УДК 351.863+338.246.87

ОЦІНКА ЗАГРОЗ КРИТИЧНІЙ ІНФРАСТРУКТУРІ ЯК ВАЖЛИВА СКЛАДОВА ЧАСТИНА ДІЯЛЬНОСТІ ІЗ ЗАХИСТУ ДЕРЖАВНОЇ БЕЗПЕКИ

Олександр ЄРМЕНЧУК,
кандидат юридичних наук, доцент кафедри
оперативно-розшукової діяльності та спеціальної техніки
Дніпропетровського державного університету внутрішніх справ
Міністерства внутрішніх справ України

АНОТАЦІЯ

У статті проаналізовано питання ідентифікації загроз критичної інфраструктури, оцінки їх потенціалу та організації протидії загрозам у процесі захисту об'єктів критичної інфраструктури і забезпечення державної безпеки. Визначено особливі походи в різних країнах. Аналіз і узагальнення іноземного досвіду дає змогу запропонувати науково обґрунтовану позицію за оцінкою загроз у процесі захисту критичної інфраструктури. Пропонується авторське визначення понять «загрози об'єкту критичної інфраструктури», «потенціал загрози», «навмисна помилка», «каскадний ефект». Серед загроз виділені конкретні види і дана їх характеристика.

Ключові слова: критична інфраструктура, захист критичної інфраструктури, національна безпека, визначення, загрози, поняття.

ASSESSMENT OF THREATS OF CRITICAL INFRASTRUCTURE AS AN IMPORTANT COMPONENT OF STATE PROTECTION

Oleksandr YERMENCHUK,
Candidate of Law Sciences, Associate Professor at the Department
of Operative-Investigative Activity Department and Specialist Equipment
Dnipropetrovsk State University of Internal Affairs
of the Ministry of Internal Affairs of Ukraine

SUMMARY

The issues of identifying threats to critical infrastructure, assessing their potential and organizing countering threats in the process of protecting critical infrastructure facilities and ensuring state security are analyzed. Defined special trips in different countries. Analysis and synthesis of foreign experience allows us to offer a scientifically based position on the assessment of threats in the process of protecting critical infrastructure. The author's definition of the concepts is proposed "threat to the object of critical infrastructure", "threat potential", "intentional error", "cascade effect". Among the threats identified specific types and given their characteristics.

Key words: critical infrastructure, protection of critical infrastructure, national security, definition, threats, concepts.

Постановка проблеми. Досвід провідних країн Європи свідчить, що захист критичної інфраструктури (далі – КІ) належить до основних напрямів державної політики з питань забезпечення державної безпеки.

Зазначене питання, безумовно, є актуальним для кожної держави. Його вагомість спричинюється різким посиленням світового тероризму, ростом злочинності, торгівельними війнами, економічними експансіями, руйнуванням та пошкодженням численних підприємств, у тому числі стратегічно важливих, інфраструктурних об'єктів, збільшенням фактів зазіхань на новітні технології конкурентів, природними катаклізмами. Все це та інші фактори вимагають від держав нових підходів до завчасного виявлення загроз та їх попередження і припинення. Адже завдяки своєчасній та якісній оцінці загроз і ризиків належного вжиття відповідних заходів із забезпечення стійкості можна передбачити наслідки і бути максимально підготовленими до них.

Якісна оцінка загроз і визначення їх потенціалу підвищує ефективність захисту КІ, оскільки дає змогу вживати превентивні заходи, націлювати сили органів державної безпеки та правоохоронних органів і спеціально уповноважених державних органів на конкретні контрзаходи.

Стан дослідження. Окремі питання, пов'язані з захистом критичної інфраструктури, були порушені в наукових працях таких українських вчених: Д.С. Бірюкова, Є.В. Брежнєва, Д.Г. Бобро, О.Ф. Величка, Д.В. Дубова, В.П. Горбуліна, С.П. Іванюти, В.В. Зубарєва, В.К. Конах, С.І. Кондратова, М.В. Мірошника, О.І. Насвіт, М.А. Ожевана, В.М. Панченко, В.В. Петрова, І.М. Рижова, П.П. Скурського, О.М. Суходолі, В.М. Щербини, О.М. Юрченка, однак основні підходи до побудови в Україні системи визначення загроз, тобто їх оцінки та прогнозу, в тому числі формування понятійно-категорійного апарату, потребують комплексного наукового дослідження.

