УДК 004.056.53

**УХАНОВА Н.С.**, старший науковий співробітник
НДІ інформатики і права НАПрН України

# ЗАХИСТ ІНФОРМАЦІЙНОГО ПРОСТОРУ ВІД ТЕРОРИСТИЧНИХ ПОСЯГАНЬ ТА НЕГАТИВНИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ

***Анотація**. В статті розглядаються інформаційно-психологічні та суспільно-правові аспекти використання сучасного інформаційного простору та інформаційно-комунікаційних технологій на шкоду людині, суспільству і державі. Розкрито питання терористичних викликів і загроз з використанням інформаційного простору. Проаналізовано інформаційно-психологічні механізми здійснення інформаційних операцій, маніпулювання, ідеологічного впливу і вербування прибічників терористичних та інших злочинних організацій з використанням інформаційно-комунікаційних технологій.*

***Ключові слова**: інформаційний простір, інформаційно-комунікаційні технології, інформаційно-психологічний вплив, інформаційний тероризм, кібератаки, маніпуляція.*

***Summary.** The article considers informational and psychological, as well as public and legal aspects of the use of modern information space and information and communication technologies to the damage of human, society and state. The issue of terrorist challenges and threats with the use of information space is explored. The informational and psychological mechanisms of implementation of information operations, manipulation, ideological influencing and recruiting of supporters of terrorist and other criminal organizations with the use of information and communication technologies are analysed.*

***Keywords:** information space, information and communication technologies, information and psychological influencing, information terrorism, cyber attacks, manipulation.*

***Аннотация**. В статье рассматриваются информационно-психологические и общественно-правовые аспекты использования современного информационного пространства и информационно-коммуникационных технологий во вред человеку, обществу и государству. Раскрыт вопрос террористических вызовов и угроз с использованием информационного пространства. Проанализированы информационно-психологические механизмы осуществления информационных операций, манипулирования, идеологического влияния и вербовки сторонников террористических и других преступных организаций с использованием информационно-коммуникационных технологий.*

***Ключевые слова:** информационное пространство, информационно-коммуникационные технологии, информационно-психологическое влияние, информационный терроризм, кибератаки, манипуляция.*

**Постановка проблеми.** Сучасний світ уже давно вступив в епоху глобалізації, яка безпосередньо позначається на усіх сферах життєдіяльності людини, суспільства і держави. Під її впливом трансформуються і активно розвиваються інформаційні технології, інформаційні ресурси, продукти і послуги, а сама інформація стала могутньою зброєю для широкого застосування.

Водночас, за нашими оцінками, правове регулювання інформаційних відносин суттєво відстає від техніко-технологічного розвитку інформаційної сфери, що “de facto” розбудовується в Україні протягом останніх 15 – 20 років. При цьому, глобальна інформаційна інфраструктура та її базові компоненти, як об’єкти правового регулювання, та проблеми транскордонного використання інформаційно-комп’ютерних технологій знаходяться на початковому етапі дослідження. Зазначене, власне, і визначає актуальність звернення до обраної теми.

**Результати аналізу наукових публікацій.** Системний аналіз правових аспектів використання віртуальних технологій почався в зарубіжній правовій доктрині у 90-х рр. минулого століття, а віртуальні технології досліджувалися як технологічний ресурс і як загальнонаукове ключове поняття та феномен, який впливає на соціальний контекст правового регулювання. Як свідчить аналіз наукових здобутків, найбільший науковий і практичний інтерес представляють фундаментальні дослідження Л. Лесссіга (Lessig L.) з проблематики нормативно-технічних і правових засобів регулювання кіберпростору, “нормативної мінливості” регулювання, об’єктивно обумовленої розвитком програмно-технологічного забезпечення; роботи В. Майера-Шонбергера (Mayer-Schqnberger V.) і М. Цівіца (Ziewitz M.), присвячені питанням неминучості правового регулювання транскордонного використання інформаціфних технологій засобами міжнародного права; роботи Дж. Голдсміта (Goldsmith J.) і Т. Ву (Wu T.) і їх фундаментальне дослідження, що узагальнило 20-річну еволюцію регулювання технологій в роботі “Хто контролює Інтернет: ілюзії безмежного світу” (2006 р).

