сутенерство, який може використовуватись як прикриття протиправної діяльності;

– свідків та очевидців сутенерства або надання сексуальних послуг;

– причини і умови, що сприяють вчиненню сутенерства чи інших злочинів;

– подальші злочині плани осіб, які готують або вчиняють сутенерство;

– інші фактичні дані про вчинення злочину.

Згідно зі ст. 10 Закону України "Про оперативно-розшукову діяльність" [4] отримані матеріали оперативно-розшукової діяльності про сутенерство використовуються як приводи та підстави для початку досудового розслідування, а також для отримання фактичних даних, які можуть бути доказами у кримінальному провадженні.

---

1. Генеральна прокуратура України: офіційний веб-сайт – [Електронний ресурс]. – Режим доступу: https://www.gp.gov.ua/ua/stst2011.html?dir_id=104402

2. Єдиний державний реєстр судових рішень – [Електронний ресурс]. – Режим доступу: http://reyestr.court.gov.ua/

3. Кримінальний кодекс України від 05.04.2001 № 2341-III // Відомості Верховної Ради України, 2001, № 25-26, ст. 131.

4. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII // Відомості Верховної Ради України, 1992, № 22, ст. 303.

Єрменчук О.П.
кандидат юридичних наук
доцент кафедри
оперативно-розшукової діяльності
та спеціальної техніки
Дніпропетровського державного
університету внутрішніх справ

ЗМІСТ ПОНЯТТЯ ТА ЗНАЧЕННЯ ЗАГРОЗ КРИТИЧНІЙ ІНФРАСТРУКТУРІ ДЛЯ ЗАХИСТУ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Захист критичної інфраструктури (далі – КІ) належить до основних напрямів державної політики з питань забезпечення державної безпеки.

Все нові та небезпечні виклики регіональній і глобальній безпеці висувають на порядок денний завдання із побудови в Україні системи захисту критичної інфраструктури, важливою складовою якої є визначення загроз. Ефективність побудови цієї системи залежить в том числі і від стану наукової розроби зазначеної проблематики.

Питання ідентифікації загроз та організації заходів з протидії їм стає

актуальним для більшості держав. При цьому зростає і значення роботи з визначення та своєчасної ідентифікації загроз для вжиття адекватних заходів реакції з кожною такою подією. Якщо спочатку цей процес характеризувався локальним чи державним рівнем, то зараз можна стверджувати про його вихід на загальноєвропейський чи міжконтинентальний формат.

У США під «загрозами КІ» розуміють природні або техногенні явища, фізичні особи, суб'єкти чи дії, що містять або несуть потенційну шкоду для життя, інформації, операцій, навколишнього середовища та / або власності [1].

Серед основних загроз відповідальні інстанції ЄС визначають: кіберзагрози, тероризм, злочинні дії, природні небезпеки, аварії та інші причини нещасних випадків [2; 3].

Згідно з нормативно-правовими актами ЄС, «загроза» - будь-яка подія, яка може порушити або знищити критичну інфраструктуру або будь-який з її елементів [3].

Майже ідентичне визначення «загроз» дається в Зеленій книзі по захисту КІ ЄС, де під цим терміном розуміються будь-які обставини або події, що можуть порушити стале функціонування або знищити критичну інфраструктуру чи будь-який її елемент. Вони також включають спроби та наміри нанесення шкоди критичним активам [4].

Серед європейських країн доцільно виділити активну діяльність по ідентифікації та аналізу загроз КІ, що проводиться Німеччиною. Згідно «Концепції основних заходів із захисту КІ Німеччини», «загроза» визначається, як можливість настання подій (стихійних явищ, технічних збоїв чи людських прорахунків, помилок в поведінці людей), що можуть спричинити шкоду особам, матеріальним цінностям і навколишньому середовищу чи призвести до розладу соціальних та економічних відносин.

Притаманні для України загрози КІ можуть мати різновекторні спрямування та прояви. Вони можуть проявлятися у припиненні надання товарів та послуг, що є життєво важливими для населення, економіки, державного управління. Такими є забезпечення населення, суб’єктів господарювання та органів державної влади та самоврядування електроенергією, зв’язком, послугами з транспортних перевезень, водопостачання, водовідведення, каналізації тощо. Припинення надання таких товарів та послуг, в деяких випадках навіть суттєве підвищення вартості тарифів, може призводити до соціально-політичної нестабільності, загострення внутрішньополітичних конфліктів, значних економічних втрат, послаблення інститутів влади.

