УДК 004.056:341
DOI https://doi.org/10.32689/2523-4625-2023-5(71)-6

Валерій КОТЛЯРОВ
докторант, Національний авіаційний університет, просп. Гузара Любомира, 1, Київ, Україна, 03058
ORCID: 0000-0002-2291-3199

Valerii KOTLIAROV
Doctoral Student, National Aviation University, 1, Huzara Lubomyra Ave, Kyiv, Ukraine, 03058
ORCID: 0000-0002-2291-3199

КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА МІЖНАРОДНІЙ БЕЗПЕЦІ

CYBERTERRORISM AS A THREAT TO INTERNATIONAL SECURITY

Стаття присвячена проблемі інформаційного тероризму у контексті загрози національній безпеці України. Визначено нормативно-правове закріплення інформаційного тероризму та окреслено суттєві прогалини в законодавстві України у регулюванні цього явища. Проведено аналіз та класифікацію видів інформаційного тероризму у сучасному глобальному кіберпросторі. Запропоновані деякі шляхи протидії інформаційному тероризму як чиннику дестабілізації національної безпеки України.

У статті досліджується феномен інформаційного тероризму на сучасному етапі. Увага сфокусована на такому понятті як кібертероризм, як основній складовій інформаційного тероризму. Висвітлено сутність даного явища, також охарактеризовано ступінь правового регулювання та запобігання інформаційному терору як на міжнародному, так і на національному рівні. Надано рекомендації, щодо запобігання інформаційного тероризму в Україні.

Зроблено висновки про те, що нині віртуальний простір та мас-медіа широко використовуються різними угрупованнями терористичного спрямування для досягнення власних цілей, оскільки доступність, відсутність цензури, наявність величезної потенційної аудиторії користувачів висока швидкість поширення інформації та комплексність її подання та сприйняття сприяють розширенню інформаційного тероризму у сучасному світі.

Аналізуються сучасні проблеми інформаційної безпеки в складі національної безпеки держави. Визначаються причини, що зумовлюють незадовільний стан у сфері забезпечення інформаційної безпеки. Особлива увага приділяється правовим основам забезпечення інформаційної безпеки та перспективам удосконалення законодавства, проблемам регулювання відносин у цій сфері. Успішний розвиток України як суверенної держави неможливий без забезпечення її національної безпеки. Інформаційна безпека суспільства і держави визначається мірою їх захищеності, а отже, стійкістю основних сфер життєдіяльності до небезпечних дестабілізуючих, деструктивних інформаційних дій, що утискають інтереси країни.

Загроза тероризму з використанням кіберпростору є комплексним викликом сучасності. Небезпека такого тероризму полягає у відсутності географічних та національних кордонів, а також у складності ідентифікації особистості терориста в інформаційному просторі та встановлення місця його перебування. Тому у зв'язку з подальшим розвитком технологій питання протидії інформаційному тероризму буде особливо актуальним.

Ключові слова: *інформаційний тероризм, загрози, національна безпека, кібертероризм, правове регулювання, нормативно-правове закріплення.*

The article is devoted to the problem of information terrorism in the context of threat to the national security of Ukraine. Author defines regulatory consolidation of information terrorism and outlines the significant gaps in the legislation of Ukraine in regulating this phenomenon. The article offers analysis and classification of information terrorism in today's global cyberspace. Author proposes some ways to counteract information terrorism as a factor of destabilization of Ukraine's national security.

This article examines the phenomenon of information terrorism at modern stage. The greatest attention is focused on concepts such as the media- and cyber-terrorism, which are the main component of information terrorism. In this article the essence of this phenomenon is reflected, as well as the degree of legal regulation and prevent terror information at both the international and national level are characterised. Also, the recommendations for the prevention of information terrorism in Ukraine are provided.

The article examines the phenomenon of informational terrorism at the current stage. The greatest respect is given to such concepts as media cyberterrorism, as the main warehouse informational terrorism. The article shows the essence of this phenomenon, and also characterizes the stage of legal regulation and the intimidation of terrorist information both on the international and on the national level. Also, recommendations were made on how to prevent information terrorism in Ukraine.

Conclusions were made that nowadays virtual space and mass media are widely used by various terrorist groups to achieve their own goals, as accessibility, lack of censorship, the presence of a huge potential audience of users, the high speed of information dissemination and the complexity of its presentation and perception contribute to the expansion of information terrorism in the modern world.

Modern problems of information security as part of the state's national security are analyzed. The reasons for the unsatisfactory state of information security are determined. Special attention is paid to the legal basis of ensuring information security and prospects for improving legislation, problems of regulating relations in this area. Successful development of Ukraine as a sovereign state is impossible without ensuring its national security. The information security of society and the state is determined by the degree of their protection, and therefore, the resistance of the main spheres of life to dangerous destabilizing, destructive information actions that oppress the interests of the country.

The threat of terrorism using media and cyberspace is a complex challenge of our time. The danger of such terrorism lies in the absence of geographical and national borders, as well as in the difficulty of identifying the identity of the terrorist in the information space and establishing his whereabouts. Therefore, in connection with the further development of technologies and mass media, the issue of combating information terrorism will be particularly relevant.

