УДК 341.1.8; JEL classification: F52; H56
DOI: https://doi.org/10.36887/2415-8453-2023-2-45

Котляров Валерій Олександрович,
докторант,
Національний авіаційний університет

Kotliarov Valerii,
Doctoral Student, National Aviation University
https://orcid.org/0000-0002-2291-3199

КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА МІЖНАРОДНІЙ БЕЗПЕЦІ
CYBER TERRORISM AS A THREAT TO INTERNATIONAL SECURITY

Котляров В. О. Кібертероризм як загроза міжнародній безпеці. *Український журнал прикладної економіки та техніки*. 2023. Том 8. № 2. С. 314 – 321.

Kotliarov V. Cyber terrorism as a threat to international security. *Ukrainian Journal of Applied Economics and Technology*. 2023. Volume 8. № 2, pp. 314 – 321.

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 і класифікацію видів інформаційного тероризму у сучасному глобальному кіберпросторі. Запропоновані деякі шляхи протидії інформаційному тероризму як чиннику дестабілізації національної безпеки України. У статті досліджено феномен інформаційного тероризму на сучасному етапі. Увага сфокусована на понятті «кібертероризм» як основній складовій інформаційного тероризму. Висвітлено сутність цього явища, також охарактеризовано ступінь правового регулювання та запобігання інформаційному терору як на міжнародному, так і на національному рівні. Надано рекомендації щодо запобігання інформаційному тероризму в Україні. Зроблено висновки про те, що сьогодні віртуальний простір і 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. Проаналізовано сучасні проблеми інформаційної безпеки в складі національної безпеки держави. Визначено причини, що зумовлюють незадовільний стан у сфері гарантування інформаційної безпеки. Особлива увага приділяється правовим основам гарантування інформаційної безпеки та перспективам удосконалення законодавства, проблемам регулювання відносин у цій сфері. Успішний розвиток України як суверенної держави неможливий без гарантування її національної безпеки. Інформаційна безпека суспільства і держави визначається мірою їх захищеності, а отже стійкістю основних сфер життєдіяльності до небезпечних дестабілізувальних, деструктивних інформаційних дій, що утискають інтереси країни. Загроза тероризму з використанням кіберпростору є комплексним викликом сучасності. Небезпека такого тероризму полягає у відсутності географічних і 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 the threat to the national security of Ukraine. The author defines regulatory consolidation of information terrorism and outlines the significant gaps in the legislation of Ukraine in regulating this phenomenon. The article analyzes and classifies information terrorism in today's global cyberspace. The author proposes ways to counteract information terrorism as a factor of destabilization of Ukraine's national security. This article examines the phenomenon of information terrorism at the modern stage. The most outstanding attention is focused on concepts such as the media- and cyber-terrorism, which are the main components of information terrorism. This article reflects the essence of this phenomenon and the degree of legal regulation and prevention of terror information at both the international and national levels. Also, the recommendations for preventing information terrorism in Ukraine are provided. The article examines the phenomenon of informational terrorism at the current stage. The most tremendous respect is given to such concepts as media cyberterrorism as the central warehouse of informational terrorism. The article shows the essence of this phenomenon. Also, it characterizes the stage of legal regulation and the intimidation of terrorist information both internationally and nationally. 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 vast 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 information security problems are analyzed as part of the state's national security. The reasons for the unsatisfactory state of information security are determined. Special attention is paid to the legal basis of ensuring information security, prospects for improving legislation, and problems regulating relations in this area. The successful development of Ukraine as a sovereign state is only possible by 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 country's interests. 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.

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

Вступ

Проблема кібертероризму має глобальний характер та є особливо актуальною в сучасному інформаційному суспільстві. За доволі 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 загроз і розроблення засобів для боротьби з ними. Однак, попри це, усе ще існує низка проблем, які країнам треба вирішити як у національних сегментах, так і в усьому кіберпросторі.