Зазначені обставини зумовлюють актуальність дослідження та стали основою для наукових пошуків автора та підготовки цих матеріалів.

Мета і задача статті. Нові та небезпечні виклики регіональній і глобальній безпеці висувають на порядок денний завдання із побудови в Україні системи захисту критичної інфраструктури, важливою складовою частиною якої є визначення загроз. Ефективність побудови цієї системи залежить, у тому числі, і від стану наукової розробки зазначеної проблематики.

Виклад основного матеріалу. Узагальнення організаційно-правових підходів до захисту КІ у різних європейських державах дає змогу сформувати думку про те, що владні органи зазвичай приділяють досить важливу увагу процесу визначення загроз та формуванню їх переліків. У різних країнах спектр загроз критичній інфраструктурі та зміст поняття, хоч загалом містять багато подібного, визначаються індивідуально з урахуванням безпекової ситуації та пріоритетів розвитку визначених державною політикою [1]. Якщо в більшості держав вони законодавчо передбачені, то поряд із цим деякі з них можуть не мати чіткого переліку загроз. Так, на відміну від європейської, зокрема німецької системи розподілу загроз для об'єктів КІ, де чітко вирізнено основні їх види та підвиди і дається вичерпний їх перелік, США чіткого переліку таких загроз не мають. При цьому не існує загального єдиного підходу і до організації протидії їм [2].

Європейський дослідник у сфері захисту КІ М. Сметана стверджує, що останніми десятиліттями в Європі питання аналізу загроз значно актуалізувалось. Питання ідентифікації загроз та організації заходів із протидії їм стає актуальним для більшості держав та є особливо пов'язаним із загрозами природного характеру. При цьому значення роботи з визначення та своєчасної ідентифікації загроз для вжиття адекватних заходів реакції з кожною такою подією зростає. Водночас зростає і глобальність підходів до визначення загроз. Якщо спочатку цей процес характеризувався локальним чи державним рівнем, то нині 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 становлять потенційну шкоду для життя, інформації, операцій, навколишнього середовища та/або власності [3].

Відповідно до національної політики США по захисту КІ, першочерговою загрозою для безпеки вбачаються кібератаки. Саме тому США були серед ініціаторів глобалізації та об'єднавчих процесів у питанні міжнародної кооперації з протидії кіберзлочинності [4]. Завдяки зусиллям американців значно активізувались процеси створення відповідних центрів та виділення сил і засобів в інших світових державах для боротьби з небезпеками такого роду. Серед інших основних видів загроз для КІ США виділяють терористичні атаки (зокрема на підприємствах хімічної промисловості, тобто такі, які у разі знищення або ураження можуть призвести до техногенних катастроф та масової загибелі людей) та стихійні лиха.

США значно вплинули на формування європейських підходів до виявлення та протидії загрозам КІ. Нині об'єднана Європа має власні органи із захисту КІ. Діють експертні групи з критичної інфраструктури (CIP), інформаційна мережа з попередження загроз критичній інфраструктурі (CIWIN) тощо. Європейська Комісія визначає принципи та інструменти, необхідні для впровадження Європейської програми захисту критично важливої інфраструктури (EPCIP), спрямованої на європейську та національну інфраструктуру кожної держави-учасниці.

Серед основних загроз відповідальні інстанції ЄС визначають кіберзагрози, тероризм, злочинні дії, природні небезпеки, аварії та інші причини нещасних випадків [5; 6].

Згідно з нормативно-правовими актами ЄС, «загроза» – будь-яка подія, яка може порушити або знищити критичну інфраструктуру або будь-який з її елементів [6]. Майже ідентичне визначення «загроз» дається в Зеленій книзі із 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 завдання шкоди критичним активам [7].

Часто дія загроз може спричиняти «каскадний ефект» (в Європі поширене вживання «ефект доміно»), коли дестабілізація однієї складової частини КІ тягне за собою порушення нормального функціонування інших складників та викликає широкомасштабне катастрофічне явище. Під *«каскадним ефектом»* від порушення функціонування КІ автором пропонується розуміти серію пов'язаних подій, кожна наступна з яких спричинена попередніми та тягне за собою настання нових.

