

УДК 351.78:005.51:004.056

В. І. Яшук, к.е.н., доцент

О. І. Полотай, к.т.н., доцент

В. С. Балацька, доктор філософії, ст. викладач

^{1,2,3}Львівський державний університет безпеки життєдіяльності¹valentina.lender@gmail.com²orest.polotaj@gmail.com³v.balatska@ldubgd.edu.ua

ПРОЄКТУВАННЯ СИСТЕМ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

У статті обґрунтовано теоретико-методичні засади проєктування комплексних систем безпеки об'єктів критичної інфраструктури України на основі системного та ризик-орієнтованого підходів. Уточнено сутність системи безпеки та взаємозв'язок понять безпеки, захисту, охорони і стійкості. Проаналізовано нормативно-правові засади, систематизовано основні групи загроз і визначено їх вплив на критичні функції та активи. Запропоновано структуру комплексної системи безпеки, що інтегрує організаційні, режимні, фізичні, інженерно-технічні, інформаційні та кібербезпекові заходи. Визначено критерії ефективності та обґрунтовано необхідність безперервного вдосконалення системи з урахуванням залишкових ризиків.

Ключові слова: об'єкти критичної інфраструктури, проєктування систем безпеки, захист критичної інфраструктури, кібербезпека, ризик-орієнтований підхід, комплексна система захисту.

DOI: 10.31474/1996-1588-2026-2-43-173-186

Вступ

Сучасні трансформаційні процеси, цифровізація економіки, зростання технологічної взаємозалежності та ускладнення характеру безпекового середовища зумовлюють підвищення ролі критичної інфраструктури у забезпеченні функціонування держави, економіки та суспільства. Енергетика, транспорт, зв'язок та електронні комунікації, охорона здоров'я, фінансовий сектор, системи життєзабезпечення та інші критично важливі сфери забезпечують виконання життєво важливих функцій та надання послуг, порушення яких може спричинити суттєві негативні наслідки для національної безпеки, економічної стабільності та життєдіяльності населення.

Відповідно до Закону України «Про критичну інфраструктуру» [1], критична інфраструктура охоплює активи, об'єкти, конструкції або системи, матеріальні та нематеріальні, функціонування яких має вирішальне значення для життєвих інтересів держави та забезпечення життєво важливих функцій і послуг суспільству. При цьому безпека критичної інфраструктури визначається як стан її захищеності, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість [2].

Особливої актуальності зазначена проблематика набуває в умовах воєнних,

терористичних, техногенних, природних та кібернетичних загроз, а також можливості їх комплексного та взаємопов'язаного впливу. Цифровізація критичної інфраструктури, інтеграція інформаційно-комунікаційних технологій з автоматизованими системами управління технологічними процесами, використання віддаленого доступу та взаємодія з численними зовнішніми інформаційними ресурсами формують нові вразливості, які можуть бути використані для порушення штатного режиму функціонування об'єкта. Водночас сучасний характер загроз потребує відходу від фрагментарного розуміння безпеки, за якого фізична охорона, інженерний захист, кібербезпека, захист інформації та організаційні заходи розглядаються ізольовано. Законодавче визначення захисту критичної інфраструктури охоплює діяльність, що здійснюється до або під час створення, функціонування, відновлення та реорганізації об'єкта і спрямована на своєчасне виявлення, запобігання та нейтралізацію загроз, а також мінімізацію і ліквідацію наслідків їх реалізації [3].

З огляду на це проєктування системи безпеки об'єкта критичної інфраструктури доцільно розглядати як комплексний, системний і ризик-орієнтований процес, результатом якого має бути формування сукупності взаємопов'язаних організаційних, режимних, інженерних, інженерно-технічних, інформаційних та

кібербезпекових заходів, спрямованих на забезпечення належного рівня захищеності та стійкості об'єкта. Нормативно-правове регулювання зазначених процесів в Україні формується насамперед на основі Закону України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX [1], а також комплексу підзаконних нормативно-правових актів, які регламентують ідентифікацію та категоризацію об'єктів, їх паспортизацію, моніторинг рівня безпеки, оцінювання стану захищеності та управління ризиками.

Важливе місце в цій системі займає Постанова Кабінету Міністрів України від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури», якою визначено відповідні механізми ідентифікації та категоризації об'єктів критичної інфраструктури [4]. Окремим напрямом є паспортизація об'єктів критичної інфраструктури (ОКІ). Паспорт безпеки законодавчо визначений як документ установленної форми, що містить відомості про об'єкт та комплекс заходів, які вживаються для його захисту від визначених загроз. При цьому інформація, що міститься в паспорті безпеки, належить до інформації з обмеженим доступом [5].

Таким чином, наукова проблема полягає у формуванні цілісного підходу до проектування систем безпеки об'єктів критичної інфраструктури, який забезпечував би узгоджене врахування характеру об'єкта, його критичних функцій, категорії критичності, актуальних і потенційних загроз, вразливостей, можливих наслідків їх реалізації та необхідних заходів захисту. Практична значущість проблеми визначається необхідністю підвищення спроможності операторів критичної інфраструктури забезпечувати безперервність функціонування об'єктів, своєчасно виявляти та нейтралізувати загрози, мінімізувати наслідки інцидентів і забезпечувати відновлення критичних функцій. Отже, проектування систем безпеки має розглядатися не як одноразове технічне завдання зі створення комплексу засобів охорони, а як безперервний процес управління безпекою та стійкістю критичної інфраструктури, який повинен враховувати зміни профілю загроз, технологічного середовища та умов функціонування об'єкта.

Проблематика забезпечення безпеки та стійкості критичної інфраструктури є предметом досліджень вітчизняних і зарубіжних науковців [6-18], міжнародних організацій та професійних інституцій [19]. Основними напрямками сучасних досліджень є управління ризиками, кібербезпека, захист інформаційних систем, безпека промислових систем управління, фізична безпека, реагування на інциденти та забезпечення

безперервності функціонування критичних об'єктів.

В українському нормативному та науково-практичному дискурсі базовою категорією виступає не лише захищеність окремого активу, а здатність критичної інфраструктури виконувати життєво важливі функції та забезпечувати відповідні послуги [1-3]. Такий підхід принципово змінює завдання проектування систем безпеки: об'єктом захисту стають не тільки матеріальні та інформаційні активи, а й критичні функції, процеси та послуги. Закон України «Про критичну інфраструктуру» [1] закріплює поняття стійкості критичної інфраструктури як стану, за якого забезпечується спроможність функціонувати у штатному режимі, адаптуватися до умов, що змінюються, протистояти загрозам та швидко відновлюватися після їх впливу. Такий підхід створює нормативне підґрунтя для переходу від традиційної концепції «захисту від загроз» до ширшої концепції стійкості, що включає підготовку до загроз, протидію їм, реагування та відновлення.

Суттєве значення для розвитку методології проектування має нормативне закріплення поняття проектної загрози об'єкту критичної інфраструктури. Закон [1] визначає її як документ установленної форми, що визначає властивості та характеристики реальних і потенційних загроз, на зниження ймовірності реалізації яких має бути спрямовано функціонування системи захисту критичної інфраструктури. Це положення є принципово важливим для проектування, оскільки пов'язує характеристики загроз безпосередньо з вимогами до системи захисту. Важливим напрямом сучасного нормативного розвитку є також перехід до ризик-орієнтованого управління безпекою. Для об'єктів критичної інфраструктури I категорії критичності відповідні вимоги щодо управління ризиками безпеки визначені Постановою Кабінету Міністрів України від 01.04.2025 № 367 [20]. Зазначений акт слід розглядати як важливий елемент сучасної української нормативної бази, однак його положення не варто механічно поширювати на всі об'єкти критичної інфраструктури незалежно від їх категорії.

