## ПРАВО НАЦІОНАЛЬНОЇ БЕЗПЕКИ; ВІЙСЬКОВЕ ПРАВО

УДК 342.1:343.9:519.8 **DOI:** https://doi.org/10.32631/v.2024.1.20

**Дмитро Сергійович Мельник,**
*кандидат юридичних наук,*
*Міжвідомчий науково-дослідний центр*
*з проблем боротьби з організованою злочинністю*
*при Раді національної безпеки і оборони України (старший дослідник);*
*https://orcid.org/0000-0002-1497-950X,*
*e-mail: d-melnik@ukr.net*

# ПОБУДОВА МОДЕЛІ ЗАГРОЗ НАЦІОНАЛЬНІЙ КРИТИЧНІЙ ІНФРАСТРУКТУРІ УКРАЇНИ ЯК ОСНОВА ЗАБЕЗПЕЧЕННЯ ЇЇ БЕЗПЕКИ ТА СТІЙКОСТІ

*Висвітлено сучасні проблемні питання захисту критичної інфраструктури України, актуальні загрози її безпеці та потреби організації належної протидії в умовах воєнного стану. Загрозами критичній інфраструктурі є чинники, що спроможні реально чи потенційно завдати шкоди безперервності її роботи, функціональності, цілісності й стійкості або призвести до руйнування. Визначено побудову моделі загроз критичній інфраструктурі як потребу забезпечення ефективного захисту її об'єктів. Формування базової моделі загроз для об'єктів критичної інфраструктури, що має включати взаємопов'язані моделі об'єкта, обстановки та порушника, нині є важливим елементом алгоритму вирішення зазначеного завдання. Окреслено перспективні заходи, що як сприятимуть стабільному функціонуванню об'єктів критичної інфраструктури, так і забезпечуватимуть їх належний захист.*

**Ключові слова:** критична інфраструктура, об'єкти, загрози, безпека, захист, протидія, нейтралізація, усунення наслідків, удосконалення.

*Оригінальна стаття*

### Постановка проблеми

Упродовж останніх 10 років Україна зазнала безпрецедентної кількості диверсій та кібератак на об'єкти критичної інфраструктури (далі – ОКІ) держави – підприємства енергетики, транспорту, життєзабезпечення, державні фінансові установи, органи, які гарантують безпеку, оборону, захист від надзвичайних ситуацій тощо [1]. Із початком повномасштабного вторгнення рф в Україну кількість таких протиправних спрямувань до ОКІ значно зросла й продовжує зростати. В умовах російської військової агресії проти України, що триває, вказані загрози доповнилися військовими загрозами, спрямованими

на руйнування національної критичної інфраструктури (далі – КІ) та підрив стійкості держави.

Безпека та захищеність ОКІ, стабільне функціонування яких необхідно забезпечувати постійно, визначені в Концепції забезпечення національної системи стійкості одними із базових елементів національної системи стійкості[1]. Забезпечення стійкості КІ до загроз усіх видів є метою створення національної системи її захисту[2]. Важливість виконання завдань із захисту КІ для національної безпеки визначена у Стратегії національної безпеки України, Стратегії державної безпеки України, Законі України «Про критичну інфраструктуру» та Концепції створення державної системи захисту критичної інфраструктури.

**Стан дослідження проблеми**

Теоретичні питання захисту КІ досліджували Д. С. Бірюков, Д. Г. Бобро, Д. М. Гладких, О. П. Єрменчук, С. І. Кондратов, О. І. Насвіт, Ю. М. Скалецький, О. М. Суходоля, Л. Г. Шемаєва та ін. У своїх роботах науковці надали визначення КІ, її складових та об'єктів, запропонували підходи до визначення загроз ОКІ, окреслили шляхи розроблення й удосконалення системи захисту від загроз та її належного правового регулювання. Потребу застосування соціального моделювання для дослідження проблем забезпечення національної безпеки, зокрема захисту КІ, обґрунтували В. М. Фурашев і Д. В. Ланде [2]. Застосування математичних методів для моделювання та оцінки сценаріїв проектних загроз ОКІ дослідили Д. С. Бірюков, В. А. Заславський, В. В. Євгієнко, О. В. Франчук [3] та ін. Актуальні підходи до визначення проектної загрози ОКІ сформували Д. Г. Бобро, С. П. Іванюта, С. І. Кондратов, О. М. Суходоля [4; 5].

