Наталія
ВАРЕНЬЯ

Сергій
АВРАМЕНКО

Віртуальна реальність як новий світовий чинник для аналізу рівня терористичної загрози

У статті, крізь призму сучасних перспективних напрямків розвитку технологій у сфері доповненої та віртуальної реальностей, розглядаються ознаки інформаційного тероризму та його складових – кібертероризму і медіа-тероризму, а також прогнозуються подальші вектори терористичних загроз у медіа-просторі. Проаналізовано актуальні документи ООН щодо боротьби з тероризмом та показано, що сьогодні у міжнародному праві та в українському законодавстві у сфері забезпечення антитерористичної безпеки акцент робиться на технічну складову – недопущення порушення працездатності інформаційних систем, а стратегія боротьби із загрозами будується здебільш на відповідних новітніх концепціях, спрямованих на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем. В доповнення до сучасних напрямків антитерористичних заходів в інформаційній сфері запропоновано концептуальні шляхи протидії терористичній загрозі у медіа-просторі.

Ключові слова: контр-тероризм, інформаційна безпека, дипфейк, віртуальна реальність, антитерористична безпека, боротьба з тероризмом, терористична загроза, постправда

In the article is viewed through a lens of modern perspective directions of development of technologies in the sphere of the augmented and virtual realities, signs of information terrorism and its components – cyber terrorism and media terrorism are considered, and also the further vectors of terrorist threats in media space are predicted. The relevant UN anti-terrorism documents have been analyzed. It has been shown that today international law and Ukrainian legislation in the field of counter-terrorism security emphasize the technical component of preventing the disruption of information systems, while the strategy to combat threats is largely based on the latest relevant concepts aimed at strengthening the security of global information and telecommunications systems. Conceptual ways of counteracting the terrorist threat in the media space have been proposed in addition to the modern directions of anti-terrorist measures in the information sphere.

Keywords: counter-terrorism, information security, deep fake, virtual reality, anti-terrorism security, the fight against terrorism, terrorist threat, post-truth

Вступ: Сутність тероризму. Визначення та мета. Дослідження та аналіз сучасного тероризму цікавить чимало науковців. Тероризм, його виникнення та динаміка змін, а також вплив політико-економічних світових процесів описані та проаналізовані низкою вчених (У. Лакер, Н. Лівінгстон, С. Ломброзо та ін.). Увага дослідників спрямована на правові аспекти тероризму, психологічні, соціально-політичні тощо. Не залишилися поза увагою й ідеологія, мотиви та напрямки терористичної діяльності, а також недоліки сучасної нормативно-правової бази у цій сфері. Слід зазначити, що явище тероризму та форми його прояву перебувають у постійному еволюційному процесі, що значно ускладнює їхнє вичерпне юридичне визначення. Вітчизняні науковці (В. Антипенко, В. Ємельянов, В. Коваленко, В. Леонов, В. Ліпкан та ін.) неодноразово наголошували на необхідності постійної актуалізації законодавства з урахуванням еволюційних процесів явища тероризму та регулярного перегляду Концепції національної безпеки України. Проте, усі дослідники стикаються з дуалістичною

УДК 341+65.012.8:007+32(477)
<https://doi.org/10.36952/uail.2020.2.46-60>

© Н. Варенья
© С. Авраменко

ВАРЕНЬЯ Наталія
кандидат юридичних наук, провідний науковий співробітник,
Національна академія Служби безпеки України
АВРАМЕНКО Сергій
науковий консультант, Українська асоціація міжнародного права

проблемою юридично-правових дефініцій: бажання максимального розширення трактування терористичної діяльності може у наслідку нести невинуватене використання його політичними силами у боротьбі з опонентами, звуження ж, зі свого боку, дозволяє залишитись поза визначенням так званим «партизанам», «ополченцям», «визволителям» та іншим «зеленим чоловічкам», як досить часто називають себе самі терористи.

В. Ємельянов зазначає, що, з огляду на кримінально-правову характеристику, тероризм повинен мати певний характер і чіткі межі. Це обумовлено формалізованістю українського права і необхідністю встановлення чітких підстав притягнення до кримінальної відповідальності. Як відомо, у кримінальному праві такою підставою є сукупність ознак складу злочину, що однозначно повинна характеризувати конкретне суспільне небезпечне явище як злочин. Проте, юридичному оформленню поняття «тероризм» у сучасних умовах заважають як мінімум дві обставини: по-перше, політизованість оцінок тероризму; по-друге, прагнення надати такому визначенню всеосяжний характер [1].

У цьому контексті доцільно згадати, що поняття тероризму щільно пов'язане з іншим терміном – терор, який тлумачиться як метод управління суспільством шляхом залякування державою в цілому або окремими політичними силами. У другій половині ХХ сторіччя терміни «терор» та «тероризм» почали розрізняти за сутністю.

Сьогодні «терор» трактується як нелегітимне насильство з боку держави по відношенню до суспільства в цілому або до дисидентів і опозиції. «Тероризм» – практика нелегітимного насильства, що реалізується силами і організаціями, які протистоять державі [2].

Юридичні визначення поняття тероризму суттєво різняться між собою. За результатами аналізу 109 визначень тероризму, американські дослідники Алекс Шмідт та Альберт Джонгмен зазначили, що більшість з цих визначень містять такі елементи: «використання насильства або сили» (83,5 % випадків), «політична вмотивованість» (65 %), «створення обстановки страху та жаху» (51 %), «загроза» (47 %), «розрахований на психологічний ефект або передбачувану реакцію» (41,5 %), «використання насильства стосовно одних осіб (невинних жертв) або майна з метою примусу до певної поведінки інших осіб (суб'єктів впливу)» (37,5 %), «цілеспрямована, спланована, систематична, організована діяльність» (32 %), «бойовий метод, стратегія, тактика» (30,5 %), «з порушенням прийнятих правил, без гуманітарних обмежень» (30 %), «примус, вимагання» (28 %), «публічний характер» (21,5 %), «свавілля; безособовий, випадковий, нерозбірливий характер» (21 %), «цивільні особи, мирні суб'єкти як жертви» (17,5 %), «залякування» (17 %), «невинність жертв» (15,5 %), «група, рух, організація як злочинець» (14 %), «символічний аспект, демонстрація іншим» (13,5 %), «непередбаченість, несподіваність виникнення насильства» (9 %), «підпільний, прихований характер» (9 %) тощо [3, р. 5-6]. Вочевидь, найпоширенішим визначенням тероризму є застосування крайнього насильства або загроза його застосування з метою залякування для досягнення публічних або політичних цілей, що, до речі, знаходить своє підтвердження у визначенні російського дослідника тероризму – В. Лунєєва [4, с. 620].

Законом України «Про боротьбу з тероризмом» [5] тероризм описується не лише як злочин терористичної спрямованості, а й у ст. 1 містять інші діяння. Терористична діяльність, згідно з визначенням у Законі, це діяльність, яка охоплює:

- планування, організацію, підготовку та реалізацію терористичних актів;
- підбурювання до вчинення терористичних актів, насильства над фізичними особами або організаціями, знищення матеріальних об'єктів у терористичних цілях;
- організацію незаконних збройних формувань, злочинних угруповань (злочинних організацій), організованих злочинних груп для вчинення терористичних актів, так само як і участь у таких актах;
- вербування, озброєння, підготовку та використання терористів;
- пропаганду і поширення ідеології тероризму;
- фінансування та інше сприяння тероризму.

На думку А. Кулікова, у боротьбі з тероризмом необхідно вживати наступні заходи.

По-перше, необхідна організація скоординованої роботи на міжнародному рівні щодо визначення загального поняття «тероризм» і комплексу причин, що його породжують. Сучасна конструкція правового визначення тероризму досить громіздка, складна і ускладнює кваліфікацію кримінально-правових діянь, що мають схожі кваліфікаційні ознаки, проте тероризмом не є.

По-друге, потрібна подальша розробка базових принципів боротьби з тероризмом на міжнародно-правовому рівні.

По-третє, необхідна розробка модельного міжнародного закону про боротьбу з тероризмом.

По-четверте, ефективність боротьби з міжнародним тероризмом немислима без створення міжнародної системи моніторингу тероризму на основі обов'язкової передачі відповідної інформації від

національних урядів, регіональних і міжнародних організацій, що беруть участь у різних формах боротьби з тероризмом, її накопичення і аналізу в спеціально створеному інформаційному банку.

