АКАДЕМІЯ НАУК ВИЩОЇ ОСВІТИ УКРАЇНИ
GLOBAL ACADEMY OF ALLIED LEADERSHIP
ACADEMY OF OPEN SOCIETY SECURITY

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ БОРОТЬБИ З ТЕРОРИЗМОМ

Матеріали науково-практичної конференції

Київ, 15 липня 2012 р.

Київ
Видавець О. С. Ліпкан
2012

УДК 34(477)
ББК 67.9(4Ук)7я7
І 741

І 741 **Інформаційні технології боротьби з тероризмом :** матеріали міжнародної науково-практичної конференції (Київ, 15 липня, 2012 р.). — К. : ФОП Ліпкан О. С., 2012. — 92 с.

ISBN 78-966-2439-39-7

У збірнику знайшли відображення результати міжнародної науково-практичної конференції, присвяченої інформаційним технологіям боротьби з тероризмом в умовах глобальних трансформацій.

Збірник розраховано на усіх тих, хто не байдужий до інформаційних, геополітичних і безпекових проблем сучасності.

УДК 34(477)
ББК 67.9(4Ук)7я7

ISBN 978-966-2439-39-7

АКАДЕМИЯ НАУК ВЫСШЕГО ОБРАЗОВАНИЯ УКРАИНЫ
ГЛОБАЛЬНАЯ ОРГАНИЗАЦИЯ СОЮЗНИЧЕСКОГО ЛИДЕРСТВА
АКАДЕМИИ БЕЗОПАСНОСТИ ОТКРЫТОГО ОБЩЕСТВА

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ БОРЬБЫ С ТЕРРОРИЗМОМ

Материалы международной научно-практической конференции

Киев, 15 июля 2012 р.

Киев
Издатель Липкан Е. С.
2012

ЗМІСТ

ТЕНДЕНЦИИ РАЗВИТИЯ ИНФОРМАЦИОННОГО ПРАВА В КОНТЕКСТЕ БОРЬБЫ С ТЕРРОРИЗМОМ

ПРАВО НА ИНФОРМАЦИАННУЮ БЕЗОПАСНОСТЬ КАК ИНСТИТУТ ПРАВА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

СУЩНОСТЬ МАНИПУЛИРОВАНИЯ СОЗНАНИЕМ И ДЕМОРАЛИЗУЮЩАЯ ПРОПАГАНАДА

СУЩНОСТЬ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ В КОНТЕКСТЕ БОРЬБЫ С ТЕРРОРИЗМОМ

ИНФОРМАЦИОННОЕ ОБЩЕСТВО И СОДЕРЖАНИЕ ИНФОРМАЦИОННОЙ ФУНКЦИИ ГОСУДАРСТВА В БОРЬБЕ С ТЕРРОРИЗМОМ

ТЕНДЕНЦИИ РАЗВИТИЯ ИНФОРМАЦИОННОГО ПРАВА В КОНТЕКСТЕ БОРЬБЫ С ТЕРРОРИЗМОМ

СИСТЕМАТИЗАЦІЯ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА ЯК НАПРЯМ БОРОТЬБИ З ТЕРОРИЗМОМ

ЛІПКАН Володимир Анатолійович,
професор кафедри управління в ОВС НАВС,
доктор юридичних наук, доцент
Академік Академії наук вищої освіти України,
Академік Міжнародної кадрової академії

Формування інформаційного суспільства супроводжується дедалі більшим проникненням його у кожну сферу суспільного життя. Змушений визнати, що нині більшість дослідників із штучним пафосом співає хвалебні оди інформаційному суспільству, занурюючись лише в інформаціологічний зміст даної проблеми, натомість, ігноруючи системний вимір даного феномену, в тому числі і безпековий. Почасти в публікаціях дослідників можна зустріти підходи до вивчення інформаційного суспільства лише в рамках концепцій, запропонованих Ф. Уебстером. Різноманітні інтерпретації ніяк не впливають на змістовний бік, адже формування інформаційного суспільства розглядається як безальтернативне. Така думка не відповідає нашому концептуальному підходу щодо неможливості аксіматизувати концептуальні положення у сфері гуманітарних наук. Адже не відкрию новину, коли скажу, що інспіровані ззовні державні перевороти в країнах північної Африки, так звана «арабська весна», «кольорові революції» — стали наслідком застування новітніх технологій деструктивізації інформаційного суспільства, використання новітніх способів та методів ведення інформаційного протиборства. На жаль дана тема і нині, незважаючи на її значний інтерес, лишається не заторкнутою у багатьох наукових школах інформаціологічного спрямування. Перманентна дестабілізація інформаційного простору, насадження псевдоукраїнських цінностей, умисне розшарування суспільства за різними ознаками тощо — це все прояви існуючого інформаційного протиборства про-

ти України. І за даного випадку важливим етапом такого антипатріотичного державного поступу є формування інформаційного права на концептуально нових безпекових засадах. Адже, будучи за своєї суттю міждисциплінарним науковим напрямом, інформаційне право фактично має стати метаправом нинішнього суспільства.

Важливим етапом формування ефективної державної антитерористичної політики виступає єдність, цілісність, мінімалізована колізійність законодавства. У даному аспекті, важливим дослідницьким завданням виступає вивчення проблем систематизації інформаційного законодавства, яке виступає своєрідним камінцем свободи дальшого правового інформаційного розвитку соборної України.

Зазначу, що визначення поняття «***систематизація***» знайшло своє відображення в численних наукових працях юридичного характеру. Хоча, з одного боку, ряд дослідників зазначають, що систематизація має на меті стабілізацію правопорядку, перетворення нормативно-правового регулювання на інструмент для забезпечення нормального життя суспільства та найбільш ефективного управління державними справами в інтересах особи. З іншого боку, деякі науковці обстоюють позицію, що введення в науковий обіг категорії «систематизація» було штучним, проведеним без переконливого обґрунтування, а отже, й без потреби [1].

Ще за радянських часів існували діаметрально протилежні наукові позиції щодо змісту поняття «систематизація законодавства». Ряд авторів (*С. О. Голунський, М. С. Строгович, О. Ф. Шебанов* та ін.) підтримували позицію, згідно з якою систематизація — це родове поняття, що охоплює всю діяльність з упорядкування законодавства. Інші вчені (*З. К. Симорот, Е. О. Монастирський, А. І. Рогожин, С. С. Алексєєв* та ін.) виступали за звуження цього поняття, вважаючи, що за допомогою систематизації можна вдосконалити лише форму, але не зміст чинного законодавства, а тому її слід розглядати як специфічний метод, що застосовується в процесі підготовки основ законодавства, кодексів, збірників законів та окремих нормативно-правових актів.

Є також ряд радянських вчених, які взагалі не оперували таким поняттям, як систематизація. Усю діяльність з упорядкування законодавства вони називали кодифікацією і поділяли її на два види: кодифікація у вузькому розумінні та кодифікація у широкому розумінні. Так, *А. М. Іодковський* під *кодифікацією у вузькому розумінні* розглядав винятково законодавчу діяльність, пов'язану з ліквідацією попереднього законодавства, і з повною його заміною новоприйнятими законами. Під *кодифікацією в широкому розумінні* — доповнення законодавчого процесу, спрямоване на технічне впоряд-

кування чинного законодавства, фіксацію його й усунення з нього актів, що втратили силу [2, с. 7–8].

Отже, в різні історичні періоди поняття «систематизація» мало неоднаковий зміст. Нині значних розбіжностей у розумінні поняття «систематизація» в юридичній науці немає.

Функціональні характеристики систематизації нормативно-правових актів надають можливість дійти висновків, що ***основними функціями систематизації*** виступають:

- уможливлює оглянути весь масив чинного законодавства;
- виявляє й усуває неузгодженості, суперечності, прогалини правового регулювання;
- підвищує ефективність законодавства;
- робить законодавство інформаційно доступнішим, зручнішим для використання, полегшує пошук потрібної норми;
- сприяє вивченню і дослідженню законодавства;
- робить законодавство інтелектуально доступнішим (полегшує з'ясування змісту норм);
- сприяє правовому вихованню громадян, формуванню їх правосвідомості.

Ураховуючи вищезазначені думки дослідників щодо розуміння поняття «систематизація законодавства», беручи до уваги функціональні характеристики цієї діяльності та екстраполюючи на предмет нашого дослідження, вважаємо за необхідне висловити авторське розуміння поняття «систематизація інформаційного законодавства».

Систематизація інформаційного законодавства — цілеспрямована діяльність компетентних органів чи окремих осіб з упорядкування нормативно-правових актів, що регулюють інформаційні відносини, з метою підвищення ефективності правореалізації у даній сфері.

Якщо визначення поняття «систематизація законодавства» в наукових колах на сучасному етапі не стало предметом широкої дискусії, то питання виокремлення основних її форм є доволі неоднозначним.

Беручи за критерій спрямованість та мету систематизації, деякі із дослідників виокремлюють два її види: зовнішню і внутрішню. Так, *метою внутрішньої систематизації* є змістовне перероблення нормативно-правових актів, що спрямоване на досягнення внутрішньої єдності юридичних норм, на усунення колізій та прогалин у праві [3, с. 164]. *Метою зовнішньої систематизації* є впорядкування форми нормативно-правових актів, зокрема їх класифікація за певними критеріями [4, с. 37].

Є. В. Погорелов зазначає, що розгляд властивостей зовнішньої і внутрішньої систематизації з урахуванням її функціональних характеристик вка-

зує на те, що за характером цієї діяльності необхідно розрізняти правотворчу та неправотворчу систематизацію. Внутрішня систематизація має правотворчий характер, а зовнішня — неправотворчий. До правотворчої систематизації слід віднести кодифікацію законодавства та консолідацію, до неправотворчої — таку її форму, як інкорпорація [5, с. 38].

Окрім вищезазначених класифікацій, контент- та івент-аналіз наукових джерел у цій сфері дає змогу виокремити *два основні підходи* щодо видів (форм) систематизації.

Згідно з *першим підходом* виділяють чотири її види:

кодифікацію,	консолідацію;
інкорпорацію,	облік [6].

Найбільш поширеним *підходом* є *другий*, відповідно до якого виокремлюються три *види систематизації*:

1) кодифікацію; *2)* інкорпорацію;

3) консолідацію [7–9].

Так, дослідники аргументують, що ***облік*** нормативно-правових актів не можна зараховувати до форм систематизації законодавства, оскільки така діяльність не усуває і не пом'якшує дефектів чинного законодавства, а є необхідним етапом здійснення кодифікаційної діяльності, технічним засобом, спрямованим на полегшення систематизації.

Опоненти цієї думки зазначають, що як різновид систематизації облік законодавства й інших нормативних правових актів є діяльністю з їх збору, збереження та підтримки в контрольному стані, а також діяльністю зі створення пошукової системи, яка забезпечує знаходження необхідної правової інформації в масиві актів, узятих на облік [6, с. 44].

Цікаво, що в цій сфері спостерігається не тільки наукова дискусія, а й ряд проектів нормативно-правових актів містять різні думки щодо цього. Так, в проекті закону України «Про нормативно-правові акти» виокремлюються тільки ***три форми систематизації:*** кодифікація, інкорпорація та уніфікація. У ст. 45 проекту закону України «Про закони і законодавчу діяльність» визначено, що систематизація законів здійснюється Верховною Радою України шляхом кодифікації, тобто зведення положень різних законів до юридично і логічно узгодженої системи та створення на цій основі і прийняття єдиного зведеного закону — кодексу, а також шляхом інкорпорації, що передбачає зведення законів у єдиний Звід законів України без зміни їх змісту.

В іншому проекті закону України «Про закони і законодавчу діяльність» міститься ще ряд дискусійних положень, зокрема зазначається, що облік не

є видом систематизації, інформація про консолідацію взагалі відсутня, а єдиним актом, що створюється в процесі кодифікації, називається кодекс [10].

Слід зазначити, що поділ систематизації законодавства на відповідні види має умовний характер, оскільки при проведенні тих чи інших систематизаційних робіт комплексно використовуються прийоми та правила всіх видів. Домінування ж тих чи інших прийомів та правил і обумовлює можливість виокремлення конкретного виду систематизації.

Ефективність державної антитерористичної політики на пряму пов'язана з ефективним регулювання функціонування та безпечного розвитку інформаційного суспільства. Систематизація інформаційного законодавства виступає цементуючою основою, методологією, напрямом розвитку правового регулювання інформаційної сфери. Важливими елементами даної проблеми виступають кодифікація, консолідація та інкорпорація інформаційного законодавства, окремі проблеми права на доступ до інформації про що йтиметься далі в статтях моїх учнів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ліпкан В. А. Систематизація інформаційного законодавства України : [Монографія] / В. А. Ліпкан, В. А. Залізняк / За заг. ред. В. А. Ліпкана. — К. : ФОП О. С. Ліпкан, 2012. — 304 с.
2. Иодковский А. Н. Вопросы кодификации законодательства : дис ... канд. юрид. наук / А.Н. Иодковский. — М., 1948. — 189 с.
3. Рабінович П. М. Основи загальної теорії права та держави. — К., 1994. — 236 с.
4. Сперанский М. М. Краткое историческое обозрение Комиссии составления законов. Предложение к окончательному составлению законов / М. М. Сперанский // Русская старина. — 1876. — № 2.
5. Погорєлов Є. В. Кодифікаційна діяльність в правовій системі України (загальнотеоретичний аспект) : дис. … канд. юрид. наук : 12.00.01 / Євген Валентинович Погорєлов. — Х., 2000. — 166 с.
6. Граціанов А. І. Процес систематизації та уніфікації законодавства і розвиток правової системи України : дис. … канд. юрид. наук : 12.00.01 / Анатолій Ігорович Граціанов. — К., 2004. — 185 с.
7. Меленко С. Г. Консолідація як вид систематизації нормативно-правових актів : дис. … канд. юрид. наук : 12.00.01 / Сергій Гаврилович Меленко. — Чернівці, 2002. — 206 с.
8. Скакун О. Ф. Теорія держави і права : [Підручник] / О. Ф. Скакун. — Харків : Консул, 2008. — 656 с.
9. Гусарєв С. Д. Теорія права і держави : [Навчальний посібник] / С. Д. Гусарєв, А.Ю. Олійник, О.Л. Слюсаренко. — К. : Всеукраїнська асоціація видавців «Правова єдність», 2008. — 270 с.
10. Проект Закону України «Про закони і законодавчу діяльність» // Офіційний сайт Верховної Ради України. — www.rada.kiev.ua

ІНКОРПОРАЦІЯ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА ЯК НАПРЯМ БОРОТЬБИ З ТЕРОРИЗМОМ

ЧЕРЕПОВСЬКИЙ Кирил Павлович,
здобувач кафедри адміністративного та фінансового права
Національного університету біоресурсів і природокористування України

Будучи одним із представників наукової школи інформаційного права В.А.Ліпкана, у своїй статті зі збереженням концептуального напряму нашої школи, положень викладених в статтях В.А.Ліпкана, М.І.Дімчогло та К.Г.Татарникової сформую власні тези щодо інкорпорації інформаційного законодавства в контексті боротьби з тероризмом [1].

Зазначу, що здійснений мною догматико-юридичний та логіко-семантичний аналіз наукової літератури за темою дослідження дозволив дійти висновку, що, незважаючи на значну кількість праць, присвячених окремим науковим аспектам інкорпорації у структурі систематизації законодавства України загалом та інформаційного законодавства зокрема, методології, методикам його комплексного і системного дослідження на рівні інкорпорації на монографічному рівні не здійснювалось. У наукових розвідках з інформаційного права значна увага присвячена переважно кодифікації як одній із форм систематизації при цьому питання інкорпорації як першого етапу і виду систематизації розглядаються фрагментарно. Такі твердження не носять еклектичний характер, а ґрунтуються на проведеному мною ретельному вивченні даного питання, оскільки моя дисертація становить перше в незалежній Україні дослідження, присвячене безпосередньо дослідженню питань інкорпорації інформаційного законодавства.

У рамках нашої наукової школи під інформаційним законодавством України пропонується розуміти систему нормативно-правових актів, що мають статус юридичних законів, чинних міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України. При інкорпорації інформаційного законодавства інші нормативно-правові акти пропонується розглядати як факультативні, такі, що є підзаконними, прийнятими відповідно до компетенції органами державної влади у розвиток положень Конституції України та законів України, Доктрини інформаційної безпеки України, що регулюють інформаційні правовідносини.

Проведений нами аналіз термінології дає можливість висновувати, що у правовій термінології поряд із категорією «систематизація законодавства» застосовуються близькі за сутністю та змістом інші категорії, зокрема: «удо-

сконалення законодавства», «розвиток законодавства», «підвищення ефективності законодавства». Застосовуючи метод формування гіперсистем у праві, категорію «удосконалення законодавства» пропонується вважати ширшою за обсягом змісту, ніж «систематизація законодавства» у зв'язку з тим, що остання є однією з інших форм удосконалення, його наслідком. При цьому не будь-яка систематизація може мати наслідком удосконалення. Про що свідчить аналіз чинного інформаційного законодавства.

Щодо категорії «розвиток законодавства», то його пропонується розглядатися як ширше за обсягом ніж категорія «удосконалення законодавства», оскільки воно охоплює не тільки зміну якісних показників законодавства, але й кількісних. Стосовно розуміння категорії «підвищення ефективності законодавства», на наш погляд, за змістом вона є ширшою за категорію «удосконалення законодавства», оскільки удосконалення є лише одним із факторів, що впливають на її ефективність. Крім удосконалення законодавства, ефективність законодавства обумовлена також практикою правореалізації, рівнем правової культури населення, соціально-культурним, економічним та політичним потенціалом конкретної країни тощо. Саме тому категорія «підвищення ефективності законодавства» є ширшим за поняття «удосконалення законодавства».

Згідно з позицією нашої наукової школи ми виділяємо три етапи систематизації інформаційного законодавства: інкорпорацію, консолідацію, кодифікацію.

Інкорпорація визначається не тільки як вид систематизації законодавства, але і першим його етапом, що присутній за наслідками і при консолідації та при кодифікації. Тобто інкорпорація може розглядатися не тільки як вид систематизації законодавства, але і як перший етап чи метод для подальшої реалізації консолідації та кодифікації [2].

При інкорпорації інформаційного законодавства, у розумінні її як процесу пов'язаного із формуванням зводу законів щодо інформації слід враховувати певні критерії: визначення інформації предметом правовідносин у законодавчих актах як прямо так і опосередковано; хронологічність прийняття законодавчих актів; визначення змісту правовідносин щодо інформації; наявність у законодавчих актах легальних гіперзв'язків, застосування консолідації (посилання) на інші законодавчі акти тощо.

Ми поділяємо позицію тих дослідників які вважають, що при інкорпорації інформаційного законодавства пропонується брати за основу його спеціальний галузевий законодавчий акт — Закон України «Про інформацію». Саме його положення мають знаходити подальший розвиток у ряді спеціальних законів за окремими юридично структурованими інститутами інфор-

маційного права, видами, напрямами інформаційної діяльності, суб'єктами інформаційних відносин за різними концептуальними підходами юридичної техніки законотворення. Цей Закон, до прийняття Кодексу України про інформацію, у комплексі має відігравати функцію як законодавчої інкорпорації, так і функцію законодавчої консолідації. У перспективі Закон України про інформацію має бути трансформований у Кодекс України про інформацію.

Найскоріше ухвалення даного кодексу значно підсилить правову складову регулювання застування інформаційних технологій боротьби з тероризмом, сприятиме формуванню антитерористичної свідомості, а також закладе фундамент для безпечного розвитку інформаційного суспільства, одним з елементів якого виступає антитерористична безпека.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ліпкан В. А. Систематизація інформаційного законодавства України : [Монографія] / В. А. Ліпкан, В. А. Залізняк / За заг. ред. В. А. Ліпкана. — К. : ФОП О. С. Ліпкан, 2012. — 304 с.
2. Череповський К.П. Елементи структуризації міжнародного інформаційного права : матеріали науково-практичної конференції (Луцьк, 22 квітня 2012 р.). — К. : ФОП О. С. Ліпкан. — С. 40–44.

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ТА ДОТРИМАННЯ ПРАВА ЛЮДИНИ ТА ГРОМАДЯНИНА НА ДОСТУП ДО ІНФОРМАЦІЇ

КАПІНУС Людмила Іванівна,
доцент кафедри міжнародного права
та порівняльного правознавства
Київського міжнародного університету

На сьогоднішній день суспільство все більше стикається з такою глобальною проблемою як сплеск терористичних актів, що мали місце в багатьох країнах майже всіх континентів Земної кулі (11 вересня 2001 р. — події в США, 1 вересня 2004 р. — захоплення заручників у школі міста Беслан в Північній Осетії та інші). Аналізуючи саме визначення тероризму, ми повинні визначити його суть, основні ознаки та наслідки цих дій для населення в

цілому, та права на доступ до інформації, зокрема. Визначення сутності тероризму є досить складним завданням, оскільки в своїй основі він має як політичні, так і етнічні чи релігійні підвалини і використовує в своєму арсеналі різні методи. Термін «тероризм» походить від слова «терор», що в перекладі з латини означає «жах», «насильство». [1; С. 158]

В даний час налічується значна кількість визначень «тероризму» як на міжнародному, так і на національному рівнях. В законодавстві України воно сформульоване наступним чином «тероризм» — суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних цілей. [2] В.А. Ліпкан пропонує розглядати тероризм ще і як негативне соціально-правове явище і не зводити його лише до вчинення вибухів і підпалів.[3; С. 25]

Крім того, що збільшується масштаб здійснення терористичних актів, не лише сухопутний чи морський простір, але й повітря, також збільшуються і сфери, які зазнають шкоди та методи вчинення даних актів. Оскільки суспільство, яке розвивається з початком XXI століття, прийнято вважати інформаційним суспільством, то перед нами стоїть задача визначити, яким же чином тероризм впливає на інформаційні відносини та запропонувати шляхи вирішення даної проблеми. Тероризм завдає шкоди стабільності в країні та окремих регіонах світу, створює перешкоди на шляху економічного, соціального та культурного прогресу, а також несе загрози життю і правам людини. Виділяють такі основні різновиди тероризму — економічний, духовний та політичний. [1; С. 158]

На нашу думку, вдалим є вирізнення ще одного виду тероризму — «інформаційний тероризм», під яким розуміють дії окремих осіб або їхніх груп щодо дезорганізації роботи автоматизованих систем і мереж зв'язку, що створюють небезпеку життю людей, спричиняють значні матеріальні збитки або інші суспільно небезпечні наслідки, а також загроза здійснення вказаних дій, якщо вони відбуваються з метою порушення суспільної безпеки, залякування населення або здійснення впливу на прийняття рішень органами влади. До кібертероризму відносять також деструктивні дії щодо інформаційних систем, які створюють умови для проведення актів тероризму.[4; С. 30]

Головною проблемою боротьби з інформаційним тероризмом та порушенням права на доступ до інформації є те, що інформаційні відносини регулюються нормами не лише інформаційного, але також і конституційного, кримінального та інших галузей права, а також звичаїв, традицій, морально-

етичних імперативів. Можна зазначити, що перед міжнародною спільнотою стоїть задача прийняття універсального імперативного нормативно-правового акту, який би чітко давав дефініції, основні ознаки інформаційного тероризму та відповідальність осіб, які безпосередньо та опосередковано приймали в ньому участь.