Серед європейських країн доцільно виділити активну діяльність по ідентифікації та аналізу загроз КІ, наприклад таку, яку проводить Німеччина. Згідно з «Концепцією основних заходів із захисту КІ Німеччини», «загроза» визначається як можливість настання подій (стихійних явищ, технічних збоїв чи людських прорахунків, помилок у поведінці людей), що можуть завдати шкоди особам, матеріальним цінностям і навколишньому середовищу чи призвести до розладу соціальних та економічних відносин.

Загрози для КІ поділяють на три основних види: загрози від стихійних явищ, людських прорахунків та технічних збоїв, а також загрози від тероризму і злочинних дій. Своєю чергою, в Німеччині чітко визначено, що екстремальними погодними умовами є паводки (включаючи підвищення рівня ґрунтових вод), повені, затоплення, штормові припливи, сніг, лід, посухи, а також бурі, урагани, землетруси, пожежі і штормові явища. Пожежі можуть виникати природним шляхом у результаті удару блискавки, самозайманя або навмисного чи ненавмисного підпалу в поєднання з тривалою посухою. Зсув може викликатися геофізичними явищами (наприклад, землетрусом, ерозією), метеорологічними впливами (наприклад, сильними опадами, повенями, таненням снігів і льоду) й антропогенними впливами (наприклад, будівельними роботами, землетрусами, вирубкою лісів). Прикладами зміщення мас є лавини, зсуви і розрідження ґрунту.

Також виділяють загрози від фізичного впливу зсередини і зовні об'єктів КІ, загрози, які виходять від людських прорахунків та технічних збоїв, тероризму або злочинних діянь.

Прикладом загрози зсередини об'єкта може бути так звана «навмисна помилка» (авт. назва), наприклад, умисне неправильне програмування систем управління, що призводить до аварій чи зупинки виробництва, втручання в роботу важливих частин установки з використанням наявних на будь-якому підприємстві допоміжних засобів і інструментів. Зовнішніми загрозами можуть вважатись аварія транспортного засобу, підпал, використання вибухових речовин, обстріл, авіакатастрофа, застосування хімічної, біологічної, радіологічної або ядерної зброї (ХБРЯ). Зловмисниками можуть бути застосовані і комбіновані дії.

Франція спочатку розпочала захищати критичну інфраструктуру в інформаційно-комунікаційній сфері. Однак у зв'язку з поширенням у світі кіберзагроз та ростом терористичних проявів, із 2009 р. організація протидії цим загрозам була покладена на Генеральний секретаріат із питань оборони та національної безпеки (SGDSN). SGDSN аналізує відкриту інформацію та розвіддані у сфері захисту КІ, стежить за недопущенням різних внутрішніх та зовнішніх загроз [8].

У Великобританії з початку побудови системи захисту КІ, насамперед, звернули увагу на необхідність захисту від загроз у сфері державної безпеки. Тому тривалий час функціонував Національний координаційний центр із безпеки інфраструктури (NISCC) та Центр консультацій із національної безпеки (NSAC). Згодом на їх базі був утворений Центр по захисту національної інфраструктури (CPNI), що надає комплексні консультації з питань безпеки підприємствам і організаціям, які є операторами критичної інфра-

структури, включаючи інформаційні, кадрові та технічні аспекти безпеки, допомагаючи знизити вразливість національної критичної інфраструктури від тероризму та інших загроз. Згодом функції з протидії загрозам у сфері комп'ютерної безпеки були передані Національному центру кібербезпеки (NCSC).

Забезпечення стійкості та підвищення захищеності Великої Британії у боротьбі з надзвичайними ситуаціями та відповідного широкого кола загроз є завданням Секретаріату з питань надзвичайних ситуацій (CCS), який сприяє діяльності Центру управління кризовими ситуаціями (COBR), що забезпечує швидке вироблення єдиної позиції та вжиття скоординованих заходів протидії наявним загрозам [9].

На відміну від вищерозглянутих країн, Данія у сфері КІ серед основних виділяє та вживає заходи з протидії загрозам від надзвичайних ситуацій (аварій, катастроф, стихійних лих). Тому значними повноваженнями наділене Данське агентство з управління надзвичайними ситуаціями (DEMA). Під захистом КІ в основному розуміють збереження та продовження важливих функцій держави та суспільства у разі аварій та катастроф.

