух етнічних, соціальних та інших конфліктів як міжнародних загроз спричиняють проблеми у визначенні еволюції змісту і характеру глобальної безпеки, потребують перегляду підходів до засобів підтримання міжнародного миру. Політичні дискусії в рамках ООН (Рада Безпеки, ГА ООН, Перший комітет ГА ООН, Конференція із роззброєння) засвідчили посилену увагу міжнародного співтовариства до концепції стратегічної стабільності XXI століття, пов'язаної з викликами інформаційної революції і впливом інформаційних чинників проблеми безпеки. Так, 54-та сесія ГА ООН серед інших документів прийняла Резолюцію 54/49 «Досягнення у сфері інформатизації і телекомунікації в контексті між-

народної безпеки» від 1 грудня 1999 року, в якій концепцію міжнародної інформаційної безпеки було визнано глобальною проблемою сучасності [7, с. 46].

Саме тому основними напрямками забезпечення інформаційної безпеки є: у сфері міжнародної співпраці — інтеграція в міжнародну систему забезпечення інформаційної безпеки і співпраця по запобіганню протиправних дій в інформаційній сфері; у сфері оборони — вдосконалення системи моніторингу загроз та їх джерел, своєчасне інформування відповідних суб'єктів влади про стан інформаційного ресурсу і інформаційних систем оборонної сфери; засобів, методів і способів здійснення, спеціальних заходів і заходів інформаційного впливу; системи підбору і спеціальної підготовки користувачів [8, с. 45].

На сучасному етапі основними реальними та потенційними загрозами національній безпеці України в інформаційній сфері, стабільності в суспільстві є: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії, комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [9].

Згідно Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» [10], вирішення проблеми забезпечення інформаційної безпеки держави 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.

Сьогодні, функцію державного управління інформаційною інфраструктурою розпорошено серед: Національної ради з питань телебачення і радіомовлення; Державного агентства з питань науки, інновацій та інформатизації України; Державного комітету телебачення і радіомовлення України; Адміністрації Державної служби спеціального зв'язку та захисту інформації України; Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації та ін. Вже простий перелік зазначених державних інституцій говорить про доцільність їх функціонального та структурного об'єднання. Головна мета їх діяльності— стимулювання розвитку галузі. Принципово, головним завданням усіх перелічених інституцій— захистити інформацію від неправомірного доступу чи поширення. Інституцій явно забагато, а координації мало.

Серед перелічених органів одну з провідних ролей щодо забезпечення ефективності інформаційно-безпекової діяльності відіграє Міністерство культури та туризму України. Саме це міністерство є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України. Міністерство культури та туризму України відповідає за формування державної політики у сфері кінематографії, культури та мистецтв, охорони культурної спадщини, вивезення, ввезення і повернення культурних цінностей, державної мовної політики, та є також спеціально уповноваженим органом для визначення та контролю особливих властивостей, певних якостей та інших характеристик виробів художніх народних промислів (на виконання Закону України «Про охорону прав на зазначення походження товарів»). Якщо до недавнього часу зростання економіки асоціювалося переважно з технологічним та інноваційним розвитком у технічних галузях (індустріальне суспільство), то з обранням Україною курсу на перехід до інформаційного суспільства сфера культури виходить на якісно новий рівень розвитку та комунікацій. Надання культурних послуг все більш перетворюються в «індустрію культури», в якій створюються та розповсюджуються різноманітні товари та послуги. Культура сприяє стимулюванню творчості та інновацій. У цьому контексті важливим завданням Міністерства культури має стати активізація та укріплення унікальних місцевих традицій і звичаїв, заохочення процесу відродження та розвитку традиційних для України народних ремесел [11].

Основними компонентами інформаційної безпеки в галузі культури, які повинно забезпечувати Міністерство культури та туризму України є: достовірність і повнота інформації; забезпечення документування

історико-культурного процесу; збереження інформації, розглянутої не тільки як збереження матеріальних носіїв культурно-історичної інформації, але і як дбайливе ставлення до емоційно-образної складової культурної спадщини; якість та ефективність культурно-історичної інформації, що визначають провідну роль достовірної культурної спадщини та культурних цінностей в регуляції масової свідомості; забезпечення відповідності об'єктів культурної спадщини та їх атрибуції з метою неприпустимості її — культурної спадщини — спотворення в комерційних та інших цілях; збереження історико-культурного контексту та інформації, що представляється різними установами культури та освіти і неприпустимості його спотворення в цілях просування ідеології окремих соціальних груп; обмін і співробітництво між установами культури, освіти, ЗМІ з метою більш повного та достовірного представлення існуючої культурно-історичної спадщини [12, с. 48].

