Електронне "**Державне управління: удосконалення та розвиток**"
включено до переліку наукових фахових видань України з питань державного управління
(Наказ Міністерства освіти і науки України від 22.12.2016 № 1604)
www.dy.nayka.com.ua | № 4 2018 р.

УДК 351.86:004:343.32/.34:327.88](477)

О. І. Жайворонок,
аспірант кафедри глобалістики, євроінтеграції та управління національною безпекою,
Національна академія державного управління при Президентові України, м. Київ

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ ПРОТИ УКРАЇНИ

O. Zhaivoronok,
post-graduate student of the Department of Globalistics, European Integration and National Security Management of the National Academy for Public Administration under the President of Ukraine

MODERN THREATS OF INFORMATION TERRORISM IN THE CONDITIONS OF HYBRID WAR AGAINST UKRAINE

В статті проаналізовано сучасні загрози інформаційного тероризму в Україні та джерела їх походження. Досліджено стійкість Українського народу до загроз інформаційного тероризму в умовах гібридної війни через призму безпеки людини, суспільства і держави. Зроблено висновок про те, що стан інформаційної безпеки України залежить від ефективного державного механізму, при якому спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне отримання інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдадуть суттєвої шкоди реалізації національних інтересів.

The article analyzes modern threats of information terrorism in Ukraine and sources of their origin. The resistance of the Ukrainian people to the threats of information terrorism in conditions of hybrid war is investigated through the prism of human, society and state security. It is concluded that the state of Ukraine's information security depends on the effective state mechanism in which special information operations, acts of external information aggression, information terrorism, illegal receipt of information by means of special technical means, computer crimes and other destructive information influence will not cause significant harm to the realization of national interests.

Ключові слова: *інформаційний тероризм, національна стійкість, державне управління, інформаційна безпека, гібридна війна, кібертероризм.*

Keywords: *information terrorism, national stability, public administration, information security, hybrid war, cyberterrorism.*

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими та практичними завданнями. Важливі реформи у нашій державі, викликані стрімким перебігом сучасних подій, починаючи з 2014 року, утвердили для України нові політичні та управлінські реалії. Гібридна війна Російської Федерації та наростаючі у світі різноманітні небезпеки, ключовим у яких є інформаційний чинник, формують довгострокові виклики для нашої країни. Загрози в інформаційній сфері зачіпають інтереси людини, суспільства та держави. Для України, яка зіткнулася з інформаційною складовою гібридної війни, питання забезпечення інформаційної безпеки набувають важливого значення. Зважаючи на це, розроблення та вдосконалення основ забезпечення інформаційної безпеки України є одним із найважливіших та особливо актуальних завдань держави. При цьому, багато проблем, пов'язаних із забезпеченням інформаційної безпеки, можуть бути успішно розв'язані лише в тісній скоординованій співпраці з міжнародними організаціями (ООН, ЄС, НАТО та ін.).

Ця обставина й визначає зв'язок загальної проблеми з найбільш важливими науковими та практичними завданнями сучасного державного управління у сфері інформаційної безпеки. Інформаційна безпека забезпечує безперешкодну реалізацію у суспільстві конституційних прав, які спрямовані на вільне одержання, створення й розповсюдження інформації. Відповідний рівень інформаційної безпеки необхідно забезпечити шляхом реалізації певних політичних, економічних та організаційних заходів, пов'язаних з попередженням, виявленням і нейтралізацією таких обставин, чинників і дій, що можуть завдати збиток чи перешкодити реалізації інформаційних прав, потреб та інтересів країни та її громадян.

Аналіз останніх досліджень і публікацій. Проведення аналізу сучасних загроз інформаційного тероризму в Україні та джерел їх утворення, а також вивчення стану наукової розробленості проблеми забезпечення інформаційної безпеки показало, що на сьогодні існує безліч наукових досліджень з цієї тематики. Так, В. Ліпкан, Ю. Максименко, В. Желіховський у своїй праці «Інформаційна безпека України в умовах євроінтеграції» глибоко аналізують і роблять очевидний висновок про те, що інформаційний тероризм застосовується з метою дезінформації, дезорієнтації і профанації для помилкового сприймання, помилкового розуміння і неадекватної поведінки суспільства [1, с.15].

