Додаток 1
до вимог

Гриф обмеження доступу

ЗВІТ
про виконання вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури
І категорії критичності
за _____ рік

_____
_____
(найменування об'єкта критичної інфраструктури)

_____
_____
(реєстровий номер об'єкта критичної інфраструктури)

_____
_____
_____
_____
(найменування/прізвище, власне ім'я, по батькові (за наявності) оператора критичної інфраструктури)

1. Особа (прізвище, власне ім'я, по батькові (за наявності), посада) або відповідальний підрозділ з управління ризиками/головного ризик-менеджера (за наявності), на яку (який) покладено повноваження щодо управління ризиками безпеки на об'єкті критичної інфраструктури

_____
_____
_____

2. Впровадження системи управління ризиками безпеки – впроваджено/не впроваджено.

3. Визначення необхідного для сталого функціонування об'єкта критичної інфраструктури персоналу (працівників) – визначено/не визначено.

4. Профіль ризиків безпеки об'єкту критичної інфраструктури – складено/не складено.

5. Забезпечення належними умовами праці на об'єкті критичної інфраструктури, зокрема для тривалого перебування в робочих приміщеннях – забезпечено/не забезпечено.

6. Визначення засобів зв'язку для оповіщення та інформування персоналу (працівників) – визначено/ не визначено.

7. Об'єктовий план заходів щодо забезпечення безпеки та стійкості критичної інфраструктури – розроблено/не розроблено.

8. Документи (політики, регламенту, процедури), які встановлюють підхід до управління ризиками безпеки – розроблено/не розроблено.

9. Методик та інших документів для аналізу впливу різних факторів ризиків – розроблено/не розроблено.

10. Проектні загрози об’єктового рівня – розроблено/не розроблено.

11. Висновки щодо ідентифікованих і задокументованих ризиків безпеки – підготовлено/не підготовлено.

№ з/п	Ідентифіковані ризики безпеки	Коментар щодо вжитих заходів для мінімізації ризиків безпеки

12. Відомості про ризики безпеки.

№ з/п	Прийнятні ризики безпеки	Неприйнятні ризики безпеки

_____
_____
_____ _____ _____

(найменування посади керівника оператора критичної інфраструктури) (підпис) (власне ім’я, прізвище)

_____

Додаток 2
до вимог

Гриф обмеження доступу

ЗВІТ
про виконання вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності
за _____ рік

_____
_____
_____
(найменування секторального органу у сфері захисту критичної інфраструктури)

_____
_____
_____
_____
(Сектор, підсектор)

1. Відомості про особу (прізвище, власне ім'я, по батькові (за наявністю) або відповідальний підрозділ з управління ризиками/головного ризик-менеджера (за наявності), на яку (який) покладено повноваження щодо управління ризиками безпеки на об'єкті критичної інфраструктури:

Найменування об'єкта критичної інфраструктури	Реєстровий номер	Особа (прізвище, власне ім'я, по батькові (за наявності), посада) або відповідальний підрозділ з управління ризиками/головного ризик-менеджера (за наявності), на яку (який) покладено повноваження щодо управління ризиками безпеки на об'єкті критичної інфраструктури

2. Впровадження системи управління ризиками безпеки – впроваджено/не впроваджено.

Найменування об'єкта критичної інфраструктури	Впроваджено/не впроваджено

3. Визначення необхідного для сталого функціонування об'єкта критичної інфраструктури персоналу (працівників) – визначено/не визначено.

Найменування об'єкта критичної інфраструктури	Визначено/не визначено

4. Профіль ризиків безпеки об'єкту критичної інфраструктури – складено/не складено.

Найменування об'єкта критичної інфраструктури	Складено/не складено

5. Забезпечення належними умовами праці на об'єкті критичної інфраструктури, зокрема для тривалого перебування в робочих приміщеннях – забезпечено/не забезпечено.

Найменування об'єкта критичної інфраструктури	Забезпечено/не забезпечено

6. Визначення засобів зв'язку для оповіщення та інформування персоналу (працівників) – визначено/ не визначено.

Найменування об’єкта критичної інфраструктури	Визначено/не визначено

7. Об’єктовий план заходів щодо забезпечення безпеки та стійкості критичної інфраструктури – розроблено/не розроблено.

Найменування об’єкта критичної інфраструктури	Розроблено/не розроблено

8. Документи (політики, регламенту, процедури), які встановлюють підхід до управління ризиками безпеки – розроблено/не розроблено.

Найменування об’єкта критичної інфраструктури	Розроблено/не розроблено

9. Методик та інших документів для аналізу впливу різних факторів ризиків – розроблено/не розроблено.

Найменування об’єкта критичної інфраструктури	Розроблено/не розроблено

10. Проектні загрози об’єктового рівня – розроблено/не розроблено.

Найменування об’єкта критичної інфраструктури	Розроблено/не розроблено

11. Висновки щодо ідентифікованих і задокументованих ризиків безпеки – підготовлено/не підготовлено.

№ з/п	Ідентифіковані ризики безпеки	Коментар щодо вжитих заходів для мінімізації ризиків безпеки
	Найменування об’єкта критичної інфраструктури	

12. Відомості про ризики безпеки.

№ з/п	Прийнятні ризики безпеки	Неприйнятні ризики безпеки
	Найменування об’єкта критичної інфраструктури	

_____
_____
_____ _____ _____

(найменування посади уповноваженої особи секторального органу у сфері захисту критичної інфраструктури) (підпис) (власне ім’я, прізвище)

Громадська організація «ІСАКА КИЇВ»
ЄДРПОУ 38744988
Україна, 01032, м. Київ, вул. Жилянська, буд. 75,
десятий поверх

Вих. № 1202 27 грудня 2023 р.

Адміністрації
Державної служби спеціального зв'язку та захисту інформації України

Щодо проєкту постанови Кабінету Міністрів України «Про затвердження вимог щодо управління ризиками безпеки на об’єктах критичної інфраструктури І категорії критичності», наданих до громадського обговорення

Шановні панове,

ГО «ІСАКА КИЇВ» висловлює Вам щиру подяку за зусилля з посилення спроможності об’єктів критичної інфраструктури з управління ризиком безпеки.

Ми проаналізували документи, запропоновані до громадського обговорення за посиланням https://cip.gov.ua/ua/news/povidomlennya-pro-oprilyudnennya-proyektu-postanovi-kabinetu-ministriv-ukrayini-pro-zatverdzhennya-vimog-shodo-upravlinnya-rizikami-bezpeki-na-ob-yektakh-kritichnoyi-infrastrukturi-i-kategoriyi-kritichnosti30112023, і надаємо загальні коментарі в тексті листа та коментарі і редакцію тексту вимог в додатку 1 до листа в файлі Проект Вимог_ІСАКА_271223.docx з контрольною сумою SHA 512 57945c276449624c01f3d26574eb6a2337c80 b0311858d0f2d57af2508f4778644614e1e2a1fd0ca45c6626709b8a83cdbd3a44626ac4c7729a6296b1528c86f.

Загальні коментарі.

1. Ми підтримуємо зусилля з посилення управління ризиками безпеки, будучи в грудні 2023 очевидцями двох подій ризику критичної інфраструктури – Київського метрополітену і послуг мобільного оператора Київстар. Як громадяни, ми зацікавлені, щоб подібних подій траплялося менше, а наслідки тих, що можуть трапитися були м’якші. Маючи досвід і знання з управління ризиками, ми пропонуємо правки до Вимог, спрямовані на такий результат.

2. Ми звернули увагу на внутрішню неузгодженість термінології постанови, та пропонуємо редакцію.

3. Ми звернули увагу на формальний характер аналізу регуляторного впливу. Вимоги до системи управління ризиками безпеки на об’єктах критичної інфраструктури І категорії критичності вимагають виділення ресурсів операторів об’єктів (включаючи фінансові). Приклад, що дає порядок оцінки витрат: https://gov.e-tender.ua/tender/dilovi-poslugi/UA-2023-11-17-003191-a-dk-021-2015-kod-79410000-1-konsultaczijni-posluhy-z-pytan-pidpryyemnyczkoyi). І справляють вплив на громадян та суб’єктів малого та середнього підприємництва. Зокрема, належне управління ризиками в інфраструктурі дозволяє громадянам покладатися на сервіси та підвищує ефективність суб’єктів підприємництва, прискорюючи економічний розвиток і загалом збільшуючи добробут. А неналежне суттєво знижує продуктивність (відповідно, можливість платити податки, з яких фінансується сектор безпеки і оборони, і ДССЗЗІ зокрема). Наголошуємо на необхідності переглянути Аналіз регуляторного впливу з огляду на це.

4. Пропонуємо узгодити проект з NIS2 та статтею 21 Закону України від 16.11.2021 № 1882-IX "Про критичну інфраструктуру" https://zakon.rada.gov.ua/laws/show/1882-20#Text

5. Наголошуємо на необхідності логічної узгодженості діяльності з управління ризиками, та уможливленні інтеграції управління ризиками в операційну діяльність операторів. Міжнародні стандарти та практика пропонують з цією метою для нефінансових ризиків (наприклад: операційних, політичних, відповідності, безпеки) наступну послідовність:

1. **Визначення керованого обсягу, профілю і схильності до ризику** - це перше управлінське рішення, профіль в п. 11 вимог вже запропонований, а схильність (ліміти) – визначені в термінах.
2. **Оцінка:**
2.1.Ідентифікація ризику для обсягу: вивчення середовища зовнішнього і внутрішнього (з врахуванням моделювання загроз, розвідки загроз, прогнозування та інших методів), формування сценаріїв (це друге управлінське рішення – які розглядаємо), створення переліку (він же реєстр),
2.2. Аналіз сценаріїв: визначення вірогідності (або потенційної можливості, або невизначеності, або часу працездатності критичної послуги), оцінка наслідків за сценаріями, заповнення переліку і ранжування сценаріїв в ньому – це розрахунки, управлінські рішення не приймаються,
3.**Обробка ризиків**: вибір з прийняття, уникнення, пом'якшення, передачі щодо сценаріїв з переліка – це основні управлінські рішення, на підставі яких формується план і виділяються ресурси на нього.
4. **Забезпечення впровадження плану** – це завдання для виконання
5. **Моніторинг, перегляд і звітність** – полягає в підтримці актуальності даних переліку та відстеження постійних процесів з індикаторами їх динаміки – це операційна діяльність ризик-менеджерів.

