УДК 341.45+343.326
Ворович Б.О., к.військ.н., доцент[1].;
Рогов П.Д., к.т.н.[1];
Мороз Я.О.[2]

[1] - Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського;
[2] - Державний університет телекомунікацій

Державний контроль глобальних інформаційних та соціальних мереж як основа завчасного виявлення терористичних угруповань та їх намірів

Государственный контроль глобальных информационных и социальных сетей как основа заблаговременного выявления террористических группировок и их намерений

The state control of the global information and social networks as a basis of beforehand revealing of terrorism groups and their intentions

Резюме. В статті розглянуто проблему контролю державними службами за діями користувачів в глобальних інформаційних та соціальних мережах для розкриття їх можливих намірів та подальшого прийняття рішення про їх причетність до терористичних угруповань.

Ключові слова: контроль, глобальні інформаційні та соціальні мережі, терористичні угруповання.

Резюме. В статье рассмотрена проблема контроля государственными службами за действиями пользователей в глобальных информационных и социальных сетях для раскрытия их возможных намерений и последующего принятия решения об их причастности к террористическим группировкам.

Ключевые слова: контроль, глобальные информационные и социальные сети, террористические группировки.

Resume. In the article the problem of control government services is considered after the actions of users in global informative and social networks for opening of them possible intentions and subsequent decision-making about their involvement to the terrorist groupments.

Keywords: control, global informative and social networks, terrorist groupments.

Постановка проблеми. Основним напрямом роботи будь-якої держави та її силових відомств є виявлення терористичних організацій та угруповань, можливих ознак їх підготовки до проведення терористичного акту. Відомості, що зібрані шляхом розвідки, моніторингу відкритих джерел (ЗМІ) та іншими методами (за результатами даних міжнародної взаємодії у сфері боротьби з тероризмом) розглядаються у даній статті. Таким чином, можна визначити напрями взаємодії національного силового сектора безпеки і міжнародних організацій при веденні боротьби з глобальним (міжнародним) тероризмом.

Аналіз публікацій в українській та зарубіжній пресі свідчить про те, що питанню боротьби з тероризмом приділяється значна увага в розвинутих країнах світу. В деяких країнах завдання боротьби з тероризмом є одним з основних завдань мирного часу. Країни, в яких нехтували завчасною підготовкою до боротьби з тероризмом, були змушені навчатися цьому вже в умовах виникнення кризової ситуації.

Після терактів 11 вересня 2001 р. відбулося відновлення примату силового підходу до розв'язання проблеми тероризму (контртерористичні операції США в Афганістані та Іраку). На відміну від США, європейське бачення забезпечення безпеки спрямоване, насамперед, на створення умов для унеможливлення діяльності терористичних організацій. Перевага надається організаційно-правовій, розвідувальній складовій та контролю за інформаційними потоками, зокрема, в глобальних інформаційних і соціальних

мережах, в першу чергу – Інтернет. Таке розуміння безпеки втілюється в стратегії умиротворення небезпечних держав і стратегії їх залучення режимів до економічної допомоги країнам "третього світу", боротьи з бідністю, хворобами та злиденністю, сприяння соціальній справедливості. Базовим орієнтиром європейської антитерористичної парадигми є дотримання балансу між правом сили та силою права в напрямку недопущення обмеження прав і свобод людини, збереження персональних даних від несанкціонованого доступу.

В останні кілька років витоки персональних даних стали однією з ключових проблем інформаційної безпеки. В той же час прийнято вважати, що такого роду випадки – справа рук комп'ютерних зловмисників або недобросовісних бізнесменів. Однак переданими по комп'ютерним мережам даними цікавляться і спецслужби. У різних країнах світу різні державні організації перехоплюють інформацію, причому часом і передану по всіх видах телекомунікацій, але аж ніяк не тільки Інтернетом. Оператори зв'язку – учасники телекомунікаційного ринку (майже скрізь) – законодавчо зобов'язані надавати силовим структурам можливість контролю над переданими даними.