**Метою статті** є висвітлення актуальних питань використання інформаційних технологій та інформаційного простору як інформаційної зброї, характеру впливу Інтернет-ресурсів на масову свідомість та відповідних правових аспектів у цій сфері.

**Виклад основного матеріалу**. Динамічне поєднання і взаємодія нових інформаційних технологій та засобів зв’язку поклали початок виникненню нового феномену, який отримав назву “інформаційний простір” (за окремими джерелами – “кіберпростір”). Це середовище електромагнітних процесів, обробки цифрових даних та їх передачі, приховане від візуального сприйняття, проте воно є вкрай важливим для стану економіки і добробуту суспільства.

Стосовно понятійно-категоріального апарату варто звернути увагу, що одним із базових в інформаційній сфері є поняття “інформаційний простір”, яке також одержало відповідне наукове визначення. Водночас, у низці досліджень і документів застосовується й дещо інший термін – “віртуальний простір”. Зокрема, на думку Л. Лесссіга, *віртуальний простір – це технічна конструкція, що базується на зведенні норм і правил, які обумовлюють формат регулювання віртуальних технологій*. При цьому, в якості норм і правил, тобто “кодексу”, або “коду” (Code), виступає програмне забезпечення, віртуальна архітектура, протоколи і стандарти Інтернету. Саме цей “звід норм” слід розглядати як нормативний “кодекс”, здатний регулювати і накладати обмеження на поведінку учасників, і який може забезпечити можливості для досить широкого контролю, оскільки технічна архітектура віртуального простору регулює свободу особистості таким же чином, яким право і правові норми регулюють суспільні відносини [1].

Основний принциповий висновок, до якого приходять Д. Голдсміт і Т. Ву стосовно правових аспектів використання інформаційно-комп’ютерних технологій полягає в тому, що всі наші припущення щодо майбутнього Інтернету були невірні, оскільки територіальне регулювання можливо і насправді затребуване, а Інтернет слід розглядати як “віртуальний простір”, в якому територіальне право, державна влада та міжнародні відносини відіграють таку ж роль, як і технологічні винаходи [2, с. 118].

Як зазначає Е. Лонгворт, інше поняття – “кіберпростір” слід розглядати як “міжнародний простір”, подібний до міжнародних вод Антарктиди, стосовно якого слід використовувати ті ж само правові регулятивні механізми [3, с. 24]. Тобто, сфера регулювання транскордонного використання інформаційно-комп’ютерних технологій пов’язана з комплексом завдань і проблем, вирішення яких лежить у площині міжнародного права.

Загалом, у нормотворчій практиці більш усталеним є використання поняття *“інформаційний простір”*, а стосовно інформаційно-комп’ютерних технологій та програмних продуктів – *“кіберпростір”*. Термін *“віртуальний простір”* переважно розглядається як синонімічний. Також слід звернути увагу на низку актуальних аспектів:

*по-перше*, питання полягає не в тому, чи можна застосовувати міжнародне право до “інформаційного простору” або “кіберпростору”, оскільки позитивна відповідь на це питання не викликає сумнівів, а в тому, які саме форми і методи при цьому мають використовуватись;

*по-друге*, рамки застосування міжнародного права не слід зводити до системи обмежень, що накладаються чинним міжнародним правом на національні або регіональні підходи у сфері регулювання застосування інформаційно-комп’ютерних технологій;

*по-третє*, міжнародне право може бути застосоване до Інтернету, а Інтернет впливає на міжнародне право. При цьому, теза про виникнення нового міжнародного права, про що йшлося в окремих працях західної правової доктрини, є дискусійною;

*по-четверте*, існуюча реальність не підтвердила припущень про те, що регулювання відносин у сфері Інтернету настільки різноманітне і “породжує такі синергетичні зв’язки”, які можуть трансформувати роль суверенних держав як суб’єктів міжнародного права.