У Нідерландах діє міжміністерська група та міжвідомча програма «національної оцінки ризиків», які визначають на основі аналізу загроз. Очолюють зазначену групу Директорат національної безпеки та Міністерство внутрішніх справ та королівських відносин. Важлива увага приділяється протидії загрозам від тероризму, кіберзагрозам, забезпеченню національної безпеки та кризового управління, за що відповідає Національний координаційний центр із питань боротьби з тероризмом та забезпечення безпеки (NCTV).

Питання протидії загрозам, пов'язаним із терористичними проявами, для Нідерландів стало актуальним давно. Ще в 2004 р. був створений Національний координаційний центр протидії тероризму (NCTb). Метою його створення була координація діяльності поліції, судової влади, служб безпеки та інших організацій у сфері боротьби з тероризмом. З часом Нідерланди почали ширше розглядати загрози КІ та для протидії їм у 2012 р. об'єднали NCTb із Дирекцією національної безпеки та Командою з реагування на інциденти в комп'ютерній сфері (GOVCERT.NL). Новоствореною організацією став Національний координаційний центр із питань боротьби з тероризмом та забезпечення безпеки.

Румунія здійснює поділ загроз КІ на такі, які можуть мати природний, випадковий або умисний характер.

Характерні 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, у деяких випадках навіть суттєве підвищення вартості тарифів може призводити до соціально-політичної нестабільності, загострення внутрішньополітичних конфліктів, значних економічних втрат, послаблення інститутів влади.

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

Завжди актуальними є загрози від надзвичайних ситуацій, які поєднують у собі загрози природнього, техногенного характеру тощо.

Саме тому Стратегією національної безпеки України, яка введена в дію Указом Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України», від 26.05.2015 р. № 287/2015 визначено актуальні загрози національній безпеці та критичній інфраструктурі зокрема. Серед загроз безпеці КІ виділені критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту, недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій, неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення. Разом із цим серед загроз кібербезпеці і безпеці інформаційних ресурсів у Стратегії також визначено уразливість об'єктів критичної інфраструктури до кібератак.

Варто 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 утворилася природним чином: «Кожне окреме відомство виділяло певний спектр загроз для підпорядкованих об'єктів та володіло певним набором інструментів і ресурсів для забезпечення їх безпеки» [10]. Зрештою, в чинному законодавстві України визначено низку категорій об'єктів, для яких регламентуються особливі умови забезпечення захисту: підприємства, що мають стратегічне значення для економіки та безпеки держави; особливо важливі об'єкти електроенергетики й нафтогазової галузі; потенційно небезпечні об'єкти, об'єкти підвищеної небезпеки; об'єкти, що підлягають обов'язковій охороні підрозділами Державної служби охорони, та об'єкти, які підлягають охороні та обороні в умовах надзвичайних ситуацій та в особливий період; інші об'єкти й системи, такі як системи зв'язку, платіжні системи тощо.

Водночас у нашій державі протидія загрозам КІ здійснюється з використанням таких державних систем реагування та захисту, зокрема: 1. Єдиної державної системи цивільного захисту (Положення затверджене постановою Кабінету Міністрів України від 09.01.2014 р. № 11); 2. Єдиної системи запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (Положення, затверджене Постановою Кабінету Міністрів України від 15.08.2007 р. № 1051); 3. Державної системи фізичного захисту (Порядок функціонування затверджений постановою Кабінету Міністрів України від 21.12.2011 р. № 1337). Крім того, у теперішній час на виконання положень введеної у дію Указом Президента України від 16 березня 2016 р. Стратегії кібербезпеки України створюється Національна система кібербезпеки, завдання якої пов'язані із захистом критичної інфраструктури в кіберсфері.

У ч. 4 ст. 1 Закону України «Про основи національної безпеки» (в редакції від 19.06.2003 р. № 964-IV) законодавцем визначено «загрози національній безпеці» – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України. В ч. 6 ст. 1 чинного Закону України «Про національну безпеку України» (від 21.06.2018 р. № 2469-VIII) під «загрозами національній безпеці України» розуміють явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України.