Key words: *information terrorism, threats, national security, cyberterrorism, legal regulation, regulatory and legal consolidation.*

Постановка проблеми. Проблема кібертероризму носить глобальний характер та є особливо актуальною в сучасному інформаційному суспільстві. За відносно короткий проміжок часу кібератаки перетворилися з окремого випадку на одну з головних загроз інформаційній безпеці держави. У глобальному контексті великі держави світу приділяють все більше уваги захисту критично важливих інформаційних ресурсів і можливості впливу на інформаційні ресурси інших держав. Більшість країн проводить активну роботу з аналізу потенційних можливостей подібних загрозі та розробки засобів для боротьби зі ними. Однак, незважаючи на це, все ще існує низка проблем, які країнам слід вирішити як у національних сегментах, так і в усьому кіберпросторі.

В умовах швидкого поширення глобалізаційних процесів в макроекономічному просторі зростають можливості інформаційного впливу на особу, суспільство та державу. Безперервне широкомасштабне поширення інформації сприяє її розповсюдженню на великі території в найкоротші терміни. Хоч це і вважається одним з важливих досягнень людства, та все ж має свої недоліки, оскільки глобалізована інформатизація збільшує можливості виникнення інформаційних загроз. Інформаційна епоха розширила сферу поширення інформаційно-комунікативних воєн, що призвело до появи інформаційного тероризму, які засобу ведення інформаційної війни, що поєднав у собі біфуркаційні процеси фізичного тероризму, скорельованого в інформаційних системах та умисним зловживанням кіберпростором, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій. Інформаційний тероризм набув нових загрозливих форм, а його швидке поширення стало наслідком зомбіювання соціуму та активізації сепаратистського руху, що в кінцевому результаті може стати причиною втрати суверенітету, незалежності та територіальної цілісності окремої держави.

Мета статті. Виходячи з викладеного, формування механізму стратегічної безпеки підприємства має бути невід'ємною частиною його стратегії або стратегічного плану, інструментом мінімізації загроз та визначення можливостей подальшого існування та розвитку підприємства.

Феномену інформаційного тероризму присвячено праці як зарубіжних, так і вітчизняних науковців. Серед теоретиків та практиків, які займалися дослідженням інформаційного тероризму як засобу ведення інформаційної війни в умовах транскордонних глобалізованих процесів та розвитку інформаційного кіберпростору, слід зазначити Д. Белла, Ж. Бодрійара, Е. Гіденса, М. Кастельса, Е. Тоффлера, Ф. Фукуяму, С. Хантінгтона, Б. Хофмана, А. Шміда та ін. Дослідженню окремих проблем тероризму та його похідної – інформаційного тероризму, розробки та застосування заходів протидії цьому негативному явищу приділялася увага у роботах таких українських фахівців, як С. Бучик, В. Войтович, М. Грайворонський, Р. Гриник, Р. Грищук, М. Зубок, В. Ліпкан, Ю. Максименко, Г. Почепцов, І. Рижов, А. Форос. Однак необхідно зауважити, що комплексний аналіз цього феномену потребує подальших наукових досліджень у контексті його нормативно-правового закріплення.

Виклад основного матеріалу. Серед глобальних проблем сучасності, до яких привернуто увагу ООН, інших авторитетних міжнародних організацій (ОБСЄ, НАТО, ЄС), політичних лідерів, науковців, широкої громадськості, є проблема об'єктивного ускладнення структури міжнародних відносин, проникаючі контакти цивілізацій і відповідно проблема глобальної міжнародної безпеки, тобто підтримання сталого миру, попередження конфліктів, уникнення нової гонки озброєнь із використанням новітніх науково-технологічних досягнень.

Проблеми глобальної безпеки посідають особливе місце в інформаційному суспільстві.

Впливаючи на сучасний стан міжнародного розвитку, вони можуть поставити під загрозу забезпечення світопорядку, реалізацію стратегій становлення глобального інформаційного (інтелектуального) суспільства, навіть саме існування цивілізації. Глобальна безпека як чинник міжнародних відносин, вплив якого має універсальний характер і врахування якого в діяльності міжнародного співтовариства та в зовнішній політиці окремих держав призводить до радикальних змін у поведінці акторів міжнародних відносин, до трансформації самої сутності проблеми безпеки після закінчення «холодної війни" і розпаду біполярної міжнародної системи, потребує концептуального перегляду принципів функціонування міжнародних та національних інститутів, що відповідають за безпеку, а також врахування в нових доктринах інформаційної складової міжнародного співробітництва [1].

