УДК 341: 343.34: 316.774

О. О. ГРИЦУН

Ольга Олександрівна Грицун, *здобувач Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка*

ПИТАННЯ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ

У XXI ст. інформаційно-комунікаційні технології та стрімкий розвиток технічного прогресу стали не лише каталізатором позитивних змін, розвитку електронної торгівлі, впровадження новітніх технологій у виробництво, медицину, освіту, науку та інші галузі, а й, на превеликий жаль, перетворились на засіб для досягнення терористичних цілей. Можливість здійснення терористичного акту з будь-якої точки земної кулі, ігноруючи державні кордони та заходи безпеки, мінімальні капіталовкладення та труднощі у виявлення джерела загрози уповноваженими органами сприяли появі однієї із найбільших загроз людства – інформаційного тероризму. Терористичні угруповання використовують мережу Інтернет як засіб та як простір для вчинення терористичних актів, а також як засіб комунікації, вербування послідовників, поширення відповідної літератури та залякування людей шляхом он-лайн трансляцій актів насилля. Важко спрогнозувати наслідки від терористичних дій у мережі Інтернет, вони можуть коштувати життя великої кількості людей, значних фінансових втрат та навіть втрати обороноздатності держав. Оскільки інформаційний тероризм має транснаціональний характер, а його наслідки можуть поширюватись на території одразу кількох держав, необхідно створити міжнародно-правові механізми протидії цьому явищу, а також розробити та реалізувати правові заходи забезпечення безпеки в інформаційному просторі.

Окремі аспекти проблеми правового регулювання інформаційного тероризму розглядались у працях В. О. Васеніна, В. Д. Недільніченко, М. Герке, А. В. Крутських, А. Д. Єлякова, Р. А. Шаряпова, Ш. Шольберга, М. Дюмонтьє та Дж. Бірда. Питання використання терористами засобів масової інформації досліджувались О. Л. Вартановою, методологічні проблеми протидії інформаційному тероризму висвітлено в роботах В. В. Ященко та А. А. Сальникова. Проте малодослідженим залишилось питання міжнародно-правового регулювання інформаційного тероризму і комплексного аналізу нормативних документів міжнародних організацій та існуючих теоретичних концепцій, присвячених цій проблемі.

Мета статті – дослідити питання розвитку міжнародно-правового регулювання співробітництва держав у боротьбі з інформаційним тероризмом, проблеми, а також ступінь розробки понятійного апарату у цій сфері.

Цілі статті: аналіз нормативних документів міжнародних та регіональних організацій у сфері регулювання проблеми використання мережі Інтернет в терористичних цілях та існуючих теоретичних підходів до розуміння поняття інформаційного тероризму.

Широкомасштабне використання інформаційно-комунікаційних технологій та підвищення рівня залежності держав, а саме їх критично-важливих інфраструктур, від новітніх технологій спровокували появу нового явища у сфері міжнародної інформаційної безпеки – інформаційного тероризму. На даний момент загальноприйнятого визначення цього поняття не існує, в теорії міжнародного права та в міжнародно-правових документах зустрічаються різні визначення: «кібертероризм», «інформаційний тероризм» та «комп'ютерний тероризм». Спільними для усіх цих понять є характерні риси, притаманні цьому поняттю, а саме: «використання комп'ютера як інструменту злочину; наявність Інтернету як міжнародного інформаційного простору, в якому розміщується об'єкт злочину; та навмисна атака з боку злочинців чи злочинних груп на комп'ютери, інформацію, програми, локальні та глобальні мережі, що може спричинити загибель людей, порушення суспільного порядку, екологічні чи техногенні катастрофи»[1].

Досліджуючи питання інформаційного тероризму, науковці акцентують увагу на подвійній ролі інформаційно-комунікаційних технологій у здійсненні актів інформаційного тероризму. З одного боку, інформаційно-комунікаційні системи та технології можуть розглядатись як об'єкт нападу, а з іншого – як зброя в руках терористів[2]. Достатньо важко провести чітку межу між інформаційним тероризмом та використанням інформаційних технологій у воєнних чи кримінальних цілях. Тому основними відмінностями інформаційного тероризму від інших протиправних діянь в інформаційній сфері є його цілі, що притаманні і терористичним актам в загальному їх розумінні. До цих цілей ми можемо віднести: «залякування населення, створення атмосфери страху та паніки, створення атмосфери загрози повторення теракту, виклик великого суспільного резонансу, наслідки, небезпечні для життя та здоров'я людей, поширення інформації про теракт для широкої аудиторії».