Аналіз ст. 19 Закону України «Про національну безпеку» дає змогу стверджувати, що основними загрозами КІ у сфері державної безпеки є: розвідувально-підривна діяльність, тероризм, кіберзагрози, загрози економічного характеру та державності, спрямування до державної таємниці. Ст. 22 розширює зону протидії загрозам у інформаційній сфері, окрім державної таємниці, до кіберзахисту критичної інформаційної інфраструктури, державних

інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

Крім того, у п. 6 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» дається визначення одного з видів загроз критичній інфраструктурі. «Кіберзагроза» – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. Вводяться такі терміни, як кіберрозвідка, кібертероризм, кібершпигунство, що дають змогу більш широко розглядати проблему загроз КІ у сфері забезпечення кібербезпеки.

Відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.2016 р. № 96/2016, з-поміж об'єктів, на які можуть бути спрямовані кіберзагрози, виділено такі: економічна, науково-технічна й інформаційна сфера, сфера державного управління, оборонно-промисловий і транспортний комплекси, інфраструктура електронних комунікацій, сектор безпеки і оборони України.

Серед загроз кібербезпеці також виділено: невідповідність інфраструктури електронних комунікацій держави, рівня її розвитку та захищеності сучасним вимогам; недостатній рівень захищеності критичної інфраструктури, державних електронних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, від кіберзагроз; безсистемність заходів кіберзахисту критичної інфраструктури; недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки та кіберзахисту критичної інфраструктури та державних електронних інформаційних ресурсів; недостатня ефективність суб'єктів сектору безпеки і оборони України у протидії кіберзагрозам воєнного, кримінального, терористичного та іншого характеру; недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення кібербезпеки.

Згідно з розпорядженням Кабінету Міністрів України від 06.12.2017 р. № 1009-р «Про схвалення концепції створення державної системи захисту критичної інфраструктури», серед загроз КІ виділено такі: загрози природного і техногенного характеру, загрози, спричинені протиправними діями та будь-якими комбінаціями з переліченого.

На думку науковців, загрози КІ також доцільно розподіляти на три групи, що включають: аварії й технічні збої, природні лиха та небезпечні природні явища, зловмисні дії (таких груп або окремих осіб, як терористи, злочинці й диверсанти, промислове шпигунство, а також бойові дії) [11].

У своїх наукових напрацюваннях О.М. Суходоля серед основних загроз КІ виділяє: надзвичайні ситуації (природні катастрофи, технологічні аварії), терористичні акти, диверсії, кіберзагрози тощо. На особливу увагу заслуговує позиція вченого щодо проблеми розширення загроз КІ, зокрема виділення втручання в систему управління КІ чи технологічний процес, руйнування об'єкта силами його ж персоналу. Таку загрозу ним пропонується ідентифікувати як чинник «внутрішнього порушника». Як вважає дослідник, саме цей чинник міг призвести до успіху кібератаки на енергорозподільчі компанії України [12].

На наше переконання, виділення загроз такого характеру дійсно є необхідним, особливо за сучасних умов «гібридної війни» та відповідає наявним тенденціям в іноземній практиці. Автором розглядається доцільність виділення категорії протиправних дій «навмисна помилка», під якими пропонується розуміти умисні дії для приведення будь-якої системи чи установки у критичний стан, що хоч частково охоплюються об'єктивною стороною складу злочину «диверсія» (ст. 113 КК України), проте становлять меншу суспільну небезпеку, та суб'єктивна сторона діяння, зокрема, мета не має такого масштабного характеру (мається на увазі зниження економічного, науково-технічного потенціалу держави), а може полягати в бажанні дестабілізувати роботу лише певного вузла, припинити певний вид діяльності об'єкта КІ тощо. Прикладом «навмисної помилки» можуть бути дії в обслуговуванні обладнання, маніпуляціях із ними, як-от умисне неправильне програмування систем управління, втручання в роботу важливих частин установки з використанням наявних на будь-якому підприємстві допоміжних засобів і інструментів.

Д. Бобро серед основних загроз КІ виділяє техногенні аварії та технічні збої, викликані, зокрема, людськими помилками, природні лиха та небезпечні природні явища, зловмисні дії [10].