Інформаційний тероризм проявляється не лише в кібер-злочинах, а також і в приховуванні інформації, яка має важливе значення, та маніпулюванні свідомістю особистості і, частіш за все, не має якогось ідеологічного, релігійного чи матеріального підґрунтя. Він здійснюється в сфері політики, права чи релігії і його небезпека підсилюється тим, що не можна ввести в законні рамки використання основного, на нашу думку, засобу здійснення інформаційного тероризму — мережі Інтернет.

Щодо порушення права на доступ до інформації, то терористичні дії прямо порушують його, оскільки при їх вчиненні, по-перше, населення не має можливості отримати повну інформацію про все, що відбувається, та, по-друге, на населення «наганяється» страх за себе, своїх рідних та близьких, шляхом надання недостовірною інформації.

Отже, інформаційний тероризм є нелегітимним засобом, формою негативного впливу на людей та громадян країни усіма видами інформації. Основною його метою, в даному випадку, є порушення конституційного ладу, незаконне отримання інформації з обмеженим доступом і методи його проведення на сьогоднішній день досить важко визначити.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Вегеша М.М. Політологія: Підручник / За ред. М.М. Вегеша. — 3-тє вид., перероб. і доп. — К.: Знання, 2008. — 384 с.
2. Про боротьбу з терроризмом. Закон України від 20.03.2003 р. — [Електронний ресурс]. — Режим доступу. — http://zakon1.rada.gov.ua/laws/show/638–15/page2
3. Ліпкан В.А. Тероризм і національна безпека України. / В.А. Ліпкан. — К.: Знання, 2000. –184 с.
4. Гуцу С.Ф. Правові основи інформаційної діяльності: Навч. посібник / С. Ф. Гуцу. — Х.: Нац. Аерокосм. Ун-т «Харк. авіац. ін.-т», 2009. — 48 с.

КОДИФІКАЦІЯ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА ЯК НАПРЯМ БОРОТЬБИ З ТЕРОРИЗМОМ

ТАТАРНИКОВА Кристина Геннадіївна,
здобувач Національного університету біоресурсів і природокористування

Будучи одним із представників наукової школи інформаційного права В.А.Ліпкана, у своїй статті зі збереженням концептуального напряму нашої школи, положень викладених в статтях В.А.Ліпкана, М.І.Дімчогло та К.П.Череповського сформую власні тези щодо кодифікації інформаційного законодавства в контексті боротьби з тероризмом.

Як форма систематизації законодавства, кодифікація виступає найкращим не лише видом, напрямом або етапом удосконалення правового регулювання інформаційних правовідносин. На відміну від інших форм систематизації інформаційного законодавства (інкорпорації, консолідації), кодифікація охоплює як зовнішню, так і внутрішню обробку нормативно-правового масиву, тобто впорядковується не тільки форма законодавства, а й за структурою переробляється його зміст. При цьому зміст структурується за чітко визначеними інституційними ознаками.

У комплексних галузях права при поділі на інституту можна виділити дві основні тенденції: поділ на дві або на три частини. Ми підтримуємо позицію тих дослідників, особливо це стосується інформаційної сфери, які пропонують поділяти інформаційне право на три частини : загальну, особливу та спеціальну [1]. За сутністю особливі та спеціальні положення не тільки повинні відповідати загальним положенням, але і розвивати їх відповідно до сучасних тенденцій розвитку інформаційного суспільства і реалізацією держави інформаційної функції у боротьбі з тероризмом [2]. У зв'язку з цим кодифікація комплексних галузей законодавства виступає найвищим рівнем їх систематизації, що передбачає переосмислення, творче переосмислення та перероблення, вдосконалення всього правового матеріалу, що існує в даний час у державі. Тобто, саме галузева кодифікація сприяє створенню якісної форми всієї системи законодавства, що, в свою чергу, позитивно впливає на ефективність протидії тероризму в Україні.

Для додаткової аргументації необхідності, доцільності, унікальності та ефективності кодифікації інформаційного законодавства звернемося до аналізу наукових поглядів Є. В. Погорєлова. Він зазначає: «У процесі

кодифікаційної діяльності на відміну від поточної правотворчості здійснюється глибокий перегляд всього чинного законодавства в даній сфері та його більш чи менш широке включення до кодифікаційних актів; кодифікація як форма правотворчості використовується для вирішення перспективних завдань розвитку законодавства; при кодифікаційній діяльності ведеться найбільш старанний і глибокий облік закономірностей суспільного розвитку, забезпечується вірне відображення перспектив цього розвитку в законодавстві, що підлягає кодифікації; об'єктивною передумовою успішної кодифікаційної роботи, життєздатності й стабільності кодифікаційних актів є відносна стабільність суспільних відносин, що підлягають кодифікаційній обробці» [3, с. 44].

Стосовно останнього, у контексті конструктивної критики, ми приєднуємося до позиції тих дослідників, які вважають, що стабільність суспільних відносин і стабільність кодифікованих актів не є обов'язковою умовою кодифікації. Відповідно до засадничих положень теорії національної безпекознавства [4–6] не виключається розгляд стабільності і як загрози безпеці. Авторитаризм, олігархізм, тоталітаризм тощо можуть створювати тільки зовнішній антураж, уявність стабільності в суспільстві. З позицій терорології [7, 8], розгляд «стабільності», статики у суспільстві може бути проявом його колапсу, внутрішньої деградації. У стабільних суспільствах значно підвищується ризик виникнення внутрішнього тероризму, оскільки суспільство постійне прагне до змін і якщо держава ці зміни не пропонує, то воно вирішує це зробити власноруч. Тут доречно нагадати мудрий народний вислів: стабільність у суспільних утвореннях існує лише на цвинтарі.

Апріорі всі соціальні системи динамічні, тому і безпека не може розглядатися як статична категорія, к на це помилково зазначається в українському безпековому законодавстві. Відтак як динамічну систему слід розглядати і право, і законодавство. Натомість відмінною ознакою права як динамічної системи є те, щоб його динаміка не стала рушієм до формування правової небезпеки, а була зумовлена динамікою суспільних відносин, які потрібно регулювати правом [9–12]. У зв'язку з цим ми поділяємо погляди тих дослідників, які вважають, що державна політика, як наука та мистецтво управління суспільними справами має враховувати фактори стримування надмірного динамізму права у законодавстві, завжди пам'ятаючи важливий принцип суспільного буття людей — розумне співвідношення потреб та інтересів людини, громадянина, суспільства, держави (національних інтересів) з урахуванням потреб та інтересів міжнародного співтовариства, але не в шкоду національним інтересам.

Стосовно реалізації зазначеного принципу ми підтримуємо погляди В. Б. Авер'янова, який зазначав, що в основу нової адміністративно-правової доктрини має бути покладена людиноцентристська ідеологія. За цією ідеологією держава повинна, служити інтересам громадян (тобто діяти на благо людини) у сфері діяльності публічної адміністрації[13, с. 11].. Це цілком відповідає загальній тенденції сучасного розвитку державно-правової науки та практики, що зумовлює своєрідний «людиноцентристський поворот» вітчизняного право-, державо- і націобезпекознавства.

Саме на основі ідеології людиноцентризму має розвиватися й інформаційне законодавство України. У даному контексті консолідуємося із позицією тих дослідників, які зазначають, що в законах мають визначатися не лише основні права та обов'язки людини, громадянина України, як суб'єктів інформаційних правовідносин, але й зобов'язання, повноваження і відповідальність держави в особі її компетентних органів, службових, посадових осіб щодо регулювання, гарантій, контролю, нагляду за реалізацією правомірної поведінки учасників правовідносин щодо інформації. Саме тому важливим аспектом антитерористичної політики є інформування громадськості про зміст антитерористичних операцій, їхні наслідки та практичну користь для держави. Адже проведення антитерористичних операцій в Іраку, Афганістані має чимало критичних зауважень із боку фахівців, особливо щодо практичної доцільності і важливості орт тримання наслідків.

Зважаючи на вихідні засади загальної теорії систем, ми приєднуємося до думки тих дослідників які вважають, що будь-який об'єкт слід розглядати як такий, що має відповідати вимогам до його структуризації, а саме: містить взаємопов'язані та такі, що взаємодіють, структурні елементи (певну будову), має відносну умовну незалежність порівняно з іншими соціальними об'єктами (розвинену організацію), внутрішню цілісність (що складає ядро структури) тощо [14, с. 26].

Визначаючи аспекти кодифікації національного інформаційного законодавства слід відзначити не тільки кібернетичну, але і синергетичну його природу. Синергетика, становлячи собою міждисциплінарну методологію досліджень, визначає можливості пошуку загальних принципів, що зумовлюють подальшу керованість поведінки елементів у переході їх структуризації від хаосу, випадковостей до систем, що самоорганізуються [15]. Застосування даних положень допомагає розумінню сутності правової системи України щодо інформаційної сфери суспільства, у значенні її як відкритої, нестійкої, неврівноваженою та нелінійної за структурою, що динамічно розвивається, а також визначається самоорганізацією че-

рез взаємодію з попередньо існуючих між собою чинників поза політичним впливом чи домінуванням держави.

Для прикладу, об'єктивізацію зазначених методологічних положень пропонується розглядати з поглядів Ю. Є. Максименко щодо ознак інформаційного суспільства під впливом техніко-технологічних чинників. Дана вчена вірно зазначила, що становлення інформаційного суспільства має як безсумнівні позитивні, так і певні негативні наслідки. На її думку серйозне занепокоєння викликає поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо. Перехід до інформаційного суспільства змінив статус інформації. Наразі, вона може бути як засобом підтримання безпеки, так і загрозою та небезпекою» [17, с. 1].

Екстраполюючи на предмет нашого дослідження можемо констатувати: сучасне інформаційне суспільство відкрило нові можливості для здійснення терористичної діяльності у транснаціональному вимірі. Причому для цього не обов'язково застосовувати бомби або інші прилади фізичного впливу на об'єкти критичної інфраструктури.

Відтак кодифікація інформаційного законодавства сприятиме формуванню правового поля регулювання суспільних інформаційних відносин, що стане запорукою ефективного здійснення антитерористичної політики держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ліпкан В. А. Систематизація інформаційного законодавства України : [Монографія] / В. А. Ліпкан, В. А. Залізняк / За заг. ред. В. А. Ліпкана. — К. : ФОП О. С. Ліпкан, 2012. — 304 с.
2. Ліпкан В. А. Боротьба з тероризмом / В. А. Ліпкан, Д. Й. Никифорчук, М. М. Руденко. — К. : Знання, 2002. — 254 с.
3. Погорєлов Є. В. Кодифікаційна діяльність в правовій системі України (загальнотеоретичний аспект) : дис. … канд. юрид. наук : 12.00.01 / Євген Валентинович Погорєлов. — Х., 2000. — 166 с.
4. Ліпкан В. А. Теорія національної безпеки : [підручник] / В. А. Ліпкан. — К.: КНТ, 2009. — 631 с.
5. Ліпкан В. А. Національна і міжнародна безпека у визначеннях та поняттях [словник] / В. А. Ліпкан, О. С. Ліпкан. — [Вид. 2- доп. і перероб.]. — К. : Текст, 2008. — 400 с.

6. Ліпкан В.А. Національна безпека України : [Навчальний посібник] / В. А. Ліпкан. — К. : Кондор, 2008. — 552 с.
7. Ліпкан В. А. Основи терорології (синергетична теорія тероризму) [монографія]. — К. : КНТ, 2006. — 84 с.
8. Рижов І. М. Основи аналізу теророґенності соціальних систем : [монографія] / І. М. Рижов. — К. : Магістр-XXI сторіччя. — 2008. — 288 с.
9. Лобода А. М. Щодо визначення поняття правової безпеки / А. М. Лобода // Підприємництво, господарство і право. — 2010. — № 2. — С. 10–12.
10. Лобода А. М. Правова безпека особи: антропологічний підхід / А. М. Лобода // Підприємництво, господарство і право. — 2010. — №.9. — С. 16–21.
11. Лобода А. М. Поняття та зміст правової безпеки особи / А. М. Лобода // Підприємництво, господарство і право. — 2010. — №.10 — С. 121–126.
12. Лобода А. М. Інформаціологічний зміст ідеології безпеки / А. М. Лобода, В. О. Кір'ян // Правова інформатика. — 2012. — № 33. — С . 39–44.
13. Авер'янов В. Нова доктрина українського адміністративного права: концептуальні позиції / В. Авер'янов // Право України. —2006.—№ 5.—С.11–17.
14. Ковальський В. Охоронна функція держави як система / В. Ковальський // Юридична Україна. — 2003. — № 11. — С. 26–30.
15. Чернавский Д. С. Синергетика и информация (динамическая теория информации). Изд. 2-е, испр.и доп. / Д.С.Чернавский — М.: Едиториал УРСС, 2004. — 288 с.
16. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права, історія політичних і правових учень» / Ю. Є. Максименко. — К., 2007. — 20 с.

КОНСОЛІДАЦІЯ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА ЯК НАПРЯМ БОРОТЬБИ З ТЕРОРИЗМОМ

ДІМЧОГЛО Марина Іванівна,
здобувач кафедри адміністративного та фінансового права
Національного університету біоресурсів і природокористування України

У попередніх статтях моїх колег-однодумців, представників наукової школі інформаційного права В.А.Ліпкана, було обґрунтовано думку про важливість систематизації інформаційного законодавства в контексті формування ефективної державної антитерористичної політики, окреслено напрями інкорпорації та кодифікації. Відтак у своїй статті я тезисно зупинюся власно на проблемах консолідації.

Інкорпорація, консолідація, кодифікація виступають складовими систематизації інформаційного законодавства України. Вони як теоретико-практичний правовий феномен є важливими, перманентними і безперервними процесами, що мають діалектичний взаємозв'язок у своїх проявах як етапи, методи, способи. Їхнє розуміння визначаються дослідником або суб'єктивно, або консенсуально — групою дослідників, тих, хто її здійснює поетапно, з прив'язкою до часу закінчення дослідження.

Досліджуючи інформаційне законодавство України як систему, слід постійно враховувати його постійну динаміку, мінливість, нестабільність в історичній перспективі, ураховуючи інформаційні, безпекові, соціально-економічні, політико-правові, світоглядно-культурні та інші чинники розвитку інформаційного суспільства країни.

Консолідація інформаційного законодавства — етап, процес, а також форма та система способів, методів та засобів його систематизації з метою взаємозв'язку положень окремих законодавчих актів як єдиного структурного цілого. Консолідовані законодавчі підсистема в цілому сприяють формування високого рівня правової безпеки, що сприятиме реалізації державної антитерористичної політики.

Важливим соціально-правовим аспектом при здійсненні консолідації є орієнтир на певні юридико-політичні критерії, що визначаються, як правило, у суспільстві в структурі Основного закону країни — Конституції. Це повною мірою стосується і України, де Конституція виступає Основним законом, і саме в ній сформовано системоутворюючі принципи консолідації правовідносин у законодавстві. Законодавство повинно відповідати саме нормам-принципам Конституції, розвивати їх у конкретній галузі, сфері, напрямі

суспільного життя. Це повною мірою стосується також інформаційного законодавства, його консолідації.

Здебільшого у наукових працях за проблематикою консолідації інформаційного законодавства України визначається необхідність удосконалення його систематизації. Натомість, незважаючи на значну кількість праць, присвячених окремим аспектам систематизації законодавства України про інформацію, комплексного дослідження консолідації на монографічному рівні не здійснювалось.

І лише в 2012 році вийшла в світ перша в Україні монографія з цієї теми під редакцією В.А. Ліпкана «Систематизація інформаційного законодавства України». Монографію присвячено теоретичним і правовим засадам систематизації інформаційного законодавства України. У даній роботі визначено такі поняття: «інформація», «інформаційне законодавство», «правове регулювання інформаційних відносин в Україні», «систематизація інформаційного законодавства». Проаналізовано стан вітчизняних нормативно-правових актів, що регулюють інформаційні відносини та міжнародне інформаційне законодавство. Обґрунтовано позицію, що Доктрина інформаційної безпеки України виступає системоутворювальним документом у сфері нормативно-правового регулювання інформаційних правовідносин, дороговказом систематизації інформаційного законодавства України. Характерним є те, що авторами надано конкретні пропозиції щодо структури Інформаційного кодексу України та етапів проведення систематизації вітчизняного інформаційного законодавства.

Водночас стосовно решти публікацій слід визнати, що левову частку уваги приділено питанням кодифікації та інкорпорації. Проблемні питання, пов'язані з консолідацією як складової систематизації, розглядалися фрагментарно як етап чи вид систематизації.

Здебільшого в юридичній науці виокремлюють два основні підходи щодо розуміння форм систематизації. За першим — виокремлюють чотири: інкорпорацію, консолідацію, кодифікацію, облік. За другим — три основні види систематизації: інкорпорацію, консолідацію, кодифікацію. Будучи представниками наукової школи інформаційного права В.А.Ліпкана, ми поділяємо позиції другого підходу.

Консолідацію інформаційного законодавства нами пропонується розглядати не тільки як вид чи етап його систематизації, а й як важливу методику реалізації його інкорпорації та кодифікації. Також консолідацію пропонується розглядати як багатоаспектну, багатозначну, багатофункціональну категорію, що можна сформулювати за універсальним змістом таким чином.

Консолідація інформаційного законодавства — це соціальний процес, що визначається комплексом наукових, організаційних, правових способів,

засобів, методів, методик, що в єдності утворюють доктринально сформовану методологію легального формування системи законодавства щодо інформації певними суб'єктами суспільних відносин [2–6].

Відтак, на сучасному етапі розвитку інформаційного суспільства консолідація інформаційного законодавства виступає важливим напрямом боротьби з тероризмом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ліпкан В. А. Систематизація інформаційного законодавства України : [Монографія] / В. А. Ліпкан, В. А. Залізняк / За заг. ред. В. А. Ліпкана. — К. : ФОП О. С. Ліпкан, 2012. — 304 с.
2. Дімчогло М. І. Консолідація як вид систематизації інформаційного законодавства / М. І. Дімчогло // Правова інформатика. — 2012. — 1 (33). — С. 15–24.
3. Дімчогло М. І. Онови теорії консолідації інформаційного законодавства / М. І. Дімчогло // Підприємництво, господарство і право. — 2012. — № 5. — С. 41–46.
4. Дімчогло М. І. Консолідація конституційних положень щодо інформаційних правовідносин у законодавстві / М. І. Дімчогло // Підприємництво, господарство і право. — 2012. — № 6. — С. 39–42.
5. Дімчогло М. І. Окремі принципи інформаційних правовідносин : матеріали конференції «Національна і міжнародна безпека в сучасних трансформаційних процесах». — К. : О. С. Ліпкан. — 2011. — С. 59–61.
6. Дімчогло М. І. Завдання інформатизації в контексті розвитку інформаційного суспільства в Україні: матеріали міжнародної науково-практичної конференції «Інформаційні стратегії в глобальному управлінні». — К. : О. С. Ліпкан. — 2011. — С. 36–37.

СТРУКТУРА ПРАВА НА ІНФОРМАЦІЮ

КІР'ЯН Вікторія Олександрівна
аспірантка Юридичного інституту
Національного авіаційного університету

ЧУПРИНА Олена Василівна,
аспірантка юридичного інституту
Національного авіаційного університету

У ч. 2 ст. 34 Конституції України право людини на інформацію — це можливість вільно збирати, зберігати, використовувати і поширювати інформацію будь-яким способом, на свій вибір [1].

У ст. 5 Закону України «Про інформацію» «кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поши-

рення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів»[2].

Отже, на відміну від конституційних норм (ст. 34 Конституції України) та ст. 302 «Право на інформацію» Цивільного кодексу України, де права на інформацію визначається через збирання, зберігання, використання та поширення інформації, у Законі України як у попередній редакції, так і новій замість терміна «збирання» використовується термін «одержання» інформації. До того ж згідно з новою редакцією цього Закону України з'являється новий структурний елемент права на інформацію — «захист».

Така невідповідність норм Закону України «Про інформації» конституційним нормам порушує важливий конституційний принцип згідно з яким «Конституція України має найвищу юридичну силу. Закони та інші нормативно-правові акти приймаються на основі Конституції України і повинні відповідати їй» [1] та загалом може ускладнити правореалізаційний процес.

Тим більше ці поняття абсолютно неможливо вважати синонімічними, оскільки «збирання» вказує на активний характер дій людини. Щодо поняття «одержання», то попередня редакція Закону України «Про інформацію» розкривала його зміст як «набуття, придбання, накопичення інформації громадянами, юридичними особами або державою відповідно до чинного законодавства України». Отже одержання охоплює збирання. Водночас конституційні норми є нормами прямої дії та жоден нормативно-правовий акт не може суперечити Конституції України. А тому є потреба змінити норми Конституції України чи використовувати ту термінологію, яка закріплена в Основному законі.

У ст. 9 Закону України «Про інформацію» зазначається також, що основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

Аналіз цієї норми дозволяє дійти декількох висновків. По-перше, законодавець все ж таки розрізняє поняття «збирання» та «одержання». По-друге, ця стаття значно розширює право на інформацію, що викладено в ст. 5 цього ж акту, оскільки поряд з «одержанням», «використанням», «поширенням», «зберіганням», «захистом», зазначається і про «охорону», і про «створення», і про «збирання».

Якщо в попередній редакції цього Закону чітко визначались складові права на інформацію, як «одержання», «використання», «поширення», «зберігання», то нова редакція цього Закону не містить статті, що визначає зміст цих видів інформаційної діяльності. Хоча у ст. 1 Закону України «про інформацію» закріплюється, що захист інформації — це сукупність

правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [2].

Попередня редакція Закону України «Про інформацію» чітко розрізняла та надавала легальну дефініцію таким поняттям як «одержання», «зберігання», «використання» та «поширення». Під одержанням інформації законодавець розумів набуття, придбання, накопичення інформації громадянами, юридичними особами або державою відповідно до чинного законодавства України. Зберігання означало забезпечення належного стану інформації та її матеріальних носіїв. Використання інформації визначалось як задоволення інформаційних потреб громадян, юридичних осіб і держави. Під поширенням інформації законодавець розумів розповсюдження, обнародування, реалізацію інформації у встановленому законом порядку.

