9. Obraztsov, V.A. (2003), *Seriynye ubiystva kak ob'ekt psikhologii i kriminalistiki. Uchebnoe i prakticheskoe posobie* [Serial murders as an object of psychology and criminology. Training and practical guide], Omega Omega-L, IMPE them. Griboyedov, Moscow, Russia.

10. Zinin, A.M. (2003), "Problems forensic identification", *Vestnik kriminalistiki*, Vol. 4 (8), p. 32.

11. Stolyarenko, A.M. (2001), *Prikladnaya yuridicheskaya psikhologiya* [Applied juridical psychology], UNITY-DANA, Moscow, Russia.

12. Saltevskiy, M.V. (1977), *Teoriya i praktika polucheniya informatsii o prestupnike dlya ego rozyska i otozhdestvleniya* [Theory and practice of receiving information about the criminal for him investigation and identification], KVS Ministry of Internal Affairs of the USSR, Kyiv, Ukraine.

13. Kalyuha, K.V. (2011), "The problem of assembly "forensic portrait" of the offender and his use of the initial investigation", *Scientific and Production Journal "State and Regions" series Law*, no. 4, pp. 164–167.

14. Kalyuha, K.V. (2012), "Areas of use "forensic portrait" at the initial stage of investigation", *Informatyzatsiya sudovo-ekspertnoyi diyalnosti : materialy "kruhloho stolu"*, [Informatization of judicial expert activity : materials "round table"], Kyiv, NNIPSK NAVS, March 29, 2012, pp. 126-131.

15. Baulin, Ju.V., Borysov, V.I., Gavrysh, S.B. et al. (2003), *Kryminalnyi kodeks Ukrainy : Naukovo-praktychnyi komentar* [The Criminal Code of Ukraine : Scientific-practical commentary], Concern Publishing House «In Jure», Kyiv, Ukraine.

УДК 343.3/.7

ЩОДО ОЦІНЮВАННЯ ТЕРОРИСТИЧНОЇ УРАЗЛИВОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Варенья Н.М., аспірант

Національна академія СБ України, вул. О. Трутенка, 22, м. Київ, Україна
karver@i.ua

У статті розглянуто підходи до прогнозування рівнів терористичної небезпеки, окреслено основні проблеми в установленні оцінки уразливості об'єкта терористичного посягання та визначено переваги застосування кількісного методу оцінювання ризику терористичної події. Подано основні організаційні заходи, спрямовані на постійне вдосконалення системи антитерористичного захисту, що дасть змогу виявляти й передбачати настання загроз терористичного характеру за допомогою одержаних даних про можливий характер і масштаби наслідків впливу на об'єкт уражаючих факторів стихійних лих, аварій, катастроф і терористичних актів, виявляти найбільш уразливі елементи підприємств тощо. Запропоновано методику оцінювання терористичної уразливості об'єктів критичної інфраструктури за допомогою реєстру загроз терористичного характеру на основі моніторингу індикаторів терористичної загрози та аналітичної підтримки процесів підготовки до прийняття управлінських рішень в умовах кризових і надзвичайних ситуацій.

Ключові слова: критична інфраструктура, профілактика тероризму, реєстр загроз, терористична уразливість об'єктів, моніторинг, оцінювання ризику.

К ОЦЕНКЕ ТЕРРОРИСТИЧЕСКОЙ УЯЗВИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Варенья Н.М.

Национальная академия СБ Украины, ул. А. Трутенко, 22, г. Киев, Украина
karver@i.ua

В статье рассмотрены подходы к прогнозированию уровней террористической опасности, обозначены основные проблемы в установлении оценки уязвимости объекта террористического посягательства и определены преимущества применения количественного метода оценки риска террористического события. Приведены основные организационные мероприятия, направленные на постоянное совершенствование системы антитеррористической защиты, что позволит выявлять и предвидеть наступление угроз террористического характера с помощью полученных данных о возможном характере и масштабах

последствий воздействия на объект поражающих факторов стихийных бедствий, аварий, катастроф и террористических актов, выявлять наиболее уязвимые элементы предприятий и тому подобное. Предложена методика оценки террористической уязвимости объектов критической инфраструктуры с помощью реестра угроз террористического характера на основе мониторинга индикаторов террористической угрозы и аналитической поддержки процессов подготовки к принятию управленческих решений в условиях кризисных и чрезвычайных ситуаций.