Питання оцінювання стану безпеки також отримали розвиток у нормативній базі України. Зокрема, окремо врегульовано моніторинг рівня безпеки об'єктів критичної інфраструктури, а також методичні підходи до оцінювання їх захищеності [21, 22]. Це формує передумови для переходу від статичного встановлення наявності певних засобів захисту до оцінювання фактичної спроможності системи протистояти визначеним загрозам. У частині кібербезпеки дослідження спираються на положення українського законодавства у сфері кібербезпеки та захисту

інформації. Водночас міжнародні підходи, зокрема NIST Cybersecurity Framework, документи ENISA [19] та положення міжнародних стандартів управління ризиками, доцільно використовувати як додаткове науково-методичне підґрунтя.

Аналіз сучасних підходів свідчить, що значний масив наукових праць присвячено окремим складовим безпеки критичної інфраструктури: кіберзахисту, захисту інформаційних систем, промислових систем управління, фізичній безпеці, управлінню ризиками та забезпеченню безперервності діяльності [10-18]. Така спеціалізація є закономірною та сприяє розвитку окремих напрямів, однак одночасно актуалізує проблему інтеграції результатів зазначених досліджень у єдину модель проектування системи безпеки конкретного об'єкта.

Недостатньо дослідженим залишається питання визначення взаємозв'язків між критичними функціями об'єкта, його активами, потенційними загрозами, вразливостями та комплексом заходів захисту. Особливої актуальності це набуває для об'єктів, у яких фізичні процеси тісно пов'язані з інформаційними системами та автоматизованими системами управління технологічними процесами. Окремою невирішеною проблемою є забезпечення узгодженості між фізичною охороною, інженерно-технічним захистом, кібербезпекою, організаційними заходами та механізмами реагування. Законодавство України прямо розмежовує поняття охорони, захисту інформації та кіберзахисту, що необхідно враховувати під час формування комплексної архітектури системи безпеки. Зокрема, законодавче визначення охорони об'єктів критичної інфраструктури охоплює режимні, інженерні та інженерно-технічні заходи [1], тоді як заходи із захисту інформації та кіберзахисту становлять окремий напрям.

Таким чином, невирішеною частиною загальної проблеми залишається формування інтегрованої методології проектування систем безпеки, яка одночасно відповідала б вимогам українського законодавства, враховувала категорію критичності та специфіку конкретного об'єкта, базувалася на аналізі актуальних загроз і ризиків та забезпечувала взаємопов'язане функціонування фізичних, інженерно-технічних, інформаційних, кібернетичних і організаційних заходів.

Метою статті є обґрунтування теоретико-методичних засад проектування комплексних систем безпеки об'єктів критичної інфраструктури України на основі системного та ризик-орієнтованого підходів з урахуванням вимог чинної нормативно-правової бази, категорії критичності об'єкта, характеру актуальних загроз

та необхідності забезпечення його стійкості. Для досягнення поставленої мети поставлено та вирішено такі **завдання**:

- проаналізувати нормативно-правові засади проектування та функціонування систем безпеки об'єктів критичної інфраструктури, визначити роль законодавчих і підзаконних актів у формуванні вимог до їх захисту;

- обґрунтувати доцільність застосування ризик-орієнтованого підходу під час проектування систем безпеки з урахуванням ідентифікації загроз, аналізу вразливостей, оцінювання ймовірності та наслідків реалізації ризиків і визначення заходів їх оброблення;

- сформувати структуру комплексної системи безпеки об'єкта критичної інфраструктури, що забезпечує взаємодію організаційних, режимних, фізичних, інженерно-технічних, інформаційних та кібербезпекових заходів;

- обґрунтувати необхідність безперервного вдосконалення системи безпеки на основі результатів моніторингу, оцінювання стану захищеності, аналізу інцидентів, зміни профілю загроз та оцінювання залишкових ризиків.

Розв'язання поставлених завдань забезпечуватиме формування цілісного науково-методичного підходу до проектування систем безпеки об'єктів критичної інфраструктури, в якому нормативна відповідність поєднується з ризик-орієнтованим управлінням, технологічною інтеграцією засобів захисту та орієнтацією на забезпечення стійкості критичних функцій. Саме така логіка, на нашу думку, найбільшою мірою відповідає сучасній українській концепції безпеки та стійкості критичної інфраструктури [1].

Виклад основного матеріалу

Проектування систем безпеки об'єктів критичної інфраструктури доцільно розглядати як комплексний процес, результатом якого є формування узгодженої системи організаційних, правових, режимних, інженерних, інженерно-технічних, інформаційних та кібербезпекових заходів, спрямованих на забезпечення безпеки, стійкості та безперервності функціонування об'єкта [1]. Такий підхід відповідає сучасній українській моделі захисту критичної інфраструктури, в якій безпека пов'язується не лише з недопущенням протиправних дій або кібератак, а передусім із забезпеченням функціональності, безперервності роботи, відновлюваності, цілісності та стійкості об'єкта.

Вихідною позицією під час проектування системи безпеки має бути ідентифікація самого об'єкта критичної інфраструктури, визначення його критичних функцій та критичних елементів. Відповідно до чинного законодавства України,

ідентифікація об'єкта критичної інфраструктури являє собою процедуру віднесення об'єкта інфраструктури до об'єктів критичної інфраструктури [1]. Водночас критичними елементами визнаються технічні засоби, споруди, системи або їх сукупність, порушення функціонування яких може призвести до унеможливлення виконання життєво важливих функцій та/або надання послуг об'єктом.

Отже, першою стадією проектування системи безпеки повинно бути не визначення переліку технічних засобів охорони, а структурно-функціональний аналіз об'єкта. Його сутність полягає у встановленні критичних функцій, визначенні ресурсів, технологічних процесів, інформаційних систем, персоналу та інженерної інфраструктури, необхідних для їх виконання, а також встановленні взаємозалежностей між окремими компонентами. Зазначений підхід дозволяє перейти від традиційної моделі «захисту об'єкта» до моделі забезпечення стійкості критичних функцій. У цьому випадку критерієм ефективності системи безпеки є не кількість встановлених камер відеоспостереження, засобів контролю доступу, міжмережевих екранів або інших технічних засобів, а спроможність об'єкта продовжувати виконувати критичні функції за умов реалізації визначених загроз, мінімізувати негативні наслідки та відновлювати нормальний режим роботи.

Наступним етапом є ідентифікація та оцінювання загроз і ризиків безпеки. У цьому контексті ризик має розглядатися не абстрактно, а у взаємозв'язку з конкретною критичною функцією, активами, вразливостями та потенційними наслідками. Особливого значення для сучасної української практики набуває постанова Кабінету Міністрів України від 01.04.2025 № 367, якою затверджено вимоги щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності [20]. Документ визначає ризик безпеки як можливість виникнення інциденту або порушення стану захищеності, що створює загрозу

функціональності, безперервності роботи, відновлюваності, цілісності та стійкості об'єкта. Це дозволяє сформулювати принципову тезу про те, що ризик у системі безпеки критичної інфраструктури повинен оцінюватися через його потенційний вплив на здатність об'єкта виконувати життєво важливі функції, а не лише через можливість компрометації окремого інформаційного чи матеріального активу. З урахуванням цього пропонується така послідовність проектування систем безпеки об'єктів критичної інфраструктури (рис. 1). Застосування запропонованої послідовності забезпечує логічний зв'язок між характеристиками об'єкта та необхідними заходами захисту.

