УДК: 323.28

© Марина Гринчук

СУЧАСНІ МЕТОДИ ТА ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ[1]

У статті розглянуті основні тенденції розвитку та функціонування інформаційного тероризму як явища, що виникло в результаті стрімкої глобалізації, інформатизації суспільства, та збільшення впливу мережі Інтернет на всі сфери життя. Було проаналізовано та систематизовано попередні напрацювання вчених в сфері інформаційного тероризму, статистичні дані провідних світових дослідницьких центрів. Було виявлено, що Інтернет надає широкий спектр можливості використання його в якості деструктивного чинника. Міжнародні організації працюють з метою протидії інформаційному тероризму та кібератакам (ОБСЄ, НАТО, Інтерпол, Рада Європи та інші). Задля підвищення потенціалу протидії, необхідно збільшувати рівень міжнародної співпраці з метою створення можливості своєчасного виявлення та боротьби з інформаційним тероризмом.

Ключові слова: *інформаційний тероризм, кібератаки, кіберзлочинність, Інтернет, соціальні мережі.*

Современные методы и технологии информационного терроризма

В статье рассмотрены основные тенденции развития и функционирования информационного терроризма как явления, которое возникло в результате стремительной глобализации, информатизации общества, и увеличения влияния сети Интернет на все сферы жизни. Были проанализированы и систематизированы предыдущие наработки ученых в сфере информационного терроризма, статистические данные ведущих мировых исследовательских центров. Констатировано, что Интернет предоставляет широкий спектр возможностей для использования его в качестве деструктивного фактора. Международные организации работают с целью противодействия информационному терроризму и кибератакам (ОБСЕ, НАТО, Интерпол, Совет Европы и другие). Для повышения потен-

[1] ***Для цитування:*** Гринчук М. Сучасні методи та технології інформаційного тероризму // Медіафорум : аналітика, прогнози, інформаційний менеджмент: збірка наукових праць. Чернівці: Чернівецький національний університет, 2017. Том 5. С. 64-75.

циала противодействия, необходимо увеличивать уровень международного сотрудничества для создания возможности своевременного выявления и борьбы с информационным терроризмом.

Ключевые слова: *информационный терроризм, кибератаки, киберпреступность, Интернет, социальные сети.*

Modern methods and technologies of information terrorism

The article describes key trends of development and operation of information terrorism that arose as a result of rapid globalization, informatization of society and the increasing influence of Internet on all areas of life. Previous achievements of scientists in the field of information terrorism were analyzed and systematized, as well as statistics of the world's leading research centers. It was found that the Internet provides a wide range of possibilities for its use as a destructive factor. International organizations(OSCE, NATO, Interpol, the Council of Europe and others) function in order to counteract information terrorism and cyber attacks. In order to increase the potential of counter measures, it is necessary to increase the level of international cooperation in order to create opportunities of early detection and control of information terrorism.

Keywords: *information terrorism, cyber attacs, cybercrime, Internet, social networks.*

Постановка проблеми. Стрімкий розвиток та розповсюдження сучасних інформаційних технологій значною мірою вплинули на усі сфери суспільного життя. Традиційні ресурси людського прогресу поступово втрачають своє первісне значення, адже головним ресурсом науково-технічного та соціально-економічного розвитку стає інформація. Надаючи майже безмежні можливості для вдосконалення, інформаційно-комунікаційні технології також можуть бути використані і для деструктивних цілей. Враховуючи всеохоплюючий влив новітніх технологій, вже ні в кого не викликає сумніву факт того, що різноманітні злочинні та терористичні організації можуть використовувати широкий спектр технологій в процесі організації своєї діяльності. Таким чином, ми можемо говорити про зростання ролі та впливу інформаційного тероризму.

Мета статті – розглянути та проаналізувати основні види та методи інформаційного тероризму, особливості використання мережі Інтернет терористичними угрупованнями. Дослідження передба-

чає вивчення базової міжнародної та національної законодавчої та правової бази в сфері протистояння інформаційному тероризму, визначення шляхів підвищення ефективності боротьби з ним.