Ключевые слова: критическая инфраструктура, профилактика терроризма, реестр угроз, террористическая уязвимость объектов, мониторинг, оценка риска.

EVALUATION ON TERRORIST VULNERABILITY OF CRITICAL INFRASTRUCTURE OBJECTS

Varenya N.M.

National Academy of Security Service of Ukraine, str. A. Trutenka, 22 s. Kyiv, Ukraine
karver@i.ua

The article discusses approaches to forecasting levels of terrorist threat, namely the “gray”, “blue”, “yellow”, “red”. The basic problem in establishing vulnerability assessment targets of terrorist attacks. Work to assess the vulnerability of objects of terrorist attacks should be analytical, a key aspect of the Security Service of Ukraine in the fight against terrorism is adaptive flexible response to changing threat levels at the sites of possible terrorist attacks. Advantages of quantitative method for assessing the risk of terrorist events.

The main organizational measures aimed at continuous improvement of antiterrorist protection system that will detect and anticipate the onset of terrorist threats character by using the received data on the possible nature and scale effects on the object of damaging factors of natural disasters, accidents and terrorist attacks, detection the most vulnerable elements of enterprises. These measures, first of all, should be directed to: forming the most complete and optimal composition of the system of anti-terrorist protection and determination Chief among them; distinction between entities of the anti-terrorist protection of basic, additional and support functions that provide the tasks based on their competence; exclusion of duplicate functions and tasks in competence of the system of antiterrorist protection; Guidance for the problem of anti-terrorist protection, including coordination and interaction The method of estimation of terrorist vulnerability of critical infrastructure register using threats of a terrorist nature based monitoring indicators of terrorist threats and analytical support processes to prepare management decisions in crisis and emergency situations.

Arrangements aimed at continuous improvement of the system of anti-terrorist protection and the fight to improve its performance and stability, based on international and domestic situation. These measures, first of all, should be directed to: forming the most complete and optimal composition of the system of anti-terrorist protection and determination Chief among them; distinction between entities of the anti-terrorist protection of basic, additional and support functions that provide the tasks based on their competence; exclusion of duplicate functions and tasks in competence of the system of antiterrorist protection; Guidance for the problem of anti-terrorist protection, including coordination and cooperation.

The primary purpose of quantitative methods of risk assessment is to identify violations of security facilities terrorism vulnerability assessment of the potential threats and develop proposals to reduce the risk of terrorist attacks. One of the most important elements of the process of risk assessment is to determine the vulnerability of critical infrastructure that is based on scenarios of possible terrorist events. Decisions taken in the assessment of vulnerabilities fall into two categories: quantitative model is based on the theory of values and adapted to complex systems using morphological analysis and model based on the theory of the likelihood of a terrorist event. Problems vulnerability assessment object of a terrorist attack are: to assess the risks of terrorism in the future can not be taken as an example of one event; the danger of underestimating the terrorist attack (to avoid criticism), or under its probability of occurrence (to justify investments in securities); Message to the media (some of the data collected can not be used in connection with the stamp of secrecy).

Key words: critical infrastructure, prevention of terrorist threats register, terrorist vulnerability facilities, monitoring, risk assessment.

В умовах підвищеного рівня небезпеки терористичної загрози в державі одним із найважливіших аспектів контртерористичної діяльності є ефективна та об’єктивна оцінка рівня терористичної уразливості об’єктів критичної інфраструктури. Крім того, в умовах глобальної інформатизації суспільства потребують значного доопрацювання підходи до моніторингу, аналізу і прогнозування рівнів терористичної небезпеки, а також до процесів підготовки управлінських рішень на різних рівнях державного управління.

