Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2025. № 2.

DOI: http://doi.org/10.32702/2307-2105.2025.2.10
УДК 338.49 (477)

М. М. Чеховська,
д. е. н., професор, завідувач кафеди фінансово-економічної безпеки,
Національна академія Служби безпеки України
ORCID ID: https://orcid.org/0000-0001-8135-7770
О. Л. Лісовська,
к. е. н., доцент, доцент кафедри фінансово-економічної безпеки,
Національна академія Служби безпеки України
ORCID ID: https://orcid.org/0000-0002-2272-3053

ЗАГРОЗИ КРИТИЧНІЙ ІНФРАСТРУКТУРІ УКРАЇНИ В СУЧАСНИХ УМОВАХ

M. Chekhovska,
Doctor of Economic Sciences, Professor,
Head of the Department of National Security,
National Academy of Security Service of Ukraine
O. Lisovska,
PhD in Economics, Associate Professor,
Senior Lecturer of the Department of National Security,
National Academy of Security Service of Ukraine,

THREATS TO UKRAINE'S CRITICAL INFRASTRUCTURE IN MODERN CONDITIONS

Стаття присвячена розгляду актуальних загроз критичній інфраструктурі України та основних шляхів забезпечення її безпеки. Авторами класифіковано напрями наукових досліджень щодо безпеки критичної інфраструктури. Здійснено аналіз вітчизняного законодавства щодо визначення переліку загроз критичній інфраструктурі. Також опрацьовано дослідження українських науковців у цій сфері. Спираючись на публікації медіа-джерел, авторами окреслено сучасні загрози критичній інфраструктурі. Окрема увага приділена досвіду країн ЄС та НАТО у забезпеченні стійкості критичної інфраструктури. У статті наголошується на необхідності застосування проактивного підходу у забезпеченні безпеки критичної інфраструктури України як сучасного напряму у процесі забезпечення стійкості критичної інфраструктури. Передбачається, що проактивний підхід підвищить стійкість до впливу на критичну інфраструктуру зовнішніх та внутрішніх викликів й загроз.

The article is devoted to the consideration of current threats to the critical infrastructure of Ukraine and the main ways to ensure its security. The authors classified the areas of scientific research on the security of critical infrastructure. Thus, scientists studied the international experience of protecting critical infrastructure, information security of critical infrastructure facilities, cyber security of critical infrastructure, economic security of critical infrastructure, risk-based approach to ensuring the security of critical infrastructure, organizational and legal principles of protecting critical infrastructure, threats to critical infrastructure facilities. An analysis of domestic legislation was carried out to determine the list of threats to critical infrastructure. It was found that the regulatory framework of Ukraine does not contain a definition of the terms "threat to a critical infrastructure facility" and "threat to critical infrastructure", and there is also no defined general, unified list of threats. Research by Ukrainian scientists on the definition and classification of threats to critical infrastructure was also studied. Based on media sources, the authors outlines modern threats to

critical infrastructure: planning and launching missile and bomb strikes and UAV strikes on critical infrastructure; illegal export of high-tech equipment outside Ukraine; establishment of control by a foreign party over domestic enterprises; illegal seizure of property during privatization; appropriation of budget funds; bankruptcy of state-owned critical infrastructure facilities; cyberattacks on critical infrastructure facilities; sabotage of critical infrastructure facilities, in particular, transport facilities. Special attention is paid to the experience of EU and NATO countries in ensuring the stability of critical infrastructure. The article emphasizes the need to apply a proactive approach to ensuring the security of Ukraine's critical infrastructure as a modern direction in the process of ensuring the stability of critical infrastructure. It is assumed that a proactive approach will increase resistance to the impact of external and internal challenges and threats on critical infrastructure.

