

24. Про затвердження Порядку подання фінансової звітності [Текст]: Постанова Кабінету Міністрів України від 28.02.2000 № 419 // Офіц. вісн. України, 2000 р., № 9, Ст. 344.

25. Про Концепцію реформування місцевого самоврядування та територіальної організації влади в Україні: Проект Указу Президента України [Електронний ресурс]. – Режим доступу: <http://minregion.gov.ua/attachments/content-attachments/995/Konceptcia.pdf>

26. Про місцеве самоврядування в Україні [Текст]: Закон України від 21.05.1997 № 280/97-ВР // Відом. Верхов. Ради України, 1997, № 24, Ст. 170.

27. Про місцеві державні адміністрації [Текст]: Закон України від 09.04.1999 № 586-XIV // Відом. Верхов. Ради України, 1999 р., № 20, Ст. 190.

28. Ткачук А. Хто такий префект? І навіщо він потрібен Україні? – 2007 // [Електронний ресурс]. – Режим доступу: <http://www.spa.ukma.kiev.ua/konst/article.php/2007112313120650>

29. Чуманова В. В. Обеспечение эффективности механизма государственного контроля и надзора в системе местного самоуправления [Текст]: автореф. дисс. ... канд. юрид. наук. / В. В. Чуманова. – Челябинск, 2009. – 24 с.

УДК 343.3/7

М.П. Стрельбицький
С.Л. Саржан

СОЦІАЛЬНІ ПЕРЕДУМОВИ (ЮРИДИЧНІ ФАКТИ) ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ ТА КІБЕРЗЛОЧИНІВ

У статті розкривається суть понять "тероризм", "інформаційний тероризм", "кібертероризм".

Ключові слова: *тероризм, інформаційний тероризм, кібертероризм, протидія інформаційному тероризму.*

В статті розкривається сутність понять "тероризм", "інформаційний тероризм", "кібертероризм".

Ключевые слова: *тероризм, информационный терроризм, кибертероризм, противодействие информационному терроризму.*

In the article essence of concepts opens up "terrorism", "informative terrorism".

Keywords: *terrorism, informative terrorism, counteraction informative terrorism.*

Постановка проблеми. Відбувається формування єдиного світового інформаційного простору. Таким чином здійснюється нав'язування малою групою людей певної лінії поведінки владі і суспільству, що вже тепер починає відчутно проявлятися на політичному полі України. Суспільство виявилось не готовим до протидії цьому явищу - позначилися об'єктивні і суб'єктивні фактори. Дослідженню їх ми присвячуємо ця статтю.

Аналіз останніх досліджень і публікацій. Чим сучаснішим стає інформаційне суспільство, тим більше значення в ньому приділяється інформаційній революції. Використовуючи віртуальний простір, нова інформація миттєво переводиться у сферу політичної дії. Використовувати інформацію для найефективніших способів її застосування на практиці – це і є політичне управління в інформаційному суспільстві. Доступ до нової інформації стає важливим ресурсом політичної влади, і цей ресурс вона може використати надалі за своїм розсудом, не виключаючи різних інформаційних маніпуляцій у своїх інтересах [1, с. 26-27].

На Заході інформаційний тероризм часто ідентифікують із *кібертероризмом* хоча, звичайно ж, вони дві частини одного явища. Інформаційний тероризм передбачає цілеспрямовані маніпуляції з інформацією або її підтасування, а в деяких випадках і подача свідомо неправдивих фактів, у результаті якої відбувається залякування населення, поширюється паніка, настрої параноїдальних думок.

Інформаційний тероризм припускає основною своєю метою саме вплив шляхом створення необґрунтованих страхів, занурення в стан жаху. На відміну від цього, кіберзлочини вчиняються з використанням нових технологій, наприклад, пограбування банку через мережу або злом торговельних Інтернет-площадок, що не є інформаційним тероризмом. Ці дії націлені тільки на одержання матеріальної вигоди. За рідкісним винятком у них немає ні ідеологічного піддрунтя, ні прагнення залякати когось. Інколи хакери зламують сервера або публікують секретну інформацію, як Джуліан Ассандж, прямо не пов'язуючи цю діяльність із грошима й мотивуючи її тими чи іншими причинами, наприклад, боротьбою із глобалізацією тощо.