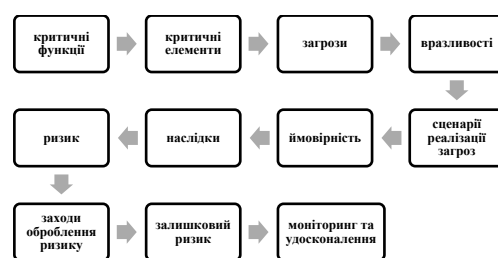


Рисунок 1 – Послідовність процесу проектування систем безпеки об'єктів критичної інфраструктури

На етапі ідентифікації загроз доцільно враховувати не лише окремі види небезпек, а сценарії комплексного впливу. Для сучасних умов характерним є поєднання фізичних атак, диверсій, порушень постачання ресурсів, техногенних аварій, кібератак, атак на інформаційні системи, компрометації облікових даних, соціальної інженерії та людського фактора. Відповідно, модель загроз повинна враховувати щонайменше групи, наведені в табл. 1. Таким чином, система безпеки повинна проектуватися не під окрему загрозу, а під сукупність сценаріїв порушення критичних функцій.

Таблиця 1 – Групи загроз при побудові моделі систем безпеки об'єктів критичної інфраструктури

№ з/п	Група загроз	Опис
1	Фізичні загрози	несанкціоноване проникнення, пошкодження або знищення обладнання, диверсійні дії;
2	Техногенні та природні загрози	пожежі, аварії, стихійні явища, порушення електропостачання та інших інженерних комунікацій;
3	Кібернетичні загрози	несанкціонований доступ, шкідливе програмне забезпечення, атаки на мережеву інфраструктуру та автоматизовані системи управління;
4	Інформаційні загрози	порушення конфіденційності, цілісності або доступності інформації;
5	Організаційні загрози	недоліки управління, порушення процедур, недостатній контроль доступу;
6	Кадрові та людські загрози	помилки персоналу, зловживання повноваженнями, соціальна інженерія;
7	Комбіновані загрози	за яких одночасно реалізуються декілька зазначених сценаріїв.

Наведена класифікація має функціональний характер і використовується не для взаємовиключного розподілу загроз, а для їх структуризації під час формування моделі загроз. Одна подія може одночасно належати до декількох груп, що особливо характерно для комбінованих сценаріїв.

Науковим результатом дослідження є обґрунтування доцільності формування багаторівневої архітектури системи безпеки, в якій окремі компоненти не дублюють один одного, а створюють взаємопов'язану систему протидії загрозам (рис. 2).

Перший рівень	• фізична та режимна безпека
Другий рівень	• інженерно-технічний захист
Третій рівень	• інформаційна та кібернетична безпека
Четвертий рівень	• організаційно-управлінський

Рисунок 2 – Багаторівнева архітектура системи безпеки об'єктів критичної інфраструктури

Перший рівень становить фізична та режимна безпека. Вона охоплює організацію контрольно-пропускного режиму, контроль доступу, охорону території, відеоспостереження, охоронну сигналізацію, фізичне розмежування зон та інші заходи. Водночас українське законодавство чітко розмежовує охорону та інші складові захисту. Закон України «Про критичну інфраструктуру» [1] визначає охорону як комплекс режимних, інженерних, інженерно-технічних та інших заходів, спрямованих на запобігання, недопущення або припинення протиправних дій на об'єктах критичної інфраструктури. При цьому заходи із захисту інформації та кіберзахисту виокремлюються законодавством окремо. Другий рівень становить інженерно-технічний захист, який включає забезпечення фізичної стійкості об'єкта, резервування критичних систем, аварійне електроживлення, системи пожежної безпеки, інженерні бар'єри та інші заходи залежно від специфіки об'єкта.

Третій рівень – інформаційна та кібернетична безпека. Він передбачає захист інформаційних та інформаційно-комунікаційних систем, сегментацію мереж, контроль привілейованого та віддаленого доступу, автентифікацію, моніторинг подій безпеки, резервування та відновлення даних, а для відповідних об'єктів – захист автоматизованих систем управління технологічними процесами.

Четвертий рівень – організаційно-управлінський. Він включає політики безпеки, розподіл відповідальності, підготовку персоналу, процедури реагування, кризове управління, планування безперервності діяльності та відновлення.

Таким чином, запропонована структура дозволяє реалізувати принцип глибокоєшелюнованого захисту, за якого компрометація одного рівня не повинна автоматично призводити до порушення критичної функції.

Особливе значення у вітчизняній системі захисту критичної інфраструктури має паспорт безпеки об'єкта критичної інфраструктури. Закон визначає його як документ установленної форми, що містить відомості про об'єкт та комплекс заходів, які вживаються для його захисту від визначених видів загроз [1]. Порядок паспортизації визначено постановою Кабінету Міністрів України від 04.08.2023 № 818 [5]. Чинна редакція постанови станом на 2026 рік передбачає, зокрема, використання таких категорій, як критичні елементи об'єкта та план захисту об'єкта критичної інфраструктури. План захисту визначається як документ, що передбачає заходи із забезпечення безпеки та протидії проєкtnим загрозам відповідно до режимів функціонування об'єкта. Отже, паспорт безпеки та план захисту доцільно розглядати не лише як адміністративно-документальні вимоги, а як інструменти формалізації результатів проєктування системи безпеки. Логіка їх взаємозв'язку може бути представлена на рис. 3. Це дозволяє забезпечити циклічність процесу та уникнути ситуації, за якої система безпеки формується один раз і надалі не адаптується до зміни загроз.



Рисунок 3 – Взаємозв'язок інструментів формалізації результатів проєктування системи безпеки об'єктів критичної інфраструктури

Важливим елементом запропонованої моделі є постійний моніторинг ефективності системи безпеки. Постанова Кабінету Міністрів України № 821 від 22.07.2022 регламентує проведення моніторингу рівня безпеки об'єктів критичної інфраструктури [21]. Подальший розвиток цього підходу відображено в наказі Адміністрації Держспецзв'язку від 14.01.2025 № 17, яким затверджено методику та критерії і показники оцінки стану захищеності об'єктів критичної інфраструктури [22]. Методика передбачає врахування, зокрема, інформації з щорічного звіту оператора, паспорта безпеки,

плану захисту та відповідних секторальних вимог. Це дає підстави запропонувати розглядати оцінювання системи безпеки як замкнений цикл управління (рис. 4). Такий підхід забезпечує принцип безперервного вдосконалення та дозволяє враховувати зміни технологічного середовища, структури критичних активів, нормативних вимог і профілю загроз. На основі проведеного дослідження пропонується розглядати систему проєктування безпеки об'єкта критичної інфраструктури як багаторівневу функціонально-ризик-орієнтовану модель, що складається з шести взаємопов'язаних етапів, наведених в табл. 2.