Аналіз останніх досліджень та публікацій. Низка зарубіжних та вітчизняних вчених досліджували явище тероризму, його еволюцію та тенденції, пов'язані з ним ключові виклики та загрози, розвиток тероризму в умовах інформаційного суспільства, роль інформаційно-комунікативних технологій та медіа. Основними зарубіжними вченими, які зробили вагомий внесок в розвиток зазначеної проблематики, були Д.Белл, Ж.Бодрійар, Е.Гіденс, М.Кастельс, Е.Тоффлер, Ф.Фукуяма, С.Гантінгтон, Б.Хофман, А.Шмід, Г.Вейман, П.Вілкінсон, У.Лакер, Б.Накос, Ф.Перл, Р.Шафферт, К.Поппер, та інші. Серед вітчизняних науковців можна відзначити праці Є.А. Макаренко, М.А. Ожевана, Д.В. Дубова, В.В. Циганова, Г.Г. Почепцова та інших.

Основні результати дослідження. Інформаційна епоха спричинила розширення методів, сфер діяльності та впливу тероризму, що призвело до появи терміну «інформаційний тероризм».

Інформаційний тероризм слід протиставляти класичному розумінню хакерських організацій, оскільки він вирізняється своїми цілями, метою та тактикою. Так, наслідки інформаційного тероризму завжди небезпечні, його акти мають на меті спричинення суспільного резонансу та широкого розголосу, на відміну від традиційних хакерських атак, де таку задачу зазвичай не ставлять. Цілі інформаційного тероризму властиві цілям тероризму загалом, вони мають публічний характер та спрямовані проти певної особи, суспільства чи влади. Різниця між інформаційним та традиційним тероризмом полягає в засобах здійснення, а також в анонімності та знеособленості.

Згідно з визначенням М. Поллітта, інформаційний тероризм – це заздалегідь сплановані, політично мотивовані атаки на інформаційні, комп'ютерні системи, програми та дані, які виражаються в застосуванні насильства по відношенню до цивільних цілей з боку субнаціональних груп або таємних агентів [1-2]. Істотно розширює дане розуміння А. Ісаков, визначаючи, що інформаційний тероризм здійснюється в сфері, що охоплює політичні, філософські, правові, релігійні та інші погляди і ідеї, тобто в духовній сфері, там, де ведеться боротьба ідей. За його словами, інформаційний тероризм - це, перш за все, форма негативного впливу на особистість, суспільство і

державу всіма видами інформації [3]. Узагальнюючи, інформаційний тероризм можна визначити як один з видів терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або безповоротного виводу з ладу інформаційної інфраструктури держави або її елементів, а також цілеспрямоване використання цієї інфраструктури для створення умов, що тягнуть за собою катастрофічні наслідки для різних сторін життєдіяльності суспільства і держави.

Розрізняють декілька видів інформаційного тероризму:

- інформаційно-психологічний тероризм - контроль над ЗМІ з метою поширення дезінформації, чуток, демонстрації потужності терористичних організацій;

- інформаційно-технічний тероризм - нанесення шкоди окремим фізичним елементам інформаційного середовища держави; створення перешкод, використання спеціальних програм, що стимулюють руйнування систем управління [4].

Методи інформаційного тероризму орієнтовані не на фізичне знищення людей і ліквідацію матеріальних цінностей, а на широкомасштабне порушення роботи фінансових і комунікаційних мереж і систем, часткове руйнування економічної інфраструктури і нав'язування владним структурам своєї волі.

За оцінкою експертів, ефективність інформаційного тероризму може бути порівняна із застосуванням зброї масового знищення, а загроза здійснення інформаційного тероризму прямо пропорційна рівню технологічного розвитку та масштабам використання комп'ютерної техніки в системах управління державою.