Статистика свідчить про постійне збільшення кількості таких терактів. Наприклад, у 2008 році співробітники Державної служби спеціального зв'язку захисту інформації України виявили і припинили більше двох мільйонів атак на комп'ютерні мережі державних органів України. У жовтні 2007 року була здійснена значна в історії нашої держави атака на сайт Президента України з метою блокування роботи президентського ресурсу. У США кібератаки за шкідливістю наслідків прирівнюють до атак із застосуванням зброї масового знищення. Співробітники Федеральної служби безпеки Російської Федерації лише за 2010 рік знешкодили більше 1 млн. 200 тис. хакерських атак, більше 280 тис. із яких були спрямовані на сайт Президента РФ. За прогнозами спецслужб, злочини саме цієї категорії будуть складати левову частину проблем у найближчому май-

¹ Авдеев Ю.А. Терроризм как социально - политическое явление / Ю. Авдеев // Современный терроризм: состояние и перспективы. Под ред. Е.И. Степанова. – М.: Эдиториал УРСС, 2000.

бутньому. Націлені вони будуть, у першу чергу, на світову економіку. Спектр характеру терористичних дій та географія розгашування злочинців досить різноманітні, тепер не обмежені лише розвиненими країнами і досить поширені.

Фахівці виділяють такі види інформаційних впливів у сучасних умовах: інформаційна війна, інформаційна експансія, інформаційний тероризм.

До факторів, що впливають на формування загроз інформаційній безпеці України відносяться: слабка інтегрованість у світове інформаційне поле; недостатня фаховість та активність її інформаційних служб, широке використання ЗМІ окремими політичними силами, які можуть залежати від організованої злочинності, мафіозних структур; формування неправдивого уявлення про Україну у світі засобами масової інформації інших, насамперед недружніх держав, які відстоюють свої власні інтереси; неможливість повноцінного протистояння інформаційно-пропагандистським та терористичним актам інших держав унаслідок слабкої матеріально-технічної бази й недостатнього фінансового забезпечення.

Інформаційний або ментальний тероризм, а саме маніпулювання людьми під впливом засобів масової інформації, інколи не лише не зустрічає належного опору, але й унаслідок тотального "промивання мізків" і зміни точки зору, ця частина терору часто зводиться в ранг державної політики зацікавленими силами і використовується радикальними правлячими або опозиційними елітами повсюдно. Досить часто політичні баталії виграються не лідерськими якостями і звичайно не пунктами передвиборних програм, а грамотно побудованим впливом в інформаційному полі. Подачею або замовчуванням деяких матеріалів, створенням правильних акцентів для зміни суспільної думки. Такі маніпуляції стали повсякденним явищем [4].

Науково-технічна революція, нові інформаційні технології, глобальні й інтеграційні процеси призвели до формування сучасного інформаційного середовища, у якому інформація є головним чинником управління сучасним світом й основним інструментом влади. Очевидність зростання впливу ЗМІ на динаміку соціальних і комунікаційних процесів усього світового співтовариства вказує на необхідність створення ефективною системи управління інформаційним середовищем і формування системи інформаційної безпеки як з боку держави, так і легітимних наддержавних інститутів, суспільства в цілому.

¹ Заманов Г. На перешкоді військовим злочинам / Г. Заманов // Персонал. – 2009. – № 1.

Оскільки ми широко вживаємо поняття "терор", "тероризм", "інформаційний тероризм" метою статті є уточнення цих понять. Ми не намагаємось здійснити аналіз семантичної структури цих понять, але вважаємо за доцільне розмежувати їх за аналогією деяких дослідників.