Рисунок 4 – Процес оцінювання системи безпеки об'єктів критичної інфраструктури

Таблиця 2 – Етапи проєктування системи безпеки об'єкта критичної інфраструктури

№ з/п	Етап	Зміст	Результат
1	Ідентифікація	Визначення об'єкта, його функцій, активів та критичних елементів	Модель об'єкта
2	Аналіз загроз	Виявлення природних, техногенних, фізичних, кібернетичних, інформаційних та комбінованих загроз	Модель загроз
3	Оцінювання ризиків	Аналіз вразливостей, імовірності та наслідків реалізації загроз	Профіль ризиків
4	Проектування заходів захисту	Формування фізичних, інженерних, інформаційних, кібернетичних та організаційних заходів	Архітектура системи безпеки
5	Реалізація та документування	Формування плану захисту, паспорта безпеки, процедур реагування та відновлення	Комплекс організаційно-технічної документації
6	Моніторинг та удосконалення	Контроль стану захищеності, аналіз інцидентів, переоцінювання ризиків	Актуалізована система безпеки

Запропонована модель відрізняється від фрагментарного підходу тим, що кожен технічний або організаційний захід пов'язується з конкретною загрозою, вразливістю, критичним елементом та ризиком. Це дозволяє обґрунтовувати доцільність витрат на безпеку не формальним переліком засобів захисту, а їх внеском у зниження ризику та забезпечення стійкості критичної функції. При цьому постанова № 367 має застосовуватися з урахуванням її предметної сфери – об'єктів критичної інфраструктури I категорії критичності [20]. Для інших категорій об'єктів відповідні процедури

повинні визначатися з урахуванням загальних вимог законодавств, галузевих нормативних актів та специфіки конкретного об'єкта. Наведений опис доцільно формалізувати як багаторівневу функціонально-ризик-орієнтовану математичну модель проєктування системи безпеки об'єкта критичної інфраструктури (ОКІ). Її принципова особливість полягає в тому, що проєктування заходів захисту здійснюється не як формування фіксованого набору засобів безпеки, а як задача оптимального вибору комплексу взаємопов'язаних заходів, спрямованих на зниження ризику порушення критичних функцій ОКІ та підвищення

його стійкості. Формалізуємо запропонований підхід у вигляді математичної моделі проектування системи безпеки об'єкта критичної інфраструктури. (ОКІ). Нехай об'єкт критичної інфраструктури описується:

– множиною критичних функцій:

$$F = \{f_1, f_2, \dots, f_m\};$$

– множиною активів та критичних елементів:

$$A = \{a_1, a_2, \dots, a_n\};$$

– множиною потенційних загроз:

$$T = \{t_1, t_2, \dots, t_p\};$$

– множиною вразливостей:

$$V = \{v_1, v_2, \dots, v_q\};$$

а множина можливих заходів захисту визначається як $M = \{m_1, m_2, \dots, m_s\}$.

При цьому загрози (T) доцільно поділяти на природні, техногенні, фізичні, кібернетичні, інформаційні та комбіновані, а заходи (M) – на фізичні, інженерно-технічні, інформаційні, кібернетичні та організаційні. Зв'язок між критичними функціями, активами, загрозами, вразливостями та заходами захисту можна представити орієнтованою структурою:

$$F \rightarrow A \rightarrow (T, V) \rightarrow R \rightarrow M \rightarrow R^{res},$$

де R – початковий ризик, а R^{res} – залишковий ризик після впровадження заходів захисту.

Опишемо етап ідентифікації. На першому етапі формується модель ОКІ:

$$O = (F, A, C, D),$$

де F – множина критичних функцій;

A – множина активів та елементів інфраструктури;

C – множина взаємозв'язків і залежностей між елементами;

D – множина параметрів критичності.

Для кожного критичного елемента (a_j) визначається коефіцієнт критичності: $c_j \in [0, 1]$. Чим більше значення c_j , тим вищим є вплив порушення функціонування відповідного елемента на здатність ОКІ виконувати критичну функцію. Для критичної функції f_i можна визначити агрегований показник критичності:

$$C_i = \sum_{j=1}^n a_{ij} c_j,$$

де a_{ij} – коефіцієнт залежності функції (f_i) від активу (a_j), причому

$$\sum_{j=1}^n a_{ij} = 1.$$

Таким чином, уже на першому етапі модель враховує не лише перелік активів, а їх

функціональну значущість для забезпечення критичних процесів.

Формалізація моделі загроз. Для кожної пари «актив – загроза» визначається можливість реалізації загрози з урахуванням відповідної вразливості.

Позначимо:

$$P_{kj} = P(t_k | a_j, v_j),$$

де P_{kj} – ймовірність реалізації загрози t_k щодо активу a_j , за наявності відповідної вразливості. Водночас доцільно враховувати не лише ймовірність виникнення загрози, а й рівень експлуатаційної доступності вразливості:

$$P_{kj} = P(t_k) E_{kj} V_{kj},$$

де $P(t_k)$ – базова ймовірність реалізації загрози;

E_{kj} – коефіцієнт експлуатованості вразливості;

V_{kj} – коефіцієнт уразливості активу.

Для кібернетичних загроз цей компонент може враховувати, зокрема, наявність експлойта, факти активної експлуатації, рівень технічної вразливості та доступність відповідних засобів атаки.

Модель ризику. Базовий ризик порушення функціонування активу a_j внаслідок загрози t_k визначимо як

$$R_{kj} = P_{kj} I_{kj},$$

де I_{kj} – величина потенційних наслідків реалізації загрози. Оскільки для ОКІ наслідки можуть мати різну природу, пропонуємо представити їх як багатокомпонентний показник:

$$I_{kj} = \omega_1 I_{kj}^s + \omega_2 I_{kj}^e + \omega_3 I_{kj}^f + \omega_4 I_{kj}^i + \omega_5 I_{kj}^{ec},$$

де

I^s – вплив на безпеку та життя людей;

I^e – екологічні наслідки;

I^f – функціональні наслідки;

I^i – інформаційні наслідки;

I^{ec} – економічні наслідки;

ω_1 – вагові коефіцієнти відповідних видів наслідків, при цьому:

$$\sum_{r=1}^5 \omega_r = 1.$$

З урахуванням критичності активу загальний ризик до впровадження заходів захисту може бути визначений як:

$$R_o = \sum_{j=1}^n \sum_{k=1}^p c_j P_{kj} I_{kj}.$$

Цей показник характеризує агрегований рівень ризику ОКІ до реалізації проектних рішень із безпеки.

Модель проектування заходів захисту. Нехай $x_l \in [0, 1]$, де $x_l = 1$, якщо захід захисту

m_l включається до проекту системи безпеки, і $x_l = 0$ – якщо захід не обирається.

Кожен захід характеризується:

K_l – вартістю впровадження;

E_{kl} – ефективністю протидії загрози (t_k);

Q_{jl} – здатністю захищати актив (a_j);

S_l – внеском у забезпечення стійкості;

Q_l – організаційними, технічними або нормативними обмеженнями його застосування.

Ефективність комплексу заходів щодо конкретної загрози можна визначити як

$$E_k(X) = 1 - \prod_{l=1}^s (1 - E_{kl}x_l),$$

де $X = x_1, x_2, \dots, x_s$ – вектор проектних рішень.

Така функція дозволяє врахувати комплексний ефект взаємодії декількох заходів: якщо застосовано декілька незалежних або частково незалежних механізмів захисту, загальна ефективність системи зростає, але не перевищує 100 %. Тоді залишкова ймовірність реалізації загрози визначається:

$$P_{kj}^{res} = P_{kj} (1 - E_{kj}(X)).$$

Відповідно, залишковий ризик:

$$P_{kj}^{res} = P_{kj} (1 - E_{kj}(X)) I_{kj}.$$

А загальний залишковий ризик ОКІ:

$$R^{res}(X) = \sum_{j=1}^n \sum_{k=1}^p c_j P_{kj} (1 - E_{kj}(X)) I_{kj}.$$

Саме ця залежність є центральним елементом запропонованої моделі, оскільки дозволяє кількісно пов'язати вибір конкретних заходів захисту зі зміною рівня ризику.