В умовах швидкого поширення глобалізаційних процесів у 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 як засобу ведення інформаційної війни, що поєднав у собі біфуркаційні процеси фізичного тероризму, скорельованого в інформаційних системах та умисним зловживанням кіберпростором, мережами або їх компонентами для сприяння здійсненню терористичних операцій. Інформаційний тероризм набув нових загрозливих форм, а його швидке поширення стало наслідком зомбування соціуму та активізації сепаратистського руху, що в результаті може стати причиною втрати суверенітету, незалежності та територіальної цілісності окремої держави.

Феномену інформаційного тероризму присвячено праці як зарубіжних, так і вітчизняних науковців. Серед теоретиків і практиків, які займалися дослідженням інформаційного тероризму як засобу ведення інформаційної війни в умовах транскордонних глобалізованих процесів і розвитку інформаційного кіберпростору, треба 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.

Формулювання цілей статті

Мета дослідження полягає у визначенні ролі кібертероризму в сучасному безпековому просторі та як загрозу міжнародній безпеці.

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, запобігання конфліктам, уникнення нових перегонів озброєнь з 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 і 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» (американо-центристська 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. Тобто 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. Вона має достатню широку основу, яка охоплює всі верстви життєдіяльності, через що є досить багатовимірною, водночас підпорядкованою єдиній стратегії. Законодавство відповідально регулює питання гарантування безпеки інформації в державних комп'ютерних системах, боротьби з кіберзлочинами, прав 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 особистих таємниць».

Адміністративно-організаційна система гарантування 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 високий рівень життя, також приділяють багато уваги розвитку інформаційної безпеки, ґрунтуючись на власній національній політиці та принципах захисту населення від неминучих у сучасному інформаційному суспільстві загроз і небезпек [3].

У Франції сфера гарантування інформаційної безпеки та інформаційний сектор є дуже важливими аспектами 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. Таким чином, інформаційний простір у Франції вважається одним з пріоритетних об'єктів захисту, що забезпечується всіма можливими законодавчими, організаційними, адміністративними, владними та інформаційними технологіями [4].

На міжнародному рівні було запропоновано підтвердити керівну роль ООН щодо розроблення міжнародних принципів інформаційної безпеки, сприяння координації діяльності міжрегіональних і регіональних структур з запобігання злочинного використання ІКТ. На національному рівні визначено за доцільне прийняти відповідні закони, зокрема про захист 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 і 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 і Катар також підтвердили необхідність розроблення міжнародно-правових принципів щодо інформаційної безпеки, включивши до переліку загроз: «шпіонаж» (запобігання несанкціонованому доступу до змісту ІКТ-систем); «саботаж» (запобігання частковому або

повному знищенню ІКТ-систем); «підробку» (запобігання підробці інформації в глобальному кіберпросторі). Від імені урядів цих держав було запропоновано ухвалити концепцію міжнародної інформаційної безпеки і сприяти підтриманню системи сталого миру. Серед них:

Принцип 1. Діяльність кожної держави та інших суб'єктів міжнародного права у міжнародному інформаційному просторі має 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 і конфліктів, незастосування сили, невтручання у внутрішні справи, поваги до прав і свобод людини.

Така діяльність має 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 задля захисту інтересів національної безпеки кожної держави.

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

Принцип 2. Держави мають прагнути до обмеження загроз у сфері міжнародної інформаційної безпеки і з цією метою утримуватися від: розроблення, 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 задля руйнування політичної, економічної та соціальної системи інших держав і 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; розроблення та ухвалення планів, доктрин, які передбачають ведення інформаційних воєн, здатних спровокувати перегони 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 задля викривлення психологічного і духовного середовища суспільства, ерозії традиційних культурних, моральних та етичних і естетичних цінностей; інформаційної експансії, 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; заборони розроблення, 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; запобігання використанню інформаційних технологій і засобів впливу на суспільну свідомість задля дестабілізації суспільства і держави; розроблення 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 (зокрема, 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 органів з запобігання провопорушенням і їх припинення в інформаційному просторі; гармонізації на добровільній основі національних законодавств для гарантування міжнародної інформаційної безпеки.