По-п'яте, при організації масштабної боротьби з тероризмом і транснаціональною злочинністю, як показує практика Афганістану, необхідна розробка міжнародно-правових основ проведення міжнародних антитерористичних операцій із закріпленням обов'язковості санкції Ради Безпеки ООН на здійснення і контроль за їх проведенням.

По-шосте, слід також вжити заходів щодо найшвидшої ратифікації членами міжнародного співтовариства конвенцій по боротьбі з тероризмом і подальшого внесення ними потрібних змін у національні законодавства. Необхідне скликання спеціальної сесії Генеральної Асамблеї ООН по боротьбі з тероризмом і ухвалення нею відповідних рішень [6].

В.А. Ліпкан виділяє такі ознаки тероризму як злочинного діяння [7, с. 67]:

1. Тероризм є однією з форм організованого насильства.
2. При тероризмі здійснюється примус більш широкої соціальної групи, ніж безпосередні жертви насильства.
3. Формування цілей здебільшого не пов'язане з конкретними проявами насильства, тобто між жертвою та метою, на яку спрямовують свої дії терористи, немає прямого зв'язку.
4. Тактична мета тероризму полягає в тому, щоб привернути увагу до проблеми, стратегічна – досягти певних соціальних змін (свобода, незалежність, звільнення з виправно-трудових установ певного контингенту осіб, революція тощо).
5. Акти тероризму самі по собі становлять традиційні форми загально-кримінальних злочинів.
6. Тероризм паралізує протидію з боку громадськості.
7. Знаряддям впливу тероризму є психологічний шок, який супроводжується усвідомленням того, що будь-хто може стати жертвою незалежно від того, до якої верстви суспільства він належить.
8. Будь-які правила чи закони не визнаються – жертвами терористичних актів можуть бути як дорослі чоловіки, так і жінки та діти.
9. Розрахунок робиться на ефект раптовості, неочікуваності та несподіваності.
10. Публічність виступає як основна ознака тероризму.
11. Демонстративність актів тероризму – бажання справити враження на широкий загал.
12. Тероризм припускає «політичне вимагання», тому він не пов'язаний із стихійними повстаннями та виступами населення.
13. Тероризм вимагає негайного задоволення висунутих вимог, інакше він вдається до реалізації погроз та ескалації насильства.
14. Може бути використаний організаціями будь-якого забарвлення.
15. Практично завжди бере на себе відповідальність за вчинені акти насильства, оскільки вони є засобом досягнення мети, а не самоціллю.
16. Являє собою антитезу політичного вбивства. Йому притаманна індиферентність щодо жертв, на противагу від селективності при політичному вбивстві.
17. Розрив між безпосередньою жертвою насильства та групою, яка становить об'єкт впливу, мету насильства.

Однак, спроби виокремити універсальне визначення тероризму, на нашу думку, повинні виходити з необхідності захисту не абстрактних прав і свобод, а забезпечувати безпекову складову певної групи суспільних відносин та не можуть бути універсальними через внутрішньодержавну специфіку, що унеможливорює створення ідеального міжнародного визначення та повинно бути досить загальним у міжнародному праві і доповнюватись та конкретизуватись у внутрішньодержавних нормативно-правових актах з урахуванням місцевих особливостей.

Будь-яка терористична діяльність здійснюється цілеспрямовано й завжди передбачає наявність певної мети. Особливістю тероризму є те, що формування цілей здебільшого не пов'язане з конкретними проявами насильства, тобто між жертвами та метою, на яку спрямовують свої дії терористи, нема прямого зв'язку. Реально сам терористичний акт не призводить до досягнення декларованих цілей. Часто це лише привід для демонстрації терористами своїх вимог і можливостей. Слід зазначити, що одним з найважливіших значень терористичних актів є їхня публічність, бо створити атмосферу страху у суспільстві можливо лише за умов широкого суспільного резонансу. Тобто, однією з ознак тероризму безумовно є публічність: за вчинені акти насильства хтось завжди бере на себе відповідальність, тому що вони є засобом досягнення мети, а не самоціллю [8, с. 50].

Таким чином, створення широкого суспільного резонансу є однією з обов'язкових умов терористичної діяльності. Без нього неможлива зміна суспільних настроїв та підвищення соціальної напруженості. Тобто, ключовим елементом є широке поширення інформації про існування сил, що настільки не погоджуються з існуючим порядком, що готові боротись з ним будь-яким способом, у тому числі

ціною життя жертв терористичних актів. Для цього використовуються легальні засоби масової інформації, які широко розповсюджують матеріали стосовно терористичних актів, а також створюються власні, підконтрольні терористам мас-медіа, через які вони популяризують свою ідеологію [9, р. 383].

Роль незалежних засобів масової інформації (ЗМІ) в досягненні терористами своєї мети заслуговує особливої уваги. В. Крутов у своєму виступі на круглому столі «ЗМІ проти тероризму» [10, с. 6-8] зауважив, що при плануванні і здійсненні терористичних акцій терористи, як правило, ставлять за мету прорив до широкої аудиторії. І в цій ситуації журналісти, висвітлюючи конкретні ситуації, стають не просто незалежними свідками, а – бажають вони того чи ні – активними учасниками подій. Де та межа, перейшовши яку, репортер стає інструментом терористів? Наскільки інформація, що передається, укріплює позиції терористів; утруднює дії співробітників спецпідрозділів; створює прямо або побічно додаткові загрози життю і здоров'ю заручників? На його думку, необхідна грамотна організація порядку і процесу інформування громадськості як про прояви тероризму, так і про контртерористичні операції.

Необхідно доповнити вищевикладене тим, що сучасні ЗМІ поступово втрачають свої позиції як щодо поширення інформації, так і щодо впливу на громадську думку. Наразі, тепер лідерство захопили засоби масової комунікації (ЗМК), зокрема, соціальні мережі, месенджери, форуми, блоги та інші ресурси мережі Інтернет, де терористи не лише підшукують найманців, а й цілеспрямовано ведуть пропагандистську роботу і намагаються здійснювати активний вплив на громадську думку, суспільно-політичні настрої тощо.

Більшість науковців вважає, що тероризм породжує загальну небезпеку, яка виникає в результаті вчинення загально-небезпечних дій або погрози такими діями. Вони зазначають, що ця небезпека повинна бути реальною (проте, далі ми доведемо, що це, нажаль, не зовсім так, прим. авт.), загрожувати невизначеному колу осіб, і об'єктивно виражатись у вчиненні або погрозі вчинення вибухів, підпалів та інших загально-небезпечних дій, які реально можуть завдати шкоди невизначеному колу осіб або спричинити інші тяжкі наслідки [11, с. 8].

Вчені, зокрема – В. Ліпкан, виділили загальні положення щодо терористичної діяльності [12, с. 70]:

а) чим менша за чисельністю терористська група, тим краще вона законспірована, а також тим жорстокіші та радикальніші методи застосовує;

б) класифікація терористських груп за визначеними критеріями дозволяє зрозуміти, чому саме ці групи людей згуртовуються для вчинення протиправних дій, чому вони вдаються до тероризму, а не беруть участь, наприклад, у загальних виборах або ж не звертаються до міжнародного суду в Гаазі, чому чинять убивства беззахисних людей;

в) метою діяльності більшості терористських груп є територіальні питання (відокремлення або возз'єднання з певною державою), тому невирішення конфліктів у минулому знаходить своє вирішення у теперішній час і цим вирішенням є вчинення актів тероризму;

г) більшість терористських груп мають зовнішню підтримку;

г) чим активніше держава бореться з тероризмом, тим менше шансів на успіх мають самі терористи, отже, боротьба з тероризмом повинна носити випереджаючий, агресивний та безжалісний до терористів характер.

Одним з видів вивчення явища тероризму є його розподіл за видами та характером вчинення терористичних актів. На сьогодні цей розподіл виглядає таким чином:

- тероризм, що використовує звичайні вибухові речовини;
- із застосуванням потужного електромагнітного випромінювання, яке може впливати як на людей, так і на електронне оснащення об'єктів критичної інфраструктури;
- що використовує хімічні, біологічні та ядерні речовини;
- дестабілізуючий економічну складову суб'єкта терористичних посягань;
- інформаційний тероризм, що містить так званий кібертероризм, який спрямований на порушення функціонування, підміну або знищення комп'ютерних мереж та сховищ даних і медіа-тероризм, що спрямований на створення інформаційного впливу на суспільство шляхом використання ЗМК.

