нення суми гривневого чи валютного вкладу громадян (клієнтів); відомостей про термін зберігання вкладу; суми, яка має бути сплачена вкладнику по закінченні договору банківського вкладу. Частина 3 статті 341 до чинників, які свідчать про порушення інформаційних прав громадян у банківській сфері, відносить інформацію про платіжні доручення, платіжні вимоги, вимоги-доручення та ін.; частина 4 цієї ж статті – інформацію про: умови відкриття і закриття рахунків; види послуг, що надаються банком; обов'язки сторін та відповідальність за їх невиконання; умови припинення договору.

Отже, є всі підстави стверджувати, що введення законодавцем згаданої глави доречне й потрібне для здійснення судового захисту інформаційних прав і свобод особи. Не маючи змоги в рамках цієї роботи провести аналіз статей глави 22 [6], лише констатуємо: така глава в Цивільному процесуальному кодексі України [6] існує.

Висновки роботи: здійснено порівняльний аналіз законодавчих можливостей ЦПК України та Російської Федерації в забезпеченні судового захисту прав і свобод людини і громадянина в інформаційній сфері.

Джерела

1. Доктрина інформаційної безпеки України. – http: // www.president.gov.ua/ dokuments/9570. html
2. Конституція України: Основний Закон: із змінами, внесеними згідно із Законом № 2222-IV від 8 груд. 2004 р. – Харків: ФОП Співак Т. К., 2009. – 48 с.
3. Постанова Пленуму Верховного Суду України № 1 від 27.02.2009 «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи». – http : // www.zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg= v_001700-09
4. Российская Федерация. Закон. Гражданский процессуальный кодекс Российской Федерации: Офиц. текст. – Екатеринбург: Издательский дом «Ажур», 2009. – 148 с.
5. Российская Федерация. Закон. Доктрина информационной безопасности Российской Федерации – www.rg.ru// oficial/doc./min_and_vedom/mir_berop/doctr.shtm
6. Цивільний процесуальний кодекс України: зі змін. та допов. станом на 15 груд. 2008 р.: Відповід. офіц. текстові. – К.: Вид. Паливода А. В., 2008. – 156 с.
7. Цивільний кодекс України: зі змін. та доп. станом на 15 січ. 2009 р.: Відповід. офіц. текстові. – К.: Вид. Паливода А. В., 2009. – 328 с.

Формування спільної політики ЄС у галузі безпеки й оборони в контексті боротьби з сучасним кібертероризмом

Станіслав СОКУР,
студент IV курсу Інституту міжнародних відносин
Київського національного університету
імені Тараса Шевченка

Завершення «холодної війни» та розвал СРСР ознаменували появу нової системи міжнародних відносин. Одним із фактичних результатів цього переходу міжнародних акторів на принципово інший рівень стосунків стала зміна характеру їхніх безпекових взаємодій. Так, у сучасних реаліях досить чітких ознак набувають процеси регіоналізації, за яких помітнішу роль відіграють регіональні структури безпеки.

Зазначені процеси притаманні і Європейському Союзу, котрий в епоху постбіполярності перейшов від переважно економічної інтеграційної моделі до якісно нової фази інтеграції – політичної. Закономірним розвитком цієї політичної складової стало «перетікання» інтеграції у військово-політичну сферу.

Сучасні тенденції вказують на те, що цей регіон у перспективі стане одним із основних центрів сили в світовій безпековій системі. Запровадження Спільної європейської політики в сфері безпеки й оборони (СЄПБО) має на меті зробити ЄС самодостатнім гравцем, незалежним від єдиної на сьогодні наддержави – Сполучених Штатів Америки.

Проблема прямо пов'язана з реалізацією зовнішньої політики України. Розширення ЄС на Схід зумовило появу його спільних кордонів із нашою дер-

жавою, що, в свою чергу, підвищило увагу до наукових підвалин європейського вектору української зовнішньої політики [3]. Проголосивши курс на європейську інтеграцію, наша держава не може ігнорувати ключових тенденцій, що наразі мають місце в європейській спільноті. Їх дослідження допоможе виробленню Україною ефективної тактики та стратегії задля реалізації стратегічної мети – членства в ЄС.