Науковці Національного інституту стратегічних досліджень України в «Зеленій книзі» обґрунтовують ймовірність виникнення загроз КІ від аварій та технічних збоїв, небезпечних природних явищ, зловмисних дій [13].

У нормативно-правовій сфері нашої держави вже є подібна класифікація. Так, ст. 5 Кодексу цивільного захисту України від 02.10.2012 р. № 5403-VI, залежно від характеру походження подій, що можуть зумовити виникнення надзвичайних ситуацій на території України, виділяє події: 1) техногенного характеру; 2) природного характеру; 3) соціальні; 4) воєнні.

Враховуючи національний досвід творення норм у сфері національної безпеки України та міжнародну практику, доцільно сформулювати загальне визначення загроз КІ. Так, під *«загрозами об'єкта КІ»* пропонується розуміти наявні або потенційно можливі явища і чинники, що можуть завдати шкоди 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 *види*:

1) загрози у сфері державної безпеки чи безпекового характеру (тероризм, диверсії, «навмисна помилка», розвідділяльність 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).

Від мети дій, що їх спричиняють, для зручності кваліфікації загроз, у т.ч. через призму правової оцінки, можливо, протиправної діяльності, пропонується виділяти події та/або явища ненавмисного характеру (технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактору), навмисні дії (терористичні акти, акти кібертероризму, диверсії, дії «внутрішнього порушника», «навмисна помилка», розвідувальна діяльність, конкурентна розвідка тощо).

Також можна класифікувати загрози за значною кількістю критеріїв: від характеру походження (природного та техногенного характеру, а також навмисні дії), ступеня поширення, розміру людських втрат та матеріальних збитків, втрат для безпеки життєдіяльності, суспільно-політичних та культурних, втрат для забезпечення державної безпеки та громадського порядку тощо. Залежно від наслідків, обсягів ресурсів, необхідних для їх локалізації, доцільно виділити такі рівні загроз: 1) державний; 2) регіональний; 3) місцевий; 4) об'єктовий.

Важливою характеристикою загрози є її потенціал. В «Академічному тлумачному словнику української мови» під ним розуміються приховані здатності, сили для якої-небудь діяльності, що можуть виявитися за певних умов; запас чого-небудь, резерв [14]. Під *«потенціалом загрози»* будемо розуміти ступінь прихованих здатностей загрози. Наприклад, енергетичних, ресурсних (матеріальних або нематеріальних, технічних та людських), діапазону кліматичних факторів та ін. Оцінка потенціалу загрози має важливе значення для визначення масштабів ураження об'єкта КІ загрозами і ризиків від них. Чим більший потенціал у загрози, тим більший ризик від неї для об'єкта КІ.

Потенціал загрози може бути оцінений кількісно з використанням методів експертних оцінок [15]. Для кількісної оцінки потенціалу загрози ***(П)*** автором пропонується розглядати його як функцію комплексу з ***n*** параметрів a_i загрози

$$П = f(a_1, a_2, \ldots, a_n).$$

Кожен із цих параметрів оцінюється експертами за однаковою бальною шкалою. Конкретний вид функції ***П*** може бути різним, але, коли важливість параметрів a_i однакова, потенціал загрози можна представити як середнє арифметичне значення їх бальних оцінок:

$$П = (a_1+a_2+ \ldots+a_n)/n.$$

У разі, коли важливість параметрів аі різна, використовується їх коефіцієнт значимості k_i.Тоді

$$П= (k_1a_1 + k_2a_2+ \ldots + k_na_n),$$

причому $k_1 + k_2 + \ldots + k_n= 1.$

Крім того, треба враховувати, що потенціал загрози як явища або події може змінюватися з часом ***t***, а тому у загальному вигляді він буде мати такий вигляд

$$П = f(a_1, a_2, \ldots, a_n; t).$$

Тим самим з'являється реальна можливість здійснювати прогнозування зміни потенціалу загрози у часі, а також прогнозування небезпеки від ураження нею об'єкта КІ. Варто підкреслити, що комплексна оцінка потенціалу загрози є однією з важливих характеристик небезпеки для об'єкта КІ від загрози.