Для ілюстрації додаємо референтний процес управління ризиками технологій з COBIT 2019, спрямований на інтеграцію в діяльність організації в додатку 2.
Доступ до офіційного перекладу COBIT 2019 українською вільний, з реєстрацією за адресою: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9IEAS

Також інформуємо, що така послідовність частково підтримується програмним забезпеченням, яке оптимізує діяльність з управління ризиками в частині збору даних, ведення переліків та відслідковування планів зокрема, може інтегруватися з моделями оцінки, але управлінські рішення, вказані вище, не приймає. Клас систем називається GRC. За посиланням можна ознайомитися з цим напрямком (доступ вільний, це дослідження 4 профорганізацій ризик-менеджерів і французького регулятора): https://www.ferma.eu/publication/the-new-edition-of-2023-amraes-rmis-panorama-15th-edition/

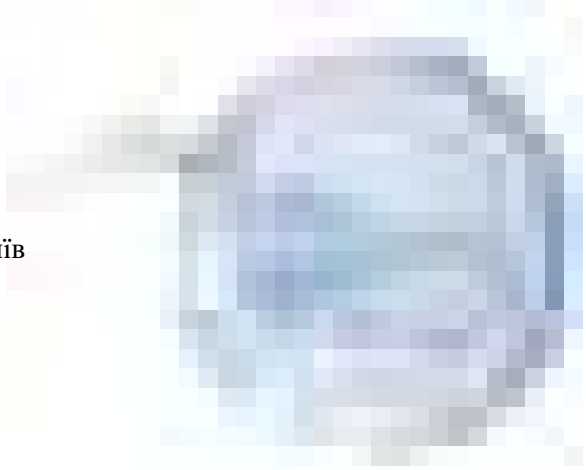
6. Зауважуємо, що в практиці управління ризиками підходи управління ризиками безпеки критичної інфраструктури використовується два різних підходи:
- для екзистенційних ризиків (наприклад: витік аміаку, підрив дамби, вибух атомної станції) – ймовірність приймається за 100%, моделюються наслідки, проектуються заходи попередження цих наслідків (порівнювані з наслідками – це ефективність),
- для операційних ризиків (наприклад: звільнення фахівців, кібератака, відмова обладнання) – оцінюється вірогідність сценарію, оцінюються наслідки, знаходиться їх добуток, приймається рішення про доцільність заходів, порівнюючи вартість заходів з цим добутком наслідків на вірогідність (це ефективність), складається план.

У випадку необхідності додаткових пояснень або запитань, звертайтеся, будь ласка, за електронною адресою office@isaca.org.ua. Ми готові провести для Держспецзв'язку, як тимчасового регулятра критичної інфраструктури, сесію з обізнаності в управлінні ризиками – чому ЗАЕС ще не вибухнула, а метро вже зупинилося і зв'язок відмовив (і є підстави вважати, що таких подій буде більше).

Додаток 1. Редакція вимог та коментарі в файлі Проект Вимог_ICAKA_271223.docx
SHA 512
57945c276449624c01f3d26574eb6a2337c80b0311858d0f2d57af2508f4778644614e1e2a1fd0ca45c6626709b8a83cdbd3a44626ac4c7729a6296b1528c86f

Додаток 2. Референтний опис процесів управління ризиками в файлі COBIT_RM_ua.pdf

З повагою,
Президент
ГО «ІСАКА КИЇВ»



Конопльова А.Є.,
CISA, CRISC, CDPSE

27 грудня 2023 року, м. Київ

Прим. № __

АДМІНІСТРАЦІЯ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-93-08, факс: (044) 281-94-83,
e-mail: info@cip.gov.ua, сайт: www.cip.gov.ua, код згідно з ЄДРПОУ 34620942

_____ № _____ На № _____ від _____

Державна регуляторна служба України

На виконання пункту 3 доручення Першого віце-прем'єр-міністра України – Міністра економіки України від 31.03.2023 № 18009/2/1-22 до листа Адміністрації Держспецзв'язку від 17.03.2023 № 07/01/02-1606/ВС Адміністрацією Держспецзв'язку розроблено проєкт постанови Кабінету Міністрів України «Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності» (далі – проєкт постанови).

Надсилаємо на погодження проєкт постанови відповідно до статті 21 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності».

Додатки: 1. Проєкт постанови на 14 арк.
2. Пояснювальна записка до проєкту постанови на 4 арк.
3. Аналіз регуляторного впливу до проєкту постанови на 7 арк.
4. Скріншот повідомлення про оприлюднення проєкту постанови на вебсайті Держспецзв'язку на 1 арк.
5. Лист Української асоціації операторів зв'язку «Телас» від 25.08.2023 № 69/23 (вх. № 16384/ВС від 26.08.2023) на 26 арк.
6. Протокол узгоджувальної наради від 27.09.2023 № 07/01/02-8695/ВН на 3 арк.
7. Лист Громадської організації «ІСАКА КИЇВ» від 27.12.2023 № 1202 (вх. № 26420/ВС від 27.12.2023) на 25 арк.
8. Протокол узгоджувальної наради від 26.04.2024 № 07/01/02-7110/ВН на 10 арк.

Голова Служби Юрій МИРОНЕНКО

Ольга ГРУДІЛОВА 281 91 03

вул. Солом'янська, 3, оф.808, м. Київ, 03110, Україна, тел./факс 248 9171, 248 9175
www.telas.kiev.ua **e-mail: astelas@ukrpack.net**

№ 69/23 від 25 серпня 2023 року

Голові Державної служби спеціального зв'язку та захисту інформації України
Щиголю Ю.Ф.

вул. Солом'янська, 13, м. Київ, 03110

Щодо надання пропозицій та зауважень до проекту постанови Кабінету Міністрів України

Шановний Юрію Федоровичу!

Українська асоціація операторів зв'язку «Телас» (далі – Асоціація «Телас»), що об'єднує провідних операторів електронних комунікацій України, висловлює Вам свою щиру повагу та повідомляє про наступне.

Експертами Асоціації «Телас» було уважно опрацьовано розроблений Адміністрацією Держспецзв'язку проект постанови Кабінету Міністрів України **«Про затвердження Вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності»** (далі – проект Постанови), який було розміщено на вебсайті Держспецзв'язку для громадського обговорення.

За результатами розгляду вищезазначеного проекту Постанови Асоціацією «Телас», надаємо пропозиції та зауваження, які у вигляді порівняльної таблиці додаються до цього листа.

Враховуючи зазначене вище, п**росимо врахувати пропозиції та зауваження Асоціації «Телас»** під час доопрацювання Адміністрацією Держспецзв'язку проекту постанови Кабінету Міністрів України **«Про затвердження Вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності»** та з метою більш детального обговорення питань, що виникли під час опрацювання проекту Постанови, **спланувати та провести робочу нараду з підведення підсумків громадського обговорення за участі його розробників та представників Асоціації.**

Додаток № 1: Порівняльна таблиця пропозицій та зауважень Асоціації «Телас» до розробленого Адміністрацією Держспецзв'язку проекту постанови Кабінету Міністрів України «Про затвердження Вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності» на 25 аркушах в 1 примірнику.

Сподіваємось на взаєморозуміння та подальшу плідну співпрацю.

З повагою,
Голова Ради Української асоціації
операторів зв'язку «Телас» Л.М. Ошеров

Прим. №__

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проєкту постанови Кабінету Міністрів України
«Про затвердження вимог щодо управління ризиками безпеки
на об’єктах критичної інфраструктури І категорії критичності»

1. Мета

Проєкт постанови Кабінету Міністрів України «Про затвердження вимог щодо управління ризиками безпеки на об’єктах критичної інфраструктури І категорії критичності» (далі – проєкт постанови) розроблено з метою встановлення методів щодо управління ризиками безпеки на об’єктах критичної інфраструктури І категорії критичності для забезпечення стійкості та захисту таких об’єктів, що здійснюється оператором критичної інфраструктури.

2. Обґрунтування необхідності прийняття акта

Проєкт постанови розроблено Адміністрацією Держспецзв’язку відповідно до вимог Закону України «Про критичну інфраструктуру» (далі – Закон) та на виконання пункту 3 доручення Першого віце-прем’єр-міністра України – Міністра економіки України від 31.03.2023 № 18009/2/1-22 до листа Адміністрації Держспецзв’язку від 17.03.2023 № 07/01/02-1606/ВС.

Відповідно до абзацу п’ятого пункту 1 Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03.09.2014 № 411, Адміністрація Держспецзв’язку є центральним органом виконавчої влади, який забезпечує здійснення Держспецзв’язку повноважень уповноваженого органу у сфері захисту критичної інфраструктури під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування, передбачених Законом.

Абзацом другим частини першої статті 22 Закону визначено, що Кабінет Міністрів України встановлює вимоги щодо управління ризиками безпеки на об’єктах критичної інфраструктури І категорії критичності, крім банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури, державне регулювання, нагляд за діяльністю яких здійснює Національний банк України, та встановлює вимоги щодо управління ризиками безпеки.

Слід зазначити, що постановою Правління Національного банку України від 11.06.2018 № 64 затверджено Положення про організацію системи управління ризиками в банках України та банківських групах.