Характерними рисами терористичних актів в інформаційній сфері є: «прихований характер підготовки та реалізації таких діянь – відсутність проявів та слідів проникнення; масштабність атак – нанесення удару по великій кількості об'єктів; синхронність атак – вони можуть бути здійснені одночасно по багатьом об'єк-

там; віддаленість – джерело атаки може знаходитись за межами країни, в якій здійснюється напад; інтернаціональність – шкода може поширюватись на території кількох держав»[3].

В. О. Васенін акцентує увагу на тому, що шкода від терористичних дій в інформаційному просторі насамперед пов'язана з: людськими жертвами чи матеріальними втратами, викликаними деструктивним використанням елементів мережевої інфраструктури; можливими втратами від несанкціонованого використання інформації з високим рівнем секретності чи мережевою інфраструктурою управління в життєво важливих сферах діяльності держави; витратами на відновлення керованості пошкодженою чи знищеною мережею; моральною шкодою власника мережевої інфраструктури та власного інформаційного ресурсу; іншими втратами від несанкціонованого доступу до інформації з високим рівнем секретності[4].

Він вводить поняття «антитерористична інформаційна безпека», що означає «сукупність механізмів, інструментальних засобів, методів та заходів, що дозволяють попередити, виявити, а в разі виявлення – оперативно зреагувати на дії, що здатні призвести до порушення інфраструктури мережі шляхом поломки системи управління нею чи її окремими елементами або до несанкціонованого доступу до інформації, що охороняється законом та має високий рівень секретності, порушення її цілісності, керованості та захищеності». Тобто, врегулювання цього питання повинно здійснюватись як на законодавчому, так і на програмно-технічному та операційному рівнях.

Досліджуючи інформаційний тероризм як один із напрямів тероризму, теоретики зробили спробу розглянути його через призму впливу на критично важливі об'єкти інфраструктури за допомогою їх комп'ютерної системи управління. При цьому до критично важливих об'єктів інфраструктури віднесено «такі об'єкти, які в разі часткової деградації чи повної втрати функціональності здатні впливати на стан національної безпеки держав чи її структурних елементів». До таких елементів належать управління енергоресурсами, транспортна система, обороноздатність та ряд інших[5].

Розглядаючи проблему інформаційного тероризму, варто зазначити, що терористичні угрупування використовують Інтернет не лише як спосіб проведення своїх атак, а й у якості елементу маніпулювання свідомістю та поведінкою людей за допомогою інформаційного впливу та з використанням глобальних комунікацій. Терористи спрямовують свої зусилля не тільки на нанесення матеріальної шкоди та загрозу життя людей, а й на інформаційно-психологічний шок великої кількості людей, з метою створення сприятливого середовища для досягнення своїх цілей[6].

Не можна оминути увагою і той факт, що терористи використовують глобальну мережу Інтернет і як засіб спілкування, підготовки до терористичних актів та вербування прибічників. Професор Дж. Бірд виокремлює п'ять основних напрямів діяльності терористів у цій сфері в мережі Інтернет: спілкування – за допомогою електронної пошти, блогів, чатів та цілих сайтів, присвячених діяльності терористичних угруповань; медіа-вплив – поширення екстремістських поглядів з метою вербування нових прибічників та здійснення масштабної пропаганди задля маніпулювання свідомістю та думкою громадськості; пошукова діяльність – пошук в мережі Інтернет карт місцевості, планів будівель, систем охорони, транспортних систем та іншої інформації, необхідної для здійснення атаки; приналежність – створення сайтів, що прямо чи опосередковано пропагують ідеї тероризму та екстремізму з використанням спеціальної символіки, графічних об'єктів та відповідного контенту; та альтернативна реальність – анонімність в мережі Інтернет допомагає людям жити паралельним життям, сповідуючи ідеї тероризму та залишатись непоміченими[7].