Вважають, що глобальна система міжнародних відносин буде розвиватися під впливом різнопланових факторів: «шестиполюсного світу» з центрами сили у США, Європі, Китаї, Японії, Росії, Індії (Г. Кіссінджер, М. Лібіцкі), трансформації і протиборства цивілізацій на основі концепції національної і культурної самобутності (С. Хантінтон), «однополюсного світу» (американоцентристська модель) як визнання лідерства США у становленні нового глобального світопорядку (Б. Бузан, А. Гіршман, З. Бжезинський), впровадження концепції «м'якої сили" (soft power) як інструменту вирішення майбутніх конфліктів (Б. Беркович Л. Джонсон Р. Шафрански, Дж. Най, У. Оуенс, О. Шерман), безконфліктності міжнародного розвитку і відмови від доктрини раціональності воєн і збройних конфліктів, забезпечення транспарентності усієї системи міжнародних відносин та її складових ресурсів для безпечного і безупинного прогресу глобальної спільноти (К. Аннан, Ф. Фукуяма, Ч. Шаохуа, Р. Інглегарт).

Різними способами провідні країни досить ефективно реалізують національну політику інформаційної безпеки. Найсучасніші та найнадійніші системи захисту інформації діють у Сполучених Штатах Америки, Ізраїлі, Німеччині, Великій Британії та Китаї. Таким чином, у країнах, що постійно перебувають під сильним зовнішнім інформаційним впливом і тому змушені створювати національні системи захисту. Останні мають досить активну складову, завдяки якій можна проводити інформаційні та психологічні заходи та кібератаки проти країн-противників [2].

Система інформаційної безпеки Сполучених Штатів Америки є особливо ефективною. Її система має достатню широку основу, яка охоплює всі верстви життєдіяльності, через що вона досить багатовимірна, водночас підпорядкована єдиній стратегії. Законодавство досить відповідально регулює питання забезпечення безпекиі інформації в державних комп'ютерних системах, боротьби з кіберзлочинами, регулювання праві громадян на доступ до інформації та таємниці особистого життя.

1. Закон «Про комп'ютерну безпеку».
2. Закон «Про вдосконалення інформаційної безпеки».
3. Закон «Про комп'ютерне шахрайство та зловживання».
4. Закон «Про зловживання комп'ютерами».
5. Закон «Про свободу інформації».
6. Закон «Про висвітлення діяльності уряду».
7. Закон «Про охорону особистихі таємниць».

Адміністративно-організаційна система забезпечення та реалізації інформаційної безпеки в США спрямована на координацію всіх дій щодо захисту інформації та реалізацію єдиної державної політики. Президент Сполучених Штатів Америки є головною відповідальною особою за забезпечення та реалізацію національної інформаційної безпеки. Інші європейські країни, які мають досить високий рівень життя, також приділяють багато уваги на розвиток інформаційної безпеки, ґрунтуючись на власній національній політиці та принципах захисту населення від неминучих у сучасному інформаційному суспільстві загроз і небезпек [3].

У Франції сфера забезпечення інформаційної безпеки разом із інформаційним сектором є дуже важливою сферою життя разом із економікою, політикою та культурою.

Отже, інформаційна сфера має такий високий рівень захисту, як і інші сфери життєдіяльності. Звідси можна дійти невтішного висновку, що саме тут концепція сучасної багатовекторної геостратегії французької правлячої еліти відбиває новий елемент, що безпосередньо впливає на оперативне прийняття рішень державних чи недержавних організацій, ЗМІ, і навіть національних спеціальних служб, що у процесі впровадження та реалізації стратегії. Таким чином, інформаційний простір у Франції вважається одним із пріоритетних об'єктів захисту, що забезпечуються всіма можливими законодавчими, організаційними, адміністративними, владними таі інформаційними технологіями [4].

На міжнародному рівні було запропоноване підтвердити керівну роль ООН щодо розробки міжнародних принципів інформаційної безпеки, сприяти координації діяльності міжрегіональних та регіональних структур зі попередження злочинного використання ІКТ. На національному рівні визначено за доцільне прийняти відповідні закони, зокрема про захисті секретної інформації, приватної інформації в процесі автоматизованої обробки даних, встановити кримінальну відповідальність за руйнування, модифікацію та викрадення комп'ютерних даних, або передачі інформації щодо питань національної безпеки, безпеки ІКТ-систем та функціонування органів державної влади, укласти двосторонні міжнародні угоди (Польща веде переговори з ФРН, Угорщиною, Словаччиною, Україною, Францією, Естонією) про захист інформації щодо медичних даних, інтелектуальної власності, наукових досліджень від будь-якого несанкціонованого втручання, включаючи незаконні банківські та фінансові операції. Йорданія, Катар також підтвердили необхідність розробки міжнародно-правових принципів щодо інформаційної безпеки, включивши до переліку загроз: «шпіонаж» (попередження несанкціонованого доступу до змісту ІКТ-систем); «саботаж» (попередження часткового або повного знищення ІКТ-систем); «підробку» (попередження підробки інформації в глобальному кіберпросторі). Від імені урядів цих держав було запропоновано ухвалити концепцію міжнародної інформаційної безпеки і сприяти підтриманню системи сталого миру. Найбільш розгорнута відповідь на вербальну ноту від Генерального секретаря ООН та пропозиції надійшли від Російської Федерації, що представила на розгляд Асамблеї типологію термінів (інформаційний простір, інформаційні ресурси, інформаційні війни, інформаційна зброя, інформаційна безпека, загрози інформаційної безпеки, міжнародна інформаційна безпека, неправомірне використання ІКТ-систем та ресурсів, несанкціоноване втручання в ІКТ-системи та ресурси, критично важливі структури, міжнародний інформаційний тероризм, міжнародна інформаційна злочинність) та принципи взаємодії держав у сфері міжнародної інформаційної безпеки [5]. Серед них:

Принцип 1. Діяльність кожної держави та інших суб'єктів міжнародного права у міжнародному інформаційному просторі повинна сприяти загальному соціальному та економічного розвитку і здійснюватися таким чином, щоб відповідати завданням підтримання сталого миру і безпеки, суверенних прав інших держав, інтересам безпеки, принципам мирного врегулювання спорів та конфліктів, незастосування сили, невтручання у внутрішні справи, поваги до прав і свобод людини.

Така діяльність повинна відповідати праву кожного шукати, отримувати та поширювати інформацію та ідеї, як це зафіксовано у документах ООН, з врахуванням того, що таке право може бути обмежене законом з метою захисту інтересів національної безпеки кожної держави.

При цьому кожна держава та інші суб'єкти міжнародного права повинні мати рівні права на захист своїх інформаційних ресурсів та критично важливих структур від неправомірного використання; несанкціонованого інформаційного втручання і можуть сподіватися на підтримку світового співтовариства у реалізації цих прав.

Принцип 2. Держави повинні прагнути до обмеження загроз у сфері міжнародної інформаційної безпеки і з цією метою утримуватися від: розробки, створення і використання засобів впливу і завдання шкоди інформаційним ресурсам і системам іншої держави; спрямованого інформаційного впливу на критично важливі структури іншої держави; інформаційного впливу з метою руйнування політичної, економічної та соціальної системи інших держав і задля дестабілізації суспільства; несанкціонованого втручання в інформаційно-телекомунікаційні системи та інформаційні ресурси, їх неправомірне використання; дій, що сприяють домінуванню і контролю в інформаційному просторі; протидії доступу до новітніх ІКТ, створення умов технологічної залежності у сфері інформатизації як загрозу іншим державам; заохочення дій міжнародних терористичних, екстремістських і злочинних угрупувань, що загрожують інформаційним ресурсам та критично важливим структурам інших держав; розробки та ухвалення планів, доктрин, які передбачають ведення інформаційних воєн, здатних спровокувати гонку озброєнь, а також викликати напруженість у відносинах між державами і самих інформаційних воєн; використання ІКТ проти основних прав і свобод людини, що реалізуються в інформаційній сфері; транскордонного поширення інформації, яка суперечить принципам і нормам міжнародного права, а також внутрішньому законодавству конкретних країн; маніпулюванню інформаційними потоками, дезінформації та засекречування інформації з метою викривлення психологічного і духовного середовища суспільства, ерозії традиційних культурних, моральних та етичних і естетичних цінностей; інформаційної експан-

сії, монополії в національних інформаційних системах інших держав, включаючи умови їх функціонування в міжнародному інформаційному просторі [6].

Принцип 3. ООН та її спеціалізовані установи сприятимуть міжнародному співробітництву, метою якого є обмеження загроз у сфері міжнародної інформаційної безпеки і формування відповідної міжнародно-правової бази для: визначення ознак та класифікації інформаційних воєн; визначення ознак і класифікації інформаційних озброєнь і засобів відповідного призначення; обмеження обігу інформаційних озброєнь; заборону розробки, поширення і використання інформаційної зброї; попередження загрози виникнення інформаційної війни; визнання безпеки застосування інформаційної зброї щодо критично важливих структур як зброї масового ураження; створення умов для рівноправного і безпечного міжнародного інформаційного обміну на основі загальновизнаних норм і принципів міжнародного права; попередження використання інформаційних технологій і засобів впливу на суспільну свідомість з метою дестабілізації суспільства і держави; розробки процедури взаємного інформування та попередження транскордонного несанкціонованого інформаційного впливу; створення системи міжнародного моніторингу для відстеження загроз в інформаційній сфері; створення міжнародної системи сертифікації технологій і засобів інформатизації і телекомунікацій (в тому числі програмно-технічних) щодо гарантій їх інформаційної безпеки; створення механізму контролю виконання умов режиму міжнародної інформаційної безпеки; створення механізму врегулювання конфліктних ситуацій у сфері інформаційної безпеки; розвитку систем міжнародної взаємодії правоохоронних органіві з попередження і припинення правопорушень в інформаційному просторі; гармонізації на добровільній основі національних законодавстві для забезпечення міжнародної інформаційної безпеки.

Принцип 4. Держави та інші суб'єкти міжнародного права повинні нести міжнародну відповідальність за діяльність в інформаційному просторі, яка здійснюється ними, під їхньою юрисдикцією або у межах міжнародних організацій, членами якої вони є і за відповідність такої діяльності принципам, що містяться у цьому документі.