У той же час, великі перспективи, що відкривають перед людством новітні технології, та зростаюча залежність від них пов’язані з низкою проблем, на які необхідно звернути увагу. Однією з таких проблем є протиправні дії в інформаційній сфері, у тому числі кібератаки, кібертероризм, комп’ютерне шпигунство та використання шкідливого програмного забезпечення для перешкоджання вкрай важливим процесам життєдіяльності суспільства.

Сьогодні інформаційно-комп’ютерні технології перестали бути якимось “єдиним” об’єктом регулювання, оскільки являють собою багаторівневу мережу, глобальна технологічна інфраструктура якої забезпечує їх транскордонне функціонування і використання, що підлягає врахуванню при правовому регулюванні відносин у досліджуваній сфері. Технологічно складна глобальна багаторівнева структура інформаційних технологій охоплює кілька інфраструктурних рівнів, починаючи від “найнижчого” – “фізичного” рівня (канали зв’язку волоконно-оптичних ліній, супутникові канали, радіочастотний спектр та ін.), закінчуючи “вищим” рівнем Інтернет-додатків (веб портали і сайти, соціальні мережі, поштові сервіси тощо). На кожному з інфраструктурних рівнів інформаційних технологій складаються стосунки, які виникають з приводу різних і досить специфічних об’єктів регулювання. При цьому, такі компоненти багаторівневої глобальної технологічної інфраструктури, як номерні ресурси адресації (глобальний пул IP-адресного простору, номери автономних систем, портів і протоколів і т.ін.), система доменних імен верхнього рівня, кореневі сервери системи доменних імен, є базовими (фундаментальними) і обумовлюють транскордонне функціонування і використання інформаційних технологій.

Протягом першого десятиліття XXI ст. у процесі правового регулювання пріоритетна увага приділялася кібератакам та інформаційним війнам. Але не так давно колишній співробітник Агентства національної безпеки США Едвард Сноуден розголосив відомості, що становлять державну таємницю, та розкрив більше інформації, ніж найкращий розвідник зміг би зібрати за часів холодної війни. Не слід забувати, що Сноуден навіть не був суперагентом – просто завдяки сучасним технологіям він мав

доступ до великого масиву даних, які в минулому отримати було б просто неможливо. У зв’язку з цим слушним видається питання: як у майбутньому забезпечити ефективний захист даних від несанкціонованого доступу? Нині ми більш повно маємо усвідомлювати необхідність захисту інформації.

Як відомо, норми міжнародного права і національні законодавства надають право національним спецслужбам здійснювати технічну розвідку та збирати за її допомогою інформацію стратегічного, оперативного чи тактичного рівня. На прикладі Сноудена варто звернути увагу на особливості технічної розвідки США (наприклад, на програму спостереження “ПРИЗМА”). Ця специфіка обумовлена тим, що такого роду діяльність реалізується з опорою на закони, які дозволяють зберігати і фільтрувати дані в технічно можливому обсязі. За необхідності – наприклад, в рамках боротьби з тероризмом – американські розвідувальні служби можуть збирати інформацію всередині країни і за кордоном. На території США на заходи зі збору відомостей поширюються положення американського законодавства, і при цьому США, керуючись зрозумілою логікою, використовують всі доступні їм нормативні та технічні засоби. Але, якщо мова йде про інформаційний простір, то в цій сфері загальновизнаних правил поки що не існує.