У рамках міжнародних організацій та форумів питання інформаційного тероризму почали підніматись з кінця 90-х років минулого століття.

У 2006 р. під час саміту Великої вісімки в Декларації саміту G8 щодо боротьби з тероризмом вперше в якості терористичної загрози було визнано «зловживання кіберпростором у терористичних цілях, включаючи підбурювання до здійснення терактів, зв'язок та планування терористичних актів, а також вербування на навчання терористів»[8]. У 2007 р. під час засідання Міністрів юстиції та внутрішніх справ G8 проблему використання Інтернету терористами було ще раз винесено на обговорення. При цьому всі учасники засідання зійшлись на думці про кримінальне переслідування терористичних груп за неправомірне використання Інтернету.

З цього часу проблема використання кіберпростору в терористичних цілях стала предметом обговорення в рамках міжнародних та регіональних організацій.

Глобальна контртерористична стратегія Організації Об'єднаних Націй була прийнята 8 вересня 2006 р. у вигляді резолюції та відповідного Плану дії. Вперше в рамках ООН питання боротьби з тероризмом в мережі Інтернет було висвітлено у другому пункті Плану дій «Заходи щодо попередження тероризму та боротьбу із ним». Держави-члени ООН взяли на себе зобов'язання здійснювати співробітництво з ООН з метою вивчення шляхів та засобів «координації зусиль на міжнародному та регіональному рівні з метою боротьби з тероризмом у всіх його формах та проявах в мережі Інтернет, а також використання мережі Інтернет в якості інструменту боротьби з поширенням тероризму, визнаючи той факт, що державам може знадобитись допомога у вирішенні цих питань»[9], дотримуючись при цьому принципів конфіденційності, поваги до прав і свобод людини й громадянина та норм міжнародного права.

Варто зазначити, що крім цього, Управлінням ООН з наркотиків та злочинності було оприлюднено документ під назвою «Використання Інтернету в терористичних цілях». Відповідно до резолюції Генеральної Асамблеї ООН 60/288, що відтворила вищезгадані положення Плану дій та підтвердила рішення держав щодо координації своїх зусиль з метою протистояння тероризму в мережі Інтернет, було створе-

но Робочу групу з питань протидії використання мережі Інтернет в терористичних цілях, що займалась розробкою цього документа. У доповіді Робочої групи висвітлюються питання: методів використання мережі Інтернет в терористичних цілях; використання мережі Інтернет з метою протидії терористичній діяльності; питання верховенства права; міжнародний контекст регулювання цього питання; досліджуються регіональні та субрегіональні документи з питань боротьби з тероризмом; норми типового законодавства; розслідування та збір оперативної інформації; інструментарій, який використовують терористи для здійснення атак у мережі Інтернет, питання криміналістичної експертизи; питання міжнародного співробітництва; судового переслідування; огляд національних підходів та співробітництво з приватним сектором[10].

Організація Північноатлантичного договору (далі – НАТО) також приділяє значну увагу питанням безпеки у кіберпросторі. Вперше це питання в рамках НАТО обговорювалось у листопаді 2002 р. під час Празького саміту. Лідери країн-членів НАТО виявили своє бажання посилювати свої можливості щодо протидії інформаційним атакам. У рамках Організації Північноатлантичного договору створено Управління з питань забезпечення кібероборони, Центр експертизи з питань кооперативної кібероборони (CCDCOE) у Таллінні, Агентство з питань комунікації та інформації НАТО, а також розпочато впровадження програми кіберзахисту NCIRC (NATO Computer Incident Response Capability). Крім цього, в Анкарі створено Центр передового досвіду НАТО у боротьбі з тероризмом, що також значну увагу приділяє питанням боротьби з інформаційним тероризмом. У травні 2014 р. експертами центру було опубліковано доповідь «Використання кіберпростору терористами», в якій висвітлювались питання розуміння поняття інформаційного тероризму, оцінки та реагування на кіберзагрози, використання терористами інформаційних технологій, а також питання спроможності новітніх технологій протистояти кібертерористам[11].

