



КАБІНЕТ МІНІСТРІВ УКРАЇНИ ПОСТАНОВА

від 1 квітня 2025 р. № 367
Київ

Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності

Відповідно до [абзацу другого](#) частини першої статті 22 Закону України “Про критичну інфраструктуру” Кабінет Міністрів України **постановляє**:

Затвердити [вимоги щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності](#), що додаються.

Прем'єр-міністр України

Д. ШМИГАЛЬ

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 1 квітня 2025 р. № 367

ВИМОГИ
щодо управління ризиками безпеки на об'єктах
критичної інфраструктури I категорії критичності

1. Ці вимоги встановлюються до управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності, що здійснюється оператором критичної інфраструктури.

Дія цих вимог не поширюється на банки, інших осіб, які провадять діяльність на ринках фінансових послуг, платіжні організації, учасників платіжних систем, операторів послуг платіжної інфраструктури, державне регулювання, нагляд за діяльністю яких здійснює Національний банк.

2. Терміни, що вживаються у цих вимогах, мають таке значення:

ліміт ризику безпеки - обмеження, встановлені оператором критичної інфраструктури для контролю за величиною ризиків, які впливають на можливість виникнення інциденту безпеки критичної інфраструктури (далі - інцидент)/порушення стану захищеності критичної інфраструктури та відповідно виконання життєво важливих функцій та/або надання послуг об'єктом критичної інфраструктури;

ризик - можливість виникнення несприятливої (негативної) події або ряду таких подій, що визначається ймовірністю, джерелами і обставинами виникнення та наслідками;

ризик безпеки на об'єктах критичної інфраструктури (далі - ризик безпеки) - можливість виникнення інциденту безпеки критичної інфраструктури/порушення стану захищеності критичної інфраструктури, що становить загрозу для забезпечення функціональності, безперервності роботи, відновлюваності, цілісності та стійкості об'єктів критичної інфраструктури.

Інші терміни вживаються у значенні, наведеному в [Законі України](#) “Про критичну інфраструктуру” та постанові Кабінет Міністрів України від 4 серпня 2023 р. [№ 818](#) “Деякі питання паспортизації об'єктів критичної інфраструктури” (Офіційний вісник України, 2023 р., № 77, ст. 4366).

3. Управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності (далі - управління ризиками безпеки) є діяльністю, спрямованою на запобігання виникненню інциденту та мінімізацію можливих наслідків у разі його настання.

Управління ризиками безпеки здійснюється із застосуванням національних та міжнародних стандартів управління ризиками безпеки, у тому числі методів, наведених у ДСТУ ІЕС/ISO 31010:2013 “Керування ризиками. Методи загального оцінювання ризиків”,

“Контроль безпеки та конфіденційності для державних інформаційних систем і організацій” (NIST Risk Management Framework SP 800-53).

4. Оператор критичної інфраструктури здійснює управління ризиками безпеки шляхом створення системи управління ризиками безпеки.

Система управління ризиками безпеки повинна відповідати таким принципам:

інтегрованість - полягає в охопленні системою управління ризиками безпеки всієї діяльності оператора критичної інфраструктури;

структурованість і комплексність - полягає в забезпеченні послідовного та взаємоузгодженого вжиття заходів в усіх сферах діяльності оператора критичної інфраструктури для досягнення цілей щодо забезпечення безпеки та стійкості критичної інфраструктури;

індивідуальність - полягає у врахуванні особливостей об'єкта критичної інфраструктури під час створення системи управління ризиками безпеки;

динамічність - полягає у належному реагуванні на зміну умов функціонування об'єкта критичної інфраструктури з метою забезпечення пропорційності та/або співрозмірності заходів реальним та потенційним ризикам;

належна поінформованість - полягає в організації постійного забезпечення оператора критичної інфраструктури актуальною, точною та повною інформацією для управління ризиками безпеки;

мінімізованість людського фактора - полягає у взаємопов'язаних заходах із зменшення участі людини в робочих процесах та процедурах з одночасним підвищенням рівня професійних навичок, знань, здібностей та покращенням морально-психологічного стану трудового колективу, що впливають на стійке функціонування об'єкта критичної інфраструктури.