Науковому осмисленню проблем реалізації інформаційної безпеки в сучасному суспільстві сприяли праці таких дослідників: А. Даллеса, М. Кастельса, В. С. Шапіро, Г. Ве- ріана, М. В. Баглая, А. В. Крутських, І. Л. Сафронова, О. А. Смірнова, Є. Б. Бєлова та ін. Серед українських дослідників, які розробляють методологічні засади інформаційної безпеки, слід відзначити таких, як: О. Г. Широкова-Мурараш, В. І. Гурковський, Г. М. Сащук, Г. Г. Почепцов, В. Г. Королько, О. П. Голобуцький, В. М. Брижко, В. С. Цимбалюк, Б. А. Кормич, Є. Я. Кравець, О. В. Олійник, Л. Є. Шиманський та ін. Відомий дослідник Фурашев В.М. визначає основні стримуючі фактори правового забезпечення інформаційної безпеки для України [4, с. 117-118].

Однак на сьогодні питання вироблення ефективних механізмів державного управління інформаційною сферою у контексті забезпечення безпеки людини, суспільства і держави залишаються відкритими і потребують подальших досліджень.

Формулювання цілей статті. Завданнями статті є здійснення аналізу сучасних загроз інформаційного тероризму в Україні та джерел їх формування у контексті забезпечення безпеки людини, суспільства і держави; окреслення чинників стійкості українського народу до загроз інформаційного тероризму в умовах гібридної війни; формулювання ознак ефективного державного механізму, спроможного адекватно реагувати та забезпечувати безпеку громадян від інформаційних загроз гібридної війни.

Виклад основного матеріалу дослідження. Останнім часом в Українській державі інституційному забезпеченню інформаційної безпеки загалом, та безпеці інформаційного простору зокрема приділяється особлива увага. Основними викликами та загрозами інформаційної безпеки для сьогодення є інформаційна війна, інформаційний тероризм і інформаційні злочини. Причиною тому є глобальні процеси інформатизації, прогрес у сфері розвитку інформаційних технологій та інформаційна складова гібридної війни РФ проти України.

Сучасний тероризм характеризується масштабністю здійснюваних терористичних атак, високим рівнем організації та фінансування, різким зростанням технічної і технологічної оснащеності (хакерські групи у РФ, терористичні організації «Хезболла», Хамас та ІГІЛ мають складну структуру, органи управління, свої теле- та радіостанції), що обумовлює появу його нових форм. З кожним роком збільшуються кількісні показники терористичної злочинності. Вкрай гострою залишається інформаційна складова гібридної війни РФ проти України, складовою якої є кібертероризм та втручання у критичну інформаційну інфраструктуру України вірусів-шпигунів, тощо.

Інформаційний тероризм як одна з форм сучасного тероризму відомий українським вченим ще з кінця XX століття, але до цих пір немає визначеності у розумінні його сутності і основних ознак. Інформаційний тероризм застосовується з метою дезінформації, дезорієнтації і профанації для помилкового сприймання, помилкового розуміння і неадекватної поведінки суспільства [1, с.15].

Тим часом, в умовах глобалізації суспільство потребує додаткового (правового, соціологічного, організаційного) осмислення відносин, що складаються у новій сфері, а також у захисті вітчизняного інформаційного простору. На сьогоднішній день вітчизняне законодавство у сфері забезпечення інформаційної безпеки розвинене слабо і в значній мірі відстає від рівня розвитку інформаційного суспільства.

Перші спроби вплинути на державному рівні на рівень інформаційного простору в Україні, пронизаного проросійською пропагандою були здійснені стосовно роботи українських медіа вже на початку війни на Донбасі. Наприкінці червня 2014 року у Нацгвардії з'явилося Управління інформаційної безпеки, а у грудні було створено Міністерство інформаційної політики України. В лютому 2015 року з'явився проект «Інформаційні війська України». Одним із завдань цього проекту було об'єднання «лідерів думок» і тролів з великою аудиторією в соцмережах з метою адекватної відповіді на інформаційні атаки Росії та формувати патріотичний порядок денний в онлайн-медіа. По суті, це була перша публічна спроба створити «дзеркальну відповідь» російській пропаганді на державному рівні.

Упродовж 2014–2016 рр. Національна рада з питань телебачення і радіомовлення заборонила мовлення на території України понад 70 російських каналів, а Держагентство з питань кіно відмовило в реєстрації і скасувало прокатні посвідчення на трансляцію понад 500 російських фільмів і серіалів.

Розвивалася й нормативно-правова база інформаційної безпеки. Так, Указом Президента України від 26 травня 2015 року № 287/2015 введено в дію рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України». Вона спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки, шляхом введення докорінних змін у зовнішньому та внутрішньому безпековому середовищі України, що обумовлює необхідність створення нової системи забезпечення національної безпеки України [2, с.1].

Хоча Стратегія й визначає пріоритети забезпечення інформаційної безпеки, кібербезпеки і безпеки інформаційних ресурсів, проте аналізуючи які можливо дійти висновку про їх поверхневий та загальний характер.