Однією з найбільш актуальних нині проблем інформаційного простору або кіберпростору є проблема запобігання і протидії кібератакам, що здійснюються в результаті проникнення чи зламу комп’ютерних програм і систем, апаратних засобів, засобів цифрового захисту тощо. Україна в умовах гібридної війни протягом тривалого часу є пріоритетною мішенню для кібератак та здійснення негативного інформаційно-психологічних впливу на шкоду людині і суспільству у національному інформаційному просторі з боку РФ та злочинних організацій. Для проведення кібератак використовуються не лише такі засоби, як програми “троянський кінь” або заражені вірусом електронні повідомлення. Тепер удари наносяться з максимальною точністю в ході “соціально-технічних нападів” з використанням вірусів спеціалізованих різновидів. При цьому атакуючий суб’єкт завчасно вивчає, хто в організаційній структурі чи системі електронного управління займає важливу позицію та хто відкриє і прочитає електронне повідомлення з певним адресним рядком.

В сучасному світі також поширюється використання інформаційного простору терористичними, сепаратистськими та екстремістськими організаціями і групами. Вони використовують цей простір для агітації, пропаганди своїх поглядів і вербування поплічників, провокації масових безладів, диверсій тощо. При цьому радикалізація стосується перш за все процесу ідеологічної обробки, який нерідко супроводжує перетворення завербованих неофітів на осіб, сповнених рішучості здійснювати насильницькі дії на основі екстремістських ідеологій. Процес радикалізації часто включає використання пропаганди, яка протягом тривалого часу ведеться або за допомогою особистого спілкування, або через Інтернет. Зазначимо, що тривалість і ефективність пропаганди та інших використовуваних засобів переконання варіюється залежно від конкретних обставин і відносин.

Свобода в інформаційному просторі робить можливим широке застосування інформаційно-психологічних технологій формування громадської думки і нав’язування людині тих чи інших міфологічних уявлень або заданих стереотипів поведінки і мислення. Маніпуляція орієнтована на елімінацію логіки, критичного аналізу і примітивізацію мислення цільової групи, підміну логічного стійкого асоціативного зв’язку, коли те чи інше явище асоціюється з деструктивним образом, що нав’язується. У цьому аспекті самостійний погляд на світ, спроби незалежного мислення на основі здорового глузду, а не в рамках нав’язуваної міфологічної парадигми, міфологічного

образу світу і вкорінених у ньому стереотипів поведінки і цінностей представляє основну небезпеку для будь-якої маніпуляційної програми.

Елементами маніпуляційної програми є міфи, в тому числі міфи про рішення долі і т.ін., що вселяє думку про покірність і безглуздість критичного аналізу існуючого порядку речей. Однак вразливим місцем будь-якої маніпуляції є альтернативні джерела інформації, альтернативний погляд, вміння критично аналізувати запропонований варіант вирішення проблеми. Умовою ефективності маніпуляції є виведення масової свідомості за звичні рамки норм, цінностей і стереотипів, дестабілізація масової свідомості за допомогою пропагандистських і відволікаючих заходів. Ступінь ефективності маніпулювання залежить від глибини і точності сканування ментальних структур групи: її норм, цінностей, стереотипів.

Наприклад, ІДІЛ можна порівняти з дуже потужною сектою. Спочатку з об’єктом вербування знайомиться людина, чоловік або жінка. Робиться це через інтернет: соціальні мережі, месенджери, сайти знайомств, спільноти, форуми і так далі. Все це на тлі дезінформації в мережі у вигляді новинних джерел. Починається спілкування та підбирається ключ до особистості. Легше працювати з людьми вразливими, з тонкою душевною організацією, невпевненими в собі, які не мають своєї особистої думки чи зі спотвореним уявленням про світ. Це – люди без “стрижня” [**Ошибка! Источник ссылки не найден.**, с. 456].

Як бачимо, характерна особливість людського сприйняття полягає в тому, що людина краще засвоює ту інформацію, яка схожа на вже існуючі у неї уявлення. Основні засоби інформаційної війни орієнтовані на цю особливість. Будь-які маніпуляції та пропагандистські компанії засновані на “ефекті резонансу”, коли інформація, що “імплантується”, спрямована на зміну поведінки спільності, маскуються під знання і стереотипи, вже існуючі в конкретній соціальній спільності, на яку спрямована пропагандистська компанія. Розвиток засобів і технологій інформаційної війни робить дедалі більш актуальними розробку засобів протидії маніпулятивним технологіям, а також розвиток методів управління і захисту інформаційного простору, заснованих на демократичних нормах свободи слова. Тому, незабаром, виявляється, що цей новий знайомий має багато схожих інтересів, аналогічне хобі, захоплення, погляд на життя.