Враховуючи вищевикладене, важливі функції щодо підтримання рівня інформаційної безпеки покладено на Міністерство культури і мистецтв України, оскільки воно виступає головним (провідним) органом у системі центральних органів виконавчої влади із забезпечення реалізації державної політики у сфері культури і мистецтв. До функцій цього Міністерства віднесено: — забезпечення реалізації державної політики та координація діяльності органів виконавчої влади у сфері культури і мистецтв; — підготовка пропозицій щодо основних напрямів державної мовної політики та участь у її реалізації; — здійснення державного управління і контролю у сфері охорони культурної спадщини, вивезення, ввезення і повернення культурних цінностей, музейної та бібліотечної справи, кінематографії; — забезпечення реалізації прав громадян на свободу літературної і художньої творчості та створення умов для задоволення національно-культурних потреб українців, які проживають за межами України тощо.

Зокрема, важливою функцією Міністерства є регулювання порядку розповсюдження і демонстрування всіх видів вітчизняних і іноземних фільмів на території України. Міністерством здійснюється державна реєстрація фільмів, встановлюються щодо них спеціальні індекси, що визначають глядацьку аудиторію та відповідно до неї умови розповсюдження і демонстрування фільму, здійснюється видача посвідчення на право розповсюдження і демонстрування фільмів (прокатного посвідчення) юридичним особам та фізичним особам — суб'єктам підприємницької діяльності. Відмова в державній реєстрації автоматично

означає заборону фільму до демонстрації і розповсюдження на території України [13, с. 16].

Згідно з переліченими вище функціями, головним методом державного управління забезпеченням інформаційної безпеки є стимулювання виробництва українського контенту державними та недержавними суб'єктами. Кількісні показники для оцінки ефективності діяльності суб'єктів управління полягають у кількості, наприклад, україномовного контенту, кількості маніпулятивних та неправдивих повідомлень, повідомлень із ознаками залякування тощо. Спроба вирішити зазначене питання—наперед невдячна справа, коли виконавець прогнозовано стане «цензором» та «придушувачем свободи слова в Україні» для представників ЗМІ та громадських організацій, що впевнено засвоюють іноземні гранти [14]. Але оскільки засоби масової інформації сьогодні постають найпотужнішим засобом впливу на свідомість, держава через систему інституцій, зокрема й Міністерство культури, повинна забезпечувати якісний національний інформаційний продукт та запобігати обігу потенційно небезпечного та аморального контенту.

Однією з головних функцій цього міністерства є забезпечення суспільної моралі та сприяння виконанню закону «Про захист суспільної моралі». Стаття 5 цього закону стверджує: «Змістом державної політики у сфері захисту суспільної моралі є створення необхідних правових, економічних та організаційних умов, які сприяють реалізації права на інформаційний простір, вільний від матеріалів, що становлять загрозу фізичному, інтелектуальному, морально-психологічному стану населення» [15]. Але в реальних умовах Міністерство культури практично не виконує дану функцію, оскільки не контролює продукт, що надходить до споживача через засоби масової інформації. Комерціалізація та монополізація основних ЗМІ у руках правлячої олігархічної верхівки унеможливають будь яке забезпечення виконання названих функцій з боку держави та відповідного міністерства.

Для забезпечення інформаційної безпеки України Міністерство культури та туризму у взаємодії з іншими міністерствами та відомствами, що відповідають за інформаційну безпеку повинно:—забезпечити виконання Державної програми розвитку національного книговидання та преси; передбачити державне фінансування реконструкції та розвитку поліграфічної бази;—створити умови для підвищення конкурентоспроможності українських ЗМІ, якості їх технічної оснащеності, підвищення фінансової спроможності; підвищити рівень соціального захисту працівників ЗМІ;—створити Національну систему

інформаційних ресурсів, електронні каталоги центральних і регіональних бібліотек, архівів та забезпечити доступ до них через Інтернет; збільшити кількість інформаційно-пошукових систем, які б могли здійснювати повноцінний пошук українською мовою, мовно адаптованих програмних продуктів; — посилити боротьбу з контрабандою іноземних друкованих видань та книг, аудіо-, відео-, кіно- та іншої інформаційної продукції; — з метою просування позитивного іміджу України у світовий інформаційний простір, запровадити цільові програми «Світові зірки України» (створення web-сайтів, закордонні поїздки відомих у світі українців, поширення матеріалів через ЗМІ тощо); залучити громадські організації, незалежних експертів до обговорення проблем інтеграції України до світового інформаційного простору, підготовки та проведення окремих заходів та багато іншого [16].