Мета роботи – визначення сутності державного антитерористичного контролю за діяльністю користувачів мережі Інтернет та інших соціальних мереж, з метою виявлення, можливих ознак підготовки терористичних організацій та угруповань до проведення терористичного акту.

Викладення основного матеріалу. Фахівці з інформаційної безпеки виділяють кілька основних видів несанкціонованого контролю (шпигунства) глобальної інформаційної мережі Інтернет та соціальних мереж: "традиційний" (державний), кримінальний, економічний (промисловий) і особистий. Після початку глобальної війни проти тероризму (після подій 11 вересня 2001 р.), на державному рівні в багатьох країнах світу був санкціонований новий різновид комп'ютерного контролю-шпигунства – "антитерористичний". Інтернет, не є скутим державними кордонами, а значить будь-яка державна несанкціонована діяльність у ньому неминуче виявляється на самій межі між законом і злочином. Також після вищеназваної дати Національне агентство безпеки США отримало розширені повноваження щодо стеження за приватним життям громадян. Їх повноваження дозволяють, наприклад, прослуховувати записи телефонних розмов. Якщо проаналізувати список телефонних дзвінків людини за вказаний проміжок часу, то можна скласти приблизну мережу його контактів. Це дуже важлива інформація, тому що вона дозволяє аналізувати, наскільки близька людина до того чи іншого нелегального формування.

Терористичні організації налагодили між собою тісні зв'язки на загальній ідеологоконфесійній, військовій, комерційній та іншій основах. Терористичні угруповання, особливо їхні керівники, в багатьох випадках тісно взаємодіють у питаннях придбання озброєння, прикриття один одного, поділу функцій і завдань при проведенні ними масштабних операцій (наприклад, в Афганістані або Лівані).

Ці приклади показують, що сучасний тероризм здатний вести диверсійно-терористичну війну, брати участь у масштабних збройних конфліктах. Тероризм перетворився на досить прибутковий бізнес глобального масштабу з розвиненим "ринком праці" і додаткового капіталу (поставки зброї, наркоторгівля). Важливою особливістю сучасного тероризму є його добре структурований й організований характер. Терористичні організації створюють єдині керівні органи, систему управління своїми підрозділами. Проводяться наради й зустрічі керівників найбільш великих угруповань, координація діяльності організацій різної національної приналежності. Для створення більшого морально-психологічного ефекту й суспільного резонансу налагоджене інформаційно-пропагандистське забезпечення.

Дослідницька робота спецслужб здійснюється в області масового автоматичного збору приватної інформації, яку люди публікують на своїх сторінках у соціальних мережах. При цьому йде пошук способів використання технологій так званої "семантичної мережі" для інтеграції відомостей з соціальних мереж до бази даних з інформацією про банківські рахунки (у тому числі руху рахунків), відомостях про володіння нерухомістю. У цю ж систему можна інтегрувати історію переміщень людини (ці відомості доступні з мереж стільникового зв'язку) та іншу інформацію. Якщо така система буде реалізована, то служба безпеки зможе генерувати докладне досьє на будь-якого громадянина або організацію країни.

Необхідність державного контролю споживачів мережі Internet та інших соціальних мереж як особливого виду соціальної реальності, його впливу на суспільство і

діяльність різних соціальних інститутів та організацій дослідниками була усвідомлена ще у середині 90-х років XX ст. В даний час у соціологічній науці склалися два основних підходи до вивчення Internet. Перший спрямований на виявлення соціальних умов і передумов, що найбільшою мірою впливають на інституціоналізацію Internet-простору як окремої, відносно автономної сфери суспільних відносин, і прогнозування позитивних і негативних наслідків даного процесу. Другий підхід, навпроти, орієнтований на виявлення й оцінку наслідків впливу Internet на діяльність соціальних інститутів і організацій, на розкриття впливу специфічних характеристик Internet-простору як особливого виду соціальної реальності на сучасне суспільство.

