УДК 351.751

Панова І.В.
кандидат юридичних наук,
доцент кафедри інформаційного права
ННІ ПМК ХНУВС

Актуальні питання захисту особи від негативного інформаційного впливу в контексті інформаційної безпеки України

Анотація. У статті здійснено аналіз актуальних аспектів захисту особи від впливу шкідливої інформацій в контексті інформаційної безпеки України.

Ключові слова: інформаційна безпека, концепція інформаційної безпеки, захист від впливу шкідливої інформації

Постановка проблеми. Доктрина інформаційної безпеки України серед життєво важливих інтересів в інформаційній сфері закріпила захищеність особи від негативного інформаційно-психологічного впливу, визначаючи викривлену, недостовірну та упереджену інформацію, що завдає шкоди національним інтересам України, та зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет як реальні та потенційні загрози інформаційній безпеці України [1].

Для України головна проблема сьогодні у тому, що людина існує в забрудненому, дуже фрагментарному, неточному, спотвореному інформаційному середовищі, в якому неможливо приймати рішення. Розв'язати цю проблему можна створюючи оптимальне інформаційне середовище, де можливим є доступ до інформації та прийняття корисних, насамперед для конкретної людини, рішень.

Кількість робіт, присвячених дослідженню наукових проблем забезпечення інформаційної безпеки України постійно збільшується, проте відсутність у цій сфері комплексного дослідження інформаційної безпеки особи істотно знижує ефективність ви-

ко-ристання отриманих висновків. Вирішення проблем забезпечення інформаційної безпеки людини стає важливим не тільки для утвердження України як демократичної правової держави, в якій права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави, але й для стійкого прогресивного розвитку українського суспільства, його духовного відродження.

Необхідно відзначити, що в правовій науці, зокрема, у сфері інформаційного права, окремим аспектам інформаційної безпеки присвятили свої праці як українські, так і російські вчені: А. Б. Агапов, А.В. Анісімов, І. В. Арістова, О.А. Баранов, Ю. М. Батурін, І. Л. Бачило, М.М. Биченок, В. М. Брижко, В.Д. Гавловський, В.П. Горбулін, О.Г. Додонов, В.Г. Заблоцький, А.В. Іщенко, Р. А. Калюжний, І.П. Козаченко, Я.Ю. Кондратьєв, В. А. Копилов, П. У. Кузнецов, З. В. Кузнецова, А. І. Марущак, О. Г. Марценюк, А.О. Рось, В.Я. Рубан, Г.П. Стежка, А. В. Стрельников, В.Г. Хахановський, В. С. Цимбалюк, М. Я. Швець, Ю. С. Шемшученко та інші. Утім, на жаль, головний акцент було зроблено на захисті державних інтересів, інформаційна ж безпека людини залишається поза увагою.

За роки незалежності в Україні зроблено суттєвий поступ щодо розвитку вітчизняної інформаційної сфери як особливої системи суспільних відносин, які виникають в усіх сферах життя і діяльності суспільства та держави в результаті одержання, використання, поширення і зберігання інформації. Насамперед це стосується законодавчого закріплення права особи на інформацію та на вільне поширення її всередині країни і за кордон, трансформації моделі взаємовідносин між органами державної влади та засобами масової інформації, створення національних систем і мереж інформації тощо.

З прагматичних позицій інформаційні процеси можна розрізняти за двома видами: у нервовій системі людини та в інформаційно-комунікаційній інфраструктурі. Перші виявляються як психологічний феномен індивідуальної, колективної та масової свідомості, що формує різноманітні й суперечливі особисті, суспільні й державні інтереси. Людська свідомість, як відомо, допускає інформаційно-психологічне маніпулювання і протидію, тобто вона може бути як об’єктом, так і джерелом негативних або позитивних інформаційних впливів.

Взаємовідносини між людиною, суспільством і державою відбиваються в інформаційній сфері, яка торкається і впливає прак-тично на всі сфери життєдіяльності. Дуалізм інформаційних впли-

вів у тому, що вони не лише породжуються особистими, суспільними й державними інтересами, а й одночасно змінюють їх. Це відбувається в інформаційно-комунікаційному середовищі, яке може або сприяти, або протидіяти виникненню чи реалізації тих або інших інтересів. Позитивні інформаційні впливи спрямовані на узгодження чи підтримку життєво важливих інтересів, негативні – на їхнє зіткнення чи порушення природного балансу.