Тому незрозуміло, що означає захист інформації як її структурний елемент, чим він вирізняється від іншого структурного елементу права на інформацію як зберігання. Чи яка відмінність між охороною та захистом чи зберіганням, якщо останнє — це забезпечення належного стану інформації та її матеріальних носіїв.

У наукових колах поняття «охорона» та «захист» є предметом дискусій. Здебільшого охорона пов'язується з превенцією, недопущенням протиправних дій, а необхідність же в захисті виникає лише тоді, коли є перешкоди в здійсненні прав і свобод, або загроза їх порушення [3, с. 42].

У практичній площині ці поняття дуже важко розрізнити. Так, будь-який орган на якого покладено завдання щодо припинення правопорушення, а також відновлення порушеного суб'єктивного права, зобов'язаний також здійснювати і превентивну функцію, тобто правоохоронну та правозахисну функції одночасно.

Тому вважаємо недоречними нові зміни в Законі України «Про інформацію», відповідно до яких право на інформацію — це можливість одержання, використання, поширення, зберігання і захист інформації через такі засади. По-перше, така норма суперечить конституційним нормам, де в п. 2 ст. 34 використана інша термінологія. По-друге, ця норма суперечить ратифікованим Україною міжнародно-правовим актам, зокрема Загальній декларації прав людини та громадянина, Міжнародному пакту про громадянські та політичні права тощо. І знову ж таки нормам Конституції України, згідно з якими міжнародні договори, що ратифіковані верховною Радою України є частиною законодавства України. По-третє, зберігання інформації охоплює захист і охорону, оскільки зберігання означає забезпечення

належного стану інформації та її матеріальних носіїв. І нема ніякої різниці хто буде забезпечувати цей належний стан чи власник цієї інформації, чи уповноважена на те інституція.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конституція України // Відомості Верховної Ради України. — 1996. — № 30. — Ст. 141.
2. Про інформацію : Закон України від 2 жовтня 1992 року // Відомості Верховної Ради України. — 1992. — № 48. — Ст. 650.
3. Кучук А. М. Теоретико-правові засади правоохоронної діяльності в Україні : дис. ... канд. юрид. наук : 12.00.01 / Кучук Андрій Миколайович. — К., 2007. — 180 с.

УРЕГУЛИРОВАНИЕ ПОРЯДКА ПРЕДОСТАВЛЕНИЯ ХОСТИНГ-УСЛУГ КАК ФАКТОР СТАНОВЛЕНИЯ ЭФФЕКТИВНОЙ АНТИТЕРРОРИСТИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

ТРОФИМОВ Сергей Анатольевич –
доцент кафедры административно-правовых и уголовно-правовых дисциплин Крымского юридического института Национального университета «Юридическая академия Украины имени Ярослава Мудрого»,
кандидат юридических наук,
заслуженный юрист Автономной Республики Крым

Общество в течение столетий имело устойчивую тенденцию к усовершенствованию технологий, которыми все чаще пользуются значительное количество его представителей. На протяжении последних десяти лет лидером распространения технологий стала сеть Интернет, без возможностей которой невозможно представить человечество на данном этапе эволюции.

С учетом развития телекоммуникационной сферы и быстро растущего интереса субъектов террористической деятельности к сети Интернет в качестве своеобразной платформы распространения идеологии терроризма, передачи информации своим сторонникам, а также исследование потенциального

деструктивного влияния на электронные системы различных государственных органов, учреждений, предприятий и организаций, встает вопрос о необходимости урегулирования процедуры предоставления хостинг-услуг, под которыми понимаются услуги по предоставлению вычислительных мощностей для физического размещения информации на сервере, который постоянно находится в сети. Как правило это сеть Интернет.

Нужно подчеркнуть, что на сегодняшний день порядок предоставления телекоммуникационных хостинг-услуг осуществляется в упрощенном порядке без необходимости проходить лицензирование или получать какое-либо специальное разрешение. Фактически субъект хозяйствования, который предоставляет указанные услуги, не несет никакой ответственности за содержание информации, размещенной на его ресурсах. По соответствующему договору между оператором (провайдером) хостинг-услуг и клиентом ответственность за размещенную информацию возлагается только на клиента хостинг-услуг. Оператор (провайдер) не обязан контролировать соответствующее наполнение веб-сайтов, которые размещены на его серверах, что создает возможность для их использования субъектами террористической деятельности и их сторонниками для достижения своей цели.

С учетом вышеизложенного можно прийти к выводу о необходимости введения административной ответственности субъекта хозяйствования, который предоставляет хостинг-услуги, т.е. техническую возможность для размещения на серверах, которые ему принадлежат, информации террористической направленности (например, призывы к совершению террористических актов, пропаганда идеологии терроризма, и т.п.), которая будет доступна пользователям веб-сайтов в сети Интернет. В данном случае мы предлагаем ввести солидарную ответственность субъекта, который разместил информацию террористической направленности и субъекта, который предоставил техническую возможность размещения такой информации. Первый субъект должен нести ответственность уголовного характера, а второй — административного. Также необходимо учитывать то, что в случае если субъект хозяйствования, который предоставляет хостинг-услуги, знает что пользователь хостинг-услуг будет использовать его технические возможности для размещения информации террористической направленности и, не смотря на это, дает такую возможность, то в данном случае встает вопрос о привлечении виновных лиц не к административной, а к уголовной ответственности.

Учитывая указанное выше, с нашей точки зрения, необходимо рекомендовать внести соответствующие изменения в отечественное законодательство, в частности в:

1. Закон Украины «О телекоммуникациях» от 18.11.2003г. № 1280-IV [1] относительно установления обязанности ежедневного мониторинга субъектами предпринимательской деятельности, которые предоставляют хостинг-услуги, информации, которая размещена на их серверах с целью выявления информации террористической направленности и оповещения соответствующих государственных органов об установленных ими случаях. Техническая возможность такого мониторинга существует и не нуждается в существенных расходах финансового характера.
2. Кодекс Украины об административных правонарушениях (далее — КоАП Украины) относительно закрепления ответственности должностного лица или гражданина, занимающегося предпринимательской деятельностью, которые предоставляют хостинг-услуги, за информацию террористической направленности, которая размещена на их технических мощностях, в случае невыполнения обязанности ежедневного мониторинга такой информации или недонесения к сведению государственных органов о случаях использования его возможностей с террористической целью.

В связи с этим мы предлагаем в Закон Украины «О телекоммуникациях» от 18.11.2003г. № 1280-IV [1] внести следующие изменения:

А) Статью 1 дополнить понятиями услуги по предоставлению хостинга и информации террористической направленности:

«Услуги хостинга — услуги по предоставлению вычислительных мощностей для физического размещения информации на сервере, который постоянно находится в сети».

«Информация террористической направленности — это сведения:

– о специальных средствах, технических приемах и тактике проведения антитеррористических операций;
– имеющие цель пропаганды или оправдания терроризма;
– содержащие высказывания лиц, которые оказывают сопротивление или призывают к сопротивлению субъектам антитеррористической деятельности;
– содержащие высказывания лиц, которые призывают к террористической деятельности;
– содержащие данные о предметах и веществах, которые непосредственно могут быть использованы для совершения террористических актов».

Б) Дополнить вышеуказанный закон статьей следующего содержания:

«Порядок администрирования услуг по предоставлению хостинга»

1. Субъекты, предоставляющие на платной или безвозмездной основе услуги по предоставлению хостинга, обязаны осуществлять ежедневный мониторинг информации, размещенной на серверах, которые находятся под их администрированием, с целью выявления информации террористической направленности.
2. В случае выявления информации террористической направленности субъекты, которые предоставляют на платной или безвозмездной основе услуги по предоставлению хостинга, обязаны закрыть доступ пользователей к такой информации и немедленно сообщить об этом территориальному управлению Службы безопасности Украины.
3. Лица, виновные в несоблюдении требований законодательства относительно администрирования услуг по предоставлению хостинга, несут ответственность согласно закону».

Для создания материальных норм, которые дадут возможность привлекать субъектов хозяйствования, предоставляющих хостинг-услуги, за несоблюдение вышеуказанных правил, предлагаем дополнить главу 15 КоАП Украины статьей с названием: «Нарушение установленного порядка администрирования услуг по предоставлению хостинга» в которой предусмотреть административную ответственность за следующие действия:

1. Нарушение установленных законом сроков мониторинга информации, размещенной в рамках предоставления услуг хостинга, -

влечет за собой наложение штрафа в размере от пятисот до тысячи необлагаемых минимумов доходов граждан.

2. Повторное на протяжении года совершение правонарушения, предусмотренного частью первой этой статьи, за которое лицо уже было подвергнуто административному взысканию, -

влечет за собой наложение штрафа в размере от тысячи до трех тысяч необлагаемых минимумов доходов граждан с конфискацией оборудования, которое использовалось для распространения информации террористической направленности, или без таковой.

3. Нарушение установленного законом порядка действий в случае выявления информации террористической направленности, -

влечет за собой наложение штрафа в размере от трех тысяч до пяти тысяч необлагаемых минимумов доходов граждан с конфискацией оборудования, которое использовалось для распространения информации террористической направленности, или без таковой».

Как вывод следует отметить о существенной опасности бесконтрольного использования рынка услуг в информационной сфере для уровня защищенности нашего государства от угрозы терроризма. Именно названная сфера

вызывает повышенный интерес со стороны субъектов террористической деятельности учитывая массовость использования и потенциальную сложность идентификации таких лиц. Итак, порядок администрирования услуг по предоставлению хостинга нуждается в четком регламентировании и будет фактором становления в Украине эффективной антитеррористической деятельности.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. О телекоммуникации: Закон Украины от 18.11.2003г. № 1280-IV // Відом. Верхов. Ради Украины. — 2004. — № 12. — Ст. 155.

КОНЦЕПТУАЛЬНІ ЗАСАДИ СТРАТЕГІЇ РОЗВИТКУ СИСТЕМИ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ ДО 2015 РОКУ

КУШНІР Ольга Василівна,
радник президента
Глобальної Організації Союзницького Лідерства

Однією з серйозних проблем, що стоять нині перед Україною та світовою спільнотою, є торгівля людьми. Жертвами цього злочину стають жінки, чоловіки і діти, які потерпають від різноманітних його форм, серед яких — торгівля людьми з метою примусової праці, сексуальної експлуатації, примусового жебрацтва, вилучення органів.

Проблема торгівлі людьми — багатогранна, тому потребує комплексного підходу до її вирішення, узгоджених дій законодавців, політиків і державних службовців, взаємодії з міжнародними організаціями, координованої співпраці неурядових організацій, спільних заходів правоохоронних органів та громадськості. Взаємодія у вирішенні цієї проблеми повинна будуватись на визначених засадах, які б стали підґрунтям для подальшого визначення механізмів, конкретних процедур і гарантій протидії торгівлі людьми.

Нині Україна є країною походження, транзиту та поступово стає країною призначення для чоловіків жінок та дітей, які є жертвами примусової праці та примусової проституції.

Підписання і ратифікація Україною Протоколу «Про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї», що доповнює Конвенцію Організації Об'єднаних Націй проти транснаціональної

організованої злочинності, Конвенції Ради Європи про заходи щодо протидії торгівлі людьми, а також приєднання до інших міжнародних зобов'язань у цій сфері, засвідчили визнання Україною необхідності вжиття заходів щодо подолання явища торгівля людьми через провадження державної політики у цій сфері на якісно новому рівні.

Оскільки тенденції у сфері торгівлі людьми постійно змінюються, їх вивчення та відповідного міжнародного досвіду мають стати невід'ємною частиною Стратегії розвитку системи протидії торгівлі людьми.

Метою цієї Стратегії є визначення заходів законодавчого, організаційного та інстутиційного характеру, спрямованих на забезпечення стабільного та ефективного функціонування національної системи протидії торгівлі людьми в Україні.

Досягненню даної мети слугуватиме вирішення наступних завдань:

забезпечити утвердження Україною статусу країни, що ефективно протидіє торгівлі людьми через:

- забезпечення реалізації положень Закону України «Про протидію торгівлі людьми»;
- здійснення заходів, спрямованих на виявлення та припинення протиправної діяльності організованих злочинних груп, що діють у сфері торгівлі людьми;
- поглиблення партнерських відносин із медичними закладами державної та недержавної форм власності у сфері протидії незаконній трансплантації органів та інших анатомічних матеріалів людини;
- удосконалення та розширення єдиного інформаційного простору електронної взаємодії державних органів — учасників національної системи протидії торгівлі людьми;
- запровадження уніфікованого підходу, що полягає у проведенні оцінки ризиків усіма суб'єктами національної системи протидії торгівлі людьми в Україні;

удосконалення діяльності правоохоронних та інших державних та недержавних суб'єктів протидії торгівлі людьми через:

- підвищення ефективності розслідування правоохоронними органами кримінальних справ за статтями 149 та 143 Кримінального кодексу України, а також проведення оперативно-розшукових заходів, зокрема в частині виявлення та припинення діяльності організованих груп або злочинних організацій, що діють у цій сфері;
- удосконалення механізму взаємодії правоохоронних органів та недержавних суб'єктів системи протидії торгівлі людьми, зокрема під час розслідування кримінальних справ;

– розроблення та впровадження ефективних механізмів розшуку коштів та іншого майна, одержаних від торгівлі людьми та незаконної трансплантації органів та інших анатомічних матеріалів людини, з метою їх подальшого арешту та конфіскації в установленому порядку;
– забезпечення подання недержавними суб'єктами протидії торгівлі людьми до Міністерства внутрішніх справ України, виявленої під час виконання своїх функцій інформації про діяльність, стосовно якої існує підозра, що вони пов'язані з торгівлею людьми або незаконною трансплантацією органів та інших анатомічних матеріалів людини;

удосконалення механізму взаємодії суб'єктів протидії торгівлі людьми через:

– проведення аналізу ефективності заходів взаємодії суб'єктів протидії торгівлі людьми в державі;
– впровадження нових форм взаємодії суб'єктів протидії торгівлі людьми;
– організації проведення навчання представників спеціально визначених суб'єктів;
– підготовки методичних рекомендацій для недержавних суб'єктів протидії торгівлі людьми з метою ідентифікації учасників торгівлі людьми;

підвищення кваліфікації спеціалістів суб'єктів протидії торгівлі людьми шляхом:

– забезпечення перепідготовки та підвищення кваліфікації спеціалістів державних суб'єктів протидії торгівлі людьми, зокрема осіб, які беруть участь у виявленні, розкритті та розслідуванні фактів торгівлі людьми;
– запровадження механізму навчання за новітніми навчальними програми для працівників суб'єктів протидії торгівлі людьми з питань застосування вимог Закону України «Про протидію торгівлі людьми»;
– підвищення кваліфікації працівників новоутворених суб'єктів протидії торгівлі людьми;

організація ефективного міжнародного співробітництва через: — продовження роботи з підготовки та укладення міжнародних договорів (меморандумів) про співробітництво з питань протидії торгівлі людьми;

– забезпечення ефективної взаємодії та інформаційного обміну з компетентними органами іноземних держав і міжнародними організаціями, діяльність яких спрямована на протидію торгівлі людьми;

забезпечення інформування громадськості про вжиті заходи щодо протидії торгівлі людьми шляхом:

– розроблення ефективного механізму доступу фізичних та юридичних осіб, а також засобів масової інформації до публічної інформації про результати діяльності державних суб'єктів протидії торгівлі людьми;
– забезпечення прозорості діяльності державних суб'єктів протидії торгівлі людьми.

Очікувані результати.

Реалізація цієї Стратегії дасть змогу забезпечити:

– системну реалізацію державної політики у сфері протидії торгівлі людьми;
– гармонізацію національної системи протидії торгівлі людьми з міжнародними правовими стандартами;
– дієву взаємодію та постійний інформаційний обмін між державними та недержавними суб'єктами протидії торгівлі людьми, а також компетентними органами іноземних держав і міжнародними організаціями в зазначеній сфері;
– дотримання та неухильне виконання вимог положень законодавства щодо діяльності суб'єктів протидії торгівлі людьми;
– підвищення кваліфікації спеціалістів державних суб'єктів із окремих питань протидії торгівлі людьми на національному рівні;
– стимулювання притоку іноземних інвестицій у сферу протидії торгівлі людьми.

Ухвалення Стратегії слугуватиме сильним конструктивним і стабільним елементом на шляху формування системи протидії торгівлі людьми, відкриє новий шлях до державотворення нашої соборної держави, і в цілому до правовладдя як найвищої мети функціонування соціокультурних систем.

НАПРАВЛЕНИЯ РАЗВИТИЯ НОРМАТИВНОЙ БАЗЫ ДЛЯ ОСУЩЕСТВЛЕНИЯ ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В РОССИИ

ВОРОНЦОВА Софья Викторовна
доцент кафедры уголовно-правовых дисциплин,
кандидат юридических наук, доцент

КУЗЬМИНА Анастасия Юрьевна
Московский институт
государственного управления и права

Дальнейшее формирование инновационной системы России сталкивается с отсутствием развитой нормативной правовой базы для осуществления инновационной деятельности, а также мер ее государственной поддержки, включая бюджетное финансирование, налоговые преференции и государственные гарантии. Должны быть созданы условия и инструменты для финансовой поддержки инновационного сектора экономики. Невозможно осуществить модернизацию отраслей промышленности только за счет средств государства.

Назрела необходимость создания новых институтов частного финансирования и расширения возможностей уже существующих. В связи с этим следует внести изменения в Федеральный закон «О банках и банковской деятельности» в части отмены ограничений банков на фондовом рынке по инвестированию в активы инновационных компаний и создания эффективной системы льготного кредитования перспективных инновационных производств. При этом у банковских организаций должна быть возможность выступать в качестве институциональных инвесторов при реализации перспективных инвестиционных проектов в сфере высоких технологий.

Для этого необходимо предоставить государственные гарантии по кредитам малому наукоемкому бизнесу и предусмотреть возможность предоставления им беззалоговых кредитов. Представляется актуальным предложение о создании специальных банков по обслуживанию малых предприятий с разделением их по видам хозяйственной деятельности, в том числе выделение инновационной составляющей.

Необходимо более эффективно использовать учетные инструменты регулирования денежного предположения. В первую очередь, это относится

к ставке рефинансирования, поскольку именно она является ориентиром для коммерческих банков при установлении размера платы за выдаваемые кредиты. Происходящее увеличение ставки рефинансирования автоматически приводит к удорожанию кредитных ресурсов для реального сектора экономики, что делает практически невозможным использование заемных средств для развития производства, технологической модернизации и внедрения инноваций.

Низкий уровень инновационной активности российских предприятий вызван тем, что инновацинная деятельность в Российской Федерации относится к высокорисковой. При этом эффективность управления рисками, особенно инновационными, у российских предпринимателей остается очень низкой. Основным же источником покрытия риска выступает, как правило, собственный капитал организации. Следовательно, одним из источников покрытия вероятных потерь является страхование.

С точки зрения иностранных экономистов, в настоящее время механизмы инновационного страхования в России находится на начальном этапе развития. Столь низкий уровень объясняется, в первую очередь, нормативной правовой базой, а также консервативностью российской страховой системы и неготовностью осуществлять оценку рисков инновационных проектов.[1]

Переход к инновационной экономике невозможно осуществить без эффективного развития человеческого потенциала и инновационного кадрового резерва страны. Сегодня повышение инвестиций в развитие человеческого капитала уже не является только государственной проблемой. Бизнес ощущает нехватку профессинальных кадров, замедлен процесс обновления кадров. Все эти негативные тенденции заставляют предпринимателей участвовать активнее в социальной политике, совместно с образовательными учреждениями разрабатывать современные инновационные программы подготовки и переподготовки специалистов, повышать личностный и творческий потенциал сотрудников за счет организации тренинговых программ и выявления талантливых молодых специалистов. С внедрением новых технологий в производство у работодателей все больше находит поддержку концепция непрерывного образования работников в течение жизни. Все чаще поднимается вопрос о разработке проекта федерального закона «О непрерывном профессиональном образовании и повышении квалификации».

Говоря о поддержке и развитии образования, необходимо отметить такое приоритетное направление социально-экономической политики

[1] См.Курс МВА по менеджменту под редакцией Аллен Р. Коэн,М.Альпина.Бизнес — курс. 2011.С 404

как развитие исследовательских вузов и сети федеральных университетов, которые должны стать важной частью нацинальной инновационной системы,основными центрами инновацинных разработок. Для достижения указанных целей необходимо постепенное увеличение бюджетных расходов до 5,5–6% ВВП в ближайшие годы.

Инновационный опыт отечественных учебных заведений наметил стратегическое направление в решении столь сложных задач, а именно обновление программно-технологического обеспечения образовательного процесса на основе переосмысления всего арсенала применяемых технологий с опорой на современные возможности и широкий культурный контекст, а также внедрение новых информационных и социальных технологий.

Образовательные технологии это необходимый инструментарий современного школьного или вузовского преподавателя. В них заложен огромный потенциал для повышения профессионального мастерства и достижения целей, которые общество ставит перед системой образования — подготовить молодое поколение к самостоятельной жизни и профессиональной деятельности как граждан, обладающих высокой степенью личностной зрелости, ориентированных на гуманистические ценности в решении любых проблем, способных к критической оценке и презентации своих достижений.[2]

Известно, что сфера образования как разновидность социальной практики ощущает влияние культуры, науки, экономики, и техники в ходе их развития. Особенно заметно влияние интегральных политико-экономических, социально-культурных и научно-технических факторов, которые проявляют себя в виде тенденций. Проявляется глобализация в глобальной информатизации общества, либерализации мировой экономики, взаисозависимости экономики и безопасности всех стран.

Глобализация представляет собой процесс преодоления отчуждения как экономики любой страны от мировой экономики, так и в жизни человеческого рода целом, поэтому характеризуется процессами становления и гармонизации многомерного мира во всех формах проявления. Втягивание экономики любой страны в мировое хозяйство представляет собой важный, но не единственный элемент этого процесса. Не менее важно осознание каждым человеком планеты чувства сопричастности жизни и деятельности всех людей и народов на Земле.

Становление открытого общества связано с процессами массовой социальной и межкультурной коммуникации, открытости новому знанию и новым технологиям, новым взглядам и культурам, новым условиям жизни

[2] См. Современные образовательные технологии под редакцией Н.В.Бодровского М.КНОРУС.2010.С .5

и деятельности, новым способам общения и средствам реализации творческого потенциала. Такая открытость на планетарном уровне приводит к деалогическим формам отношений западной и восточной цивилизации, возможности свободного развития и свободного выбора любой формы самореализации в рамках конкретной культуры (религиозной, этнической и пр.), что требует активного применения в образовательной практике и освоения диалогических и коммуникативных технологий.