Проектування системи безпеки пропонується розглядати як задачу багатокритеріальної оптимізації.

Основними критеріями є мінімізація залишкового ризику; мінімізація витрат на створення та експлуатацію системи; максимізація стійкості критичних функцій; забезпечення відповідності нормативним вимогам.

Функцію оптимізації можна представити у вигляді:

$$J(X) = \lambda_1 \frac{R^{res}(X)}{R_0} + \lambda_2 \frac{C(X)}{C_{max}} + \lambda_3 \frac{S(X)}{S_{max}} \rightarrow \max,$$

де

$R^{res}(X)$ – залишковий ризик;

$C(X)$ – сукупна вартість системи захисту;

$S(X)$ – рівень стійкості ОКІ;

$\lambda_1, \lambda_2, \lambda_3$ – вагові коефіцієнти;

C_{max}, S_{max} – нормувальні величини.

При цьому:

$$\lambda_1 + \lambda_2 + \lambda_3 = 1.$$

Високе значення λ_1 означає пріоритет зниження ризику, тоді як збільшення λ_2 підвищує

значущість економічної ефективності, а λ_3 – стійкості системи.

6. Обмеження моделі.

Оптимальний набір заходів не може визначатися лише мінімізацією вартості. Він повинен відповідати низці обмежень.

Обмеження допустимого ризику:

$$R^{res}(X) \leq R_{dop},$$

де R_{dop} – максимально допустимий рівень залишкового ризику.

Бюджетне обмеження:

$$\sum_{l=1}^s K_l x_l \leq B,$$

де B – доступний бюджет.

Обов'язкове покриття критичних елементів.

Для кожного критичного активу:

$$\sum_{l=1}^s Q_{jl} x_l \geq Q_j^{min}.$$

Обмеження нормативної відповідності. Для множини обов'язкових заходів M^{req} :

$$x_l = 1, l \in M^{req}.$$

Це означає, що заходи, обов'язковість яких визначається законодавством, нормативними документами або встановленою категорією критичності ОКІ, не можуть бути виключені з оптимального рішення лише з економічних міркувань.

Важливою відмінністю запропонованої моделі від традиційного ризик-орієнтованого підходу є врахування стійкості. Для кожної критичної функції f_i можна визначити показник її стійкості:

$$S = w_a A_i + w_r R_i + w_c C_i + w_{rec} Rec_i,$$

де

A_i – здатність функції протистояти впливу загрози;

R_i – здатність до адаптації;

C_i – здатність підтримувати функціонування під час інциденту;

Rec_i – здатність до відновлення.

Тоді інтегральна стійкість ОКІ:

$$S(X) = \sum_{i=1}^m \beta_j S_j(X),$$

де β_j – ваговий коефіцієнт критичної функції,

$$\sum_{i=1}^m \beta_j = 1.$$

Отже, система безпеки вважається ефективною не лише тоді, коли вона запобігає реалізації загрози, а й тоді, коли у разі реалізації загрози забезпечує підтримання критичної функції, локалізацію наслідків та відновлення функціонування ОКІ.

Динамічна складова моделі. Оскільки система безпеки ОКІ функціонує в умовах

постійної зміни загроз і вразливостей, запропонована модель має бути циклічною.

На момент t ризик визначається як

$$R_t = R(T_t, V_t, A_t, C_t),$$

а після отримання інформації про нові загрози, вразливості та інциденти здійснюється переоцінювання:

$$R_{t+1} = f(R_t, \Delta T, \Delta V, \Delta A, \Delta I),$$

де:

ΔT — зміна множини загроз;

ΔV — зміна множини вразливостей;

ΔA — зміна складу та стану активів;

ΔI — інформація про нові інциденти.

Відповідно, вектор заходів захисту також може змінюватися:

$$X_{t+1} = X_t + \Delta X.$$

Таким чином, шостий етап — моніторинг та удосконалення — не є завершальним у лінійному розумінні. Він забезпечує зворотний зв'язок із першим етапом:

$$I \rightarrow T \rightarrow R \rightarrow M \rightarrow D \rightarrow I',$$

де I — ідентифікація, T — аналіз загроз, R — оцінювання ризику, M — проектування заходів, D — реалізація та документування, I' — актуалізована ідентифікація об'єкта.

Таким чином, математично узагальнену модель проектування системи безпеки ОКІ можна представити як задачу:

$$\min_x J(X) = \lambda_1 \frac{R^{res}(X)}{R_0} + \lambda_2 \frac{C(X)}{C_{max}} + \lambda_3 \frac{S(X)}{S_{max}} \rightarrow \max,$$

$$\text{за умов } R^{res}(X) \leq R_{dop}, \sum_{l=1}^s K_l x_l \leq B,$$

$$\sum_{l=1}^s Q_{jl} x_l \geq Q_j^{min}, j = 1, \dots, n,$$

$$x_l = 1, \quad l \in M^{req}, x_l \in \{0, 1\}.$$

Отже, оптимальним рішенням є такий набір заходів захисту

$$X^* = (x_1^*, x_2^*, \dots, x_s^*),$$

який за встановлених ресурсних та нормативних обмежень забезпечує мінімальний залишковий ризик при одночасному досягненні необхідного рівня стійкості критичних функцій.

Запропонована математична модель дає змогу перейти від фрагментарного переліку засобів захисту до формалізованого процесу прийняття проектних рішень. Її концептуальна відмінність полягає у встановленні причинно-наслідкового зв'язку (рис. 5).

Це дозволяє обґрунтовувати включення кожного організаційного, фізичного, інженерно-технічного, інформаційного або кібернетичного заходу до архітектури системи безпеки через його

вимірюваний внесок у зниження ризику та забезпечення безперервності критичної функції.

Водночас модель має практичну цінність: залежно від категорії критичності ОКІ, типу критичних функцій, характеру актуальних загроз, наявних вразливостей, ресурсних обмежень і нормативних вимог можуть змінюватися параметри $c_j, P_{kj}, I_{kj}, E_{kl}, K_l$ та вагові коефіцієнти λ_i . Це забезпечує адаптивність моделі до конкретного об'єкта критичної інфраструктури.



Рисунок 5 — Формалізація процесу прийняття проектних рішень захисту ОКІ

Висновки та перспективи подальших досліджень. Проведене дослідження дозволило обґрунтувати необхідність переходу від фрагментарного забезпечення окремих напрямів захисту до інтегрованого проектування систем безпеки об'єктів критичної інфраструктури. Визначено, що сучасна система безпеки повинна формуватися з урахуванням не лише характеристик окремих активів, а передусім критичних функцій об'єкта, критичних елементів, взаємозалежностей між його технологічними, інформаційними та інженерними компонентами, а також потенційних наслідків порушення їх функціонування.

Установлено, що нормативно-правове регулювання України створює необхідне підґрунтя для такого підходу. Закон України «Про критичну інфраструктуру» визначає базові поняття та принципи функціонування національної системи захисту критичної інфраструктури, тоді як підзаконні нормативні акти деталізують процедури ідентифікації та категоризації об'єктів, паспортизації, моніторингу рівня безпеки, оцінювання стану захищеності та управління ризиками [2,3]. Обґрунтовано, що ризик-

орієнтований підхід є одним із ключових методологічних принципів проектування систем безпеки, оскільки дозволяє встановити причинно-наслідковий зв'язок між критичними функціями об'єкта, загрозами, вразливостями, можливими сценаріями інцидентів та заходами захисту. При цьому для об'єктів I категорії критичності зазначений підхід отримав безпосереднє нормативне закріплення у вимогах, затверджених постановою Кабінету Міністрів України № 367 від 01.04.2025 [20].