**Мета і завдання дослідження**

*Метою* статті є розроблення актуальної моделі загроз, яка формалізує ймовірні впливи на КІ України, що дасть змогу підвищити ефективність її захисту. *Завданням* дослідження є вироблення алгоритму побудови узагальненої моделі загроз для забезпечення необхідного рівня безпеки КІ шляхом ефективного захисту від таких загроз.

---

[1] Концепція забезпечення національної системи стійкості : затв. Указом Президента України від 27.09.2021 № 479/2021 // Рада національної безпеки і оборони України : офіц. сайт. URL: https://www.rnbo.gov.ua/ua/Ukazy/5017.html?PRINT (дата звернення: 14.02.2024).

[2] Концепція створення державної системи захисту критичної інфраструктури : схвал. розпорядженням Кабінету Міністрів України від 06.12.2017 № 1009-р // База даних (БД) «Законодавство України / Верховна Рада (ВР) України. URL https://zakon.rada.gov.ua/laws/show/1009-2017-р (дата звернення: 14.02.2024).

**Наукова новизна дослідження**

Досліджено актуальні потреби та наявні проблемні аспекти формування сучасної моделі загроз КІ насамперед в умовах повномасштабної військової агресії рф.

**Виклад основного матеріалу**

Модель загроз є одним із базових понять кібербезпеки та кіберзахисту інформації в інформаційно-комунікаційних системах для формулювання загальних вимог до створення комплексних систем захисту інформації[1]. Також моделі загроз і порушника широко використовують в Україні та у світі під час захисту інформаційних ресурсів та кіберзахисту ОКІ. Адже саме в цій сфері дослідники здійснили перехід від розгляду загроз протиправних дій до ширшого кола загроз.

Глобальні тенденції до посилення природних і техногенних загроз, підвищення рівня терористичних загроз, збільшення кількості та зростання складності кібератак, систематичне знищення й пошкодження українських ОКІ під час російської збройної агресії зумовили актуалізацію питання захисту об'єктів та інформаційних ресурсів, які є критично важливими для життєдіяльності суспільства, соціально-економічного розвитку держави і забезпечення національної безпеки в умовах воєнного стану.

На стан захисту ОКІ впливають: незавершеність формування загальнодержавної системи захисту КІ та нереалізоване рішення про створення державного органу, відповідального за організацію й координацію дій у цій сфері[2]; об'єктивна нездатність Державної служби спеціального зв'язку та захисту інформації України як тимчасового виконувача функції державного регулятора забезпечити необхідну координацію дій у цій сфері; невизначеність завдань, повноважень і відповідальності інших уповноважених суб'єктів у сфері захисту КІ; відсутність єдиних критеріїв та недосконалість методології віднесення об'єктів до КІ; відсутність нормативних вимог та

[1] НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі : затв. наказом ДСТСЗІ СБУ від 04.12.2000 № 53 (зі змінами згідно з наказом Адміністрації ДССЗЗІ України від 28.12.2012 № 806) // Технічний захист інформації : сайт. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf (дата звернення: 14.02.2024).

[2] Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості : постанова Кабінету Міністрів України від 12.07.2022 № 787 // БД «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua/laws/show/787-2022-п (дата звернення: 14.02.2024).

єдиної методології проведення оцінки загроз і ризиків для КІ[1]; стан наукових досліджень щодо розвитку методів оцінки зовнішніх і внутрішніх процесів, небезпечних для ОКІ, аналізу ризику та вразливості систем їх фізичного захисту.

Такий стан справ перешкоджає ефективному виконанню першочергових завдань уповноваженими суб'єктами у сфері безпеки КІ, не дозволяє організувати ефективний захист ОКІ, що суттєво підвищує небезпечність загроз національній безпеці в цій сфері. Саме *неефективне управління безпекою КІ* було визнане на державному рівні однією з ключових загроз національній безпеці України в сучасних умовах[2].

Це вказує на необхідність завершення процесу формування загальнодержавної системи захисту КІ, покращення координації й управління ресурсами систем безпеки, розмежування завдань і функцій суб'єктів захисту КІ, вдосконалення правового й організаційно-методичного забезпечення захисту КІ від загроз, зокрема шляхом формування моделі загроз для ОКІ.