Стратегическим направлением совершенствования законодательства на ближайшие годы определено тенденциями обеспечение развития в стране производства продукции, конкурентоспособной на мировом рынке, при значительном улучшении жизни населения и уменьшении вредного воздействия на окружающую среду путем модернизации производства и достижения допустимых для России норм экологической безопасности. ООН также определяет в числе мировой «наилучшей практики» устойчивого развития достижение одновременно экономических, экологических и социальных результатов. Для этого требуется комплексное совершенствование законодательства в области охраны окружающей среды, в том числе с целью обеспечения требований соблюдения производственных возможностей среднего и крупного бизнеса.[3]

Системный подход предусматривает определение принципов и целей формирования инновационной системы, основных требований к инновационной системе, включая определение конкретной модели инновационного развития Российской Федерации, а также разработку необходимых мер и способов ее реализации. Инновационная система представляет собой совокупность институтов, обеспечивающих генерацию, распространение и практическое использование знаний. Инновационная система обеспечивает реализацию государственной политики инновационного развития.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Курс МВА по менеджменту под редакцией Аллен Р. Коэн,М.Альпина.Бизнес курс.2011.
2. Современные образовательные технологии под редакцией Н.В.Бодровского М.КНОРУС.2010.
3. Ивасенно Н.Г Инновационный менеджмент М.КНОРУС.2011.

[3] См.Ивасенно Н.Г Инновационный менеджмент М.КНОРУС.2011.С.169

ПРАВО НА ИНФОРМАЦИАННУЮ БЕЗОПАСНОСТЬ КАК ИНСТИТУТ ПРАВА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

ОКАЗАНИЕ СОДЕЙСТВИЯ ИНЫМИ УЧАСТНИКАМИ (СУБЪЕКТАМИ) УГОЛОВНОГО СУДОПРОИЗВОДСТВА РОССИИ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОМУ ТЕРРОРИЗМУ

ЛАТЫПОВ Вадим Сагитьянович –
преподаватель кафедры уголовного процесса
Уфимского юридического института МВД России

Человек живущий в современном мире во всех сферах общественных отношений непрерывно сталкивается с информационными технологиями и от уровня развития и защищенности данных технологий зависит качество его жизни.

Так, Сочнев Д. В. и Хайтаров И. Н. в одной из своих работ выделяли новые информационные технологии (НИТ), а так же произвели ее классификацию на программно-математические инструментальные средства информатизации, предназначенные для проектирования современных НИТ, и прикладные информационные технологии, обеспечивающие принятие и поддержку решений. К числу инструментальных НИТ они отнесли гипертекстовые технологии, машинную графику, телекоммуникационные методы доступа, CASE-технологии, системы искусственного интеллекта, мультимедиа, возникновение которых связано главным образом с новыми техническими возможностями средств вычислительной техники. При создании прикладных информационных систем имеет смысл опираться только на эти более совершенные технологии, которые позволят выйти на современный уровень компьютеризации в экономике и во многом повлиять на развитие общества [1].

Мы больше не представляем своей жизни без использования компьютеризированной техники (компьютеров, телефонов, iPod, iPad и т.п.), подо-

бная тенденция заставила «эволюционировать» и криминальное общество и породило так называемую компьютерную преступность к которой относят манипуляцию сознанием людей через Интернет, подталкивающее на совершение преступлений различных категорий тяжести, «сетевые войны», информационный терроризм, всевозможные способы мошенничества с использованием Интернет ресурсов и т.д.

Согласно Концепции противодействия терроризму в Российской Федерации подписанной в 2009 году Президентом Российской Федерации Медведевым Д. А. — основными внешними факторами, способствующими возникновению и распространению терроризма в Российской Федерации, являются:

е) распространение идей терроризма и экстремизма через информационно-телекоммуникационную сеть Интернет и средства массовой информации;

Основными задачами противодействия терроризму являются:

– противодействие распространению идеологии терроризма и активизация работы по информационно-пропагандистскому обеспечению антитеррористических мероприятий.

Предупреждение (профилактика) терроризма предполагает решение такой основополагающей задачи как:

– противодействие распространению идеологии терроризма путем обеспечения защиты единого информационного пространства Российской Федерации; совершенствование системы информационного противодействия терроризму [2];

Раскрытие и расследование подобного рода преступлений (когда средства компьютерной техники используются при подготовке, совершении, сокрытии рассматриваемого преступного деяния) не мыслимо без использования специальных познаний в этой области и проведении соответствующих судебных экспертиз в рамках действующего уголовно-процессуального законодательства РФ.

Судебная компьютерно-техническая экспертиза (далее по тексту СКТЭ) в данном случае является основной формой использования специальных знаний. Как справедливо отмечают Егорышева Е. А. и Егорышев А. С. экспертные исследования придают изъятым аппаратным средствам, программному обеспечению и компьютерной информации доказательственное значение. В таких условиях основными задачами следователя являются поиск, фиксация, изъятие и предоставление эксперту необходимых материальных объектов — носителей информации. Причем при собирании доказательств участие специалиста обязательно, так как даже малейшие неквалифицированные дей-

ствия с компьютерной техникой могут закончиться безвозвратной утратой ценной розыскной и доказательственной информации [3].

В науке выделяют классификацию СКТЭ организованую на основе обеспечивающих компонент любого компьютерного средства (аппаратного, или технического, программного и информационного обеспечения). Соответственно этому в СКТЭ выделяются:

1) аппаратно-компьютерная экспертиза;
2) программно-компьютерная экспертиза;
3) информационно-компьютерная экспертиза (данных);
4) компьютерно-сетевая экспертиза.

Данная классификация может быть эффективно использована при назначении комплексных экспертиз и решении большого перечня задач [4].

Учитывая международный характер совершаемых компьютерных преступлений мы разделяем мнение Усова А. И. о необходимости развития сотрудничества в области судебной экспертизы, прежде всего, с партнерами из числа государств — участников Содружества Независимых Государств (СНГ), и в первую очередь с СЭУ министерств юстиции Союзного государства (России и Беларуси) и Евразийского экономического сообщества (далее — ЕврАзЭС, Сообщество) с учетом геополитического положения Российской Федерации и практических потребностей правосудия [5].

Так, 23 сентября 2011 г. во время очередного 18-го заседания Совета министров юстиции ЕврАзЭс было утверждено Положение о Координационно-методической комиссии по судебной экспертизе при Совете министров юстиции государств — членов Евразийского экономического сообщества [6].

Координационно-методическая комиссия по судебной экспертизе при Совете министров юстиции государств — членов Евразийского экономического сообщества (далее — Комиссия) является консультативным органом Совета министров юстиции по судебно-экспертной деятельности государственных судебно-экспертных учреждений государств — членов Евразийского экономического сообщества. Комиссия ответственна перед Советом министров юстиции государств — членов Евразийского экономического сообщества (далее — Совет) и подотчетна ему: Комиссия ежегодно представляет Совету отчет о своей работе [7].

Подводя итог вышесказанному, следует отметить, что научно-технический прогресс заметно облегчил жизнь человеку, создал комфортные условия для существования, увеличил в разы скорость обмена информации между людьми, что безусловно влечет угрозу использования подобной возможности в корыстных, криминальных целях. В настоящее время сложилась отлаженная практика по раскрытию и расследованию подобного рода пре-

ступлений, а государство заняло твердую позицию защиты национальной безопасности в том числе и в сфере информационного терроризма, приняв при этом соответствующие нормативно-правовые акты. Однако не стоит забывать, что для наиболее полного о объективного расследования преступлений совершенных с использованием вычислительных машин нам требуются специальные познания, которыми обладают специалисты и эксперты.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Сочнев Д. В., Хайтаров И. Н. Новые информационные технологии и их роль в развитии современного общества // Российская юстиция. 2011. № 11. С. 44 — 46.
2. «Концепция противодействия терроризму в Российской Федерации» (утв. Президентом РФ 05.10.2009)
3. Егорышева Е. А., Егорышев А. С. Некоторые вопросы использования специальных знаний при расследовании неправомерного доступа к компьютерной информации // Эксперт-криминалист. 2011. N 3. С. 14 — 16.
4. Россинская Е. Р., Галяшина Е. И. Настольная книга судьи: судебная экспертиза. Москва: Проспект, 2011. 464 с.
5. Усов А. И. Сотрудничество судебно-экспертных учреждений Министерств юстиции как одно из практических звеньев международной интеграции государств — членов ЕврАзЭС // Эксперт-криминалист. 2011. N 4. С. 27 — 31.
6. Положение о Координационно-методической комиссии по судебной экспертизе при Совете министров юстиции государств — членов Евразийского экономического сообщества. Утверждено решением Совета министров юстиции государств — членов Евразийского экономического сообщества 23 сентября 2011 г. N 36 // www.evrazes.com/ docs/ view/ 555.
7. Хазиев Ш. Н. Евразийское экономическое сообщество и вопросы судебной экспертизы // Адвокат. 2011. N 12. С. 17 — 22.

О НЕКОТОРЫХ АСПЕКТАХ ИНФОРМАЦИОННОГО ТЕРРОРИЗМА И МЕТОДАХ БОРЬБЫ С НИМ

СМИРНОВА Лада Ярославовна –
старший преподаватель кафедры философских и экономических дисциплин Московского областного филиала Московского университета МВД России,
кандидат экономических наук

В 21 веке остро стоит проблема «разгула» терроризма. Данное явление приобрело множество форм, а именно основывается на физическом и духовном воздействии. Пытки, избиение, лишение жизни — это все можно отнести к физическому воздействию. Психологическое же намного сложнее — это применение информационно-психологических методов, включая личное общение и информационные средства. Естественно понятно, что обе формы терроризма направлены на достижение единой цели: физическое и моральное сокрушение своих жертв.

В федеральном законе «О борьбе с терроризмом» указывается, в порядке развития ст. 205 УК РФ, что терроризм представляет собой насилие или угрозу его применения в отношении физических лиц или организаций, а также уничтожение (повреждение) или угрозу уничтожения (повреждения) имущества и других материальных объектов, создающую опасность гибели людей, причинения значительного ущерба, либо наступления иных общественно-опасных последствий, осуществляемых в целях нарушения общественной опасности, устрашения населения или оказания воздействия на принятие органами власти решений, выгодных террористам.[1]

Большое значение в данной проблематике играет информация. В настоящее время информацию можно назвать оружием, не зря говорят о том, что кто владеет информацией, тот владеет миром. Информационный терроризм осуществляется в области, охватывающей политические, философские, правовые, эстетические, религиозные и другие взгляды и идеи, то есть в духовной сфере, там, где ведется борьба идей.

Информационный терроризм — это, прежде всего, форма негативного воздействия на личность, общество и государство всеми видами информации. Его цель — ослабление и расшатывание конституционного строя. Он ве-

[1] ФЗ от 6 марта 2006 г. N 35-ФЗ «О противодействии терроризму» (с изменениями от 27 июля 2006 г., 8 ноября, 22, 30 декабря 2008 г., 27 июля, 28 декабря 2010 г., 3 мая, 8 ноября 2011 г.)

дется разнообразными силами и средствами — от агентуры иностранных спецслужб до отечественных и зарубежных СМИ.

В мирное время прямыми исполнителями акций информационного терроризма в России являются:

– иностранные спецслужбы и организации;
– зарубежные и определенная часть российских СМИ;
– организации сектантов и церковников;
– различного рода миссионерские организации;
– отдельные экстремистские элементы и группы.[2]

Немалую лепту в проведение акций информационного терроризма против России вносят такие организации проамериканской ориентации, как «Фонд Шамиля» (Турция), «Германо-Кавказское общество», «Исламский верховный совет Америки», «Братья мусульмане» (Саудовская Аравия), «Хамас», «Комитет Польша-Чечня» и др. Указанным организациям власти соответствующих стран предоставляют благоприятные условия для подрывных выступлений по радио, телевидению, в печати.

Государство, в лице исполнительной власти — правоохранительных органов, не должно проходить мимо таких явлений. В первую очередь они должны оградить отдельных граждан и общество в целом от разлагающего действия подобного рода организаций, свести к минимуму их отрицательное влияние, изучить возможности для разоблачения и уголовного преследования их лидеров и участников. В отдельных случаях, когда деятельность таких организаций содержит состав преступлений, предусмотренных Уголовным Кодексом Российской Федерации (организация объединений, посягающих на личность и права граждан, укрывательство преступлений, самоуправство и др.), они подлежат уголовному преследованию.

Если взять деятельность современных СМИ как зарубежных, так и отечественных, то она в значительной степени несет на себе прямые признаки информационного терроризма, является опасным орудием духовного перерождения личности за счет негативного воздействия на нее посредством СМИ. Особенно усердствуют в оболванивании и морально-психологическом растлении граждан России некоторые телевизионные компании, прежде всего, недавно прекратившая свое вещание ТВ-6.

Не посягая на свободу слова, для уменьшения отрицательного воздействия отдельных СМИ на должностных лиц государственных учреждений, правоохранительных органов и население, правоохранительные органы должны принимать меры по ослаблению действий подобного рода, а для локализации наиболее одиозных сотрудников СМИ, использовать другие

[2] Информационный терроризм /http://www.rau.su/observer/N5–6_02/5–6_10.htm.

рычаги воздействия на них, например, привлечение к уголовной ответственности за допущенные ими нарушения российского законодательства.

Информационный терроризм проявляется и в области сектантства.

Нашу страну буквально наводнили сектанты-фанатики — «Свидетели Йеговы», «Церкви преподобного Муна» (секта запрещена даже в США), «Церкви Христа», «Церкви Объединения», «Церкви сайентологии», «Пирамида». Можно с уверенностью утверждать, что не без влияния последних и соответствующего лоббирования, был отвергнут, Государственной думой прежнего состава, закон «О свободе совести». Сектанты с удивительной легкостью проникают и в российские учебные заведения, школы, сиротские учреждения, детские сады, площадки под флагом медицинских, общеобразовательных, культурных, благотворительных и коммерческих организаций.

Правоохранительные органы, используя различные методы для предупреждения подрывной деятельности сектантских организаций должны:

- вести наблюдение за ними;
- устанавливать и поддерживать контакт с радикально настроенными членами сект, с целью привлечения их на свою сторону;
- оказывать через прогрессивно настроенных лиц, сдерживающие влияние на наиболее экстремистски настроенных сектантов;
- инициировать меры местной администрации по локализации (запрету) наиболее опасных сект.

Что касается экстремистских элементов и групп, то их деятельности присущи бескомпромиссность, агрессивность, претензии на абсолютную правоту, установки на незаконное применение силы для достижения своих целей. Правоохранительные органы в области борьбы с экстремистскими организациями должны постоянно отслеживать их деятельность, вести работу по их разложению. Самое важное здесь — не допустить превращения экстремистских лозунгов в прямые акции терроризма.

В настоящее время, особенно в чрезвычайных ситуациях и вооруженных конфликтах особую актуальность приобретает борьба правоохранительных органов с акциями информационного терроризма. Можно выделить то, что сейчас прослеживается деморализующая пропаганда через Интернет. По данным Интерпола, Интернет стал тем сектором, где преступность растет самыми быстрыми темпами, а вместе с тем и информационный терроризм. Речь идет о такого рода преступлениях, как незаконный доступ и перехват данных и т. п. Убытки от киберпреступлений составляют миллиарды долларов. Необходимо наводить порядок в Сети. Возможно, уже скоро контроль над Интернетом возьмет на себя новый правоохранительный орган — меж-

дународная киберполиция. Как бороться с киберпреступностью? Во-первых, модернизировать национальные законодательства. Во-вторых, создать базовые правила, способные облегчить проведение расследований в виртуальном мире и одновременно представляющие собой новые формы юридической взаимопомощи. Например, быстрое сохранение (дублирование) данных. Европейская конвенция по борьбе с киберпреступностью предлагает каждой из стран защитить, прежде всего, финансовую информацию, базы данных и log-файлы (специальные файлы на серверах, содержащие служебную информацию). Ну и, наконец, главное — международное сотрудничество. Ведутся попытки создания общеевропейской киберполиции, состоящей из киберполиций разных стран, способных не только быстро обмениваться информацией, но и запрашивать коллег на предмет ареста или выдачи преступника. Такие киберполиции уже существуют во многих европейских странах, в том числе и в России.

Острота и значение борьбы с таким явлением как информационный терроризм XX — начала XXI в. сейчас не только не снизились, но и значительно возросли. Правоохранительные органы должны максимально способствовать ослаблению влияния на общество и его граждан акций информационного терроризма, ставить на его пути надежный заслон.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Уголовный кодекс Российской Федерации от 13.06.1996 года №63-ФЗ (ред. от 04.05.2011) с изм. и доп., вступившими в силу с 01.07. 2011)
2. ФЗ от 6.03. 2006 года N 35-ФЗ «О противодействии терроризму» (с изменениями от 8.11.2011)
3. Европейская Конвенция по борьбе с киберпреступностью / http://pravo.ru/interpravo/legislative/view/27.
4. Информационный терроризм / http://www.rau.su/observer/N5–6_02/5–6_10.htm.
5. Седьмая Международная конференция «Электронные СМИ и терроризм», Кипр, 24 — 28 октября 2011 года. / http://www.panarin.com/comment/16232.

ОКРЕМІ АСПЕКТИ СПІВВІДНОШЕННЯ ІНФОРМАЦІЙНОГО ТА КОМП'ЮТЕРНОГО ТЕРОРИЗМУ

ПРАВДЮК Сергій Андрійович
здобувач кафедри адміністративного та фінансового права
Національного університету біоресурсів
і природокористування України

Поряд з безсумнівними перевагами інформаційної стадії розвитку суспільства серйозного занепокоєння викликають негативні наслідки впровадження інформаційно-телекомунікаційних технологій, а саме динаміка вчинення правопорушень інформаційного характеру.

Порушення авторських прав, розголошення державної таємниці чи іншої конфіденційної інформації без дозволу, несанкціонований доступ до персональних даних, інформаційний тероризм тощо — це лише деякі правопорушення інформаційного характеру (інформаційні правопорушення).

Нині у кримінальному, цивільному, адміністративному законодавстві містяться норми, що передбачають відповідальність за порушення тих чи інших інформаційних прав і свобод.

Незважаючи на прийняті зміни та доповнення у вітчизняному законодавстві недостатньо адекватно відображено тенденції розвитку інформаційних правопорушень. У зв'язку з чим збільшується кількість нерозкритих таких правопорушень чи неможливість притягнення осіб до відповідальності за їх вчинення. Більше того можна стверджувати, що недосконалість правової бази, низький рівень правової культури детермінують їх вчинення.

Юридична наука покликана розробити рекомендації щодо подолання цієї проблеми чи хоча б мінімізації їх шкідливих наслідків. Натомість нині відсутні комплексні дослідження у цій сфері які б надали стійке уявлення про сутність, зміст, специфіку, різноманіття інформаційних правопорушень, а також шляхів їх подолання. Кожна з галузевих наук розглядає лише окремий спектр цієї багатогранної проблематики. Деякі засади інформаційних правопорушень здебільшого розглядались крізь призму проблеми забезпечення інформаційної безпеки. Це, насамперед, пов'язано з тим, що саме інформаційна безпека визначається як стан захищеності від зовнішніх та внутрішніх загроз в інформаційній сфері. Тобто по суті відсутність порушень в інформаційній сфері і становить собою сутність інформаційної безпеки.

У Законі України «Про основи національної безпеки України» закріплено, що на сучасному етапі основними реальними та потенційними загроза-

ми національній безпеці України, стабільності в суспільстві в інформаційній сфері 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 [1]. Тобто законодавець визначив лише деякі види правопорушень інформаційного характеру. Особливе місце серед перерахованих вище загроз в інформаційній сфері має інформаційний тероризм.

Незважаючи на закріпленість іншої термінології, вважаємо адекватнішим саме поняття «інформаційний тероризм».

Хоча позицію законодавця підтримують і деякі науковці. Наприклад, І. Л. Бачило зауважує, що «слабка вивченість комп'ютерних правопорушень та інших правопорушень є причиною низького відсотку виявлення інформаційних і комп'ютерних правопорушень…»[2, с. 417]. Оскільки дане правопорушення, як правило, скоюється не лише через використання комп'ютерної техніки, інших ЕРМ і інших комп'ютерних технологій. Спектр засобів, знарядь цього правопорушення значно ширший.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про основи національної безпеки України : Закон України // Офіційний Вісник України. — 2003. — № 29. — Ст. 1433
2. Бачило И.Л. Информационное право : [учебник] / И. Л. Бачило. — М. : Издательство Юрайт; ИД Юрайт, 2010. — 454 с., С. 417

СУЩНОСТЬ МАНИПУЛИРОВАНИЯ СОЗНАНИЕМ И ДЕМОРАЛИЗУЮЩАЯ ПРОПАГАНАДА

КІБЕРСУГЕСТІЯ ЯК ОСНОВНИЙ МЕТОД ІНФОРМАЦІЙНОГО ВПЛИВУ НА ПОЛІТИЧНУ КУЛЬТУРУ

РУДНЄВА Анна Олегівна
асистент кафедри політології
Запорізького національного університету

XXI сторіччя стало епохальним за всю історію розвитку людства. Змінилася традиційна система життя суспільства, а з нею і класичні засоби досягнення поставлених цілей, що особливо відобразилось на політичній сфері, яка виступає паровим двигуном для всіх інших сфер. Аналізуючи «традиційні» війни минулих століть, можемо стверджувати, що головними об'єктами, стосовно яких вони розв'язувались, були переважно природні ресурси: територіальні, родовища корисних копалин та ін. На противагу їм війни нової епохи спрямовані на більш витончений та більш ціннісний ресурс — людську свідомість. Здатність впливати на свідомість окремої людини, певного суспільства та людства загалом, змінюючи його у бік власних інтересів, визначати характер думок цілих націй, стати творцем ментального простору — це приваблива стратегічна мета будь-якої інформаційної кампанії чи війни.

В XXI сторіччі в епоху інформаційної революції головну роль в політиці відіграють культурно-інформаційні технології, які набули значення вирішальної ноосферної зброї. Сучасні інформаційні впливи здатні змінити головний геополітичний потенціал держави — національний менталітет, культуру та моральний стан людей. Всі ці процеси надають капіталу культури, особливо політичної культури, не абстрактно-теоретичне, а стратегічне значення. Тому для політичної влади дуже важливо усвідомити необхідність посилення та вдосконалення стратегічного капіталу політичної культури.