У 2008 р. в рамках Європейського Союзу було розпочато роботу над внесенням змін і доповнень до Рамкового рішення про боротьбу із тероризмом. У вступі до проекту змін та поправок було зазначено, що існуючі правові рамки поширюються на такі злочини, як публічні заклики до здійснення терористичних злочинів, найм для тероризму, підготовку кадрів для здійснення терористичних дій та багато інших, але не визнають в якості кримінальних дій поширення терористичних навиків через Інтернет[12]. Таким чином, Європейський Союз не просто намагається гармонізувати законодавство на всій його території із положеннями Конвенції Ради Європи про попередження тероризму, а й висловлює намір врегулювати питання загрози терористичних актів через мережу Інтернет.

Проблема інформаційного тероризму обговорювалась і в рамках інших міжнародних та регіональних організацій. Так, у 2007 р. Організацією Економічного Співробітництва та Розвитку було опубліковано Доповідь щодо законодавчих рішень стосовно «кібертероризму» в рамках внутрішнього законодавства окремих країн. Організацією Азіатсько-тихоокеанського співробітництва було оприлюднено Заяву про боротьбу із тероризмом та сприяння зростанню, в якій питання інформаційної безпеки були винесені окремим розділом.

У 2004 р. Рада Міністрів Організації з безпеки та співробітництва в Європі прийняла рішення № 3/04 «Боротьба з використанням Інтернету в терористичних цілях», в якому йшлося про масштабність використання мережі Інтернет терористичними організаціями для організації терористичних актів, збору фінансів, вербування прихильників та пропаганди і підбурювання до вчинення терористичних дій. Відповідно до цього документа держави зобов'язались обмінюватись інформацією про використання Інтернету в терористичних цілях та про стратегії боротьби з цим явищем[13].

Також у 2004 р. було проведено спеціальну нараду ОБСЄ про взаємозв'язок між расистською, ксенофобською й антисемітською пропагандою в Інтернеті та злочинами, здійсненими на підставі ненависті. У 2005 р. відбувся експертний семінар ОБСЄ щодо боротьби з використанням Інтернету у терористичних цілях, а у 2006 р. – спільний експертний семінар ОБСЄ та Ради Європи щодо попередження тероризму.

Крім цього, у 2006 р. Радою Міністрів ОБСЄ було прийнято більш розширене рішення № 7/06 «Протидія використанню Інтернету в терористичних цілях». Цей документ постановив активізувати діяльність ОБСЄ та держав-учасників у сфері протидії використанню Інтернету в терористичних цілях, закликав їх активізувати зусилля для захисту критично важливих інформаційних інфраструктур, наголосив на необхідності приєднання до Конвенцій Ради Європи про кіберзлочинність та про попередження тероризму. Також у документі державам-учасницям було запропоновано розширити моніторинг веб-сайтів, що мають терористичне чи екстремістське спрямування та активізувати обмін інформацією з цього питання, залучати інститути громадянського суспільства до протидії використанню Інтернету в терористичних цілях та здійснювати обмін інформацією про можливі загрози у зв'язку з таким використанням через Контртерористичну мережу ОБСЄ[14].

У рамках Ради Європи 23 листопада 2001 р. було прийнято Конвенцію Ради Європи про кіберзлочинність, що врегулювала лише питання відповідальності за кримінальні злочини, пов'язані з комп'ютерними системами і даними, але залишила поза предметом свого регулювання питання відповідальності за інформаційний тероризм.

На сьогодні єдиним документом, що регулює питання співробітництва держав у боротьбі з інформаційним тероризмом, є Угода між урядами держав-членів Шанхайської організації співробітництва про співробітництво у сфері забезпечення міжнародної інформаційної безпеки від 16 червня 2009 року. Ця угода визначає шість основних загроз у сфері міжнародної інформаційної безпеки, однією з яких є інформаційний тероризм, а також напрями співробітництва держав у сфері забезпечення міжнародної інформаційної безпеки. До таких напрямів належать: «протидія загрозам використання інформаційно-комунікаційних технологій в терорис-

тичних цілях; створення системи моніторингу та спільного реагування на загрози в інформаційному середовищі; обмін інформацією про законодавчу базу у цій сфері; вдосконалення міжнародно-правової бази та практичних механізмів співробітництва держав; взаємодія в рамках міжнародних організацій та форумів; обмін досвідом, підготовка спеціалістів у сфері забезпечення міжнародної інформаційної безпеки»[15] та інші.