Ключові слова: *критична інфраструктура, безпека критичної інфраструктури, збройна агресія, загрози критичній інфраструктурі, проактивний підхід, стійкість.*

Keywords: *critical infrastructure, critical infrastructure security, armed aggression, threats to critical infrastructure, proactive approach, resilience.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Увага до питань безпеки національної критичної інфраструктури прикута тривалий час, що пов'язано, зокрема, із зношеністю основних виробничих фондів; значним антропогенним та техногенним перевантаженням території країни та зростанням ризиків виникнення надзвичайних ситуацій техногенного й природного характеру; небезпекою техногенного, у тому числі ядерного тероризму. Збройна агресія російської федерації проти України лише погіршила ситуацію у зазначеній сфері, адже здебільшого вітчизняна критична інфраструктура є легкодоступною та розміщена по території усієї

держави і ворог намагається максимізувати свій руйнівний вплив всіма можливими способами.

Загалом, повномасштабне вторгнення російської федерації в Україну окреслило багато проблемних питань, пов'язаних із забезпеченням безпеки критичної інфраструктури, не лише в нашій країні, а й за кордоном. Так, якщо мова йде про ситуацію в нашій державі, то це здебільшого нанесення ракетно-бомбових ударів та ударів БПЛА по критичній інфраструктурі, а щодо європейських країн, то ворог застосовує диверсії на об'єктах критичної інфраструктури.

Аналіз останніх досліджень і публікацій. Критична інфраструктура та забезпечення її безпеки є предметом уваги багатьох вітчизняних науковців. Наукові дослідження за зазначеною тематикою можна класифікувати за такими напрямами:

міжнародний досвід захисту критичної інфраструктури (Бірюков Д.С., Єрменчук О.П.);

інформаційна безпека об'єктів критичної інфраструктури (Гончар С.Ф., Леоненко Г.П., Юдін О.К. Юдін О.Ю., Комаров М.Ю., Жевелєва І.С., Куперштейн Л.М., Іванов Ю.А.);

кіберзахист критичної інфраструктури (Ємельянов В.М., Бондар Г.Л., Рогов П.Д, Ворович Б.О., Ткаченко В.А.);

економічна безпека критичної інфраструктури (Брожко О.О., Сокотенюк С.М., Кудряшов В.П., Шемаєва Л.Г.);

ризик-орієнтований підхід до забезпечення безпеки критичної інфраструктури (Тарасенко Ю.С., Савченко Ю.В., Гонтаренко Ю.Д., Зачосова Н.В.);

організаційно-правові засади захисту критичної інфраструктури (Суходоля О.М., Кудряшов В.П., Єрменчук О.П., Франчук В.І., Мельник С.І., Бірюков Д.С., Теленик С.С., Хрутьба В.О.);

загрози об'єктам критичної інфраструктури (Герасименко О.М., Мельник Д.С., Магомедов А.О.).

Формулювання цілей статті (постановка завдання). Разом з цим, залишається недостатньо опрацьованим питання забезпечення безпеки критичної інфраструктури України в умовах збройної агресії російської федерації. Зважаючи на зазначене, *метою статті* є визначення актуальних загроз критичній інфраструктурі та напрямів забезпечення її безпеки.

Виклад основного матеріалу дослідження. Важливим етапом формування нормативно-правового забезпечення процесу функціонування критичної інфраструктури України стало прийняття Закону України «Про критичну інфраструктуру» у листопаді 2021 року, який «визначає правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури» [11]. Наголосимо, що у Законі чітко визначено такі терміни, як «безпека критичної інфраструктури», «захист критичної інфраструктури», «критична інфраструктура», «національна система захисту критичної інфраструктури», «об'єкти критичної інфраструктури», «проектна загроза об'єкту критичної інфраструктури», «стійкість критичної інфраструктури» тощо. У той же час а ні визначення дефініцій «загроза об'єкту критичної інфраструктури» або «загроза критичній інфраструктурі», а ні визначеного загального, уніфікованого переліку загроз немає.