З огляду на вищевказані загрози й виклики, які мають тенденцію до посилення, подальший розвиток воєнної ситуації в Україні вимагає концептуального перегляду засад діяльності всієї національної системи захисту КІ. Відповідно потреби забезпечення захисту й безпеки національної КІ вимагають не лише чіткого розуміння змісту сучасних загроз та їхніх проявів, а й побудови актуальної моделі загроз ОКІ для організації ефективної протидії. Водночас українське законодавство нині не містить ані визначення загрози для ОКІ, ані чітко визначеного переліку загроз національній КІ та її об'єктам.

Фактично загрозу ОКІ становлять процеси, явища, тенденції тощо, які реально або потенційно негативно на них впливають, що може призвести до порушення стабільності виконання ними функцій, руйнування цілісності та зниження стійкості або її знищення. Отже, можна погодитися із запропонованим визначенням загроз КІ як чинників, що спроможні реально чи потенційно завдати шкоди безперервності її роботи, функціональності, цілісності й стійкості або призвести до руйнування [6, с. 143].

Сьогодні необхідність захисту КІ зумовлюють низка серйозних *загроз та викликів національній безпеці*, перелік яких визначений у

[1] Концепція створення державної системи захисту критичної інфраструктури : схвал. розпорядженням Кабінету Міністрів України від 06.12.2017 № 1009-р // БД «Законодавство України / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-р (дата звернення: 14.02.2024).

[2] Стратегія національної безпеки України : затв. Указом Президента України від 26.05.2015 № 287/2015 // Президент України : офіц. сайт. URL: http://president.gov.ua/documents/2872015-19070 (дата звернення: 14.02.2024).

Стратегії національної безпеки України (пункти 10, 15, 17, 19, 22–24, 26, 27 розд. ІІ), Концепції розвитку сектору безпеки і оборони України (п. 1 розд. ІІ), доповнений і уточнений у Стратегії кібербезпеки України (розд. 3), Стратегії забезпечення державної безпеки (розд. ІІ). Такі загрози мають тривалий термін дії, здійснюють негативний вплив на безпеку КІ та на стан національної безпеки в цілому.

Ураховуючи викладене, в умовах повномасштабної російської військової агресії перед державою постають нові завдання, спрямовані на протидію загрозам і викликам, захист КІ шляхом забезпечення стійкості функціонування її систем і елементів, запобігання виникненню надзвичайних ситуацій, вчиненню терористичних актів і диверсій на ОКІ, припинення інших актів незаконного втручання в діяльність систем життєзабезпечення; упередження, стримування й недопущення тяжких наслідків.

Важливим елементом алгоритму вирішення вказаних завдань нині вбачається формування базової моделі загроз для ОКІ. Однак сьогодні поняття моделі загроз для ОКІ не визначене українським законодавством. Закон України «Про критичну інфраструктуру» у п. 17 ч. 1 ст. 1 містить визначення лише *проектної загрози ОКІ* – документ встановленої форми, який визначає властивості, характеристики реальних і потенційних загроз ОКІ, на зниження ймовірності реалізації яких має бути спрямовано функціонування системи захисту КІ[1]. Цей документ розглядається дослідниками як інструмент формалізації актуальних викликів і загроз ОКІ для суб'єктів державної системи захисту КІ, сформований на основі розвідувально-аналітичної роботи сектору безпеки [7, с. 69].

Відповідно до пунктів 4 і 6 ч. 1 ст. 19 зазначеного Закону секторальні органи у сфері захисту КІ розробляють і затверджують проектні загрози КІ секторального рівня, а також затверджують проектні загрози КІ об'єктового рівня у визначених секторах. Відповідно до приписів постанови Кабінету Міністрів України «Деякі питання подання інформації у сфері захисту критичної інфраструктури» від 14 жовтня 2022 р. № 1175[2] вжиті заходи щодо проектних загроз повинні знаходити відображення у звітах про виконання секторальними органами повноважень, визначених Законом України «Про критичну інфраструктуру».

[1] Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 14.02.2024).

[2] Деякі питання подання інформації у сфері захисту критичної інфраструктури : постанова Кабінету Міністрів України від 14.10.2022 № 1175 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1175-2022-п (дата звернення: 14.02.2024).

