УДК 351.746:351.861:005.334(477)

В. О. Торічний, В. В. Залож, І. В. Шашкун

АНАЛІЗ ЗАГРОЗ І РИЗИКІВ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

У статті здійснено системний аналіз загроз і ризиків, що впливають на об'єкти критичної інфраструктури Державної прикордонної служби України. Обґрунтовано актуальність проблеми забезпечення стійкості функціонування критично важливих об'єктів прикордонного відомства, від яких безпосередньо залежить прикордонна безпека, обороноздатність держави, стабільність систем управління, зв'язку, логістики та життєзабезпечення, в повсякденних умовах та в умовах особливих правових режимів. Розкрито, що сучасні загрози для об'єктів критичної інфраструктури Державної прикордонної служби України мають комплексний, багатовимірний характер і включають воєнні, терористичні, техногенні, кібернетичні, інформаційно-психологічні та соціально-економічні чинники прояву.

Отримані результати дозволяють визначити пріоритети захисту об'єктів критичної інфраструктури, оптимізувати розподіл ресурсів та формувати основу для побудови інтегрованої системи управління ризиками в Державній прикордонній службі України. Запропонований підхід забезпечує можливість своєчасного виявлення вразливих елементів, прогнозування загроз, розроблення превентивних і компенсаційних заходів. Практичне впровадження результатів дослідження стане важливою умовою підвищення стійкості критичної інфраструктури прикордонного відомства, забезпечуючи її безперервне та ефективне функціонування як у повсякденних умовах, так і за дії особливих правових режимів.

Ключові слова: *Державна прикордонна служба України, державний кордон, прикордонна безпека, організаційна стійкість, критична інфраструктура, захист об'єктів, загрози, ризики, аналіз, класифікація, ризик-менеджмент, управління.*

Постановка проблеми. Події останнього десятиліття в Україні, а саме – збройна агресія російської федерації (далі – рф) та запровадження у 2022 році воєнного стану, призвели до суттєвого зростання спектра загроз, які завдають шкоди прикордонній безпеці та обороноздатності держави, її соціально-економічній стабільності та іншим життєво важливим національним інтересам. У сучасних умовах широкомасштабної війни особливої актуальності набуває питання забезпечення стійкості та безпеки функціонування об'єктів критичної інфраструктури (далі – ОКІ) сектору безпеки й оборони (далі – СБО), зокрема Державної прикордонної служби України (далі – ДПСУ), яка виконує ключову роль у забезпеченні охорони та захисту державного кордону (далі – ДК), підтриманні оборонної спроможності країни та стабільності системи інтегрованого управління державним кордоном України.

Критична інфраструктура ДПСУ є невід'ємною складовою системи національної безпеки, оскільки забезпечує виконання завдань у системі інтегрованого управління державним кордоном України, організаційну стійкість систем управління, зв'язку, інформаційних та логістичних мереж тощо. Загрози, спрямовані проти таких об'єктів, мають комплексний характер і поєднують у собі воєнні, терористичні, кібернетичні, інформаційно-психологічні, техногенні та інші фактори. Їх реалізація може призвести до порушення організаційної стійкості систем управління, втрати функціональної спроможності органів ДПСУ, зниження ефективності оперативно-службової діяльності (далі – ОСД) та дестабілізації роботи в цілому.

У сучасних умовах спостерігається суттєве підвищення рівня загроз, спрямованих безпосередньо на ОКІ прикордонного відомства. Ці загрози характеризуються високою динамікою проявів, складністю прогнозування та потенційно тяжкими наслідками.

Водночас специфіка діяльності ДПСУ зумовлює наявність особливих ризиків, пов'язаних із географічним розташуванням об'єктів, ступенем їх інженерного захисту, рівнем технічного оснащення та залежністю від зовнішніх комунікацій і постачань. З огляду на окреслену ситуацію нагальною є потреба у створенні науково обґрунтованої системи ідентифікації, класифікації та аналізу загроз і ризиків для об'єктів критичної інфраструктури ДПСУ. Це дозволить своєчасно виявляти вразливі елементи, оцінювати рівень ризику, формувати ефективні механізми запобігання та мінімізації негативних наслідків.