Якщо виходити із переліку завдань формування та реалізації державної політики у сфері захисту критичної інфраструктури, визначених Законом України «Про критичну інфраструктуру», то до загроз для критичної інфраструктури можна віднести «несанкціоноване втручання в її функціонування», «кризові ситуації на об'єктах критичної інфраструктури», «кризові ситуації, що порушують безпеку критичної інфраструктури» [11].

Деякі загрози для критичної інфраструктури зазначаються в основних нормативних документах стратегічного характеру. Так, у Стратегії національної безпеки України зазначено, що «посилюються загрози для критичної інфраструктури, пов'язані з погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим

втручанням у її функціонування, зокрема фізичного і кіберхарактеру, триваючими бойовими діями, а також тимчасовою окупацією частини території України» [18]. Також до загроз у зазначеній сфері можна віднести «недостатній рівень конкуренції та панування монополій, зокрема в енергетичній сфері та інфраструктурі, низька енергоефективність» [18].

В контексті забезпечення виробничої безпеки у Стратегії економічної безпеки України на період до 2025 року йдеться про «незадовільний технічний стан та рівень захисту об'єктів критичної інфраструктури, недостатність інвестицій в її оновлення та розвиток, потенційна загроза несанкціонованих втручань фізичного і кіберхарактеру в її функціонування» [15]. Серед загроз для критичної інфраструктури також можна визначити наступні: «деіндустріалізація економіки; втрата частини промислового потенціалу внаслідок збройної агресії російської федерації та тимчасової окупації частини території України; низький рівень ресурсоефективності економіки та значний рівень ресурсоємності виробництва; низький рівень запровадження новітніх технологій виробництва; висока зношеність основних засобів в основних видах економічної діяльності; наявність частки іноземного капіталу у стратегічних галузях економіки; втрата потенціалу та невирішеність проблеми імпортозаміщення у високотехнологічних виробництвах, насамперед у космічному та авіаційному виробництві; недостатня ефективність державного регулювання у сфері природних монополій; відсутність виробництва повного циклу критично важливої для забезпечення життєдіяльності людини продукції в умовах прояву новітніх тенденцій поширення пандемій, санкційних політик та інших ізоляційних процесів у світі» [15].

У Стратегії забезпечення державної безпеки йдеться про «загрози для критичної інфраструктури, пов'язані з тимчасовою окупацією частини території України, триваючими гібридними впливами з боку суб'єктів розвідувально-підривної діяльності, погіршенням технічного стану такої інфраструктури та намаганнями несанкціонованого втручання в її

функціонування, зокрема фізичного і кіберхарактеру» [16]. Актуальними також «є намагання суб'єктів розвідувально-підривної діяльності отримати доступ до відомостей, що становлять державну таємницю та службову інформацію, а також іншої інформації з обмеженим доступом, вимога щодо захисту якої встановлена законодавством, зокрема передових технологій та розробок, що здійснюються в оборонно-промисловому комплексі, економічній та науково-технічній сферах» [16].

Стратегія кібербезпеки України наголошує, що «набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами» [17].

Підходи вітчизняних науковців, що опрацьовували питання визначення загроз критичній інфраструктурі, зокрема від початку збройної агресії російської федерації проти нашої країни у лютому 2014 року, є значно ширшими, ніж їх нормативне опрацювання. Так, фахівцями Національного інституту стратегічних досліджень було виділено наступні категорії загроз для критичної інфраструктури:

«аварії та технічні збої, зокрема, авіаційні катастрофи, ядерні аварії, пожежі, аварії у системах енергозабезпечення, викиди небезпечних речовин, відмови систем, аварії та надзвичайні події обумовлені недбалістю, організаційними помилками тощо;

небезпечні природні явища, зокрема, надзвичайні погодні умови, лісові, степові та торф'яні пожежі, сейсмічні явища, епідемії та пандемії, космічні явища, урагани, торнадо, землетруси, цунамі, повені і т. ін.;

зловмисні дії, зокрема, зловмисні дії груп або окремих осіб, таких як терористи, злочинці і диверсанти, а також військові дії в умовах війни» [6, с. 12].