Особливе місце в загальній картині загроз національній безпеці посідають загрози терористичного характеру (далі – ЗТХ), що свідчить про актуальність і нагальну необхідність створення дієвої системи аналізу ЗТХ та оцінювання їх впливу на найважливіші сфери забезпечення національної безпеки, яка б базувалася на сучасних інформаційних технологіях і забезпечувала оперативну протидію цим загрозам.

Сучасні наукові праці вітчизняних і закордонних науковців переважно присвячені кримінологічному аспекту тероризму та розробці оперативно-тактичних прийомів боротьби з терористичною діяльністю. Принципово важливим моментом є уточнення функцій і завдань суб’єктів боротьби з

тероризмом, а також розробка алгоритмів їхніх дій у різних умовах. Неабияка увага приділяється науковому супроводженню цих питань, дослідженню та формальному опису загроз у сфері національної безпеки, розробці паспортів загроз для подальшого застосовування механізмів прогнозування [1]. Про це свідчать публікації таких вітчизняних авторів, як В.І. Абрамов, В.В. Крутов, А.Б. Качинський, В.А. Ліпкан, В.А. Мандрагеля, Г.П. Ситник, І.М. Рижов, А.І. Семенченко, В.І. Строгий, І.В. Романов, І.В. Вещицький, М.В. Сунгуровський, В.М. Телелим та інші вчені-дослідники. Проте науково-методична база формалізації загроз теоретичного характеру та механізмів їх моделювання потребує розширення й подальшого вдосконалення.

Метою статті є аналіз методик оцінювання терористичної уразливості об'єктів критичної інфраструктури за допомогою реєстру загроз терористичного характеру, яка ґрунтуватиметься на моніторингу індикаторів терористичної загрози, а також забезпечення інформаційної й аналітичної підтримки процесів підготовки управлінських рішень на різних рівнях державного управління в умовах кризових і надзвичайних ситуацій.

Інформатизація останніми роками стає основою інтенсивного перетворення процесу підготовки управлінських рішень на всіх рівнях державного управління й починає забезпечувати адекватне наявним умовам прогнозування, планування й управління; збір, передачу, переробку й збереження інформації; залучення інтелектуального потенціалу до процесу прийняття рішень тощо. Інформатизація стає найважливішим фактором, що забезпечує погодженість під час вироблення й реалізації управлінських рішень і враховує відомості про прогнозовані й такі, що вже виникли, надзвичайні ситуації природного й техногенного характеру та їх наслідки, про радіаційну, хімічну, біологічну, терористичну, екологічну безпеку на відповідних територіях, а також відомості щодо діяльності підприємств, установ і організацій незалежно від форм власності, органів місцевого самоврядування, центральних і територіальних органів влади, інших об'єктів критичної інфраструктури [5].

У чинному законодавстві досі не визначено термін «критична інфраструктура», хоча в новій редакції Стратегії національної безпеки серед шляхів зміцнення енергетичної безпеки визначено «дієвий захист критичної інфраструктури паливно-енергетичного комплексу від еколого-техногенних впливів та зловмисних дій», а одним зі шляхів забезпечення інформаційної безпеки зазначається «забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури». Водночас необхідно розуміти, що підготовка території держави до оборони – категорія набагато ширша, ніж захист критичної інфраструктури [2, с. 22].

У лютому 2016 року Кабінет Міністрів України затвердив чотири рівні терористичної загрози в Україні. Про це йдеться в Постанові від 18 лютого 2016 р. № 92, опублікованій на офіційному сайті Уряду, де рівень терористичної загрози тимчасово встановлюється для всіх або окремих суб'єктів боротьби з тероризмом і діє на всій території України, в окремих її місцевостях або на об'єктах можливих терористичних посягань [4].

Залежно від наявної інформації про загрозу вчинення теракту, встановлюються такі рівні терористичних загроз:

– «сірий» (можлива загроза) – за наявності чинників (умов), які сприяють учиненню терористичного акту;

– «синій» (потенційна загроза) – за наявності інформації, яка потребує підтвердження, про підготовку до вчинення терористичного акту;

– «жовтий» (можлива загроза) – за наявності достовірної (підтвердженої) інформації про підготовку до скоєння терористичного акту;

– «червоний» (реальна загроза) – найвищий рівень терористичної загрози.

