ІНФОРМАЦІЙНА ТА ФІНАНСОВО-ЕКОНОМІЧНА БЕЗПЕКА

УДК 1.316.4

Панфілов О. Ю.

ДО ПРОБЛЕМИ ОЦІНКИ СУЧАСНОГО РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

У статті робиться спроба розкрити методологічний підхід щодо оцінювання сучасного рівня інформаційної безпеки українського суспільства. Надається аналіз широкого кола проблем, напрямків та їх інтерпретації, як основи побудови системи оцінки рівня інформаційної безпеки.

В статье осуществлена попытка раскрыть методологический подход к оценке современного уровня информационной безопасности украинского общества. Представляется анализ широкого круга проблем, направлений та их интерпретаций как основы построения системы оценки уровня информационной безопасности.

In article is carried out attempt to open the methodological approach to an estimation of modern level of information security of the Ukrainian society. The analysis of a wide range of problems, directions that of their interpretations as bases of construction of system of an estimation of level of information security is represented.

Постановка проблеми. Інформаційна безпека посідає одне із провідних місць у системі забезпечення життєво важливих інтересів усіх країн, зокрема України. Це зумовлено нагальною потребою створення розвиненого інформаційного середовища українського суспільства, однак саме через таке середовище найчастіше здійснюються загрози національної безпеці.

Дійсно, інформаційні технології знаходять усе ширше застосування у таких сферах, як фінансовий обіг і ринок цінних паперів (особливо у банківських і біржових організаціях), зв'язку, транспорті, високотехнологічних виробництвах (особливо атомних, хімічних тощо), державних системах управління тощо. Зрозуміло, що будь-яка диверсія у згаданих сферах життєдіяльності держави і суспільства може призвести до тяжких наслідків, паралізувати як ординарні, так і складні, «високі» системи управління, збройні сили і спецслужби, спровокувати руйнівні аварії на екологонебезпечних об'єктах.

Не слід залишати без уваги і вплив таких безпосередніх носіїв інформації, як творчі колективи телебачення і радіомовлення, газет і журналів, інформаційних агентств, які влучно названі «четвертою владою». Особливої ваги вирішення проблем інформаційної безпеки одержує в сучасних умовах глобалізації інформаційних процесів, а також в умовах бажання США, Росії, ряду інших держав досягти інформаційного домінування у світі. Виходячи з цього, актуалізується проблема оцінки сучасного рівня інформаційної безпеки в контексті забезпечення безпеки національної.

Аналіз останніх досліджень. Проблема інформаційної безпеки є предметом дослідження багатьох вчених, спеціальних інститутів та центрів, що представляють різні наукові галузі знання, причому як гуманітарні, так і технічні. За останні роки у вітчизняній та зарубіжній науці в цілому накопичено потенціал для поглибленого дослідження проблеми інформаційної безпеки.

Зокрема, характеристикам інформатизації як об'єктивної закономірності розвитку суспільства, проблемам становлення інформаційної цивілізації та прогнозам її розвитку, технічним й гуманітарним фактори цього процесу присвячені праці Д. Белла, Зб. Бжезинського, Е. Дайсона, М. Кастельса, Й. Масуди, А. Мінка, Дж. Нейсбіта, Е. Паркера, Е. Тоффлера, Р. Абдєєва, В. Афанасьєва, Т. Березі, В. Глушкова, В. Лекторського,

© Панфілов О. Ю., 2012

В. Лисицького, Е. Моргунова, Б. Парахонського, Г. Почепцова, А. Ракітова та інших.

Дослідженням методологічних, сутнісних та змістовних основ інформаційної безпеки присвячені праці Е. Бєляєва, М. Бусленка, С. Гриняєва, О. Данильяна, О. Дзьобаня, Г. Ємельянова, В. Лопатіна, О. Позднякова, Л. Сергієнка, В. Циганкова, М. Чеснокова та інших дослідників.

Однак, незважаючи на те, що існує велика кількість наукових праць з проблем інформаційної безпеки, варто підкреслити той факт, що їхній зміст має, з одного боку, полемічний характер, сутність інформаційної безпеки та сенс її забезпечення надано у фрагментарному вигляді, а з іншого — проблема оцінки інформаційної безпеки практично не досліджена.

Метою статті є спроба розкрити криз призму соціально-філософської рефлексії методологічні засади оцінки рівня інформаційної безпеки суспільства.