Розв'язання зазначеної проблеми науковим шляхом сприятиме вдосконаленню правових, організаційних і технічних заходів захисту об'єктів критичної інфраструктури ДПСУ, підвищенню її організаційної стійкості, насамперед в умовах особливих правових режимів, та забезпеченню безперервності управління діяльністю. Враховуючи наведене, проведення дослідження, присвяченого аналізу загроз і ризиків об'єктів критичної інфраструктури ДПСУ, є актуальним, своєчасним і таким, що логічно продовжує попередні дослідження авторів.

Аналіз останніх досліджень і публікацій. Проблематика забезпечення безпеки ОКІ вже тривалий час залишається одним із пріоритетних напрямів досліджень українських учених. Аналіз сучасних публікацій щодо зазначеної теми [1-12] свідчить про стале зростання уваги до питань захисту критичної інфраструктури в контексті національної безпеки, зокрема в умовах запровадження особливих правових режимів. Такий інтерес обумовлений необхідністю забезпечення стійкості функціонування державних інституцій, складових СБО та їх систем управління в умовах постійних загроз гібридного характеру.

Попри значну кількість наукових праць, присвячених проблемам безпеки критичної інфраструктури держави, питання комплексного та системного аналізу загроз і ризиків для об'єктів критичної інфраструктури ДПСУ залишаються недостатньо дослідженими. У наукових публікаціях фахівців [13-14] розглядаються окремі аспекти проблеми – зокрема, аналіз ризиків і розроблення методичного апарату їх оцінювання в умовах воєнного стану. Водночас такі дослідження здебільшого мають фрагментарний характер і не формують цілісної наукової концепції оцінювання загроз та ризиків у різних умовах функціонування ДПСУ.

Досі відсутній системний підхід, який би поєднував аналіз ризиків у повсякденних умовах діяльності ДПСУ та в умовах особливих правових режимів, що істотно ускладнює формування ефективної системи управління безпекою критичної інфраструктури. У цьому контексті актуальним є проведення дослідження, спрямованого на визначення, систематизацію та оцінювання потенційних загроз і ризиків для об'єктів критичної інфраструктури прикордонного відомства, а також на розроблення аналітичної бази для побудови моделей управління ризиками. Отримані результати матимуть важливе практичне значення – вони сприятимуть підвищенню рівня стійкості функціонування критичної інфраструктури ДПСУ у повсякденній діяльності та умовах особливих правових режимів.

Метою статті є здійснення системного аналізу загроз і ризиків об'єктів критичної інфраструктури ДПСУ в умовах повсякденної діяльності та особливих правових режимів з метою подальшої їх ідентифікації, оцінювання та управління в межах системи ризик-менеджменту.

Виклад основного матеріалу. Критична інфраструктура ДПСУ у статті розглядається як сукупність об'єктів, їх частин і систем, що є важливими для забезпечення прикордонної безпеки та управління державним кордоном України, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам держави, мати значний негативний вплив на національну безпеку, оборону та життєдіяльність суспільства [18].

Функціонування таких об'єктів супроводжується впливом широкого спектра загроз різного характеру. У цьому контексті доцільним є проаналізувати наявні класифікації загроз критичній інфраструктурі та, спираючись на результати такого аналізу, запропонувати авторську класифікацію загроз. Таке дослідження має практичне значення для розробки ефективних заходів протидії та захисту критичної інфраструктури ДПСУ в сучасних умовах.

Аналіз зарубіжного досвіду свідчить, що класифікація загроз критичній інфраструктурі у різних країнах має як спільні риси, так і значні національні відмінності, що обумовлено специфікою безпекової ситуації, пріоритетами державної політики та рівнем розвитку інфраструктури. Так, у США загрози визначаються як природні або техногенні явища, суб'єкти чи дії, які можуть завдати шкоди життю, інформації, власності тощо, при цьому пріоритетна увага зосереджена на кібератаках, терористичних актах і природних катаклізмах.