Зважаючи на міжнародний досвід, науковці наголошували на особливій небезпечності так званих комбінованих загроз та загроз, реалізація яких, внаслідок взаємозалежності елементів критичної інфраструктури, може призвести до катастрофічних, у т.ч. каскадних ефектів. Зауважимо, що вказаний підхід до класифікації загроз для безпеки критичної інфраструктури підтримують у своїх роботах такі науковці, як Собкарь А.О., Бобро Д.Г. [14, с. 266; 2, с. 46].

Єрменчук О.П. виділяє загрози критичній інфраструктурі через призму захисту державної безпеки і відносить до них наступні:

- «загрози у сфері державної безпеки чи безпекового характеру (тероризм, диверсії, «навмисна помилка», розвід діяльність іноземних спецслужб, економічні експансії, економічне та промислове шпигунство, конкурентна розвідка);
- кіберзагрози (інформаційні атаки, кібертероризм);
- загрози від надзвичайних ситуацій (аварії, катастрофи, стихійні лиха, пожежі, епідемії та пандемії, застосування засобів ураження або інші небезпечні події)» [4, с. 53].

Собкарь А.О. окреслює наступні загрози для критичної інфраструктури:

- «недостатній розвиток організаційно-технічного забезпечення захисту об’єктів критичної інфраструктури і державних електронних інформаційних ресурсів;
- брак спроможностей суб’єктів сектору безпеки і оборони для забезпечення захисту об’єктів критичної інфраструктури та боротьби з кіберзагрозами, кібершпигунством, кібертероризмом та кіберзлочинністю, які негативно впливають на їх стале функціонування;
- запізнення та неефективність дій органів державної влади та силових структур з реагування на загрозу пошкодження критичної інфраструктури та забезпечення її відновлення тощо» [14, с. 267].

Мельник Д.С. запропонував класифікацію загроз критичній інфраструктурі за такими сферами: воєнна, інформаційна, політична, економічна, науково-технологічна, екологічна [8, с. 246-247].

Спираючись на висновки оцінювання загроз критичній інфраструктурі за методом експертного оцінювання, автори Мурасов Р.К. та Мельник Я.В. виділили наступні актуальні загрози: ракетно-дронові удари, кібератаки, аварії на суміжних об'єктах, технічна несправність, втрата контрольованого енергоспоживання, природні катастрофи, теракти, наявність резервування критичних об'єктів, відсутність системи стратегічного планування та координування, недостатнє електропостачання, відсутність паливних резервів, захист потенційно-небезпечних об'єктів критичної інфраструктури, зношеність основних фондів та підвищення аварійності, відсутність енергетичних резервів, штучні природні катастрофи, технічне перевантаження об'єктів, нечітке розмежування повноважень і відповідальності, втрата кваліфікованого персоналу, неспроможність до кризового реагування, блокування необхідних постачань [9, с. 86].

Цікавим є досвід наших західних партнерів у визначенні загроз критичній інфраструктурі та наданні рекомендацій з її захисту. Так, спеціально створена Цільова група ЄС та НАТО щодо стійкості критичної інфраструктури (далі – Цільова група) у 2023 році описала поточні виклики безпеці, до яких було віднесено, у тому числі й зважаючи на досвід збройної агресії росії проти України: збої в роботі критичної інфраструктури через вплив природних та/або антропогенних факторів; вразливість критичної інфраструктури до навмисних атак або аварій; діяльність терористичних організацій; стихійні лиха або екстремальні погодні умови; використання кібератак; шпигунство; використання залежностей або захоплення критичної інфраструктури [1]. Крім того, Цільовою групою було визначено основні сектори критичної інфраструктури, а саме енергетику, транспорт, цифрову інфраструктуру та космос.