Виклад основного матеріалу. Інформаційна безпека — стратегічна категорія, яка входить складовою у ширші, багатокомпонентні поняття, такі як «міжнародна безпека», «національна безпека», «національна стратегія» тощо.

Інформаційна безпека може розглядатися в різних аспектах: і як фактор соціально-економічного розвитку, і як відстеження і класифікація комп'ютерних і мережевих загроз, і як збереження і захист технічної і мовної інформації. І як новий вид озброєння, і як запобігання інформаційній війні тощо [1, с. 675]

З метою оцінки рівня інформаційної безпеки слід провести аналіз діяльності органів державної влади щодо виявлення, попередження та протидії загрозам інформаційної безпеці в сучасних умовах. Проілюструємо окреслені підходи в оцінці рівня інформаційної безпеки, ескізно розглянувши сучасну ситуацію в Україні.

У житті сучасного суспільства і його найбільше важливого інструмента — держави, інформація відіграє важливу, а останнім часом навіть центральну роль. Існує потужна школа суспільствознавців, які стверджують, що в розвинених країнах сьогодні відбувається процес зміни суспільно-економічної формації з індустріальної на постіндустріальну або інформаційну. Процеси, що відбуваються в суспільному житті можна охарактеризувати як посилення ролі і значення інформації як у суспільстві в цілому, так і в житті кожної окремої людини [2; 3; 4].

Тому не випадково, в Законі України «Про основи національної безпеки» інформаційна безпека пов'язуються зі станом захищеності життєво важливих інтересів її об'єктів, причому об'єктами називаються: людина і громадянин — їхні конституційні права і свободи; суспільство — його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; держава — її конституційний лад, суверенітет, територіальна цілісність і недоторканність [5].

Одночасно у Концепції національної програми інформатизації, інформаційна безпека називається (п. 3. розділу VI) «невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки». А об'єктами інформаційної безпеки визначаються «інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни» [6].

Саме на аспекті багатоплановості поняття «інформаційна безпека» наголошує цілий ряд фахівців у галузі інформаційного права, зокрема, підкреслюється, що «інформаційна безпека і, головне, її забезпечення формується як комплексне завдання, яке створює баланс між потребою в інформації великого різноманіття суб'єктів та необхідністю розумно використовувати наявний інформаційний ресурс під девізом «не зашкодь». Такий підхід допомагає розкрити зміст «захисту»: захисту чого, від чого, в ім'я чого або кого і, нарешті, як.

Конституція України не розглядає окремо інформаційні права суспільства в цілому, крім, мабуть, норм ч. 1 ст. 15 Конституції щодо багатоманітності суспільного життя. Але суб'єктами суспільного життя є окремі члени цього суспільства, а не воно саме. Таким чином, для визначення рівня інформаційної безпеки суспільства необхідно пов'язати його із визначеними рівня інформаційної безпеки окремих його членів.

Отже, оцінка рівня інформаційної безпеки пов'язується в першу чергу з інформаційної безпекою людини.

Такій комплексній характер оцінки рівня інформаційної безпеки визначається цілим рядом елементів, в тому числі рядом базових, до яких належать:

– права і свободи людини і громадянина в сфері інформації;

– державні механізми забезпечення та реалізації інформаційних прав і свобод людини та права нації на самовизначення (політичне, культурне, економічні);

– демократичній механізм формування політичної влади в державі, який дає можливість окремій людині та суспільству в цілому через механізми народовладдя визначати основні параметри інформаційних процесів, у державі.

В той же час на державу покладено обов'язки забезпечення відповідних прав людини і народу в цілому. Так, частина 2 статті 3 Конституції України визначає, що «утвердження і забезпечення прав і свобод людини є головним обов'язком держави», а стаття 11 Конституції України визначає, що «держава сприяє консолідації і розвиткові української нації, її історичної свідомості, традицій, культури, а також розвиткові етнічної, культурної, мовної та релігійної самобутності всіх корінних народів і національних меншин України». Що, в свою чергу; доповнюється функцією держави щодо захисту інформаційної безпеки (ч. 1. ст. 17 Конституції України) [10].

Таким чином, оцінка рівня інформаційної безпеки включає конкретні дії держави щодо забезпечення безпечних умов існуючих інформаційних процесів та забезпечення безпечного розвитку таких процесів у майбутньому. Це охоплює регулювання питань захисту самої інформації, захисту інформаційної інфраструктури держави, захисту інформаційного ринку та створення безпечних умов розвитку інформаційних процесів.