Термін «кібертероризм» означає дії з дезорганізації інформаційних систем (несанкціоноване втручання в комп'ютерні мережі, перепрограмування, порушення роботи серверів та ін.), що становлять небезпеку для життя людей, призводять до значних майнових збитків або інших суспільно небезпечних наслідків, якщо їх здійснено з метою порушення громадської безпеки, залякування населення або впливу на прийняття рішення органами влади, а також загрози здійснення зазначених дій [6].

У літературі найточнішим вважається трактування співробітника ФБР М. Політа, згідно з яким ідеться про «заздалегідь спланований мотивований напад на інформаційні, комп'ютерні системи, комп'ютерні програми та дані» [10]. Приблизно такої самої точки зору дотримується заступник керівника Інституту дослідження тероризму в Ессені (ФРН) К. Хіршман [8]. Американський дослідник Д. Деннінг визначає кібертероризм як комп'ютерні атаки, сплановані для завдавання максимальних втрат життєво важливим об'єктам інформаційної інфраструктури [9]. Спеціалісти Центру іноземних військових досліджень академії *Fort Livenword (CIF)* характеризують кібертероризм так – незаконне знищення цифрового майна з метою залякування людей [1].

Питаннями кібертероризму також займаються і російські вчені: С. Н. Гриняев, Д. Т. Малишенко, Е. В. Старостина, В. Л. Васильев та інші. Однак загальноприйнятого визначення наразі не існує. Але зрозуміло, що в теоретичному аспекті йдеться про інтеграцію таких понять, як «тероризм» та «комп'ютерний злочин». Для кібертероризму є характерним, по-перше, використання комп'ютера як інструмента злочину; по-друге, існування Інтернету як міжнародного інформаційного простору, в якому перебуває об'єкт злочину; по-третє, зловмисна атака з боку кримінальних індивідів чи їх угрупувань на такі специфічні об'єкти, як інформація, програми, комп'ютери, локальні та глобальні мережі.

Сьогоднішній тероризм є багатогранним і може стосуватися багатьох сфер життєдіяльності. Зрештою, однією з найважливіших є протидія саме кібертероризму.

Боротьба з тероризмом як напрям діяльності ЄС набула документального оформлення після терактів у США «чорного вівторка» 11 вересня 2001 року.

ЄС продемонстрував здатність до вироблення спільних позицій, прийнявши 12 вересня 2001 року декларацію, в якій беззастережно засуджував акцію, висловлював солідарність із США і готовність до всебічного співробітництва в боротьбі з тероризмом.

У 2003 році Рада Європи затвердила в Салоніках першу з серії щорічних доповідей про реалізацію програми ЄС із попередження конфліктів, які супроводжуються застосуванням сили. Програма доповнювала СЄПБО такими напрямами, як боротьба з тероризмом, запобігання поширенню зброї масового знищення, включаючи засоби її доставки.

Надзвичайно важливим став саміт у бельгійському замку Лакен 14–15 грудня 2001 року, де були визначені механізми прийняття рішень та застосування оперативних сил і засобів СЄПБО, розвитку військових можливостей ЄС, засоби збирання та обробки інформації. Ішлося про готовність країн Європейського Союзу взяти участь у миротворчих операціях із мандатом ООН для підтримання миру в Афганістані. Учасники саміту схвалили декларацію про оперативний потенціал СЄПБО.

У міжнародних відносинах тероризм становить гостру загрозу міжнародній безпеці, дестабілізує відносини між державами і групами держав та провокує міжнародні конфлікти. Тероризм виступає інструментом втручання у внутрішні справи держави, грубо порушує права людини, міжнародний правопорядок. Принципово нові загрози міжнародній стабільності виникли з розробкою, використанням і розповсюдженням інформаційної зброї, що уможливлює інформаційні війни та інформаційний тероризм.