Виклад основного матеріалу. Слово "терор" у перекладі із латинської мови означає "страх", "жах". "Терор" - це насильство, застосовуване "сильним" проти "слабкого". Як правило, мається на увазі відкрите насильство, що спирається на міць державних інститутів. "Тероризм" слід розглядати як насильство "об'єктивно слабкого", спрямоване проти "сильного", маючи на увазі й таке визначення, що "в остаточному підсумку тероризм – це насамперед самозахисна реакція політичної, соціальної, релігійної, економічної і т. д. меншості проти тих або інших дій більшості. Рідше - це реакція більшості, яку пригнічують" [1, с. 209]. Явища ці різного порядку, але в обох випадках мета насильства - прагнення змінити інститути суспільства (або рішення якого-небудь інституту) за допомогою масштабної зміни картини світу в людей, які підтримують ці інститути [2, с. 132].

Відмінною рисою інформаційного тероризму від кримінального є примус представників влади, посадових осіб до певної дії актом насильства або загрозою його здійснення, що має на меті, зазвичай, широкий соціальний резонанс, дестабілізацію ситуації або падіння існуючого режиму, підлив впливу органів державного управління та самоврядування на суспільство, дезорганізацію їхньої діяльності. Це – одна із форм ведення політичної боротьби, яка включає в себе дві складові: змістовну (ідеологія та культура) і технічну (інформаційна інфраструктура).

На сьогодні не існує однозначного тлумачення поняття "інформаційний тероризм". Фахівцями він характеризується з найрізноманітніших позицій. Ми ж розглядаємо це поняття в широкому і вузькому розумінні в залежності від мети. В широкому розумінні – це маніпулювання суспільною свідомістю шляхом масованого поширення неправдивої і сфабрикованої інформації з метою створення напруженості у суспільстві, нестабільності, хаосу, спрямованих на реалізацію політичних чи економічних цілей в інтересах терористів. У вузькому розумінні – це кібератаки на інформаційні системи, що працюють в контурах управління державними і соціально важливими технологічними об'єктами і системами (атомними чи гідроелектростанціями, банками, хімічним виробництвом, авіацією та

¹ Ольшанський Д. Психологія тероризма / Д. Ольшанський. – СПб.: Питер, 2002. – 288 с.

² Петров К.Е. Структура концепта «тероризм» / К.Е. Петров // Поліс. – 2003. – № 4. – С. 4 – 8.

іншими видами транспорту тощо) з метою виведення їх із ладу, спричинення економічних, екологічних та інших катастроф.

Характерною рисою сучасного інформаційного тероризму є, насамперед, публічність, забезпечення якої покладається на традиційні мас-медіа (пресу, радіо, телебачення) і Інтернет-медіа. Технологічний прогрес і розвиток засобів масової комунікації вимагають переосмислення значення ролі ЗМІ в суспільстві, усвідомлення значимості характеру, форм і методів подачі інформації в управлінні суспільною свідомістю. Сучасний інформаційний тероризм; з настанням епохи інформаційного суспільства, перейшов у якісно нову стадію – ведення інформаційно – психологічних війн, створюючи інформаційний привид жаху й хаосу.

Інформаційний тероризм нині не тільки відповідає ері інформаційних технологій, а й прагне підкорити її собі. Терористичні організації провадять широку інвестиційну політику. Крім традиційного підпорядкування активів легальних компаній і поліпшення інфраструктури наявного нелегального бізнесу сфери інформаційних технологій, терористичні організації активно втручаються в інформаційний простір. Створюють медіа - імперії з власних інформаційних ресурсів (друковані видання, радіостанції, телеканали, Інтернет - медіа), знаходять агентів впливу в авторитетних світових інформаційних носіях, провадять ефективні інформаційні операції, розробляють і застосовують методи маніпулювання масовою свідомістю.