Науковим результатом дослідження є систематизація етапів проектування системи безпеки об'єкта критичної інфраструктури, зокрема, ідентифікація об'єкта та його критичних функцій; визначення критичних елементів; формування моделі загроз; оцінювання ризиків; проектування комплексу заходів захисту; документування; моніторинг та безперервне вдосконалення. Запропоновано розглядати систему безпеки як багаторівневу структуру, що поєднує фізичну та режимну безпеку, інженерно-технічний захист, інформаційну та кібербезпеку, а також організаційно-управлінські заходи. Такий підхід відповідає комплексному характеру сучасних загроз і дозволяє забезпечити взаємне посилення окремих рівнів захисту.

Доведено, що паспорт безпеки та план захисту об'єкта повинні розглядатися не виключно як документи нормативного характеру, а як інструменти формалізації та практичної реалізації результатів проектування системи безпеки. Встановлено також, що ефективність системи безпеки не може визначатися виключно наявністю певного набору технічних засобів. Основним критерієм має виступати здатність об'єкта забезпечувати функціональність, безперервність роботи, відновлюваність, цілісність та стійкість критичних функцій. Саме така орієнтація відповідає законодавчому розумінню безпеки критичної інфраструктури.

Таким чином, запропонований підхід дозволяє сформулювати методологічну основу для проектування систем безпеки, у якій нормативна відповідність, ризик-орієнтоване управління, багаторівневий захист, моніторинг та забезпечення стійкості розглядаються як взаємопов'язані складові єдиного процесу.

Перспективним напрямом подальших досліджень є розроблення кількісної моделі оцінювання ефективності системи безпеки об'єкта критичної інфраструктури, яка дозволила б визначати рівень захищеності та стійкості на основі системи кількісних і якісних показників. Доцільним є також розроблення інтегрованої

моделі оцінювання ризику, яка одночасно враховуватиме критичність функцій, вразливості активів, імовірність реалізації різних типів загроз, масштаб потенційних наслідків, взаємозалежності між критичними елементами та ефективність уже впроваджених заходів захисту. Окремим напрямом є дослідження кіберфізичної безпеки критичної інфраструктури, зокрема взаємозв'язку інформаційних систем, мережевої інфраструктури та автоматизованих систем управління технологічними процесами. Перспективним є формування моделей, які дозволять оцінювати каскадні наслідки реалізації комбінованих фізичних і кібернетичних загроз.

Подальшого розвитку потребує також питання автоматизації моніторингу стану захищеності на основі даних систем відеоспостереження, контролю доступу, SIEM/SOAR, систем моніторингу технологічних процесів та інших джерел інформації. Це створює передумови для переходу від періодичного оцінювання до безперервного моніторингу стану безпеки. У подальших дослідженнях доцільно також розробити методику вибору оптимального комплексу заходів захисту за критерієм «вартість – ризик – ефективність», що дозволить оператору критичної інфраструктури обґрунтовувати пріоритетність інвестицій у безпеку та визначати найбільш критичні напрями підвищення стійкості об'єкта.

Отже, перспективним результатом подальших досліджень має стати формування інтелектуальної ризик-орієнтованої моделі проектування та управління системою безпеки об'єкта критичної інфраструктури, здатної адаптуватися до зміни профілю загроз, автоматично підтримувати актуальність оцінки ризиків та забезпечувати обґрунтоване прийняття управлінських рішень щодо підвищення рівня захищеності і стійкості критичної інфраструктури.

Використання штучного інтелекту та технологій на основі ШІ

У процесі роботи над рукописом використано інструмент штучного інтелекту chatgpt для перевірки граматики та стилістики, а також для швидкого структурування первинних даних із логів тестування додатків. ШІ не залучався до інтерпретації наукових даних, формулювання висновків чи розробки теоретичного підґрунтя дослідження. Автор несе повну відповідальність за остаточний текст статті, отримані результати та їх наукову інтерпретацію.

Література

1. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/1882-20> (дата звернення: 27.08.2026).
2. Термінологія законодавства України [Електронний ресурс] : офіц. вебпортал парламенту України. URL: <https://zakon.rada.gov.ua/laws/term/36366> (дата звернення: 24.08.2026).
3. Критична інфраструктура // Термінологія законодавства : база даних / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/term/1882-20> (дата звернення: 29.08.2026).
4. Деякі питання об'єктів критичної інфраструктури : постанова Кабінету Міністрів України ; Порядок, Перелік, Методика від 09.10.2020 № 1109 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/1109-2020-%D0%BF> (дата звернення: 27.08.2026).
5. Деякі питання паспортизації об'єктів критичної інфраструктури : постанова Кабінету Міністрів України ; Порядок, Форма типового документа, Паспорт від 04.08.2023 № 818 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/818-2023-%D0%BF> (дата звернення: 27.08.2026).
6. Запорожець Т. В. Державна політика у сфері захисту критичної інфраструктури : навч. посіб. Київ : ДКС Центр, 2024. 186 с. ISBN 978-617-8080-12-9.
7. Довгань О. Д., Ткачук Т. Ю. Кіберризика критичної інфраструктури: від аналізу загроз до впровадження рішень : наук.-практ. посіб. Київ ; Одеса : Фенікс, 2024. 70 с. ISBN 978-617-8430-50-4.
8. Когут Ю. І. Кібервійна та безпека об'єктів критичної інфраструктури. 2-ге вид. Київ : Консалтингова компанія «Сідкон», 2024. ISBN 978-617-95100-3-8.
9. Фізичний та кібернетичний захист об'єктів критичної інфраструктури України органами та підрозділами поліції : навч. посіб. Вінниця, 2025.
10. Tekinerdogan B., Aksit M., Catal C., Hurst W., AlSkaif T. (eds.). Management and Engineering of Critical Infrastructures. Amsterdam : Academic Press, 2023. ISBN 978-0-323-99330-2. DOI: <https://doi.org/10.1016/C2021-0-02364-2>.
11. Küfeoğlu S., Akgün A. T. Cyber Resilience in Critical Infrastructure. 1st ed. Boca Raton : CRC Press, 2024. ISBN 978-1-032-58306-8.
12. Raval K. J., Jadav N. K., Rathod T., Tanwar S., Vimal V., Yamsani N. A Survey on Safeguarding Critical Infrastructures: Attacks, AI Security, and Future Directions. *International Journal of Critical Infrastructure Protection*. 2024. Vol. 44. Art. 100647. DOI: <https://doi.org/10.1016/j.ijcip.2023.100647>.
13. Tabansky L., Lichterman E. PROGRESS: The Sectoral Approach to Cyber Resilience. *International Journal of Information Security*. 2025. Vol. 24. Art. 18. DOI: <https://doi.org/10.1007/s10207-024-00910-3>.
14. Wang F., Tian J., Ling J., Chen Z., Xu Z. A Multi-Stage Resilience Analysis Framework of Critical Infrastructure Systems Based on Component Importance Measures. *Reliability Engineering & System Safety*. 2025. Vol. 256. Art. 110720. DOI: <https://doi.org/10.1016/j.res.2024.110720>.
15. Паршина О. А., Метеленко Н. Г., Коваленко В. Л., Паршина М. Ю. Системне забезпечення інформаційної безпеки на об'єктах критичної інфраструктури. *Philosophy, Economics and Law Review*. 2023. Т. 3, № 2. С. 66–80. DOI: <https://doi.org/10.31733/2786-491X-2023-2-66-80>.
16. Юдіна Д. О. Метод розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*. 2025. № 2 (30). С. 473–487. DOI: <https://doi.org/10.28925/2663-4023.2025.30.986>.
17. Гречанінов В. Ф. Інтелектуальна система сценарного моделювання оцінки захищеності об'єктів критичної інфраструктури. *Технічні науки та технології*. 2025. № 3 (41). С. 131–145. DOI: [https://doi.org/10.25140/2411-5363-2025-3\(41\)-131-145](https://doi.org/10.25140/2411-5363-2025-3(41)-131-145).
18. Гречанінов В. Ф. Моделі та технології інтелектуального захисту інформаційних систем критичної інфраструктури для підвищення стійкості. *Кібербезпека: освіта, наука, техніка*. 2025. № 1 (29). С. 877–896. DOI: <https://doi.org/10.28925/2663-4023.2025.29.948>.
19. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg : NIST, 2024. DOI: <https://doi.org/10.6028/NIST.CSWP.29>.
20. Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності : постанова Кабінету Міністрів України ; Вимоги, Форма типового документа, Звіт від 01.04.2025 № 367 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/367-2025-%D0%BF> (дата звернення: 27.08.2026).
21. Про затвердження Порядку моніторингу рівня безпеки об'єктів критичної інфраструктури : постанова Кабінету Міністрів України від 22.07.2022 № 821 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/821-2022-%D0%BF> (дата звернення: 27.08.2026).