В контексті зазначеного, проведення необхідної державної політики інформаційної безпеки та створенням необхідних правових та організаційних засад має ув'язуватися з існуючими загрозами в інформаційній сфері.

У Законі України «Про основи національної безпеки» (ст. 7), серед загроз національній безпеці України в інформаційній сфері називаються:

– 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 [5].

На нашу думку, наведений перелік загроз в інформаційній сфері слід доповнити. Так, в науковій доповіді Національного інституту стратегічних досліджень було визначено такі загрози інформаційній безпеці:

– слабка інтегрованість України у світове інформаційне поле, не достатня кваліфікація й активність її інформаційних служб;

– використання засобів інформації окремими політичними силами;

– негативні наслідки міжпартійних відносин;

– вплив міжконфесійних конфліктів;

– некомпетентність працівників державних органів і установ;

– недостатній професійний рівень працівників засобів масової інформації;

– вплив на засоби масової інформації організованої злочинності, мафіозних структур;

– недостатність технічного захисту інформаційного простору України [11, с. 124–125].

Отже, можна стверджувати, що проблема оцінки стану інформаційної безпеки полягає в безпосередньому аналізі сучасного становища інформаційної сфери в Україні і на його базі створенні певного експертного передбачення всіх можливих загроз інформаційній безпеці. Виходячи із зазначеного та ряду наукових напрацювань, сучасний рівень інформаційної безпеки може бути оцінений за декількома напрямами [12; 13].

Перший напрямок — це захист персональних даних особистості.

Другий напрямок — це діяльність правоохоронних органів в контексті інформаційної безпеки.

Третій напрямок — це можливість доступу особи до правової інформації.

Четвертий — це можливість доступу до екологічної інформації.

П’ятий — це захист від негативного інформаційного впливу.

Шостий — забезпечення інформаційної безпеки громадян як суб’єктів політичного процесу.

Розглянемо визначені напрямки.

Загрози інформаційній безпеці людини однаковою мірою можуть стосуватися і реалізації тих прав, що надають можливість людині бути повноправним суб’єктом інформаційних відносин, і тих, що захищають людину від неправомірного інформаційного втручання. Але механізми порушення цих прав мають істотні відмінності. Так, обмеження реалізації свободи слова означає вимогу до суб'єкта утриматися від певних дій, а обмеження реалізації права на конфіденційність приватного життя, навпаки, передбачає надання компетентним органам держави дозволу на здійснення певних дій.

Крім того, і способи реалізації та захисту цих прав, як ми вже зазначали, мають свою специфіку. Перший тип прав, які забезпечують вільну участь в інформаційних процесах, є практично самодостатнім, тобто для їх реалізації потрібне закріплення в нормативно-правових актах, воля суб'єкта та наявність механізмів, передусім судових, їх захисту. Навпаки, захист від неправомірного інформаційного втручання вимагає передусім створення цілого комплексу нормативно-правових актів, що регулюють діяльність органів державної влади, фізичних та юридичних осіб у сфері інформації з метою встановлення чітких юридичних рамок і параметрів такої діяльності [14]

Слід зазначити, що захист від неправомірного інформаційного втручання є дуже важливим аспектом інформаційної безпеки особи, оскільки, на відміну від порушень свободи слова, таке втручання може мати прихований характер і створювати значну загрозу.

Взагалі, відносини між людиною і державою є сферою багато в чому визначальною для забезпечення інформаційної безпеки, особливо інформаційної безпеки особи. В рамках соціального управління, що його здійснюють відповідні органи державної влади та місцевого самоврядування, формуються конкретні механізми забезпечення гарантованих Конституцією умов участі людини в інформаційних процесах. Виходячи з духу та змісту правової й адміністративної реформ, які здійснюються в Україні, можна говорити про те, що «створення дійових механізмів забезпечення прав і свобод людини є одним з орієнтирів трансформації адміністративного права», одним з напрямків досягнення цієї мети можна назвати «деталізацію закріплених у Конституції України процедур, не пов'язаних з юрисдикційною діяльністю органів виконавчої влади і суду» [15].

Серед подібних процедур фахівці, зокрема, називають процедури захисту конфіденційної інформації про особу в органах державної влади, процедури захисту інформації в комунікаційних системах, що забезпечує таємницю кореспонденції, процедури отримання інформації від органів державної влади та місцевого самоврядування, процедуру щодо отримання інформації про стан навколишнього середовища на основі ст. 50 Конституції тощо [8, с. 218—219].