Через високий рівень інформаційно-технічного розвитку Євросоюзу особливого значення в діяльності ЄС набула проблема забезпечення інформаційної безпеки. Спільна позиція країн–членів Європейського Союзу щодо змісту поняття «інформаційна безпека» була висловлена представником Швеції при обговоренні на 56-й сесії Генеральної Асамблеї ООН питань міжнародної інформаційної безпеки, згідно з якою інформаційна та мережева безпека означає: 1) захист особистої інформації про відправників і одержувачів; 2) унеможливлення несанкціонованої зміни інформації; 3) контроль доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації. Інформаційна безпека також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки [9]. Недостатній захист життєво важливих інформаційних ресурсів та інформаційних і телекомунікаційних систем може створити загрозу міжнародній безпеці.

Позиція з приводу інформаційної безпеки відзначається раціоналізмом, адже предметом безпеки називаються конкретні поняття різних видів інформації. Крім того простежується досить чітке розмежування їхніх особливостей.

Глобалізація сучасної економіки, її насиченість новітніми інформаційно-телекомунікаційними технологіями, інформатизація таких життєво важливих сфер діяльності суспільства, як зв'язок, енергетика, транспорт, системи зберігання газу та нафти, фінансова й банківська система, оборона й національна безпека, структури забезпечення стабільної роботи міністерств і відомств, перехід до методів електронного врядування, створюють умови для поширення кібертероризму [7]. Сучасні війни ведуться передусім в інформаційній сфері, яка випереджає і безперервно супроводжує так званий прямий контакт протиборчих сторін. Спецслужби ведуть війни безпосередньо в Інтернеті. Як повідомлялося, для боротьби з потенціальним супротивником в експортне мережеве обладнання США встановлюються чіпи з логічними вірусами, що можуть бути активізовані в потрібний момент. Для боротьби з певними людьми є комп'ютерні програми обнуління банківських рахунків і багато чого іншого. За даними аналітичних центрів США, розробки нової інформаційної зброї відбуваються у 120 країнах світу.

Велику занепокоєність експертів-аналітиків викликає той факт, що терористичні організації гнучкіші, аніж державні інституції щодо застосування технічних інновацій. Відповідно вони мають істотні переваги у проведенні добре координованих операцій. А високий ступінь організації й реалізації останніх резонансних терористичних актів, на думку деяких експертів, засвідчує: за злочинами стояли інтереси різних держав.

Терористи з цією метою використовують технічні засоби, які є у вільному продажу, й об'єкти інфраструктури країни перебування. Простежується також їхній зв'язок із великими потоками нелегальних, передусім кримінальних, грошей. На шостому засіданні Робочої групи із співробітництва правоохоронних

органів країн Центральної та Східної Європи з питань боротьби з комп'ютерною злочинністю (Монстер, 28–30 серпня 2000 р.) оприлюднили такі дані Інтерполу: прибутки комп'ютерних злочинців у світі посідають третє місце після прибутків наркодилерів і нелегальних постачальників зброї.

Кібертероризм є частиною такого явища, як інформаційний тероризм. У середині 1980-х років Беррі Коллін, співробітник американського Інституту безпеки та розвідки, запровадив термін «кібертероризм» для визначення терористичних дій у віртуальному просторі. Автор терміна зазначив: про реальний кібертероризм можна говорити не раніше, як у першому десятилітті XXI століття. Проте вже 1990-го було зафіксовано перші серйозні кібератаки. А згодом Пентагон наказав Агентству супутникових телекомунікацій розробити стратегію ведення кібервійни (*OPLAN* 3600), яка передбачає «безпрецедентне об'єднання комерційних і державних структур країни». До її розробки залучається і ФБР, оскільки ситуація вимагає рішучого об'єднання всіх зусиль для протидії можливим атакам через Інтернет. Уряди європейських країн також розпочали розробку своїх стратегій ведення інформаційної війни [2].