Одночасно усі державні органи управління — від міністерств до відомств мають здійснити глибокі внутрішні трансформації, спрямовані на реорганізацію діяльності щодо забезпечення належного рівня інформаційної безпеки країни.

Список використаних джерел:

1. Руснак О. В. Медіа-інформаційна безпека України: правові аспекти / О. В. Руснак // Стратегічні пріоритети. — 2013. — № 3. — С. 147–150.
2. Малик І. Народження «Доктрини інформаційної безпеки України» / І. Малик // Українська національна ідея: реалії та перспективи розвитку. — 2010. — Вип. 22. — С. 76–81.
3. Закон України «Про основи національної безпеки України» // Із змінами, внесеними згідно із Законом № 3200-IV (3200–15) від 15.12.2005. ВВР. — 2006. — № 14. — Ст. 116.
4. Федорук О. В. Концептуальні засади формування системи забезпечення національної інформаційної безпеки / О. В. Федорук // Вісн. соціально-економічних досліджень. — 2013. — Вип. 2 (1). — С. 182–188.
5. Кісілевич-Чорнойван О. М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять / О. М. Кісілевич-Чорнойван // Юриспруденція: теорія і практика. — 2009. — № 8. — С. 11–18.
6. Малик Я. Й. Забезпечення інформаційної безпеки України у контексті світового досвіду / Я. Й. Малик, О. І. Береза // Ефективність державного управління. — 2012. — Вип. 32. — С. 20–27.

7. Макаренко Є. А. Політичні доктрини глобальної інформаційної безпеки / Є. А. Макаренко // Вісн. Ін-ту міжнародних відносин Київськ. нац. ун-ту ім. Т. Шевченка. — 2007. — № 2. — С. 45–51.
8. Присяжнюк М. Інформаційна безпека України в сучасних умовах / М. Присяжнюк, Я. Белошевич // Вісн. Київського нац. ун-ту ім. Т. Шевченка. Військово-спеціальні науки. — 2013. — Вип. 30. — С. 38–42.
9. Закон України «Про основи національної безпеки України» // Із змінами, внесеними згідно із Законом № 3200-IV (3200–15) від 15.12.2005. ВВР. — 2006. — № 14. — Ст. 116.
10. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» // Відомості Верховної Ради України (ВВР). — 2007. — № 12. — Ст. 102.
11. Національна стратегія розвитку сфери інтелектуальної власності в Україні на період до 2020 року / [Електронний документ]. — Режим доступу: sips.gov.ua/i.../file/ip-strategy28082014-1.doc
12. Алиева М. Ф. Информационная безопасность как элемент информационной культуры / М. Ф. Алиева // Вестн. Адыгейского гос. ун-та. — Сер. 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. — 2012. — Вип. № 4 (108). — С. 96–101.
13. Кормич Б. А. Інформаційна безпека: організаційно-правові основи. Навч. посібн. / Б. А. Кормич. — К.: Кондор, 2008. — 384 с.
14. Полевий В. Що захищаємо в інформаційній війні та хто за це відповідає? / Володимир Полевий // [Електронний документ] Рідна країна: світоглядний портал. 15 жовт. 2014. — Режим доступу: ridna.ua > Громадянська > Громадська думка.
15. Закон України «Про захист суспільної моралі» // ВВР. — 2004. — № 14. — Ст. 192.
16. Доктрина Інформаційної безпеки України // [Електронний документ] Офіційна вебсторінка Верховної Ради України: Законодавство. — Режим доступу: <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009&p=1267772861313087>

Стаття надійшла до редакції 18.01.2015 р.

Константин Захаренко. Государство как субъект информационной безопасности общества

Государство рассматривается основным субъектом информационной безопасности общества.

Ключевые слова: человек, культура, информация, государство, информационная сфера, информационный суверенитет, информационная безопасность.

Kostyantyn Zakharenko. Global Nature of Information Security

However, information security has a global nature, and therefore requires a review in the system of global information space.

Keywords: human being, culture, information, information space, information civilization, information security.