У країнах Європейського Союзу підхід до класифікації загроз формується на основі принципів Європейської програми захисту критично важливої інфраструктури, де виділяються кіберзагрози, тероризм, злочинні дії, техногенні аварії та природні небезпеки. Німеччина пропонує більш деталізовану класифікацію, що охоплює природні явища (повені, бурі, посухи, землетруси, лавини тощо), людські помилки та технічні збої, а також терористичні акти та злочинні дії, що спрямовані на порушення функціонування критичної інфраструктури. У Франції та Великобританії акцент робиться на кіберзагрози та терористичні дії, спеціалізовані органи мають координувати заходи протидії та

аналізувати розвідувальні дані. У країнах Північної та Східної Європи, зокрема в Данії та Нідерландах, загрози ОКІ розглядаються через призму надзвичайних ситуацій, аварій та кризового управління, а в Румунії класифікація базується на природних, випадкових та умисних загрозах [15].

Наведений досвід демонструє, що незалежно від конкретної країни, класифікація загроз критичній інфраструктурі базується на системному підході, що враховує джерела загроз, їхні види та потенційний вплив на функціонування об'єктів. Водночас конкретні підходи до ідентифікації та пріоритезації загроз формуються з урахуванням національної специфіки, безпекової ситуації та технологічних особливостей держави. Для України та, зокрема, для об'єктів критичної інфраструктури ДПСУ важливими є аспекти, пов'язані з сучасною воєнною агресією, ракетно-дроновими ударами, диверсійними діями, кіберзагрозами та інформаційно-психологічними впливами.

Спираючись на міжнародні підходи та специфіку функціонування ДПСУ, доцільним є виділення основних категорій загроз та ризиків їх реалізації, що враховують як традиційні джерела небезпеки (природні, техногенні, кримінальні), так і сучасні фактори бойового і гібридного впливу.

У табл. 1 наведено авторську класифікацію загроз для об'єктів критичної інфраструктури ДПСУ, яка буде слугувати аналітичною основою для оцінки ризиків і побудови системи управління ризиками.

Таблиця 1 – Класифікація загроз для об'єктів критичної інфраструктури ДПСУ

Категорія загроз	Типові сценарії (вектори) реалізації загрози	Характер впливу на ОКІ ДПСУ
Воєнно-політичні загрози	Ракетні та дронові удари, артилерійські обстріли, окупація територій із важливою інфраструктурою, порушення логістичних ланцюгів постачання тощо	Фізичне руйнування споруд і обладнання, що мають стратегічне значення для безпеки та обороноздатності держави, ураження особового складу, порушення безперервності реалізації функцій, логістики, дестабілізації ситуації в країні тощо
Терористичні та диверсійні загрози	Фізичні напади на прикордонні наряди, пункти пропуску, закладення вибухових пристроїв або підпали, підрив транспортної та енергетичної інфраструктури в прикордонній смузі	Виведення з ладу об'єктів, порушення режимів функціонування, локальні руйнування, створення паніки та підрив довіри до державних органів тощо
Природно-кліматичні загрози	Стихійні лиха (землетруси, повені, буревії, урагани, зсуви, лісові пожежі), кліматичні зміни, епідемії та пандемії	Пошкодження інфраструктури, фізичної цілісності споруд, ускладнення руху і постачання, загроза життю та здоров'ю особового складу (зниження працездатності), зниження рівня укомплектованості підрозділів (унаслідок захворювань або травм), порушення (пошкодження) комунікацій тощо
Експлуатаційні загрози	Природне зношення інженерних конструкцій і комунікацій, відмова або несправність обладнання через порушення регламентів технічного обслуговування, недотримання правил експлуатації, помилки особового складу під час технічного обслуговування або експлуатації, використання неякісних матеріалів чи комплектувальних виробів, відсутність резервних систем або недостатній рівень їх готовності	Часткове або повне виведення з ладу елементів критичної інфраструктури, зниження ефективності функціонування систем життєзабезпечення, зв'язку, енергопостачання, переривання або зниження стійкості функціонування об'єктів, зростання витрат на ремонт і відновлення, підвищення ризику аварій, пожеж чи інших надзвичайних ситуацій техногенного характеру