Державна політика у сфері захисту критичної інфраструктури ґрунтується на засадах створення умов та впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, на зниження ризику реалізації

можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів (пункт 4 частини другої статті 4 Закону).

До завдань формування і реалізації державної політики у сфері захисту критичної інфраструктури належить розроблення комплексу заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об'єктах критичної інфраструктури (пункт 6 частини другої статті 5 Закону).

Разом з тим, пунктом 3 частини першої статті 21 Закону визначено, що основними завданнями операторів критичної інфраструктури, зокрема є проведення оцінки ризиків на об'єктах критичної інфраструктури та обмін інформацією про ризики та загрози з іншими суб'єктами національної системи захисту критичної інфраструктури.

Таким чином, прийняття постанови дозволить визначити комплекс заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів.

3. Основні положення проєкту акта

Проєктом постанови пропонується затвердити вимоги щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності.

4. Правові аспекти

У цій сфері правового регулювання діють такі акти:

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»;

Закон України «Про критичну інфраструктуру»;

Закон України «Про основні засади забезпечення кібербезпеки України»;

Постанова Кабінету Міністрів України від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури»;

Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затверджене постановою Кабінету Міністрів України від 03.09.2014 № 411.

5. Фінансово-економічне обґрунтування

Реалізація постанови не потребує додаткового фінансування з державного чи місцевих бюджетів.

6. Позиція заінтересованих сторін

Проєкт постанови 29.07.2023 оприлюднено на офіційному вебсайті Держспецзв'язку (https://cip.gov.ua) з метою проведення консультацій із заінтересованими сторонами. Від Української асоціації операторів зв'язку

«Телас» надійшли пропозиції до проєкту постанови листом від 25.08.2023 № 69/23. З метою врегулювання розбіжностей та формування консолідованої правової позиції щодо редакції проєкту постанови з Українською асоціацією операторів зв'язку «Телас» проведено узгоджувальну нараду 26.09.2023 (протокол від 27.09.2023 № 07/01/02-8695/ВН), за результатами якої зауваження в частині уточнення стосовно чого здійснюватиметься інформування персоналу (працівників) знято, а на зауваженні щодо необхідності доопрацювання аналізу регуляторного впливу проєкту постанови у частині, що стосується витрат суб'єктів господарювання, не наполягають, але висловили щодо нього застереження, інші зауваження враховані повністю.

Водночас доопрацьований проєкт постанови 27.09.2023 оприлюднено на офіційному вебсайті Держспецзв'язку (https://cip.gov.ua).

Так, від Громадської організації «ІСАКА Київ» надійшли пропозиції до проєкту постанови листом від 27.12.2023 № 1202. З метою врегулювання розбіжностей та формування консолідованої правової позиції щодо редакції проєкту постанови з Громадською організацією «ІСАКА Київ» проведено узгоджувальну нараду 16.04.2024 (протокол від 26.04.2024 № 07/01/02-7110/ВН), за результатами якої всі розбіжності врегульовано.

Від інших заінтересованих сторін пропозицій та зауважень не надходило.

Проєкт постанови не стосується питань функціонування місцевого самоврядування, прав та інтересів територіальних громад, місцевого та регіонального розвитку, соціально-трудової сфери, прав осіб з інвалідністю, функціонування і застосування української мови як державної, тому не потребує погодження з уповноваженими представниками всеукраїнських асоціацій органів місцевого самоврядування чи відповідними органами місцевого самоврядування, уповноваженими представниками всеукраїнських профспілок, їх об'єднань та всеукраїнських об'єднань організацій роботодавців, Урядовим уповноваженим з прав осіб з інвалідністю та всеукраїнськими громадськими організаціями осіб з інвалідністю, їх спілками, Уповноваженим із захисту державної мови.

Проєкт постанови не стосується сфери наукової та науково-технічної діяльності, тому не потребує погодження з Науковим комітетом Національної ради з питань розвитку науки і технологій.

7. Оцінка відповідності

Проєкт постанови не стосується зобов'язань України у сфері європейської інтеграції.

Проєкт постанови не стосується прав та свобод, гарантованих Конвенцією про захист прав людини і основоположних свобод.

Проєкт постанови не впливає на забезпечення рівних прав та можливостей жінок і чоловіків.

Проєкт постанови не містить ризики вчинення корупційних правопорушень та правопорушень, пов'язаних з корупцією.

Проєкт постанови не створює підстави для дискримінації.

Громадська антикорупційна, громадська антидискримінаційна та громадська гендерно-правова експертизи не проводилися.

8. Прогноз результатів

Прийняття постанови дозволить визначити методи щодо управління ризиками безпеки на об’єктах критичної інфраструктури I категорії критичності та забезпечить стійкість таких об’єктів, що дасть можливість підвищити рівень національної безпеки.

Реалізація постанови не матиме впливу на ринкове середовище, забезпечення захисту прав та інтересів суб’єктів господарювання, громадян; розвиток регіонів, підвищення чи зниження спроможності територіальних громад; ринок праці, рівень зайнятості населення; громадське здоров’я, покращення чи погіршення стану здоров’я населення або його окремих груп; екологію та навколишнє природне середовище, обсяг природних ресурсів, рівень забруднення атмосферного повітря, води, земель, зокрема забруднення утвореними відходами, інші суспільні відносини.

Вплив на інтереси заінтересованих сторін:

Заінтересована сторона	Вплив реалізації акта на заінтересовану сторону	Пояснення очікуваного впливу
Держава	Позитивний	забезпечить стійкість та захист об’єктів критичної інфраструктури шляхом управління ризиками безпеки на таких об’єктах та посилить національну безпеку в частині безперервності надання життєво важливих функцій та/або послуг.
Секторальні органи у сфері захисту критичної інфраструктури	Позитивний	
Оператори критичної інфраструктури	Позитивний	

Голова Державної служби спеціального зв’язку та захисту інформації України Юрій МИРОНЕНКО

___ _____ 2024 р.

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 2024 р. №

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

Загальні положення

1. Ці вимоги поширюються на об’єкти критичної інфраструктури I категорії критичності, крім банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжні організації, учасників платіжних систем, операторів послуг платіжної інфраструктури, державне регулювання, нагляд за діяльністю яких здійснює Національний банк України.

Управління ризиками безпеки на об’єктах критичної інфраструктури I категорії критичності здійснюється оператором критичної інфраструктури.

2. У цих вимогах терміни вживаються у такому значенні:

аналіз ризиків безпеки на об’єктах критичної інфраструктури (далі – аналіз ризиків безпеки) – визначення наслідків та їх вірогідностей стосовно ідентифікованих ризиків безпеки;

вірогідність (likelihood) – ймовірність настання ризиків та/або потенційної події протягом певного періоду часу;

джерело ризику – подія, зокрема: явище, інцидент, дія, бездіяльність або їх сукупність, які потенційно можуть спричинити ризик;

ймовірність – числова характеристика можливості того, що потенційна подія відбудеться в умовах, які можуть бути відтворені необмежену кількість разів;

звіт про виконання вимог – документ встановленої форми, який містить узагальнені відомості про управління ризиками безпеки на об’єктах критичної інфраструктури;

ліміт ризику – обмеження, встановлені оператором критичної інфраструктури для контролю величини ризиків, які впливають на надання життєво важливих функцій та/або послуг об’єктом критичної інфраструктури;

наслідок – результат події, що впливає на діяльність оператора критичної інфраструктури щодо сталого функціонування об’єкта критичної інфраструктури;

оцінювання ризиків безпеки на об’єктах критичної інфраструктури (далі – оцінка ризиків безпеки) – процес ідентифікування, аналізування та зіставлення

вагомості ризику з метою забезпечення ухвалення рішень, спрямованих на мінімізацію виникнення кризових ситуацій;

потенційна подія – подія, яка може статися чи не статися, може бути джерелом ризику, мати один або більше випадків реалізації, мати кілька причин та/або наслідків;

профіль ризиків безпеки об’єкта критичної інфраструктури – сукупність властивих об’єкту критичної інфраструктури ризиків безпеки;

ризик – потенційна можливість виникнення небажаних наслідків потенційної події, яка визначається вірогідністю, джерелами реалізації та пов'язаними з ними наслідками;

ризик безпеки на об’єктах критичної інфраструктури (далі – ризик безпеки) – потенційна можливість порушення стану захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість об’єктів критичної інфраструктури;

система управління ризиками безпеки на об’єктах критичної інфраструктури (далі – система управління ризиками безпеки) – це комплекс процесів та заходів із забезпечення безпеки та стійкості критичної інфраструктури, спрямованих на забезпечення функціональності, безперервності роботи, відновлюваності, цілісності і стійкості об’єктів критичної інфраструктури;

суттєвий ризик – це ризик, який значною мірою перевищує ліміт ризику;

управління ризиками безпеки на об’єктах критичної інфраструктури (далі – управління ризиками безпеки) – процес прийняття рішень з оброблення ризиків безпеки на підставі аналізу ризиків безпеки та організації заходів, які направлені на запобігання виникнення інциденту безпеки критичної інфраструктури та мінімізацію можливих наслідків у разі його настання.

Інші терміни вживаються у значенні, наведеному у Законі України «Про критичну інфраструктуру».

Завдання, права та обов’язки операторів критичної інфраструктури

3. Для забезпечення стійкості критичної інфраструктури оператор критичної інфраструктури:

оцінює та визначає необхідний для сталого функціонування об’єкта критичної інфраструктури персонал (працівників);

забезпечує підготовку та навчання персоналу;

здійснює заходи щодо забезпечення належними умовами праці на об’єкті критичної інфраструктури, зокрема для тривалого перебування в робочих приміщеннях;

визначає технічні засоби електронних комунікацій для оповіщення та інформування персоналу (працівників).