Принцип 5. Будь-які спори між державами та іншими суб'єктами міжнародного права, які виникають при застосуванні цих принципів, регулюються за допомогою встановлених процедур мирного врегулювання спорів. 55 сесія ГА ООН прийняла Резолюцію 55/28 (A/RES/55/28) від 20.11.2000 р. «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», в якій, посилаючись на попередні резолюції про роль науки і техніки в контексті міжнародної безпеки та відзначаючи відповіді держав щодо оцінки проблем інформаційної безпеки, закликає всі держави-члени ООН сприяти на багатосторонній основі подальшому розгляду концепцій глобальної інформаційної безпеки та загроз у сфері ІКТ для завершення дискусії і ухвалення міжнародної конвенції з інформаційної безпеки. 56 сесія ГА ООН розглянула доповіді Генерального Секретаря та представника Першого комітету С. Екундайо Рове (Сьєра-Леоне) щодо визнання інформаційної безпеки глобальною проблемою, обговорила відповіді держав щодо загальної оцінки, визначення основних критеріїв і змісту відповідних міжнародних концепцій і прийняла резолюцію 56/19/A/PES/56/19) від 29.11.2001 р. «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», в якій відзначено, що поширення і використання інформаційних технологій і засобів торкається інтересів всього міжнародного співтовариства. Ці технології і засоби потенційно можуть бути використані з метою нестабільності міжнародної безпеки як у воєнній, так і у цивільній сферах, тому необхідно проведення міжнародної зустрічі експертів для конкретизації сутності проблеми міжнародної інформаційної безпеки та її правового забезпечення. Серед відповідей держав (Болівія, Мексика, Філіппіни та Швеція) особливу увагу привертає позиція держав Європейського союзу, в якій підкреслюється, що країни ЄС підтримали ухвалену консенсусом резолюцію 55/28 ГА ООН «Досягнення у сфері інформації і телекомунікацій в контексті міжнародної безпеки» [7].

Щодо загальної оцінки проблеми інформаційної безпеки, то ЄС вважає, що ІКТ сприяють вільному потоку інформації, демократизації суспільства та економічному прогресу. ЄС визнає, що існують потенційні загрози неправомірного та несанкціонованого використання ІКТ у різних сферах життєдіяльності держав, що створює небезпеку для міжнародної безпеки. Щодо змісту міжнародних концепцій про безпеку глобальних ІКТ-систем ЄС підкреслює, що, незважаючи на ефективність міжнародного співробітництва у сфері інформаційної безпеки, в першу чергу кожна держава має право і несе відповідальність за захист власних інформаційних ресурсів та інформаційних систем. Існуючі

ризики мають транскордонний характер, і будь-які превентивні заходи, спрямовані на обмеження потенційних втрат від злочинного чи терористичного нападу, зокрема і для міжнародної безпеки, повинні здійснюватися з урахуванням захисту ІКТ-ресурсів та систем. ЄС вважає, що саме ООН має стати основним форумом з обговорення проблем міжнародної інформаційної безпеки [8].

Як вже вище зазначалося, що становлення інформаційної цивілізації, що супроводжується динамічними поширенням новітніх комп'ютерних технологій, спричинило появу як нових позитивних перспектив подальшого розвитку світової спільноти, так й появу низки глибоких проблем у сфері суспільної безпеки. Передусім, це стосується інформаційних загроз терористичного характеру. У науковій літературі цей феномен набув назви, «інформаційний тероризм», який загалом тлумачиться як дії з дезорганізації інформаційних систем, що створюють небезпеку загибелі людей, завдання значного майнового збитку або інших суспільно небезпечних наслідків, якщо вони здійснені з метою порушення суспільної небезпеки, залякування населення або впливу на прийняття рішень органами влади, а також як політично вмотивовані хакерські операції, з тяжкими наслідками для функціонування державних і суспільних систем, зорієнтований на широке висвітлення в засобах масової інформації та спричинення суспільного резонансу [9].

Дослідники проблеми кібертероризму виокремлюють, зокрема, вісім основних способів використання терористами Інтернет-сайтів [10]: а) ведення психологічної війни, б) пошук необхідної інформації, в) навчання терористів, г) збирання коштів, д) пропаганда тероризму, е) вербування кадрів, є) організація мережі, ж) планування та координування дій. У своїй психологічній війні за вплив на громадську думку терористи основну ставку роблять саме на активне використання мережі «Інтернет», за допомогою чого вони намагаються поширити загрози, ескалацію страху, відчуття неминучості тощо. Для цього демонструються кадри вчинених терактів та їх жертв (наприклад, показ жорстокого вбивства в Іраку американського журналіста Даніеля Пірла, що транслювався паралельно на кількох вебсайтах). Небезпеку становлять і поширені хакерські атаки на інформаційні системи з метою виведення їх з ладу та здійснення на аудиторію впливу протерористичного характеру.