Для детального аналізу та конкретизації інструктивно-методичних рекомендацій доцільно в загальному вигляді виділити вісім типових ситуацій:

1. Загострення криміногенної обстановки в регіоні або місті у зв'язку з несприятливими соціально-політичними та економічними процесами в країні.

2. Отримання керівником або персоналом об’єкта конкретних погроз терористичного характеру телефоном, у вигляді анонімних листів або іншими засобами комунікації.
3. Виявлення персоналом об’єкта предмета з явними ознаками вибухо-запалювального пристрою чи іншого вибухонебезпечного предмета, здатного заподіяти смерть, серйозні каліцтва людям або істотну матеріальну шкоду об’єкту.
4. Виявлення підозрілих предметів, що потребують спеціальної перевірки з метою встановлення їх реальної вибухо-пожежної небезпеки.
5. Учинення терористичної акції (або диверсії) способом вибуху, підпалу, що призвело до людських жертв, знищення й пошкодження матеріальних цінностей, паніки.
6. Учинення терористичної акції шляхом захоплення й утримання заручників на території об’єкта.
7. Взаємодія з правоохоронними органами та іншими відомствами, які прибули на об’єкт за фактом події терористичного чи диверсійного характеру.

Робота з оцінювання уразливості об’єктів терористичних посягань має бути аналітичною. На нашу думку, ключовим аспектом діяльності Служби безпеки України щодо боротьби з тероризмом є адаптивне гнучке реагування на зміни рівня загрози на об’єктах можливих терористичних посягань.

Як відомо, соціальна система характеризується наявністю множини теророгенних факторів, які формують загрози терористичного характеру. За певних умов (у разі неможливості розв’язання сутності суперечності) соціальний конфлікт може призвести до насильства в суспільстві. Тому для діяльності державної системи боротьби з тероризмом виявлення загроз терористичного характеру є основним етапом організаційно-профілактичної діяльності. Розрізняючи конкретні види терористичної діяльності за різними ознаками (за формою, засобами здійснення, історичними, національними, релігійними, географічними й іншими особливостями, за окремими елементами структури діяльності тощо), можна виробити практично нескінченний ряд видів загроз терористичного характеру [3]. Це різноманіття має під собою реальну основу – конкретні вияви тероризму на практиці, становить теоретичний інтерес як специфічна особливість явища. При цьому ряд теророгенних факторів буде на порядок вищим.

Варто нагадати: якщо причини та цілі терористичної діяльності – категорії реальні й конкретні, то її мотивація в повному обсязі рідко усвідомлюється діючим суб’єктом і значною мірою знаходиться на несвідомому рівні. Тому за всієї важливості психофізіологічного й біологічного аспектів дослідження терористичної діяльності результати, що виявляються в процесі їх аналізу, не можуть бути використані як параметри для типологічної класифікації в межах моделювання теророгенності соціальних систем, але мають бути опосередковано враховані в експертному висновку щодо ступеня захищеності від терористичної загрози.

У процесі реалізації принципу системності в загальнодержавному процесі боротьби з тероризмом особливе місце відводиться організації та забезпеченню дієвості системи превентивних заходів. Основною метою є відпрацювання комплексного усунення причин та умов, що сприяють виникненню злочинних виявів у тому числі терористичної спрямованості.

Для регулювання рівня загроз використовується спеціальний інструментарій, основу формування якого становить класифікація загрозливих факторів [3]. Надалі можливе прогнозування розвитку цих факторів з урахуванням вірогідних змін ситуації, впливів інших факторів, норм і правил тощо. Якщо в результаті прогнозування матимемо на увазі такий вихід, що прямо або побічно сприяє виникненню ЗТХ, можливо визначити об’єкт, який підпадає під сферу впливу цього фактора. Прогнозування може здійснюватися будь-яким із відомих методів, при цьому повинні враховуватися необхідні й достатні умови переростання конфлікту в терор.

З метою об’єктивного визначення ступеня небезпеки або теророгенного потенціалу тієї чи іншої загрози, можуть бути запроваджені формальні критерії, визначення яких і становить основне завдання інформаційно-аналітичної діяльності.