Розглядаючи теракт як вияв політичної активності й метод регуляції соціальних процесів, теоретики тероризму у своїй методології досягнення мети основне місце відводять засобам масової комунікації. Оперативність, масштабність, унікальна здатність впливати на суспільну свідомість властиві мас-медіа. Інформаційний потенціал терористичного акту величезний, і це прекрасно розуміють і суб'єкти терористичної діяльності, і ті, хто стоять за ними. Терористи апелюють до суспільства за допомогою мас-медіа, при цьому терористичний акт засобів масової комунікації творить свій власний віртуальний простір, визначальною характеристикою якого стає тривале існування, активне поширення й значне тиражування насильства. Ретрансляція насильства ЗМІ підсилює ефект самого насильства, тим самим викликаючи деструкцію суспільної свідомості.

Страх і непевність у завтрашньому дні людей і, як наслідок, психологічний ступор суспільної свідомості, найдієвіший із погляду дезорганізації, який проявляється слабкістю й бездіяльністю влади або підвищеною тривожністю, і посиленням напруженості в суспільстві, негативними емоціями, які повинні знайти вихід, і врешті бути спрямованими проти влади, - до цього прагнуть ідеологи тероризму. Терористичний акт створює інформаційний привид і жорстко змінює порядок денний, а ЗМІ пос-

тають як засіб інформаційно-пропагандистського забезпечення терористичної діяльності. Таким чином, не тільки задається інформаційний привід як ініціалізатор певних смислотворчих процесів в індивідуальній і масовій свідомості, а й реалізується можливість управління суспільною свідомістю як формування суб'єктів дії – великих соціальних груп, сконсолідованих навколо лідерів думок і готових до масових виступів, зокрема і до антисоціальних дій. При цьому люди можуть висувати різні вимоги, а їх дії, найчастіше, далекі від логіки подій і способів вирішення існуючих, а тим більше уявних проблем.

У постіндустріальному суспільстві засоби масової комунікації є провідним соціальним інститутом, що організує соціальну взаємодію в суспільстві й визначає основні комунікативні процеси, відіграє чільну роль в управлінні суспільством. Інформація стала головним, а не просто одним із ресурсів політики [1 с. 26]. Безсумнівно, мас-медіа можуть і повинні протистояти тероризму.

Сучасні психоінформаційні технології модифікування як індивідуальної, так і масової свідомості уможливають це. Інакше можливостями засобів масової комунікації продовжуватимуть користуватися терористи. Ідеться не про запровадження цензури, а це не означає, що необхідно повністю обмежити доступ терористів до ЗМІ, з ростом тероризму це прямо ніяк не пов'язане. Водночас, деякі дослідники тероризму зауважують [2], якщо політична свобода неконтрольована, це надає терористам повну свободу дій. Тому першим спонуканням, першою реакцією на теракт владних структур було й буде обмеження цих свобод. Кожна з гілок влади, кожен інститут, які визначають правила функціонування соціальної й політичної систем, намагатимуться обмежити ці свободи, вважаючи, що інші учасники ліберальнішими рішеннями можуть послабити політичну систему відразу зазначаючи, що будь-яке обмеження свобод починає, врешті, стримувати економічний розвиток [2, с. 192]. Проте все гучніше звучать твердження, що рішення проблем тероризму – це й "проблема самообмеження на всіх рівнях. Наприклад, самообмеження діяльності телевізійних каналів, пов'язане з показом насильства, висвітленням терактів тощо" [6. с. 193].

Існують твердження, що "навіть демократична держава не повинна допустити, щоб демократії було занадто багато" [3, с. 212]. Але "жорсткість репресивного контролю в цілому не є виходом зі сформованої ситуації, оскільки тільки підсилює ймовірність миттєвих терористичних від-

¹ Василенко И.А. Информационные ресурсы власти и формирования новой пост-классической картины политического мира XXI в. / И.А. Василенко // Вест. Моск. ун. – та. Сер. 12. Политические науки. – 2004. – № 2. – С. 12 – 14.

² Інформаційний тероризм [Електронний ресурс] / Режим доступу: [http:// mary - donnu. Livejournal.com./1238.html](http://mary-donnu.Livejournal.com./1238.html).