Інформаційна складова тероризму набирає стрімких обертів, викликаючи занепокоєння суспільства. Виступаючи перед Конгресом США, тодішній директор національної розвідки США Джеймс Клеппер назвав кібератаки більш небезпечними для США, ніж інші види тероризму [5]. На сьогоднішній день Інтернет широко використовується різноманітними угрупованнями терористичного спрямування задля досягнення поставлених цілей. Глобальна мережа привертає оперативністю, економічністю, доступністю, слабкою цензурою або її повною відсутністю, наявністю величезної потенційної аудиторії користувачів по всьому світу, швидким і відносно дешевим поширенням інформації, комплексністю її подачі і сприйняття. Безперечною перевагою вважається також можливість анонімного зв'язку,

скритність джерела впливу, та дистанційний характер впливу в різних регіонах світу.

Г. Вейман виділяє наступні методи використання Інтернету терористичними угрупованнями:

- психологічна війна (використання Інтернету для дезінформації, поширення загроз, спрямованих на те, щоб посіяти страх і відчуття безпорадності);

- реклама і пропаганда (розповсюдження інформації про діяльність, поширення агітаційно-пропагандистської інформації про терористичні рухи, їх цілі і завдання, намічені дії, форми протесту). Раніше цей фактор залежав від залучення уваги телебачення, радіо або друкованих ЗМІ;

- збір даних (можливість доступу до інформації за допомогою Інтернету). Згідно з доповіддю тодішнього міністра оборони США Д. Рамсфельда 15 січня 2003 року, в посібнику Аль-Каїди, знайденому в Афганістані, було вказано: «Використовуючи громадські джерела відкрито без застосування незаконних засобів, можна зібрати про ворога як мінімум 80% необхідної інформації» [6];

- збір коштів (збір пожертвувань задля поповнення фондів);

- вербування і мобілізація (одним із шляхів пошуку нових учасників є використання он-лайн технологій, наприклад, переміщення по чатах і форумах в пошуку найбільш сприйнятливих членів аудиторії, особливо молодих людей. Електронні конференції та дискусії з певних проблем можуть також служити засобом для звернення до потенційних нових членів);

- створення мереж (можливість підтримки контакту один з одним та з представниками інших терористичних організацій). Нові технології сильно скоротили час передачі, дозволяючи розсіювати місцезнаходження осіб, при цьому є можливість швидкого зв'язку і ефективної координації;

- розподілення інформації (розміщення у вільному доступі та розсилка відкритих та зашифрованих інструкцій про створення хімічної зброї, вибухові речовини тощо) [7].

Окрім виокремлених Г. Вейманом методів та засобів використання Інтернету терористичними угрупованнями, існує ряд інших, серед яких можна виокремити семантичні атаки, метою яких є злом сторінок і подальше розміщення на них свідомо помилкової інформації. Подібним атакам, як правило, піддаються найбільш часто від-

відувані інформаційні сторінки, змісту яких користувачі повністю довіряють. Досить частою є заміна інформаційного змісту сайтів, яка полягає в підміні електронних сторінок або їх окремих елементів. Такі дії робляться в основному для залучення уваги до атакуючої сторони, демонстрації своїх можливостей або є способом вираження певної політичної позиції. Крім прямої підміни сторінок широко використовується перенаправлення посилань на іншу адресу, що призводить до відкриття спеціально підготовлених сторінок. Одним з методів також є виведення з ладу або зниження ефективності функціонування структурних елементів інформаційно-телекомунікаційних систем шляхом застосування спеціальних програмних засобів на основі програмного коду, масової розсилки електронних листів, DDoS-атак, проведення яких аналогічно технології масової розсилки електронних листів, що призводить до уповільнення роботи обслуговуючого сервера, або повного припинення зовнішнього доступу до його ресурсів.

За даними провідної статистичної компанії Statista, яка оприлюднила світові статистичні показники основних типів кібератак в 2016, зловмисні програми використовувались в якості інструментів здійснення кібератак найчастіше (98%). Друге та третє місце посіли фішинг, соціальна інженерія (70%) та веб-атаки (63%) відповідно. Внутрішні зловмисники виявились досить рідкісним явищем, що трапляється в 41% випадках [8].