Водночас за відсутності законодавчо визначеного універсального переліку загроз для КІ такий документ (проектна загроза ОКІ) навіть з абстрактним переліком загроз, критерії для з'ясування властивостей та характеристик яких теж нині не визначені, навряд чи може бути ефективно застосований та виконає передбачену для нього місію.

Тому більш гнучким та практично значущим для захисту КІ видається застосування базової *моделі загроз*. Базова модель загроз КІ України є основою, на якій держава визначає, від кого та від чого потрібно захищатися на національному рівні. Модель загроз ОКІ формується завдяки застосуванню методу моделювання. Така модель містить перелік можливих загроз (небезпек) для ОКІ, що впливають на його безпечне функціонування. Водночас слід зауважити, що окрім відомих (прогнозованих) загроз (небезпек) існує ще й низка інших потенційних загроз, а для вже відомих загроз може бути багато сценаріїв їх реалізації.

Ураховуючи досвід аналізу загроз електроенергетичному сектору США, можемо побачити, що така модель включає: загрози природного характеру (торнадо, повені, землетруси тощо); техногенні аварії внаслідок людських помилок і прорахунків; протиправні дії (загальнокримінальні або терористичні угруповання, активісти екстремістських груп, хакери тощо)[1]. У цілому під час аналізу моделей загроз КІ США на національному рівні у межах підходу «all hazards approach» [8, с. 20] фахівцями розглядається низка загроз природного й техногенного характеру, а також зловмисних дій, пов'язаних, зокрема, з використанням як зброї повітряних суден, актів ядерного, радіологічного, хімічного та біологічного тероризму[2]. Аналогічний підхід до аналізу загроз КІ впроваджено в ЄС [9] після ухвалення Рекомендації Ради Європи зі скоординованого підходу до стійкості критичної інфраструктури[3].

За результатами аналізу досліджень загроз ОКІ, проведених фахівцями у сфері національної [4; 5], економічної [10; 11], інформаційної

[1] Electric Grid Security and Resilience. Establishing a Baseline for Adversarial Threats. June 2016. URL: https://securethegrid.com/electric-grid-security-and-resilience-establishing-a-baseline-for-adversarial-threats-pdf/ (дата звернення: 14.02.2024).

[2] The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-BasedApproach toward a Secure and Resilient Nation. URL: https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf (дата звернення: 14.02.2024).

[3] Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure. Brussels, 9 December 2022 (OR. en) 15623/22 // European Council : офіц. сайт. URL: https://data.consilium.europa.eu/doc/document/ST-15623-2022-INIT/en/pdf (дата звернення: 14.02.2024).

[12] та воєнної безпеки [13], базова модель загроз ОКІ має включати: *модель об'єкта, модель обстановки та модель порушника.* При цьому варто враховувати, що зазначені вище моделі є взаємопов'язаними та взаємозалежними.

Водночас в аспекті захисту КІ модель загроз для неї є більш широким поняттям і базується на результатах пошуку відповіді на питання щодо чинників, які можуть завдати шкоди функціонуванню ОКІ. Отже, виникає потреба в дослідженні не лише потенційних порушників, а й самого ОКІ: місце розташування (зокрема, географічні, кліматичні умови, сейсмічні показники); потенційно небезпечні технології, що використовуються на об'єкті; місце та спосіб розміщення обладнання, шляхи доступу, чинники впливу на його роботу; інші об'єкти, що розташовані поруч із досліджуваним об'єктом та можуть потрапити під дію вражаючих чинників; місце об'єкта у виробничих ланцюжках і споживачі його продукції (взаємозалежність з іншими господарськими об'єктами) тощо [4, с. 46].

Відповідно в запропонованій моделі згідно зі згаданим підходом «all hazards approach» мають бути враховані загрози/небезпеки будь-якого походження: природного й техногенного характеру – аварії та стихійні лиха (враховуються в моделях об'єктів); протиправного характеру – кіберзагрози і загрози диверсійно-терористичного характеру (враховуються в моделях порушника); соціально-політичного та воєнного характеру (враховуються в моделях обстановки) [5, с. 141]. Водночас варто зауважити, що крім наявних чи прогнозованих загроз може існувати ще й багато інших, а для вже відомих загроз є низка можливих сценаріїв їх реалізації, які слід враховувати.