Завчасне виявлення зловмисних дій терористів пов'язане з оцінкою їх загроз або інших первинних ознак тероризму. А виділення латентних намірів терористів неможливе без обробки величезного масиву різної інформації, яка надходить, у тому числі і від населення. Така робота просто не можлива без застосування нових технологій обробки і аналізу інформації.

Для визначення задумів терористів і без інформації, що поступає від населення (хоча з нею ці дані стануть набагато точніші), силові структури можуть використовувати алгоритм аналізу інформації в своїх базах даних з метою пошуку аномалій і трендів без з'ясування смислового значення «записів від населення». Англійською це звучить набагато коротше – «data mining algorithm». Але, саме з нечітких і маловірогідних повідомлень від населення, які наділяються значенням певного атрибуту та набувають модального значення, стають зрозумілими наміри терористів, а, отже, і стратегія контртероризму. Математично вивірені моделі фокусуються на соціальних аномаліях, як індикаторах зародження системного тероризму. Іншими словами, озброєні математичними і соціологічними інструментами «силові структури» зможуть виявляти і нейтралізувати терористів.

На сьогоднішній день скласти всеосяжну інформаційну базу на всіх користувачів Інтернету – досить складне завдання, тому що інформація в мережі представлена в безлічі форматів, несумісних один з одним. Так чи інакше, але сьогодні у всіх країнах Заходу (та й у більшості країн світу) діють закони, що дають широкі повноваження силовим структурам з моніторингу інформації, переданої з телекомунікаційних систем. Чим розвиненіша економіка тієї чи іншої країни, чим більше її населення, тим більший обсяг інформації доводиться обробляти національним спецслужбам. Тому не дивно, що найбільш щільно Інтернет контролюють в Сполучених Штатах, Великій Британії, Німеччині, Російській Федерації та ін. Цим займається багато їхніх фахівців спецслужб. Країни ЄС та Російська Федерація також докладають величезних зусиль з "антитерористичного" контролю за телекомунікаціями. У Китаї контролюється мережа Інтернет не стільки для боротьби з терористами, скільки для придушення внутрішнього інакомислення. Трохи осібно стоїть Японія: там і населення велике, і економіка розвинена, і Інтернет в кожному будинку – а спецслужби не дуже-то щільно здійснюють моніторинг інформаційних мереж та контролюють потоки інформації.

Антитерористична політика кожної країни має свої особливості, зважаючи на суспільно-політичну ситуацію, культурні й релігійні традиції, правову систему та систему державного управління, розвиток демократичних інститутів та рівень усвідомлення терористичної загрози. Акцентований наголос на силові, воєнні та поліцейські заходи протидії тероризму є характерним для політики США та Ізраїлю, наочним свідченням чого є беззастережне використання керівництвом цих країн збройних сил у масштабних контртерористичних операціях. Реалізація такої політики покладається на розгалужену загальнодержавну систему антитерористичних дій, побудовану на принципах гнучкості та динамічності, яка в концептуальному та інституційному сенсі відповідає завданням боротьби з тероризмом.

Гнучкий підхід до проблеми профілактики тероризму демонструють Італія та Німеччина. Тривала практика впровадження антитерористичних стратегій у Великобританії щодо урегулювання міжконфесійного та міжнаціонального конфлікту в Північній Ірландії (від залучення політичних механізмів до «нормалізації» ситуації за допомогою армії та поліції) свідчить, що в сучасних умовах не завжди вдається обмежитися застосуванням політичних методів відвернення терористичної загрози.

На сучасному етапі посилення небезпеки тероризму спонукає уряди таких країн як США, Ізраїль, Великобританія, Іспанія, Російська Федерація та інші до оперативного реагування, оптимізації державних антитерористичних систем та удосконалення правових механізмів. В цілому, в реалізації антитерористичних

стратегій держави враховують три взаємопов'язані напрями: превентивний, регулятивний та репресивний, які лежать в основі сутнісного розуміння організації протидії тероризму. За результатами спостереження за інформаційними та соціальними мережами встановлено, що найбільш важливою передумовою викорінення екстремізму й тероризму є: зміцнення можливостей держави шляхом застосування політичних, економічних, освітніх, інформаційних заходів; протидія екстремістській ідеології; врегульовання внутрішніх й регіональних конфліктів без застосування сили. У цьому контексті важливого значення набуває здійснення оперативного контролю за інформаційним простором.