На нашу думку, протистояння сучасному кібертероризму обмежує той факт, що так званий, терористичний «Інтернет» у глобальному інформаційному просторі є динамічною системою, що постійно змінює свою зовнішню конфігурацію і орієнтована, передусім, на створення міфологізованого образу мужнього борця за віру і справедливість. У цьому сенсі мережа «Інтернет» з успіхом використовується терористичними організаціями: справляє відповідний вплив не лише на формування громадської думки, але інколи під цей вплив попадає і частина експертів [11].

Особливістю сучасної інформаційної терористичної мережі є також те, що сполучені горизонтальні ланки, які виходять від автономних користувачів, багато раз переплітаються, а вчинювані акції мають анонімний характер. Саме завдяки активному використанню ресурсів сучасного інформаційного простору новітній тероризм набув системних вимірів, успішно реалізуючи свою стратегію і тактику за допомогою застосування так званих дифузійних війн (коли відбувається дифузія часових і просторових меж різних конфліктів). «Новий тероризм» будує свою стратегію з урахуванням тенденцій розвитку нинішніх глобалізаційних процесів, зокрема, вдало використовуючи при цьому їхні конфлікти та кризові явища [12].

У цілому кіберзагрози можуть існувати як для військової (оборонної), так і для цивільної інфраструктури. Наприклад, в атомній енергетиці зміна інформації або блокування інформаційних центрів може спричинити припинення подачі електроенергії у міста і на військові об'єкти, викликати ядерну катастрофу, перекручування інформації або блокування інформаційних систем у фінансовій сфері може призвести до економічної кризи, а виведення з ладу систем керування військами та військовою технікою здатне спровокувати початок бойових дій, стати причиною втрат серед цивільного населення і військових, крім того, колосальні людські втрати та екологічна криза можуть бути наслідками терористичного втручання в роботу транспортних систем, об'єктів біологічної або хімічної промисловості [13].

Водночас деякі експертиі недооцінюють можливі наслідки застосування високих технологій з терористичноюі метою, заявляючи про те, що терористична атака, здійснена за допомогою Інтернету, навряді чи здатна призвести до масової загибелі людей і не може порівнюватися із загрозами хімічного, бактеріологічного чи ядерного тероризму. Допускаючи, що такий теракт матиме менш серйозні наслідки і не завдасть суспільству руйнівного впливу, як традиційний терористичний акт,

високі технології у діяльності терористичних угруповань можуть стати досить грізною і вигідною для них зброєю. Фахівці вважають, що кібертероризм може супроводжувати традиційні терористичні дії, оскількиі порушення в роботі, наприклад, систем зв'язку або інформаційних мереж критичних інфраструктур країни можуть посилити їх ефект і викликати паніку у суспільстві. Крім того, такі порушення можуть серйозно ускладнення проведення відновлюваних робіт після теракту.

Очевидно, що проблема кібертероризму є більш актуальною для постіндустріальних інформаційно розвинених країн, про що свідчать кібератаки проти компаній «Дженерал Електрік» і «Нешнл Бродкастінг Корпорейшин» у листопаді 1994 року, коли на кілька годин було порушено роботу внутрішніх інформаційних мереж, а відповідальність за цю акцію взяла на себе організація «Фронт визволення Інтернету», оголосивши цим компаніям кібервійну. За повідомленнями британських ЗМІ, на початку 1999 року було захоплено керування військовими телекомунікаційним супутником серії Скайнет та змінено його орбіту, а терористичні угруповання вимагали від британської влади викуп за порушення втручання в керування супутником, незважаючи на те, що подібні дії могли спровокувати збройний конфлікт [14].

Розглядаючи це питання, не варто забувати про те, що у реальності відмічається поява і активізація прихованого (латентного) тероризму – терористичних актів, замаскованих під стихійні лиха, епідемії, нещасні випадки і техногенні катастрофи. Метою прихованого тероризму може бути поширення за допомогою сучасних інформаційно-комунікаційних технологій паніки і відчаю серед населення, тобто створення терористами вигідної соціально-політичної ситуації у країні чи регіоні, адже ефект від прихованого тероризму не обов'язково проявляється відразу, а відбувається повільне руйнування країни і суспільної свідомості терористичними угрупованнями.

Наразі не варто й переоцінювати масштаби і можливості інформаційного тероризму. Зокрема хакерські атаки ісламістських кібертерористів, на переконання директора відділу технологічної політики Центру стратегічних і міжнародних досліджень США Дж. Льюїса, не завдають істотних збитків, а Дослідницька служба Конгресу Сполучених Штатів вважає, що взагалі терористам вигідніше вчинювати традиційні теракти, ніж розраховувати на проблематичні дивіденди від ведення кібервійни. На користь таких висновків свідчить й те, що розпорошений, дисперсійний характер присутності терористів у мережі не дає можливості контролювати їхні дії, а надає лише загальний ідеологічний, морально-психологічний і технологічний імпульс діям індивідуальних агентів терору і замкнутих бойових груп. Аморфність анонімних зв'язків, структурна розпливчатість обрисів номінально організованих груп створюють підґрунтя для потенційної внутрішньої роз'єднаності.