Проте забезпечити високий рівень захисту всієї КІ від будь-яких потенційних загроз об'єктивно неможливо. Потрібно здійснити їх фільтрацію та ранжування. Так, дослідники пропонують використати для цього такі характеристики загроз, як імовірність (виключення малоймовірних загроз), величину (виключення загроз, вплив яких на функціонування ОКІ не перевищує допустимі межі) та потенційні втрати (виключення загроз, наслідки реалізації яких є прийнятними). Однак такий підхід до фільтрації загроз є відсівом «знизу», а потрібно провести ще й відсів «згори», тобто розподілити на проектні та позапроектні загрози, нейтралізація яких є завданням держави (загрози бойових дій, терористичної атаки із застосуванням важкої зброї) [4, с. 47].

Тому варто погодитися з позицією вітчизняних дослідників безпеки й стійкості КІ, яка зводиться до того, що більш коректно здійснювати фільтрацію загроз за ризиками їх реалізації, оскільки саме ризик, оцінений для різних сценаріїв розвитку подій, є необхідною *мірою критичності* ОКІ. Водночас модель загроз має враховувати

навіть малоймовірні події, якщо є суттєвими їх наслідки, які створюватимуть ризик вразливості ОКІ [4, с. 47; 5, с. 143].

Таким чином, у *моделі об'єкта* мають враховуватися загрози природного й техногенного характеру, зумовлені місцем розташування ОКІ, тим, що його оточує, кліматичними умовами, технологічними процесами, які відбуваються на об'єкті, потребами в сировині для виробництва продукції, зв'язками з іншими ОКІ [5, с. 182]. Модель об'єкта містить такі загрози:

– небезпечні природні процеси та явища: землетруси; зсуви; провалювання земної поверхні; критично високі/низькі температури; вологість повітря; рухи повітряних мас; високий/низький рівень води; пожежі у природних екосистемах; падіння метеоритів тощо; епідемії та пандемії; епізоотії та епіфітотії;

– руйнівні техногенні процеси: збої в роботі та відмова обладнання; помилки персоналу; аварії на виробництві або під час транспортування сировини/палива/продукції тощо; пожежі, вибухи, затоплення приміщень ОКІ, не пов'язані з протиправними діями; аварії на залізничному, авіа-, автотранспорті або водному транспорті, наслідком яких може стати ураження об'єкта; втрата живлення; зниження частоти струму в системі електропостачання чи тиску в мережі водо- чи газопостачання;

– непередбачуване переривання виробничих зв'язків: розриви транспортних комунікацій; тривалі перерви в постачанні сировини, матеріалів, води, палива, енергії; розриви контрактів, зокрема викликані політико-економічними чинниками; обмеження на використання технологій; форс-мажорні обставини, що призводять до впливу непереборної сили;

– відсутність альтернатив та резервів у виробничих процесах: немає альтернативних джерел і шляхів постачання сировини, матеріалів, води, палива, енергії, а також альтернативних технологій та необхідних резервів.

Варто погодитися з позицією дослідників, згідно з якою модель загроз буде неповною без *моделювання соціально-політичної обстановки*, в якій ОКІ функціонує [4, с. 46; 5, с. 141], оскільки від цього залежить можливість реалізації низки воєнних та соціально-політичних загроз.

*Модель обстановки* має базуватися на результатах аналізу розвитку ситуації у світі/регіоні, соціально-політичної ситуації в державі, ситуації в окремому секторі КІ або в окремому регіоні країни, на конкретному ОКІ.

Таким чином, модель обстановки містить загрози, зумовлені:

– сучасною моделлю глобалізації, яка уможливила поширення міжнародного тероризму, релігійного та ідеологічного фундаменталізму й екстремізму;

– недружніми діями держав – світових лідерів, сусідніх та інших держав, які здійснюють вплив на розвиток ситуації у світі/регіоні, соціально-політичної ситуації в державі (зокрема, дії країни-агресора та її союзників з продовження повномасштабної військової агресії та гібридної війни проти України);

– радикалізацією суспільства в країні, що здійснює негативний вплив на стабільне функціонування КІ (укорінення радикальних настроїв і середовищ, діяльність незаконних збройних формувань, поширення тероризму; використання ресурсів ОКІ для фінансування тероризму, сепаратизму та поширення зброї масового знищення);

– проблемами у функціонуванні державного апарату, що ускладнюють вироблення і реалізацію ефективної політики держави щодо захисту КІ та підвищують уразливість до загроз (корупція, непослідовність і незавершеність реформ, недостатня ефективність органів держави тощо);

– незадовільним станом економіки, причиною якого став недостатній рівень конкуренції та панування монополій, низька енергоефективність тощо;

– незадовільним технологічним станом і низьким рівнем кіберзахисту через відсутність інвестицій в оновлення та розвиток ОКІ, несанкціоноване втручання (зокрема, кібернетичне) в їх функціонування.