Аналіз медіа-джерел дав нам змогу виокремити такі актуальні загрози критичній інфраструктурі [13]:

- планування та нанесення ракетно-бомбових ударів та ударів БПЛА по критичній інфраструктурі;
- нелегальне вивезення за межі України високотехнологічного обладнання;
- встановлення контролю іноземною стороною над вітчизняними підприємствами;
- незаконне заволодіння майном під час приватизації;
- привласнення бюджетних коштів;
- банкрутство державних об’єктів критичної інфраструктури;
- здійснення кібератак на об’єкти критичної інфраструктури;
- диверсії на об’єктах критичної інфраструктури, зокрема, транспортної.

Важливо наголосити, що визначення загроз критичній інфраструктурі передбачає й окреслення напрямів забезпечення безпеки критичної інфраструктури.

Так, погоджуємося із колективом авторів щодо запропонованих ними заходів протидії загрозам за наступними напрямами захисту:

«фізичний захист – спрямований на забезпечення захищеності об’єктів від несанкціонованого доступу, попередження та припинення диверсій, крадіжки або будь-якого іншого незаконного вилучення обладнання, пристроїв та матеріалів;

технічний захист – підвищення відмовостійкості і живучості систем, функціональне резервування;

персонал – підготовка та перевірка персоналу, контроль його здатності до виконання визначених функцій, захищеність персоналу;

інформаційні технології – захист інформації, систем зв’язку і управління;

юридичний – врегулювання питань реагування персоналу та функціонування інфраструктури у кризових ситуаціях, закріплення розподілу

відповідальності у нормативних і правових документах, розробка керівництв і інструкцій для персоналу, в тому числі щодо взаємодії в умовах кризової ситуації;

плани відновлення – створення планів, резервів та сервісів для швидкого відновлення втрачених функцій» [6, с. 13].

Крім того, як ми вже зазначали раніше, цікавим є досвід ЄС і НАТО щодо зміцнення стійкості критичної інфраструктури та її захисту. Так, іноземними фахівцями пропонується: налагодити механізм забезпечення швидкої взаємодії між суб'єктами захисту критичної інфраструктури у випадку виявлення загроз; розробляти регулярні оцінки загроз для критичної інфраструктури; аналізувати збройну агресію росії проти України в контексті забезпечення стійкості критичної інфраструктури; сприяти взаємодії між державами-членами НАТО та приватним сектором у питаннях посилення кіберстійкості критичної інфраструктури та у питаннях безпеки при проєктуванні критичної інфраструктури; використовувати синергію та потенційні сфери співпраці у діяльності із забезпечення безпеки критичної інфраструктури, включаючи виклики, пов'язані з новими технологіями або безпекою ланцюга поставок [1].

Наголосимо, що сучасним напрямом у процесі забезпечення стійкості критичної інфраструктури є реалізація проактивного підходу. Варто зазначити, що проактивний підхід на сьогодні використовується в багатьох сферах, зокрема, управлінській, проєктного менеджменту, безпековій. Так, термін «проактивний» було запроваджено австрійським психіатром Віктором Франклом «для позначення особи, що бере відповідальність за себе і своє життя, а не шукає причин для подій, які відбуваються з ним, у навколишніх людях і обставинах» [7, с. 42]. У Кембриджському словнику терміну «проактивний» надається наступне значення: «той, хто виконує дії, які сприяють змінам, а не тільки реагує на зміни, коли вони відбуваються» [12]. Ньюстром Д.В. та Девіс К. визначили термін «проактивность» як

«передбачення подій, ініціацію змін, прагнення «тримати в своїх руках» долю організації» [19].