Останнім часом діяльність терористичних організацій значно вдосконалила методи внутрішнього управління шляхом використання сучасних інформаційних технологій. Терористи мають свої координаційно-аналітичні та пропагандистські центри, розвідку, систему закритого зв'язку між своїми членами та іншими терористичними організаціями.

Використання мережі Інтернет (і, зокрема, ЗМК) значно підвищило рівень комунікації та, як наслідок, мобільності та автономності окремих груп і цілих терористичних організацій, створило підґрунтя для низки вузьких спеціалізацій у терористичних структурах, дозволило приховано координувати свої дії не лише у регіональних, а й у світових масштабах. Діяльність терористичних угруповань

сьогодні має усі ознаки наявності стратегічного планування та інших сучасних досягнень у сфері прийняття управлінських рішень.

Терористичні організації та сучасні технології. Терористи ХХІ сторіччя мають досить високий рівень підготовки, який цілком співвідноситься з рівнем підготовки державних контртерористичних формувань та контррозвідки. Вони опанували сучасні оперативні методи прихованого пересування, маскуванню, обходу охоронних систем та систем захисту. До того ж терористичними угрупованнями активно беруться на озброєння досягнення у сфері інформаційних технологій, що дозволяє досить успішно збирати, накопичувати, формалізувати, обробляти і аналізувати великі масиви неструктурованої інформації (так звану *big data*). Отримана інформація може використовуватись для проникнення, втручання та пошкодження комп'ютерних систем державних установ, банків, науково-дослідних центрів та інших об'єктів критичної інфраструктури (так званий кібертероризм). Перевагою для терористів цього напрямку є можливість діяти з великої відстані та анонімізації безпосередніх виконавців, а також відносна дешевизна та зменшення власних ризиків у порівнянні з класичними підривами, підпалами тощо. Єдиним недоліком є значно менший суспільний резонанс від кібертерористичних атак, що унеможливило активне використання емоційної складової.

Однак, недооцінювати вплив кібертероризму не варто. Деякі дослідники вже відмітили, що інформаційна революція дала можливість військовій компанії провести у віртуальному варіанті. До того ж, віртуальною може стати і сама війна, хоч результати її будуть цілком реальні. Можна не задіювати жодного солдата, тільки в інформаційних мережах і системах обробки інформації зробити дії, наслідком яких буде повне підпорядкування економіки і політики противника [13].

Дійсно, кількість злочинів у кібер-сфері має тенденцію до суттєвого зростання з кожним роком. Постійно фіксуються намагання представниками екстремістських та терористичних організацій атакувати електронні мережі та банки даних у державному, промисловому та банківському секторах.

Окрім проявів кібертероризму, світ все більш масово стикається з проявами медіа-тероризму – впровадженням інформаційно-психологічних операцій з метою, шляхом маніпулятивних дій, вплинути на свідомість громадськості для досягнення своїх завдань у політичній та економічній сферах. Як зазначалось вище, терористичні дії – це не тільки людські жертви та матеріальні збитки, скільки привертання уваги та залякування. Це, до речі, одна з ключових відмінностей між терористичними та диверсійними діями (диверсія має за мету саме знищення живої сили або важливих об'єктів супротивника). Для досягнення результату, терористичні угруповання активно використовують ЗМІ у пропагандистських цілях, через їхню економічну залежність, та у маніпулятивних – через бажання представників преси розповсюджувати «гарячі» сенсаційні новини. Останнє дозволяє здійснювати психологічний тиск на широку аудиторію, залякувати та провокувати на певні дії (або, навпаки, на бездіяльність).

Таким чином, ми бачимо активне використання терористичними структурами методів інформаційної війни, що дозволяє при мінімумі затрат здійснювати вплив на значно більш сильні як у військовому, так і у фінансовому сенсі, соціальні групи (етнічні громади, країни, групи країн тощо).

Сучасні інформаційні технології та розвиток сфери засобів масової комунікації (ЗМК) дозволив вийти інформаційному тероризму на новий рівень. До цього моменту, використовуючи для поширення своїх поглядів та вимог засоби масової інформації, терористичні організації не могли досягти достатнього рівня впливу. Тепер, нажалі, ситуація змінилась. Використовуючи ЗМК, терористи отримали могутні важелі впливу на свідомість, що завдяки маніпулятивним технологіям, методам нейролінгвістичного програмування та іншим засобам інформаційного впливу стають вже достатньо вагомими для спричинення дестабілізації у суспільстві, роздмухування страхів і панічних настроїв та, як наслідок, отримують реальну можливість нав'язування своїх вимог. Такі прогнози вже не можуть залишатись поза увагою. Інформаційний тероризм – це цілком реальний новий вид тероризму сьогодення, який можна визначити, як «прямий вплив на психіку і свідомість людей з метою формування потрібних думок і суджень, які певним чином спрямовують поведінку людей. На практиці під інформаційним тероризмом завжди розуміють такий насильницький пропагандистський вплив на психіку, який не залишає для людини можливостей для критичної оцінки отримуваної інформації. Як правило, така інформація є відверто тенденційною і досягає своєї мети не за рахунок якості маніпулятивного впливу, а за рахунок його обсягу. Окрім використання офіційних засобів масової інформації, інформаційний тероризм спирається на поширення певного типу чуток» [14].

Зазначене вказує, що терористичним актом в інформаційній сфері (зокрема, йдеться про медіа-тероризм) є прямий психологічний вплив на громадськість, що викликає відчуття страху, недовіру до органів влади та інші дестабілізуючі суспільство емоційно-психологічні стани. Нагадаємо, що такий вплив може бути спрямовано і на невеликі групи людей, і на цілі держави, і, навіть, на групи країн. За

умов успішного досягнення у об'єктів такого впливу необхідного емоційного та психологічного стану, цілком можливим стає використання штучно створеної «громадської думки» для тиску на владу з метою примусу прийняття останньою неадекватних управлінських рішень. Це, у свою чергу, прямо впливає на безпековий стан, стан економіки та соціальної сфери. Тобто, напрямок інформаційного тероризму можна розглядати як такий, що несе загрозу не лише окремим групам, а має суттєві важелі для руйнівного впливу на складові людської цивілізації взагалі.

Новітні дослідження в інформаційній сфері методів впливу на громадськість за допомогою ЗМІ та ЗМК, технології підготовки та, навіть, створення віртуальних інформаційних приводів, вочевидь, не лишаються поза увагою терористичних угруповань, дозволяють їм відносно невеликими ресурсами (як людськими, так і фінансовими) виходити на глобальний рівень впливу на людство на відміну від вже традиційного тероризму, який переслідує досить вузьку національну, релігійну або політичну мету. Тому логічним виглядає намір використовувати терористичними та екстремістськими формуваннями інформаційно-психологічні операції та здійснювати штучне втручання у світовий порядок навіть без фізичного вчинення терористичних актів у їхньому класичному розумінні.

Віртуальна реальність та епоха постправди. Інформаційне середовище сьогодні знаходиться у стадії стрімкого розвитку технологій обробки відео- та аудіо-потоків та, що найбільш важливо, відпрацьовуються та удосконалюються алгоритми створення віртуальної та доповненої реальностей. На наш погляд, найбільш вдале визначення віртуальної реальності – «штучно створене комп'ютерними засобами середовище, в яке можна потрапити, змінюючи його зсередини, спостерігаючи трансформації і отримуючи при цьому реальні відчуття. Потрапивши в цей новий тип аудіовізуальної реальності, можна вступати в контакти не лише з іншими людьми, а й зі штучними персонажами» [15].

Важливість ролі, що відіграє Інтернет-контент у житті людства можна проілюструвати результатами, опублікованими дослідницькою організацією з Великобританії «We Are Social» [16]. За її даними, кількість інтернет-користувачів у всьому світі вже перевищило 4,5 мільярди (приблизно 65% від всього населення Світу), з яких близько 3,8 мільярдів – користувачі соціальних медіа. Крім того, результати досліджень свідчать про уповільнення зростання аудиторії соціальної мережі Фейсбук та значне пришвидшення динаміки росту кількості користувачів мереж візуального контенту (TikTok, Pinterest). Розглянута у звіті демографія аудиторії Pinterest особливо цікава – незважаючи на меншу у шість разів кількість користувачів у порівнянні з Instagram, можливий охопит цільової аудиторії виявляється практично таким самим. Згідно ж дослідженням компанії Cisco, до 2022 року 82% всього онлайн-контенту буде складати відео-контент [17]. З урахуванням тенденції на зростання аудиторії споживачів саме візуального контенту та розуміючи досягнення алгоритмів створення дипфейків (визначення дипфейку наведемо нижче, прим. авт.), ми вбачаємо досить серйозною ситуацію з комунікативними напрямками створення медіа-контенту та можливістю суттєвого впливу медіа-реальності на соціальні групи різного напрямку, розміру та географії.