Таким чином, розуміння особливостей і закономірностей негативного інформаційного впливу на людську свідомість стає не тільки обов'язковим елементом загальної людської культури, а й необхідною умовою для виживання і безпеки людини в сучасному світі. Людина, яка володіє цими знаннями, спроможна самостійно створити психологічний фільтр для інформаційних потоків, що впливають на її свідомість, сформувати установку на аналітичне і критичне відношення до будь-якої інформації, що надходить від зовнішнього середовища.

Дослідження правових аспектів захисту особи від дії шкідливої інформації неможливе без аналізу інформаційної безпеки України, оскільки шкідлива інформація, як було сказано вище, є об'єктом інформаційної безпеки, де забезпечення належного захисту від її дії є пріоритетним напрямом цієї сфери.

Кормич Б.А. аналізує інформаційну безпеку з урахуванням глобалізаційних процесів, що відбуваються в світі. Це актуалізує завдання адаптації вітчизняного законодавства до загальноприйнятих міжнародних стандартів, імплементації міжнародно-правових норм в національне законодавство. Україна бере на себе зобов'язання згідно з цілим переліком міжнародно-правових актів, які стають частиною національного законодавства. Її аналіз дозволяє узагальнювати міжнародний досвід та співставляти його з сучасним національним, корегувати останній відповідно до норм та принципів, що виправдали себе в системі міжнародних відносин; перекривати та заповнювати існуючі прогалини у вітчизняному правовому полі, використовуючи запозичення і використання норм міжнародного права [2, с. 28-32]. Схожими є положення нормати-

вно-правових актів окремих зарубіжних країн, зокрема, Російської Федерації, Сполучених Штатів Америки, Канади, країн Європейського Союзу, їх аналіз допомагає враховувати позитивний та негативний досвід, що може значно прискорити і полегшити демократичні трансформації українського суспільства.

Марущак А.І. діяльність щодо захисту інформаційної безпеки класифікує як складну систему, що містить цілий комплекс векторів державної політики, яка зумовлена специфікою об'єктів інформаційної безпеки. При цьому виділяє два комплекси питань, які диференціюються відповідно до природи правових норм, що становлять їх нормативно-правову базу. По-перше, це інформаційна безпека людини і суспільства, яка базується на нормах природного права і вимірюється ступенем свободи від втручання держави та інших осіб, можливостями самореалізації та самовизначення. По-друге, це інформаційна безпека держави, яка побудована на позитивному праві, пов'язана із застосуванням обмежень, заборон, жорсткою регламентацією, невід'ємним елементом яких стає сила державного примусу

На його думку, комплекс питань інформаційної безпеки людини та суспільства має такі вектори, як:

- забезпечення інформаційних прав і свобод людини і громадянина,

- захист людини від неправомірного інформаційного втручання,

- забезпечення національної, культурної і духовної ідентичності від неправомірного втручання,

- забезпечення дієздатних правових та організаційних механізмів захисту відповідних прав тощо [3, с. 78-79].

Найбільшою загрозою на сучасному етапі розвитку українського суспільства зазначені автори називають інформаційні війни (гуманітарні та технічні). Інформаційна війна, інформаційне протиборство та інформаційна боротьба є проявами одного більш широкого поняття – загрози інформаційній безпеці. При цьому під системою забезпечення інформаційної безпеки пропонується розуміти сукупність інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на за-

безпечення стійкого розвитку об'єктів інформаційної безпеки, а також суб'єктів, які її забезпечують [4].

На думку Шамрай В.О. інформаційна безпека суспільства, держави характеризується ступенем їх захищеності, та, як наслідок стійкістю головних сфер життєдіяльності щодо небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати такі впливи. Загальноприйнятним є таке визначення інформаційної безпеки, як стан захищеності життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері [5].