У Додатку 1 до Угоди ШОС міститься визначення інформаційного тероризму, під яким автори документу розуміють «використання інформаційних ресурсів та (чи) вплив на них в інформаційному просторі в терористичних цілях». Додаток 2 до Угоди деталізує це поняття через визначення його джерел та основних ознак. Так, джерелом інформаційного тероризму відповідно до положень Додатку 2 є «терористичні організації та особи, причетні до терористичної діяльності, що здійснюють протиправні дії шляхом чи по відношенню до інформаційних ресурсів», а ознаками: «використання інформаційних мереж терористичними організаціями для здійснення терористичної діяльності та залучення нових прибічників; деструктивний вплив на інформаційні ресурси, що здатен спричинити порушення суспільного порядку; контроль чи блокування каналів передачі масової інформації; використання мережі Інтернет чи інших інформаційних мереж для пропаганди тероризму, створення атмосфери страху та паніки в суспільстві, а також інший негативний вплив на інформаційні ресурси». Таким чином, Угода держав-членів ШОС закріпила визначення «інформаційного тероризму» та визначила його в якості загрози на нормативному рівні.

Досліджуючи питання інформаційного тероризму, доцільно згадати два концептуальних підходи до регулювання цього питання, що закріплені в концепції Конвенції про забезпечення міжнародної інформаційної безпеки, представленої у Лондоні у 2011 р. на Конференції з питань кіберпростору, та у проекті «Загального договору з питань кібербезпеки та кіберзлочинності», так званому Договорі Шольберга.

Не зважаючи на те, що визначення інформаційного тероризму, запропоноване у концепції Конвенції про забезпечення міжнародної інформаційної безпеки, повністю відтворює визначення, закріплене в Угоді держав-членів ШОС, автори концепції використовують термін «тероризм в інформаційному просторі», а основною загрозою міжнародному миру та безпеці у цій сфері вважають: «використання міжнародного інформаційного простору державними та недержавними структурами, організаціями, групами та окремими особами в терористичних, екстремістських чи інших злочинних цілях[16]». Розділ 3 вищезгаданої концепції визначає заходи протидії використання інформаційного простору в терористичних цілях. До таких заходів належать наступні: «напрацювання єдиних підходів до припинення функціонування Інтернет-ресурсів терористичного характеру; застосування спільних дій; встановлення та розширення обміну інформацією про загрози здійснення комп'ютерних атак, факти, методи та засоби використання мережі Інтернет в терористичних цілях, а також обмін досвідом у сфері моніторингу інформаційних ресурсів мережі Інтернет, проведення криміналістичних комп'ютерних експертиз і правового регулювання діяльності щодо протидії використання інформаційного простору в терористичних цілях; законодавчі та інші необхідні заходи для проведення слідчих, пошукових та інших процесуальних заходів щодо протидії проведення терористичних дій в інформаційному просторі та покарання винних, а також необхідні заходи для гарантування законного доступу на територію держав-учасників до окремих частин інформаційно-комунікаційної інфраструктури, за умови, що є законні підстави вважати, що вони використовуються для терористичної діяльності». Таким чином, вищезгадана концепція ширше підходить до розуміння інформаційного тероризму, але досі не вдалось досягнути консенсусу та прийняти цей нормативно-правовий акт.

У рамках дослідження питання міжнародно-правового регулювання інформаційного тероризму варто згадати проект «Загального договору з питань кібербезпеки та кіберзлочинності», запропонований професором Штайном Шольбергом, який займав посаду голови Групи Експертів високого рівня з питань кібербезпеки, засновану у 2007 р. задля вивчення можливостей створення загального документа з питань кіберзлочинності в рамках Організації Об'єднаних Націй, та професором Соланж Гернуті-Елі.