Як зазначає І. Волкова, доповнена реальність являє собою медіа-контент, що цілком укладається у потреби сучасної масової культури, де лідером є індустрія інтерактивних ігор [18]. Вочевидь, медіа-індустрія все більшу роль приділяє розвитку саме доповненню реальності і намагається частково підміняти об'єктивну. Віртуальна реальність хоч і вступає у вагоме протиріччя зі сприйняттям реальності об'єктивної, викликає психологічну залежність та, до того ж, спричиняє своєрідні втрати смислів, коли у новій ситуації сприйняття не працюють визнані схеми тлумачень. Тому для ефективного моделювання відео- та аудіо-контенту медіа змушені використовувати передові дослідження у сфері психології та нейропсихології, філософії та соціології задля створення відповідних затребуваних форм медіа-програм, які формуватимуть смисли, потребу у яких відчуває соціум або потребу у яких соціуму буде нав'язано.

Прогнози щодо лідерства у найближчий час саме сегменту штучного інтелекту та, як наслідок, алгоритмів створення віртуальної реальності (до 46% мобільних пристроїв матимуть змогу її відтворювати навіть самостійно) знаходять своє підтвердження у дослідженнях PwC «Global Entertainment & Media Outlook 2019-2023» [19].

Популярність технологій моделювання та відтворення віртуальної реальності серед населення додатково підтверджується дослідженнями Інституту сучасних медіа MOMRI [20]. Результати опитування дозволили з'ясувати, що з терміном «віртуальна реальність» знайомі 68% респондентів віком 18-24 роки, 70% – віком 24-34 роки, 75% – віком 35-44 роки.

Безумовно, технології віртуальної реальності викликають велику зацікавленість рекламного бізнесу (перш за все – у сфері трансляції потокового відео-контенту онлайн), що знайшло своє відображення у дослідженнях IAB [21]. «Потокове мовлення знаходиться на підйомі, і цей відео-феномен допомагає створювати бренди», – сказав Ерік Джон (Eric John), заступник директора, IAB Digital Video Center

of Excellence. За даними IAB, понад дві третини (67%) споживачів всього світу дивляться трансляції потокового відео в реальному часі, а більше половини (52%) цієї групи вважають за краще безкоштовне потокове мовлення з підтримкою реклами, а не платну підписку. З них близько 70% переглядають потокові онлайн-трансляції щоденно, а основним джерелом відеосигналу в прямому ефірі для них є соціальні платформи. 47 відсотків споживачів стверджують, що збільшили обсяг перегляду трансляцій в прямому ефірі у 2018 році в порівнянні з 2017 роком, що досить показово. Така популярність потокового відео впевнено використовується провідними медіа-гігантами. Так BBC News Labs вже звітувала про понад дванадцять категорій інноваційного моделювання новин (онлайн-ЗМІ, телебачення), які здатні привернути велику аудиторію. До цих категорій увійшли, у тому числі, й технології віртуальної відео- та аудіо-реальностей. Найближчим часом технології телебачення використовуватимуть все більше алгоритмів створення віртуальної реальності як у розважальному сегменті, так і у сегменті відео-інформаційного напрямку. Цілком прогнозоване й виникнення нових форм відео-контенту, здатному привернути увагу глядачів, і якщо звичний вже випуск новин інформує аудиторію про якусь подію, то сюжет у форматі віртуальної реальності робить глядача своєю частиною, дає змогу відчувати йому подію від першої особи. Фахівці Google пояснюють перехід до такого формату як перехід від т.зв. сторітеллінгу (розповідь історії, від англ. story та to tell) до сторілівінгу (жити в історії, від англ. story та to live). Такий формат більше орієнтований на емоції та почуття, ніж на донесення конкретної інформації.

Соціальні мережі також залучились до розвитку нових видів медіа-контенту та зосередились на технологіях віртуальної реальності, що підтверджується дослідженням «Journalism, Media, and Technology Trends and Predictions 2018» [22].

Таким чином, можна стверджувати, що принципи і напрямки подальшого розвитку алгоритмів створення медіа-контенту достатньо чітко визначені та полягають у вдосконаленні технологій віртуальної реальності та їхнього застосування у більшості видів Інтернет-контенту від ЗМІ та телебачення до соціальних мереж та ЗМК, а формат цього контенту буде максимально містити емоційну складову, майже залишивши поза увагою інформаційну.

Синтез зображення за допомогою штучного інтелекту та з використанням нейромереж, що створює цілком або частково штучний контент, отримав окремий термін – Діпфейк (Deepfake, від англ. Deep learning – глибинне навчання та Fake – підробка). Безумовно, для наукового моделювання, створення розважального контенту тощо досягнення у сфері створення віртуальної і доповненої реальностей стали революційними. Проте, вже є чимало доведених фактів використання діпфейку у політичній сфері, як, наприклад, у Сполучених Штатах Америки, коли комік Джордан Піл (Jordan Peele) створив та виклав у мережу Інтернет змодельоване відео, на якому Барак Обама заявляє, що ми вступаємо в епоху, коли наші вороги можуть змусити когось сказати що завгодно в будь-який момент часу та обзиває Дональда Трампа [23].

Дослідники вже зараз визнають наявність суттєвої проблеми з фейковими новинами. Це й стурбованість аудиторії з приводу упередженої журналістики, введення в оману політиками, неправдива реклама, а також свідомо сфабриковані історії, що поширюються через соціальні медіа. За прогнозами, швидкого вирішення цих проблем, нажаль, не вбачається. Намагання відновити довіру громадськості до ЗМІ шляхом перевірки фактів та більшої прозорості стикається з важкістю переконання аудиторії фактами, що суперечать їхнім власним поглядам, а неминучим наслідком викриття фейкової інформації є збільшення рівня скептицизму до фактів.

Само по собі використання фейкових (неправдивих) новин вдало використовувалось і раніше. Перекручені або цілком брехливі інформаційні потоки створювались за допомогою мас-медіа з політичних, військових та ідеологічних міркувань. Проте, як відзначив соціолог О. Фірсов у своїй доповіді «Зміна в розумінні достовірності в сучасному світі» [24], раніше для встановлення істини можна було апелювати до, так би мовити, експертних центрів, які могли претендувати на володіння знаннями і розумінням істини – влада, наукові та енциклопедичні видання, церква, а поділення на правду і неправду у той час ще зберігалось. Тепер під сумнів підпадає сама категорія достовірності через деномінацію самого поняття правди, а раз віри нікому немає, аудиторія починає сприймати інформацію як ігрову, а себе – фігурою на ігровому майданчику. Природа медіа опиняється в іншій реальності, яка будується за принципово іншими принципами, зникає система відліку, у якій може існувати істина, остаточно пропадає межа між правдою та фейками, соціум потрапляє у ситуативний світ миттєвих емоціональних реакцій. У цьому світі правда матеріалізується самими медіа, котрі створюють фейкові інформаційні потоки, які поширюються багатьма ЗМІ, що викликає відчуття реальності і починає вже насправді народжувати дійсність. Такий феномен штучно створеної правди можна розглянути на прикладі протестів «жовтих жилетів» у Франції [25]. Прихильники «жовтих жилетів» широко розповсюджували відео та зображення людей, поранених в Барселоні (Іспанія), сили бельгійської армії,

які носять жовті жилети, як ніби це відбувалося у Франції. Дехто з журналістів телебачення (як, наприклад, журналісти RT) робили репортажі з металевими касками на голові, намагаючись переконати свою аудиторію, що ведуть репортаж з «фронту» та брали інтерв'ю у людей, які стверджували, що начебто бачили, як поліція сама підпалювала машини. Сенсаційний заголовок та палаюча машина в кадрі – серед усіх цих фальшивих новин здавалося, що інші репортажі з місця подій, де Париж не горить і немає ні куль, ні зброї, також можуть бути перекручені, хоча фактично, більшість демонстрацій «жовтих жилетів» у Франції були тихими і мирними та проходили у віддалених місцях, але посилювались після створення «навіяної» реальності.