Кінець таблиці 1

Категорія загроз	Типові сценарії (вектори) реалізації загрози	Характер впливу на ОКІ ДПСУ
Техногенні загрози	Техногенні аварії на енергетичних об’єктах, витоки небезпечних речовин, вибухи, пожежі на виробництві; технічні збої, порушення роботи транспорту; збої у системах зв’язку, водо- та теплопостачання тощо	Втрати енергопостачання, порушення транспортних і логістичних зв’язків, збої у системах управління, відмова технічних систем тощо
Кіберзагрози	Хакерські втручання, кібератаки на інформаційні та комунікаційні системи, DDoS-атаки, шкідливе ПЗ, викрадення або знищення даних, маніпуляції системами автоматичного управління	Несанкціонована зміна або спотворення інформації (цілісність даних), доступ до конфіденційної інформації, порушення роботи систем управління, втрати даних, дезорганізація управлінських процесів, розповсюдження шкідливого програмного забезпечення тощо
Кримінальні (злочинні) загрози	Руйнування прикордонної інфраструктури, напади (захоплення) об’єктів несення служби та пунктів дислокації	Порушення правового режиму кордону, порушення безпеки об’єктів і особового складу, дестабілізація логістики, втрати матеріальних ресурсів, ускладнення контролю тощо
Інформаційно-комунікаційні загрози	Інформаційно-психологічні операції (ІПсО), дезінформація, пропаганда, психологічний тиск на особовий склад	Компрометація репутації та підрив довіри суспільства, дестабілізація роботи підрозділів, зниження бойового духу особового складу, помилкові рішення, внутрішня дестабілізація, паніка тощо
Соціально-економічні загрози	Корупція, недофінансування, кадровий дефіцит, зростання вартості енергії або палива, скорочення бюджету на обслуговування інфраструктури, залежність від імпорту критичних матеріалів, фінансові злочини (шахрайство, відмивання коштів, інші незаконні фінансові операції)	Порушення безперервності функціонування ОКІ, збільшення витрат на забезпечення роботи, недотримання норм безпеки та обслуговування через обмеження ресурсів, що призводить до каскадного зростання експлуатаційних та техногенних загроз, ускладнення виконання проєктів, завдань, обмеження можливостей модернізації та утримання ОКІ тощо
Управлінські (адміністративно-організаційні) загрози	Відсутність або неузгодженість планів реагування на надзвичайні ситуації, недостатня координація між органами управління, службами та підрозділами, недоліки у системі внутрішнього контролю, низька кваліфікація особового складу, кадровий дефіцит, порушення процедур управління безпекою чи реагування.	Зниження ефективності функціонування систем безпеки, затримка або неадекватність реагування на інциденти, підвищення ймовірності реалізації інших загроз, втрата керованості підрозділів у кризових умовах тощо

Запропонована класифікація загроз об’єктам критичної інфраструктури ДПСУ базується на комплексному аналізі сучасних викликів, з якими стикається держава і безпосередньо прикордонне відомство. Її доцільність полягає у здатності забезпечити всебічний підхід до аналізу загроз, який охоплює як традиційні, так і сучасні фактори, що виникають у контексті воєнного стану та гібридної

війни. Такий підхід ґрунтується на принципах системності, комплексності, аналізу причинно-наслідкових зв'язків, адаптивності та актуальності для прикордонної сфери. Він дозволяє не лише систематизувати загрози та враховувати всі можливі аспекти їхнього впливу на об'єкти критичної інфраструктури ДПСУ, а й ефективно розподіляти ресурси для запобігання та нейтралізації негативних наслідків.

Водночас для практичного застосування аналізу дослідження також необхідно проаналізувати ризики, що дозволить оцінити ймовірність реалізації конкретних загроз і потенційний масштаб їхнього впливу.