Відповідно у науковому середовищі сформувалося розуміння терміну «проактивний підхід». Так, Зайцева І.Ю. наголошує, що «проактивний підхід дозволить заздалегідь бути готовим до процесів, що викликають нестабільність та незбалансованість діяльності», крім того, використання проактивного підходу «дасть можливість передбачити ризики та загрози внутрішнього та зовнішнього середовища, підготуватися до попередження проблем, виділити пріоритетні і найбільш важливі задачі, врахувати необхідні для цього ресурси та ефективно їх використовувати, змінити план після початку роботи, додати нові задачі, отримати додатковий час для аналізу поточних дій для покращення якості їх виконання, а також для планування розв'язання проблем» [5, с. 181, 183]. Олексієнко М.М. зазначає, що «проактивний підхід дає змогу на основі точних і актуальних даних запобігти можливим проблемам або миттєво реагувати на них у випадку виникнення та мінімізувати наслідки» [10, с. 68]. Науковці Національного університету оборони України звертають увагу, що «проактивний підхід дозволяє передбачити можливі ризики, їхні наслідки та рівень впливу на підприємство», і саме «за допомогою проактивного підходу можна приймати запобіжні заходи щодо управління ризиками, щоб зменшити їхній негативний вплив» [3, с. 77].

Проактивний підхід у забезпеченні безпеки критичної інфраструктури, на нашу думку, полягає у застосуванні випереджувальних дій щодо аналізу загроз критичній інфраструктурі та негативних чинників внутрішнього та зовнішнього середовища, що нададуть можливість попередити або мінімізувати їх несприятливі наслідки. Безпековий напрям проактивного підходу підвищить стійкість до впливу на критичну інфраструктуру зовнішніх та внутрішніх викликів й загроз.

Серед чинників застосування проактивного підходу у забезпеченні безпеки критичної інфраструктури зазначимо процес управління ризиками, механізм кризового управління, забезпечення ланцюгів постачання тощо.

Висновки та перспективи подальших розвідок у даному напрямі. Сучасні методи та засоби ведення воєнних дій сприяють збільшенню загроз та руйнівному впливу на критичну інфраструктуру, що вимагає підвищення стандартів її безпеки. Підтримуючи напрацювання вітчизняних та іноземних дослідників щодо безпеки критичної інфраструктури, особливо в умовах продовження збройної агресії російської федерації проти України, наголошуємо на необхідності застосування проактивного підходу у цій сфері. Зазначений підхід надасть можливість здійснювати системний аналіз та оцінку ризиків, оперативно та своєчасно реагувати на виявлені слабкі місця у забезпеченні безпеки критичної інфраструктури.

Література

1. EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564 (дата звернення 07.01.2025).

2. Бобро Д.Г. Урахування проектних загроз у розбудові державної системи захисту критичної інфраструктури. *Стратегічні пріоритети.* 2017. № 3 (44). С. 42-51.

3. Дриньов Д., Войтех К., Тимошенко Р. Штучний інтелект в процесі прийняття та реалізації управлінських рішень. *Таврійський науковий вісник. Серія: Економіка*. 2023. № 18. С. 74-79. URL: https://doi.org/10.32782/2708-0366/2023.18.7 (дата звернення 09.01.2025).

4. Єрменчук О.П. Оцінка загроз критичній інфраструктурі як важлива складова частина діяльності із захисту державної безпеки. *Jurnalul juridic naţional: teorie şi practică.* 2018. № 12. С. 50-54.

5. Зайцева І.Ю., Ковтун Т.В. Застосування проактивного підходу при формування економічної безпеки на залізничному транспорті. *Вісник*

економіки транспорту і промисловості. 2015. № 50. С. 180-184. URL: http://nbuv.gov.ua/UJRN/Vetp_2015_50_10 (дата звернення 09.01.2025).

6. Зелена книга з питань захисту критичної інфраструктури в Україні / Бірюков Д.С. та ін. Київ: НІДД, 2015. 35 с. URL: https://cdn.regulation.gov.ua/6a/69/2a/fa/regulation.gov.ua_File_188.pdf (дата звернення 04.01.2025).