Головне в тактиці інформаційного тероризму – щоб терористичний акт мав небезпечні наслідки, був широко відомий населенню і викликав потужний резонанс у суспільстві. Вимоги терористів супроводжуються погрозами повторення акту без зазначення конкретного об'єкта. Таким чином, характерною особливістю кібертероризму є те, що, на відміну від кіберзлочинності, умови терориста широко висвітлюються в інформаційній мережі.

Європейці також вирішують питання про неправомірне використання інформаційних засобів. Злочини в сфері високих технологій у центрі уваги Ради Європи з 1980-х років. 1995-го було прийнято Рекомендації для боротьби проти кіберзлочинності, які закликають налагодити міжнародну співпрацю з зазначених питань. У 1997 році в рамках Ради Європи було утворено Комітет експертів зі злочинів у кіберпросторі. Комітет досліджував доцільність і можливості уніфікації та гармонізації законодавств держав–членів ЄС, зокрема, щодо кіберзлочинності. За результатами цієї роботи підготовлено проект Конвенції Ради Європи «Про кіберзлочинність», ухвалений 23 листопада 2001 року в Будапешті. Нині разом з європейськими державами до Конвенції приєдналися Канада, Японія, ЮАР та США [4].

23 листопада 2001 року Україна підписала разом з іншими країнами Європейську Конвенцію про кіберзлочинність. 7 вересня 2005-го Верховна Рада ратифікувала, а 25 вересня 2005-го Президент підписав закон про ратифікацію Конвенції про кіберзлочинність. Конвенція відкрита для підпису іншими державами світу та набула чинності 1 липня 2004 року, після ратифікації документа Литвою.

Конвенцію прийнято через занепокоєння країн тим, що комп'ютерні мережі й електронна інформація можуть використовуватися під час кримінальних правопорушень. А докази, пов'язані з такими правопорушеннями, можуть зберігатися й передаватися цими мережами. Крім комп'ютерного хакерства та вірусів, положення Конвенції забороняють (віртуальну) дитячу порнографію та вчинене за посередництва комп'ютерів шахрайство. Правоохоронні органи країн, котрі ратифікують Конвенцію, отримають нові повноваження у боротьбі зі згаданими видами правопорушень.

З метою організації протидії «комп'ютерному тероризму», зокрема поширенню через глобальні та національні мережі зв'язку ідеології тероризму, пропаганди насильства, війни й геноциду, Постановою Кабінету Міністрів від 14 грудня 2001 року розроблено з урахуванням рекомендацій Парламентської асамблеї Ради Європи заходи щодо боротьби з міжнародним тероризмом. Вони передбачали проекти законів «Про моніторинг телекомунікацій», «Про захист інформації в мережах передачі даних», «Про регулювання українського сегмента мережі Інтернет». Однак спроби силових структур (зокрема, СБУ) напрацювати проекти відповідного законодавства та провести ці законопроекти в Верховній Раді наштовхнулися через низку об'єктивних і суб'єктивних причин на опір тих народних депутатів, котрі вбачають у цьому законодавстві замах на невід'ємні свободи та права людини.

Положення Конвенції Ради Європи «Про кіберзлочинність» знайшли своє відображення в Законі «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» від 23.12.2004 року, відповідно до якого в розділі 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» викладені у новій редакції статті 361 («Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»), ст. 362 («Несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчиненні особою, яка має право доступу до неї»), ст. 363 («Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється») Кримінального кодексу та передбачена кримінальна відповідальність за статтями 361-1 («Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»), 361-2 («Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається на комп'ютерах, комп'ютерних мережах або на носіях такої інформації») та 363-1 («Перешкоджання роботі комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку») [5].

Отже, проблема загальносвітової протидії загрозам інформаційної безпеки поглиблюється у зв'язку з тим, що тероризм повністю перейшов у сферу міжнародних відносин. Відповідно, шляхи створення ефективних систем протидії також перебувають у компетенції міжнародного права.