Такий аналіз слугує основою для побудови системи управління ризиками, розробки превентивних заходів та визначення пріоритетів у забезпеченні захищеності ОКІ прикордонного відомства.

У попередніх дослідженнях [16] авторами було розроблено класифікацію ОКІ за основними ознаками: функціональним призначенням; рівнем критичності (важливістю для функціонування); ступенем уразливості та характером загроз; просторово-територіальною ознакою; типом ресурсів, що забезпечують функціонування; видами потенційних загроз; ступенем захищеності.

Слід також зауважити, що у дослідженнях, присвячених управлінню ризиками ОКІ, доцільним і методологічно коректним, на думку авторів, є використання однакових або аналогічних назв для категорій загроз і відповідних категорій ризиків. Такий підхід ґрунтується на логічному зв'язку між джерелами потенційної небезпеки та можливими негативними наслідками їх реалізації. У цьому контексті загроза розглядається як подія або сукупність умов, що можуть спричинити небажаний вплив на ОКІ, тоді як ризик визначається як імовірність реалізації цієї загрози у поєднанні з масштабом можливих наслідків.

Саме тому назви категорій авторами статті були синхронізовані: наприклад, воєнно-політичні загрози відповідають воєнно-політичним ризикам, техногенні загрози – техногенним ризикам, кіберзагрози – кіберризикам тощо. Така термінологічна узгодженість спрощує структурування аналітичних матеріалів, забезпечує логічну єдність класифікації. Разом з тим, важливо підкреслити, що співпадіння назв не означає тотожності змісту: загроза описує потенційний вплив, тоді як ризик характеризує можливість та очікувані наслідки цього впливу. Таким чином, використання однойменних категорій загроз і ризиків є обґрунтованим, підвищує структурованість аналітичного процесу та забезпечує методичну сумісність моделі управління ризиками в системі ДПСУ.

На основі отриманих результатів аналізу є можливість узагальнити їх у вигляді матриці «об'єкт ризику – типи ризиків – важливість для функціонування – категорія критичності» (табл. 2).

Таблиця 2 – Матриця ризиків об'єктів критичної інфраструктури ДПСУ

Об'єкти ризику	Типи ризиків	Категорія критичності відповідно до нормативних документів [17], [18]
Інженерно-технічні споруди державного кордону	воєнно-політичні; терористичні та диверсійні; природно-кліматичні; експлуатаційні; техногенні; кримінальні (злочинні)	II (життєво важливі)
Технічні засоби охорони державного кордону	кіберризики; експлуатаційні; природно-кліматичні; воєнно-політичні	II (життєво важливі)
Системи комунікації	кіберризики; інформаційно-комунікаційні; воєнно-політичні, терористичні; диверсійні	I особливо (критично) важливі
Об'єкти управління та контролю	кіберизики; воєнно-політичні; терористичні; диверсійні; організаційні; експлуатаційні	I особливо (критично) важливі
Логістичні об'єкти	воєнно-політичні; терористичні; диверсійні; організаційні; техногенні; експлуатаційні; соціально-економічні	II (життєво важливі)

Кінець таблиці 2

Об’єкти ризику	Типи ризиків	Категорія критичності відповідно до нормативних документів [17], [18]
Об’єкти забезпечення життєдіяльності	воєнно-політичні; терористичні; диверсійні; організаційні; техногенні; експлуатаційні; природно-кліматичні	II (життєво важливі)
Об’єкти забезпечення безпеки	терористичні; диверсійні; кримінальні (злочинні); воєнно-політичні; техногенні; організаційні	II (життєво важливі)
Об’єкти тилового забезпечення	воєнно-політичні; терористичні; диверсійні; техногенні; експлуатаційні; соціально-економічні; організаційні	III важливі
Об’єкти соціальної інфраструктури	воєнно-політичні; терористичні; диверсійні; соціально-економічні, експлуатаційні; техногенні	IV необхідні

Аналіз наведеної матриці дозволяє зробити низку узагальнених висновків щодо структури ризиків, категорій критичності та пріоритетів управління безпекою об’єктів критичної інфраструктури ДПСУ.