Автор підтримує точку зору Логінова О.В. та Рося А.О., які зазначають, що інформаційну безпеку не варто розуміти лише як окремий стан. Вона має враховувати майбутнє, отже, є не станом, а процесом. Таким чином, інформаційну безпеку слід розуміти крізь органічно поєднуючі ознаки, такі, як стан, властивість, а також управління загрозами і небезпеками, за допомогою якого забезпечується обрання оптимального шляху їх усунення і мінімізації впливу негативних наслідків. Одним з механізмів гарантування такого процесу є ефективна система органів виконавчої влади, яка є суб'єктом і об'єктом забезпечення інформаційної безпеки одночасно. Питання інформаційної безпеки пов'язані з поняттями «інформаційна боротьба», «інформаційна війна», «інформаційне протиборство» тощо [4].

Одним з ключових чинників інформаційної безпеки людини є її право на достатню інформованість для здійснення свідомого і обґрунтованого вибору. Свобода вибору практично є підгрунтям більшості прав і свобод людини, торкається більшості видів людської діяльності.

Сьогодні порушення прав людини і загрози її безпеки дуже часто носять латентний характер, й інформаційний чинник за цих умов починає виходити на перший план. Сфера інформаційної безпеки людини дуже тонка і відповідальна. З одного боку, вона вимагає втручання держави з метою забезпечення необхідного рівня безпеки і уникнення суспільно небезпечного непередбачуваного розвитку інформаційних відносин. З іншого боку, надмірне державне втручання створює загрозу і може призвести до негативних наслідків, обмеження прав людини і руйнації демократичних інститутів громадянського суспільства.

Варто погодитися з Рубаном В.Я., що "Під інформаційною безпекою людини, суспільства, держави слід розуміти такий стан їхньої інформаційної озброєності (мається на увазі духовної, інтелектуальної, морально-етичної, політичної), за якого ніякі інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів". Спираючись на зазначене, можна зробити висновок, що головним завданням інформаційної безпеки є формування менталітету стійкого прогресивного розвитку. У цьому процесі надзвичайно велика питома вага саме інформаційного впливу як на людину, так і на все те, що відбувається у колективі людей, у суспільстві, у державі [4].

Заступник голови національного агентства з питань інформації при Президентові України Баранов О.А. уважає, що під інформаційною безпекою слід розуміти такий стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення. На переконання Баранова О.А., таке визначення тією чи іншою мірою торкається практично усіх сфер інформаційної взаємодії суб'єктів у суспільстві, державі й у всіх соціальних утвореннях. При цьому під інформаційною взаємодією слід розуміти весь процес створення інформації, накопичення, опрацювання, збереження і поширення. Важливого значення набувають два наступні визначення: інформаційного простору та інформаційної інфраструктури. Вони несуть, як і перше визначення, методологічне навантаження з погляду побудови політики інформаційної безпеки держави [4].

З таким твердженням варто погодитися, підкреслюючи, що основою такого визначення є те, що держава повинна забезпечити кожному суб'єктові інформаційних відносин право на одержання повної, достовірної і своєчасної інформації; ніхто не може порушити інтереси суб'єкта інформаційних відносин шляхом якогось інформаційно впливаючи. Власні інтереси мають поєднуватися з інтересами оточуючих.

Додонов О.Г. доречно зауважує, що інформаційна безпека – це стан захищеності. Можна також сказати, що це є властивістю

системи мінімізувати інформаційні загрози. При розгляді проблеми інформаційної безпеки слід спочатку говорити про загрози і вже по тому – про захищеність від цих загроз. Первинною стає інформаційна загроза. Для окремої особистості існують одні інформаційні загрози, для суспільства – інші, для держави – ще інші [4]. Якщо говорити про інформаційну безпеку як про властивість мінімізувати загрози для людини, то це, на думку автора, правильно. Використовуючи такий підхід, можна розглядати не загальнометодологічні питання інформаційної безпеки, а різні рівні інформаційної взаємодії, інформаційних відносин, виділити методологічні і теоретичні проблеми інформаційної безпеки особи, які необхідно вирішувати. А тоді вже можна шукати засоби, методи протидії інформаційним загрозам, ураховуючи ці методи у відповідних інформаційних системах для адекватного реагування на загрози.

Підтримуючи точку зору Заблоцького В.Г., варто сказати, що захист людини, її часу, витраченого на споживання інформації – це головне в інформаційній безпеці. Щонайкраще структурувати цю складну різноманітну проблему можна технологічно. Будь-яка інформаційна технологія складається з трьох елементів: створення інформації, її зберігання та споживання. З огляду на безпеку необхідно забезпечити надійність роботи усіх трьох елементів системи [4].