Принцип 4. Держави та інші суб'єкти міжнародного права мають 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 під час застосування цих принципів, регулюються за допомогою встановлених процедур мирного врегулювання спорів. 55 сесія ГА ООН прийняла Резолюцію 55/28 (A/RES/55/28) від 20 листопада 2000 р. «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», у якій, посилаючись на попередні резолюції про роль науки і техніки в контексті міжнародної безпеки та відзначаючи відповіді держав щодо оцінювання 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 листопада 2001 р. «Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки», у якій відзначено, що поширення і використання інформаційних технологій і засобів торкається інтересів усього міжнародного співтовариства. Ці технології і засоби потенційно можуть бути використані задля 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, у якій підкреслено, що країни-члени 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 неправомірному та несанкціонованому використанню ІКТ у різних сферах життєдіяльності держав, що створює загрозу для міжнародної безпеки. Щодо змісту міжнародних концепцій про безпеку глобальних ІКТ-систем ЄС підкреслює, що, попри ефективність міжнародного співробітництва у сфері інформаційної безпеки, насамперед кожна держава має право і несе відповідальність за захист власних інформаційних ресурсів та інформаційних систем. Наявні ризики мають транскордонний характер і будь-які превентивні заходи, спрямовані на обмеження потенційних втрат від злочинного чи терористичного нападу, зокрема і для міжнародної безпеки, мають здійснюватись з урахуванням захисту ІКТ-ресурсів і систем. ЄС вважає, що саме ООН має стати основним форумом з обговорення проблем міжнародної інформаційної безпеки [8].

Як вже зазначалося вище, становлення інформаційної цивілізації, що супроводжується динамічним поширенням новітніх комп'ютерних технологій, спричинило появу як нових позитивних перспектив подальшого розвитку світової спільноти, так і низки глибоких проблем у сфері суспільної безпеки. Передусім це стосується інформаційних загроз терористичного характеру. У науковій літературі цей феномен отримав назву «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 задля 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; ґ) пропаганда тероризму; д) вербування кадрів; е) організація мережі; є) планування та координування дій. У своїй психологічній війні за вплив на громадську думку терористи основну ставку роблять саме на активне використання Інтернету, за допомогою чого вони намагаються поширити загрози, ескалацію страху, відчуття неминучості тощо. Для цього демонструють кадри вчинених терактів і їх жертв (наприклад, показ жорстокого вбивства в Іраку американського журналіста

Даніеля Пірла, що транслювався паралельно на кількох веб-сайтах). Небезпеку становлять і поширені хакерські атаки на інформаційні системи для 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 мережу «Інтернет» з успіхом використовують терористичні організації: відповідний вплив чинить не лише на формування громадської думки, але інколи під цей вплив потрапляє 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 їхні конфлікти та кризові явища [12].

Загалом 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 в 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 експерти недооцінюють можливі наслідки застосування високих технологій з терористичною метою, заявляючи про те, що терористична атака, здійснена за допомогою Інтернету, навряд 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, проте високі технології у діяльності терористичних угруповань можуть стати досить грізною і вигідною для них зброєю. Фахівці вважають, що кібертероризм може супроводжувати традиційні терористичні дії, оскільки порушення в роботі, наприклад систем зв'язку або інформаційних мереж критичних інфраструктур країни, можуть посилити їх ефект і викликати паніку в суспільстві. Крім того, такі порушення можуть серйозно ускладнити 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 р., коли на кілька годин буде 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 р. 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 відзначається 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 вигідної терористам 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 та перспективи подальших розвідок

Підсумовуючи, зазначимо, що друга половина XX – початок XXI ст. знаменували новий етап розвитку суспільства, спричинений потужною хвилею науково-технічної революції, розвитком нових інформаційних і 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 почали використовувати як справжню зброю. 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 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.