Передвісниками тероризму стають зовні невинні грошові операції, "випадковий" інтерес до критично важливих об'єктів або проектів і т.п. Важливо створити механізм розпізнавання (визначення) націленості атак терористів для їх запобігання спецслужбами. Сучасні інформаційні технології дозволяють оперативно працювати з великими об'ємами такого роду даних: збирати і зберігати їх. Але володіння початковим фактичним матеріалом саме по собі не народжує нового знання. Тільки обробка і аналіз даних забезпечують обґрунтоване ухвалення рішень. Причому, із збільшенням об'ємів даних незмінно зростає і роль інформаційного аналізу. Для цього потрібні найсучасніші аналітичні інструменти, які дозволять скласти осмислену картину, яка відбувається, на підставі отриманих даних, виявити дійсний стан речей, розкрити природу і масштаб проблем, ухвалити обґрунтоване рішення, розробити відповідні плани дій і використовувати наявні засоби найбільш ефективним чином.

Спецслужби Сполучених Штатів Америки почали займатися перехопленням даних в Інтернеті ще на початку 90 -х років. Наприкінці 90-х вперше з'явилася інформація про діяльність системи "Ешелон", завданням якої є перехоплення даних на міжнародному рівні. У 2000 р. американська влада визнала існування "Ешелону" як системи глобального моніторингу даних, створеної спецслужбами англо-саксонського альянсу (США, Великобританія, Канада, Австралія і Нова Зеландія). Проте, не зовсім зрозуміло, коли ця система була створена. Перші згадки про "Ешелон" датуються 1991-м р., але експерти вважають, що система діяла задовго до цього, і працювала проти СРСР буквально з часів початку холодної війни. Техніка "Ешелону" автоматично перехоплює дані з різних каналів комунікацій на основі їх зіставлення з матрицею заданих ключових фраз. Втім, система "Ешелон" залишається глибоко засекреченою і всі відомості про неї не дуже достовірні.

Про тотальне стеження американських спецслужб стало відомо влітку 2013 р., коли екс-співробітник ЦРУ Едвард Сноуден розголосив секретні матеріали про роботу АНБ і ЦРУ. Виявилося, що спецслужби відстежують дзвінки, СМС-листування і спілкування в Інтернеті мільйонів людей по всьому світу. Також з'ясувалося, що американські спецслужби стежать за переговорами світових лідерів. Повідомлялося про прослуховування АНБ розмов, щонайменше, високопосадовців 35 держав. Серед них опинилася канцлер Німеччини Ангела Меркель, яка висловила невдоволення діями спецслужб США.

Але перехопленням конфіденційних даних у Інтернеті в США займається аж ніяк не тільки АНБ. У 2000 р. в США вибухнув скандал у зв'язку з розкриттям системи Carnivore ("Хижак", інша назва - DCS-1000), яка діє на благо ФБР. Система фільтрувала всі електронні листи американців на підставі заданих ключових фраз. Більш того, система Carnivore примусово встановлювалася у Інтернет-провайдерів і оператори зв'язку не мали права втручатися в процес моніторингу трафіку з боку агентів ФБР. Але, у 2005 р. ФБР вирішило відмовитися від системи, визнавши її застарілою. Замість неї була створена нова структура, частиною якої стала система обробки бази даних Virtual Case File, розроблена компанією Science Applications International. Її вартість склала $124 млн.

В Російської Федерації ще кілька років тому на багатьох сайтах Рунета можна було бачити банер з написом "СОРМ-2: завтра над вашим любовним листуванням буде плакати все ФСБ". Однак потроху масове обурення активністю спецслужб в російському сегменті інтернету зійшло нанівець. З одного боку цьому посприяли численні теракти, з іншого – поява в Мережі великого числа новачків-підлітків, які просто не замислюються про такі "високі матерії" як приватність.