Важливу роль відіграють адміністративно-правові відносини і в гарантуванні права людини на інформацію. Виходячи зі змісту Закону «Про інформацію», можна стверджувати, що гарантування в даному випадку розглядається законодавцем саме як створення необхідних умов. Адже названий закон (ст. 10) як гарантії права на інформацію називає [14]:

– обов’язок органів державної влади, а також органів місцевого і регіонального самоврядування інформувати про свою діяльність та прийняті рішення; створення у державних органах спеціальних інформаційних служб або систем, що забезпечували б у встановленому порядку доступ до інформації;

– вільний доступ суб’єктів інформаційних відносин до статистичних даних, архівних, бібліотечних і музейних фондів, обмеження якого зумовлюються лише специфікою цінностей та особливими умовами їх зберігання, що визначаються законодавством;

– створення механізму здійснення права на інформацію;

– здійснення державного контролю за додержанням законодавства про інформацію;

– встановлення відповідальності за порушення законодавства про інформацію.

Особливо в даному контексті слід виділити «механізм здійснення права на інформацію»,

який включає передусім різні аспекти відносин держави та засобів масової інформації, розвиток комунікаційної інфраструктури, системи освіти тощо.

Іншим аспектом проблеми є забезпечення інформаційних аспектів приватного життя. Конституційні права людини щодо приватного життя виступають у ролі обмежень компетенції органів державної влади. Тобто виконувати свої владні повноваження ці органи можуть лише за умови дотримання відповідних прав і свобод людини. Одною із значних загроз інформаційній безпеці людини в цій сфері залишаються можливості протиправного порушення відповідних її прав у процесі правоохоронної діяльності держави. Ця діяльність все ще вимагає значного реформування, аби відповідати тим вимогам демократичного суспільства, дотримання яких випливає з Конституції України та її міжнародно-правових зобов'язань.

В цілому, як стверджують фахівці, законодавчі приписи створюють доволі міцну правову базу гарантування інформаційної безпеки особи в процесі виконання органами внутрішніх справ своїх повноважень [16, с. 65—67]. Інша річ, що корені негативних явищ багато фахівців вбачають у тому, що на сьогодні правоохоронні органи занепокоєні в основному лише досягненням необхідної статистики розкриття злочинів, дуже часто будь-якими засобами. Внаслідок цього незаконні дії виявляються у вигляді безпідставних затримань і обшуків, у необ'єктивному інформуванні слідчого про наслідки оперативно-розшукових заходів, у збиранні компрометуючих матеріалів з метою відповідного впливу на громадянина, а іноді й у складанні оперативними працівниками хибних документів і фальсифікації злочинів [17]. Така ситуація, на нашу думку, має негативний вплив на рівень інформаційної безпеки в суспільстві.

Важливим напрямком, що визначає сучасний рівень інформаційної безпеки є, безумовно, забезпечення права особи на доступ до правової інформації. Адже якщо незнання закону не звільняє від відповідальності, то знання його надає додаткових можливостей, як утримуватися від дій, що можуть створювати загрозу державі або іншим, аргументовано вимагати забезпечення належного рівня власної безпеки.

Право на доступ до правової інформації ґрунтується на нормах ст. 57 Конституції, згідно з якими «кожному гарантується право знати свої права і обов'язки». Слід зазначити, що можливе також розширювальне тлумачення права громадян на доступ до правової інформації як можливості не лише знайомитися з текстами законів, а й отримувати певні правові знання, потрібні для того, щоб бути повноправним членом демократичного суспільства. Так, наприклад, досить поширеними є думки щодо необхідності здійснення державою заходів щодо поширення правових знань та правової пропаганди серед населення [18]. Але на сьогодні проблема загальнодоступного поширення правових знань, правової інформації, надання безкоштовних консультацій з правових питань вирішується в основному виключно зусиллями громадських організацій.

Наступним напрямом, що забезпечує належний рівень інформаційної безпеки є доступ людей до екологічної інформації. Екологічна безпека є загальносвітовою проблемою людства і тому повинна розглядатися за межами національної безпеки окремих держав. Разом з тим можна виділити її інформаційний аспект, який безпосередньо впливає на рівень захищеності конкретної особи і суспільства в цілому. Адже доступ до екологічної інформації може розглядатися як право і необхідність людини, громадянина бути поінформованим про можливі загрози, викликані змінами у навколишньому середовищі.