4. Оператор критичної інфраструктури забезпечує інтеграцію управління

ризиками безпеки шляхом:

впровадження системи управління ризиками безпеки (проєктування, впровадження, оцінка та постійне вдосконалення системи управління ризиками безпеки тощо);

розробки та затвердження документів (політики, регламенту, процедури), які встановлюють підхід до управління ризиками безпеки;

забезпечення необхідними ресурсами в частині управління ризиками безпеки;

визначення відповідального підрозділу з управління ризиками/головного ризик-менеджера (за наявності) (далі – відповідальний з управління ризиками). У разі якщо оператором критичної інфраструктури не забезпечено створення та діяльність відповідального з управління ризиками, його функції виконує керівник оператора критичної інфраструктури;

розподіл повноважень, відповідальності та підзвітності на відповідних рівнях в організації (рівень відповідального з управління ризиками, керівника оператора критичної інфраструктури, вищих органів управління (за наявності).

5. Відповідальний з управління ризиками забезпечує:

1) своєчасне виявлення, моніторинг, контроль та звітування керівнику оператора критичної інфраструктури щодо ризиків безпеки;

2) моніторинг, контроль наближення величини ризиків безпеки до лімітів ризику;

3) підготовку звітів про виконання вимог;

4) розробку та затвердження методик та інших документів для аналізу впливу різних факторів ризиків;

5) вимірювання ризиків;

6) складання профілю ризиків безпеки об’єктів критичної інфраструктури оператора критичної інфраструктури;

7) підготовку висновків щодо ідентифікованих і задокументованих ризиків безпеки;

8) розробку внутрішніх документів з питань управління ризиками безпеки.

Вимоги до розробки об’єктового плану заходів щодо забезпечення безпеки та стійкості критичної інфраструктури

6. Оператор критичної інфраструктури на підставі аналізу ризиків безпеки повинен розробити та затвердити об’єктовий план заходів щодо забезпечення безпеки та стійкості критичної інфраструктури (далі – план), який повинен включати:

визначення суттєвих ризиків;

план мінімізації ризиків для запобігання інцидентів та критичних ситуацій, де має бути враховано ризики для активів критичної інфраструктури.

7. Оператор критичної інфраструктури повинен зазначити в плані та забезпечити:

1) персонал (працівників) альтернативним робочим приміщенням (альтернативним місцем розташування) у разі відсутності постійних робочих приміщень. Для цього оператор критичної інфраструктури оцінює особливості об’єкта критичної інфраструктури;

2) визначення відповідної інфраструктури (альтернативне місце розташування), яка розташована щонайменше на відстані 50 кілометрів від існуючої інфраструктури та придатна для забезпечення життєво важливих функцій та/або послуг;

3) розроблення процедури переміщення персоналу (працівників) та технологічного обладнання (далі – обладнання) на альтернативні робочі місця, визначаючи необхідні засоби та заходи;

4) визначення можливості залучення персоналу (працівників), обладнання та матеріально-технічних ресурсів, наявних в альтернативному місці;

5) визначення обладнання та матеріально-технічних ресурсів, необхідних для надання життєво важливих функцій та/або послуг, включно з:

переліком критичних елементів об’єкта критичної інфраструктури та матеріально-технічних засобів;

визначенням альтернатив критичних елементів об’єкта критичної інфраструктури та матеріально-технічних засобів, можливостей заміни;

забезпеченням безперебійності роботи у разі втрати обладнання та матеріально-технічних засобів;

забезпеченням здійснення ремонтних робіт, оновлення, вдосконалення або створення альтернатив обладнання (включаючи зміну зовнішніх постачальників);

своєчасним резервним копіюванням інформаційних ресурсів із інформаційних, інформаційно-комунікаційних та інших систем, а також резервування програмних та апаратних компонентів для забезпечення доступу до даних, систем і процесів;

дублюванням підключення електропостачання інформаційних,

інформаційно-комунікаційних систем та обладнання до системи автономного електропостачання;

6) організацію надання електронних комунікаційних послуг та енергопостачання на постійних та альтернативних робочих місцях;

7) визначення ресурсів необхідних для сталого функціонування критичної інфраструктури, а також способів їх постачання;

8) стабільність поставок, зокрема:

визначити важливих для забезпечення надання життєво важливих функцій та/або послуг об'єктів критичної інфраструктури постачальників та їх географічне розташування, оцінити їх фінансову надійність з метою виявлення вразливостей у разі порушення постачання товарів, послуг та продукції, визначення можливих альтернатив;

розподілити ризики постачання товарів, послуг та продукції, уникнувши залежності лише від одного постачальника;

забезпечити відповідність постачання послуг, товарів та продукції національному законодавству, в тому числі моніторингом дотримання спеціальних економічних та інших обмежувальних заходів (санкцій);

9) визначення алгоритму дій під час кризової ситуації, включно із заходами:

забезпечення надання життєво важливих функцій та/або послуг;

визначення порядку оповіщення та інформування персоналу (працівників);

визначення порядку та правил дій групи антикризового управління, а також механізм координації з секторальним органом у сфері захисту критичної інфраструктури, функціональними органами у сфері захисту критичної інфраструктури та уповноваженим органом у сфері захисту критичної інфраструктури України;

визначення протоколу кризової комунікації, що включає засоби та заходи комунікації для структурних підрозділів оператора критичної інфраструктури та суб'єктів національної системи захисту критичної інфраструктури;

визначення процедури оперативного реагування на інциденти шляхом впровадження процедур та протоколів кризового менеджменту.

Підпункти 1 – 4 цього пункту зазначаються в плані та забезпечується за можливості здійснення відповідних заходів.

8. План повинен також передбачити перевірку та визначення ефективності системи управління ризиками безпеки, включаючи навчання у співпраці з секторальним органом у сфері захисту критичної інфраструктури, функціональними органами у сфері захисту критичної інфраструктури та уповноваженим органом у сфері захисту критичної інфраструктури України не рідше одного разу на три роки.

9. План та зміни до плану затверджуються оператором критичної інфраструктури.

Вимоги до системи управління ризиками безпеки

10. Система управління ризиками безпеки повинна відповідати наступним вимогам:

інтегрованість – управління ризиками є невід'ємною частиною всієї діяльності оператора критичної інфраструктури;

структурованість і комплексність – підхід до управління ризиками сприяє послідовним і порівнюваним результатам;

індивідуальність – структура та процес управління ризиками адаптовані та пропорційні зовнішньому та внутрішньому контексту оператора критичної інфраструктури, пов’язаному з його цілями;

динамічність – реагування на зміну зовнішнього і внутрішнього контексту;

належна поінформованість – вхідні дані для управління ризиками безпеки базуються на попередній та поточній інформації, а також на майбутніх очікуваннях;

управління людським фактором – професійні навички, знання, фізичні здібності та соціально-психологічні відносини персоналу, що впливають на стійке функціонування об’єктів критичної інфраструктури.

11. Ризики безпеки включають, зокрема:

1) матеріальні ризики, до яких відносяться фізичні та природні ризики для частин активів, критичних для функціонування об’єкта критичної інфраструктури (фізичний доступ до об’єкта критичної інфраструктури, об’єктів інфраструктури, систем, їх частин), в тому числі аварія, катастрофа, епідемія, стихійне лихо, епізоотія, епіфітотія, пожежа, застосування засобів ураження, що призвели або можуть призвести до людських і матеріальних втрат;

2) ризики кібербезпеки та інформаційної безпеки – ризики для об’єктів критичної інформаційної інфраструктури, які забезпечують стале функціонування об’єкта критичної інфраструктури;

3) ризики, пов’язані з людським фактором – ризики, які створює персонал (працівники) об’єкта критичної інфраструктури;

4) ризики ланцюжка постачання – ризик зриву, злочинного або ненавмисного використання постачання послуг, товарів та продукції, що призводить до порушення стійкості критичної інфраструктури;

5) ризики, пов’язані з процесами – ризик втрат через неадекватну або неспроможну систему управління технологічними процесами об’єктів критичної інфраструктури.

Оператор критичної інфраструктури визначає ризики безпеки з обов’язковим урахуванням визначеного цим пунктом вимог переліком, а також інших суттєвих ризиків, які можуть впливати на забезпечення функціональності, безперервності роботи, відновлюваності, цілісності і стійкості критичної інфраструктури.

12. Управління ризиками безпеки здійснюється у такому порядку:

організація управління ризиками безпеки;

оцінювання ризиків безпеки;

оброблення ризиків безпеки;

моніторинг та перегляд актуальності ризиків безпеки;

обмін інформацією та взаємодія із суб’єктами національної системи захисту критичної інфраструктури.

13. Організація управління ризиками безпеки включає:

визначення вихідних даних щодо функціонування об’єкта критичної інфраструктури (область застосування, внутрішні і зовнішні чинники, критерії щодо управління ризиками безпеки, ліміти ризиків);

визначення суб’єктів національної системи захисту критичної інфраструктури, які виконують завдання/заходи щодо управління ризиками безпеки;

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

визначення методів, інструментів та механізмів, які використовуються в ході управління ризиками безпеки;

ідентифікацію та планування ресурсів, необхідних для управління ризиками безпеки, зокрема людські, інформаційні, фінансові, матеріально-технічні;

визначення засобів та заходів щодо забезпечення комунікації в ході управління ризиками безпеки, в тому числі взаємодія з суб’єктами національної системи захисту критичної інфраструктури;

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

Управління ризиками безпеки здійснюється із застосуванням національних та міжнародних стандартів управління ризиками безпеки.

Оцінювання ризиків безпеки передбачає визначення вірогідності, джерел ризиків, характеристик потенційних подій безпеки критичної інфраструктури, ймовірності та вагомості їх наслідків і сценаріїв розвитку, а також методів управління ризиками та їх ефективності.

У ході оцінювання ризиків безпеки проводяться:

ідентифікування ризиків безпеки;

аналізування ризиків безпеки;

зіставлення ризиків безпеки впровадженим рішенням щодо їх оброблення.