Сьогодні найбільшою проблемою є відсутність законодавства, у якому було б чітко визначено це поняття, передбачено відповідальність за протиправні дії. Пріоритетним напрямом у боротьбі з кібертероризмом є організація зусиль і взаємовідносин правоохоронних органів із спецслужбами, судовими органами, спрямовані на протидію і розслідування таких видів злочинів, а також потреба у вдосконаленні законодавчої бази України.

Список літератури

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.
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/3475-15#Text.
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*. 2016. №3. С. 48-61.
4. Гораш І.А., Січко Т.В. Аналіз популярних корпоративних інформаційних систем. *Ком*п'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, Liu C.-C. Cybersecurity for criticalinfrastructures: Attack and defense modeling. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. 2020. Vol. 40. no. 4. pp. 853-865.
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., Толюпа С.В., Семко В.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник. Київ. ДУТ-КНУ, 2016. 178 с.
10. Hryshchuk R., Yevseiev S., Shmatko A. Construction methodology of information security system of banking information in automated banking systems: monograph. Vienna. Premier Publishing. 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.
12. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. *Міжнародна науково-практична конференція «Інформаційна безпека в сучасному суспільстві»*: Зб. тез доповідей 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. Contemporary challenges for China and Ukraine and perspectives for overcoming these challenges. *Global Trade and Customs Journal*. 2019. №14(6).
15. Reznik N., Hridin O., Chukina I., Krasnorutskyy O., Mykhaylichenko M. Mechanisms and tools of personnel management in institutional economics. AIP Conference Proceedings. 2022. 2413. 040012 URL:https://doi.org/10.1063/5.0089330.

16. Про боротьбу з тероризмом: Закон України № 638-IV від 20.03.2003 р. URL: https://zakon.rada.gov.ua/laws/show/638-15.
17. Про основні засади забезпечення кібербезпеки України: Закон України № 2469-VIII від 05.10.2017 р. URL: https://zakon.rada.gov.ua/laws/show/ru/2163-19/sp:max100.
18. Конвенція про кіберзлочинність : Закон України № 994_575 від 07.09.2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575.
19. Проект Закону про внесення змін до Кримінального кодексу України щодо встановлення відповідальності за кібертероризм № 2439а від 24.07.2015 р. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JH1VR68A.html.
20. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016.