Втім, зазначає Б. Кормич, сьогодні в Україні існує невизначеність конкретних механізмів доступу до цієї інформації, що, в свою чергу, свідчить про певну декларативність конституційних норм. Адже екологічні проблеми є для України дуже болючими. І це не тільки наслідки Чорнобильської катастрофи, а й велика кількість локальних проблем, багато з яких пов'язані з наслідками діяльності військових об'єктів (підрозділів ракетних військ, різного роду сховищ небезпечних матеріалів тощо). Проблема в даному разі ускладнюється тим, що подібна інформація військового характеру дуже часто є таємною, тож недоступною для громадськості. Така ситуація вимагає розробки відповідного нормативно-правового регулювання забезпечення населення необхідною інформацією. На даному ж етапі, вочевидь, вказане конституційне право повинне реалізовуватися в порядку отримання громадянами інформації від органів державної влади та місцевого самоврядування [8, с. 228-229].

Ще один ключовий напрям, що дозволяє оцінити рівень інформаційної безпеки є

достатня поінформованість людини для здійснення свідомого і обґрунтованого вибору.

Свобода вибору практично лежить в основі більшості прав і свобод людини і охоплює більшість видів людської діяльності. В минулі століття розвиток прав людини багато в чому був спрямований на забезпечення цієї свободи вибору. Але якщо раніше головними чинниками, що обмежують цю свободу, вважалися неправедні закони, свавілля правителів, соціальна нерівність тощо, то на сьогоднішній день ситуація дещо змінилася. Залишилося не дуже багато держав, де утиски і порушення прав людини відбуваються відкрито, адже це викликало б негативну реакцію з боку світового співтовариства. Сьогодні порушення прав людини і загроза її безпеці дуже часто носять латентний характер, а інформаційний чинник виходить на перший план [19].

Сьогоднішні реалії такі, що на пересічну людину обрушується не бачений досі обсяг інформації різними каналами. Це новини, комерційна реклама і політична пропаганда, наукові, художні та інші подібні витвори, що розповсюджуються за допомогою як звичайних друкованих видань, радіо, телебачення, так і досить нових комп'ютерних програм, ігор, Інтернету тощо. І вплив такого інформаційного потоку на свідомість та діяльність людини лише вивчається. В цьому зв'язку О.Проскуріна зазначає, що Інтернет, як матеріальна основа інформації суспільства, незважаючи на його переваги, стає серйозною перешкодою на шляху гармонійного і стійкого інформаційного суспільства, оскільки виникає нова нерівність викликана неоднаковим доступом інформації, домінуванням одних країн та їх інформації над іншими [19, с. 105].

Так чи інакше, але, на нашу думку, питання інформаційно-психологічно впливу, тобто питання безпеки особи від інформації, на сьогоднішній день набуло важливого суспільного значення. Це означає, що ця проблема має вийти за рамки суто наукових дискусій та досліджень і вимагає розробки також у площині нормативно-правового регулювання.

Умовно цю проблему можна розділити на такі основні аспекти:

– інформаційна безпека індивідуальної, групової і суспільної свідомості в сфері комерційної реклами;

– інформаційна безпека індивідуальної, групової і суспільної свідомості від впливу відео, аудіо– і друкованих творів, комп'ютерних програм та ігор тощо;

– інформаційна безпека громадян як суб'єктів політичного процесу.

У перших двох випадках проблема інформаційної безпеки охоплює саме можливість провокування у людини певних несвідомих дій або дій, які не ґрунтуються на власному розсуді, досягнення яких було метою інформаційного впливу, а також побічних ефектів: певних протиправних дій або дій, які створюють небезпеку самій особі або третім особам, суспільству, досягнення яких не було метою інформаційного впливу, але було ним спровоковане.

Одним з яскравих прикладів можуть слугувати масові заворушення та порушення громадського порядку, що відбулися 9 червня 2002 р. у Москві на Манежній площі під час прямої трансляції матчу чемпіонату світу 2002 р. між збірними Японії та Росії. На думку багатьох представників мас-медіа та ряду працівників правоохоронних органів, одним з каталізаторів масових заворушень став рекламний ролик, який демонструвався перед матчем та під час перерви. Герой цього рекламного ролика за допомогою підручних засобів розбивав автомобіль. Можливо, що такі дії рекламного героя спровокували натовп біля екранів для вчинення аналогічних дій. Крім того, могла також мати ефект істерія з приводу очікуваної перемоги російської збірної над японцями, яка нагніталася в ЗМІ напередодні матчу, причому іноді використовувалися не реальні спортивні факти, а заклики, звернені до таких понять, як національна гордість, велич нації тощо. Це стосується впливу інформації на свідомість великої групи осіб, натовпу. Але й окремі особи можуть бути потерпілими від різних ефектів інформаційного впливу.