Втім, СОРМ (Система оперативно-розшукових заходів) діяла в Росії з 1995 р. У 1998 р. Мінзв'язку Росії почало включати в ліцензії на надання послуг зв'язку спеціальну умову про сприяння силовим структурам. При цьому оператори повинні були "вживати заходів до недопущення розкриття організаційних і тактичних прийомів проведення зазначених заходів". Однак незабаром телекомунікаційні компанії почали скаржитися на ФСБ, яка вимагала від них придбання за свій рахунок

дорогого ($15-20 тис.) спецобладнання для встановлення в своїх мережах.

На початку 2000 р. світ побачив СОРМ-2. З цього моменту навіть податкова поліція отримала можливість самостійно, минаючи ФСБ, використовувати можливості перехоплення даних. У 2005 р. система була дещо змінена і отримала в пресі назву СОРМ-3. Почало діяти нова урядова постанова, яка зобов'язує операторів встановлювати спецзасоби, призначені для перехоплення даних клієнтів. Згідно з ним, російські оператори зв'язку зобов'язані підключати інформаційні системи, що містять бази даних, а також технічні засоби до пункту управління органу федеральної служби безпеки. При цьому бази даних повинні містити наступну інформацію про абонентів оператора зв'язку: прізвище, ім'я, по-батькові, місце проживання і реквізити основного документа, що посвідчує особу. Для юридичної особи – її назва, місце знаходження, а також список осіб, які використовують кінцеве обладнання, із зазначенням їх особистих даних.

Крім усього перерахованого вище, оператори зв'язку зобов'язані вести бази даних про розрахунки за надані послуги зв'язку, у тому числі про з'єднання, трафік і платежі абонентів. Телекомунікаційна компанія зобов'язана зберігати всю цю інформацію протягом трьох років.

У європейських країнах дуже педантично ставляться до таємниці особистої інформації, але якщо вже вирішуються її порушити, то діють непохитно. Зараз у Західній Європі існує контроль над потоками даних за всіма можливим телекомунікаційним системам. У 2005 р. всіма країнами Євросоюзу були прийняті умови, згідно з якими всіх операторів зв'язку зобов'язали протягом шести місяців зберігати повну інформацію про всі телефонні дзвінки, сеанси підключення до Інтернету, повідомлення електронної пошти тощо. В Ірландії цей термін збільшили до чотирьох років, в Італії – до трьох.

У Великобританії на підставі Акту по боротьбі з тероризмом, злочинністю та безпеки (Anti-Terrorism, Crime and Security Act, прийнятий у грудні 2001 р.) спецслужби мають право отримувати інформацію користувача у операторів без рішення суду, а тільки на підставі рішень міністерства внутрішніх справ або інших високопосадовців. Тим часом, ще в 2000 р. британський уряд в рамках служби MI5 почав формування, так званого, Центру технічної підтримки уряду (Government Technical Assistance Center). Його завдання – проводити моніторинг всього інтернет-трафіку в країни. Цікавий момент: у Великобританії перехоплення даних легалізовано не тільки для держави. У 2001 р. було прийнято закон, який дозволяє компаніям прослуховувати робочі телефонні лінії і переглядати корпоративні адреси електронної пошти своїх співробітників.

Досвід країн Європи, свідчить про наявність налагодженої системи своєчасного надходження інформації про діяльність і наміри екстреміських угруповань, а також існування відповідного законодавства відносно боротьби з тероризмом.

Китай, що нараховує близько 150 млн. Інтернет-користувачів, в останні роки стає все більш відкритим для міжнародного бізнесу, але в той же час дуже строго контролює Інтернет в рамках національної доменної зони. Автоматизована система тотального контролю за мережею вже отримала назву "Велика китайська електронна стіна". Результати її роботи очевидні: китайські органи нагляду у 2005 р. закрили більше 2000 веб-сайтів з метою усунення інформації, яку вони вважають незаконною. Одночасно в країні діють десятки тисяч "кібер-поліцейських", що слідкують за Web-сайтами.