*Модель порушника* містить загрози протиправних дій будь-якого характеру і становить сукупність кількісно-якісних характеристик порушника, його цілі та мотиви [4, с. 47]. Отже, модель порушника включає: опис порушника (його тип; категорії осіб; чисельність і склад); потенційні цілі (фізичні елементи ОКІ, системи управління/комунікації/захисту, персонал об'єктів); мотиви порушника; обґрунтовані припущення про його знання, кваліфікацію, практичні навички, можливості та налаштованість, а також оснащення й екіпірування; тактика дій у фізичному й кіберпросторі; сценарії дій порушника, що мають розроблятися в межах об'єктової моделі загроз для всіх можливих цілей на ОКІ.

Таким чином, базова *модель загроз* становить сукупність зазначених вище моделей об'єкта, обстановки і порушника, що містить *перелік реальних і потенційних загроз КІ* (небезпечних чинників, подій, інцидентів, інших джерел ризику), які впливають на її безпечне функціонування та на захист від яких має бути розрахована державна система захисту КІ.

В умовах збройної агресії, що триває, як складової гібридної війни проти України держава-агресор застосовує комбіновані воєнні, інформаційні, політичні, економічні, технологічні та інші методи впливу, кожен з яких використовує як зброю для ослаблення нашої

держави. Вказані негативні прояви зафіксовані [6, с. 161–166; 14, с. 110–111] та продовжують фіксуватися у різних сферах життєдіяльності держави й суспільства:

– *воєнній* – руйнування військових та цивільних логістичних об'єктів, виробничих потужностей, транспортних комунікацій і систем життєзабезпечення в зонах ведення бойових дій та на іншій території України; незаконне демонтування та вивезення на територію рф виробничих фондів підприємств оборонно-промислового комплексу й інших високотехнологічних галузей промисловості тощо;

– *інформаційній* – використання новітніх інформаційних технологій та електронних комунікацій для втручання в життєво важливі сфери держави; вчинення кібератак, кібердиверсій та інших протиправних дій на ОКІ; поширення недостовірної інформації про розкрадання ресурсів іноземної допомоги, нездатність України виконувати боргові зобов'язання, прояви корупції серед українських високопосадовців, невідповідність української продукції міжнародним стандартам якості, наявність збудників епідемічних захворювань тощо з метою формування образу ненадійного позичальника, військового і торгового партнера;

– *політичній* – дискредитація України на міжнародній арені з метою відмови в наданні міжнародної військової, фінансової та технічної допомоги, закриття міжнародних ринків збуту, створення передумов для втрати наявного промислового й транзитного потенціалу та усунення України як економічного конкурента; дискредитація органів влади й управління держави як нездатних забезпечити оборону та безпеку країни, вирішувати інспіровані ззовні системні кризові політичні та соціальні явища, спровоковані в суспільстві протестні настрої, конфлікти і протистояння;

– *економічній* – економічна експансія з використанням капіталу країни-агресора (до 2014 р.); монополізація стратегічних галузей національної економіки російським капіталом (до 2022 р.); просування підконтрольного менеджменту на ключові посади у провідні галузі економіки з метою встановлення контролю над стратегічно важливими ОКІ, здійснення негативного впливу на їх функціонування й розвиток, зниження рівня обороноздатності та безпеки держави, гальмування процесів реформування, процесів модернізації КІ, виведення державних активів; використання фінансових інструментів для виснаження матеріальних ресурсів держави; штучне створення економічного протистояння та провокування торговельно-економічних воєн із сусідніми країнами; блокування транспортних комунікацій та міжнародних транспортних коридорів, ослаблення транзитного потенціалу України; маніпулювання системами транспортування енергоресурсів;

– *науково-технологічній* – формування і тривале використання технологічної залежності України в інтересах держави-агресора; промислове шпигунство з метою викрадення іноземною стороною передових українських технологій і розробок; постачання на життєво важливі ОКІ неякісного обладнання, використання якого може призвести до виникнення надзвичайних ситуацій і збоїв виробничих або управлінських систем; знищення промислових потужностей, порушення виробничих циклів;

– *екологічній* – створення загрози виникнення надзвичайних ситуацій техногенного та природного характеру внаслідок пошкодження об'єктів енергетики, життєзабезпечення, руйнування або аварійного стану небезпечних виробництв у зоні бойових дій і на тимчасово окупованих територіях України тощо.