Інформаційні війни по відношенню до політичної культури здійснюють свій вплив через основні елементи її структури. Цей процес набуває форми **кіберсугестії** — вплив на свідомість людини, заснований на некритичному сприйнятті інформації об'єктом впливу, з використанням прийомів, методів і

тактик інформаційних технологій. Для детального розгляду інформаційного впливу на політичну культуру звернемось до Схеми 1 (Структурно-функціональна модель політичної культури). Інформаційний вплив на політичну культуру здійснюються по основних ключових точках:

1. «Вхідні» елементи структури — політична свідомість, традиції та символи, менталітет, моделі та норми політичної поведінки, соціальні цінності.
2. «Ядро» — когнітивний, аксіологічний, афективний, діяльний, інституціональний рівні.
3. «Вихідні» елементи — політична свідомість, ідентифікація та само ідентифікація, культура політичної поведінки та політичної діяльності.

На основі вищезазначеного можна стверджувати, що першочерговою антропологічною проблемою XXI сторіччя є вплив інформаційного простору на формування свідомості сучасної людини.

Ключова точка — свідомість, когнітивний та аксіологічний рівні «ядра» політичної культури. Інформаційний вплив на політичну свідомість опирається на її два взаємопов'язані блоки елементів — мотиваційний та пізнавальний. Мотиваційний блок представлений політичними потребами та інтересами, політичними цілями та цінностями, переконаннями. Цей елемент відповідальний за політичну поведінку людей, тому вплив на нього дає можливість задавати вектори спрямування цієї поведінки, знову ж таки у вигідному для суб'єкту впливу ключі, одночасно викликаючи відповідні цьому емоції та почуття. Пізнавальний блок включає політичну інформованість, політичні знання, теорії, уявлення, політичну ідеологію. Через систему освіти та через засоби масової інформації відбувається «фільтрація» політичної інформації, задається характер та об'єм інформованості, формуються «необхідні» уявлення стосовно світу політичного.

Наступна ключова точка впливу — традиції та символи, менталітет та аксіологічний рівень «ядра». Необхідно зазначити, що політична культура є найбільш консервативним елементом політичної системи. На цій основі можна стверджувати, що стабілізація політичного процесу певної країни багато в чому залежать від перетворень в політико-культурній сфері. Національні традиції, звичаї, ритуали та символи є могутнім інструментом підтримки національної самосвідомості. Політичні символи — це певна знакова система, дієвий механізм політичної влади. Цей механізм пов'язаний із свідомим та несвідомим у людській психіці, та є каталізатором певної політичної поведінки та політичної діяльності. Політична символіка відображає особливості світосприйняття певного соціуму, його соціально-психологічний досвід, характерні риси його само ідентифікації. Створення певної символічної системи із

заданими параметрами для досягнення певної мети дає можливість надавати політичному життю, поведінці, діям явний, або ж, навпаки, прихований зміст.

Ключова точка — моделі та норми політичної поведінки, соціальні цінності. Людина, позбавлена соціальних цінностей, стає спустошеною, втрачає вектори розвитку та сенс буття. Моделі та норми політичної поведінки є певними кліше у політичному просторі. Змінюючи їх вихідні параметри, а також особливості соціальних норм та цінностей, ініціатор інформаційного впливу викликає корінні зміни у формуванні політичної культури. Формування «необхідних» характеристик на «вході» призводить до зміни особливостей кінцевого продукту — політичної культури. Таким чином, інформаційний агресор може спричинити порушення ґенези та ланцюга формування політичної культури, впливаючи, в свою чергу, на деградацію наступних поколінь.

Ми досить багато знаємо про перекручування історії за радянських часів, але не звертаємо майже ніякої уваги на сьогоднішні «трансформації» історії. Все частіше «продукти» кінематографії відображають перекручені історичні факти, події, які підчас навіть не підлягають логіці здорового глузду. Перекроюються не тільки історичні факти, події, а й соціальні цінності — руйнується навіть найстаріша у світі система моралі, формується атмосфера підозри, повсякчасної зради та ін. Крім того наноситься відчутний удар навіть по найпростіших закономірностях та речах, яскравим прикладом є дитячі мультфільми, де фантазія виступає впливовим інструментом зміни дитячої психіки та свідомості. В результаті ми не можемо не тільки відрізнити епоху Античності від Середньовіччя, а Першу світові війну від Другої, а й можемо бути поставлені у глухий кут, чи насправді відбувалися певні події чи це тільки інформаційний міф. І найбільша небезпека цих процесів не стільки в руйнуванні минулого та впливі на сьогодення, а скільки у тому, що воно перетворюється на бомбу із часовим механізмом для майбутнього, при чому наслідки спрацювання цієї бомби передбачити, нажаль, ми не можемо.

Однією із важливих ключових точок інформаційного впливу є «ідентичність» — як результат саморефлексії особистості, ототожнення та усвідомлення своєї приналежності до різноманітних соціальних, політичних, культурних та інших груп та спільнот. «Криза ідентичності» може призвести до втрати людиною сенсу життя, життєвої рівноваги та здібності вести конструктивний спосіб життя.

Ключова точка — культура політичної поведінки та політичної діяльності, практично-поведінковий рівень «ядра». Людина стає маріонеткою політичних маніпуляцій та технологій, втрачаючи виборений філософами-гуманістами статус «творця».

Ключова точка — емоційно-психологічний рівень «ядра». Дуже часто виникає питання, чому сьогоднішні засоби масової інформації переповненні різного роду кримінальною інформацією, кінематограф представлений у переважній більшості фільмами жахів, чим не обділені навіть «товари», розраховані на дитячу аудиторію, телепередачі висвітлюють жорстокість та найгірші якості людини, реклама будь-якого товару перетворюється на ролик з елементами еротики та ін. І це не є випадковістю. Це досить складна та добре розрахована технологія. Даного типу інформація є своєрідною «їжею», якою намагаються наповнити розум людей. Звернемось до піраміди потреб А.Маслоу: кожен вищий рівень передбачає разом із задоволенням потреб нижчого рівня також розвиток людської особистості. Чим вище рівень цієї піраміди, відповідно більш складною та багатосторонньо розвиненою є людина, яка, по-перше, здатна критично сприймати та оцінювати пропоновану їй інформацію, по-друге, може робити власний аналіз та аналітично мислити, по-третє, готова приймати участь у політичному, соціальному, економічному та духовному житті суспільства. Не тільки таку людину зокрема, а суспільство в цілому, яке представлене таким типом людей, підкоряти своїй волі та нав'язувати власні інтереси досить складно. Значно легше управляти масою, основна енергія якої спрямована на задоволення фізіологічних, максимум екзистенціальних (в безпеці існування) потреб. Така людина практично не здатна піддавати критиці впроваджувану політику, аналітично сприймати пропоновану інформацію та робити власні висновки стосовно процесів, які відбуваються в конкретній державі. Це ідеальний об'єкт для кіберсугестії.

ЗМІ є надзвичайно ефективним засобом впливу, оскільки активізує емоційно-чуттєву сферу, в свою чергу, це призводить до зниження критичності сприйняття інформації і людина стає більш схильною до засвоєння інформації будь-якого характеру та до навіювання. Основний акцент також робиться на особливому психічному механізмі особистості — властивості до наслідування.

Сенсаційні новини, «гостро актуальні» події можна назвати «інформаційними кульовими блискавками», бо виникають вони настільки ж моментально, наскільки й затихають, викликаючи у суспільстві сильні резонанси, невиправні зміни по відношенню до людської свідомості.

Інформаційні війни по відношенню до політичної культури здійснюють свій вплив не тільки через її структуру, а й через її основні та найважливіші функції: по-перше, прогностична функція, що виявляється у впливі на динаміку політичного життя. Контроль над цією функцією надає суб'єкту впливу можливість задавати шляхи розвитку держави та суспільства у вигідному для нього спрямування, з метою реалізації власних цілей. По-друге, нормативно-

регулююча функція, основне завдання якої — забезпечення ефективного і стабільного функціонування політичної системи, що передбачає також включення людини в задану систему політичної поведінки та політичної участі. Втручання в суспільство через цю функцію дозволяє втілювати власні зразки та шаблони поведінки людей в політичному просторі, регулювати характер та ступінь їх участі у політичних процесах. По-третє, виховна функція. Її призначення полягає в підвищенні політичної свідомості й національної самосвідомості через безпосередню участь громадян в управлінні, політичному житті, зростанні їх інформованості й компетентності, освіченості. В цьому ключі інформаційні впливи можуть бути спрямовані на продукування власних «особливих» фільтрів, які будуть пропускати тільки вигідну суб'єкту впливу інформацію, а життєво необхідну для людини інформацію перетворювати на «шум» та лишати її актуальної значимості. Такий дисонанс між нав'язаною «фільтрованою» інформацією та власною системою цінностей особистості негативно впливає на психіку, на нервову систему й загалом на настроєво-емоційну сферу. По-четверте, комунікативна функція, яка представляє собою передачу зразків політичної поведінки від одного покоління до іншого через політичні традиції та ритуали, забезпечуючи тим самим спадкоємність в суспільному розвитку.

Треба зробити особливий акцент також на вікових особливостях кібер-сугестії. Найбільш уразливою в цьому сенсі є молодь. По-перше, сучасна молодь зростає на інноваціях та інформаційних технологіях, та вихована на інформаційно-електронній культурі, в цьому сенсі не треба навіть докладати додаткових зусиль для впливу, по-друге, саме молодь є базисом для формування і зародження концепту політичної культури, тому вплив на свідомість цієї вікової категорії дає можливість впроваджувати власні цілі та систему цінностей «без крові», крім того, покоління із зміненою свідомістю буде генерувати своїх наступників із заздалегідь заданими ініціатором інформаційного впливу параметрами. Показовим фактом тут є залучення молоді у різноманітні розважальні ток-шоу («Майданс», «Співай, якщо можеш», «Фермер шукає жінку», «Весільні битви», «Шоу №1» та ін.), які, на перший погляд, несуть в собі конструктивний момент — піклування про молодь, але по суті в них відсутня будь-яка виховна мета, що ще більше підкріплює споживацькі настрої та характер суспільства. Різноманітні гумористичні передачі (на зразок «Наша Раша», «Файна Юкрайна», «Рюрики» та ін.) «висвітлюють» всі негативні сторони держави, національного характеру, менталітету, відносин у суспільстві, розтинають і без того тендітне поняття патріотизму, яке стало сьогодні більш саркастичним висловом, ніж гідною похвалою. З іншого боку, менш за всіх піддаються маніпулюванню люди з чітко вираженою соціаль-

ною та політичною позиціями, бо, як правило, вони відрізняються досить високим рівнем освіченості, соціокультурної ідентичності, групової солідарності та ін.

Таким чином, політична культура, як привабливий стратегічний об'єкт інформаційного впливу, виступає детермінантою у визначенні характеру політичної дії суб'єктів політичного простору, вона формує певну ціннісну програму функціонування політичних процесів та інститутів, та в свою чергу залежить від існуючих традицій, цінностей, переконань, ідеалів, духовної основи політичної спільноти та ін. Враховуючі дані факти, діючому керівництву держави необхідно залучити всі необхідні ресурси з метою розробки на цій основі діючої ефективної інформаційної політики, спрямованої на захист власної країни та громадян від інформаційних впливів інших держав.

Схема 1:

ОПАСНЫЙ КОНТЕНТ ИНТЕРНЕТА КАК УГРОЗА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ УКРАИНСКИХ ПОДРОСТКОВ

ШАХОВА Наталия Владимировна –
доцент кафедры социально-экономических дисциплин
Крымского юридического института Национального университета
«Юридическая академия Украины имени Ярослава Мудрого»,
кандидат физико-математических наук, доцент

В настоящее время информационно-психологическая безопасность понимается как состояние защищенности личности, социальной группы, общества от воздействий, способных против их воли и желания изменять психологические характеристики человека, модифицировать поведение, влиять на личное и общественное сознание. Эти воздействия осуществляются в форме организованных информационных потоков и специальных технологий, которые распространяются с помощью средств телекоммуникаций, главным из которых сегодня становится Интернет.

Выражение «опасный контент»[1] является относительно новым — под ним понимают информацию, представляющую угрозу или вызывающую неприязнь. В Интернет основными видами опасного контента являются: порнография, пропаганда наркотиков, суицида, насилия.

В Украине была принята Доктрина информационной безопасности [1], в которой, в частности, говорится о реальных и потенциальных угрозах информационной безопасности нашего государства. Во внешнеполитической сфере — внешние деструктивные информационные влияния на общественное сознание через средства массовой информации, а также сеть Интернет; во внутриполитической сфере — распространение техники манипулирования общественным сознанием, деструктивные информационные влияния, в том числе с применением специальных средств, на индивидуальное, групповое и общественное сознание.

Особенно уязвимой частью украинской интернет — аудитории являются психологически и социально незрелые личности, в первую очередь дети и подростки. Сегодня говорят об Интернет как о пятой власти, причем для подростковой аудитории, в отличие от взрослой, эта власть может стать

[1] Контент — «содержимое», любая информация, содержащаяся на сайте: текстовая, видео, графическая.

абсолютной. Сначала молодежь просто собирается на флэш — мобы[2], им весело, они чувствуют свою принадлежность к какой-то социальной группе. А завтра, незаметно для себя, они станут игрушками в руках опытных кукловодов. Ведь одна из главных задач пропаганды — убедить всех, что ее не существует.

Бесконтрольное использование интернет — ресурсов подростком может изменить его в самые короткие сроки до неузнаваемости. Попав в мир порно сайтов, виртуальных казино и компьютерных игр, не каждый вернется оттуда самостоятельно в мир реальности. Подросток, чрезмерно увлекающийся серфингом в сети, еще быстрее теряет навыки адекватного поведения в реальности, чем взрослый.

Для того, чтобы оценить масштаб проблемы, приведем ряд статистических данных, касающихся украинской интернет — аудитории.

По данным компании InMind на март 2012г. [2] , 16,9 млн. жителей Украины старше 15 лет регулярно пользуются Интернетом (что составляет 42% взрослого населения страны). В исследовании Gemius-Украина, опубликованном в начале 2012г. [3], приводятся следующие цифры: распределение пользователей по способу доступа в Интернет — выходят с домашнего компьютера 89%, на работе — 39%. Из городов с населением больше 500 тыс. человек пользователей Интернет — 50% от общего количества, из сел — 10%.

Можно сделать оценку количества украинских детей и подростков, которые пользуются Интернетом: если учесть, что 89% пользователей выходят в Интернет из дома — очевидно, что в отсутствие взрослых Интернетом пользуются дети. В городах активными интернет — пользователями являются не менее 80% от общего количества данной социальной группы. По опросам автора за последние 3 года, 100% первокурсников нашего ВУЗа были зарегистрированы в социальных сетях и имели дома доступ в Интернет.

Самые популярные интернет — ресурсы для украинцев — поисковые сервера, социальные сети и сайты, откуда можно скачать или на которых можно посмотреть фильмы. Верхние позиции рейтинга популярности занимают google.com (72%), mail.ru (62%), vk.com (61%).

Примечательно, что в первую двадцатку сайтов не вошел ни один специализированный новостной проект и всего 7 украинских проектов (первые 9 мест занимают сайты иностранного происхождения — России и

[2] Флэш-моб — заранее спланированная массовая акция, в которой большая группа людей появляется в общественном месте, выполняет заранее оговоренные действия (сценарий), и затем расходится.

США). Очевидно то, что украинские пользователи чаще посещают сеть с целью получения информации и развлечения, общения в социальных сетях.

На начало 2012 г. число активных пользователей сети «Одноклассники» в Украине составляло около 6 млн. в месяц, зарегистрированных — около 8 млн. В социальной сети ВКонтакте 16 млн. зарегистрированных украинских профилей, в сети Facebook — более 2 млн. украинских пользователей. При этом нет статистических данных о том, сколько украинских детей и подростков входят в это количество. Так, по правилам первых двух сетей завести свой аккаунт можно с 6 —летнего возраста, на Facebook — с 13 лет, но никто не контролирует это ограничение и не проверяет возраст пользователя.

В настоящее время социальные сети, создаваемые группы в этих сетях — одно из самых мощных средств воздействия как на взрослую аудиторию, так и на подрастающее поколение. С их помощью можно деформировать хрупкую психику подростков, манипулировать сознанием, влиять на их мнение и побуждать к каким-то реальным действиям.

По данным исследования «Майкрософт Украина», 92% украинцев недостаточно осведомлены о киберугрозах. Подавляющее число родителей не задумывается над тем, какие ресурсы посещают их дети, чем они занимаются, с кем общаются. Многие ли из украинских родителей, выходя вечером в Интернет со своего домашнего компьютера, проверяют список тех ресурсов, которые посетил сегодня их ребенок? Обычно подростки, являясь «поколением большого пальца»[3], лучше родителей разбираются в современных технологиях, а 67% из них, по заявлению компании Microsoft, подчищают историю навигации по Интернет в своих браузерах.

Автором был проведен поиск по наиболее актуальным в настоящее время интернет — угрозам информационно — психологической безопасности личности с помощью поискового сервера google.com.ua. Результаты представлены в виде таблицы.

Ключевые слова для поиска	Количество результатов
Порно видео	729 000 000
Сайты с порнографией	130 000 000
Порно со школьницами	6 810 000
Смотреть видео ужасы триллеры	78 800 000

[3] У современных подростков выработана привычка управления мобильными устройствами посредством больших пальцев рук. В результате тренировок мышцы этих пальцев обретают необычную силу; специалисты обнаружили, что у подростков происходят изменения в той части головного мозга, которая отвечает за моторику больших пальцев рук

Ключевые слова для поиска	Количество результатов
Видео с драками	26 400 000
Видео драки в школе	2 040 000
Видео издевательства над животными	520 000
Видео жестокие приколы	693 000
Курительные смеси	1 380 000
Дизайнерские наркотики	154 000
Суицид	6 180 000
Суицид без боли	3 000 000

Даже учитывая то, что некоторые ссылки повторяются, а также то, что обычно результаты поиска выводятся в порядке убывания релевантности (в конце списка могут быть ссылки, уже не соответствующие смыслу запроса), количество доступных ресурсов производит впечатление. Кроме того, хорошо организованный поисковый сервис дает подсказки пользователю: вместе с понятием «суицид» ищут «суицид без боли» — и т.д. Все найденные ресурсы находятся на открытом доступе; крайне редко они сопровождаются лицемерным предупреждением о том, что их можно смотреть, если вам больше 18 лет. При этом пользователь может без всякой проверки утвердительно ответить на этот вопрос.

Практически во всем мире, в том числе и в Украине, предусмотрена уголовная ответственность [4] за распространение детской порнографии. Но по запросу «Порно со школьницами» — около 7 млн. ссылок. Возможно, актрисы в этих видео — совершеннолетние, но одеты как школьницы и юному пользователю, в сущности, все равно — это его ровесницы или 20-летние, главное, что он получает крайне искаженное представление о взаимоотношениях полов, которое потом не исправить ни на каких уроках этики.

Следующие 5 запросов — поиск ресурсов, на которых представлены фильмы ужасов, триллеры, видеоролики с жестокими драками, издевательствами над животными. При этом особенно тревожит огромное количество такой видеопродукции, снятой подростками: они не вмешиваются, чтобы прекратить драку, а старательно снимают ее. При этом слышны их комментарии, зачастую нецензурные. В видео с жестокими приколами и издевательствами над животными слышен неудержимый смех операторов съемки.

2 запроса сделаны с целью поиска информации о наркотиках. Дилеры и пропагандисты наркотиков в Интернет используют те синтезированные химические вещества, которые не успели внести в перечень прекурсоров [5]; желающим подробно объясняют, действию какого «нелегального» наркотика соответствует предлагаемая «легальная» курительная смесь.

Курительным смесям посвящено почти 1,5 млн. ссылок: здесь сайты, посвященные «изменению сознания» и сайты, на которых можно купить эти смеси (от 150 до 500 грн. за 1 г, этого количества хватает на 10 раз). Чего стоят открытые форумы на этих сайтах с описанием — сколько, чего и как курить, какие после этого испытываются ощущения.

Особая тема — суициды. Как известно, направленным информационным влиянием человека можно довести до самоубийства. Например, в России в последние годы резко возросло количество самоубийств среди подростков: по уровню смертности от самоубийств среди подростков 15–19 лет Россия занимает первое место в Европе и одно из первых мест в мире. На 100 тысяч подростков приходится 19,8 случаев суицида. В среднем в стране ежегодно убивают себя более 200 детей и 1,5 тысяч подростков, а количество подростков, убивших себя, ежегодно возрастает в два раза. Специалисты считают, что немалую роль в этом играют группы в социальных сетях, которые посвящены пропаганде суицидов, легкодоступной информации о суицидах (более 6 млн. ссылок).

У автора имеются ссылки на 17 групп в сети Вконтакте, посвященных суициду, которые функционировали достаточно продолжительное время. В апреле 2012 г. была проведена проверка их наличия — и оказалось, что 1 из групп заблокирована, 10 удалены, а 6 продолжают функционировать. Названия этих групп: «Самоубийство: за и против», «Задумывающиеся о самоубийстве»; есть группа, посвященная «спортивному повешению», пропаганде суицида среди несовершеннолетних ради развлечения, и т.д. Все эти группы пропагандируют суицид различными способами, представлены изображения и видеоролики соответствующего содержания.

В феврале 2012 г., после очередной волны подростковых суицидов, в прессе [6] было сообщение о том, что такие группы ВКонтакте закрываются, пользователям сети достаточно пожаловаться администрации сайта на подозрительный контент. Поскольку автор не является пользователем сети, сообщить о подозрительном содержимом не удалось, а зайти на ресурс можно беспрепятственно, если известен адрес группы.

В Украине делаются определенные шаги в направлении обеспечения информационно — психологической безопасности детей и подростков — так, во исполнение поручения Президента Украины В.Ф.Януковича [7] 8.02.2012г. Национальным советом по вопросам телевидения и радиовещания создана рабочая группа по разработке национальной системы защиты детей от вредной информации на телевидении. Уполномоченный по правам ребенка Ю. Павленко подчеркнул, что работа по защите ребенка от вредного контента теперь параллельно ведется на телевидении, радио и в Интернете.

Существует также ряд ресурсов, посвященных безопасности детей в Интернете — например, onlandia.org.ua.

Для ограждения украинских подростков от опасного контента Интернет необходимо принимать следующие безотлагательные меры:

- ✓ Использовать специализированное программное обеспечение с функцией «Родительский контроль», с помощью которой можно перекрыть доступ к определенным ресурсам.
- ✓ Нужна широкомасштабная пропаганда среди родителей о необходимости контроля за тем, чем занимается в Интернет его ребенок.
- ✓ Можно обратиться к опыту таких стран, как Турция и Китай, где действует ряд государственных интернет — фильтров, блокирующих сайты с запрещенным контентом.
- ✓ Необходимо более строгое регулирование правовых отношений в данной области — прежде всего, определение интернет — ресурсов как средств массовой информации. Существуют противники данного подхода, говорят о цензуре, называют множество проблем, связанных с глобальной природой Интернет. Но безнаказанно подавать не всегда проверенные, а иногда порочащие честь и достоинство факты — это еще не свобода слова. Кроме того, многие новостные порталы имеют принудительный сервис — перед тем, как откроется анонсируемая статья, появляется дополнительная страница «эти удивительные картинки» с такими изображениями, что смотреть на них — это уже нагрузка на психику.