Описаний приклад відповідає визначенню Оксфордським словником терміну «постправда» (англ. post-truth) – це обставини, при яких об'єктивні факти є менш значимими під час формування громадської думки, ніж заклики до емоцій і особисте переконання [26]. Тобто, вагомість фактів вже не має суттєвого значення і розуміння «істини» залежить від суб'єктивних поглядів та емоцій. Професорка Єльського університету, дослідниця історії Східної Європи Марсі Шор (Marcy Shore) на своїй Інавгураційній промові на Lviv MediaForum 2017 [27] відзначила, що ми маємо велику кількість альтернативних реальностей. І жодна з них не є більш правдивою за інші. Більш розгорнуто щодо постправди висловився доктор філологічних наук, професор, автор багатьох книжок з комунікативних технологій та інформаційних війн Георгій Почепцов. У своєму інтерв'ю «Дзеркалу тижня» [28] він зазначив, що постправда не виникає на порожньому місці, вона як чутки – часто підтверджує те, про що ми вже думали, як про можливе. Тепер наші страхи отримують підтвердження. Реально постправда стала результатом того, що право голосу, завдяки Інтернету, отримали всі відразу. Обсяг інформації, як наслідок, став настільки більшим, що вже ніхто не в змозі перевіряти її на вірогідність. Швидкість змін така велика, що ми весь час ніби живемо завтрашнім днем, тому перевіряти вчорашнє вже не має сенсу. Крім того, він відзначив пріоритетність саме форми подання інформації, надавши наступний приклад: американські військові активно почали вивчати літературознавче поняття наративу, тобто типу оповідання – історично і культурно обґрунтованій інтерпретації певного аспекту світу з певної позиції, коли побачили, що наративи Аль-Каїди більш достовірні для населення, ніж їхні. Було підключено об'єктивний інструментарій нейропсихології, щоб зрозуміти, що й чому викликає в нашому мозку такі реакції. Тож це цілком серйозний науковий напрямок – як сказати так, щоб цьому повірили.

Таким чином, можна коротко визначити: постправда являє собою велику кількість таких правд, що співпадають з поглядами споживачів інформації, які стають амбівалентними до істини, тобто, як зазначає медіа-аналітик Андрій Мирошніченко, категоричне «або/або» змінюється на «і/і».

Визначення інформаційного тероризму. Протидія медіа-тероризму: окремі аспекти та пропозиції. Розвиток технологій впливу на інформаційний простір та тенденції превалювання емоційної складової медіа-контенту над інформаційним не могли бути проігнорованими терористичними організаціями. Саме визначення основної мети тероризму як залякування для досягнення публічних або політичних цілей свідчить про використання терористами, перш за все, засобів впливу на масовий емоційний, когнітивний та інформаційний стан. Широке залучення для цього сучасних досягнень у сфері мас-медіа, використання технічних засобів для виводу з ладу елементів державних інформаційних інфраструктур або ж використання цих інфраструктур з метою катастрофічного впливу на життєдіяльність суспільства – цілком логічний та прогнозований крок, який названо відносно новим терміном: «інформаційний тероризм». Визначаючи стан сучасних загроз інформаційного тероризму, слід зазначити, що інформаційний тероризм – це, насамперед, форма негативного впливу на особистість, суспільство і державу усіма видами інформації. Іншим визначенням інформаційного тероризму є діяльність, що виражається в залякуванні населення й органів влади з метою досягнення злочинних намірів. Особливістю негативних інформаційних впливів разом із актами інформаційного терору є їхня непрозорість або напівпрозорість [29, с. 162-166].

За своїми ознаками інформаційний тероризм можна поділити на кібертероризм та медіа-тероризм, тобто на технічну та медіа складову. І якщо кібертероризм полягає у зовнішньому втручанні у роботу комп'ютерних мереж та інформаційних систем технічними та/або програмними засобами з метою пошкодження цих мереж або несанкціонованого їх використання, – медіа-тероризм є різновидом інформаційно-психологічного впливу шляхом зловживання особливостями функціонування таких комп'ютерних мереж та інформаційних систем і використання для маніпулятивного впливу засобів ЗМІ та ЗМК.

Найбільш доступним сьогодні стає саме напрямок медіа-тероризму як такий, що не потребує будь-яких зовнішніх втручань у роботу інформаційно-комп'ютерних систем та, відповідно, не може бути швидко та однозначно розпізнаний. Технології створення віртуальної реальності вже зараз доз-

воляють виробляти діпфейки достатньої якості та продовжують вдосконалюватись і ставати більш доступними як по вартості, так і простотою виготовлення. Очевидним стає нездатність громадян орієнтуватись в інформаційному просторі, заповненому діпфейками, а можливості впливу на їхній психо-емоційний стан та погляди стають дедалі простішими у реалізації.

Особливістю сучасного тероризму є активне застосування у якості важливого елемента маніпуляції інформаційно-психологічних технологій для впливу на людську свідомість та суспільну думку, з можливістю використання глобальних комунікацій. Такі дії терористів розраховані, в основному, на виклик своїми діями інформаційно-психологічного шоку серед великих мас, що має забезпечити таким чином досягнення зловмисниками своїх цілей. Вміло враховуючи здобутки інформаційної епохи та існування глобальних ЗМІ, терористи зробили своєю основною зброєю та інструментами впливу телебачення та кіберпростір [30].

Таким чином, сучасна діяльність терористичних організацій може використовувати у якості медіа-впливу:

- здійснені терористичні акти або штучний витік інформації про начебто підготовку до таких актів;
- кримінальні злочини, що не мають відношення до терористичних дій;
- техногенні аварії та катастрофи, які виникли без втручання з боку терористів;
- події, змодельовані та візуалізовані засобами штучного інтелекту з використанням віртуальної та/або доповненої реальності (діпфейки);
- будь-які поєднання усіх вищезазначених пунктів.

Сучасний інформаційний простір остаточно став одним з головних напрямків політичної, економічної, етноконфесійної боротьби та використовується у т.ч. терористичними організаціями, бо дії у медіа-сфері дозволяють завдати значної шкоди суб'єкту атаки без застосування будь-якого фізичного втручання, а виключно шляхом нав'язування суспільству потрібних смислів, наративів. Зникла потреба у нав'язуванні своєї волі шляхом безпосереднього насильства, поступившись місцем тероризму інформаційному, що вимагає від суспільства нових підходів у сфері права, зміни стандартів та підходів до обміну інформацією та її розповсюдження. І хоча сучасні дослідження інформаційного тероризму досить чисельні, на сьогодні відсутнє як його уніфіковане визначення, так і системне юридичне бачення правопорушень у цій сфері та протидії їм, хоча необхідність доопрацювання та уніфікації законодавства з метою регулювання такого явища постало на міжнародному рівні.

На цей час існує лише 16 діючих міжнародних угод у сфері боротьби з тероризмом [31]:

- Конвенція про злочини та деякі інші акти, що здійснюються на борту повітряних суден, 1963 року;
- Конвенція про боротьбу з незаконним захопленням повітряних суден, 1970 року;
- Конвенція про боротьбу з незаконними актами, спрямованими проти безпеки цивільної авіації, 1971 року;
- Конвенція про запобігання та покарання за злочини проти осіб, які користуються міжнародним захистом, у тому числі дипломатичних агентів, 1973 року;
- Міжнародна конвенція про боротьбу із захопленням заручників, 1979 року;
- Конвенція про фізичний захист ядерного матеріалу, 1979 року та Поправки до Конвенції про фізичний захист ядерного матеріалу, 2005 року;
- Протокол про боротьбу з незаконними актами насильства в аеропортах, що обслуговують міжнародну цивільну авіацію, 1988 року, що доповнює Конвенцію про боротьбу з незаконними актами, спрямованими проти безпеки цивільної авіації;
- Конвенція про боротьбу з незаконними актами, спрямованими проти безпеки морського судноплавства, 1988 року;
- Протокол про боротьбу з незаконними актами, спрямованими проти безпеки стаціонарних платформ, розташованих на континентальному шельфі, 1988 року, що стосується терористичної діяльності на морських стаціонарних платформах;
- Конвенція про маркування пластичних вибухових речовин з метою їх виявлення, 1991 року;
- Міжнародна Конвенція про боротьбу з бомбовим тероризмом, 1997 року;
- Міжнародна Конвенція про боротьбу з фінансуванням тероризму, 1999 року;
- Міжнародна Конвенція про боротьбу з актами ядерного тероризму, 2005 року;
- Міжнародна Конвенція про взаємну правову допомогу і видачу з метою боротьби з тероризмом, 2008 року;
- Протокол, що доповнює Конвенцію про боротьбу з незаконним захопленням повітряних суден, 2010 року;
- Конвенція про боротьбу з незаконними актами щодо міжнародної цивільної авіації, 2010 року.