Можна погодитися з думкою А. Силенко, що поступовий розвиток інформаційно-комунікативних технологій, ставши найвпливовішим фактором економічного й соціального розвитку, обіцяє новому суспільству низку соціальних проблем, які згодом проявляться чіткіше й вимагатимуть свого рішення [20, с. 110]. А. Нальотов зазначає, що маніпулятивні технології — є найбільш небезпечними для масової свідомості [21, с. 128]. Це вже не кажучи про більш загальні негативні ефекти інформаційного впливу, що є наслідком рекламної або іншої інформації.

Останнім часом лунають думки і політиків, і широкої громадськості щодо загрози

моральним і етичним засадам українського суспільства, яку несуть у собі відео-, аудіо– і друкована продукція, що містить елементи насильства, жорстокості, жахів, порнографії тощо. В цьому контексті є цілий ряд норм, спрямованих на обмеження поширення інформації подібного роду [22], [23]. Проте, слід зазначити, що рівень захисту моральності в інформаційному просторі України ще не достатньо високий. На сьогоднішній день існують лише законопроекти з цих питань, обговорення яких все ще триває. Крім того, на нашу думку питання захисту моральності також межують із правом на свободу інформації. І в даному разі на перше місце потрібно ставити право кожної дієздатної людини самостійно вирішувати питання про отримання інформації непристойного з точки зору загальної моралі змісту.

У рамках захисту людини від негативного інформаційного впливу, що обмежує її свободу вибору, можна виділити ще один, досить специфічний і самостійний напрямок інформаційної безпеки людини і суспільства, який має виключне значення для оцінки рівня інформаційної безпеки як держави, так і громадянського суспільства. Це інформаційна безпека громадян — суб'єктів політичного процесу або інформаційна безпека прямого народовладдя.

Процеси проходження інформації, пов'язаної з проведенням виборів та референдумів, завжди були важливим елементом, що впливає як на їх перебіг, так і на їх результати. Інформація, що використовується при реалізації прямого народовладдя, зветься електоральною. Для більш чіткого аналізу існуючих загроз цьому процесу важливою є класифікація відносин, пов'язаних з електоральною інформацією, адже ні ця інформація, ні ці відносини не є однорідними.

Серед правових відносин, що виникають з приводу реалізації прямого народовладдя, фахівці виділяють такі основні групи:

Відносини, пов'язані із забезпеченням виборцям та учасникам виборів і референдумів поінформованості (розширення кола об'єктивних знань) з питань виборчого законодавства, законодавства про референдуми; з проблем державотворення, місцевого самоврядування з метою розвитку політико-правової культури громадян, підвищення їхньої правосвідомості як реальних і потенційних учасників названих процесів [24].

Відносини, пов'язані з інформаційним забезпеченням проведення виборів і референдумів на всіх основних стадіях. Серед них — підвищення професійних знань організаторів виборів та референдумів (членів виборчих комісій та комісій з референдумів, органів, що утворюють ці комісії) з метою забезпечення кваліфікованого проведення відповідних заходів; забезпечення правової поінформованості кандидатів та їхніх довірених осіб з питань висування та реєстрації кандидатів у депутати, правил ведення передвиборчої агітації, встановлених чинним законодавством, спілкування з виборцями, представниками засобів масової інформації та ін. Особливо слід завважити інформаційні відносини, пов'язані зі створенням іміджу кандидата або політичного об єднання (політична реклама зокрема) [25].

Більшість дій, що формують негативний, деструктивний вплив на означені електоральні інформаційні відносини, охоплюються широко вживаними в останні роки термінами «брудні виборчі технології» або «чорний PR».

Слід зазначити, що пропагандистсько-ідеологічні засади є найдавнішою опорою державної влади, адже вони свого часу стали одним з факторів формування цього феномена. Достатньо згадати різні теологічні концепції, що обстоювали «божественне» походження влади. З плином часу ідеологічні засади постійно змінювалися, але головне їхнє завдання залишалося однаковим — пояснити народові, чому саме ця влада повинна існувати, чому саме ці особи повинні управляти суспільством. Своє оригінальне бачення феномена державної влади було запропоноване свого часу М. Бердяєвим, який зазначав, що «державна влада може дуже раціонально правити народом, але саме джерело влади є зовсім ірраціональне. Вдача людей влади міститься в здатності до навіювання. Володарює той хто вергає народні маси в гіпнотичний стан. Пропаганда відіграє тут колосальну роль, вона є вульгарною формою гіпнозу. І якби люди володіли здатністю не піддаватися гіпнозу, то невідомо, яка влада могла б втриматися» [26, с. 268].