1. *Загальна структура ризиків.* У системі об’єктів критичної інфраструктури ДПСУ простежується комплексна багаторівнева структура ризиків, що охоплює практично всі категорії, визначені класифікацією. Найбільш розповсюдженими є:

– воєнно-політичні ризики – характерні для всіх без винятку об’єктів, що відображає актуальний стан воєнної загрози та збройної агресії проти України;

– терористичні та диверсійні загрози – наявні у переважній більшості об’єктів, зокрема у системі охорони та захисту ДК, управління та логістики;

– експлуатаційні та техногенні ризики – притаманні інженерно-технічним, логістичним і тиловим об’єктам, що свідчить про необхідність посилення технічного контролю, сервісного обслуговування та модернізації;

– кіберризики та ризики інформаційної безпеки – концентруються у системах комунікації, управління та технічного контролю, тобто в сегментах, які забезпечують стійкість управлінського контуру ДПСУ.

2. *Основні закономірності та тенденції:*

– найбільша щільність воєнно-політичних, техногенних, диверсійних та терористичних ризиків спостерігається на рівні I–II категорій критичності об’єктів, що визначає пріоритетність їхнього захисту;

– стійка взаємозалежність ризиків різного характеру. Наприклад, руйнування об’єктів унаслідок бойових дій (воєнно-політична загроза) може провокувати техногенні аварії або порушення зв’язку (кіберризики, інформаційні ризики);

– організаційні ризики мають вагомий вплив на стабільність об’єктів II–III категорій, особливо у питаннях логістики, управління ресурсами та координації між підрозділами;

– ризики з нижчою категорією критичності (III–IV) виступають множником загальної вразливості системи, оскільки їхній кумулятивний ефект може знижувати здатність до оперативного реагування та відновлення критично важливих елементів.

Отже, для підвищення стійкості критичної інфраструктури ДПСУ необхідне впровадження інтегрованої системи управління ризиками, яка охоплюватиме моніторинг загроз, підготовку особового складу, оновлення нормативної бази та застосування сучасних підходів у сфері захисту ОКІ.

Висновки

У ході проведеного дослідження встановлено, що питання аналізу ризиків у сфері захисту критичної інфраструктури ДПСУ є недостатньо розробленим у науковому середовищі, попри його особливу актуальність. Проведене дослідження підтвердило, що критична інфраструктура ДПСУ є

системоутворюючим елементом, від стійкості та захищеності якої залежить ефективність охорони та захисту ДК.

Ідентифіковано основні категорії загроз і ризиків, що мають комплексний характер і охоплюють воєнно-політичні, диверсійні, терористичні, техногенні, кібернетичні, інформаційні, соціально-економічні та організаційні фактори.

Найбільш критичний вплив мають воєнно-політичні, терористичні, диверсійні, техногенні та експлуатаційні ризики, реалізація яких може спричинити системне порушення функціонування ДПСУ. У межах дослідження уточнено сутність понять «загроза» та «ризик» як базових елементів системи управління безпекою критичної інфраструктури.

Запропонована класифікація загроз і матриця ризиків у подальшому дозволяють здійснювати системне оцінювання категорії критичності об'єктів та визначати пріоритети їхнього захисту залежно від важливості для функціонування відомства та держави в цілому.

Результати аналізу підтверджують необхідність створення інтегрованої системи управління ризиками в ДПСУ, яка б передбачала безперервний моніторинг, оцінювання, попередження та мінімізацію наслідків реалізації загроз. Практичне впровадження результатів дослідження сприятиме підвищенню стійкості критичної інфраструктури ДПСУ та системи інтегрованого управління державним кордоном України як у повсякденнях умовах, так і в умовах особливих правових режимів.