Особливу загрозу становить збройний конфлікт та гібридна війна, що активно проводиться стосовно України та пов'язані із ними загрози деструктивних дій з боку диверсійних груп, вчинення терактів, диверсій, шпигунства, кібератак, економічної експансії відносно об'єктів КІ тощо.

Завжди актуальними є загрози від надзвичайних ситуацій, які

поєднують в собі загрози природнього, техногенного характеру тощо.

Слід констатувати, що в Україні відсутнє законодавче визначення поняття «загроза критичній інфраструктурі» та немає загального підходу щодо їх класифікації. Як зазначають вітчизняні дослідники цієї наукової проблеми, така ситуація склалася природним чином: «кожне окреме відомство виділяло певний спектр загроз для підпорядкованих об'єктів та володіло певним набором інструментів і ресурсів для забезпечення їх безпеки» [5].

На думку ряду науковців, загрози КІ також доцільно розподіляти на три наступні групи, що включають: аварії й технічні збої, природні лиха та небезпечні природні явища, зловмисні дії (груп або окремих осіб, таких як терористи, злочинці й диверсанти, промислове шпигунство, а також бойові дії) [6].

Українські вчені з НІСД серед основних загроз КІ виділяють: надзвичайні ситуації (природні катастрофи, технологічні аварії), терористичні акти, диверсії, кіберзагрози; аварії та технічні збої, небезпечні природні явища, зловмисні дії, а також: техногенні аварії та технічні збої, викликані, зокрема, людськими помилками; природні лиха та небезпечні природні явища; зловмисні дії [5; 7; 8].

Здатність загроз уражати важливі елементи, що значно впливають на стан економічної безпеки держави та на суспільно-політичні аспекти зумовлює їх особливе значення для захисту національної безпеки.

Враховуючи національний досвід творення норм у сфері національної безпеки України та міжнародну практику, пропонується під визначенням «загроз об'єкту КІ» розуміти наявні або потенційно можливі явища і чинники, що можуть нанести шкоду такому об'єкту (фізичному або у кіберпросторі), вивести його з ладу або порушити функціонування відповідно до призначення чим створюють небезпеку життєво важливим національним інтересам України.

Загалом, серед загроз критичній інфраструктурі автором пропонується виділяти їх наступні види:

1) Загрози у сфері державної безпеки чи безпекового характеру (тероризм, диверсії, «навмисна помилка», розвіддіяльність іноземних спецслужб, економічні експансії, економічне та промислове шпигунство, конкурентна розвідка). Вони можуть включати внутрішні загрози та фізичне знищення КІ (при хуліганстві, підпалах, діяльності організованих злочинних угруповань, чинник «внутрішнього порушника»).

2) Кіберзагрози (інформаційні атаки, кібертероризм).

3) Загрози від надзвичайних ситуацій (аварії, катастрофи, стихійні лиха, пожежі, епідемії та пандемії, застосування засобів ураження або інші небезпечні події).

Часто, дія загроз може спричиняти «каскадний ефект» чи поширену у Європі назву процесу «ефект доміно», коли дестабілізація однієї складової КІ

тягне за собою порушення нормального функціонування інших складових та викликає широкомасштабне катастрофічне явище. Під «каскадним ефектом» від порушення функціонування КІ пропонується розуміти серію пов'язаних подій, кожна наступна з яких спричинена попередніми та тягне за собою настання нових.

На наше переконання, виділення загроз КІ та якісна організація протидії цим загрозам є необхідним процесом для підвищення захисту національної безпеки, особливо за сучасних умов та відповідає існуючим тенденціям в іноземній практиці.

1. National Critical Infrastructure Security and Resilience Research and Development Plan, 2015. URL: https://www.dhs.gov/publication.

2. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l33260 / European Program for Critical Infrastructure Protection.

3. Повідомлення Комісії Раді та Європейському Парламенту від 20.10.2004 року «Запобігання, готовність та реагування на терористичні напади» / COM (2004) 698 final – Official Journal від 20.01.2005. URL: https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex: 52004DC0702.

4. https://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf.

5. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі // Стратегічні пріоритети. Серія: Економіка. 2015. № 4. С. 90-92.

6. Радаев Н. Оценка террористической угрозы для объекта / Н. Радаев, А. Бочков. URL: http://mx1.algoritm.org/arch/77/77_3.pdf.

7. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України // Стратегічні пріоритети. Серія: Політика. 2016. № 3. С. 65-67.

8. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. нарад / упоряд. Д.С. Бірюков, С.І Кондратов; за заг. ред. О.М. Суходолі. Київ, 2016. 176 с.