Для представників терористичних організацій Інтернет-комунікація служить дуже важливим інструментом впливу на громадську думку через великі маніпулятивні можливості. Прихована небезпека Інтернету та інших інтерактивних систем полягає в тому, що на відміну, наприклад, від телеглядача, користувач мережі психологічно впевнений в свободі свого інформаційного вибору, в неможливості маніпулювання його поведінкою з боку інших мережевих суб'єктів. Крім того, Інтернет дозволяє задіяти набагато ширший інструментальний спектр інформаційної стимуляції свідомості і підсвідомості індивіда, ніж друковані ЗМІ та навіть телебачення: звук, візуальний ряд з величезною палітрою фарб і геометричних побудов, текстовий матеріал, а також інтерактивний зворотний зв'язок, що породжує у об'єкта маніпуляції почуття причетності до подій.

Соціальні мережі активно використовуються представниками терористичних організацій. Згідно з дослідженнями Інституту Брукінга, прихильники ІДІЛ контролюють понад 46000 Twitter-акаунтів (однак, не всі є активними), через які вони розповсюджують повідомлення безпосередньо до смартфонів своєї цільової аудиторії, уникаючи посередництва в традиційних засобах масової інформації. Приблизна кількість послідовників таких акаунтів – близько тисячі, що дозволяє не привертати занадто велику увагу служб протидії.

Представники ІДІЛ також використовують сегментацію як інструмент донесення інформації до цільової аудиторії. В рамках цього інструменту була створена мережа з 29 спеціалістів аудіовізуального контенту: троє для глобальних проектів, інші 26 створюють аудіовізуальний контент для певних категорій та країн (Сирія, Ірак, Єгипет, Ємен, Афганістан та інші).

Сегментація також передбачає використання різних мов, в залежності від ключової аудиторії. З понад 120 аудіовізуальних кампаній ІДІЛ, 27% зроблені англійською мовою, 15% – російською, 13% – французькою, 3% - німецькою [9-10].

Окрім Twitter, використовуються і інші соціальні мережі, такі як Facebook, Ask.fm, Pinterest, YouTube, WordPress, Kik, WhatsApp, Tumblr та інші. За попередніми оцінками, близько 25 тис. іноземців з більш ніж 100 країн приєдналися до організації [11].

Враховуючи широкий спектр використання терористичними організаціями інформаційно-комунікаційних технологій, постає питання можливості боротьби з явищем інформаційного тероризму.

Значну роль у протидії інформаційному тероризму відіграють міжнародні організації, такі як ОБСЄ, НАТО, Інтерпол, Рада Європи та інші. Вони відіграють важливу роль в координації міжнародних зусиль, побудові міжнародної співпраці в боротьбі зі злочинами в сфері високих технологій. Так, наприклад, однією з сфер діяльності антитерористичного підрозділу ОБСЄ є протидія використання Інтернету в терористичних цілях. На офіційному сайті міститься інформація про те, що підрозділ бореться з випадками використання Інтернету терористами шляхом ідентифікації таких тенденцій і пропаганди потенційних контрзаходів. Працюючи в рамках цієї програми, ОБСЄ визнає, що Інтернет став стратегічним інструментом і тактичним засобом посилення потенціалу терористичних угруповань, і використовується ними для різних цілей, таких як ідентифікація, вербування та підготовка нових членів, збір і переказ фінансових коштів тощо [12].

Іншим прикладом може слугувати Європейський центр по кіберзлочинності ЄС, діяльність якого спрямована на надання оперативної і аналітичної підтримки в боротьбі з кіберзлочинами правоохоронним органам країн ЄС, а також партнерам, що не входять до ЄС [13]. Щодо Інтерполу, то до його функцій в сфері протидії кіберзагрозам входить оперативна і слідча підтримка, кіберрозвідка і аналіз, цифрова судово-медична експертиза, інновації та дослідження, підвищення потенціалу з протидії кібертероризму тощо [14]. В рамках діяльності НАТО кіберзахист є складовою завдання колективної оборони Альянсу. НАТО несе відповідальність за захист своїх власних мереж, проводить діяльність з розширення обміну інформацією та взаємної допомоги в галузі попередження, пом'якшення наслідків і відновлення після кібератак [15]. Міжнародним регулюючим документом в сфері інформаційного тероризму є Конвенція Ради Європи із кіберзлочинів, укладена 23 листопада 2001. Дана Конвенція включає основні принципи для розробки національного законодавства з кіберзлочинності, а також рамки для міжнародного співробітництва між країнами-учасницями. Документ включає положення про створення цілодобової і щоденної системи боротьби зі злочинністю в режимі онлайн, а також сприяє партнерським зв'язкам між державним і приватним секторами [16].