14. Ідентифікування ризиків безпеки передбачає визначення всіх потенційно можливих подій, які можуть спричинити негативні наслідки на функціонування об’єкта критичної інфраструктури та документуванні показників (характеристик) та сценаріїв їх розвитку.

Ідентифікування ризиків безпеки проводиться шляхом:

складання переліку ризиків безпеки;

формування сценаріїв розвитку інцидентів;

ідентифікації найбільш вірогідних для даного об’єкта критичної інфраструктури ризиків безпеки.

15. Аналізування ризиків безпеки передбачає вивчення ідентифікованих ризиків безпеки з метою визначення показників – вірогідності та наслідків потенційних подій.

Аналізування ризиків безпеки проводиться шляхом:

визначення причин та джерел виникнення ризиків безпеки;

визначення вірогідності та наслідків ідентифікованих ризиків безпеки на підставі отриманих кількісних, якісних або комбінованих характеристик ризиків безпеки;

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

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

16. Зіставлення ризиків безпеки варіантам рішень щодо їх оброблення передбачає порівняння результатів аналізу ризиків безпеки рішенням, які можуть бути прийняті щодо управління такими ризиками.

17. Зіставлення ризиків безпеки передбачає визначення завдань (заходів), які направлені на зниження (виключення) ймовірності інциденту критичної інфраструктури та мінімізацію можливих наслідків такого інциденту.

Оброблення ризиків безпеки проводиться шляхом:

визначення підходів до обробки кожного ідентифікованого ризику безпеки;

визначення прийнятних (не потребують додаткових заходів для мінімізації наслідків та ймовірності їх настання) та неприйнятних ризиків безпеки;

формування переліку альтернативних заходів протидії ризикам;

визначення найбільш ефективного заходу протидії ризикам безпеки, зокрема з урахуванням необхідних ресурсів;

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

підготовки об’єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, а також планів захисту об’єкта критичної інфраструктури, що є невід’ємною складовою паспорта безпеки на об’єкт критичної інфраструктури.

18. Моніторинг та перегляд актуальності ризиків безпеки передбачає забезпечення оператора критичної інфраструктури актуальною, об’єктивною та достовірною інформацією з питань, що відносяться до управління ризиками безпеки.

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

перевірки актуальності інформації щодо стану захищеності об’єкта критичної інфраструктури, яка зазначена в паспорті безпеки на об’єкт критичної інфраструктури;

прогнозування виникнення нових інцидентів, ступеня вразливості об’єкта критичної інфраструктури та результатів наслідків впливу;

відстеження загальної ситуації в системі управління ризиками безпеки.

19. 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, 2022 р., № 84, ст. 5184).

Звітування

20. Оператори критичної інфраструктури подають 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 до 30 січня кожного року за попередній.

21. Секторальні органи у сфері захисту критичної інфраструктури подають уповноваженому органу у сфері захисту критичної інфраструктури України звіт про виконання вимог щодо управління ризиками безпеки на об’єктах критичної інфраструктури I категорії критичності за формою згідно з додатком 2 до 15 лютого кожного року за попередній.

Проект

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 2024 р. №

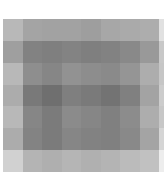
Київ

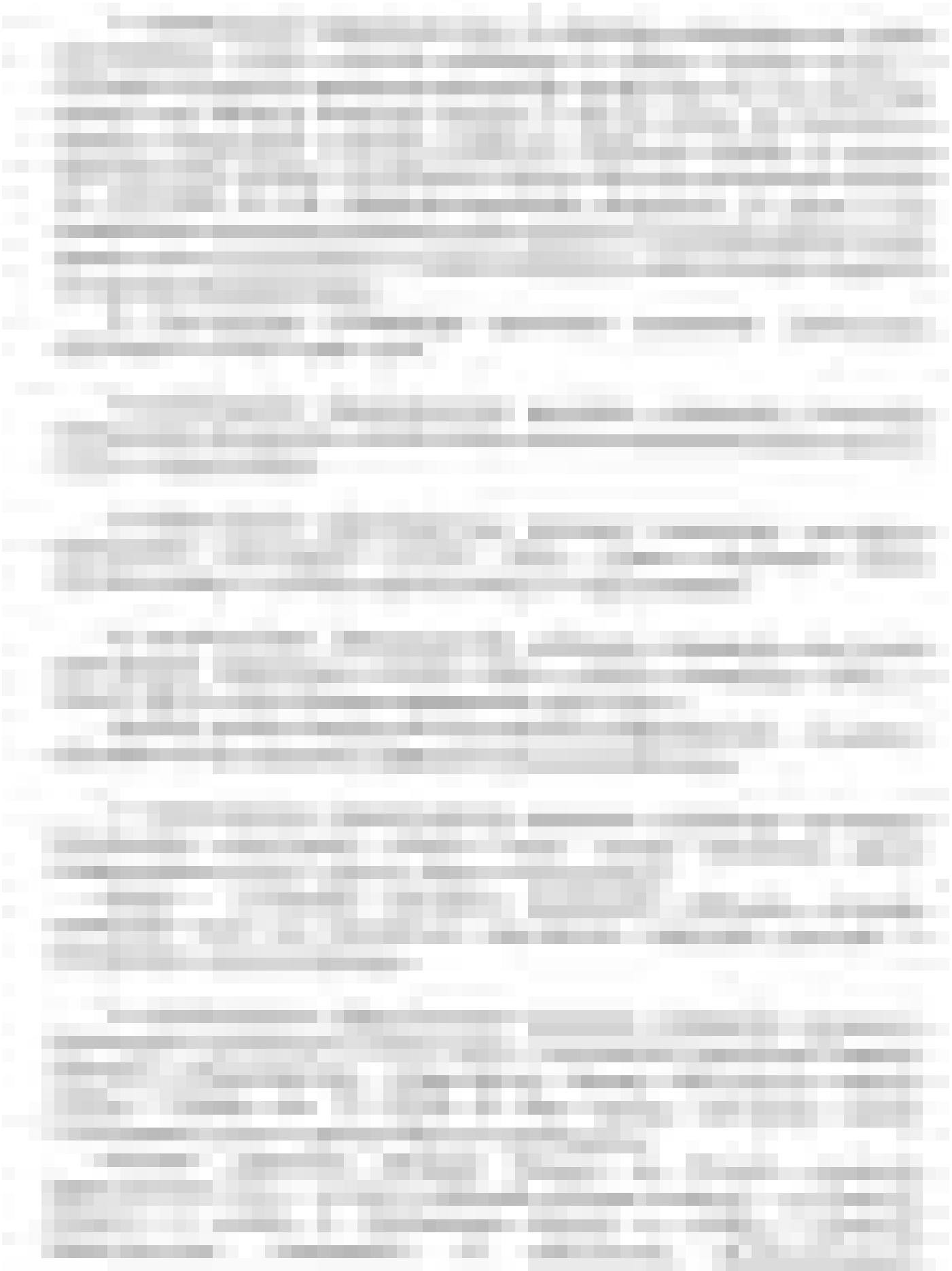
Про затвердження вимог щодо управління ризиками безпеки на об’єктах критичної інфраструктури I категорії критичності

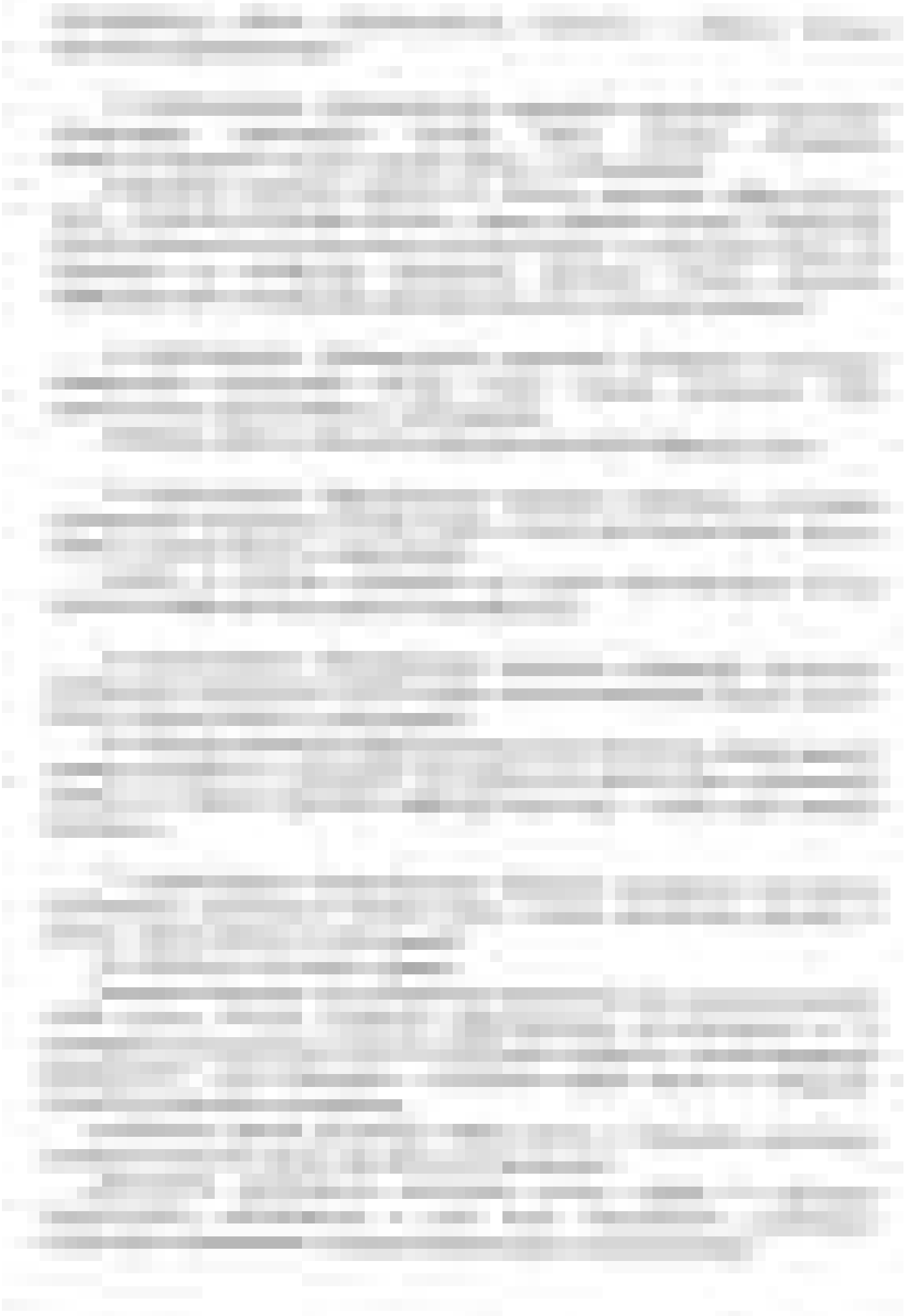
Відповідно до абзацу другого частини першої статті 22 Закону України «Про критичну інфраструктуру» Кабінет Міністрів України **постановляє:**