Намагаючись упорядкувати наявні класифікації за загальними критеріями, пропонуємо ділити сучасний тероризм двох видів (міжнародний і внутрішній) на п’ять типів – соціальний, націоналістичний, релігійний, «лівий» і «правий», виділяючи декілька форм – політичну, кримінальну, інформаційну, психологічну тощо. У загальному вигляді алгоритм розпізнавання

теророгенних факторів можна умовно звести до двох стадій. Перша стадія, у процесі якої з усієї сукупності факторів, що визначають стан соціального середовища, вибираються (найчастіше на інтуїтивній основі) такі, що призводять до виникнення конфліктних ситуацій. У нашому випадку ми визначили 13 таких класів у сферах:

1) зовнішньополітичній;
2) державної та громадської безпеки;
3) внутрішньополітичній (соціальній);
4) етноконфесійній;
5) фінансово-економічній;
6) екологічній;
7) воєнній;
8) інформаційної безпеки;
9) фінансування тероризму;
10) санітарно-епідеміологічній і медичній;
11) функціонування об'єктів критичної інфраструктури;
12) функціонування об'єктів транспорту і зв'язку;
13) функціонування об'єктів системи державного управління та місцевого самоврядування.

Кодування загроз складається з трьох рівнів класифікації: клас, підклас, група. Метод класифікації – ієрархічний, послідовний, шестизначний. Позиція класифікатора має блок ідентифікації та блок назви класифікаційного угруповання.

Друга стадія передбачає прогнозування розвитку цих факторів з урахуванням можливих змін ситуації, впливів інших факторів, норм і правил тощо. Якщо в результаті прогнозування можливий такий вихід, що прямо або побічно сприяє виникненню тероризму, ці фактори можна вважати небезпечними. Прогнозування може здійснюватися будь-яким із відомих методів, при цьому повинні враховуватися необхідній достатні умови переростання конфлікту в терор.

Наступним кроком використання реєстру загроз терористичного характеру є визначення конкретного типу загрози. Варто зазначити, що реєстр повинен бути відкритим, тобто давати змогу нарощувати як класи, так і типи загроз кожного класу.

Підсумком роботи з оцінювання уразливості є одержання науково обґрунтованих даних про можливий характер і масштаби наслідків впливу на об'єкт уражаючих факторів стихійних лих, аварій, катастроф і терористичних актів, виявлення найбільш уразливих елементів підприємств (будинків, споруджень, комунально-енергетичних мереж, транспорту тощо), а також упровадження необхідних заходів у відповідних сферах.

Політичні заходи спрямовані на викриття підривного характеру діяльності тероризму через ЗМІ, проведення широкої роз'яснювальної роботи серед місцевого населення, виховання робітників і службовців об'єктів підвищеної небезпеки (потенційно небезпечних об'єктів), населення та військовослужбовців у дусі високої пильності й постійної готовності до боротьби з терористичними виявами. У здійсненні політичних заходів у боротьбі з тероризмом повинні брати участь органи державної влади та управління, громадські організації, прокуратура, суди тощо [6, с. 72].

Організаційні заходи спрямовані на постійне вдосконалювання системи антитерористичного захисту й боротьби для підвищення ефективності її функціонування та стійкості, виходячи з міжнародної і внутрішньої обстановки. Ці заходи повинні бути направлені передусім на таке:

– формування найбільш повного й оптимального складу суб'єктів системи антитерористичного захисту та визначення головного серед них;
– розмежування між суб'єктами системи антитерористичного захисту основних, додаткових і допоміжних функцій, які забезпечать виконання завдань, виходячи з їхньої компетенції;

– виключення дублюючих функцій і завдань у компетенції суб'єктів системи антитерористичного захисту;

– науково-методичне забезпечення виявлення проблем організації антитерористичного захисту, враховуючи питання координації та взаємодії [9].