Отметим, что запретительных мер недостаточно — необходимо на государственном и региональных уровнях финансировать работу интернет — порталов, которые будут предназначены для детей и подростков, наполнены интересным для данной возрастной категории контентом.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Про Доктрину інформаційної безпеки України: Указ Президента України // Офіційний вісник України. — 2009. — № 52. — Ст. 1783.
2. http://ain.ua/tag/inmind
3. http://ain.ua/tag/gemius
4. Про внесення змін до деяких законодавчих актів України щодо протидії розповсюдженню дитячої порнографії : Закон України // Відомості Верховної Ради України. — 2010. — № 10. — Ст. 105.
5. Про наркотичні засоби, психотропні речовини і прекурсори: Закон України // Відомості Верховної Ради України . — 1995. — № 10. — Ст. 60.
6. http://www.kp.ru/online/news/1084669
7. http://www.president.gov.ua/ru/news/22454.html

СУЩНОСТЬ ИНФОРМАЦИОННЫХ ОПЕРАЦИЙ В КОНТЕКСТЕ БОРЬБЫ С ТЕРРОРИЗМОМ

ЗАСАДИ СТВОРЕННЯ ТА ЗАСТОСУВАННЯ СИЛ СПЕЦІАЛЬНИХ ОПЕРАЦІЙ

ГАЛУШКО Сергій Олександрович,
здобувач кафедри воєнної історії
Національного університету оборони України

Спробуємо проаналізувати підходи до сил спеціальних операцій (ССпО) за поглядами іноземних військових фахівців.

Існують варіанти визначення «сил спеціального призначення» та «сил спеціальних операцій». Наприклад, сили спеціального призначення — військові частини та підрозділи, що застосовуються у ході спеціальних операцій та призначені для ведення спеціальної розвідки, проведення протидиверсійних, диверсійно-розвідувальних дій та організації руху опору в тилу противника.

В той же час Сили спеціальних операцій — визначені сили і засоби військових частин спеціального призначення, аеромобільних військ, морської піхоти, армійської та транспортної авіації, інших частин і підрозділів родів військ і спеціальних військ тощо, які залучаються до проведення спеціальних операцій.

Є й інші визначення. Наприклад, у спеціальній доповіді, підготовленій для конгресу США, визначено: «*Сили спеціальних операцій є елітними військовими частинами, які можуть проникнути «за лінію фронту» сушею, морем або повітрям для проведення різноманітних операцій, багато з яких є таємними*».

Відповідно, існують **різні погляди** на створення ССпО — екстенсивний і інтенсивний. Прикладом першого є ССО ЗС США, де їх чисельність постійно зростає і вже досягає 60 тис. осіб. Приклад інтенсивного шляху — Велика Британія, де чисельність ССО хоча і дещо зросла за останній час, але кількість особового складу в бойових підрозділах принципово не змінюється (22 полк «SAS» — до 300 чол.).

Існують **різні моделі** створення ССпО:

координаційна — коли адміністративна і оперативна функції належать видам ЗС, а на рівні ГШ/МО існує орган координації їх діяльності;

оперативного підпорядкування — коли адміністративна функція належить видам ЗС, а оперативна — спеціально створеному органу управління ССпО;

безпосереднього підпорядкування — коли адміністративна і оперативна функції належать спеціально створеному органу управління ССпО.

Характерною ознакою усіх моделей є наявність сил і засобів, спеціально призначених для ведення спеціальних операцій. Чисельність достатньо різна, залежно від визначеного переліку завдань.

При створенні ССпО в ЗС країн світу спостерігається дотримання таких концептуальних положень:

- підготовка сил спеціальних операцій для реагування на потенційні загрози, особливо асиметричні (тероризм, рух опору тощо), не може бути надлишковою і повинна здійснюватися завчасно у повному обсязі;
- створення ССпО розглядається не як реформування системи спеціальної розвідки, а як створення нового функціонального і організаційного компоненту збройних сил зі своєю системою управління і забезпечення;
- усі заходи щодо створення ССпО, їх функції, завдання і порядок застосування мають чітко визначену нормативу базу;
- чисельність ССО має вирішальний вплив на рівень підготовки особового складу та якість їх забезпечення.

В загальному вигляді створення і розвиток ССпО ЗС країн світу здійснюється за такими напрямками:

- визначення завдань ССпО та їх нормативне закріплення;
- створення (доопрацювання) нормативної бази діяльності і застосування ССпО;
- створення органу управління і підпорядкування йому визначених сил і засобів;
- уточнення бойового і чисельного складу, удосконалення організаційно-штатної структури та організація управління силами спеціальних операцій;
- створення системи відбору, комплектування та підготовки усіх категорій особового складу;
- створення системи логістики, переозброєння і переоснащення військових частин і підрозділів сучасними зразками;

- підвищення привабливості служби у ССпО шляхом здійснення заходів соціальної сфери.

Що стосується ефективності ССпО, то відомі розрахунки, згідно яких закупівля одного нового танка приблизно дорівнює утриманню протягом року батальйону (загону) спеціального призначення (озСпП). Очевидно, що для збройних сил потрібне і перше, і друге. Але давайте згадаємо недавні події в Лівії або слова НГШ РФ про те, що за їхніми поглядами до 90% цілей противника тепер будуть уражуватися в глибині. І змоделюємо ситуацію сучасного воєнного конфлікту та спробуємо уявити: хто має більше шансів дійти до лінії безпосереднього зіткнення з противником та виконати бойове завдання? Новий сучасний танк чи підрозділи (яких є кілька) з складу зазначеного батальйону (загону) СпП? І яка може бути бойова ефективність кожного? Беремо на себе сміливість стверджувати, що в таких умовах є більш витребуваним озСпП.

Слід звернути увагу, що в більшості країн світу ССпО з'явилися як відповідь на ті чи інші виклики та загрози національній безпеці. Тобто це не було примхою або амбіціями тих чи інших керівників. Виникали ті чи інші проблеми і виникало питання пошуку шляхів реагування на них.

В повній мірі зазначене має відношення до нашої держави. ССпО — це спроба компенсувати наше відставання в сучасних далекобійних засобах високоточного ураження в необхідній кількості.

Інший чинник — це поява низки завдань мирного часу, вирішення яких найбільш доцільне методами спеціальних дій, а в деяких випадках — навіть єдино можливе. Більш того, СпО органічно вписуються в асиметричні, адаптивні дії та інші сучасні форми і способи протиборства.

З аналізу досвіду ЗС США та інших країн світу стає очевидним, що **деякі потенційно можливі завдання для ССпО для сучасних умов України є неможливими або недоцільними, перш за все з огляду на певні нормативно-правові обмеження.** Але думати про них потрібно сьогодні і відповідним чином готуватися. Адже у випадку життєво важливої необхідності органи влади зможуть швидко врегулювати те чи інше питання в нормативному плані та виділити необхідні ресурси. Але в такому ж оперативному режимі отримати необхідні сили та засоби, підготувати і провести СпО поки що не вдавалося нікому. Тому успіх майбутніх СпО повинен формуватися сьогоднішніми діями. І завдання збройних сил при цьому — завчасно підготувати і у випадку необхідності надати керівництву держави дієвий і ефективний інструмент для реагування на загрози.

Світова історія свідчить, що ті чи інші держави, перш за все США стикалися з ситуацією, коли приходилося діяти, керуючись не нормами права, а

принципом доцільності забезпечення реалізації національних інтересів. Звичайно, таку «привілею» можуть собі дозволити сильні провідні країни світу. Але сподіваємось, що ми самі себе не записуємо до переліку країн «третього світу».

Існує також думка щодо можливого включення частин і підрозділів аеромобільних військ до складу ССпО. Але давайте уважно подивимося на досвід країн світу:

ФРН: основу дивізії СпО, крім елітної частини «KSK», складають дві повітрянодесантні бригади;

Республіка Білорусь: основу КССпО складають — одна обрСпП та дві опдбр.

В 2001 році під час операції в Афганістані основу наземного компоненту угруповання ЗС США складали частини і підрозділи ССО, а в значній мірі підтримували і забезпечували їх дії — підрозділи і частини 10 легкої піхотної дивізії СВ.

Чому так? На практиці реалізується принцип сполучення «ядра і оболонки». Ядром є частини СпП, оболонкою — інші сили і засоби, в т.ч. аеромобільні частини, які забезпечують ефективні дії «спецназу». Час підтвердив доцільність реалізації зазначеного варіанту у зарубіжних країнах.

Дослідження показали, що стосовно умов нашої держави така інтеграція дуже ефективна у випадку проведення протидиверсійної операції, участі в антитерористичних заходах і, частково, у випадку проведення розвідувально-диверсійної операції.

Є низка питань **щодо ролі і місця авіаційної компоненти у складі ССпО.**

В ЗС країн світу існує кілька підходів з зазначеного питання:

- варіант штатної авіаційної компоненти;
- варіант оперативного підпорядкування для виконання конкретних завдань визначеного складу завчасно підготовлених сил і засобів;
- варіант виділення ресурсу із складу звичайних авіаційних частин і підрозділів.

Очевидно, що останній варіант можуть собі дозволити країни з надзвичайно високим рівнем підготовки всього льотного складу та високим рівнем оснащеності сучасними зразками ОВТ, які є універсальними та можуть без додаткової підготовки забезпечувати дії ССпО.

Є прихильники другого, так званого компромісного варіанту. Його сутність полягає у визначенні в складі авіаційних частин видів ЗС необхідних підрозділів, які оснащуються відповідними зразками спеціально обладнаних літальних апаратів та цілеспрямовано готуються до дій в інтересах ССпО. При такому варіанті для підвищення ефективності авіаційної компоненти ССпО

командувачу ССпО надаються необхідні повноваження щодо участі в організації та контролю її розвитку, підготовки авіаційних підрозділів, а також можливості оперативного та у більшості випадків прихованого залучення авіаційних підрозділів для виконання завдань в інтересах ССпО.

І, звичайно, найбільш ефективним з позицій нарощування бойового потенціалу ССпО є перший варіант. Хоча слід визначити, що він в економічному відношенні є дуже спірним. Тому цей варіант може бути прийнято або не прийнято в залежності від того рівня амбіцій, який ми собі можемо дозволити сьогодні, або ж його доцільно розглядати на більш віддалену перспективу.

Що стосується безпілотних авіаційних комплексів, а також літальних апаратів так званої малої авіації (наприклад, мотодельтапланів), то їх слід мати безпосередньо у складі частин і підрозділів ССпО.

Таким чином, ми повинні вже зараз дивитися на перспективу і чітко розуміти, які можуть бути подальші заходи в державі з зазначеного напрямку. З високою долею вірогідності ми можемо говорити, що для умов України буде доцільно:

- суттєве розширення переліку та кількості СпО, які проводяться державою в умовах мирного часу;
- підготовка та проведення СпО на стратегічному рівні;
- подальша інтеграція відомчих сил для проведення СпО в міжвідомчу функціональну структуру, які будуть виконувати завдання під керівництвом єдиного органу управління (в нашій державі зазначене вже частково реалізовано в форматі антитерористичної діяльності);

Досвід розвитку воєнного мистецтва показує, що за умов постійно зростаючого рівня «асиметричних» загроз, особливу роль для їхньої ліквідації або упередження відіграватимуть спеціальні методи ведення війни (спеціальні операції, психологічні операції тощо). При цьому прослідкується стала тенденція збільшення ролі сил спеціальних операцій у збройній боротьбі. Значної шкоди національній безпеці держави може завдати недооцінка важливості сучасних спеціальних методів боротьби.

Опоненти можуть зазначити, що наведене вище є чимось фантастичним та неможливим для умов України. Саме в цьому полягає одна з унікальних та ефективних властивостей ССпО. Коли в результаті їх дій відбувається саме те, в що ніхто не вірить та не очікує в принципі. Тобто мають місце низки подій, коли здійснюється виведення з ладу критично важливих об'єктів, зміни урядів або настроїв та масової свідомості у суспільстві. Але, створення і розвиток ССпО неможливі без принципових, радикальних і рішучих рішень і дій. Без наявності необхідних ресурсів, в першу чергу фінансових, за проблему створення ССпО можна не братися.

ВПЛИВ ТЕРОРИЗМУ НА ПРОЦЕСИ СОЦІАЛЬНОЇ ТРАНСФОРМАЦІЇ

РИЖОВ Ігор Миколайович,
докторант НА СБ України,
кандидат юридичних наук, доцент

Тероризм як базовий фактор соціоморфозу, можна порівняти зі своєрідним кесаревим розтином у процесі народжування нових цивілізацій. Його небезпека насамперед у тому, що на фоні людських трагедій, сучасний тероризм є своєрідною технологією втручання в соціальні процеси, коли шляхом провокації масової теророфобії, шляхом формування недовіри, ненависті і відвертої ворожнечі між соціальними групами певні кола намагаються змінити або скорегувати алгоритм соціального управління, підмінити природний хід розвитку соціальних процесів і систем. Вплив тероризму на процеси соціальних трансформацій величезний. Достатньо пригадати, що всі світові війни та наступний перерозподіл світових цивілізаційних кордонів було спровоковано саме терористичними актами. Безпосереднім приводом до початку Першої світової війни стало вбивство австрійського ерцгерцога Франца Фердинанда. В результаті війни припинили своє існування чотири імперії, країни-учасниці втратили близько 10 млн. чоловік, 22 млн. було поранено. Початок сучасної фази зіткнення цивілізацій теж характеризується сплеском терористичної діяльності — від замахів на лідерів та терористичних актів до масштабних військових кампаній з наступною окупацією. Восени 2001 року США було розпочато операцію «Тривала свобода», яка мала на меті повалення в Афганістані режиму «Талібан» та знищення підтримуваної ним терористичної організації «Аль-Каїда». Ця військова операція була відповіддю на масштабні атаки проти США 11 вересня 2001 року, що були здійснені міжнародним терористичним угрупованням Аль-Каїда на чолі з Усамою Бін Ладеном. Цими подіями розпочалося глобальне протистояння, в якому тероризм представлено як ґрунтовний принцип протиборства сторін глобального соціального конфлікту. Процес тільки розпочато, про його наслідки судити рано, можемо тільки оцінити його протікання. Історія свідчить про те, що будь-яке штучне втручання в її хід не лише не має позитивних результатів, а викликає іноді трагічні наслідки, виправляти які мають цілі покоління. Саме тому, боротьба з тероризмом має глобальне завдання — оберігати цілісність цивілізаційних процесів, і це завдання набагато складніше, ніж всі задекларовані на цей час. Сутність такої місії набагато ширша, ніж примітивна ней-

тралізація і знешкодження саме терористів або їх угруповань, організацій та рухів терористичного спрямування.

Сучасний тероризм має сприйматися як екстремальна, вкрай девіантна соціальна діяльність, яка реально демонструє свої можливості за допомогою залякування суспільства. Криза керованості сучасного суспільства має багато причин (зростання динаміки соціальних перетворень, ускладнення взаємодії і глобалізація впливають на суспільну еволюцію факторів; посилення дестабілізуючих тенденцій), серед них і новий інформаційний режим, що сформувався на рубежі XX і XXI ст. Він характеризується формуванням (під впливом інформатизації та вдосконалення інформаційних технологій) глобальної інформаційно-комунікаційної системи, що кардинально змінила базові параметри інформаційного середовища. Це проявлено в знищенні бар'єрів між різними каналами трансляції інформації і формами її існування, в можливості глобального охоплення аудиторії єдиним контентом, швидкості проходження інформаційних повідомлень, інтелектуалізації інформаційної інфраструктури тощо. З'явилася можливість безпосереднього цільового впливу на соціальний елемент на рівні соціальної ментальності, відмінна від традиційно застосовуваних в ході еволюції соціальних систем інструментів переконання і примусу (фізична і військова сила, держава, з її тоталітарною машиною примусу та правовою системою тощо). Ефективність останніх залежить від наявності та передавальних характеристик численних проміжних середовищ, які часто кардинально спотворюють зміст і цільову функцію такого впливу. Соціальний креатив примусив соціум на розв'язання його головної проблеми — участь індивідуума в процесі вироблення управлінських рішень, реалізувавши за допомогою інформаційних технологій функцію зворотного зв'язку. Саме тому соціально-інформаційні технології, що володіють системоутворювальними функціями стали своєрідним імперативом для соціальних процесів і абсолютно затребувані як інструмент конструктивної чи деструктивної діяльності, а імперативність інформаційних повідомлень в управлінні особистістю стали базовим елементом соціальної системи — технологічним базисом соціального управління. Сумнів у їх раціональності, ігнорування або протест, підкріплений маніпулятивними технологіями, заснованими на більш тонких впливах на людину (переконання, формування емоційної заангажованості, цінностей, стимулів до певних дій тощо), можуть призвести до провокації кризових явищ соціального характеру з радикальними наслідками. Криза керованості завжди породжує соціальні конфлікти.

Як вважають деякі вчені, зараз ми перебуваємо в стані четвертої світової війни. По суті нова світова війна — це не «гаряча» війна у сенсі протиставлення її «холодній». Ця війна підняла тероризм до рівня головної зброї у

з'ясуванні відносин між керівними елітами, які претендують на світове панування. Терор і терористична діяльність — соціальні процеси що стали характерною ознакою сучасної епохи. Тероризм — дія з перетворення суспільства відповідно до ідеалів суб'єкта терористичної діяльності. Дія жорстка та незворотна в часі. Саме ця функція є основою, підґрунтям тероризму. Пошук спільних підходів до проблеми вивчення цих форм насильства триває понад 30 років, однак, незважаючи на це, немає однозначного визначення, що таке тероризм, які дії слід відносити до терористичних актів, у чому сутність терору, в чому першооснови того чи іншого явища. Очевидно, що протидія тероризму неможлива без комплексного теоретичного вивчення глибинних витоків, причин і умов його виникнення й активізації, осмислення наслідків його суспільно-перетворюючої функції та реалізації системи науково обґрунтованих державних або міждержавних соціально-правових заходів, спрямованих на зменшення вірогідності терористичної діяльності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ :

1. Волтер Л. Витоки / Л. Волтер // Насильство, влада, терор. Незалежний культурологічний часопис «Ї». — 2002. — №25. — С. 26–77.
2. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України: Монографія. — К.: Текст, 2003. — 600 с.
3. Петухов Ю. Четвертая мировая. Вторжение. Хроника оккупации Восточного полушария / Ю. Петухов — М.:Серия: IMPERIA-RUSSIA. Метагалактика, 2004. — 414 с.
4. Рижов І.М. Основи аналізу теророґенності соціальних систем: монографія. — К. : Магістр-XXI сторіччя. — 2008. — 288 с.
5. Сенченко М. Четверта світова війна / М. Сенченко. — Івано-Франківськ : Місто НВ, 2008. — 102 с.

РОЛЬ УПРАВЛІННЯ ДЕРЖАВНОЇ ОХОРОНИ УКРАЇНИ В БОРОТЬБІ З ТЕРОРИЗМОМ

ТКАЧЕНКО Олександр Олександрович,
здобувач Національної академії внутрішніх справ

Мінливий світ зумовлений постійними змінами як в ціннісних орієнтаціях, так і в світоглядних настановах призводить до формування нових суспільних відносин. На жаль, більшість публікацій, в яких розглядаються різноманітні аспекти боротьби з тероризмом обмежуються проблемами кримінологічної характеристики та питаннями кримінально-правової охорони. Причому переважна більшість публікацій написана особами, які не зовсім точно представляють зміст безпосереднього процесу протидії тероризму, оскільки окрім книжок на полицях бібліотек нічого в житті не бачили. Тематика тероризму є доволі розповсюдженою і майже чи не кожен дослідник вважає, що розбирається в ній. Однак, не вдаючись до причин такого поверхового підходу до серйозної проблеми, констатую, що нині майже відсутні публікації відкритого характеру щодо сутності виконуваних завдань, змісту та ролі Управління державної охорони України в боротьбі з тероризмом.

Ця тема є актуальною, оскільки в літературі, особливо в українській, взагалі розглядається діяльність лише двох суб'єктів боротьби з тероризмом: СБУ та МВС. Хоча в ст. 4 та 5 Закону України «Про боротьбу з тероризмом» визначено вісімнадцять таких суб'єктів, причому Управління державної охорони належать до першої групи суб'єктів — які безпосередньо здійснюють боротьбу з тероризмом у межах своєї компетенції.

Тому така неадекватність наукового пошуку українських дослідників дещо насторожує.

Управління державної охорони України бере участь в операціях з припинення терористичних актів, спрямованих проти посадових осіб та об'єктів, охорону яких доручено підпорядкованим цьому Управлінню підрозділам.

Правові основи організації і діяльності Управління державної охорони України визначені в Законі України «Про державну охорону органів державної влади та посадових осіб ».

Державна охорона органів державної влади України та посадових осіб — це система організаційно-правових, режимних, оперативно-розшукових, інженерно-технічних та інших заходів, які здійснюються спеціально уповноваженими державними органами з метою забезпечення нормального функціонування органів державної влади України, безпеки посадових осіб та об'єктів, визначених цим Законом. Не вважаються державною охороною,

регульованою цим Законом, заходи охоронного характеру, які здійснюються державними органами з метою забезпечення безпеки учасників кримінального судочинства, інших осіб та об'єктів, крім визначених цим Законом.

Державна охорона здійснюється щодо: Верховної Ради України; Кабінету Міністрів України; Конституційного Суду України; Верховного Суду України.

Державна охорона здійснюється щодо будинків, де працюють Верховна Рада України, Президент України, Кабінет Міністрів України, Конституційний Суд України, Верховний Суд України, споруд і спеціальних транспортних засобів, що перебувають в їх користуванні, інших місць постійного і тимчасового перебування осіб, які охороняються відповідно до цього Закону, важливих державних об'єктів та прилеглих до них територій і акваторій, визначених Президентом України.

Президентові України забезпечується безпека в місцях його постійного і тимчасового перебування шляхом здійснення державної охорони. Протягом строку повноважень Президента України також забезпечується безпека членів його сім'ї, які проживають разом з ним або супроводжують його. Після припинення повноважень Президент України забезпечується державною охороною довічно, якщо тільки він не був усунений з поста в порядку імпічменту.