Західні фахівці так коментують те, що відбувається в Китаї: "Владі досить неважко стежити за Інтернет-кафе і подібними закладами. А в ширшому контексті, якщо ви маєте в своєму розпорядженні потрібну технологію, можна вести спостереження за Інтернетом в певних точках мережі Інтернет. Можна використовувати фільтри або ключові слова, які полегшують стеження за інформацією. Китайський механізм цензури не займається виключно пошуком підривних елементів. Він також формулює ідеї “морального еталону” в суспільстві. Так, наприклад, контролюються такі елементи як порнографія чи інші подібні, які на погляд держави неприйнятні для населення.

У той же час в Китаї нещодавно вступили в силу нові закони, що обмежують права громадян в Інтернет-сфері. Згідно з цими правилами, новинні сайти повинні пройти перереєстрацію (попередня реєстрація мала місце раніше цього року). Після цього інформація, яку публікують на сайтах, береться під ретельний контроль з боку державних органів. Заявлена мета нових правил – захист “національної безпеки” і “суспільних інтересів”.

Статистика свідчить, що в Україні набуває загрозливого характеру тенденція вчинення злочинів терористичної спрямованості з використанням вибухових пристроїв. За

останні два роки зареєстровано понад 560 таких актів, внаслідок яких загинуло 90 осіб і понад 200 дістали поранення. Ці злочини вчинені, в основному, у кримінальному середовищі з метою розподілу сфер впливу в незаконній підприємницькій діяльності, усунення конкурентів та залякування представників органів державної влади.

Вже сьогодні досить серйозною небезпекою для України є мережа Інтернет – невід'ємна складова в життєдіяльності держави. В чому ж її небезпека? Виявляється, суть у тому, що вся інформаційна інфраструктура повинна підключатися до мережі Інтернет. Україна вже стала частиною світового інформаційного простору, в якому фактично можуть виявитися не тільки електронні мережі навчальних закладів, а й парламентські, й урядові. База для цього вже підготовлена. Так, складання документів в Адміністрації Президента ведеться в рамках окремої мережі, Верховна Рада також має свою мережу, міністерства, регіональні адміністрації – свої. Тепер завдання полягає в тому, щоб накинути на всі ці мережі загальне павутиння і прив'язати їх через Інтернет до глобального інформаційного простору. Таким чином, центральні та місцеві електронні інформаційні мережі України можуть виявитися об'єктами впливу інформаційної зброї. Як Україна могла б протидіяти потенційним терористичним загрозам? Передусім необхідна оцінка загрози. І тут перше слово, напевне, належить розвідці. Необхідно безперервне відстеження всього комплексу проблем, що стосуються розвитку інформаційної зброї і підготовки до інформаційної війни у кіберпросторі держав, які мають найбільш досконалу інформаційну інфраструктуру.

Говорячи конкретно, необхідна достовірна та компетентна оцінка інформаційної зброї та способів її застосування. Потрібний також періодичний аналіз геостратегічної ситуації з точки зору ймовірності виникнення загрози скоєння терористичних актів. Ці оцінки та аналіз можуть бути підгрунттям для вироблення національної концепції протидії (нейтралізації) загрози такої небезпеки.

Суворе дотримання правил та превентивних заходів протидії тероризму має стати одним з основних вимог в економічній, військовій та науково-технічній політиці України. Ці правила слід чітко систематизувати і конкретизувати. А загалом кажучи, необхідний "Інформаційний антитерористичний кодекс", що містить чітке визначення: інформаційна політика держави повинна бути протекціоністською, спрямованою на розвиток українських розвідувальних інформаційних технологій, що захищає від терористів. Ось чому необхідний технічний контроль над інформаційними системами, контроль за спеціальною методикою, розробку якої варто було б доручити відповідним науково-дослідним інститутам. Крім того варто було б подумати над питання розробки власної операційної системи з дотриманням вимог конфіденційності розробки і захисту програмних кодів.