Висновки. Підсумовуючи, зазначимо, що друга половина XX – початок XXI століття знаменувала новий етап розвитку суспільства, спричинений потужною хвилею науково-технічної революції, розвитком нових інформаційних та телекомунікаційних технологій, що у підсумку змінили спосіб життя людини, виробничі відносини, методи управління, ціннісні орієнтації, свідомість планетарного масштабу. Водночас, епоха Інтернету відкрила необмежені можливості для терористичних організацій, який став використовуватися як справжня зброя. Маючи у своєму арсеналі власні ЗМІ, радіо- і телестанції, свої інтернет-сайти, терористи вміло пристосовуються до надбань інформаційної революції, поширюючи свою ідеологію та політичну пропаганду серед величезної аудиторії. Практично ця діяльність через легкість доступу, відсутність цензури, анонімність вийшла з-під контролю як окремих країн, так і впливових міжнародних інституцій. Тому світова спільнота через останніх має сформувати ефективне правове поле, скоординувати свої зусилля та дії, аби запобігти діяльності таких небезпечних організацій, якими є терористичні угрупування, або ж мінімізувати їхню силу впливу.

Нині найбільшу проблему складає відсутність законодавства, в якому було б чітко визначено це поняття, передбачено відповідальність за протиправні діяння. Пріоритетним напрямом у боротьбі з кібербтероризмом є організація зусиль та взаємовідносин правоохоронних органів із спецслужбами, судовими органами, спрямовані на протидію і розслідування таких видів злочинів, як кібертероризм, а також потреба у вдосконаленні законодавчої бази України.

Література:

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». УКАЗ Президента України № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 12.04.2022).

2. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України № 3475-IV від 23.02.2006 р. Верховна Рада України. Відомості Верховної Ради України. 2006, № 30, ст. 258. URL: https://zakon.rada.gov.ua/laws/show/3475-15iText (дата звернення: 10.11.2022).

3. Киричок Р.В., Складанний П.М., Бурячок В.Л., Гулак Г.М., Козачок В.А. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення. *Наукові записки Українського науково-дослідного інституту зв'язку.* № 3, 2016. С. 48–61.

4. Гораш І.А., Січко Т.В. Аналіз популярних корпоративних інформаційних систем. *Комп'ютерні технології обробки даних.* 2020. С. 26–30.

5. Вітер М.Б. Технологія побудови оптимальної моделі сховища даних у державних органах. *Науково-технічна інформація.* № 1. 2014. С. 35.

6. Бучик С.С. Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів. *Захист інформації.* 2016. № 1. С. 81–89.

7. W. Ten, G. Manimaran, and C.C. Liu, "Cybersecurity for criticalinfrastructures : Attack and defense modeling", IEEETrans. Syst., Man Cybern. A, vol. 40, no. 4, pp. 853–865, 2020.

8. Борсуковський Ю.В., Борсуковська В.Ю. Рекомендації по категоріюванню інформації з обмеженим доступом. *Сучасний захист інформації.* № 4. 2017. С. 9–17.

9. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В.Л. Бурячок, С.В. Толюпа, В.В. Семко та ін.]. К. : ДУТ-КНУ, 2016. 178 с.

10. Hryshchuk R. Construction methodology of information security system of banking information in automated banking systems : monograph / R. Hryshchuk, S. Yevseiev, A.Shmatko // Vienna: Premier Publishing s. r. o., 2018. 284 p.

11. Information Systems Audit and Control Association (ISACA). IT-Governance and Process Maturity. URL: https://www.isaca.org/bookstore/it-governance-and-business-management/wgpm (дата звернення: 13.03.2022).

12. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція «Інформаційна безпека в сучасному суспільстві». 24–25 листопада 2016 р. Львів : ЛДУБЖД, 2016. С. 23–24.

13. Грайворонський М.В. Сучасні підходи до забезпечення кібернетичної безпеки / Матеріали XVII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики», НТУУ «КПІ», 2015 р.

14. Danko Y. I. & Reznik N. P. (2019). Contemporary challenges for China and Ukraine and perspectives for overcoming these challenges. Global Trade and Customs Journal, 14(6).

15. Reznik N., Hridin O., Chukina I., Krasnorutskyy O., Mykhaylichenko M. (2022). Mechanisms and tools of personnel management in institutional economics // AIP Conference Proceedings. 2413, 040012 https://doi.org/10.1063/5.0089330.

16. Про боротьбу з тероризмом : Закон України від 20.03.2003 р. № 638-IV (зі змін.та доп.). URL: https://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 20.03.2019).

17. Про основні засади забезпечення кібербезпеки України : Закон України VIII від 05.10.2017 р. № 2469-VIII (зі змін. та доп. від 21.06.2018). URL: https://zakon.rada.gov.ua/laws/show/ru/2163-19/sp:max100 (дата звернення: 20.03.2019).

18. Конвенція про кіберзлочинність : Закон України від 07.09.2005 р. № 994_575 (зі змін.та доп.). URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 20.03.2019).