Ризик настання терористичної події в тому чи іншому місці може бути успішно змодельований як процес управління. Що стосується галузі інженерного аналізу ризику, де загроза розглядається як навантаження або сила, що діє на систему, то уразливість можна розглядати як здатність системи реагувати на цю загрозу. Щоб використовувати це визначення для вимірювання, треба ставити конкретне запитання: «До чого уразливий об'єкт посягання?» Таке визначення ймовірності може бути використане в процесі запобігання терористичним нападам [10, с. 115].

Міра (вразливість): Об'єкт, який пошкоджує ймовірність (де збитки можуть бути пов'язані зі смертельними наслідками, травмами, пошкодженням майна або іншими наслідками) статися, враховуючи конкретний тип атаки, в певний час. Уразливість = Можливість (результати атаки на шкоду | атака відбувається).

Іншими словами, уразливість об'єкта може бути сформульована як імовірність того, що атака заданого типу буде успішною [11, с. 74].

Основна мета застосування кількісних методів оцінювання ризику полягає у виявленні порушень системи безпеки об'єктів терористичної уразливості, оцінюванні ймовірності виникнення загроз і виробленні пропозицій для зниження ризиків терористичних нападів. Одним із найважливіших елементів процесу оцінювання ризику є визначення уразливості критичної інфраструктури, що заснована на можливих сценаріях терористичної події. Рішення, прийняті в результаті оцінювання уразливості, діляться на дві категорії: кількісна модель, побудована на основі теорії значень і адаптована до складних систем із використанням морфологічного аналізу, і модель, що заснована на теорії ймовірності настання терористичної події [7, с. 8].

Щоб зрозуміти аналіз ризиків зовнішніх тисків у встановленні рівня загрози особливо для оцінювання уразливості й наслідків можливих атак, ми пропонується використовувати кількісний підхід. Застосування кількісного методу оцінювання ризику терористичної події має такі переваги:

1. Зниження ризику атаки для деяких об'єктів шляхом перетворення їх у менш привабливі для терористичних нападів.

2. Підвищення стійкості системи захисту об'єктів.

3. Скорочення часу відновлення після нападу.

4. Запобігання поширенню каскадних ефектів.

Процес оцінювання ризику тероризму можна розглядати в контексті загальної структури, в якій рівень уразливості визначає ефективність системи (див. рис. 1.1).

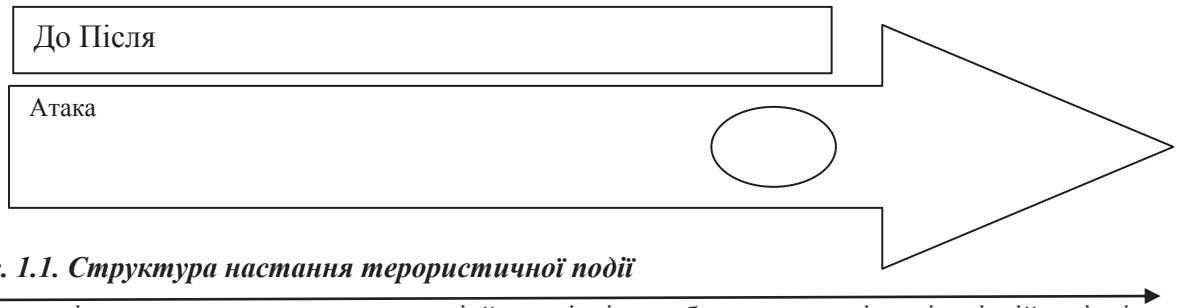

Рис. 1.1. Структура настання терористичної події

Етапи оцінювання загрози, уразливості й наслідків особливо важливі в кількісній оцінці ризику, оскільки вона вимагає, з одного боку, наявності фахівців у сфері розвідки критичної структури, з іншого – взаємодії та забезпечення своєчасної інформації, необхідної для подальших випробувань. Ми можемо говорити про такий процес управління ризиками з метою підвищення рівня розуміння самого ризику, уразливості й наслідків нападу з використанням кількісної та якісної оцінки, що дає змогу прийняти рішення щодо впровадження механізмів запобігання терористичним загрозам, їх потенційним наслідкам і виявлення їх [8, с. 89]. Ризик безпеки тоді розглядається як функція від

характеру загрози, уразливості для атаки на системи й наслідків, пов'язаних із можливим сценарієм атаки.