Автори цього проекту розглядають інформаційний тероризм як один із видів кібератак. Тому стаття, присвячена врегулюванню цього питання, має назву «запобігання тероризму та іншим серйозним кібератакам»[17]. Відповідно до положень проекту договору до таких дій належать: публічне підбурювання до вчинення терористичного злочину, пошук та схилення людей для вчинення терористичного акту та проведення терористичних навчань. Також договором передбачено кримінальну відповідальність за такі дії згідно з внутрішнім законодавством держав-членів. Під публічним підбурюванням до вчинення терористичного злочину розуміється поширення чи іншим чином доведена до відома громадськості інформація, націлена на підбурювання до вчинення терористичного злочину, незалежно від того, є така поведінка прямою пропагандою терористичних злочинів чи ні. Важливим є й таке: вона створює небезпеку, що такі злочини може бути вчинено. Що ж стосується схилення людей до вчинення терористичного злочину, то під цим поняттям розуміють вимогу від іншої особи вчинити чи взяти участь у вчиненні терористичного акту, або вимогу вступити до групи осіб з метою сприяння вчинення ними терористичних злочинів. Під терористичними навчаннями розуміють надання інструкцій чи іншої інформації щодо створення або використання вибухових речовин, вогнепальної зброї, інших видів зброї, шкідливих або небезпечних речовин, інших конкретних методів чи засобів, необхідних для вчинення чи сприяння терористичному акту, або ж використання з цією метою відповідних навичок.

До інших серйозних кібератак автори відносять знищення, пошкодження або унеможливлення використання критично важливих інформаційних інфраструктур, що призводить до порушення основ національної безпеки, цивільної оборони, державного управління, здоров'я людей чи безпеки надання банківських і фінансових послуг.

Проект цього договору підготовлений авторами з власної ініціативи, тому не може розглядатись у рамках ініціатив ООН, присвячених питанням міжнародної координації боротьби із інформаційним тероризмом та забезпечення безпеки кіберпростору.

Дослідивши нормативні документи міжнародних та регіональних організацій у сфері регулювання проблеми інформаційного тероризму та існуючі теоретичні й концептуальні підходи до розуміння цього поняття, доходимо висновку, що на даний момент ще не сформовано єдиної термінологічної бази та уніфікованого підходу до розуміння питання інформаційного тероризму. Жодна держава світу не спроможна протистояти загрозі інформаційного тероризму самотужки, враховуючи масштабність його дії та транснаціональний характер. Тому необхідність нормативно-правового врегулювання цієї проблеми на міжнародному рівні, розробка єдиного підходу до розуміння та протидії інформаційному тероризму, а також опрацювання механізмів міжнародного співробітництва й обміну досвідом є ключовими моментами співробітництва усіх держав світу та потребує міжнародної координації зусиль.

---

[1] *Еляков А. Д.* Компьютерный терроризм / А. Д. Еляков // Мировая экономика и международные отношения. – 2008. – № 10. – С. 102.

[2] *Сальников А. А.* Методологические проблемы противодействия кибертерроризму / А. А. Сальников, В. В. Ященко // Научные и методологические проблемы информационной безопасности (сб. статей) ; под ред. В. П. Шерстюка. – М. : МЦНМО, 2004. – С. 98.

[3] *Недильниченко В. Д.* Информационные угрозы в контексте противодействия терроризму / В. Д. Недильниченко // Материалы третьей международной научной конференции по проблемам безопасности и противодействия терроризму (г. Москва, МГУ, 25–27 октября 2007 г.). – М. : МЦНМО, 2008. – С. 288.

[4] *Васенин В. А.* Информационная безопасность и компьютерный терроризм / В. А. Васенин // Научные и методологические проблемы информационной безопасности (сб. статей) ; под ред. В. П. Шерстюка. – М. : МЦНМО, 2004. – С. 71.

[5] *Васенин В. А.* Научные проблемы противодействия кибертерроризму / В. А. Васенин // Материалы международной научной конференции по проблемам безопасности и противодействия терроризму (г. Москва, МГУ, 2–3 ноября 2005 г.). – М. : МЦНМО, 2006. – С. 36.