7. Лозова О.В., Тимошенко І.С. Проактивна поведінка підприємства в сучасних умовах господарювання. *Бізнес Інформ*. 2023. № 4. С. 155-160. URL: http://nbuv.gov.ua/UJRN/binf_2023_4_23 (дата звернення 09.01.2025).

8. Мельник Д.С. Побудова моделі загроз національній критичній інфраструктурі України як основа забезпечення її безпеки та стійкості. *Вісник Харківського національного університету внутрішніх справ*. 2024. № 1(1). С. 237-250. URL: http://nbuv.gov.ua/UJRN/VKhnuvs_2024_1(1)__22. (дата звернення 09.01.2025).

9. Мурасов Р.К., Мельник Я.В. Результати оцінювання загроз критичній інфраструктурі методом експертного оцінювання. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 3 (48). С. 83-88.

10. Олексієнко М.М. Проактивний підхід до управління екологічними проектами. *Управління розвитком складних систем*. 2013. № 14. С. 68-71. URL: http://nbuv.gov.ua/UJRN/Urss_2013_14_14 (дата звернення 09.01.2025).

11. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. Дата оновлення: 21.09.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення 06.01.2025).

12. Проактивність в IT: що це та як її використовувати. URL: https://aw.club/global/uk/blog/proactivity-in-tech-what-it-is-and-how-to-use-it (дата звернення 07.01.2025).

13. Сайт Служби безпеки України. Новини. URL: https://ssu.gov.ua/novyny (дата звернення 04.01.2025).

14. Собкарь А.О. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки України. *Російсько-українська війна: право, безпека, світ* : матеріали VI Міжнародної науково-практичної конференції, м. Київ, 29-30 квітня 2022 р.). URL:

http://confuf.wunu.edu.ua/index.php/confuf/article/view/951/933 (дата звернення 07.01.2025).

15. Стратегія економічної безпеки України на період до 2025 року : Указ Президента України від 11.08.2021 р. № 347/2021. URL: https://zakon.rada.gov.ua/laws/show/347/2021#n23 (дата звернення 06.01.2025).

16. Стратегія забезпечення державної безпеки : Указ Президента України від 16.02.2022 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#n5 (дата звернення 06.01.2025).

17. Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення 06.01.2025).

18. Стратегія національної безпеки України «Безпека людини – безпека країни» : Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text. Дата оновлення: 07.01.2025. (дата звернення 09.01.2025).

19. Толпежніков Р.О. Управління змінами сукупного потенціалу підприємства. *Ефективна економіка.* 2015. № 3. URL: http://www.economy.nayka.com.ua/?op=1&z=4930 (дата звернення 07.01.2025).

References

1. European Commission (2023), “EU-NATO Task Force: Final assessment report on strengthening our resilience and protection of critical infrastructure”, available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3564 (Accessed 07.01.2025).

2. Bobro, D.H. (2017), “Taking into account project threats in the development of the state system of critical infrastructure protection”, Stratehichni priorytety, vol. 3 (44), pp. 42-51.

3. Dryn'ov, D. Vojtekh, K. and Tymoshenko R. (2023), “Artificial intelligence in the process of making and implementing managerial decisions”,

Tavrijs'kyj naukovyj visnyk. Seriia: Ekonomika, vol. 18, pp. 74-79. https://doi.org/10.32782/2708-0366/2023.18.7

4. Yermenchuk, O.P. (2018), "Assessment of threats to critical infrastructure as an important component of activities to protect state security", Jurnalul juridic naţional: teorie şi practică, vol. 12, pp. 50-54.

5. Zajtseva, I.Yu. and Kovtun, T.V. (2015), "Application of a proactive approach in the formation of economic security in railway transport", Visnyk ekonomiky transportu i promyslovosti, vol. 50, pp. 180-184, available at: http://nbuv.gov.ua/UJRN/Vetp_2015_50_10 (Accessed 09.01.2025).