Після довгого листування один пропонує модель іншого суспільства з аналогічними можливостями і псевдоцінностями. Головне – закласти фундамент. Вибір людини і закладка фундаменту – це перший етап. Далі “мотиватор” формує уявлення про те, що є несправедливості, що “жертва” може і повинна знайти своє місце в житті. Реалізувати плани. Внести особистий внесок. Адже кожен хоче бути корисним, необхідним. Потрібно зробити щось важливе. Промивання мізків відбувається повільно і поступово.

В останні роки терористичні організації все частіше вдаються до використання Інтернету в якості альтернативної бази для підготовки терористів. Дедалі ширший спектр засобів інформації надає платформи для поширення практичних посібників у вигляді інтерактивних навчальних посібників, аудіо- та відеокліпів, інформаційних повідомлень і рекомендацій. На цих Інтернет-платформах також публікуються докладні інструкції, часто в легкодоступному мультимедійному форматі і на декількох мовах, з таких питань, наприклад, як вступити до терористичних організацій, як виготовити вибухові боєприпаси, вогнепальну та інші види зброї або небезпечні матеріали і як планувати і здійснювати терористичні акти. Ці платформи виступають в якості навчальної бази. Крім того, вони використовуються, зокрема, для обміну спеціальними методами, прийомами та сучасними знаннями з метою вчинення терористичних актів.

У наявних в Інтернеті навчальних матеріалах пропонуються інструменти для протидії або захисту від оперативно-розшукової та розвідувальної діяльності, неавторизованого доступу до комп'ютерних даних, а також для підвищення рівня захищеності протизаконних комунікацій і діяльності у інформаційно просторі шляхом використання доступних засобів шифрування і методів анонімізації. Інтерактивний характер інтернет-платформ допомагає створити відчуття спільності між людьми, що живуть в різних географічних регіонах і мають різне походження, сприяючи створенню мереж для обміну матеріалами навчального і тактичного характеру. Терористичні мережі часто характеризуються як “клітинні” – створені з майже незалежних клітинок. Формальне визначення “літинних мереж” було надане у термінах мережевих компонентів і властивостей. Клітинні мережі мають такі властивості, як надмірність, наявність тісно зв‘язаних клітинок (4 – 6 осіб), відсутність управління вертикальним способом (нечіткі директиви), відсутність планування (формування за рахунок локальних обмежень), можливість еволюціонування у відповідь на деструктивну діяльність [5, с. 111].

Відзначимо, що інформаційні війни спрямовані не тільки проти держави і найважливіших об’єктів її інфраструктури, але і проти екстремістів-опонентів. У більшості випадків потенціал скоєних кібератак та інформаційних операцій обмежений у зв’язку з дефіцитом знань. Це позбавляє їх організаторів можливості здійснювати великомасштабні напади. Але досягнувши необхідного професійного рівня, екстремісти зможуть завдавати більшої шкоди.

Чинна міжнародно-правова база у сфері боротьби з тероризмом міститься в різних джерелах, включаючи резолюції Генеральної Асамблеї та Ради Безпеки ООН, договори, судову практику і міжнародне звичаєве право. Резолюції Ради Безпеки можуть накладати на держави-члени юридично зв’язуючі та політичні зобов’язання, що належать до сфери т.зв. “м’якого права”, або сприяти формуванню нових міжнародно-правових норм. Резолюції Ради є обов’язковими для всіх держав-членів. Генеральна Асамблея також прийняла ряд резолюцій про боротьбу з тероризмом, які є корисними джерелами “м’якого права” та мають велике політичне значення, хоча і не є юридично обов’язковими. Юридичні зобов’язання також накладаються на держави відповідно до двосторонніх і багатосторонніх документів щодо боротьби з тероризмом. Обов’язок притягати винних у скоєнні терористичних актів до судової відповідальності лягає, насамперед, на внутрішньодержавні органи влади, оскільки міжнародні суди, як правило, не мають юрисдикції щодо таких актів.