*Особи, яким у місцях постійного і тимчасового перебування забезпечується безпек*а є: Голова Верховної Ради України; Прем'єр-міністр України; Голова Конституційного Суду України; Голова Верховного Суду України; Перший заступник Голови Верховної Ради України; Перший віце-прем'єр-міністр України; Міністр закордонних справ України; Генеральний прокурор України.

Протягом строку повноважень зазначених вище посадових осіб також забезпечується безпека членів їхніх сімей, які проживають разом з ними або супроводжують їх.

Після припинення повноважень зазначені посадові особи забезпечуються державною охороною протягом року, крім випадків набрання законної сили обвинувальним вироком щодо них.

Для здійснення покладених на Управління державної охорони завдань у сфері боротьби з тероризмом ***УДО України уповноважене***:

- надавати згоду на допущення громадян на об'єкти, щодо яких здійснюється державна охорона;
- одержувати в установленому порядку від керівників органів державної влади України, органів місцевого самоврядування, підприємств, установ, організацій незалежно від форм власності за письмовим запитом Начальника Управління або його заступників відомості, необхідні для здійснення державної охорони;

- використовувати форму одягу та документи, які зашифровують особу чи відомчу належність військовослужбовців і транспортних засобів Управління державної охорони України;
- проводити у порядку, визначеному Законом України «Про оперативно-розшукову діяльність» гласні та негласні оперативні заходи з метою запобігання терористичним актам проти посадових осіб і членів їхніх сімей та об'єктів, щодо яких здійснюється державна охорона, виявлення і припинення терористичної діяльності;
- проводити кіно-, фотозйомку, аудіо- і відеозапис на об'єктах, щодо яких здійснюється державна охорона;
- залучати за погодженням з керівниками правоохоронних та інших державних органів їх військовослужбовців і працівників, технічні та інші засоби;
- здійснювати на об'єктах, щодо яких здійснюється державна охорона, протипожежний, санітарно-гігієнічний, екологічний, радіаційний і протиепідемічний контроль та контроль за станом технічного захисту інформації, вживати заходів щодо усунення виявлених порушень, з'ясовувати причини, що призвели до їх вчинення;
- прикомандировувати в установленому порядку військовослужбовців Управління державної охорони України для здійснення державної охорони до органів державної влади, підприємств, установ і організацій, перелік яких визначається Президентом України;
- здійснювати підготовку, перепідготовку, підвищення кваліфікації військовослужбовців та працівників Управління державної охорони України відповідно до Закону України «Про освіту»;
- утворювати відповідно до законодавства госпрозрахункові підрозділи адміністративно-господарського характеру.

Отже, роль УДО України в боротьбі з тероризмом є вагомою, а з урахуванням сучасних тенденцій щодо несилового тиску на вищі органи державної влади, лобіювання антидержавних проектів і відстоювання всупереч національним інтересам крізь агентів впливу псевдодержавних ідей постає низка нових завдань у сфері забезпечення безпеки Президента України та вищих посадових осіб держави, передусім їхньої інформаційної безпеки.

Управління державної охорони України на сучасному етапі має перетворитися на орган, який забезпечує не лише фізичну безпеку, а й інформаційну недоторканність Президента, унеможливлює вплив на вищих посадових осіб держави передусім інформаційними методами, формує безпечний інформаційний простір для вищих посадових осіб з метою реалізації ними державної політики відповідно до національних інтересів.

Адже практика показує, що нині лобістські технології і завуальовані громадські організації, які реалізують політику транснаціональних корпорацій або іноземних спецслужб здатні завдати більше шкоди державним інтересам, ніж простий фізичний напад на вищих посадових осіб держави або терористичний акт. Адже і перше і друге носить одноразовий характер, а наявність інформаційних технологій перетворює на незалежних дану категорію осіб, які вже на постійній основі реалізують інтереси даних іноземних служб. Тобто фактично механізм маніпуляції формується під конкретних і для конкретних чиновників, якими потім керують.

У сучасному інформаційному світі зростає роль несилових методів вирішення конфліктів, водночас самі конфлікти і необхідність та здатність держави щодо їх подолання в тому числі і силового існуватиме завжди. Конфлікти є притаманними будь-якій державі, і від того, наскільки служба безпеки Президента буде готова саме в інформаційному плані, залежатиме ефективність здійснення вищими посадовими особами держави своїй функціональних обов'язків. А від цього залежатиме і здатність держави щодо відстоювання власних національних інтересів і реалізації суверенного і самостійного курсу на розвиток.

Інформаційна складова за нинішніх умов стає домінантною, а інформаційні технології боротьби з тероризмом мають стати одними з провідних в арсеналі Управління державної служи охорони України.

ОСОБЛИВОСТІ ВЗАЄМОДІЇ СУБ'ЄКТІВ БОРОТЬБИ З ТЕРОРИЗМОМ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

ФАТХУТДІНОВ Василь Гайнулович,
кандидат юридичних наук, доцент,
Заслужений юрист України

В умовах формування та розвитку інформаційного суспільства важливого значення набуває збереження визначальної ролі держави, як політико-територіальної організації громадянського суспільства. За цих умов і в даному контексті боротьба з тероризмом нами розглядається як системний процес, який має включати вжиття не лише силових, а й передусім системи інформаційних заходів. Причому вжиття даних заходів має відбуватись

також і на системній основі. Логічним у даному аспекті порушити питання про необхідність визначення нових орієнтирів взаємодії суб'єктів боротьби з тероризмом на сучасному етапі.

Термін взаємодія належить здебільшого до сфери управління. **Взаємодія суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом** — погоджена у часі і місці спільна діяльність даних суб'єктів, спрямована на припинення злочинної діяльності осіб, причетних до тероризму, в тому числі міжнародного, фінансування, підтримки чи вчинення терористичних актів та терористичних злочинів.

Взаємодію як управлінське поняття також розглядають як форму зв'язку елементів системи, за допомогою якої вони взаємно доповнюючи один одного, створюють умови для успішного функціонування всієї системи в цілому. Причому необхідно мати на увазі, що взаємодія як управлінська категорія проявляється не тільки у внутрішньо-організаційній діяльності системи, але й в зовнішніх функціях. Відтак боротьба з тероризмом є нічим іншим, як процесом керованої взаємодії системи суб'єктів боротьби з тероризмом та терористичної злочинності.

Термін «взаємодія» широко використовується у теорії й на практиці, оскільки відображає характер спільних зусиль різних органів та організацій у здійсненні державної політики боротьби з тероризмом.

Необхідність системного реформування суб'єктів боротьби з тероризмом є необхідною з огляду на активний розвиток інформаційного суспільства і все зростаючу частку інформаційних технологій, що їх використовують терористи. Реформування даної системи суб'єктів також корелює із вступом у дію нового КПК України. Внаслідок цього зазнають системних змін функціонал правоохоронної системи, яка і становить основу системи суб'єктів боротьби з тероризмом. Натомість слід констатувати, що нині керівництво держави не розглядає потребу реформування даної системи як головну і взагалі нагальну, хоча рівень терористичних загроз, рівень напруженості і конфліктності українського соціуму, претензій інших держав, в тому числі і територіальних є високим і тероризм для України за умов може стати реальністю. З метою запобігання цьому процесу потрібно розробляти не лише антитерористичне законодавство, про що можна знайти чимало публікацій, а й передусім розв'язувати конкретні питання взаємодії суб'єктів боротьби з тероризмом з урахуванням нових реалій щодо впровадження інноваційних та інформаційних технологій у їхню діяльність.

Відтак постають актуальні завдання щодо розроблення нових принципів функціонування даної системи, які мають відповідати потребам українського суспільства.

Разом із цим дані процеси спричинюють виникнення певних складнощів. Збільшилася кількість зв'язків, через які реалізується кооперація елементів системи боротьби з тероризмом. Самі зв'язки ускладнились, виникла необхідність у виконанні та регламентації спеціальних дій, які мають на меті координацію і узгодження усього різмаїття зв'язків для отримання системного ефекту — антитерористичної безпеки.

Нині можу чітко констатувати, що в системі боротьби з тероризмом після чисельних кадрових змін особливо в Антитерористичному центрі при СБУ набуло поширення дублювання повноважень. Ці дії в умовах збільшення загроз українському суспільству зумовлюють необхідність організації взаємодії суб'єктів даної системи.

Шлях підвищення ефективності роботи системи боротьби з тероризмом проходить через все більш широке і раціональне використання взаємодії як всередині системи цих органів, її ланок, так і за її межами — з державними, громадськими і міжнародними організаціями. Дедалі більшого значення набуває залучення громадських та неурядових організацій для здійснення протидії тероризму. Отже, обґрунтовуємо висновок: взаємодія суб'єктів боротьби з тероризмом — поняття широке та багатоаспектне.

Характерними ознаками взаємодії суб'єктів боротьби з тероризмом є:

- ❒ *наявність спільної діяльності декількох органів державної влади* (у даному випадку 18);
- ❒ *погодженість заходів за метою, місцем, часом, методами* (дане завдання покладено на АТЦ, який визначає місце, час та методи проведення антитерористичної операції);
- ❒ *спрямованість функціонування взаємодіючих суб'єктів* (припинення злочинної діяльності осіб, причетних до тероризму, в тому числі міжнародного, фінансування, підтримки чи вчинення терористичних актів та злочинів, які скоєні з терористичною метою);
- ❒ наявність нормативно-правової бази взаємодії (окрім Закону України «Про боротьбу з тероризмом», також існують закони, що регулюють діяльність кожного суб'єкта боротьби з тероризмом: Закони України «Про міліцію», «Про Службу безпеки України» тощо, а також відомча нормативна база, яка закріплює порядок і форми взаємодії конкретних суб'єктів);
- ❒ *зміст завдань, що виконуються суб'єктами взаємодії* (запобігання, виявлення, припинення, мінімізації наслідків терористичної діяльності);
- ❒ *становище, яке обіймають суб'єкти взаємодії в ієрархії системи* (у коментованому законі чітко окреслено, як саму дворівневу ієрархії

суб'єктів, так і визначено головний орган у загальнодержавній системі боротьби з терористичною діяльністю — Службу безпеки України);

- ❒ *спільна діяльність* (комплекс скоординованих спеціальних заходів, спрямованих на попередження, запобігання та припинення злочинних діянь, здійснюваних з терористичною метою, звільнення заручників, знешкодження терористів, мінімізацію наслідків терористичного акту чи іншого злочину, здійснюваного з терористичною метою).

Питання взаємодії є досить важливими, через що, майже у всіх законах, що регулюють порядок діяльності суб'єктів, які безпосередньо здійснюють боротьбі з тероризмом, зазначено на взаємодію (ст. 8 Закону України «Про міліцію», ст. 16 Закону України «Про Службу безпеки України», ст. 10 Закону України «Про державну охорону органів державної влади України та посадових осіб» тощо).

Отже взаємодія суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом, може дати очікуваний ефект, якщо матиме конкретний характер і ґрунтуватиметься на законі, дотриманні принципів взаємодії та правильному поєднанні форм і методів професійної діяльності, властивих кожному із суб'єктів взаємодії. Водночас має бути чітке розмежування повноважень та обов'язків кожного суб'єкта взаємодії відповідно до предметної компетенції кожного з них, ґрунтуючись на відповідному законодавстві.

ИНФОРМАЦИОННОЕ ОБЩЕСТВО И СОДЕРЖАНИЕ ИНФОРМАЦИОННОЙ ФУНКЦИИ ГОСУДАРСТВА В БОРЬБЕ С ТЕРРОРИЗМОМ

ИНФОРМАЦИОННАЯ ФУНКЦИЯ ГОСУДАРСТВА В БОРЬБЕ С ТЕРРОРИЗМОМ И ЭКСТРЕМИЗМОМ В КАЗАХСТАНЕ

АЙТБАЕВ Кайрат Ташкулович –
начальник Учебного центра
МВД Республики Казахстан им. Б. Момышулы,
доктор юридических наук

С момента установления независимости в Республике Казахстан, как и во многих странах содружества, переходный период сопряжен с развитием как позитивных, так и негативных процессов во взаимодействии государств в области обеспечения всеобщего мира и безопасности.

Трагические события в сентябре 2001 года в Нью-Йорке и Вашингтоне, а также терактами, совершаемыми по сей день в России, являются неоспоримой первостепенной задачей всего мирового сообщества.

В наши дни особое значение приобретает информационная функция государства в борьбе с терроризмом и экстремизмом.

Противодействие терроризму является одним из приоритетных направлений в обеспечении национальной безопасности страны.

Казахстан решительно осуждает терроризм во всех его формах и проявлениях и выступает за принятие коллективных усилий мирового сообщества по борьбе с этим явлением. Закон Республики Казахстан «О противодействии терроризму» от 13 июля 1999 года № 416 устанавливает основные принципы, цели, правовые и организационные основы противодействия терроризму, профилактики терроризма, минимизации и (или) ликвидации последствий терроризма, а также обязанности и права человека и гражданина,

гарантии их соблюдения в связи с осуществлением деятельности в сфере противодействия терроризму [1].

Республика неукоснительно выполняет требования Резолюции СБ ООН и ежегодно представляет Национальный доклад о проделанной работе в Контртеррористический Комитет ООН. Поддержано создание и принято активное участие в деятельности Международной контртеррористической коалиции.

Казахстан присоединился ко всем тринадцати международным универсальным конвенциям о борьбе с терроризмом. В настоящее время Казахстаном проводятся внутригосударственные процедуры по ратификации 3-х протоколов и поправок к ним. Казахстан считает, что международное сотрудничество в борьбе с терроризмом должно осуществляться в полном соответствии с нормами международного права, а также поддерживает дальнейшее совершенствование антитеррористических договорных механизмов, в том числе в отношении принятия Всеобъемлющей конвенции о борьбе с международным терроризмом.

В соответствии с решениями Совета безопасности ООН в стране налажена система противодействия отмыванию денег и финансированию террористических организаций.

На территории Казахстана запрещены организации, деятельность которых носит террористический характер. Организации признаются террористическими, если их уставные цели и деятельность противоречат Конституции и Законам Республики Казахстан и международным договорам, участником которых является Республика Казахстан; в случае, если существует потенциальная опасность активизации функционирования этих организаций по дестабилизации обстановки в государствах центрально-азиатского региона [2].

В 2004 году Верховный суд запретил в Казахстане 4 организации, чья причастность к террористическим актам доказана. В 2005 году этот список пополнился ещё 9 организациями («Аль-Каеда», «Асбат аль-Ансар», «Братья-мусульмане», «Боз гурд», «Жамаат моджахедов Центральной Азии», «Исламское движение Узбекистана», «Исламская партия Восточного Туркестана», «Курдский народный конгресс», «Талибан», «Лашкар-и-Тайба», «Хизб-ут-Тахрир», «Таблиги джамаат», и «Общество социальных реформ»).

Понимая, что борьба с международным терроризмом и экстремизмом требует взаимодействия государств на всех уровнях (глобальном, региональном и двустороннем), республикой подписан ряд международных и межгосударственных договоров и соглашений в данной сфере.

Большое значение придается развитию регионального сотрудничества, представленного в настоящее время деятельностью Антитеррористического

центра Содружества Независимых Государств, Региональной антитеррористической структуры Шанхайской организации сотрудничества, а также в рамках предпринимаемых мер в сфере борьбы с терроризмом и экстремизмом Организации Договора о коллективной безопасности. Осуществляется практическое взаимодействие государств-участников СНГ, входящих в состав созданного по инициативе Президента Казахстана в 2000 году Антитеррористического центра. Определен порядок организации и проведения совместных антитеррористических мероприятий на территории стран Содружества. Механизм его функционирования успешно апробирован в ходе крупномасштабного совместного учения специальных служб и органов безопасности стран Содружества «Каспий-Антитеррор-2005», состоявшегося в Казахстане в августе 2005 года.

Весомым компонентом обеспечения безопасности и стабильности, региональным и общемировым политическим фактором становится «Шанхайская организация сотрудничества» (ШОС), основанная 15 июня 2001 года. В рамках регионального и субрегионального контртеррористического сотрудничества реализованы мероприятия по укреплению правовых основ противодействия терроризму в формате ШОС. Подписаны конвенция ШОС против терроризма, а также соглашения ШОС о подготовке кадров для антитеррористических формирований и о сотрудничестве в борьбе с незаконным оборотом оружия, боеприпасов и взрывчатых веществ. Ратифицировано Положение о политико-дипломатических мерах и механизмах реагирования ШОС на ситуации, ставящие под угрозу мир, безопасность и стабильность в регионе. Утверждена Программа сотрудничества государств-членов ШОС в борьбе с терроризмом, сепаратизмом на 2010–2012 годы.

В рамках ШОС с 1 января 2004 года действует Исполком Региональной антитеррористической структуры (РАТС) в г.Ташкент. С момента создания Региональной антитеррористической структурой ШОС налажено взаимодействие с региональным представительством Управления ООН по наркотикам и преступности в Центральной Азии.

В целях укрепления в формате ОДКБ на территории Казахстана проведено стратегическое оперативно-тактическое учение «Взаимодействие-2009» (октябрь 2009г.) Коллективных сил оперативного реагирования, рассматриваемых в качестве компонента постоянной готовности сил и средств ОДКБ для адекватного реагирования на вызовы и угрозы, в том числе возможные террористические действия и чрезвычайные ситуации.

Казахстан участвует в реализации контртеррористических мероприятий в рамках Индивидуального плана действий партнерства с НАТО. Расширяется сотрудничество с Советом Евро-Атлантического партнерства. Показателем

доверия к Казахстану стало проведение в г.Астане 24–26 июня 2009 года 3-го Форума безопасности НАТО/СЕАП и межпарламентского семинара Роуза-Рота.

Принят Закон «О противодействии легализации (отмыванию) доходов, полученных незаконным путем, и финансированию терроризма», в соответствии с которым создан соответствующий уполномоченный орган — Комитет финансового мониторинга Министерства финансов. Вступил в силу Закон «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационно-коммуникационных сетей» регламентирующий механизмы пересечения и приостановления распространения в Интернете информации противоправного характера, в том числе террористического и экстремистского содержания. 8 апреля 2010 года принят Закон «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам противодействия терроризму», которым корректируются 5 кодексов и 11 законов, в соответствии с международными нормами устанавливаются принципы и модель государственной системы противодействия терроризму.

6 июня 2008 г. в г.Алматы, на базе Института ядерной физики Национального ядерного центра состоялись международные антитеррористические учения «Атом — Антитеррор — 2008» в рамках Глобальной инициативы по борьбе с актами ядерного терроризма в июне 2007 года. 11–12 сентября 2008 года в г.Усть-Каменогорске на базе АО «Ульбинский Металлургический Завод» был проведен международный практический семинар «Проектная угроза». Представители стран-сопредседателей — России и США — оценили их как весомый вклад нашей страны в практическую реализацию Глобальной инициативы [3].

Наша страна на практике поддерживает усилия международного сообщества по борьбе с терроризмом, развивает всестороннее сотрудничество и взаимодействие.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений.

Распределение и использование информации для удовлетворения социальных потребностей является едва ли не главнейшей задачей государства на любом этапе развития. Таким образом, информационная функция всегда существовала как функция государственных органов, то есть как реализация компетенции, прав и обязанностей отдельных органов в соответ-

ствии с их местом и назначением в государственном механизме и политической системе общества.

До самого последнего времени проблеме информационной функции в работах ученых по теории государства и права не уделялось внимания, и в трудах Н.Г. Александрова, М.И. Байтина, А.И. Денисова, Л.И. Загайнова, А.П. Косицына, Г.Н. Манова, Н.П. Фарберова, Н.В. Черноголовкина, М.А. Сарсембаева и др., посвященных этой проблематике, рассматривались основные функции государства без выделения информационной [4].

В процессе развития общества появились определенные факторы, которые привели к возрастанию роли информации, а, следовательно, к более четкому выделению информационной функции государства. К таким факторам можно отнести: 1) формирование единого мирового информационного пространства и углубление процессов информационной интеграции; повышение уровня доступности, распространения и использования информации, ее реальное обеспечение техническими средствами; 2) возрастание роли информационно — коммуникационной инфраструктуры в системе общественного производства; 3) становление и в последующем доминирование в экономике новых технологических укладов, базирующихся на массовом использовании информационных технологий, средств вычислительной техники и телекоммуникаций; производство информации в объемах, необходимых и достаточных для обеспечения жизнедеятельности и развития общества во всех его частях и направлениях.

Экономика общества ориентирована на производство, прежде всего продуктов информационной и интеллектуальной деятельности, связанных с получением новой информации и новых знаний, и реализацией этих продуктов. А государственные структуры призваны решать задачи по созданию эффективной системы обеспечения прав граждан и социальных институтов на свободное получение, распространение и использование информации как важнейшего условия демократического развития, улучшение взаимодействия населения с органами власти.

Указанные факторы привели к новой эволюции функций государства, к повышенному интересу к этой сфере деятельности государства. Не случайно в последние годы появился ряд исследований, в которых предпринимались попытки изучить информационную политику государства [5].

Известно, что основные функции государства — это наиболее общие, важнейшие направления его деятельности по осуществлению коренных стратегических задач и целей, стоящих перед ним в определенный исторический период. Сообразно с этим основные функции государства группиру-

ют по наиболее важным направлениям его воздействия на общественные отношения.

Информатизация предполагает преобразование всего комплекса способов и условий развития информационных процессов, создание соответствующей технической базы и необходимого государственно — правового обеспечения. Иными словами, процесс информатизации можно воспринимать как совокупность действий и мер по формированию и реализации материальной основы развития информационного общества.

Главными целями государства в сфере информатизации являются информационное обеспечение деятельности органов государства; информационное обеспечение внешних по отношению к государственным органам субъектов, в том числе физических лиц; сохранение и структурирование информационного пространства.

Для правового регулирования этих задач необходимо определить те государственные органы, которые будут отвечать за формирование и курирование различных государственных информационных ресурсов; обеспечение полноты, точности, достоверности и своевременности предоставления информации организациям и гражданам независимо от их территориального размещения; установление прав и обязанностей соответствующих субъектов в информационных отношениях. Эти задачи государства в сфере информатизации являются основой для определения содержания его информационной функции.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Закон Республики Казахстан «О противодействии терроризму» от 13 июля 1999 года № 416. «Казахстанская правда» от 30.07.99 г. № 182–183; (Ведомости Парламента РК), 1999 г., N 19, ст. 649.
2. Сарсембаев М.А. Уголовное право. Международное право. А. «Данекер». 1999 г.
3. Кудайбергенов М.Б. Международное уголовное право в документах. Данекер. 1999 г.
4. Бачило И.Л. Глобальная информатизация и право. Http:// www.fact.ru/ num05/ batchilo.html.
5. Мелюхин И.С. Проблемы развития информационной политики // Научно — техническая информация. Сер. 1. 1996. N 8. С. 27.