повідей" [5, с. 361]: по-перше, вони розглядатимуться суб'єктами терористичної діяльності як показник ефективності застосовуваних ними засобів і, відповідно, продукуватимуть терористичну активність; по-друге, ініціюватимуть поширення соціальної бази тероризму й збільшення кількості терористичних організацій; по-третє, сприятимуть інтернаціоналізації тероризму.

Терористична загроза нині стала одним із визначальних факторів внутрішньої політики держав, приводом і способом вирішення геополітичних завдань у зовнішній політиці основних політичних акторів - структуризаторів світового простору. Аналіз соціально-політичних, політико-правових процесів свідчить, що в Україні присутні основні теригенні фактори, що створюють політичні, економічні, соціальні й етнорелігійні передумови для виникнення й розвитку інформаційного тероризму. Комунікативний вплив на тероризм може чинити надзвичайний рівень корупції в державі (*зміна влади й перехід останніх в опозицію ще більше збільшує ризик*), живучість соціально-революційних традицій і постулатів (*"мітингова демократія", яка набула нині популярності як основний спосіб вирішення суперечливих питань*), а також висока концентрація озброєнь і потенційних об'єктів терору [1, с. 8].

Посилення *геополітичної* напруженості у світі й серединне розташування України в Європі, значимість українських транспортних коридорів для Європи, наявність АЕС, насамперед Чорнобильської (через стан об'єкта криття, характер забезпечення охорони).

На відміну від інформаційних війн аналогічні терористичні акти носять одноразовий характер і мають знищуючу силу. Частіше в таких випадках інформаційні терористи мають тільки одне на меті - досягти якомога швидше потрібної цілі. Інформаційний тероризм є особливим різновидом психологічного терору, який застосовує зловживання інформаційними системами, мережами та їх компонентами для здійснення терористичних дій. Цей вид тероризму здійснюється у сфері, що охоплює політичні, філософські, правові, естетичні, релігійні й інші погляди й ідеї, тобто в духовній сфері, там, де ведеться боротьба. Доступність інформаційних технологій значно підвищує його ризики, бо чим більш інформатизованим є суспільство, тим більше воно піддається впливам масово-психологічного терору. Інформаційний тероризм - це насамперед форма негативного впливу на особистість, суспільство і державу всіма видами інформації. Його ціль - ослаблення й розкитвання конституційного ладу. Він ведеться різноманітними силами і засобами - від агентури іноземних спецслужб до вітчизняних і закордонних ЗМІ.

¹ Антипенко В.Ф. Современный терроризм: монография / В.Ф. Антипенко. - К., 1998. - 201 с.

Більш помірне формулювання інформаційного тероризму дають деякі правознавці, наприклад, В.І.Смелянов, В.А.Кульба й ін. Вони стверджують, що різного роду погрози, дії щодо залякування окремих осіб і суспільства в цілому є злочинами з ознаками тероризування. Як підтвердження розвитку своїх поглядів вони приводять відмінні ознаки тероризування, серед яких відзначають створення в суспільстві атмосфери страху і погроз. Ближче до визначення інформаційного тероризму підійшли автори словника з кримінального права, які вважають, що тероризм узагалі, і духовний зокрема, являє собою діяльність, що виражається в залякуванні населення й органів влади з метою досягнення злочинних намірів.

Такий тероризм полягає також у спробах організації спеціальних медіа-кампаній, покликаних зруйнувати знаково-символьну інфраструктуру суспільства, створити в ньому атмосферу громадянської непокори, недовіри до дій та намірів влади й особливо - її силових структур, що мають захищати суспільний порядок. У мирний час прямими виконавцями акцій інформаційного тероризму є: іноземні спецслужби й організації; закордонні та значна частина українських ЗМІ; організації сектантів і церковників; різного роду місіонерські організації; окремі екстремістські елементи і групи. Яскравим представником такого тероризму в новітній історії України було "Біле братство". Сотні людей підпали під вплив сектантів-фанатиків. Такі дії навіть спричинили закриття шкіл на деякий час, люди боялися випускати дітей на вулиці. Мету терористів було досягнуто - у суспільстві панував страх [5].