6. Biriukov, D.S. (2015), Zelena knyha z pytan' zakhystu krytychnoi infrastruktury v Ukraini. [Green Paper on Critical Infrastructure Protection in Ukraine], NISD, Kyiv, Ukraine, available at: https://cdn.regulation.gov.ua/6a/69/2a/fa/regulation.gov.ua_File_188.pdf (Accessed 04.01.2025).

7. Lozova, O.V. and Tymoshenko, I.S. (2023), "Proactive behavior of an enterprise in modern business conditions", Biznes Inform, vol. 4, pp. 155-160, available at: http://nbuv.gov.ua/UJRN/binf_2023_4_23 (Accessed 09.01.2025).

8. Mel'nyk, D.S. (2024), "Construction of a model of threats to the national critical infrastructure of Ukraine as a basis for ensuring its security and stability", Visnyk Kharkivs'koho natsional'noho universytetu vnutrishnikh sprav, vol. 1 (1), pp. 237-250, available at: http://nbuv.gov.ua/UJRN/VKhnuvs_2024_1(1)__22 (Accessed 09.01.2025).

9. Murasov, R.K. and Mel'nyk, Ya.V. (2023), "Results of assessing threats to critical infrastructure using the expert assessment method", Suchasni informatsijni tekhnolohii u sferi bezpeky ta oborony, vol. 3 (48), pp. 83-88.

10. Oleksiienko, M.M. (2013), "Proactive approach to environmental project management", Upravlinnia rozvytkom skladnykh system, vol. 14, pp. 68-71, available at: http://nbuv.gov.ua/UJRN/Urss_2013_14_14 (Accessed 09.01.2025).

11. Verkhovna Rada of Ukraine (2021), The Law of Ukraine "About critical infrastructure", available at: https://zakon.rada.gov.ua/laws/show/1882-20#Text (Accessed 06.01.2025).

12. Serhieieva, S. (2023), “Proactivity in IT: what it is and how to use it”, available at: https://aw.club/global/uk/blog/proactivity-in-tech-what-it-is-and-how-to-use-it (Accessed 07.01.2025).

13. Security Service of Ukraine (2025), “News”, available at: https://ssu.gov.ua/novyny (Accessed 04.01.2025).

14. Sobkar', A.O. (2022), “Threats to critical infrastructure and their impact on the state of national security of Ukraine”, Rosijs'ko-ukrains'ka vijna: pravo, bezpeka, svit : materialy VI Mizhnarodnoi naukovo-praktychnoi konferentsii [Russian-Ukrainian war: law, security, peace: materials of the VI International Scientific and Practical Conference], Kyiv, Ukraine, available at: http://confuf.wunu.edu.ua/index.php/confuf/article/view/951/933 (Accessed 07.01.2025).

15. President of Ukraine (2021), Decree “Strategy of economic security of Ukraine for the period until 2025”, available at: https://zakon.rada.gov.ua/laws/show/347/2021#n2Z (Accessed 06.01.2025).

16. President of Ukraine (2022), Decree “Strategy for ensuring state security”, available at: https://zakon.rada.gov.ua/laws/show/56/2022#n5 (Accessed 06.01.2025).

17. President of Ukraine (2021), Decree “Cybersecurity Strategy of Ukraine “A secure cyberspace is the key to the successful development of the country””, available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text (Accessed 06.01.2025).

18. President of Ukraine (2020), Decree “National Security Strategy of Ukraine “Human security is the security of the country””, available at: https://zakon.rada.gov.ua/laws/show/392/2020#Text (Accessed 09.01.2025).

19. Tolpezhnikov, R.O. (2015), “Mastering change of total potential of enterprise”, Efektyvna ekonomika, vol. 3, available at: http://www.economy.nayka.com.ua/?op=1&z=4930 (Accessed 07.01.2025).

Стаття надійшла до редакції 20.01.2025 р.