5. Основними ризиками безпеки, зокрема, є:

1) матеріальні ризики - ризики настання інциденту як для об'єкта критичної інфраструктури, так і для критичних елементів об'єкта критичної інфраструктури, що можуть призвести до заподіяння їм шкоди, а також шкоди життю та здоров'ю людей;

2) ризики кібербезпеки та захисту інформації - ризики щодо забезпечення безпеки, функціональності, безперервності роботи, відновлюваності, цілісності і стійкості інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, електронних комунікаційних мереж;

3) ризики людського фактору - ризики порушення штатного режиму функціонування об'єкта критичної інфраструктури (у тому числі зриву та/або блокування роботи, та/або несанкціонованого управління його ресурсами) та безпосередньо пов'язані з працівниками об'єкта критичної інфраструктури, іншими особами, які перебувають на об'єкті, що можуть призвести до виникнення інциденту/порушення стану захищеності критичної інфраструктури та відповідно виконання життєво важливих функцій та/або надання послуг об'єктом критичної інфраструктури;

4) ризики порушення взаємозв'язків - ризики зриву, злочинного або ненавмисного порушення штатного режиму функціонування об'єкта критичної інфраструктури, що ставлять під загрозу його захищеність, виконання життєво важливих функцій та/або надання життєво важливих послуг, надання об'єктом критичної інфраструктури основних послуг іншим об'єктам критичної інфраструктури/отримання таких послуг від інших об'єктів критичної інфраструктури, що вплине на функціонування інших об'єктів критичної інфраструктури, призведе до порушення стійкості критичної інфраструктури;

5) ризики, пов'язані з процесами, - ризики щодо забезпечення безпеки, функціональності, безперервності роботи, відновлюваності, цілісності і стійкості об'єктів критичної інформаційної інфраструктури, спричинені неоптимальною організацією робочих процесів.

Оператор критичної інфраструктури визначає ризики безпеки для об'єкта критичної інфраструктури з обов'язковим урахуванням основних ризиків безпеки, визначених цим пунктом, а також інших ризиків, які можуть вплинути на забезпечення безпеки, функціональності, безперервності роботи, відновлюваності, цілісності і стійкості критичної інфраструктури.

6. Для управління ризиками безпеки оператор критичної інфраструктури:

1) забезпечує ресурсами, необхідними для організації управління ризиками безпеки, створений окремий структурний підрозділ або визначену особу, відповідальну за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб'єктами національної системи захисту критичної інфраструктури;

2) розробляє та затверджує документи (правила, політики тощо) щодо управління ризиками безпеки, що передбачають:

організацію управління ризиками безпеки;

оцінювання ризиків безпеки;

запобігання ризикам (мінімізація ризиків) безпеки;

моніторинг і контроль за ризиками безпеки та перегляд їх актуальності;

обмін інформацією та взаємодію із суб'єктами національної системи захисту критичної інфраструктури;

3) забезпечує:

визначення необхідного для сталого функціонування об'єкта критичної інфраструктури персоналу (працівників);

складення профілю ризиків безпеки об'єкта критичної інфраструктури;

створення належних умов праці на об'єкті критичної інфраструктури, зокрема для тривалого перебування в робочих приміщеннях;

визначення засобів зв'язку для оповіщення та інформування персоналу (працівників);

розроблення об'єктового плану заходів щодо забезпечення безпеки та стійкості критичної інфраструктури;

розроблення проектних загроз об'єктового рівня.