Дестабілізація суспільства чи то у внутрішній політиці країни, між ворогуючими публічними особистостями, чи то у зовнішньополітичних стосунках завдяки інформаційному тероризму стає дедалі популярнішим. Адже вдалою інформацією можна знищити все, і зброя стане зайвою.

Інформаційним терористичним актам залежно від часу і місця їх проведення властиві цілий ряд характерних особливостей, які відрізняють їх від інших терористичних актів. Це, у першу чергу, мета, риси, суб'єкти, об'єкти, загрози, що визначають відповідні сили, засоби, методи його реалізації. Автори виділяють серед найбільш поширених із них такі.

Риси:

- висока латентність і конспірація замовників, джерел фінансування та виконавців;
- швидка ескалація, що забезпечує миттєве досягнення запланованої мети;
- представляють реальну загрозу владі, органам управління, викликають нестабільність у суспільстві;

- легко контролюються, що дає змогу оперативно вносити корективи ззовні;
- дешеві за вартістю, масштабні за охопленням і відчутні за наслідками;
- безпосередньо впливають на прийняття політичних та управлінських рішень;
- грукують населення навколо певних ідей та лідерів або проти них.

Суб'єкти:

- держави, юридичні та фізичні особи, які проводять агресивну інформаційну політику щодо України;
- іноземні спецслужби та організації;
- закордонні та окремі вітчизняні ЗМІ;
- релігійні фанатики (ваххабізм, ісламський фундаменталізм тощо), організації сектантів та церковників;
- різного роду місіонерські організації;
- окремі екстремістські організації та групи.

Об'єкти:

- суспільні відносини, на які посягають терористи;
- акти тероризму, що вчиняються проти безпеки та життєдіяльності держави, суспільства, прав і свобод окремих громадян;
- система державного управління та її органи (Адміністрація Президента України, Кабінет Міністрів, міністерства і відомства, органи місцевого самоврядування);
- лідери держав, партій, громадських рухів;
- інформаційні ресурси, бази даних, статзвітність;
- молодь, студенти, соціально незахищені прошарки населення, безробітні, чорнобильці, афганці, дрібні підприємці.

Засоби:

- поширення повідомлень через видання засобів масової інформації (ЗМК Інтернет, телебачення), що викликають паніку серед населення;
- не зафіксовані на матеріальних носіях погрози;
- хибні повідомлення про очікуваний дефолт країни, вибухи, які готуються, вбивства, отруєння тощо.

За злочини, що мають ознаки інформаційного тероризму, передбачені сьогодні законодавством України, покарання суттєво менші, ніж за скоєння "традиційних" терористичних актів, що ускладнює боротьбу з ними. На жаль, у нас відсутній правовий механізм віднесення інформації, розміщеної в Інтернеті, до терористичної чи екстремістської діяльності, і можливість винесення відповідного попередження на адресу провайдерів, операторів, зобов'язавши їх знищити такі матеріали із комп'ютерної мережі на вимогу користувача.

Окрім внесення відповідних змін до законодавства України, спрямованих на посилення кримінальної відповідальності за злочини в інформаційній сфері, необхідно підготувати комплексний план превентивних заходів протидії інформаційному тероризму, а також зі створення національного простору довіри. Настав час підготувати й прийняти Кодекс про національний інформаційний простір, який має сприяти забезпеченню національної безпеки в інформаційній сфері. Необхідно активізувати наукові дослідження й розробки з питань технологій підготовки та проведення інформаційних терористичних актів. Сформувати скоординовану контрпропагандистську політику. Запровадити на державному рівні систему підготовки кадрів у галузі інформаційної безпеки. Ці та інші заходи зможуть суттєво поліпшити стан інформаційної безпеки України та антитерористичну діяльність.