Указаний перелік загроз і викликів має стати основою, на якій держава визначатиме, від кого та від чого потрібно захищатися на національному рівні, на відміну від проектної загрози, що передбачає потребу захисту на секторальному чи об'єктовому рівні. Отже, на базі такого переліку мають бути розроблені секторальні та об'єктові моделі загроз (проектні загрози) КІ, вкрай важливі для її захисту від руйнування та забезпечення стійкості держави в умовах воєнного стану.

Роль держави має полягати в розробленні та впровадженні єдиних методологічних підходів, на основі яких мають бути проаналізовані загрози КІ; формуванні базової моделі загроз національного рівня та проектні загрози КІ на секторальному й об'єктовому рівнях; наданні методологічної підтримки операторам КІ в розробленні об'єктових проектних загроз, планів їх попередження та нейтралізації; оцінці ефективності захисту КІ.

Однак нині ані положеннями Закону України «Про критичну інфраструктуру», ані Національним планом захисту та забезпечення безпеки та стійкості критичної інфраструктури[1] не передбачено необхідності формування моделі загроз національній КІ, лише підготовку щорічної оцінки ризиків і загроз КІ національного рівня (п. 7 Плану), з урахуванням якої будуть надаватися пропозиції щодо проектних загроз та ризиків КІ України та визначені проектні загрози секторального й об'єктового рівнів (п. 8 Плану).

[1] Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури : розпорядження Кабінету Міністрів України від 19.09.2023 № 825-р // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/825-2023-р (дата звернення: 14.02.2024).

**Висновки**

Українське законодавство нині не містить визначення загрози для ОКІ, не передбачає чіткого переліку загроз національній КІ та її об'єктам. Як загрози КІ можна розглядати чинники, які спроможні реально чи потенційно завдати шкоди безперервності її роботи, функціональності, цілісності й стійкості або призвести до руйнування. В умовах повномасштабної російської військової агресії перед державою постають нові завдання, спрямовані на протидію загрозам і викликам, захист КІ від знищення/пошкодження. Важливим елементом алгоритму вирішення вказаних завдань нині вбачається формування базової моделі загроз для ОКІ, що має включати взаємопов'язані моделі об'єкта, обстановки та порушника. Однак українським законодавством сьогодні не передбачено потреби формування вказаної моделі загроз. Це негативно впливає на стан забезпечення безпеки й стійкості КІ України та вимагає внесення відповідних змін до Закону України «Про критичну інфраструктуру» та пов'язаних підзаконних нормативно-правових актів. Крім того, необхідно ухвалити нормативні документи з питань стандартизації процесів управління ризиками для КІ з метою попередження появи нових загроз.

**Список бібліографічних посилань: 1.** Лемешенко Я. Василь Грицак, голова Служби безпеки України. У планах Кремля – дестабілізація не тільки в Україні, а й у «старій Європі» // Укрінформ : сайт. 22.12.2016. URL: http://ukrinform.ua/rubric-politics/2144501-vasil-gricak-golova-sluzbi-bezpeki-ukraini.html (дата звернення: 14.02.2024). **2.** Фурашев В. М., Ланде Д. В. Соціальне моделювання – один із базових сучасних засобів забезпечення національної безпеки. *Інформація і право.* 2011. № 1 (1). С. 69–75. DOI: https://doi.org/10.37750/2616-6798.2011.1(1).271468. **3.** Бірюков Д. С., Заславський В. А., Євгієнко В. В., Франчук О. В. Моделювання та оцінка сценаріїв загроз для об'єктів критичної інфраструктури. *Наукові записки НаУКМА. Комп'ютерні науки.* 2009. Т. 99. С. 97–101. **4.** Бобро Д. Г. Урахування проектних загроз у розбудові державної системи захисту критичної інфраструктури. *Стратегічні пріоритети.* 2017. № 3 (44). С. 42–51. **5.** Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / за заг. ред. О. М. Суходолі. Київ : НІСД, 2019. 224 с. **6.** Організаційно-правове забезпечення захисту Службою безпеки України критичної інфраструктури : монографія / авт. кол.: А. Л. Баланда, О. М. Герасименко, В. М. Гребенюк та ін. ; за заг. ред. В. О. Ходановича. Київ : Нац. акад. Служби безпеки України, 2020. 328 с. **7.** Суходоля О. М. Захист критичної інфраструктури: сучасні виклики та пріоритетні завдання сектору безпеки. *Науковий часопис Академії національної безпеки.* 2017. Вип. 1–2 (13–14). С. 50–80. **8.** Зелена книга з питань захисту критичної інфраструктури в Україні : зб. матеріалів міжнар.