7. Для організації управління ризиками безпеки окремий структурний підрозділ оператора критичної інфраструктури або визначена ним особа, відповідальна за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб'єктами національної системи захисту критичної інфраструктури, забезпечує:

- 1) розроблення документів (правил, політик тощо) щодо управління ризиками безпеки;
- 2) своєчасне виявлення та оцінювання ризиків безпеки;
- 3) організацію заходів, спрямованих на запобігання ризикам (мінімізацію ризиків) безпеки;
- 4) моніторинг і контроль за ризиками безпеки та перегляд їх актуальності;
- 5) обмін інформацією та взаємодію із суб'єктами національної системи захисту критичної інфраструктури;
- 6) підготовку звітної та аналітичної інформації, інформування керівника оператора критичної інфраструктури щодо ризиків безпеки;
- 7) виконання інших завдань щодо організації управління ризиками безпеки.

Структурний підрозділ оператора критичної інфраструктури або визначена ним особа, що відповідальні за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб'єктами національної системи захисту критичної інфраструктури, повинні відповідати професійним стандартам, затвердженим Адміністрацією Держспецзв'язку.

У разі відсутності відповідних професійних стандартів структурний підрозділ оператора критичної інфраструктури або визначена ним особа, відповідальна за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб'єктами національної системи захисту критичної інфраструктури, повинні відповідати кваліфікаційним характеристикам професій працівників у сфері захисту та стійкості критичної інфраструктури, затвердженим Адміністрацією Держспецзв'язку.

8. Організація управління ризиками безпеки передбачає:

визначення вихідних даних щодо функціонування об'єкта критичної інфраструктури (загальна характеристика об'єкта критичної інфраструктури, у тому числі інформація про оператора критичної інфраструктури, зв'язок об'єкта критичної інфраструктури з іншою інфраструктурою, природно-кліматичні умови місцезнаходження об'єкта критичної інфраструктури, небезпечні технологічні процеси на об'єкті критичної інфраструктури, проектні загрози національного, секторального та об'єктового (у разі наявності) рівня, а також критеріїв щодо управління ризиками безпеки, лімітів ризиків безпеки);

визначення суб'єктів національної системи захисту критичної інфраструктури, які беруть участь у виконанні завдань/здійсненні заходів щодо управління ризиками безпеки;

формування системних та структурованих підходів до організації управління ризиками безпеки та їх застосування;

визначення методів, інструментів та механізмів, які використовуються під час управління ризиками безпеки;

визначення обсягів і джерел фінансових, матеріально-технічних, людських та інших ресурсів, необхідних для управління ризиками безпеки;

визначення засобів і заходів, необхідних для забезпечення комунікації в ході управління ризиками безпеки, в тому числі організації взаємодії між суб'єктами національної системи захисту критичної інфраструктури;

забезпечення узгодженості заходів щодо управління ризиками безпеки із заходами, що сплановані за іншими напрямками функціонування об'єкта критичної інфраструктури.

9. Оцінювання ризиків безпеки передбачає:

ідентифікацію ризиків безпеки;

проведення аналізу ризиків безпеки;

оброблення ризиків безпеки.

10. Ідентифікація ризиків безпеки передбачає визначення потенційно можливих інцидентів та їх показників (характеристик), документування отриманих відомостей.

За результатами ідентифікації ризиків безпеки складається перелік таких ризиків.

11. Проведення аналізу ризиків безпеки передбачає дослідження ідентифікованих ризиків безпеки з метою визначення лімітів ризику безпеки та ймовірності настання відповідних інцидентів, характеристик потенційних інцидентів, визначення ймовірності та вагомості їх наслідків.

Аналіз ризиків безпеки проводиться шляхом:

визначення причин та джерел виникнення ризиків безпеки;

визначення ймовірності настання відповідних інцидентів за ідентифікованими ризиками безпеки на підставі отриманих кількісних, якісних або комбінованих їх показників (характеристик);

ранжування (визначення вагомості) ризиків безпеки на підставі вивчення їх кількісних, якісних або комбінованих показників (характеристик) ризиків безпеки.

Аналіз ризиків безпеки проводиться з урахуванням досвіду суб'єктів національної системи захисту критичної інфраструктури у разі наявності та рішень, прийнятих внаслідок інцидентів, які виникали раніше, методів загального оцінювання ризику.

12. Оброблення результатів аналізу ризиків безпеки здійснюється шляхом зіставлення ризиків безпеки із заходами щодо управління ними, зокрема через порівняння результатів аналізу ризиків безпеки та зазначених заходів.