[6] *Вартанова Е. Л.* Терроризм и СМИ: симбиоз или противостояние? К вопросу о природе современных взаимоотношений / Е. Л. Вартанова // Материалы третьей международной научной конференции по проблемам безопасности и противодействия терроризму (г. Москва, МГУ, 25–27 октября 2007 г.). – М. : МЦНМО, 2008. – С. 102.

[7] *Bird J.* Terrorist Use of the Internet / J. Bird // Материалы второй международной научной конференции по проблемам безопасности и противодействия терроризму (г. Москва, МГУ, 25–26 октября 2006 г.). – М. : МЦНМО, 2006. – С. 509.

[8] G8 Summit Declaration on Counter-Terrorism : [Електронний ресурс]. – Режим доступу : http://www.mofa.go.jp/policy/economy/summit/2006/terro.html

[9] The United Nations Global Counter-Terrorism Strategy : [Електронний ресурс]. – Режим доступу : http://www.un.org/en/terrorism/strategy-counter-terrorism.shtml

[10] The Use of the Internet for Terrorist Purposes / United Nations Office on Drugs and Crime : [Електронний ресурс]. – Режим доступу: http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

[11] Terrorist Use of Cyberspace Course Report : [Електронний ресурс]. – Режим доступу : http://www.coedat.nato.int/publication/course_reports/11-Terrorist_Use_of_Cyberspace.pdf

[12] *Герке М.* Понимание киберпреступности: Руководство для развивающихся стран / М. Герке : [Електронний ресурс]. – Режим доступу : www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[13] Решение Совета Министров ОБСЕ о борьбе с использованием Интернета в террористических целях № 3/04 : [Електронний ресурс]. – Режим доступу : http://www.osce.org/ru/mc/41817?download=true

[14] Решение Совета Министров ОБСЕ о борьбе с использованием Интернета в террористических целях № 7/06 : [Електронний ресурс]. – Режим доступу: http://www.osce.org/ru/mc/36573?download=true

[15] Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16 червня 2009 р. : [Електронний ресурс]. – Режим доступу: http://base.spinform.ru/show_doc.fwx?rgn=28340

[16] Проект Конвенции об обеспечении международной информационной безопасности (концепция) : [Електронний ресурс]. – Режим доступу : http://www.scrf.gov.ru/documents/6/112.html

[17] A Global Treaty on Cybersecurity and Cybercrime : [Електронний ресурс]. – Режим доступу : http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf

Резюме

Грицун О. О. **Питання міжнародно-правового регулювання інформаційного тероризму.**

У статті надається аналіз діяльності та відповідних документів міжнародних і регіональних організацій, присвячених проблематиці інформаційного тероризму, а також огляд теоретичних концепцій щодо розуміння цього поняття. Це дає змогу визначити основні підходи до регламентації питання інформаційного тероризму на міжнародному рівні та в розрізі діяльності окремих регіональних організацій.

Ключові слова: інформаційний тероризм, інформаційна безпека, терористичні злочини, мережа Інтернет, інформаційний простір.

Резюме

Грицун О. А. **Вопросы международно-правового регулирования информационного терроризма.**

В статье анализируется деятельность и соответствующие документы международных и региональных организаций, посвященные проблематике информационного терроризма, а также раскрываются теоретические концепции понимания этого

вопроса. Это позволяет определить основные подходы к регламентации проблемы информационного терроризма на международном уровне и в разрезе деятельности отдельных региональных организаций.

Ключевые слова: информационный терроризм, информационная безопасность, террористические преступления, сеть Интернет, информационное пространство.

Summary

Grytsun O. **The Issues of International Legal Regulation of Cyber Terrorism.**

This article analyses activity and relevant documents of international and regional organizations devoted to the problem of cyber terrorism, and also this article gives a short review of theoretical concepts in understanding this notion, which allows us to determine the main approaches to the regulation of cyber terrorism at both, the international level and in terms of certain regional organizations.

Key words: cyber terrorism, cyber security, terrorist offences, Internet, cyberspace.