References

1. Pro rishennia Rady natsional'noi bezpeky i oborony Ukrainy «Pro Doktrynu informatsijnoi bezpeky Ukrainy». Ukaz Prezydenta Ukrainy [On the decision of the National Security and Defense Council of Ukraine "On the Information Security Doctrine of Ukraine". Decree of the President of Ukraine]. №47/2017 dated December 29, 2016. Available at: https://www.president.gov.ua/documents/472017-21374.
2. Pro Derzhavnu sluzhbu spetsial'noho zv'iazku ta zakhystu informatsii Ukrainy: Zakon Ukrainy. [On the State Service of Special Communications and Information Protection of Ukraine: Law of Ukraine]. № 3475-IV dated of February 23, 2006. Verkhovna Rada Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy. 2006, № 30, st. 258. Available at: https://zakon.rada.gov.ua/laws/show/3475-15#Text.
3. Kyrychok, R.V., Skladannyj, P.M., Buriachok, V.L., Hulak, H.M., Kozachok, V.A. (2016). «Problems of ensuring security control of corporate networks and ways to solve them». *Naukovi zapysky Ukrains'koho naukovo-doslidnoho instytutu zv'iazku*. №3. pp. 48-61.
4. Horash, I.A., Sichko, T.V. (2020). «Analysis of popular corporate information systems». *Komp'iuterni tekhnolohii obrobky danykh*. pp. 26-30.
5. Viter, M.B. (2014). «The technology of building an optimal model of data storage in state bodies». *Naukovo-tekhnichna informatsiia*. №1. pp. 35.
6. Buchyk, S.S. (2016). «Methodology of risk analysis of the tree of identifiers of state information resources». *Zakhyst informatsii*. №1. pp. 81-89.
7. W.Ten, G. Manimaran, Liu, C.-C. (2020). «Cybersecurity for criticalinfrastructures: Attack and defense modeling». *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. Vol. 40. no. 4. pp. 853-865.
8. Borsukovs'kyj, Yu.V., Borsukovs'ka, V.Yu. (2017). «Recommendations for categorizing information with limited access». *Suchasnyj zakhyst informatsii*. №4. pp. 9-17.
9. Buriachok, V.L., Toliupa, S.V., Semko, V.V. (2016). *Informatsijnyj ta kiberprostory: problemy bezpeky, metody ta zasoby borot'by*. [Information and cyberspace: security issues, methods and means of combating]. DUT-KNU. Kyiv. Ukraine.
10. Hryshchuk, R., Yevseiev, S., Shmatko, A. (2018). *Construction methodology of information security system of banking information in automated banking systems*. [Construction methodology of information security system of banking information in automated banking systems]. Premier Publishing. Vienna. Austria.
11. Information Systems Audit and Control Association (ISACA). IT-Governance and Process Maturity. [Information Systems Audit and Control Association (ISACA)]. Available at: https://www.isaca.org/bookstore/it-governance-and-business-management/wgpm.
12. Vojtovych, V.S., Hrynyk, R.O. (2016). «The main security problems of cyberspace of Ukraine». *Mizhnarodna naukovo-praktychna konferentsiia «Informatsijna bezpeka v suchasnomu suspil'stvi»*. [Osnovni bezpekovi problemy kiberprostoru Ukrainy]. International scientific and practical conference "Information security in modern society". L'viv.
13. Hrajvorons'kyj, M.V. (2015). «Modern approaches to ensuring cybernetic security». *Materialy KhVII Vseukrains'koi naukovo-praktychnoi konferentsii studentiv, aspirantiv ta molodykh vchenykh «Teoretychni i prykladni problemy fizyky, matematyky ta informatyky»*. [Suchasni pidkhody do zabezpechennia kibernetychnoi bezpeky]. NTUU «KPI».
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*. [Mechanisms and tools of personnel management in institutional economics]. AIP Conference Proceedings. Kanpur, India. Available at: https://doi.org/10.1063/5.0089330.
16. Pro borot'bu z teroryzmom: Zakon Ukrainy. (2003). [On the fight against terrorism: Law of Ukraine].№ 638-IV dated March 20, 2003. Available at: https://zakon.rada.gov.ua/laws/show/638-15.
17. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy. (2017). [On the main principles of ensuring cyber security of Ukraine: Law of Ukraine].Zakon Ukrainy № 2469-VIII dated October 5, 2017. Available at: https://zakon.rada.gov.ua/laws/show/ru/2163-19/sp:max100.
18. Konventsiia pro kiberzlochynnist': Zakon Ukrainy. (2005). [Convention on cybercrime: Law of Ukraine].№ 994_575 dated September 7, 2005. Available at: https://zakon.rada.gov.ua/laws/show/994_575.
19. Proekt Zakonu pro vnesennia zmin do Kryminal'noho kodeksu Ukrainy schodo vstanovlennia vidpovidal'nosti za kiberteroryzm. (2015). [Draft Law on Amendments to the Criminal Code of Ukraine on Establishing Liability for Cyberterrorism].№ 2439a dated July 24, 2015. Available at: http://search.ligazakon.ua/l_doc2.nsf/link1/JH1VR68A.html.
20. Hryschuk, R.V., Danyk, Yu.H. (2016). *Osnovy kibernetychnoi bezpeky*. [Fundamentals of cyber security]. ZhNAEU. Zhytomyr. Ukraine.

Стаття надійшла до редакції 20.02.2023 р.