експерт. наради / упоряд.: Д. С. Бірюков, С. І. Кондратов ; за заг. ред. О. М. Суходолі. Київ : НІСД, 2015. 176 с. **9.** Суходоля О. Стійкість критичної інфраструктури ЄС: посилення політики та координації // Національний інститут стратегічних досліджень : сайт. 24.02.2023. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/stiykist-krytychnoyi-infrastruktury-yes-posylennya-polityky-ta (дата звернення: 14.02.2024). **10.** Економічна безпека України : навч. посіб. / З. С. Варналій, П. В. Мельник, Л. Л. Тарангул та ін. ; за ред. З. С. Варналія. Київ : Знання, 2009. 647 с. **11.** Сазонов В. В. Кримінологічна модель внутрішніх загроз економічній безпеці України. *Право і суспільство.* 2019. № 3. С. 111–117. DOI: https://doi.org/10.32842/2078-3736-2019-3-1-19. **12.** Кучернюк П. В., Довгаль А. О. Модель загроз безпеки в інформаційно-комунікаційних системах на основі регресійного аналізу. *Електроніка та зв'язок.* 2017. № 2 (97), т. 22. С. 79–84. DOI: https://doi.org/10.20535/2312-1807.2017.22.2.94613. **13.** Гаценко С. С., Пащенко К. В., Свередюк Ю. А., Стариш М. Є. Модель процесу визначення загроз воєнній безпеці, як складової національної безпеки держави. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2021. № 3 (42). С. 111–116. DOI: https://doi.org/10.33099/2311-7249/2021-42-3-111-116. **14.** Мельник Д. С. Правовий захист національної критичної інфраструктури України: актуальні проблеми та потреби удосконалення. *Науковий вісник Національної академії Служби безпеки України.* 2019. № 72. С. 105–114.

*Надійшла до редколегії 18.02.2024*

*Прийнята до опублікування 19.03.2024*

**Melnyk D. S. Creating a model of threats to Ukraine's national critical infrastructure as a basis for ensuring its security and resilience**

*The article presents the current problems of protecting Ukraine's critical infrastructure, current threats to its security and the need to organise proper counteraction under martial law. Threats to critical infrastructure include factors that can actually or potentially harm the stability of its operation, functionality, integrity, resilience or lead to its destruction.*

*The purpose of the article is to create an up-to-date threat model that formalises the likely impacts on Ukraine's critical infrastructure, which will improve the effectiveness of its protection. The scientific novelty of the article is that it examines the actual needs and problematic issues of forming a modern model of threats to critical infrastructure, primarily in the context of the ongoing full-scale military aggression of the russian federation against Ukraine.*

*Creating a threat model is defined for critical infrastructure as a necessity to ensure effective protection of its facilities. The formation of a basic threat model for critical infrastructure facilities, which should include related models of the facility, situation and intruder, is currently an important element of the algorithm for solving this problem.*

*The basic model of threats to critical infrastructure is the framework on which the state determines who and what it needs to protect itself from at the national level. However,*

*Ukrainian legislation currently does not provide for the need to develop a model of threats to the national critical infrastructure, which negatively affects the state of its security and resilience.*

*The perspective measures that will contribute to both the stable functioning of critical infrastructure facilities and ensure their proper protection are outlined: enshrining in Ukrainian legislation the need to develop a model of threats to critical infrastructure, adopting regulations on standardisation of risk management processes for critical infrastructure in order to prevent threats, and more.*

**Key words:** critical infrastructure, facilities, threats, security, protection, counteraction, neutralisation, mitigation, improvement.