Рішенням Ради національної безпеки і оборони України від 29 грудня 2016 року, затвердженим Указом Президента України від 25 лютого 2017 року № 47/2017 введено в дію Доктрину інформаційної безпеки України (далі – Доктрину). Згідно Доктрини основні напрями державної політики в цій сфері повинні бути пов'язані з забезпеченням інформаційної безпеки, захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію, відкритості і прозорості держави перед громадянами, формування позитивного міжнародного іміджу країни, прийняттям на цій основі кримінально-правових, цивільно-правових та адміністративно-правових заходів протидії можливим загрозам [3, с. 2].

Публікація Доктрини інформаційної безпеки викликала неоднозначну реакцію в експертному середовищі й українському суспільстві взагалі. Спектр оцінок документа змінюється від визнання його важливості й упевненості, що доктрину слід було прийняти ще кілька років тому, до порівняння цього документа зі схожою доктриною інформаційної безпеки, яка була прийнята в Росії у грудні 2016 року.

Слід сказати, що останнім часом в Україні було розроблено значну кількість документів, що регламентують питання забезпечення захисту інформаційного простору. Проте більшість з них не мають певного юридичного статусу, а положення, які в них закріплені, не знаходять свого відображення в змісті вітчизняного законодавства.

Названі обставини ускладнюють можливість створення спільних профілактичних, попереджувальних і спеціальних кримінально-правових, адміністративно-правових, організаційних, економічних, технічних, технологічних та інших заходів протидії інформаційному тероризму.

Інформаційний простір використовується терористичними організаціями (спільнотами) з метою втручань в інформаційно-технологічні системи великих організацій і підприємств, фінансування терористичної діяльності, встановлення зв'язків між терористами, організації діяльності терористичних організацій (спільнот), пропаганди, вербування населення і т.п.

Розглядаючи стійкість українського народу, як нації (національну стійкість) до загроз інформаційного тероризму в умовах гібридної війни робимо висновок, що питання забезпечення інформаційної безпеки лежать у площині «забезпечення прав і свобод людини – забезпечення прав суспільства – забезпечення виконання функціональних обов’язків держави».

За словами дослідника Фурашева В.М. основними стримуючими факторами правового забезпечення інформаційної безпеки є:

- забезпечення інформаційної безпеки людини, суспільства, держави неможливе без об`єктивно вимушеного правового обмеження прав і свобод людини у сфері інформаційних відносин;

- правове обмеження прав і свобод людини збирати, зберігати, використовувати і поширювати інформацію повинно мати чітку, зрозумілу мотивацію вибору спрямованості цієї інформації та чіткі критерії, які дозволяють провести грань між дозволеним та обмеженим (забороненим) з максимальним ступенем об’єктивізму;

- визначальним під час створення та вдосконалення правових основ розвитку інформаційних технологій є чітке визначення об`єктів та суб`єктів права у всій його сукупності, виходячи з сутності явища, процесу, процедур тощо [4, с. 117-118].

Розвиваючи свою думку Фурашев В.М. небезпідставно вважає, що головним стримуючим фактором у сфері забезпечення інформаційної безпеки є природна непідготовленість людини, визначеної частки суспільства до сприйняття будь-яких обмежень, заборон у сфері інформаційних відносин. Подібні дії сприймаються як порушення демократичних цінностей, прав і свобод людини, повернення цензури у класичному значенні цього слова, не сприймаючи це як об’єктивну необхідність.

Серед основних факторів, що впливають на ефективність та адекватність механізму політики інформаційної безпеки, слід назвати, насамперед, загальні негативні тенденції системи державного управління, які, в більшості, були наслідувані ще від радянської системи, а в українських умовах набули гіпертрофованих і найбільш потворних форм. До цієї категорії можна віднести такі явища як: бюрократизм, значні масштаби корупції, недостатні моральні та професійні якості певної частини державних службовців та нерідко орієнтованість на задоволення власних потреб, а не потреб громадян і суспільства. Також слід відзначити вже сучасну національну українську проблему, яка пов’язана із неузгодженістю, незбалансованістю або недостатньою визначеністю компетенції багатьох органів влади, що призводить до зіткнення їх інтересів і ряду правових колізій.

Але найбільшою руйнівною силою, яка фактично нівелює всі спроби формування ефективної державної політики в сфері забезпечення інформаційної безпеки України, є корупція, яка «пронизала» майже всі органи державного управління та всі верстви населення. Основними визначальними чинниками поширення та зміцнення корупції є природа людської сутності та незадовільне соціально-економічне становище кожної конкретної людини.