Здатність якісно оцінювати потенціал загроз значно впливає на підвищення ефективності діяльності в цій сфері органів державної безпеки та правоохоронних органів і спеціально уповноважених державних органів, сприяє покращенню захисту КІ та зміцненню державної безпеки.

Висновки. Таким чином, першочерговим та надзвичайно важливим етапом функціонування ефективної системи захисту КІ в будь-якій державі є можливість своєчасного виявлення та створення умов для якісної протидії загрозам КІ.

Оцінка загроз критичній інфраструктурі є важливою складовою частиною діяльності із захисту державної безпеки.

Аналіз змісту категорії *«загроз об'єкту КІ»* дає змогу розглядати їх як наявні або потенційно можливі явища і чинники, що можуть завдати шкоди 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. Доцільно здійснювати їх класифікацію: від характеру походження, мети дій, що їх спричиняють, ступеня поширення, розміру людських втрат та матеріальних збитків, втрат для безпеки життєдіяльності, суспільно-політичних та культурних, втрат для забезпечення державної безпеки та громадського порядку, обсягів ресурсів, необхідних для їх локалізації. Вид загроз та їхня можлива інтенсивність враховується під час визначення критичності об'єкта для формування переліку об'єктів КІ.

Здатність загроз уражати важливі елементи, що значно впливають на стан економіки держави та на суспільно-політичні аспекти, зумовлює необхідність удосконалення діяльності із захисту державної безпеки та є рушійним фактором виникнення складних процесів організаційно-безпекового характеру і залучення до них партнерів із державного та приватного сектору.

Список використаної літератури:

1. Єрменчук О.П. Побудова системи захисту критичної інфраструктури в Україні з використанням досвіду сектору безпеки іноземних держав. Актуальні проблеми вдосконалення чинного законодавства України. 2017. № XLIV. С. 224–235.

2. Єрменчук О.П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США. Науковий вісник ДДУВС. Дніпро. 2017. № 3. С. 135–140.

3. National Critical Infrastructure Security and Resilience Research and Development Plan. 2015. URL: http://www.dhs.gov/publication.

4. Формирование организационно-правовой системы защиты национальной инфраструктуры от киберугроз / Бык В.В., Климчук А.А., Панченко В.Н., Петров В.В. К.: Академпресс, 2013. 220 с.

5. URL: http://eur-lex.europa.eu/legal-content/TXT-LEGISSUM:l33260 European Programme for Critical Infrastructure Protection.

6. Запобігання, готовність та реагування на терористичні напади: повідомлення Комісії Ради та Європейському Парламенту від 20 жовтня 2004 р. /COM (2004) 698 final – Official Journal від 20.01.2005. URL: http://eur-lex.europa.eu/legal-content/GA/TXT/?uri=celex:52004DC0702.

7. URL: http://www.ab.gov.tr/files/ardb/evt/1_avrupa_birligi/1_6_raporlar/ 1_2_green_papers/com2005_green_paper_on_critical_infrastructure.pdf.

8. Secrétariat général de la défense et de la sécurité nationale URL: http://www.sgdsn.gouv.fr.

9. URL: http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx.

10. Бобро Д.Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. Стратегічні пріоритети. Серія: Економіка. 2015. № 4. С. 83–93.

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

12. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. Стратегічні пріоритети. Серія: Політика. 2016. № 3 (40). С. 65–67.

13. 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. К.: НІСД, 2016. 176 с.

14. Словник української мови в 11 томах / Академічний тлумачний словник (1970–1980). Том 7. К., 1976.

15. Сиденко В.М., Грошко И.М. Основы научных исследований. Харьков: Вища школа, 1970. 200 с.

ІНФОРМАЦІЯ ПРО АВТОРА

Єрменчук Олександр Петрович – кандидат юридичних наук, доцент кафедри оперативно-розшукової діяльності та спеціальної техніки Дніпропетровського державного університету внутрішніх справ Міністерства внутрішніх справ України

INFORMATION ABOUT THE AUTHOR

Yermenchuk Oleksandr Petrovich – Candidate of Law Sciences, Associate Professor at the Department of Operative-Investigative Activity Department and Specialist Equipment Dnipropetrovsk State University of Internal Affairs of the Ministry of Internal Affairs of Ukraine

eop242012@gmail.com