ПРАВОВА ОСНОВА СТАНОВЛЕННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В ЄС В КОНТЕКСТІ БОРОТЬБИ З ТЕРОРИЗМОМ

МАКСИМЕНКО Юлія Євгенівна,
Доцент кафедри теорії держави і права НАВС
кандидат юридичних наук,

Становлення європейського інформаційного суспільства має давню правову історію.

Одними з перших нормативно-правових актів, що регулюють питання становлення інформаційного суспільства в ЄС є *Резолюція Європейського Союзу «Біла Книга. Зростання, конкурентоспроможність, зайнятість: виклики та стратегії XXI століття» 1993 року, Директива ЄС «Зелена Книга. Життя і працевлаштування в інформаційному суспільстві» та Рекомендація «Інформаційна магістраль для глобального суспільства»* 1996 року.

Так, у 1993 році *Комісія ЄС* визначила інформаційне суспільство як суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій та технологій зв'язку. Вже у 1997 році Єврокомісія зазначає, що ***інформаційним суспільством*** слід вважати:

1) суспільство нового типу, що формується внаслідок глобальної соціальної революції та породжується вибуховим розвитком і конвергенцією інформаційних та комунікаційних технологій;

2) суспільство знань, тобто суспільство, у якому головною умовою добробуту кожної людини і кожної держави стає знання, що здобуте завдяки безперешкодному доступу до інформації та вмінню працювати з нею;

3) глобальне суспільство, в якому обмін інформацією не матиме ані часових, ані просторових, ані політичних меж; яке, з одного боку, сприяє взаємопроникненню культур, а з іншого — відкриває кожному суспільству нові можливості для самоідентифікації.

До основних ***напрямів інформаційна політики*** ЄС належать:

1) політика лібералізації і приватизації телекомунікацій.

2) розвиток інформаційних послуг та мереж.

3) розвиток технічного і соціально-інформаційного забезпечення.

4) протидія інформаційним монополіям.

5) створення ринку інформаційних послуг.

6) недискримінація за інформаційною ознакою.

Створення інформаційного законодавства та адекватної законодавчої бази, яка враховує як національні, так і міжнародні принципи регулювання інформаційних відносин, вважається головним чинником зростання прибутку країни від потенціалу інформаційно-комунікаційних технологій.

Досить важливим є *Ліссабонський самміт країн ЄС*, що проходив 23–24 березня 2000 року. На даній зустрічі були зазначені ***загрози та виклики розвитку*** для країн ЄС:

1) якісний стрибок у світовій економіці,

2) детермінована глобалізація,

3) становлення постіндустріальної (інтелектуальної) цивілізації, які впливають на всі сфери життєдіяльності європейської спільноти та потребують радикальної трансформації європейської політики та економіки.

Новою **стратегічною метою** Європейського Співтовариства до 2015 року визнано формування європейського інтелектуального потенціалу, удосконалення інформаційної та телекомунікаційної інфраструктур, стимулювання інноваційної діяльності й структурної реформи економіки, модернізацію системи освіти, розробку підходів до європейської соціальної моделі, криза якої супроводжується прогресуючим демографічним дисбалансом населення. Перед організацією також стоїть дилема: як досягти прискореного економічного зростання і водночас зберегти європейські цінності соціальної солідарності.

Серед основних заходів для вирішення вищезазначених проблем на даному Самміті було ухвалено реалізувати *План дій «e-Europe»* на основі документів Європейської Комісії — «Ініціатива e-Europe» та «Стратегія працевлаштування в інформаційному суспільстві».

Даний План передбачає широке впровадження технологій Internet для розвитку електронної комерції та інформаційних послуг, а також розвиток знань і навичок населення європейських країн, необхідних для існування в інформаційному суспільстві.

Загалом, на основі здійсненого аналізу вищевикладених норм ряду нормативно-правових актів Євросоюзу, можна виокремити, *основні європейські інтереси в інформаційній сфері,* а саме:

а) для людини:

- охорона персональних даних;
- безпека інформації про приватне життя;
- забезпечення конфіденційності міждержавних інформаційних відносин;

б) для суспільства та Союзу:

– вплив на структуру європейської спільноти і систему цінностей;
– відтік інтелектуальних ресурсів;
– технологічна залежність від США та Японії.

До ***основних напрямів інформаційної політики ЄС*** для управління загрозами з метою реалізації вище зазначених інтересів належать:

1) удосконалення нового суспільного середовища;
2) поглиблення міждержавного співробітництва в умовах становлення інформаційного суспільства;
3) забезпечення вільного обігу інформації в суспільстві для підвищення ступеня демократичної участі країн у політичних процесах;
4) побудова економіки знань (інформаційної економіки);
5) створення та використання конкурентноспроможних інформаційних ресурсів та потенціалу Європи в міжнародному економічному середовищі;
6) недопущення злочинів у кіберпросторі;
7) забезпечення працевлаштування європейського населення в інформаційному суспільстві;
8) вільний доступ до ресурсів мережі Internet;
9) недопущення розшарування суспільства за інформаційною ознакою на «інформаційно багатих» та «інформаційно бідних»;
10) поширення ідей, знань, інформації на рівноправних підставах для всіх народів європейського регіону;
11) використання спільної європейської інформаційної спадщини на благо цивілізації;
12) захист інформаційної інтелектуальної власності;
13) розширення інформаційної інфраструктури в Європі шляхом створення панєвропейської інформаційної магістралі «EuroNet».

Необхідно зазначити, що в інформаційному суспільстві кожний громадянин країн-учасниць ЄС має право доступу до даних відкритого характеру (закони, урядові рішення, інформацію засобів масової комунікації), культурної спадщини (літературні твори, не обмежені авторським правом і віднесені до національного надбання, наукові праці, безоплатне програмне забезпечення, непатентовані стандарти), а також до інформації відкритого характеру в комп'ютерних мережах і системах, що потребує осмислення відповідальності за здійснення нової політики. Натомість така відкритість стала причиною хвилі терористичних актів у Великій Британії у 2011 році, коли за допомогою відкритих ресурсів терористи домовлялися про здійснення своїх намірів.

Глобальні інформаційні процеси також негативної впливають на рівень антитерористичної безпеки ЄС, що значно ускладнює відносини всередині

ЄС. Поєднані із фінансовою кризою і постійним бажанням щодо тотального домінування Німеччини в ЄС, а також лібералізація міжнародних відносин у Франції у 2012 році після програшу Саркозі, поєднана із економією бюджетних коштів в частині асигнування на різноманітні програми ЄС, частково можуть сприяти зниженню рівня безпеки ЄС.

У даному аспекті основним завданням європейської спільноти полягає у виробленні спільного світогляду на системні проблеми, а не жорсткий диктат Німеччини, котра фактично перетворили на васалів чимало Європейських країн. Внутрішня напруга, поєднана з бідністю, зокрема у таких країнах як, Греція, Іспанія, Італія, Португалія; невиважена інформаційна політика потурання анархізму та неонацизму на противагу більш виваженій безпековій політиці Європи, можуть за певних умов стати каталізатором для активізації терористських угруповань і терористичної діяльності.

Трансформація демократичних інститутів має відбуватись не лише в бік розкриття інформаційних ресурсів і створення безмежних умов для користування інформаційними ресурсами громадянами, а й. передусім, для формування безпечного інформаційного суспільства, формування надійного механізму охорони інформаційних прав і свобод людини в нових умовах. Адже захист плюралізму не означає захист тероризму, неонацизму, анархізму та інших видів антигромадської і ант суспільної поведінки. Так само, як захист незалежності засобів масової комунікації не означає відсутність можливості притягнення до відповідальності за розпалювання міжнаціональної ворожнечі, або ж формування через ЗМІ нігілізму до органів державної влади, поневіряння і законні засоби вирішення конфліктних ситуацій і таким чином формування умов для пропаганди тероризму або екстремізму.

Незалежність це гармонія справедливості, рівня добра і сталості конструктивних цінностей суспільства, збереженні національного розвитку, культурної самобутності і мовного розмаїття країн Європи.

Саме тому становлення інформаційного суспільства має відбуватись на чіткій виваженій правовій основі, що в врешті-решт сприятиме закладенню міцного фундаменту для формування ефективної державної антитерористичної політики.

КОНЦЕПЦІЯ МЕРЕЖЕВОГО СУСПІЛЬСТВА В КОНТЕКСТІ БОРОТЬБИ З ТЕРОРИЗМОМ

СОПІЛКО Ірина Миколаївна,
директор Юридичного інституту Національного авіаційного університету,
кандидат юридичних наук, доцент

Нинішня глобалізація виступає чи не найнеоднозначнішим виявом сучасної дійсності. З одного боку чимало дослідників описують позитивні моменти як формування інформаційного суспільства, так і необхідності розроблення інформаційного права як загального регулятора інформаційних правовідносин. Інша група дослідників зосереджує увагу у власних пошуках на забезпеченні інформаційної безпеки, реалізації окремих положень державної інформаційної політики. Не вдаючись до полеміки з авторами даних наукових позицій, хочу висловити свою думку щодо загального напряму цих досліджень.

Інформаційне суспільство, або як його спочатку називали — постіндустріальне, набуло свого розвитку в контексті значного збільшення обсягів інформації і неможливості державних установ щодо її повного контролю, особливо в частині її передавання. Таким чином формування інформаційного суспільства як такого можна розглядати лише як *форму* прояву змін, які назріли в індустріальному соціумі. Натомість, я не розділяю такий настрій щодо *змісту* формування соціуму. Адже змістовно інформація завжди була, є і буде, і питання не у тому, яким чином ми передаємо інформацію і отримуємо до неї доступ, а у тому, що з цією інформацією ми можемо зробити, які вигоди, користь та переваги від цього отримати.

Відповіді на ці питання концепція інформаційного суспільства не дає, адже вона є надто загальною, я ба навіть сказала метаконцепцією. В ній немає конкретики, яка б чітко визначили ознаки і переваги цього суспільства над іншими саме для людини. Відтак постає питання у формуванні надінформаційного суспільства — мережевого суспільства.

Мережеве суспільство це суспільство вище за інформаційне, оскільки окрім усіх ознак інформаційного його вирізняє кластерізація групи користувачів за певними критеріями, і отримання на підставі них певних не тільки інформаційних, а й економічних, політичних, культурних та інших переваг.

В українській науковій літературі, особливо з інформаціологічної тематики, дана тема майже не порушується. Захопленість різноманітними аспектами інституціоналізації інформаційного права (роботи А.І.Марущака та його учнів), структуризації інформаційного законодавства (роботи М.Я.Швеця,

В. А. Ліпкана, Р.А.Калюжного та їх учнів), різноманітними проектами інформаційного Кодексу (роботи В.М.Брижка, К.І.Бєлякова, В.С.Цимбалюка, В.Д.Гавловського та їх учнів), аналіз напрямів державної інформаційної політики (роботи І.В.Арістової та її учнів) насправді відволікає від справжнього контексту сучасної інформаційної проблематики: нагальна потреба у дослідженні концепції мережевого суспільства.

Підґрунтям формування мережевого суспільства стало розроблення і кіберпросторі соціальних мереж: мереж, які за допомогою розроблених алгоритмів визначають спільні інтереси, самі здійснюють пошук і фактично формують замкнений та цікавий світ для конкретної людини: починаючи від її інтересів в книжках, закінчуючи привілеями щодо спілкування з тими чи іншими особами за фаховими та іншими ознаками. У рамках даних мереж людина отримує нове реальне життя із реальним привілеями та перевагами перед іншими — не членами даної мережі.

Схильність людей до більш відкритого спілкування саме у віртуальному просторі була дуже чітко відстежена і використана програмістами, внаслідок чого за допомогою різноманітних скриптів, фішінгових та інших програм можна скласти психологічний та інтелектуальний портрет конкретної людини за лічені секунди. Привабливість даних мереж також пояснюється тим, що заздалегідь закладені похибки у пошукові механізми даних мереж складають нове відкриття для людей, які здебільшого це сприймають як свій власний вибір, і фактично починають думати і обирати за розробленим в рамках даної мережі алгоритмом. Маніпулювання свідомістю і фактичний вплив на неї чиниться в таких мережах опосередковано, оскільки самі події не сприймаються і не є початково наслідком суворо детермінованих причин, натомість мають дуже відчутний ефект: адже людина, що має проблеми в реальному житті зі спілкуванням, у віртуальному світі через соціальні мережі та різноманітні програми пошуку контактів фактично набуває нового життя.

Недостатність на даному етапі статистичного матеріалу, а також великий масив імовірнісних рішень дають змогу на даному етапі поки що висувати гіпотези. Натомість, переконана, що з часом, наші положення набудуть більшої, передусім наукової, аргументації через їх верифікативність на практиці.

Ключовим моментом будови соціальних мереж виступає те, що в них потрібно аналізувати не зв'язки між вузлами мережі, а властивості відносин між учасниками даної мережі. Застосування банальних методів інформаційного моделювання, зокрема метода графів не дають змогу проаналізувати різнорідні і почасти різнокласові вибірки вузлів, які пов'язані різними типами зв'язків.

Притаманною рисою соціальної мережі є не тільки джерела невідомостей, а й знання методів, які можуть досліджувати ці невідомості. У реальних соціальних мережах невизначеність інформації є іманентною, чим саме і пояснюється необхідність застування положень синергетики до вивчення мережевих суспільств. Одним із методів, які можна застосувати для вивчення невизначеностей є байесовські імовірнісні мережі, які використовуються в умовах невизначеності, коли сутність набутого знання полягає в розумінні того, чи впливає отримана інформація на наші очікування відносно інших подій.

Концепція мережевого суспільства є важливою для розуміння сучасного змісту боротьби з тероризмом, адже терористи утворюють власні соціальні мережі і нагальність підготовки мережевих фахівців виступає кричущою потребою, оскільки терористичні мережі, які нині функціонують в Інтернеті носять завуальований конспіративний характер, а їхнє виявлення співробітниками правоохоронних органів, які не володіють спеціальним передусім методологічним інструментарієм, відповідними знанням і та інформаційними технологіями, стає дедалі складнішим. Не зовсім правильний підхід можна спостерігати у відомчій освіті, зокрема з підготовки фахівців боротьби з тероризмом. Адже нині системні прорахунки і помилки, спричинені нефаховим управлінням освітою у ВНЗ правоохоронних органів, призвели до того, що боротьба з кіберзлочинністю ведеться випускниками навчальних закладів МВС, СБУ, ЗСУ тощо, які не мають фахової освіти щодо протидії злочинам у кіберпросторі, не орієнтуються у сучасних методах будови і структурного аналізу мереж інформаційного суспільства, не володіють сучасними аналітичними методами дослідження соціальних мереж.

За таких умов для держави постає необхідність не лише у розробленні концепції мережевого суспільства, а й в усвідомленні необхідності підготовки відповідних фахівців для захисту інтересів громадян і держави в інформаційному просторі. Показовим прикладом ефективного аналізу соціальних мереж є затримання Саддама Хусейна, а також чисельних учасників масових безладів, які відбувались у Великій Британії у 2011 році, коли за допомогою всесвітньо відомої мережі Twitter здійснювалося управління групами людей для вчинення масових безладів у групових порушень громадського порядку. Водночас саме ефективний аналіз даних мереж дозволив своєчасно виявити організаторів даних злочинних дій, а також затримати більшість її активних учасників.

Підбиваючи підсумок зазначу, що моя позиція зумовлена не стільки намаганням викласти не схожу на інших наукову позицію, скільки прагненням застосувати адекватну сучасним реаліям методологію і отримати нові науко-

во значущі результати. Мережеве суспільство має стати об'єктом окремого наукового розгляду, а формування і вивчення закономірностей його побудови надасть змогу до обрання вірної та ефективної методології щодо його дослідження та управління з метою досягнення всезагального блага.

Адже мережеве суспільство несе в собі чимало загроз для держави, тому знання методології побудови, базових концептів та аксіоматичних ймовірностей вирахування деструктивних зв'язків стане запорукою в успішній боротьбі з тероризм умом у XXI столітті.

ГАРАНТІЇ ЗАБЕЗПЕЧЕННЯ ПРАВ І СВОБОД ЛЮДИНИ І ГРОМАДЯНИНА ПРИ ЗДІЙСНЕННІ ПРОТИДІЇ ТЕРОРИЗМУ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

ТЮРІНА Оксана Володимирівна,
доцент кафедри теорії держави та права НАВС,
кандидат юридичних наук, доцент

Основи правового статусу людини і громадянина становлять самостійний правовий інститут в рамках конституційного права як фундаментальної галузі права певної національної правової системи кожної країни-члена ЄС, так і правової системи Європейського Союзу в цілому. Даний правовий інститут має системний вимір і охоплює такі базові компоненти, як інститут громадянства ЄС, принципи правового статусу особи, сукупність основних прав, свобод та обов'язків людини і громадянина, а також їх гарантії. Право Європейського Союзу не містить власних, особливих стандартів прав людини, воно сприйняло та захищає ті досягнення у сфері прав і свобод людини, які є спільними для конституційних традицій держав-членів та відтворюються в їхніх правових системах.

У 1999р. на вищому політичному рівні Європейська Рада створила Європейський Конвент як тимчасовий орган, що складався з представників глав держав-членів ЄС та їх урядів, Голови Європейської комісії, членів Європейського Парламенту та національних парламентів країн-членів ЄС, головним завданням якого було розробити проект Хартії основних прав ЄС відповідно до основоположних документів Європейського Союзу як документ, що міс-

тить фундаментальні права і свободи, процесуальні права, гарантовані Конвенцією про захист прав людини і основоположних свобод від 4.11.1950р., що відносилися б саме до громадян Європейського Союзу. Згідно положень установчих договорів (Договір про діяльність Європейського Союзу) громадянство Європейського Союзу поширюється на всіх осіб, що мають громадянство будь-якої держави-члена ЄС, тобто кожен громадянин держави-члена є громадянином Союзу. Розроблений проект Хартії основних прав ЄС був схвалений Європейською Радою, Європейським Парламентом, Радою ЄС та Європейською комісією у 2000р. В подальшому Хартія основних прав ЄС була включена до Лісабонського Договору (2007р.), що надало їй обов'язкової юридичної сили на території Європейського Союзу.

Текст Хартії основних прав ЄС складається з преамбули та сьоми розділів, в яких систематизовані основні права людини і громадянина ЄС щодо цінностей, на захист яких вони спрямовані, а саме гідність, свобода, рівність, солідарність. Обов'язки громадян Європейського Союзу викладені у Хартії як похідні від основних прав, головними з яких визначено повага та захист людської гідності інших осіб.

Право Європейського Союзу надає достатньо значні можливості індивідам для захисту своїх суб'єктивних прав, порушених державами-членами або інститутами ЄС. Європейський Суд Правосуддя в результаті розгляду та вирішення відповідних юридичних справ сформулював універсальний принцип відповідальності держав-членів за порушення права ЄС, який встановлює, що держава-член ЄС, визнана винною у порушенні права ЄС, зобов'язана відшкодувати збитки, завдані неімплементацією директив ЄС та порушенням інших зобов'язань, які випливають з установчих договорів ЄС (Справи C-6&9/90, Francovich and Bonifaci v. Italy (1991) ECR I-5357, (1993) 2 CMLR 66; Справа C-46/93, Brasserie du Pecheur SA v. Germany (1996) ECR I-1029, (1996) 1 CMLR 889, та Справа C-48/93, R. v. Sekretary of State for Transport, ex parte Factortame Ltd. (Factortaem III) (1996) ECR I-1029,(1996) 1 CMRL 889).[1]

При цьому Європейський Суд Правосуддя визначив, що відповідальність держав у вигляді відшкодування збитків може наступити не лише коли держава-член не вжила імплементаційних заходів з впровадження директиви до національного законодавства, але також коли національний законодавець своїми діями порушує положення Договору про ЄС. Відповідальність держави-члена ЄС настає за певних умов: норма права ЄС, яку порушено, повинна надавати індивідові певні суб'єктивні права (відносно неімплементованої директиви, вона повинна містити обсяг цих прав), порушення має бути достатньо серйозним, має бути прямий причинно-наслідковий зв'язок між

[1] http://www.curia.europa.eu

порушенням зобов'язання, яке покладено на державу-члена ЄС, та шкодою, яку зазнав індивід (позивач).

Європейський Союз є юридичною особою і тому здатен нести юридичну відповідальність, яку згідно Договору про діяльність ЄС (ст.340) поділяють на договірну та позадоговірну. Договірна відповідальність ЄС має місце за наявності контракту між ЄС та індивідом, умови якої визначені самим контактом або положеннями національного права. Такі спори, як правило, розглядаються національними судами відповідної юрисдикції. Позадоговірна відповідальність ЄС полягає у зобов'язанні ЄС згідно із загальними принципами права відшкодовувати збитки, завдані діями інститутів ЄС або їх службовцями при виконання ними своїх службових обов'язків, якщо між неправомірними діями чи бездіяльністю інституту або службовця ЄС та шкодою позивача має місце причинно-наслідковий зв'язок.

Тим самим, в Європейському Союзі для забезпечення реальності основних прав і свобод громадян сформована необхідна система відповідних гарантій, до якої відносяться матеріальні гарантії як можливості осіб на відшкодування завданої шкоди при порушенні їх прав; процесуальні гарантії, що реалізуються при здійсненні правосуддя та процедурі судового перегляду актів інститутів Європейського Союзу; а також інституційні гарантії, що визначаються правовою регламентацією функціонування органів, діяльність яких спрямована на охорону та захист порушених прав громадян ЄС.

Навчально-наукове видання

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ БОРЬБЫ С ТЕРРОРИЗМОМ

Матеріали міжнародної науково-практичної конференції
Луцьк, 22 квітня 2012 р.

Голова редакційної колегії: *В.А.Ліпкан*
Відповідальний за випуск: *О.С.Ліпкан*
Художній редактор *О.Г. Новіков*
Редактор *О. О. Машкова*
Комп'ютерне верстання *Д. Лепешин*

Підписано до друку 24.08.2012 р. Формат 60х84/16. Папір офсетний.
Гарнітура Times New Roman. Друк офсетний. Умов.друк.арк. 5,35
Наклад 300 прим. Зам. № 12-179

Видавець ФОП Ліпкан Олена Сергіївна
03058, Київ, вул. М.Донця, 23, б, кв. 33
Тел. +38.098.00.88.777 , факс: +38 044 4040 483
E-mail: **book@market-ua.com**., сайт: **www.book.market-ua.com.**
Свідоцтво суб'єкта видавничої справи ДК № 3535 від 27.07.09.

Виготівник ТОВ «Дорадо-Друк»
09000, м.Сквира, вул. Щорса, 7
www.doradoalliaNce.com
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру ДК № 2600 від 01.09.2006 р.