22. Про затвердження Методики та критеріїв оцінки стану захищеності об'єктів критичної інфраструктури : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14.01.2025 № 17 // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/> (дата звернення: 27.08.2026).
23. Івануса А., Яшук В., Федина Б. Дослідження процесу оцінювання ризиків кібербезпеки об'єктів критичної інфраструктури. *Інформаційна безпека та інформаційні технології* : збірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 30 листопада 2023 року. Львів : ЛДУ БЖД, 2023. 489 с. С. 84–87.
24. Яшук В., Балацька В. Підвищення кіберстійкості критичної інформаційної інфраструктури держави через вдосконалення процесів реагування на кіберінциденти. *Дивільний захист в умовах війни* : збірник тез доповідей II Міжнародної науково-практичної конференції, м. Львів, 15 квітня 2026 року. Львів : ЛДУБЖД, 2026. С. 92–95.
25. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/2163-19> (дата звернення: 27.08.2026).
26. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80> (дата звернення: 27.08.2026).
27. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури : розпорядження Кабінету Міністрів України ; План від 19.09.2023 № 825-р // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/825-2023-%D1%80> (дата звернення: 27.08.2026).

References

1. Verkhovna Rada of Ukraine (2021), "On critical infrastructure" ["Pro krytychnu infrastrukturu"], Law of Ukraine No. 1882-IX, 16 November 2021, Legislation of Ukraine database, available at: <https://zakon.rada.gov.ua/go/1882-20> (accessed 27 August 2026).
2. Verkhovna Rada of Ukraine, "Terminology of Ukrainian legislation" ["Terminolohiia zakonodavstva Ukrainy"], official web portal of the Parliament of Ukraine, available at: <https://zakon.rada.gov.ua/laws/term/36366> (accessed 24 August 2026).
3. Verkhovna Rada of Ukraine, "Critical infrastructure" ["Krytychna infrastruktura"], Legislation Terminology database, available at: <https://zakon.rada.gov.ua/laws/term/1882-20> (accessed 29 August 2026).
4. Cabinet of Ministers of Ukraine (2020), "Certain issues of critical infrastructure objects" ["Deiaki pytannia ob'ektiv krytychnoi infrastruktury"], Resolution No. 1109, 9 October 2020 (Procedure, List, Methodology), Legislation of Ukraine database, available at: <https://zakon.rada.gov.ua/go/1109-2020-%D0%BF> (accessed 27 August 2026).
5. Cabinet of Ministers of Ukraine (2023), "Certain issues of certification of critical infrastructure objects" ["Deiaki pytannia pasportyzatsii ob'ektiv krytychnoi infrastruktury"], Resolution No. 818, 4 August 2023 (Procedure, Standard document form, Certificate), Legislation of Ukraine database, available at: <https://zakon.rada.gov.ua/go/818-2023-%D0%BF> (accessed 27 August 2026).
6. Zaporozhets, T.V. (2024), *State policy in the field of critical infrastructure protection* ["Derzhavna polityka u sferi zakhystu krytychnoi infrastruktury"], textbook, DKS Tsentr, Kyiv, 186 p., ISBN 978-617-8080-12-9.
7. Dovhan, O.D., Tkachuk, T.Yu. (2024), *Cyber risks of critical infrastructure: from threat analysis to solution implementation* ["Kiberryzyky krytychnoi infrastruktury: vid analizu zahroz do vprovadzhennia rishen"], scientific-practical guide, Feniks, Kyiv; Odesa, 70 p., ISBN 978-617-8430-50-4.
8. Kohut, Yu.I. (2024), *Cyberwar and security of critical infrastructure objects* ["Kiberviina ta bezpeka ob'ektiv krytychnoi infrastruktury"], 2nd ed., Sidkon Consulting Company, Kyiv, ISBN 978-617-95100-3-8.
9. *Physical and cyber protection of critical infrastructure objects of Ukraine by police bodies and units* ["Fizychnyi ta kibernetychnyi zakhyst ob'ektiv krytychnoi infrastruktury Ukrainy orhanamy ta pidrozdilamy politsii"], textbook, Vinnytsia, 2025.
10. Tekinerdogan, B., Aksit, M., Catal, C., Hurst, W., AlSkaif, T. (eds.) (2023), *Management and Engineering of Critical Infrastructures*, Academic Press, Amsterdam, ISBN 978-0-323-99330-2. DOI: <https://doi.org/10.1016/C2021-0-02364-2>.
11. Küfeoğlu, S., Akgün, A.T. (2024), *Cyber Resilience in Critical Infrastructure*, 1st ed., CRC Press, Boca Raton, ISBN 978-1-032-58306-8.
12. Raval, K.J., Jadav, N.K., Rathod, T., Tanwar, S., Vimal, V., Yamsani, N. (2024), "A Survey on Safeguarding Critical Infrastructures: Attacks, AI Security, and Future Directions", *International Journal of Critical Infrastructure Protection*, Vol. 44, Art. 100647. DOI: <https://doi.org/10.1016/j.ijcip.2023.100647>.