Правову основу кібербезпеки України становлять закони України «Про основи національної безпеки», «Про інформацію», «Про захист

інформації в інформаційно-телекомунікаційних системах» тощо. Україна ратифікувала Конвенцію Ради Європи із кіберзлочинів 10 березня 2006, згодом був ратифікований Додатковий протокол до Конвенції про кіберзлочинність щодо криміналізації дій расистського або ксенофобного характеру, вчинених за допомогою комп'ютерної системи [17]. Результатом нових викликів та загроз національній кібербезпеці стало створення Стратегії кібербезпеки України, що була введена в дію указом Президента України від 15 березня 2016.

В ній, зокрема, зазначено, що невідповідність інфраструктури електронних комунікацій сучасним вимогам, недостатній рівень захищеності критичної інформаційної інфраструктури, безсистемність заходів кіберзахисту критичної інформаційної інфраструктури, недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки є одними з тих чинників, дія яких ставить під загрозу забезпечення національної безпеки України в кіберпросторі. Задля зменшення рівня кіберзагроз вирішено залучати експертний потенціал наукових установ, підвищувати цифрову грамотність громадян, проводити навчання щодо надзвичайних ситуацій та інцидентів у кіберпросторі, розвивати та удосконалювати систему державного контролю за станом захисту інформації тощо [18].

Висновки. Отже, інформаційний тероризм, як нова форма тероризму, ставить на меті вчинення свідомого і цілеспрямованого інформаційного впливу для створення умов, що мають катастрофічні наслідки для держави, політиків, що мають приймати ефективні рішення у кризових ситуаціях. А також для корпорацій та державних структур, що забезпечують життєдіяльність країни (критична інфраструктура).

Основними методами використання мережі Інтернет задля здійснення акту інформаційного тероризму є методи психологічної війни, реклами і пропаганди, збору даних та коштів, вербування і мобілізація, створення мереж та розподілення інформації. Окрім цього, широко використовуються спеціальні програмні засоби, масова розсилка електронних листів, DDoS-атаки тощо. Останнім часом набуло розповсюдження активне використання соціальних мереж (Twitter, Facebook, Ask.fm, Pinterest, YouTube, WordPress, Kik, WhatsApp, Tumblr) у терористичних цілях.

У протидії інформаційному тероризму значну роль відіграє діяльність міжнародних організацій (ОБСЄ, НАТО, Інтерпол, Рада Європи та інших) з метою побудови міжнародної співпраці в боротьбі з кіберзлочинами.

Міжнародна законодавча база протидії інформаційному тероризму представлена Конвенцією Ради Європи із кіберзлочинів. Правову основу для нашої країни з даної тематики складають такі документи, як закони України «Про основи національної безпеки» (2003), «Про інформацію» (1992), «Про захист інформації в інформаційно-телекомунікаційних системах» (1994), Стратегія кібербезпеки України (2016) тощо.

Задля підвищення ефективності протидії інформаційному тероризму, необхідно вдосконалити технології своєчасного виявлення і нейтралізації несанкціонованого доступу до інформації, в тому числі і у відкритих мережах. Безперечно необхідним чинником протидії є організація міждержавного співробітництва в роботі міжнародних організацій, громадських комітетів і комісій в проектах розвитку світових інформаційних мереж.