Перелік джерел посилання

1. Гора І. В., Батюк О. В. Окремі питання захисту об'єктів критичної інфраструктури: зарубіжний досвід. *Соціально-правові студії.* 2021. С. 132–139. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3709/1/18-.pdf (дата звернення: 21.06.2025).
2. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. К.: НІСД, 2016.176 с. URL: https://niss.gov.ua/sites/default/files/2014-11/1125_zelknuga.pdf (дата звернення: 24.06.2025).
3. Бірюков Д. С., Кондратов С. І. Стратегія захисту критичної інфраструктури в системі національної безпеки держави. *Стратегічні пріоритети*. 2012. Вип. 3. С. 107–113. URL: https://www.researchgate.net/publication/301698438_Strategy_of_Critical_Infrastructure_Protection_within_National_Security_System_of_the_State (дата звернення: 21.06.2025).
4. Уряднікова І. В., Заплатинський В. М. Наукові підходи до визначення терміну «критична інфраструктура». *Вісті Донецького гірничого інституту.* 2020. № 2 (47). DOI: https://doi.org/10.31474/1999-981X-2020-2-184-193.
5. Франчук В. І., Пригунов П. Я., Мельник С. І. Безпека об'єктів критичної інфраструктури в Україні: організаційно-нормативні проблеми та підходи. *Соціально-правові студії.* 2021. Вип. 3 (13). С. 142–148. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3984/1/19.pdf (дата звернення: 25.06.2025).
6. Гаврись А. П., Філіппова В. В., Тур Н. Ю. Інформаційний аналіз систем захисту об'єктів критичної інфраструктури в період дії воєнного стану. *Вісник ЛДУБЖД,* 2024. №30. С. 173 – 187. DOI: https://doi.org/10.32447/20784643.30.2024.17.
7. Верголяс О. О. Реформування системи захисту та підвищення стійкості критичної інфраструктури Україні в розрізі актуальних загроз. 2020. URL: https://coolyanews.info/reformuvannya-sistemi-zahistu-ta-piidvischennya-stiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-v-rozriizii-aktual.html (дата звернення: 10.10.2025).
8. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети. Серія: Економіка.* 2015. № 4. С. 83–93.
9. Єрменчук О. П. Оцінка загроз критичній інфраструктурі як важлива складова частини діяльності із захисту державної безпеки. *Національний юридичний журнал: теорія і практика*. 2018. С. 50-54. URL: https://ibn.idsi.md/ sites/default/files/imag_file/50-54_4.pdf (дата звернення: 30.10.2025).
10. 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.
11. Мурасов, Р., Нікітін А., Мещеряков І., Підгородецький М., Поплавець С. Методика оцінювання загроз і ризиків для об'єктів критичної інфраструктури за сценаріями розвитку надзвичайних ситуацій.

Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 48(3).С. 35–43. DOI: https://doi.org/10.33099/2311-7249/2023-48-3-35-43.

12. Іванюта, С. П., Панов, Є. М., Іваненко, О. І., Гапон, С. В. Оцінка ризиків критичній інфраструктурі України в умовах російської військової агресії . *Вісник НТУУ "КПІ імені Ігоря Сікорського". Серія: Хімічна інженерія, екологія та ресурсозбереження.* 2024. №(2). С. 47–61. DOI: https://doi.org/10.20535/2617-9741.2.2024.307360.

13. Залож В. В., Торічний В. О., Глуздань О. П. Аналіз ризиків у сфері захисту критичної інфраструктури Державної прикордонної служби України в умовах воєнного стану. *Національні інтереси України: науково-практичний журнал.* 2025. № 8(13) С. 130-141. DOI: https://doi.org/10.52058/3041-1793-2025-8(13)-130-141.

14. Залож В. В., Торічний В. О., Глуздань О. П., Антох О. В. Модель оцінювання ризиків у сфері критичної інфраструктури Державної прикордонної служби України в умовах воєнного стану. *Національні інтереси України: науково-практичний журнал.* 2025. № 9(14) С. 176-193. DOI: https://doi.org/10.52058/3041-1793-2025-9(14)-176-193.

15. Герасименко О. М. Загрози об'єктам критичної інфраструктури України в умовах воєнного стану. *Науковий вісник Ужгородського національного університету: серія Право.* 2024. № 3(84). С. 257-263. DOI: https://doi.org/10.24144/2307-3322.2024.84.3.39.