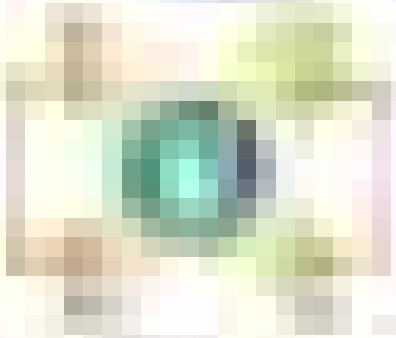
Затвердити вимоги щодо управління ризиками безпеки на об’єктах критичної інфраструктури I категорії критичності, що додаються.

Прем'єр-міністр України **Д. ШМИГАЛЬ**









Прим. № ___

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
до проєкту постанови Кабінету Міністрів України «Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності»

І. Визначення проблеми

Відповідно до абзацу п'ятого пункту 1 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03.09.2014 № 411, Адміністрація Держспецзв'язку є центральним органом виконавчої влади, який забезпечує здійснення Держспецзв'язку повноважень уповноваженого органу у сфері захисту критичної інфраструктури під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування, передбачених Законом України «Про критичну інфраструктуру» (далі – Закон).

Абзацом другим частини першої статті 22 Закону визначено, що Кабінет Міністрів України встановлює вимоги щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності, крім банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури, державне регулювання, нагляд за діяльністю яких здійснює Національний банк України, та встановлює вимоги щодо управління ризиками безпеки.

Реалізація державної політики у сфері захисту критичної інфраструктури спрямована на ефективне зниження і контроль за ризиками безпеки на об'єктах критичної інфраструктури, зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів (пункт 4 частини другої статті 4 Закону).

До завдань під час формування і реалізації державної політики у сфері захисту критичної інфраструктури належить розроблення комплексу заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об'єктах критичної інфраструктури (пункт 6 частини другої статті 5 Закону).

Крім того, пунктом 3 частини першої статті 21 Закону визначено, що основними завданнями операторів критичної інфраструктури, зокрема є проведення оцінки ризиків на об'єктах критичної інфраструктури, а також обмін інформацією про ризики та загрози з іншими суб'єктами національної системи захисту критичної інфраструктури.

Однак, наразі відсутні механізми, що регулюють діяльність операторів критичної інфраструктури в частині управління ризиками безпеки на об'єктах критичної інфраструктури.

Слід зазначити, що постановою Правління Національного банку України від 11.06.2018 № 64 затверджено Положення про організацію системи управління ризиками в банках України та банківських групах.

Враховуючи викладене, Адміністрацією Держспецзв'язку розроблено проєкт постанови Кабінету Міністрів України «Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності» (далі – проєкт постанови, регуляторний акт) з метою виконання вимог Закону та на виконання пункту 3 доручення Першого віце-прем'єр-міністра України – Міністра економіки України від 31.03.2023 № 18009/2/1-22 до листа Адміністрації Держспецзв'язку від 17.03.2023 № 07/01/02-1606/ВС.

Прийняття постанови дозволить визначити комплекс заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів.

Основні групи (підгрупи), на які проблема впливає:

Групи (підгрупи)	**Так**	**Ні**
Громадяни	-	+
Держава	+	-
Суб'єкти господарювання,	+	-
у тому числі суб'єкти малого підприємництва	-	+

Зазначена проблема не може бути розв'язана за допомогою ринкових механізмів, оскільки вона стосується управління ризиками безпеки на об'єктах критичної інфраструктури, крім банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжних організації, учасників платіжних систем, операторів послуг платіжної інфраструктури, державне регулювання, нагляд за діяльністю яких здійснює Національний банк України.

Проблема не може бути розв'язана за допомогою чинних регуляторних актів, оскільки на сьогодні вона не врегульована жодними іншими нормативно-правовими актами.

II. Цілі державного регулювання

Основною ціллю проєкту постанови є встановлення вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	**Опис альтернативи**
Альтернатива 1	*Залишення існуючої на цей момент ситуації без змін:* є неприйнятною, оскільки не забезпечить досягнення поставленої цілі регулювання

Альтернатива 2	*Прийняття регуляторного акта:* дозволить нормативно врегулювати питання стосовно встановлення вимог щодо управління ризиками безпеки на об’єктах критичної інфраструктури I категорії критичності та забезпечить досягнення поставленої цілі регулювання

2. Оцінка вибраних альтернативних способів досягнення цілей.

Оцінка впливу на сферу інтересів держави

Вид альтернативи	**Вигоди**	**Витрати**
Альтернатива 1	Немає	Додаткових витрат не потребує
Альтернатива 2	Дозволить нормативно врегулювати питання щодо встановлення вимог управління ризиками безпеки на об’єктах критичної інфраструктури I категорії критичності, визначить комплекс заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки, що як наслідок забезпечить безпеку та стійкість об’єктів критичної інфраструктури	Додаткових витрат не потребує

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	**Вигоди**	**Витрати**
Альтернатива 1	Немає	Немає
Альтернатива 2	Немає	Немає

Оцінка впливу на сферу інтересів суб’єктів господарювання

Показник	**Великі**	**Середні**	**Малі**	**Мікро**	**Разом**
Кількість суб’єктів господарювання, що підпадають під дію регулювання, одиниць	усі*	усі*	-	-	усі*
Питома вага групи у загальній кількості, відсотків	100%	100%	-	-	X

*У таблиці взято до уваги всіх операторів критичної інфраструктури, що на правах власності, оренди або на інших законних підставах здійснюють управління об’єктами критичної інфраструктури І категорії критичності. Водночас Закон, постанова Кабінету Міністрів України від 09.10.2020 № 1109 та Порядок ведення Реєстру об’єктів критичної інфраструктури, включення таких об’єктів до Реєстру, доступу та надання інформації з нього, затверджений постановою Кабінету Міністрів України від 28.04.2023 № 415, не містять вимог, відповідно до яких зазначених суб’єктів господарювання можна поділити на «великі», «середні», «малі» та «мікро». Однак, відповідно до пункту 1 частини другої статті 10 Закону І категорія критичності – особливо важливі об’єкти, які мають загальнодержавне значення, значний вплив на інші об’єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації державного значення.

Вид альтернативи	**Вигоди**	**Витрати**
Альтернатива 1	Немає	Додаткових витрат не потребує
Альтернатива 2	Дозволить нормативно врегулювати питання щодо встановлення вимог управління ризиками безпеки на об’єктах критичної інфраструктури І категорії критичності, визначить комплекс заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки, що як наслідок забезпечить безпеку та стійкість об’єктів критичної інфраструктури	Додаткових витрат не потребує

Сумарні витрати за альтернативами	**Сума витрат, гривень**
Альтернатива 1. Сумарні витрати для суб’єктів господарювання великого і середнього підприємництва згідно з додатком 2 до Методики проведення аналізу впливу регуляторного акта	Додаткових витрат не потребує
Альтернатива 2. Сумарні витрати для суб’єктів господарювання великого і середнього підприємництва згідно з додатком 2 до Методики проведення аналізу впливу регуляторного акта	Додаткових витрат не потребує

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	**Бал результативності** (за чотирибальною системою оцінки)	**Коментарі щодо присвоєння відповідного бала**
Альтернатива 1	1	Цілі прийняття регуляторного акта не можуть бути досягнуті (проблема продовжить існувати)
Альтернатива 2	4	Зазначений спосіб є найбільш доцільним та дасть змогу визначити вимоги щодо управління ризиками безпеки на об’єктах критичної інфраструктури І категорії критичності (проблема більше існувати не буде)

Рейтинг результативності	**Вигоди (підсумок)**	**Витрати (підсумок)**	**Обґрунтування відповідного місця альтернативи у рейтингу**
Альтернатива 1	Немає	Додаткових витрат не потребує	Продовження існування проблеми
Альтернатива 2	Визначення комплексу заходів, спрямованих на управління ризиками безпеки	Додаткових витрат не потребує	Проблема більше існувати не буде

Рейтинг	**Аргументи щодо переваги обраної альтернативи/причини відмови від альтернативи**	**Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта**
Альтернатива 1	Альтернатива є неприйнятною, оскільки не відповідає поставленим цілям	Х
Альтернатива 2	Прийняття регуляторного акта є найбільш обґрунтованим та ефективним способом досягнення поставлених цілей	немає

V. Механізми та заходи, які забезпечать розв’язання визначеної проблеми

Механізмом, який забезпечить розв’язання визначеної проблеми, є прийняття регуляторного акту та, як наслідок:

визначення комплексу заходів, спрямованих на управління ризиками безпеки;

зниження ризику реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів.