Участь України у міжнародних системах телекомунікацій та обміну інформацією повинна носити плановий характер і бути монополією держави. Тільки за цієї умови Україна може зберігати "інформаційну незалежність" і приймати в централізованому порядку необхідні контрзаходи для протидії терористичним нападам. Оскільки сьогодні неможливо чітко визначити сили та засоби для проведення терористичних актів, на наш погляд, доцільно створення колегіального органу, головними напрямками діяльності якого могли б бути: координація зусиль та розподіл повноважень між силовими та іншими відомствами, розвиток теоретичної бази, розвідка та постійний моніторинг тенденцій до змін форм і способів проведення терористичних актів. В такому колегіальному органі повинні мати обов'язкове представництво всі силові відомства.

Нині в Україні відсутні як цілісна система інформаційної безпеки держави в частині протидії агресії (у тому числі військової, терористичної тощо), так і механізм координації заходів з превентивних заходів щодо виявлення терористичних угруповань в державних інтересах. Вся мережева активність кимось пильно відстежується і фіксується. Мова йде не про терористів, хакерів або педофілів, а й про простих користувачів. Яскравим прикладом активної роботи спецслужб України та інших держав щодо контролю інформаційних та інших мереж є перехоплення спілкування на території України іноземних спостерігачів, послів та представників іноземних держав, учасників євромайданів, самооборони, сепаратистів, бандформувань та інших.

Висновки

1. На різних етапах насильницького протистояння, залежно від його форм та інтенсивності, а головне – природи терористичного конфлікту – держави вживають багатосторонні заходи, спрямовані на своєчасне виявлення та усунення причин і умов, що можуть призвести до проявів тероризму (не виключаючи й силового). У практичному плані це означає потребу у диверсифікації антитерористичних методів, що враховують

специфіку та модифікацію виявів тероризму, а також у диференційованому підході до протидії даній загрозі в кожній окремій країні та регіоні світу.

2. Забезпечення ефективної реалізації державної політики у сфері боротьби з тероризмом досягається шляхом розроблення і впровадження комплексу заходів, які визначені Концепцією боротьби з тероризмом (Указ Президента України від 25 квітня 2013 р.). Необхідно продовжити створення дієвої загальнодержавної системи координування антитерористичної діяльності з використанням наявних сил та засобів.

3. Своєчасне виявлення і припинення терористичної діяльності має здійснюватися шляхом підвищення ефективності розвідувальних, оперативно-розшукових і оперативно-технічних заходів шляхом надання їм доступу до інформаційних ресурсів органів державної влади у порядку, встановленому законодавством; підготовки, організації і здійснення комплексних скоординованих антитерористичних заходів у разі вчинення або загрози вчинення терористичних актів.

СПИСОК ЛІТЕРАТУРИ

1. Концепція боротьби з тероризмом, яка схвалена Указом Президента України від 25 квітня 2013 року.
2. Закон України “Про боротьбу з тероризмом” від 20 березня 2003 року // Відомості Верховної Ради України: – 2003 – № 25.
3. China's Information Revolution: Managing the Economic and Social Transformation, by Christine Zhen-Wei Qiang, p. 39-51
4. Linux Journal. Volume 2011 Issue 210, October 2011, Article No. 6.
5. Назаркин М.В. Криминологическая характеристика и предупреждение терроризма: Дис. канд. юрид. наук. – М., 1998.
6. Fox News from August 06, 2013.
7. http://en.wikipedia.org/wiki/Edward_Snowden.
8. http://www.wisegeek.org/what-is-a-packet-sniffer.htm.
9. http://www.dss.gov.au/our-responsibilities/indigenous-australians/publications-articles/evaluation-research/petrol-sniffing-in-indigenous-communities/whole-of-strategy-evaluation-of-the-petrol-sniffing-strategy-future-directions-for-the-pss-2013.
10. http://www.smh.com.au/comment/blogs/blunt-instrument/tea-and-sympathy-over-internet-threats-20131105-2wxuz.html.
11. Миньковський Г.М., Ревин В.П. Характеристика терроризма и некоторые направления повышения эффективности борьбы с ним // Государство и право. – 1997. №8.