**Висновки.**

В цілому, розгляд сучасних викликів і загроз, пов’язаних із розвитком інформаційно-комп’ютерних технологій та інформаційного простору або кіберпростору, а також питань захисту інформаційного простору від терористичних посягань та негативних інформаційно-психологічних впливів підсумуємо низкою висновків та пропозицій, зокрема:

1. У XXI столітті захист даних та безперебійне функціонування інформаційно-комунікаційних систем і систем зв’язку значною мірою впливають на усі сфери життєдіяльності людини, суспільства і держави. В інформаційному просторі формуються новітні виклики і загрози щодо захисту даних, комп’ютерних систем і мереж та приватного життя громадян. Все більшого поширення набувають факти здійснення інформаційно-психологічних операцій на шкоду людині та суспільству, які також створюють реальні загрози державному суверенітету і територіальній цілісності

держав. Динаміка трансформації сучасних викликів і загроз не відстає від темпів розвитку інформаційно-комп’ютерних технологій та інформаційного простору.

2. Сучасну інформаційну війну, як одну із основних складових гібридної війни, за нашими оцінками, варто розглядати як боротьбу за цілком реальну владу, спробу глобального перерозподілу сфер впливу та розшарування суспільств і країн-членів ЄС і НАТО. Застосування інформаційної зброї, у т.ч. кібератак, відбувається за різними векторами екстремістського спектру *(наприклад, “партизанські” напади в кіберпросторі лівих екстремістів, заклики до створення “інституту віртуального джихаду” тощо)*. При цьому життєво необхідно запобігти можливому нанесенню кібератак на системи контролю даних і нападів з метою заволодіння контролем за системами електронного (цифрового) управління об’єктами критичної інфраструктури *(електро-, водо- і газопостачання, авіаційного і залізничного руху, біржовою і банківською діяльністю тощо)*.

3. Використання інформаційного простору (кіберпростору) в терористичних та інших злочинних цілях стало суттєвою транснаціональною проблемою. Для її вирішення потрібні узгоджені заходи транскордонного характеру за участі міжнародних і національних правоохоронних систем та систем безпеки. Значна роль у зв’язку з цим має приділятися комплексу двосторонніх і багатосторонніх заходів та обміну досвідом між державами, а також досягненню консенсусу щодо питань боротьби з тероризмом та іншими злочинами в інформаційній сфері. Також актуалізується проблема розвитку міжнародної, регіональних і національних систем інформаційної безпеки та потреба підвищення ефективності міжнародного співробітництва національних спецслужб і правоохоронних органів у цій сфері.

## Використана література

1. Lessig L. Code and other Laws of Cyberspace. – Режим доступу : http://www.archiv.orgc yber.law.harvard.edu/lessigbio

2. Goldsmith J. and Wu T. Who Controls the Internet? : Illusions of a Borderless World. – New York : Oxford University Press, 2006. – 219 p.

3. Longworth E. Possibilities of a Legal Framework for Cyberspace: Including a New Zealand Perspective. Prepared for the Unesco Experts Meetings on Cyberspace Law. 2010. – Pp. 23-29.

4. Lipton Jacqueline D. Bad Faith in Cyberspace : Grounding Domain Name Theory in Trademark, Property, and Restitution. Harvard Journal of Law & Technology. Volume 23. Number 2 Spring 2010. – P. 451-457.

5. Ланде Д.В. Основи інформаційного та соціально-правового моделювання : навч. посіб. / Д.В. Ланде , В.М. Фурашев , К.В. Юдкова. – К. : НТУУ “КПІ”, 2014. – 220 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~