Всі ці чинники дійсно негативно впливають на інформаційну безпеку, але для повного розуміння ситуації, що складається в вітчизняному інформаційному просторі, в якому співіснує Український народ слід приділити пильну увагу ще й такому явищу, як інформаційний тероризм та кібертероризм.

Учасники демократичного політичного процесу повинні мати у своєму розпорядженні важелі впливу, достатні для захисту своїх інтересів, але не достатні для монополізації влади. Якщо ці умови не витримуються, тобто порушуються базові цінності суспільства, в країні з демократичними правовими засадами може спостерігатися протиборство політичних сил, підкріплених народним резонансом. Останній, у свою чергу, може провокувати народ до радикальних дій – до проявів сепаратизму, екстремізму та навіть, дій терористичного характеру. До цього необхідно додати ще й військовий конфлікт на сході країни, спровокований агресивними діями РФ, вираженими в так званій гібридній війні, що в сою чергу породжує прояви терористичного характеру (у тому числі інформаційний тероризм) проти української влади, суспільства, людини. Високотехнологічні терористичні акції нової епохи здібні сьогодні продукувати системні кризи всієї світової спільноти і поставити під загрозу існування окремих регіонів світу, наприклад цілісності української держави.

Інформаційний фактор став невід'ємною складовою тероризму як суспільно-політичного явища, а дослідження останнього вказує на необхідність розвитку дієвого антитерористичного механізму, як складової загальнодержавної системи кризового реагування.

Отже, говорячи про національну стійкість в умовах гібридної війни, слід спочатку дослідити самі загрози терористичного характеру і вже потім говорити про захищеність від них, адже первинною є саме інформаційна загроза. Окрім того, необхідно звернути увагу на те, що для окремої особистості існують одні інформаційні загрози, для суспільства – інші, для держави – ще інші.

Є багато визначень поняття інформаційних загроз. Спробуємо їх не стільки узагальнити, як дати тлумачення через призму сьогодення української держави. Інформаційна загроза для України – це такий інформаційний тероризуючий вплив (внутрішній чи зовнішній) на свідомість та підсвідомість українців і українського народу, інформаційні ресурси, інформаційну складову об'єктів критичної інфраструктури країни, при якому створюється потенційна чи актуальна (реальна) небезпека нанесення шкоди життєво-важливим інтересам людини, суспільства та держави у цілому.

Інформаційні загрози є не тільки самостійним класом загроз, вони ще й слугують основою (першопричиною) для реалізації інших загроз терористичного характеру.

З проблемою інформаційних загроз тісно пов'язане поняття джерел загроз інформаційній безпеці. Джерела загроз інформаційній безпеці класифікуються за великою кількістю критеріїв, наприклад: відповідно від носіїв загроз, за місцем виникнення та локалізації, за сферою знаходження об'єкта загрози тощо.

Найбільш популярним є розподіл на внутрішні та зовнішні загрози інформаційної безпеки. Під внутрішніми загрозами розуміють відсутність історичного, політичного та соціального досвіду життя у правовій державі, що напряму відноситься до процесу практичної реалізації конституційних прав та свобод громадян, у тому числі в інформаційній сфері. До зовнішніх загроз належать діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері; політика домінування деяких країн в інформаційній сфері; діяльність міжнародних терористичних груп; розробка концепцій інформаційних війн будь-якими структурами; культурна експансія у відношенні до конкретної країни.

Основні реальні та потенційні загрози національній безпеці України, стабільності в суспільстві та в інформаційній сфері наведені у Законі України «Про основи національної безпеки України» [5, с. 1]. Але перелік цих загроз неповний, тому науковим суспільством було запропоновано розширити перелік основних загроз національній безпеці України в інформаційній сфері, що дає можливість для якісного проведення наукових досліджень та використання їх на практиці. Отже, до основних загроз національній безпеці України в інформаційній сфері віднесено:

- розповсюдження ідей, що провокують конфлікти на національному, релігійному, міжетнічному і соціальному підґрунті та масові заворушення, а також розпалювання серед українського народу ідей сепаратизму;
- заклики щодо спонукають на посягання, з боку окремих груп та осіб, на державний суверенітет, територіальну цілісність, економічний, науково-технічний і оборонний потенціал України;
- проведення, на шкоду національним інтересам України, спеціальних інформаційних операцій та актів зовнішньої інформаційної агресії;
- комп'ютерна злочинність;
- інформаційний та комп'ютерний тероризм;
- розвідувально-підривна діяльність іноземних спеціальних служб;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- дискредитація політики нашої держави та підрив авторитету органів державної влади та окремих державних діячів;
- прояви обмеження свободи слова і доступу до інформації, а також інші обмеження прав та свобод людини і громадянина, у даній сфері;
- поширення ЗМІ культу насильства, жорстокості, порнографії та інших проявів аморальності;
- намагання маніпулювати громадською думкою, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації;
- небезпечне, для економічної незалежності України, зростання частки іноземного капіталу у стратегічних галузях економіки, пов'язаних з інформаційною сферою;
- науково-технологічне відставання України від розвинутих країн;
- нерозвиненість внутрішнього ринку високотехнологічної продукції та відсутність його ефективного захисту від іноземної технічної і технологічної експансії;
- зниження внутрішнього попиту на підготовку науково-технічних кадрів для наукових, конструкторських, технологічних установ та високотехнологічних підприємств, незадовільний рівень оплати науково-технічної праці, падіння її престижу, недосконаліть механізмів захисту прав інтелектуальної власності;
- еміграція учених, фахівців, висококваліфікованих працівників за межі України;
- інспірування інших деструктивних процесів у інформаційній сфері нашої держави;
- постійно зростаюча кількість баз і банків даних, що містять персональні дані та вимог підприємств, установ та організацій різних форм власності стосовно надання персональних даних без належного обґрунтування та гарантій їх захисту.

Висновки та перспективи подальших досліджень. Підсумовую вищезазначене, можливо зробити висновок про те, що національна стійкість України до загроз інформаційного тероризму в умовах гібридної війни повинна лежати у площині трьох похідних: безпеки людини, суспільства та держави. Слід пам'ятати, шо вони взаємопов'язані між собою і вплив на одну з них може слугувати (провокувати) основою для впливу на інші. Так, захищеність психіки

та здоров’я людини від деструктивного інформаційного впливу забезпечить існування сприятливих можливостей для задоволення та реалізації життєвих, духовних і матеріальних потреб громадян, створить для них необхідний мінімум сталості, стабільності, соціального імунітету, готовності та здатності протистояти деструктивним впливам, небезпекам та загрозам життю, здоров’ю, майну, всій сукупності прав, свобод, законних інтересів. Забезпечити такий стан інформаційної захищеності українського народу повинен ефективний державний механізм, при якому спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне отримання інформації за допомогою спеціальних технічних засобів, комп’ютерні злочини та інший деструктивний інформаційний вплив не завдадуть суттєвої шкоди національним інтересам.

Визначені та обґрунтовані пріоритетні напрями аналізу інформаційної безпеки українського суспільства та удосконалення державного механізму реагування на виклики і загрози інформаційного тероризму не можна вважати закінченими. Очевидно, що удосконалення безпекових процесів у цій сфері вимагає подальших фахових дискусій науковців і практиків.

Список літератури.

1. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції / В. Ліпкан, Ю. Максименко, В. Желіховський [Електронний ресурс]. – Режим доступу: http://mobile.pidruchniki.com/15800119/politologiya/ponyattya_zmist_zagroz_informatsiyniy_bezpetsi

2. Указ Президента України від 26 травня 2015 року № 287/2015 про введенння в дію рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» [Електронний ресурс]. – Режим доступу: // http://zakon3.rada.gov.ua/laws/show/287/2015

3. Указ Президента України від 25 лютого 2017 року № 47/2017 про введення в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» [Електронний ресурс]. – Режим доступу: // http://www.president.gov.ua/documents/472017-21374

4. Фурашев В.М. Основні стримуючі фактори правового забезпечення інформаційної безпеки / В.М. Фурашев // Інформація і право. – 2013. – № 2 (8). – С. 117-118.

5. Закон України «Про основи національної безпеки України» [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/964-15

References.

1. Lipkan, V. Maksymenko, Yu. and Zhelikhovskyi, V. "Information Security of Ukraine in the Conditions of European Integration", [Online], available at: http://mobile.pidruchniki.com/15800119/politologiya/ponyattya_zmist_zagroz_informatsiyniy_bezpetsi

2. President of Ukraine (2015), Decree of the President of Ukraine "On the Strategy of National Security of Ukraine", available at: http://zakon3.rada.gov.ua/laws/show/287/2015

3. President of Ukraine (2017), Decree of the President of Ukraine "On the Doctrine of Information Security of Ukraine", available at: http://www.president.gov.ua/documents/472017-21374

4. Furashev, V.M. (2013), "The main constraints of the legal security of information security", *Informatsiia i pravo*, vol. 2 (8), pp. 117-118.

5. The Verkhovna Rada of Ukraine, The Law of Ukraine "On the Fundamentals of National Security of Ukraine", available at: http://zakon2.rada.gov.ua/laws/show/964-15

Стаття надійшла до редакції 18.04.2018р.