Автор підкреслює, що чинна в Україні нормативно-правова база у сфері інформаційної безпеки в основному орієнтована на питання захисту інформації через обмеження доступу особи до певного виду відомостей. Проте залишаються відкритими питання захисту осіб від інформації, тобто захисту людської свідомості від негативного інформаційного впливу. Разом з тим, головною проблемою інформаційної безпеки постає балансування між свободою доступу до інформації та необхідністю її обмеження в інтересах безпеки життєдіяльності. Забезпечення балансу між інформаційною свободою і безпекою життєдіяльності суттєво залежить від рівня культурного й економічного розвитку суспільства. Для вирішення цієї проблеми потрібен системний нормативно-правовий механізм, який забезпечуватиме, з одного боку, захист інформаційних прав і свобод, а з іншого – громадський і державний контроль та регулювання рівня інформаційної безпеки.

Для запобігання неузгодженої, вузьковідомчої нормотворчості, тобто для мінімізації втрат від правових суперечностей і помилок, потрібна кодифікація інформаційного законодавства, тобто цідесне системне його упорядкування. Йдеться про ієрархічну систему нормативно-правових документів, що мають узгоджено й ефективно регулювати суспільні відносини на різних рівнях інформаційної безпеки. Оскільки подібні документи існують у багатьох країнах, доцільно скористатися таким досвідом, зокрема, стратегічних партнерів України: країн - членів ЄС, а також США та РФ.

Оптимізація законодавства у сфері забезпечення інформаційної безпеки особи необхідна передусім для ефективного здійснення правотворчої діяльності, в тому числі для виявлення причин протиріч і невідповідностей у нормативному регулюванні та їх усунення. У свою чергу, систематизація інформаційного законодавства сприятиме поліпшенню інформаційного впливу права на правосвідомість як окремих громадян, так і суспільства в цілому.

Підводячи підсумки вищевикладеному, можна зробити наступні *висновки*:

- із настанням третього тисячоліття для людства починається ера інформатизації, де разом з перспективами прогресу на нас чекає загроза «інформаційного шквалу». Разом з інформацією та інформаційними системами треба захищати і саму людину від дії інформації. Схоже, що значення і роль особи як об'єкту захисту в системі забезпечення інформаційної безпеки у найближчі десятиліття зростатиме, так само як компонент інформаційної безпеки вийде на перше місце в системі національної безпеки країни. Причини цього знаходяться як у великій залежності людини і суспільства від інформації, так і в реалізації економічних і політичних інтересів з використанням інформаційних технологій, зокрема деструктивного порядку (інформаційна зброя), де головним об'єктом впливу є людина;

- чинне українське законодавство містить низку норм, спрямованих на захист людини, організацій і суспільства від шкідливої інформації. Проте ці норми носять безсистемний характер, регулюють лише окремі вузькі групи суспільних відносин і в більшості випадків не мають механізму реалізації. Тим часом право на захист від шкідливої інформації, як і право на інформацію відносяться до основних інформаційних прав. Тому необхідне закріплення в Кон-

ституції права на захист від шкідливої інформації, а також розробляння механізму його реалізації в галузевому законодавстві. Тільки тоді можна буде говорити про відповідність правової системи швидко змінним умовам життя, тому що право – це один ізголовних регуляторів суспільного розвитку.

Література

1. Про Доктрину інформаційної безпеки України: Указ Президента України № 514/2009: [Електронний ресурс] – Режим доступу: http://www.president.gov.ua/documents/9570.html. – Заголовок з екрану.

2. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: Автореф. дис…. докт. юрид. Наук: 12.00.07 / Національний університет внутрішніх справ. – Харків, 2004. 41 с.

3. Марущак А.І. Інформаційне право: Доступ до інформації: Навчальний посібник. – К.: КНТ, 2007. – 532 с.

4. Інформаційна безпека України: сутність та проблеми: [Електронний ресурс] – Режим доступу: http://www.niurr.gov.ua/ukr/publishing/panorama3_4/kr_stil_a.htm. – Заголовок з екрану.

5. В.О. Шамрай. Інформаційна безпека як складова національної безпеки України: [Електронний ресурс] – Режим доступу: http://www.crime-research.ru/library/Shamray.htm. – Заголовок з екрану.