Виходячи з того, що права і свободи людини і громадянина, закріплені Конституцією України, не є вичерпними (ст. 22), слід розглядати «чорний PR» як спосіб обмеження вільного волевиявлення або ж як певні дії, що принижують гідність людини, впливають на її свідомість без її згоди.

Так, наприклад, найбільш поширеними під час виборчої кампанії 2004 р. були:

– масові порушення заборони на агітацію;

– використання службового становища керівниками органів місцевої влади та місцевого самоврядування;

– адміністративний тиск на суб'єктів виборчого процесу і ЗМІ;

– агітація шляхом безкоштовного або за зниженими цінами надання товарів та послуг;

– використання брудних передвиборчих технологій (чорний PR) — поширення інформації (агітація) від імені конкурента, порушення процедури формування виборчих комісій, факти насилля щодо учасників виборчого процесу;

– пряма агітація з боку посадових осіб [27, с. 23—26].

Як можна побачити, більшість з перерахованих порушень являє собою негативне інформаційне втручання у хід виборчої кампанії. На жаль, українське виборче законодавство дуже мало уваги приділяє безпосередньо питанням інформаційної безпеки, а навіть нечисленні існуючі норми не мають механізмів реалізації.

Оцінка рівня інформаційної безпеки вимагає врахування впливу нового явища, що останнім часом з'явилося в світі — це інформаційний тероризм. Доцільно зауважити, що проблеми інформаційного тероризму сьогодні ще недостатньо вивчені, але є найбільш реальною загрозою для так званого кібернетичного простору (кіберпростору) як окремих розвинених країн, так і усього світу. Для України ця проблема, безумовно, актуалізується з розвитком і активним поширенням на її території глобальної системи Інтернет.

Терміном «кіберпростір» характеризують інформаційно-технологічні складові сучасного суспільства. Його характерними і специфічними рисами є відсутність географічних кордонів, значні труднощі у визначенні національної належності об'єктів та можливість анонімного доступу до ресурсів [28]. Такі властивості кіберпростору роблять його уразливим з боку недружніх країн, терористичних організацій, кримінальних груп і окремих злочинців. У кіберпросторі можуть використовуватися різноманітні прийоми досягнення політичних, воєнних, кримінальних чи терористичних цілей (нанесення шкоди суспільному устрою, окремим фізичним елементам, крадіжка чи знищення інформаційного, програмного та технічного ресурсу, вплив на операторів тощо). Зокрема, К. Сарксова вказує, що Інтернет справляє серйозний вплив на політичне життя суспільства, незважаючи на те, що існує багато причин теоретичного і практичного характеру, які змушують сумніватися в існуванні безпосереднього зв'язку між змінами у сфері комунікаційних технологій і політичної активністю населення [29, с. 71]

Висновок. Таким чином, оцінка сучасного рівня інформаційної безпеки українського суспільства є досить складним завданням, що вимагає аналізу широкого кола проблем, напрямків та їх інтерпретації в організаційно-правовому полі, як основи побудови всієї системи національної безпеки. В її основі повинна бути методологія щодо оцінки діяльності органів державного управління з надання гарантій інформаційної безпеки особі, соціальним групам та суспільству в цілому.

Література

1. Глобалізація і безпека розвитку : монография / [О. Г. Білорус, Д. Г. Лук'яненко та ін.]. — К. : КНЕУ, 2001. — 733 с.

2. Белл Д. Социальные рамки информационного общества: Пер.с англ / Д. Белл. — М. : Прогресс, 1986. — 310 с.

3. Почепцов Г. Г. Информационные войны / Г. Г. Почепцов. — М. : «Рефл.-бук», — К. : «Ваклер», 2000. — 574 с.

4. Рейман Л. Д. Информационное общество и роль телекоммуникаций в его становлении / Л. Д. Рейман // Вопросы философии. — 2001. — № 3. — С. 3-9.

5. Закон України «Про основи національної безпеки України» від 19 червня 2003 р. // Голос України. — 22 липня 2003 р. — № 134.