16. Торічний В. О., Залож В. В., Шашкун І. В. Аналіз та класифікація об'єктів критичної інфраструктури Державної прикордонної служби України. *Національні інтереси України: науково-практичний журнал.* 2025. № 11(16) С. 510-520. DOI: https://doi.org/10.52058/3041-1793-2025-11(16)-510-520.

17. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: Розпорядження Кабінету Міністрів України № 1009-р від 06 грудня 2017 р. ВРУ. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text (дата звернення: 27.06.2025).

18. Про критичну інфраструктуру: Закон України № 1882-IX від 16 листопада 2021 року. ВРУ. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 05.06.2025).

Стаття надійшла до редакції 17.11.2025 р.

UDC 351.746:351.861:005.334(477)

V. Torichnyi, V. Zalozh, I. Shashkun

ANALYSIS OF THREATS AND RISKS TO CRITICAL INFRASTRUCTURE FACILITIES OF THE STATE BORDER SERVICE OF UKRAINE

The article provides a systematic analysis of threats and risks affecting critical infrastructure facilities of the State Border Guard Service of Ukraine. It substantiates the relevance of ensuring the stability of critically important facilities of the border agency in everyday conditions and under special legal regimes, on which border security, the state's defense capability, and the stability of management, communication, logistics, and life support systems directly depend. It is shown that modern threats to critical infrastructure facilities of the State Border Service of Ukraine are complex and multidimensional in nature and include military, terrorist, man-made, cybernetic, information-psychological, and socio-economic factors.

Scientific sources on critical infrastructure security issues have been analyzed, and an insufficient level of complexity in approaches to risk assessment in the border area has been identified. It is emphasized that there is a need to develop a holistic approach to the analysis of threats and risks to critical infrastructure facilities of the State Border Service of Ukraine, which would combine aspects of everyday activities and functioning under special legal regimes.

The study clarifies the essence of the concepts of "threat" and "risk" as basic elements of the critical infrastructure security management system. The author proposes a classification of threats to critical infrastructure facilities of the State Border Guard Service of Ukraine. For each category, typical scenarios of their implementation and the nature of their impact are identified. The classification is based on the principles of systematicity, comprehensiveness, adaptability, and practicality, and takes into account international experience in critical infrastructure protection.

A generalized risk matrix for critical infrastructure facilities of the State Border Guard Service of Ukraine has been developed, which systematizes typical risk categories by facility and determines their criticality levels. Analysis of the matrix revealed the dominance of military-political, terrorist, sabotage, cyber, and operational risks, the realization of which could lead to a violation of the organizational stability of the management system and a decrease in the effectiveness of operational and service activities.

The results obtained make it possible to determine the priorities for protecting critical infrastructure facilities, optimize the allocation of resources, and form the basis for building an integrated risk management system in the State Border Service of Ukraine. The proposed approach provides the opportunity to identify vulnerable elements in a timely manner, predict threats, and develop preventive and compensatory measures. The practical implementation of the research results will be an important factor in increasing the resilience of the critical infrastructure of the border agency, ensuring its continuous and effective functioning both in everyday conditions and under special legal regimes.

Keywords: *State Border Service of Ukraine, state border, border security, organizational resilience, critical infrastructure, facility protection, threats, risks, analysis, classification, risk management.*

Торічний Вадим Олександрович – доктор наук з державного управління, доцент, професор кафедри управління, Національна академія Державної прикордонної служби України імені Богдана Хмельницького

https://orcid.org/0000-0003-3336-6386

Залож Віктор Вікторович – кандидат військових наук, доцент, заслужений працівник освіти України, доцент кафедри управління, Національна академія Державної прикордонної служби України імені Богдана Хмельницького

https://orcid.org/0000-0001-8974-8661

Шашкун Ірина Володимирівна – ад'юнкт, Національна академія Державної прикордонної служби України імені Богдана Хмельницького

https://orcid.org/0009-0002-5355-5248