Зіставлення ризиків безпеки із заходами щодо управління ними здійснюється з метою забезпечення пропорційності та/або співрозмірності заходів відповідним ризикам, запобігання виникненню ризиків безпеки (їх мінімізації) та наближенню величини ризиків до лімітів ризику безпеки.

Оброблення ризиків безпеки передбачає визначення заходів з управління такими ризиками безпеки, запобігання виникненню інциденту та мінімізацію можливих наслідків у разі його виникнення.

Оброблення ризиків безпеки проводиться за такими етапами:

визначення підходів до оброблення кожного ідентифікованого ризику безпеки;

визначення прийнятних (таких, що не потребують додаткових заходів для мінімізації можливих наслідків виникнення інциденту та ймовірності їх настання) та неприйнятних ризиків безпеки;

формування переліку альтернативних заходів з управління ризиками безпеки та протидії таким ризикам;

визначення найбільш ефективного заходу з управління ризиками безпеки та протидії таким ризикам;

визначення супутніх ризиків безпеки, які можуть виникнути у зв'язку із запровадженням додаткових заходів управління ризиками безпеки, та протидії таким ризикам, проведення їх аналізу;

підготовка об'єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, паспорта безпеки на об'єкт критичної інфраструктури та його складових.

13. Підготовка до проведення моніторингу і контролю за ризиками безпеки та перегляд їх актуальності передбачають забезпечення оператора критичної інфраструктури актуальною, об'єктивною та достовірною інформацією з питань, що стосується управління ризиками безпеки, контроль за наближенням величини ризиків до лімітів ризику безпеки.

Перегляд актуальності ризиків безпеки проводиться не рідше ніж один раз на рік шляхом:

проведення перевірки актуальності інформації, яка зазначена в паспорті безпеки на об'єкт критичної інфраструктури;

прогнозування виникнення нових інцидентів, визначення ймовірності та вагомості їх наслідків і прогнозування варіантів їх розвитку, визначення ступеня вразливості об'єкта критичної інфраструктури;

проведення моніторингу в системі управління ризиками безпеки.

14. Обмін інформацією та взаємодія суб'єктів національної системи захисту критичної інфраструктури здійснюються відповідно до [Регламенту обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури](#), затвердженого постановою Кабінету Міністрів України від 14 жовтня 2022 р. № 1174 (Офіційний вісник України, 2022 р., № 84, ст. 5184).

15. Оператор критичної інфраструктури на підставі результатів аналізу ризиків безпеки повинен розробити та затвердити об'єктовий план заходів щодо забезпечення безпеки та стійкості критичної інфраструктури відповідно до плану заходів та рекомендацій з розроблення плану заходів, що затверджуються Адміністрацією Держспецзв'язку.

16. Оператори критичної інфраструктури подають щороку до 30 січня секторальним органам у сфері захисту критичної інфраструктури звіт про виконання вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності за формою згідно з додатком 1.

17. Секторальні органи у сфері захисту критичної інфраструктури подають щороку до 15 лютого Адміністрації Держспецзв'язку звіт про виконання вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності за формою згідно з додатком 2.

Додаток 1
до вимог

ЗВІТ

**про виконання вимог щодо управління ризиками безпеки на
об'єктах критичної інфраструктури I категорії критичності**

Додаток 2
до вимог

ЗВІТ

**про виконання вимог щодо управління ризиками безпеки на
об'єктах критичної інфраструктури I категорії критичності**



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

Прийняття від **01.04.2025**

Постійна адреса:

<https://zakon.rada.gov.ua/go/367-2025-%D0%BF>

Законодавство України
станом на 06.05.2025

чинний



367-2025-р

Документи та файли

- Сигнальний документ — [f544003n103.docx](#) від 04.04.25 15:55, 19 кб
- Сигнальний документ — [f544003n104.docx](#) від 04.04.25 15:55, 18 кб

Публікації документа

- Урядовий кур'єр від 04.04.2025 — № 70