Нажаль, сьогодні у міжнародному праві не розглянуто нюанси сучасних перспективних напрямків розвитку терористичних дій у медіа-просторі та не в повній мірі охоплено всі ознаки інформаційного тероризму. Досягненням у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки (див. Резолюцію Генеральної Асамблеї ООН № 71/28 від 5 грудня 2016 року [32]) вважається, що цілям стратегій боротьби із загрозами в інформаційній сфері відповідало б продовження вивчення відповідних міжнародних концепцій, які були б спрямовані на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем. Тобто, акцент робиться виключно на технічну складову – порушення працездатності інформаційних систем.

Стосовно ж українського законодавства – у ньому наразі взагалі відсутнє визначення інформаційного тероризму. Для цього використовується термін «кібертероризм» – терористична діяльність, що здійснюється у кіберпросторі або з його використанням [33]. Проте, на наш погляд, таке визначення потребує уточнень. Означене розуміння законодавством кібертероризму більше відповідає терміну «інформаційний тероризм», як більш загальному. Окремо ж доцільно визначити терміни «кібертероризм» (як акт технічного апаратного та/або програмного втручання у терористичних цілях у роботу комп'ютерних мереж та їхніх фрагментів з метою несанкціонованого використання чи завдання шкоди або повного унеможливлення їх функціонування) та медіа-тероризм (використання у терористичних цілях ЗМІ, ЗМК та інших засобів масового поширення інформації, а також комп'ютерних мереж та інформаційних систем, для проведення медіа-заходів з метою здійснення масового психологічного тиску, дестабілізації суспільства, впливу на його фоновий емоційний стан та ментальність).

Для успішного протистояння загрозам слід виокремити ряд основних напрямів такої протидії [34]:

- уніфікація та гармонізація національного законодавства та міжнародних актів;
- проведення наукових розробок в області створення сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси;
- удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності та комп'ютерному тероризму;
- удосконалення багаторівневої системи підготовки кадрів у сфері інформаційної безпеки.

Протидія медіа-тероризму повинна містити у собі три загальні напрямки: протидія у юридичній сфері (законодавство, ККУ тощо); протидія у технологічній сфері (засоби виявлення, моніторингу, локалізації, знешкодження тощо); протидія у соціально-освітній площині (шляхом підвищення медіа-грамотності населення).

Стосовно юридичної сфери: необхідно переосмислити та сформулювати визначення інформаційного тероризму та його складових – кібер- та медіа-тероризму з урахуванням технологій превентивної нейтралізації соціальних конфліктів, що виступають основними каталізаторами тероризму. За сучасних умов нагальною потребою є створення ефективного ризик-менеджменту антитерористичної безпеки, законодавче закріплення та чітке визначення механізмів його функціонування в мирний час й у кризових ситуаціях.

Технологічна площина протидії медіа-тероризму полягає у впровадженні засобів моніторингу інформаційного простору та використанні відповідних напрацювань у сфері обробки структурованої та слабо структурованої інформації. Дослідження у цьому напрямку проводились такими вітчизняними науковцями, як І. Рижов, Н. Варення та ін. У своїх роботах вони описали та довели дієвість та доцільність ведення так званого реєстру загроз терористичного характеру (РЗТХ), обґрунтували комплексний метод оцінювання загроз терористичного характеру, що передбачає виявлення складових загроз, порівняльний аналіз, деталізацію і визначення взаємозв'язків та узагальнення отриманих результатів. В результаті досліджень було встановлено, що найбільш доцільно використовувати методи теорії управління ризиками. Зокрема, завдяки математичним моделям можна зобразити максимальну кількість загроз, а в подальшому сформувати матриці протидії тероризму. Також визначено, що під час використання наукових методів з кримінальної науки, соціології, філософії, математики тощо необхідно виявити та побудувати взаємозв'язок загроз терористичного характеру, деталізувати їх, здійснити порівняльний аналіз, визначити величини впливу факторів та узагальнити дані. Крім того, було доведено, що важливими факторами в реєстрі загроз є врахування загального емоційного фону соціуму та рівень соціальної напруженості в регіоні проведення моніторингу. Зазначене окреслює перспективний напрям подальших досліджень – розроблення моделей аналізу соціальної напруженості та протестного потенціалу.

Проте, юридична і технологічна складові організації протидії медіа-тероризму спрямовані на виявлення й нейтралізацію таких процесів в інформаційному просторі, що вже відбулись або відбуваються. Завдяки відповідним компенсуючим заходам можна нейтралізувати або зменшити негативний вплив терористичних посягань, юридично обґрунтувати сам факт інформаційно-терористичних дій та розпочати процедуру кримінального переслідування організаторів. Але найважливішою, на наш

погляд, сьогодні стає соціально-освітня складова протидії медіа-тероризму. Саме вона дозволяє здійснювати упереджувальні заходи, які, у свою чергу, майже не залежатимуть від векторів потенційних терористичних загроз у медіа-сфері. Тому необхідно є розробка загальнодержавної системи інформаційної протидії тероризму шляхом чіткого визначення функцій та повноважень державних органів, громадських організацій, засобів масової інформації в комплексі заходів щодо інформаційної блокади будь-яких дій терористів. Не менш важливим видається формування за допомогою мас-медіа комплексу науково-просвітницьких програм, покликаних сприяти ідеології ненасильства, толерантної поведінки, формуванню «антитерористичної свідомості» в суспільстві, повазі культурного розмаїття. Міжкультурний діалог, що має реалізовуватися за допомогою мас-медіа, може допомогти уникнути виникнення різних видів екстремізму, насильства, ксенофобії, релігійної нетерпимості в державі [35, с. 19].

Слід зауважити, що соціально-освітні заходи необхідно розробляти і впроваджувати у принципово новому форматі. Потрібно враховувати, що, як зазначалось вище, сьогодні активно проходять процеси переформатування підходів до медійного впливу на громадськість, коли емоційна складова стає значно вагомішою за інформаційну. Тому доречно звернутись до таких понять, як наратив та СММ (маркетинг у соціальних медіа, від англ. SMM – Social Media Marketing).

Важливість створення власних наративів полягає у тому, що саме уява є ключовою у досягненні поставленої мети. Гра на загальнолюдських цінностях та емоціях створює систему взаємопов'язаних концептуальних платформ. Шлях від існуючого до очікуваного завжди починається з розповіді, що містить дії, персонажів та бажаний уявний пункт призначення. Наратив – це свого роду міфологічна історія, що містить необхідні акценти та, у нашому випадку, повинна стати конкурентною альтернативою наративам терористичного складу. Проте, хоч розуміння того, що терористичні угруповання залучають своїх прибічників через активне просування своїх поглядів у вигляді міфологізованих ідеологічних контекстів, не залишилось сьогодні поза увагою безпекових антитерористичних напрацювань, цілий ряд досліджень у цьому напрямку не враховує багато параметрів, що визнається, наприклад, у доповіді англійського інституту стратегічного діалогу, який є одним з лідерів оперативного реагування на проблеми екстремізму та міжгромадських конфліктів [36, р. 23]: впровадження інформаційних кампаній дозволяє зібрати величезну кількість даних, однак розуміння впливу контр-наративу на думки та поведінку людей залишаються величезною проблемою.

Як зазначає кандидат психологічних наук, член Асоціації політичних психологів України В. Зеленін, – міфи надзвичайно могутні у віртуальній та медійній сферах. Через емоційне залучення вони алегорично (опосередковано) вказують масам правильний шлях для досягнення бажаної мети в ідеальному просторі. Власна система міфів – це така ж критично важлива частина системи державної безпеки і національної політики будь-якої країни, як енергетична незалежність або модернізація армії.

Проблема професійного сприйняття більшої вітчизняних фахівців, які займаються сьогодні інформаційними технологіями, полягає в тому, що вони мимоволі звужують своє сприйняття тактичних й оперативних завдань. Необхідно піднятися на стратегічний рівень, щоб зрозуміти: новинні портали, бренди, іміджі, історії успіху, культурні події, наукові відкриття і витвори мистецтва, виборчі і рекламні кампанії – усе це не більш ніж розділи великого «сайту». Усі соціальні сфери – політика, економіка, культура, релігія, освіта, військова справа, наука, мистецтво – підпорядковані ідеології того міфу, за законами якого живе зараз конкретна спільнота людей на цьому етапі розвитку цивілізації [37, с. 25]. Виходячи з цього, можна виокремити генеральний напрямок побудови контртерористичного наративу, який полягатиме не у штучному створенні «сценарію» або «версії», а у визначенні напрямку інформаційного втручання, пошуку груп, лояльних до потрібного нам вектору, які самостійно створювали б високоякісні продукти впливу, координації та управління ними.