Для впровадження регуляторного акта необхідно вжити таких організаційних заходів, як забезпечення інформування органів державної влади, органів місцевого самоврядування, юридичних та фізичних осіб про вимоги регуляторного акта шляхом оприлюднення його в засобах масової інформації, мережі Інтернет та проведення Адміністрацією Держспецзв’язку інформаційно-роз’яснювальної роботи.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

Реалізація регуляторного акта не потребує додаткових витрат із державного бюджету, матеріальних та інших витрат.

За результатами введення в дію регуляторного акта не передбачається нанесення шкоди суб’єктам господарювання.

Тест малого підприємництва не проводився, оскільки додаткових витрат для реалізації вимог постанови суб’єктами господарювання не передбачається.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Строк дії регуляторного акта не обмежений у часі, що дасть змогу повністю вирішити проблемні питання.

Зміна строку дії регуляторного акта можлива у разі зміни законодавства України у сфері захисту критичної інфраструктури.

Регуляторний акт набирає чинності з дня його офіційного опублікування.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозовані показники результативності дії регуляторного акта:

розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов’язаних з дією постанови (грн.) – не передбачається;

кількість суб’єктів господарювання та/або фізичних осіб, на які поширюватиметься дія постанови, – дія постанови поширюється на всіх операторів критичної інфраструктури, що на правах власності, оренди або на

інших законних підставах здійснюють управління об’єктами критичної інфраструктури I категорії критичності;

рівень поінформованості суб’єктів господарювання – високий, проєкт постанови розміщено на офіційному вебсайті Держспецзв’язку (https://cip.gov.ua) з метою одержання пропозицій і зауважень;

кількість звернень заінтересованих сторін щодо необхідності внесення змін до проєкту постанови;

кількість скарг суб’єктів господарювання щодо реалізації постанови;

розмір коштів і час, що витрачатимуться суб’єктами господарювання – не передбачається.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Відстеження результативності регуляторного акта буде проводитись Адміністрацією Держспецзв’язку у строки, визначені законодавством, шляхом аналізу даних щодо управління ризиками безпеки на об’єктах критичної інфраструктури I категорії критичності.

Базове відстеження результативності дії регуляторного акта здійснюватиметься через 1 рік після набрання чинності регуляторним актом шляхом збирання статистичних даних, одержаних пропозицій до нього, їх аналізу.

Повторне відстеження результативності дії регуляторного акта здійснюється в межах строків, установлених статтею 10 Закону України «Про засади державної регуляторної політики у сфері господарської діяльності», – через 2 роки з дня набрання чинності постанови.

Періодичне відстеження планується здійснювати раз на кожні три роки, починаючи з дня виконання заходів з повторного відстеження, з метою перевірки сталого досягнення регуляторним актом цілей, задекларованих під час його прийняття, після здійснення повторного відстеження результативності регуляторного акта на основі показників і даних, визначених під час проведення аналізу регуляторного впливу.

Голова Державної служби
спеціального зв’язку та
захисту інформації України Юрій МИРОНЕНКО
«___» _____ 2024 р.

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 2023 р. №

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

Загальні положення

1. Ці вимоги поширюються на об’єкти критичної інфраструктури I категорії критичності, крім банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжні організації, учасників платіжних систем, операторів послуг платіжної інфраструктури, державне регулювання, нагляд за діяльністю яких здійснює Національний банк України.

Управління ризиками безпеки на об’єктах критичної інфраструктури I категорії критичності здійснюється оператором критичної інфраструктури.

2. У цих вимогах терміни вживаються у такому значенні:

аналіз ризиків безпеки на об’єктах критичної інфраструктури (далі – аналіз ризиків безпеки) – визначення наслідків та ~~їх~~ ймовірностей їх настання стосовно ідентифікованих ризиків безпеки;

вірогідність (likelihood) – ймовірність настання ризиків та/або потенційної події протягом певного періоду часу;

джерело ризику – подія, зокрема: явище, інцидент, дія, бездіяльність або їх сукупність, які потенційно можуть спричинити ризик;

ймовірність – числова характеристика можливості того, що потенційна подія відбудеться в умовах, які можуть бути відтворені необмежену кількість разів;

європейська критична інфраструктура – це об’єкти критичної інфраструктури України, які надають життєво важливі функції та/або послуги більше ніж 6 державам членам Європейського Союзу;

звіт про виконання вимог – документ встановленої форми, який містить узагальнені відомості про управління ризиками безпеки на об’єктах критичної інфраструктури;

ліміт ризику – обмеження, встановлені оператором критичної інфраструктури для контролю величини ризиків, які впливають на надання життєво важливих функцій та/або послуг об’єктом критичної інфраструктури;

~~модель загроз безпеці об’єкта критичної інфраструктури – формалізований або неформалізований опис методів та засобів реалізації ризиків безпеки;~~

наслідок – результат події, що впливає на діяльність оператора критичної інфраструктури щодо сталого функціонування об’єкта критичної інфраструктури;

оцінка ризиків безпеки на об’єктах критичної інфраструктури (далі – оцінка ризиків безпеки) – процес ідентифікації, аналізу та оцінювання вагомості ризику з метою забезпечення ухвалення рішень, спрямованих на мінімізацію виникнення кризових ситуацій;

потенційна подія – подія, яка може статися чи не статися, може бути джерелом ризику, мати один або більше випадків реалізації, мати кілька причин та/або наслідків;

профіль ризиків - сукупність властивих певній установі видів ризиків;

ризик – потенційна можливість виникнення небажаних наслідків потенційної події, яка визначається вірогідністю, джерелами реалізації та пов'язаними з ними наслідками;

ризик безпеки на об’єктах критичної інфраструктури (далі – ризик безпеки) – потенційна можливість порушення стану захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури;

система управління ризиками безпеки на об’єктах критичної інфраструктури (далі – система управління ризиками безпеки) – це сукупність задокументованих і затверджених політики, правил, методик і процедур управління ризиками безпеки, які визначають порядок дій оператора критичної інфраструктури, спрямованих на здійснення систематичного процесу вимірювання, моніторингу, контролю, звітування та обробки ризиків безпеки, в тому числі Паспорт безпеки на об’єкт критичної інфраструктури;

управління ризиками безпеки на об’єктах критичної інфраструктури (далі – управління ризиками безпеки) – процес прийняття рішень з обробки ризиків безпеки на підставі ~~обробки~~ аналізу ризиків безпеки та організації заходів, які направлені на зниження (виключення) вірогідності~~ймовірності інциденту~~ події безпеки критичної інфраструктури та мінімізацію можливих наслідків такої~~го~~ події~~інциденту~~.

Інші терміни вживаються у значенні, наведеному у Законі України «Про критичну інфраструктуру».

Основні завдання операторів критичної інфраструктури

3. Для забезпечення стійкості критичної інфраструктури оператор критичної інфраструктури:

оцінює та визначає необхідний для сталого функціонування об’єкта критичної інфраструктури персонал (працівників) та здійснює резервування критичних співробітників~~бронювання військовозобов’язаних в порядку визначеному чинним законодавством~~;

забезпечує підготовку та навчання персоналу;

здійснює заходи щодо забезпечення належними умовами праці на об’єкті критичної інфраструктури, зокрема для тривалого перебування в робочих приміщеннях;

визначає засоби зв'язку для оповіщення та інформування персоналу

(працівників).

4. Оператор критичної інфраструктури забезпечує інтеграцію управління ризиками безпеки шляхом:

впровадження системи управління ризиками безпеки (проєктування, впровадження, оцінка та постійне вдосконалення системи управління ризиками безпеки тощо);

розробки та затвердження документів (політики, регламенту, процедури), які встановлюють підхід до управління ризиками безпеки;

забезпечення необхідними ресурсами в частині управління ризиками безпеки;

визначення відповідального підрозділу з управління ризиками/головного ризик-менеджера (за наявності) (далі – відповідальний з управління ризиками). У разі якщо оператором критичної інфраструктури не забезпечено створення та діяльність відповідального з управління ризиками, його функції виконує керівник оператора критичної інфраструктури;

розподіл повноважень, відповідальності та підзвітності на відповідних рівнях в організації (рівень відповідального з управління ризиками, керівника оператора критичної інфраструктури, вищих органів управління (за наявності).

5. Відповідальний з управління ризиками забезпечує:

1) своєчасне виявлення, моніторинг, контроль та звітування керівнику оператора критичної інфраструктури щодо ризиків безпеки;

2) моніторинг, контроль наближення величини ризиків безпеки до лімітів ризику;

3) підготовку звітів про виконання вимог;

4) розробку та затвердження методик та інших документів для аналізу впливу різних факторів ризиків;

5) вимірювання ризиків;

6) складання профілю ризиків безпеки об’єктів критичної інфраструктури оператора критичної інфраструктури;

7) підготовку висновків щодо ідентифікованих і задокументованих ризиків безпеки;

8) розробку внутрішніх документів з питань управління ризиками безпеки.

Вимоги до розробки об’єктового плану заходів щодо забезпечення безпеки та стійкості критичної інфраструктури

6. Оператор критичної інфраструктури на підставі аналізу ризиків безпеки повинен розробити та затвердити об’єктовий план заходів щодо забезпечення безпеки та стійкості критичної інфраструктури (далі – план), який повинен включати:

визначення суттєвих ризиків;

план мінімізації ризиків для запобігання інцидентів та критичних ситуацій,

де має бути враховано ризики для активів критичної інфраструктури.