19. Проєкт Закону про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм від 24.07.2015 р. № 2439а. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JH1VR68A.html (дата звернення: 20.03.2019).

20. Грищук Р.В. Основи кібернетичної безпеки: Монографія / Р.В. Грищук, Ю.Г. Даник. Житомир: ЖНАЕУ, 2016.

References:

1. On the decision of the National Security and Defense Council of Ukraine dated December 29, 2016 "On the Information Security Doctrine of Ukraine". Decree of the President of Ukraine No. 47/2017. Retrieved from https://www.president.gov.ua/documents/472017-21374 (accesse date: 04/12/2022).

2. On the State Service of Special Communications and Information Protection of Ukraine: Law of Ukraine No. 3475-IV dated 23.02.2006 Verkhovna Rada of Ukraine. Information of the Verkhovna Rada of Ukraine. 2006, No. 30, Art. 258. Retrieved from https://zakon.rada.gov.ua/laws/show/3475-15iText (access date: 11/10/2022).

3. Kyrychok R.V., Skladanniy P.M., Buryachok V.L., Gulak H.M., Kozachok V.A. (2016). Problems of ensuring security control of corporate networks and ways to solve them. Scientific notes of the Ukrainian Research Institute of Communications. No. 3, P. 48–61.

4. Horash I.A., Sichko T.V. (2020). Analysis of popular corporate information systems. Computer technologies of data processing. P. 26–30.

5. Wind M.B. (2014). The technology of building an optimal model of data storage in state bodies. Scientific and technical information. No. 1. P. 35.

6. Buchyk S.S. (2016). Methodology of risk analysis of the tree of identifiers of state information resources. Protection of information. No. 1. P. 81–89.

7. W. Ten, G. Manimaran, and C.-C. Liu. (2020). "Cybersecurity for critical infrastructures : Attack and defense modeling," IEEETrans. Syst., Man Cybern. A, vol. 40, no. 4, pp. 853–865.

8. Borsukovsky Yu.V., Borsukovsky V.Yu. (2017). Recommendations for categorizing information with limited access. Modern information protection. No. 4. P. 9–17.

9. Buriachok V.L. (2016). Information and cyberspace: security problems, methods and means of combating them: manual / [V.L. Buriachok, S.V. Tolyupa, V.V. Semko et al.]. K.: DUT-KNU, 178 p.

10. Hryshchuk R. (2018). Construction methodology of information security system of banking information in automated banking systems: monograph / R. Hryshchuk, S. Yevseiev, A. Shmatko // Vienna.: Premier Publishing p. r. o., 284 p.

11. Information Systems Audit and Control Association (ISACA). IT-Governance and Process Maturity. Retrieved from https://www.isaca.org/bookstore/it-governance-and-business-management/wgpm (access date: 03/13/2022).

12. Voytovych V.S., Hrynyk R.O. (2016). The main security problems of cyberspace of Ukraine. Coll. abstracts of reports International scientific and practical conference "Information security in modern society". November 24-25, 2016. Lviv: LDUBZHD, P. 23–24.

13. Graivoronsky M.V. (2015). Modern approaches to ensuring cyber security / Materials of the XVII All-Ukrainian scientific and practical conference of students, postgraduates and young scientists "Theoretical and applied problems of physics, mathematics and informatics", NTUU "KPI".

14. Danko Y. I. & Reznik N. P. (2019). Contemporary challenges for China and Ukraine and prospects for overcoming these challenges. Global Trade and Customs Journal, 14(6).

15. Reznik N., Hridin O., Chukina I., Krasnorutskyy O., Mykhaylichenko M. (2022). Mechanisms and tools of personnel management in institutional economics // AIP Conference Proceedings. 2413, 040012 https://doi.org/10.1063/5.0089330.

16. On the fight against terrorism: Law of Ukraine dated March 20, 2003 No. 638-IV (as amended and supplemented). Retrieved from https://zakon.rada.gov.ua/laws/show/638-15 (access date: 03/20/2019).

17. On the main principles of ensuring cyber security of Ukraine: Law of Ukraine VIII of 05.10.2017 No. 2469-VIII (as amended and supplemented as of 21.06.2018). Retrieved from https://zakon.rada.gov.ua/laws/show/ru/2163-19/sp:max100 (access date: 03/20/2019).

18. Convention on cybercrime: Law of Ukraine dated September 7, 2005 No. 994_575 (as amended and supplemented). Retrieved from https://zakon.rada.gov.ua/laws/show/994_575 (access date: 03/20/2019).

19. Draft Law on Amendments to the Criminal Code of Ukraine on Establishing Liability for Cyberterrorism dated July 24, 2015 No. 2439a. Retrieved from http://search.ligazakon.ua/l_doc2.nsf/link1/JH1VR68A.html (access date: 03/20/2019).

20. Hryschuk R.V. (2016). Fundamentals of cyber security: Monograph / R.V. Hryshchuk, Yu.G. Danik Zhytomyr: ZhNAEU.