Робота з наративами буде малоефективною, якщо не приділити достатньо уваги питанням їхнього втілення. З результатів багатьох досліджень вже зрозуміло, що найближчим часом лідерство утримуватиме відео-контент, який сьогодні має тенденцію до широкого залучення можливостей доповненої та віртуальної реальності. Тому найбільший акцент доцільно робити саме на цей напрямок та серйозно відпрацьовувати шляхи його просування, для чого існує достатньо ефективний напрямок – маркетинг у соціальних мережах. SMM полягає не лише у роботі з цільовою аудиторією, а й з позитивними та негативними відгуками, тобто використовує аналіз реакцій, зворотній зв'язок. Важливою складовою цього процесу є організація налагодженої системи моніторингу і реагування.

Хоча маркетинг у соціальних мережах народився у сфері бізнесу з метою просування товарних знаків і брендів, вимоги сьогодення призвели до створення політичного SMM (напрямку, який цілком підходить і для антитерористичних превентивних заходів, прим. авт.), де замість бренду є політичні партії, громадські течії, окремі політики тощо. Проте, на відміну від комерційного мар-

кетингу, тут принципово інший споживач, інша мотивація і, як наслідок, інша цільова аудиторія. Тому «комерційний» підхід до SMM призводить до швидкого росту кількості підписників у групах в соціальних мережах, у соціальних профілях політиків тощо. Але практичних результатів це не дає. Спостерігається сегментація користувачів соціальних мереж за своїми політичними, релігійними, соціальними поглядами, де вони у окремих спільнотах і групах отримують «приємний» для себе медіа-продукт. Завданням SMM тут є не стільки кількісний показник підписників, скільки залучення означених цільових груп до цитування та обговорення спектру ключових карбів потрібного наративу.

Тож, подальші дослідження у цьому напрямку не лише необхідні, а й конче потрібні. Розробка прообразів наративів, створення відповідного медіа-контенту із застосуванням сучасних досягнень у сфері доповненої і віртуальної реальностей та напрямки залучення широкої аудиторії до обговорення такого контенту – найефективніший шлях до втілення в життя розвитку антитерористичної свідомості громадськості.

Висновки. Підсумовуючи викладений матеріал, вважаємо за доцільне виокремити наступні тези.

Однією з обов'язкових умов терористичної діяльності є створення широкого суспільного резонансу. Сам факт терористичного акту не призводить до досягнення декларованих цілей.

Нажаль, сьогодні у міжнародному праві не розглянуто нюанси сучасних перспективних напрямків розвитку терористичних дій у медіа-просторі та не в повній мірі охоплено всі ознаки інформаційного тероризму. Досягненням у цій сфері акцент робиться виключно на технічну складову – порушення працездатності інформаційних систем, визначаючи цілі стратегії боротьби із загрозами в інформаційній сфері у вивченні відповідних новітніх концепцій, спрямованих на зміцнення безпеки глобальних інформаційних та телекомунікаційних систем.

Вдосконалення технологій віртуальної реальності та їхнього застосовування у більшості видів Інтернет-ЗМІ та ЗМК – пріоритетні напрямки подальшого розвитку алгоритмів створення медіа-контенту, завдяки чому остаточно пропадає межа між правдою та фейками, а споживачі контенту, поставши перед великою кількістю різних альтернативних правд, опиняються у ситуативному світі миттєвих емоціональних реакцій та стають амбівалентними до істини.

Існуючі підходи до планування контртерористичних заходів найближчим часом остаточно втраять більшу частину своєї ефективності. Використання терористами методів сучасного інформаційного впливу дозволить їм охоплювати значний масив різних за своїм світоглядом соціальних груп та здійснювати штучне втручання у світовий порядок. Діями у медіа-сфері можна буде завдати навіть більшої шкоди суб'єкту атаки без застосовування будь-якого фізичного втручання, виключно шляхом нав'язування суспільству потрібних смислів, наративів. Тому перспективним напрямком подальших напрацювань у сфері протидії тероризму є розроблення моделей аналізу соціальної напруженості та протестного потенціалу, впровадження засобів моніторингу інформаційного простору і математична обробка структурованої та слабо структурованої інформації з метою раннього прогнозування та завчасного компенсаційного впливу.

Новий погляд на стандарти та підходи до обміну інформацією та її розповсюдження вимагає інших підходів у сфері права, переосмислення визначення інформаційного тероризму та його складових – кібер- та медіа-тероризму з урахуванням таких форматів медіа-контенту, які найближчим часом міститимуть майже одну емоційну складову, залишивши поза увагою складову інформаційну.

Превентивні заходи повинні містити напрацювання і впровадження еволюційних методів посилення антитерористичної свідомості громадян. Сценарії таких дій повинні плануватися на стратегічному рівні, використовувати досягнення у інформаційних технологіях та не обмежуватись виконанням тактичних і оперативних завдань.

1. Емельянов В.П. Терроризм и преступления с признаками терроризирования. Уголовно-правовое исследование / В.П. Емельянов. – М., 2000. – С. 12-23.

2. Ляшенко В.М. Загрози сучасного тероризму в Україні та завдання органів державного управління щодо їх запобігання в науковій літературі. / В. М. Ляшенко // Актуальні проблеми державного управління: – Зб. наук. праць. ХарПІДУ НАДУ – Харків: Магістр, 2006. – № 3 (30). – с. 181-188.

3. Alex P. Schmid, Albert J. Jongman. Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature. New Brunswick, Transaction Books, 1988. – 701 p., P. 5-6.

4. Лунеев В. В. Преступность XX века: мировые, региональные и российские тенденции / В. В. Лунеев. – Изд. 2-е, перераб.и доп. – Москва : Волтерс Клувер, 2005. – 912 с.

5. Про боротьбу з тероризмом : Закон України від 20 березня 2003 р. № 638-IV // Відомості Верховної Ради України. – 2003. – № 25. – Ст. 180.

6. Куликов А.С. Глобальный терроризм и некоторые проблемы борьбы с ним. URL: <http://www.concourt.am/hr/ccl/vestnik/2.20-2003/Kulikov.htm>

7. Ліпкан В.А. Тероризм: юридична дефініція та зміст // Тероризм і боротьба з ним. Президенту України, ВРУ, Уряду України, органам центр. і місцев. виконав. влади; Аналіт. розробки, пропоз. наук. і практ. працівників: Міжвід. наук. зб. / За ред. А.І.Комарової, Ю.В.Землянського, В.О.Євдокимова та ін. – К.: НДІ «Проблем людини», 2000. – Т. 19(1). – 610 с.

8. Тероризм: теоретико-прикладні аспекти : навч. посіб. / кол. авт.; за заг. ред. проф. В. К. Грищука. – Львів : ЛьвДУВС, 2011. – 328 с, с. 50.

9. The SAGE encyclopedia of terrorism: second edition / ed. by Gus Martin. – London, SAGE publications ltd, 2011. – 693 p.

10. Виступи учасників круглого столу “ЗМІ проти тероризму” // Проблеми безпеки особистості, суспільства, держави. – 2005. – № 4, с. 6-8.

11. Проблеми систематизації та комплексного розвитку антитерористичного законодавства України: монографія / [кол. авт.: В.С. Зеленецький, В.П. Ємельянов, В.Я. Настюк та ін.]; за заг ред. В.С. Зеленецького та В.П. Ємельянова. –Х.: Право, 2008. – 96 с.

12. Ліпкан В.А. Тероризм і національна безпека України / В.А. Ліпкан. – К.: Знання, 2000. – с. 70.

13. Илларионов С.И. Террор и антитеррор в современном мироустройстве / С.И. Илларионов. – М.: РИЦ Проф Эко, 2003. – 592 с.

14. Галамба М. Інформаційно-психологічна складова терористичної діяльності: юридическіе статьи // Юридичний журнал. 2006. № 11. С. 53-57. URL: <http://www.justinian.com.ua/article.php?id=2464>.

15. Маньковская Н.Б., Мотлевский В.Д. Виртуальная реальность // Энциклопедия культурологии. URL: https://dic.academic.ru/dic.nsf/enc_culture/278/ВИРТУАЛЬНАЯ.

16. The Global State Of Digital In October 2019, URL: <https://wearesocial.com/blog/2019/10/the-global-state-of-digital-in-october-2019>.