Прийняття Україною низки нормативно-правових актів та законів в сфері кібербезпеки свідчить про розуміння необхідності захисту інформаційного простору України в комп'ютерних мережах та протидії кіберзлочинності. Проте, законодавча база України в сфері кібербезпеки не охоплює повний спектр можливих кіберзагроз. Тому, вкрай важливим є більш досконале подальше дослідження та виявлення додаткових потенційних загроз, розроблення стратегії їх подолання і протидії, та розширення законодавчої бази з метою створення ефективної системи забезпечення національної кібербезпеки. Також, необхідно підвищувати обізнаність населення в сфері кіберзлочинності, сформувати в них потужний потенціал протидії шляхом проведення навчань з залученням експертів для спільного обміну досвідом.

Джерела та література:

1. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України : аналітична доповідь / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 30 с.

2. What is Cyber-terrorism? [Електронний ресурс] // Computer crime research center – Режим доступу до ресурсу: http://www.crime-research.org/library/Cyber-terrorism.htm.

3. Исаков А. Информационный терроризм/ А. Исаков. - Обозреватель-Observer. - 2002. - N 5/6. - С. 79-84

4. Королев А. Киберпространство и информационный терроризм [Електронний ресурс] / А. Королев // Центр анализа террористических угроз. – 2016. – Режим доступу до ресурсу: http://www.catu.su/analytics/1250-kiberprostranstvo-i-informacionnyj-terrorizm.

5. James Clapper Jr. Cyber Attack Poses More Threats Than Any Other Type Of Terrorism: Security Chief [Електронний ресурс] / James Clapper Jr. – Режим доступу до ресурсу: https://www.fastcompany.com/3006916/fast-feed/cyber-attack-poses-more-threats-any-other-type-terrorism-security-chief.

6. Kevin Poulsen. Rumsfeld orders .mil Web lockdown [Електронний ресурс] / Kevin Poulsen // SecurityFocus – Режим доступу до ресурсу: http://www.securityfocus.com/news/2062.

7. Вейманн Г. Специальный доклад № 116. Как современные террористы используют Интернет [Електронний ресурс] / Габриель Вейманн – Режим доступу до ресурсу: http://scienceport.ru/library/liball/5170-spetsialnyiy-doklad-%E2%84%96-116-kak-sovremennyie-terroristyi-ispolzuyut-internet/.

8. Types of cyber attacks experienced by companies worldwide as of August 2016 [Електронний ресурс] // The Statistics Portal – Режим доступу до ресурсу: https://www.statista.com/statistics/474937/cyber-crime-attacks-experienced-by-global-companies/.

9. How ISIS Recruits Through Social Media [Електронний ресурс] // Fordham Political Review – Режим доступу до ресурсу: http://fordhampoliticalreview.org/how-isis-recruits-through-social-media/.

10. Lesaca J. On social media, ISIS uses modern cultural images to spread anti-modern values [Електронний ресурс] / Javier Lesaca // Techtank – Режим доступу до ресурсу: https://www.brookings.edu/blog/techtank/2015/09/24/on-social-media-isis-uses-modern-cultural-images-to-spread-anti-modern-values/.

11. Hahn J. How the World\'s Most Dangerous Group Uses Social Media [Електронний ресурс] / Jason Hahn – Режим доступу до ресурсу: http://www.complex.com/pop-culture/2015/04/isis-social-media-methods.

12. Антитеррористическое подразделение [Електронний ресурс] // ОБСЕ. Справочная информация – Режим доступу до ресурсу: http://www.osce.org/ru/atu/13579?download=true.

13. European cybercrime centre [Електронний ресурс] – Режим доступу до ресурсу: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

14. Cybercrime [Електронний ресурс] // Interpol – Режим доступу до ресурсу: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

15. Cyber defence [Електронний ресурс] – Режим доступу до ресурсу: http://www.nato.int/cps/en/natohq/topics_78170.htm.

16. Convention on cybercrime [Електронний ресурс] – Режим доступу до ресурсу: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

17. Участь України у міжнародних договорах Ради Європи [Електронний ресурс] // Міністерство Юстиції – Режим доступу до ресурсу: http://old.minjust.gov.ua/201.

18. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року \»Про Стратегію кібербезпеки України\» [Електронний ресурс] – Режим доступу до ресурсу: http://www.president.gov.ua/documents/962016-19836.