Під час аналізу ризику уразливість об'єкта оцінюється за ймовірністю відомих даних або сприймається як існування недоліків інфраструктури для певного періоду часу в контексті сценарію певного типу загрози (див. залежність 1.2):

Уразливість = Імовірність (успішної атаки) (1.2).

Оцінка уразливості визначається здатністю системи виявляти терористичні події, щоб їм запобігти, або ж у разі настання надати відповідний опір.

Проблеми оцінювання уразливості об'єкта терористичного посягання полягають у такому [12, с. 4]:

1. Для оцінювання ризиків тероризму в майбутньому не можна брати за приклад одну подію.
2. Небезпека недооцінки теракту (щоб уникнути критики) або завищення його ймовірності настання (для обґрунтування вкладів у цінні папери).
3. Повідомлення для засобів масової інформації (деякі зібрані дані не можуть бути використані у зв'язку з грифом секретності).

Виходячи з викладеного, можемо констатувати, що формування реєстру загроз терористичного характеру у вигляді уніфікованого інформаційного ресурсу сприятиме вивченню ступеня готовності територіальних громад, регіональних підрозділів суб'єктів боротьби з тероризмом й окремих об'єктів до протидії можливим терористичним загрозам. Запропоновані підходи до оцінювання терористичної уразливості об'єктів критичної інфраструктури можуть бути використані для отримання результатів і подальшого аналізу процесів і явищ, що виникають за умови виявлення загроз терористичного характеру, розробки організаційно-профілактичних заходів щодо локалізації найбільш небезпечних загроз, а також як вихідні дані під час проведення математичного та імітаційного моделювання. Крім цього, системний підхід дасть змогу розробити комплекс заходів щодо парирування загроз уже на стадії проектування, тим самим позбавивши себе зайвих витрат надалі, а встановлення та осмислення принципів антитерористичної медіаінформаційної діяльності дасть можливість розробити комплекс відповідних і дієвих заходів щодо нейтралізації медіатероризму.

ЛІТЕРАТУРА

1. Богданович В.Ю. Теоретико-методологічні основи забезпечення національної безпеки України : [монографія] : у 7 т. / В.Ю. Богданович, І.Ю. Свида, Є.Д. Скулиш ; за заг. ред. Є.Д. Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2012. – Т. 1 : Теоретичні основи, методи й технології забезпечення національної безпеки України. – 2012. – 548 с.
2. Нормативно-правова база у галузі безпеки і оборони України. – 2-е видання, доповнене. – К. : Центр дослідження армії, конверсії та роззброєння, 2012. – 820 с.
3. Рижов І.М. Досвід Федеративної Республіки Німеччини з формування концепції антитерористичного захисту критичної інфраструктури / І.М. Рижов, В.Г. Хлань, М.В. Мірошник // Зб. наук. пр. НА СБ України. – 2014. – № 51. – С. 134–141.
4. Ситник Г.П. Державне управління національною безпекою України (теорія і практика) : [монографія] / Г.П. Ситник. – К. : НАДУ, 2004. – 408 с.
5. Тероризм : визначення і сутність : [монографія] / [А.В. Коростиленко, Б.Д. Леонов, І.М. Рижов та ін.] ; під заг. ред. В.В. Крутова, І.І. Мусієнка, В.О. Глушкова. – К. : Нац. акад. СБУ, 2015. – 192 с.
6. Устименко О.В. Захист критичної інфраструктури держави як складова підготовки території країни до оборони / О.В. Устименко // Національні інтереси України : ступінь реалізації та загрози : матеріали круглого столу (Київ, 27.11.2013). – К. : Національна академія державного управління при Президентові України, 2013. – С. 27–32.
7. ФЦП «Снижение рисков и смягчение последствий чрезвычайных ситуаций природного и техногенного характера в Российской Федерации до 2010 года» [Электронный ресурс]. – Режим доступа : http ://www.mchs.gov.ru/activities/fcp/archive_fcp/FCP_Snizhenie_riskov_i_smjagchenie_posle.