13. Tabansky, L., Lichterman, E. (2025), "PROGRESS: The Sectoral Approach to Cyber Resilience", *International Journal of Information Security*, Vol. 24, Art. 18. DOI: <https://doi.org/10.1007/s10207-024-00910-3>.
14. Wang, F., Tian, J., Ling, J., Chen, Z., Xu, Z. (2025), "A Multi-Stage Resilience Analysis Framework of Critical Infrastructure Systems Based on Component Importance Measures", *Reliability Engineering & System Safety*, Vol. 256, Art. 110720. DOI: <https://doi.org/10.1016/j.res.2024.110720>.
15. Parshyna, O.A., Metelenko, N.H., Kovalenko, V.L., Parshyna, M.Yu. (2023), "Systemic provision of information security at critical infrastructure objects" ["Systemne zabezpechennia informatsiinoi bezpeky na ob'ekтах krytychnoi infrastruktury"], *Philosophy, Economics and Law Review*, Vol. 3, No. 2, pp. 66–80. DOI: <https://doi.org/10.31733/2786-491X-2023-2-66-80>.
16. Yudina, D.O. (2025), "A method for calculating the level of cyber protection of critical information infrastructure objects" ["Metod rozrakhunku rivnia kiberzakhystu ob'ektiv krytychnoi informatsiinoi infrastruktury"], *Cybersecurity: Education, Science, Technique*, No. 2 (30), pp. 473–487. DOI: <https://doi.org/10.28925/2663-4023.2025.30.986>.
17. Hrechaninov, V.F. (2025), "Intelligent system of scenario modeling for assessing the security of critical infrastructure objects" ["Intelektualna systema stsenarnoho modeliuvannia otsinky zakhyschenosti ob'ektiv krytychnoi infrastruktury"], *Technical Sciences and Technologies*, No. 3 (41), pp. 131–145. DOI: [https://doi.org/10.25140/2411-5363-2025-3\(41\)-131-145](https://doi.org/10.25140/2411-5363-2025-3(41)-131-145).
18. Hrechaninov, V.F. (2025), "Models and technologies of intelligent protection of critical infrastructure information systems for resilience enhancement" ["Modeli ta tekhnolohii intelektualnogo zakhystu informatsiinykh system krytychnoi infrastruktury dlia pidvyshchennia stiikosti"], *Cybersecurity: Education, Science, Technique*, No. 1 (29), pp. 877–896. DOI: <https://doi.org/10.28925/2663-4023.2025.29.948>.
19. National Institute of Standards and Technology (2024), *The NIST Cybersecurity Framework (CSF) 2.0*, NIST, Gaithersburg. DOI: <https://doi.org/10.6028/NIST.CSWP.29>.
20. Cabinet of Ministers of Ukraine (2025), "On approval of requirements for security risk management at critical infrastructure objects of criticality category I" ["Pro zatverdzhennia vymoh shchodo upravlinnia ryzykamy bezpeky na ob'ekтах krytychnoi infrastruktury I katehorii krytychnosti"], Resolution No. 367, 1 April 2025 (Requirements, Standard document form, Report), Legislation of Ukraine database, available at: <https://zakon.rada.gov.ua/go/367-2025-%D0%BF> (accessed 27 August 2026).
21. Cabinet of Ministers of Ukraine (2022), "On approval of the Procedure for monitoring the security level of critical infrastructure objects" ["Pro zatverdzhennia Poriadku monitorynhu rivnia bezpeky ob'ektiv krytychnoi infrastruktury"], Resolution No. 821, 22 July 2022, Legislation of Ukraine database, available at: <https://zakon.rada.gov.ua/go/821-2022-%D0%BF> (accessed 27 August 2026).
22. Administration of the State Service of Special Communications and Information Protection of Ukraine (2025), "On approval of the Methodology and criteria for assessing the state of protection of critical infrastructure objects" ["Pro zatverdzhennia Metodyky ta kryteriiv otsinky stanu zakhyschenosti ob'ektiv krytychnoi infrastruktury"], Order No. 17, 14 January 2025, Legislation of Ukraine database, available at: <https://zakon.rada.gov.ua/> (accessed 27 August 2026).
23. Ivanusa, A., Yashchuk, V., Fedyna, B. (2023), "Study of the process of assessing cybersecurity risks of critical infrastructure objects" ["Doslidzhennia protsesu otsiniuvannia ryzykiv kiberbezpeky ob'ektiv krytychnoi infrastruktury"], *Information Security and Information Technologies: collection of abstracts of the VI All-Ukrainian scientific-practical conference of young scientists, students and cadets, Lviv, 30 November 2023*, LDU BZhD, Lviv, 489 p., pp. 84–87.
24. Yashchuk, V., Balatska, V. (2026), "Enhancing the cyber resilience of the state's critical information infrastructure through improved cyber incident response processes" ["Pidvyshchennia kiberstiikosti krytychnoi informatsiinoi infrastruktury derzhavy cherez vdoskonalennia protsesiv reahuvannia na kiberintsydeny"], *Civil Protection in Wartime: collection of abstracts of the 2nd International scientific-practical conference, Lviv, 15 April 2026*, LDUBZhD, Lviv, pp. 92–95.
25. Verkhovna Rada of Ukraine (2017), "On the basic principles of ensuring cybersecurity of Ukraine" ["Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy"], Law of Ukraine No. 2163-VIII, 5 October 2017, Legislation of Ukraine database, available at: <https://zakon.rada.gov.ua/go/2163-19> (accessed 27 August 2026).
26. Verkhovna Rada of Ukraine (1994), "On protection of information in information and telecommunication systems" ["Pro zakhyt informatsii v informatsiino-komunikatsiinykh systemakh"], Law of Ukraine No. 80/94-VR, 5 July 1994, Legislation of Ukraine database, available at: <https://zakon.rada.gov.ua/go/80/94-%D0%B2%D1%80> (accessed 27 August 2026).
27. Cabinet of Ministers of Ukraine (2023), "On approval of the National Plan for the Protection and Ensuring the Security and Resilience of Critical Infrastructure" ["Pro zatverdzhennia Natsionalnogo planu zakhystu ta zabezpechennia bezpeky ta stiikosti krytychnoi infrastruktury"], Order No. 825-r, 19 September 2023 (Plan),

Legislation of Ukraine database, available at: <https://zakon.rada.gov.ua/go/825-2023-%D1%80> (accessed 27 August 2026).

Надійшла до редакції 21.08.2026

V. I. YASHCHUK, O. I. POLOTAY, V. S. BALATSKA

^{1,2,3}Lviv State University of Life Safety, Lviv, Ukraine

¹valentina.lender@gmail.com, ²orest.polotaj@gmail.com, ³v.balatska@ldubgd.edu.ua

DESIGNING SECURITY SYSTEMS FOR CRITICAL INFRASTRUCTURE OBJECTS

The article substantiates the theoretical and methodological principles of designing integrated security systems for critical infrastructure objects in Ukraine based on systemic and risk-oriented approaches. The purpose of the study is to develop a generalized approach to designing security systems that integrates organizational, physical, engineering, information and cybersecurity measures according to identified threats and risks. The methodological basis of the research includes systemic, structural-functional and risk-oriented approaches, as well as methods of analysis, classification, systematization and modeling. The essence of a security system for a critical infrastructure object is clarified, and the relationship between security, protection and resilience is substantiated. The main groups of threats to critical infrastructure are systematized, including natural, technological, physical, military, information, cyber and combined threats. The influence of these threats on critical functions, assets and infrastructure dependencies is considered. It is emphasized that disruption of one critical infrastructure object may cause cascading effects in related sectors, which requires a comprehensive approach to security system design. A generalized six-stage model for designing a security system is proposed. It includes identification of the object, its critical functions and assets; threat identification and analysis; risk assessment; design of security measures; implementation and documentation; monitoring and continuous improvement. The model establishes a direct relationship between threats, vulnerabilities, critical assets, potential consequences, risks and corresponding security measures. This approach enables the selection and justification of security measures based on their contribution to risk reduction and preservation of critical functions rather than on a formal list of protective measures. The structure of an integrated security system is proposed as a combination of organizational, access-control, physical, engineering, information-security and cybersecurity measures. The necessity of continuous monitoring, reassessment of risks and management of residual risks is substantiated. The practical significance of the research lies in the possibility of applying the proposed approach to the development of security systems, security plans, risk management procedures and organizational and technical documentation for critical infrastructure objects. The proposed model provides a methodological basis for further research on quantitative risk assessment, optimization of security measures and modeling of cascading effects.

Keywords: *critical infrastructure objects, security system design, critical infrastructure protection, cybersecurity, risk-oriented approach, integrated protection system.*