6. Закон України «Про Концепцію національної програми інформатизації» від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України, 1998. — № 27-28. — Ст. 182

7. Рабинович П. М. Основи загальної теорії права та держави / П. М. Рабинович. — К. : Атака, 2001. — 160 с.

8. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посібник / Б. А. Кормич. — К. : Кондор, 2004. — 384 с.

9. Тарасов А. Право народов на самоопределение как фундаментальный демократический принцип / А. Тарасов // Свободная мысль. Теоретический и политический журнал. — 2002. — № 9. — С. 60-70.

10. Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради, 1996. — № 30. — Ст. 141.

11. Національна безпека України, 1994-1996 рр. Наукова доповідь НІСД / Редкол.: О. Ф. Бєлов (голова) та ін. — К. : НІДС, 1997. — С. 124-125.

12. Лисенко В. Проблеми інформаційної незалежності держави / В. Лисенко // Політичний менеджмент. — 2006. —№ 4. — С. 135-147.

13. Дзьобань О. П. Національна безпека в суспільствах транзитивного типу : монографія / О. П. Дзьобань. — Х. : НАУ ім. М. Є.Жуковського «ХАІ», 2004. — 291 с.

14. Закон України «Про інформацію» від 02 жовтня 1992 р. // Відомості Верховної ради України, 1992. — № 48. — Ст. 650.

15. Скриль С. А. Адміністративно-правові засоби реалізації прав людини в Україні / С. А. Скриль // Актуальні проблеми політики. 36. наук, праць. Вип. 13 — 14. — Одеса, 2001. — С. 194-197.

16. Проскуріна О. Політико-правові аспекти розвитку інформаційного суспільства в Україні / О. Проскуріна // Політичний менеджмент. — 2006. — № 3. — С. 62-68.

17. Отношения между милицией и населением в Украине: данные и анализ в контексте украинско-британского проекта / А. Дж. Бек, Ю. Б. Чистякова, А. В. Паволоцкий [и др.]. // Право і Безпека. — 2002. — № 2. — С. 161-170.

18. Лісний В. В. Політико-правовий всеобуч як засіб формування суспільної свідомості / В. В. Лісний / Шляхи формування громадянського суспільства в Україні. Забезпечення прав людини на свободу слова і інформацію. (За матеріалами засідання «круглого столу», проведеного 11 квітня 2001 р. в м. Харкові) : наук. збірник. — Х.: УАДУХФ, 2001. — С. 94-101.

19. Проскуріна О. Виклик комунікацій і відповідь культурного поля політики / О. Проскуріна // Політичний менеджмент. — 2005. — № 2. — С. 103-107.

20. Силенко А. Інформаціні технології — новий імпульс для пошуку парадигм майбутнього суспільства / А. Силенко // Політичний менеджмент. — 2007. — № 3. — С. 96-112.

21. Нальотов А. Виборчі технології як чинник впливу на масову свідомість / А. Нальотов // Політичний менеджмент. — 2007. — № 5. — С. 126-137.

22. Закон України «Основи законодавства України про культуру» від 14 лютого 1992 р. № 2117–XII // Відомості Верховної Ради України, 1992. — № 21. — Ст. 294.

23. Закон України «Про видавничу справу» від 5 червня 1997 р. № 318/97–ВР // Відомості Верховної Ради України, 1997. — № 32. — Ст. 206.

24. Бортніков В. Особливості участі громадян в концептуальних моделях демократії / В. Бортніков // Політичний менеджмент. — 2007. — № 3. — С. 38-50.

25. Ротар Н. Політична участь громадян в умовах е-демократизації / Н. Ротар // Політичний менеджмент. — 2006. — № 2. — С. 78-106.

26. Бердяев Н. А. Судьба России / Н. А. Бердяев. — М. : Советский писатель, 1990. — 342 с.

27. Мацієвський Ю. Між авторитаризмом і демократією: політичний режим після помаранчевої революції / Ю. Мацієвський // Політичний менеджмент. — 2006. — № 5. — С. 18-32.

28. Требін М. Інформаціне суспільство. Війни нової епохи / М. Требін // Віче. — 2002. — № 4 (121) — С. 64-68.

29. Саркісова К. Електронна демократія як форма політичної комунікації у сучасному суспільстві / К. Саркісова // Політичний менеджмент. — 2007. —№ 1. — С. 66-74.

Надійшла до редколегії 20.02.2012 р.