8. Ezell, B. C. (2007). Infrastructure Vulnerability Assessment Model (I-VAM), Risk Analysis, 27 (3), 571-83.

9. Haimes, Y.Y. (2004). Risk Modeling, Assessment, and Management, Second Edition, John Wiley & Sons, New Jersey, U.S.A., pp. 276-294.

10. Parnell, G.S., Jackson, J.A., Jones, B.L., Lehmkuhl, L.J., Conley, H.W., Andrew, J.M. (1998) : Foundations 2025 : A Value Model for Evaluating Future Air and Space Forces, Management Sciences, 44 :10, pp.1336–1350.

11. Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks programme (CIPS) [Electronic resource]. – Access mode : http ://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrori sm/l33262_en.htm.

12. U.S. Congress (2001). U.S. Patriot Act of 2001, P.L. 107-56, Sec. 1016(e), The Library of Congress, 2001.

REFERENCE

1. Bohdanovych, V. Yu. (2012), *Teoretyko-metodolohichni osnovy zabezpechennya natsionalnoyi bezpeky Ukrayiny : monohrafiya. : u 7 t.* [Theoretical bases, methods and technology of national security Ukraine], vyd. viddil NA SB Ukrainy, vol. 1 *Teoretychni osnovy, metody y tekhnolohiyi zabezpechennya natsionalnoyi bezpeky Ukrayiny* [Theoretical bases, methods and technologies of providing of national safety of Ukraine], Kyiv, Ukraine.

2. (2012), *Normatyvno-pravova baza u haluzi bezpeky i oborony Ukrainy* [The legal framework in the field of security and defense of Ukraine], Tsentr doslidzhennia armii, konversii ta rozzbroiennia, Kyiv, Ukraine.

3. Ryzhov, I.M. (2014), "Experience the Federal Republic of Germany to form the concept of anti-terrorist protection of critical infrastructure", *Zbirnyk nauk. prac NA SB Ukrainy*, vol. 51, pp. 134-141.

4. Sytnyk, H.P. (2004), *Derzhavne upravlinnya natsionalnoyu bezpekoyu Ukrayiny (teoriya i praktika) : monografiya* [Public administration national security of Ukraine (theory and practice) : monograph], NADU, Kyiv, Ukraine.

5. Korostylenko, A.V., Leonov, B.D., Ryzhov I.M. et al. (2015), *Teroryzm : vyznachennya i sutnist : monohrafiya* [Terrorism : definition and nature : monograph], Kyiv, Nats. akad. SBU, Ukraine.

6. Ustymenko, O.V. (2013), "Protecting critical infrastructure of the state as part of the preparation of the country for defense", *Natsionalni interesy Ukrainy : stupin realizatsii ta zahrozy : materialy kruhloho stolu*, [The national interests of Ukraine, and the extent to which threats : roundtable], Kyiv, National academy of state administration is at President of Ukraine, November 27, 2013, pp. 27-32.

7. FTsP "Decline of risks and softening of consequences of extraordinary situations of natural and technogenic character in Russian Federation to 2010 year", available at : http ://www.mchs.gov.ru/activities/fcp/archive_fcp/FCP_Snizhenie_riskov_i_smjagch enie_posle.

8. Ezell, B. C., (2007). Infrastructure Vulnerability Assessment Model (I-VAM), Risk Analysis, 27(3), 571–83.

9. Haimes, Y.Y. (2004). Risk Modeling, Assessment, and Management, Second Edition, John Wiley & Sons, New Jersey, U.S.A, pp. 276–294.

10. Parnell, G.S., Jackson, J.A., Jones, B.L., Lehmkuhl, L.J., Conley, H.W., Andrew, J.M. (1998) : Foundations 2025 : A Value Model for Evaluating Future Air and Space Forces, Management Sciences, 44 :10, pp.1336–1350.

11. "Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks programme (CIPS)", available at : http ://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrori sm/l33262_en.htm.

12. U.S. Congress (2001). U.S. Patriot Act of 2001, P.L. 107-56, Sec. 1016(e), The Library of Congress.