Важливо розвивати національні антитерористичні законодавства й водночас гармонізувати законодавчі системи всіх членів світового співтовариства з урахуванням нових форм тероризму та нових умов.

На рубежі XX–XXI століть інформаційний тероризм виступає як один із найважливіших чинників міжнародних відносин. Сьогодні тероризм узято на озброєння радикально налаштованими ідеологами й політиками, а також деякими державами, котрі починають активно використовувати його для зміни картини світового устрою.

Джерела

1. *Гаврилов Б.* Реальная война в виртуальном мире // Труд. – 2005. – 1 сентября.
2. *Еляков А.* Компьютерный терроризм. / Мировая экономика и международные отношения. – 2008. – № 10. – С. 102–105.
3. *Копійка В. В.* Європейський Союз: Досвід розширення і Україна. – К.: Юрид. Думка, 2005. – 448 с.
4. *Кудрявцева Е. Ю.* Латинская Америка / Меркосур: трудности и ожидания современного этапа. – 2008. – № 3. – С. 56–59.
5. *Макаренко Є. А., Рижиков М. М., Ожеван М. А.* Міжнародні інформаційна безпека: сучасні виклики та загрози. – К.: Центр вільної преси, 2006. – 916 с.
6. *Носенко В.* Компьютерный терроризм. – Мировая экономика и международные отношения. – 2007. – № 3. – С. 29–36.
7. *Пузырёв Д.* Терроризм в современных международных отношениях / Мировая экономика и международные отношения. – 2008. – № 8. – С. 63–67.
8. *Хиршман К.* Меняющееся обличье терроризма / Международный терроризм и право. – М., 2004. – С. 562
9. *Denning D.* Cyber Terrorism. Testimony Before Before the Special Oversight Panel on Terrorism. Georgetown. – 2000. – P. 415.
10. *Politt M.* Cyber Terrorism. Flack of Fancy / Proceed of the 20th National Information Systems Security Conference. Washington October 1997. – P. 347.

«Уся Польща ближча до тебе!»

Юрій СОКАЛЬСЬКИЙ,
доктор політології

Супутниковий канал громадського (суспільного) телебачення Польщі *TV Polonia* («ТБ Полонія») розпочав трансляцію 31 березня 1993 року. Адресна аудиторія канала – переважно поляки, котрі мешкають за кордоном, а також іноземці[1].

Поважна місія

Він народився третім серед телеканалів Польщі (після *TVPI* і *TVP2*) на підставі Закону Республіки Польща «Про радіомовлення та телебачення» від 29 грудня 1992 року. В розділі 4-му «Громадське радіомовлення і телебачення» (стаття 26, пункт 2) законодавчий орган закріпив таке положення: «Громадське телебачення створюється товариством «Польське телебачення – Акціонерне товариство», заснованим з метою створення й поширення загальнодержавних каналів I, II і *TV Polonia*, а також регіональних телестанцій».

«ТБ Полонія» – невід'ємна частина громадського (суспільного) телебачення Польщі (*Telewizji Polskiej S. A.* – акціонерного товариства Державного казначейства), яке нині є досить розгалуженим і складається з дев'яти телеканалів: трьох загальнодержавних – *TVP1, TVP2, TVP INFO*, супутникового для закордону – *TV Polonia*, першого канала високої роздільності – *TVP HD*[2], а також

[1] Пробна трансляція канала відбулася 24 жовтня 1992 року.

[2] Перший канал у стандарті *HD (high definition)*. Старт *TVP HD* збігся з початком літніх Олімпійських ігор у Пекіні – 8 серпня 2008 року. Нині це загальнотематичний канал, який використовує програми інших каналів публічного телебачення, художні й документальні фільми, серіали, культурно-розважальні програми. Згідно з ліцензією пріоритетом канала є спорт (турніри, матчі тощо), на що відведено майже 25% часу трансляції. Канал працює в ефірі щодня з 08.00 до 24.00.