УДК 347.6

О. В. МЕЛЬНИЧЕНКО

Оксана Вікторівна Мельниченко, *здобувач Київського університету права НАН України*

МІЖНАРОДНІ ДОГОВОРИ В СИСТЕМІ СІМЕЙНОГО ЗАКОНОДАВСТВА УКРАЇНИ ТА ЄС

Загальновідомо, що наразі наша держава намагається зблизити свої стосунки з європейськими країнами у різних сферах суспільних відносин, насамперед приватних. Зокрема, позитивних запозичень зазнала сфера правового регулювання сімейних відносин, що особливо було відчутно на етапі первинного реформування сімейного законодавства та подальшого уточнення й внесення змін до Сімейного кодексу України. Міждержавні інтеграційні процеси не лише стосуються правового регулювання у широкому сенсі, а й переплітаються з живим імміграційним рухом. Численні сімейні зв'язки пов'язують наших громадян з громадянами Німеччини, Франції, Італії, Польщі та інших європейських країн.

Мета статті – встановити, які держави ЄС уклали двосторонні міжнародні договори з Україною щодо допомоги у сімейних відносинах, значення міжнародних договорів для врегулювання сімейних відносин у цілому та майнових відносин подружжя зокрема та виявлення можливості покращення правової допомоги у тих країнах, з якими ще нема таких договорів.

Об'єктом є суспільні відносини у сфері сімейного права України та країн-членів ЄС, а предметом – міжнародне законодавство, наукова доктрина.

Гаазька конференція з міжнародного приватного права продукувала вісім конвенцій у сфері сімейного права. З них: Конвенція про право, що застосовується до аліментарних зобов'язань стосовно дітей (1956 р.)[1]; Конвенція про визнання та виконання рішень у справах щодо аліментарних зобов'язань стосовно дітей (1958 р.)[2]; Конвенція про компетенцію та застосовуване право стосовно захисту неповнолітніх (1961 р.)[3]; Конвенція про укладання шлюбу і визнання його недійсним (1978 р.)[4]; Конвенція про захист дітей і співробітництво в сфері міжнародного усиновлення (удочеріння) (1993 р.)[5]; Конвенція про визнання розлучень та рішень про роздільне проживання подружжя (1970 р.); Конвенція про право, застосовуване до правових режимів власності подружжя (1978 р.)[6]; Конвенція про юрисдикцію, застосовуване право, визнання, застосування та співпрацю стосовно батьківських обов'язків та заходів захисту дітей (1996 р.)[7]; Конвенція про міжнародне стягнення аліментів для дітей та інших видів сімейного утримання від (2007 р.)[8].

До іншої групи договорів у сфері сімейного права належать Конвенції ЄС: Європейська конвенція про усиновлення дітей 2008 р.[9], Європейська конвенція про репатріацію неповнолітніх 1970 р.[10], Європейська конвенція про правовий статус позашлюбних дітей 1975 р.[11], Європейська конвенція про визнання та виконання рішень про тюремне ув'язнення дітей та відновлення тюрем для дітей 1980 року.

Комітет міністрів ЄС ухвалив резолюції: про громадянство подружжя з різним громадянством 1977 р.[12], про громадянство дітей, які народилися у шлюбі, 1977 р.[13], про рівність подружжя у цивільному праві 1978 року[14]. Цей же орган прийняв низку документів, що носять рекомендаційний характер. ООН прийняла ряд конвенцій у сфері захисту прав дітей. Серед них: Конвенція про громадянство одруженої жінки від 20 лютого 1957 р.[15] (набрала чинності для України ще 16 грудня 1958 р.), стосується правового статусу одруженої жінки; Конвенція ООН про права дитини від 20 листопада 1989 р.[16]; Декларація ООН про соціальні та правові принципи від 3 грудня 1986 р.[17], що стосуються захисту та добробуту дітей; резолюція 41/85 Генеральної Асамблеї ООН від 3 грудня 1986 р. про передання дітей на виховання та їх усиновлення на національному й міжнародному рівнях.

Варто зазначити, що Україна заінтересована врегульовувати відносини як із заходом, так і зі сходом у сфері цивільних та сімейних справ. Для цього вона бере участь у Конвенції про правову допомогу і правові