17. Cisco: VNI Global Fixed and Mobile Internet Traffic Forecasts, URL: <https://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html>.

18. Волкова И.И. Компьютерные игры и новые медиа: игровой подход к коммуникациям в виртуальном пространстве // Вестник Российского университета дружбы народов. Серия: Литературоведение. Журналистика. 2017. т. 22. № 2. с. 312-320.

19. Global Entertainment & Media Outlook 2019 – 2023: 20 years of intelligent insights // PWC Global. URL: <https://www.pwc.com/gx/en/industries/tmt/media/outlook/segment-findings.html>.

20. Ринок віртуальної реальності: аналітичний огляд Жовтень / Листопад 2016 // MOMRI Institute. URL: <http://momri.org/wp-content/uploads/2018/08/obzor-vr-oktyabr-noyabr-2016.pdf>.

21. Live Video Streaming: A Global Perspective. Jun. 13, 2018, URL: <https://iabrus.ru/news/1313>.

22. Newman N. Journalism, Media and Technology Trends and Predictions 2018 // Reuters Institute for the Study of Journalist. URL: <https://reutersinstitute.politics.ox.ac.uk/our-research/journalism-media-and-technology-trends-and-predictions-2018>.

23. You Won't Believe What Obama Says In This Video! BuzzFeedVideo. 2017. URL: <https://www.youtube.com/watch?v=cQ54GDm1eL0>.

24. Матеріали круглого столу на тему «Як зберегти достовірність ЗМІ». URL: <https://interaffairs.ru/news/show/22465>.

25. The Brief – A ‘yellow vest’ fake news paradise by Aline Robert with Alexandra Brzozowski. URL: <https://www.euractiv.com/section/politics/news/the-brief-a-yellow-vest-fake-news-paradise/>.

26. Oxford Dictionaries. Lexico Dictionaries. URL: https://www.lexico.com/definition/oxford_english_dictionary.

27. Марці Шор. Інавгураційна промова на Lviv MediaForum 2017. URL: <https://medialab.online/news/sy-la-bezsy-ly-h/>

28. Міжнародний громадсько-політичний тижневик «Дзеркало тижня», № 11, 25-31 березня 2017 р. URL: https://dt.ua/SOCIUM/pravda-ochima-postpravdi_.html

29. Герасименко К.С. Сучасні ознаки загроз «інформаційного тероризму» // Форум права. 2009. № 3. с. 162-166.

30. Кукса І. Інформаційний аспект тероризму та переговорний процес із терористами. URL: <http://mskod.com/informatsiyniy-aspekt-terorizmu-ta-peregovorniy-protses-iz-teroristami/>

31. Перелік чинних міжнародних угод ООН у сфері боротьби з тероризмом . URL: https://www.un.org/ru/documents/decl_conv/conv_terrorism.shtml.

32. Резолюція Генеральної Асамблеї ООН № 71/28 від 5 грудня 2016 року. URL: <https://undocs.org/en/A/RES/71/28>.

33. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII // Відомості Верховної Ради України від 10.11.2017 - 2017 р., № 45, с. 42, ст. 403.

34. Гавриш С.Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії / С.Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2009. – № 20. – С. 3-14.

35. Свентицька О.В. Інформаційний тероризм як феномен сучасної міжнародної політики: автореф. дис. канд. політ. наук: 23.00.03 / Свентицька О.В. – К., 2007. – 19 с.

36. Silverman, Stewart, Amanullah & Birdwell. The Impact of Counter-Narratives, The Institute for Strategic Dialogue, London, United Kingdom 2016, 54 p.

37. В. Зеленін. Основи міфодизайну: Психотехнології керування медіареальністю. Навчально-методичний посібник. – К.: Вид-во «Гнозис», 2017. – 168 с.

Summary

VIRTUAL REALITY AS NEW WORLD FACTOR FOR ANALYSIS OF LEVEL OF TERRORIST THREAT

Today there are 16 existing international agreements in the field of combating terrorism. International law does not consider the nuances of modern perspective directions of development of terrorist actions in media space and does not fully cover all signs of information terrorism. Achievements in the field of information and telecommunications in the context of international security are considered to be in line with the objectives of a strategy to combat threats in the information sphere, and to continue to explore relevant international concepts that are aimed at strengthening the security of global information and telecommunications systems. Consequently, the accent is made exclusively on a technical component – infringement of working capacity of information systems.

The development of affecting technologies informative space and the tendencies of prevalence of the emotional component of media content over information content did not pass over the attention of terrorist organizations. The definition of the main purpose of terrorism as intimidation to achieve one's goals testifies the use of means by abusers to influence the mass emotional, cognitive and information states.

Wide use of modern achievements in the field of mass media, use of technical means for disabling elements of state information infrastructures or using them for the purpose of disastrous influence on the vital activity of society is a quite logical and predictable step marked by a relatively new term: «information terrorism». Inability of citizens to be oriented in informative space, filled with fake is also obvious, and the possibilities of influencing their psychoemotional state and views become more and more simple in realization.

The need to impose will by means of direct violence has disappeared, giving way to information terrorism and, which requires the development of new approaches in the sphere of law, changing standards and approaches to information exchange and dissemination. Post-truth represents a large number of truths that match the views of information consumers, who become ambivalent to the truth. At present, Ukrainian legislation does not define information terrorism at all. Since only the term «cyberterrorism» is used for this purpose, the authors of the article, taking into account such formats of media content, which in the near future will contain almost one emotional component, leaving out the information component, separately proposed its clarification and provided a definition of «media terrorism».

The article reflects a new view on the standards and approaches to information exchange and dissemination. It is proved that it is necessary to rethink the definition of information terrorism and its components and their consolidation in the field of law. Confidence is expressed that the existing approaches to planning of counterterrorism measures in the near future will finally cease to be effective, since the use of modern methods of information influence by terrorists allows to cover a significant array of different social groups in their worldview and carry out artificial interference in the world order.

Legislation should be constantly updated to take into account the evolutionary processes of the phenomenon of terrorism and the regular review of the Concept of National Security of Ukraine. However, there is a dualistic problem of legal definitions: if the interpretation of terrorist activity is expanded, there is a threat of its unjustified use by political forces in the fight against opponents. Preventive measures should contain developments and introduction of evolutionary methods to strengthen the anti-terrorist consciousness of citizens. Scenarios of such actions should be planned at the strategic level, use achievements in information technologies and not be limited to tactical and operational tasks.

Besides, modern media are gradually losing their positions both in disseminating information and in influencing public opinion. The use of modern technologies has significantly increased the level of mobility and autonomy of individual groups and entire terrorist organizations, and allowed them to coordinate their actions not only in the regional but also on a global scale. Information terrorism is a direct influence on psyche and consciousness of people for the purpose of forming necessary opinions and judgments which in a certain way direct people's behavior. It becomes possible to use artificially created «public opinion» to pressure the authorities to make inadequate managerial decisions, which directly affects the security, economy and social sphere.

Defining a condition of modern threats of information terrorism, authors noted that it is a form of negative influence of all kinds of information on the person, a society and the state. Therefore, the important factors in the register of threats of terrorist character are the account of the general emotional background of society and level of social tension in the region of monitoring. Through appropriate compensatory measures, it is possible to neutralize or reduce the negative impact of terrorist threats (attacks), justify the very fact of information-terrorist actions and initiate criminal proceedings against organizers. At the same time, a leading social and educational component of countering media terrorism is becoming available, which makes it possible to implement proactive measures that are practically independent of the vectors of potential terrorist threats in the media sphere.

Therefore, according to the authors of the article, the resistance to media terrorism should contain three general directions: 1) counteraction in the legal sphere (legislation, criminal code, etc.); 2) counteraction in the technological sphere (means of detection, monitoring, localization, neutralization, etc.); 3) counteraction in the social and educational sphere (by increasing media literacy of the population). In order to successfully counter threats, the main directions of such counteraction have been identified: a) unification and harmonization of national legislation and international acts; b) scientific developments in the field of modern technologies for detecting and preventing criminal and terrorist impacts on information resources; c) Improvement of international organizational and legal cooperation in combating computer crime and computer terrorism; d) Improvement of a multi-level system for training personnel in the area of information security. In today's environment, an urgent need is to establish effective risk management of counter-terrorism security, to establish legislation and to clearly define the mechanisms for its functioning in times of peace and crisis. Intercultural dialogue through the mass media can help avoid the emergence of various types of extremism, radical violence, xenophobia, religious intolerance, separatism, terrorism, etc.