7. Оператор критичної інфраструктури повинен зазначити в плані та забезпечити:

1) персонал (працівників) альтернативним робочим приміщенням (альтернативним місцем розташування) у разі відсутності постійних робочих приміщень. Для цього оператор критичної інфраструктури оцінює особливості об'єкта критичної інфраструктури;

2) визначення відповідної інфраструктури (альтернативне місце розташування), яка розташована щонайменше на відстані 50 кілометрів від існуючої інфраструктури та придатна для забезпечення життєво важливих функцій та/або послуг;

3) розроблення процедури переміщення персоналу (працівників) та технологічного обладнання (далі – обладнання) на альтернативні робочі місця, визначаючи необхідні засоби та заходи;

4) визначення можливості залучення персоналу (працівників), обладнання та матеріально-технічних ресурсів, наявних в альтернативному місці;

5) визначення обладнання та матеріально-технічних ресурсів, необхідних для надання життєво важливих функцій та/або послуг, включно з:

переліком критичних елементів об'єкта критичної інфраструктури та матеріально-технічних засобів;

визначенням альтернатив критичних елементів об'єкта критичної інфраструктури та матеріально-технічних засобів, можливостей заміни;

забезпеченням безперебійності роботи у разі втрати обладнання та матеріально-технічних засобів;

забезпеченням здійснення ремонтних робіт, оновлення, вдосконалення або створення альтернатив обладнання (включаючи зміну зовнішніх постачальників);

своєчасним резервним копіюванням інформаційних, інформаційно-комунікаційних та інших систем і резервування обладнання для забезпечення доступу до даних, систем і процесів;

дублюванням підключення електропостачання інформаційних, інформаційно-комунікаційних систем та обладнання до системи автономного електропостачання;

6) організацію зв'язку та енергопостачання на постійних та альтернативних робочих місцях;

7) визначення ресурсів необхідних для сталого функціонування критичної інфраструктури, а також способів їх постачання;

8) стабільність поставок, зокрема:

визначити ланцюги поставок, зокрема для критичних процесів

визначити головних постачальників та їх географічне розташування, оцінити їх фінансову надійність та з метою виявлення вразливостей у разі порушення ланцюгів постачання та визначення можливих альтернатив;

розподілити ризики постачання, уникнувши залежності лише від одного

іноземного постачальника;

забезпечити відповідність ланцюгів постачання національному законодавству, в тому числі моніторингом дотримання спеціальних економічних та інших обмежувальних заходів (санкцій)~~не залучати до ланцюгів постачання суб'єктів господарювання, до яких застосовано спеціальні економічні та інші обмежувальні заходи (санкції)~~;

визначити можливість надання переваги національним ланцюгам постачання та національним виробникам, переробникам і постачальникам послуг;

9) визначення алгоритму дій під час кризової ситуації, включно з заходами:

забезпечення надання життєво важливих функцій та/або послуг;

визначення порядку зв'язку з персоналом (працівниками);

визначення порядку та правил дій групи антикризового управління, а також механізм координації з секторальним органом у сфері захисту критичної інфраструктури, функціональними органами у сфері захисту критичної інфраструктури та уповноваженим органом у сфері захисту критичної інфраструктури України;

визначення протоколу кризової комунікації, що включає засоби та заходи комунікації для структурних підрозділів оператора критичної інфраструктури та суб'єктів національної системи захисту критичної інфраструктури;

визначення процедури оперативного реагування на інциденти шляхом впровадження процедур та протоколів кризового менеджменту.

Підпункти 1 – 4 цього пункту зазначаються в плані та забезпечуються за можливості здійснення відповідних заходів.

8. План повинен також передбачити перевірку та визначення ефективності системи управління ризиками безпеки, включаючи навчання у співпраці з секторальним органом у сфері захисту критичної інфраструктури, функціональними органами у сфері захисту критичної інфраструктури та уповноваженим органом у сфері захисту критичної інфраструктури України не рідше одного разу на три роки.

9. План та зміни до плану затверджуються оператором критичної інфраструктури.

Вимоги до системи управління ризиками безпеки

10. Система управління ризиками безпеки повинна відповідати наступним вимогам:

інтегрованість – управління ризиками є невід'ємною частиною всієї діяльності оператора критичної інфраструктури;

структурованість і комплексність - підхід до управління ризиками сприяє послідовним і порівнюваним результатам;

індивідуальність – структура та процес управління ризиками адаптовані та пропорційні зовнішньому та внутрішньому контексту оператора критичної

інфраструктури, пов’язаному з його цілями;

динамічність – реагування на зміну зовнішнього і внутрішнього контексту;

належна поінформованість – вхідні дані для управління ризиками безпеки базуються на попередній та поточній інформації, а також на майбутніх очікуваннях;

управління людським фактором – професійні навички, знання, фізичні здібності та соціально-психологічні відносини персоналу, що впливають на стійке функціонування об’єктів критичної інфраструктури.

11. Ризики безпеки включають, зокрема:

1) матеріальні ризики, до яких відносяться фізичні та природні ризики для частин активів, критичних для функціонування об’єкта критичної інфраструктури (фізичний доступ до об’єкта критичної інфраструктури, об’єктів інфраструктури, систем, їх частин), в тому числі аварія, катастрофа, епідемія, стихійне лихо, епізоотія, епіфітотія, пожежа, застосування засобів ураження, що призвели або можуть призвести до людських і матеріальних втрат;

2) ризики кібербезпеки та інформаційної безпеки – ризики для об’єктів критичної інформаційної інфраструктури, які забезпечують стале функціонування об’єкта критичної інфраструктури;

3) ризики, пов’язані з людським фактором – ризики, які створює персонал (працівники) об’єкта критичної інфраструктури;

4) ризики ланцюжка постачання – ризик зриву, злочинного або ненавмисного використання ланцюгів постачання, що призводить до порушення стійкості критичної інфраструктури.

Оператор критичної інфраструктури визначає ризики безпеки з обов’язковим урахуванням визначеного цим пунктом вимог переліком, а також інших суттєвих ризиків, які можуть впливати на забезпечення функціональності, безперервності роботи, відновлюваності, цілісності і стійкості критичної інфраструктури.

12. Управління ризиками безпеки здійснюється у такому порядку:

організація управління ризиками безпеки;

оцінка ризиків безпеки;

обробка ризиків безпеки;

моніторинг та перегляд актуальності ризиків безпеки;

обмін інформацією та взаємодія із суб’єктами національної системи захисту критичної інфраструктури.

13. Організація управління ризиками безпеки включає:

визначення вихідних даних щодо функціонування об'єкту критичної інфраструктури (область застосування, внутрішні і зовнішні чинники, критерії щодо управління ризиками безпеки, ліміти ризиків безпеки);

визначення суб’єктів національної системи захисту критичної інфраструктури, які виконують завдання/заходи щодо управління ризиками

безпеки;

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

визначення методів, інструментів та механізмів, які використовуються в ході управління ризиками безпеки;

ідентифікацію та планування ресурсів, необхідних для управління ризиками безпеки, зокрема людські, інформаційні, фінансові, матеріально-технічні;

визначення засобів та заходів щодо забезпечення комунікації в ході управління ризиками безпеки, в тому числі взаємодія з суб'єктами національної системи захисту критичної інфраструктури;

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

Управління ризиками безпеки здійснюється із застосуванням національних та міжнародних стандартів управління ризиками безпеки.

Оцінка ризиків безпеки передбачає визначення вірогідності, джерел ризиків, характеристик ~~інцидентів~~ потенційних подій безпеки критичної інфраструктури, ймовірності та вагомості їх наслідків і сценаріїв розвитку, а також методів управління ризиками та їх ефективності.

У ході оцінки ризиків безпеки проводяться:

ідентифікація ризиків безпеки;

аналіз ризиків безпеки;

~~**оцінка відповідності ризиків безпеки варіантам рішень щодо їх обробки, у тому числі планам захисту об'єктів критичної інфраструктури.**~~

[14.] Ідентифікація ризиків безпеки передбачає визначення всіх потенційно можливих ~~інцидентів~~подій, які можуть спричинити~~мати~~ негативні~~ий~~ наслідки~~вплив~~ на функціонування об'єкта критичної інфраструктури та документуванні показників (характеристик) та сценаріїв їх розвитку.

Ідентифікація ризиків безпеки проводиться шляхом:

складання переліку ризиків безпеки;

формування сценаріїв розвитку інцидентів;

ідентифікації найбільш вірогідних для даного об'єкта критичної інфраструктури показників ризику безпеки.

[15.] Аналіз ризиків безпеки передбачає вивчення ідентифікованих ризиків безпеки з метою визначення показників – вірогідності та наслідків потенційних подій.~~щодо рівня їх потенційної загрози та можливого впливу на функціонування об'єкта критичної інфраструктури~~.

Аналіз ризиків безпеки проводиться шляхом:

визначення причин та джерел виникнення ризиків безпеки;

визначення вірогідності та ~~впливу~~ наслідків ідентифікованих ризиків безпеки на підставі отриманих кількісних, якісних або комбінованих характеристик ризиків безпеки;

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

~~Під час аналізу ризиків безпеки необхідно попередньо прийняти рішення, які ризики обробляти, при цьому відхилити незначні ризики, оброблення яких недоцільне.~~

Аналіз ризиків безпеки здійснюється на основі аналізу досвіду суб'єктів національної системи захисту критичної інфраструктури, у разі наявності, та аналізу рішень прийнятих внаслідок інцидентів, які виникали раніше, методів математичного моделювання.

14.[16.] ~~Оцінка відповідності ризиків безпеки варіантам рішень щодо їх обробки передбачає визначення відповідності результатів аналізу ризиків безпеки рішенням, які можуть бути прийняті щодо управління такими ризиками.~~

15.[17.] **Обробка ризиків безпеки передбачає визначення завдань (заходів), які направлені на зниження (виключення) ймовірності інциденту критичної інфраструктури та мінімізацію можливих наслідків такого інциденту.**

Обробка ризиків безпеки проводиться шляхом прийняття рішення щодо оцінених ризиків з наступного переліку з визначенням найбільш ефективного заходу протидії ризикам безпеки, зокрема з урахуванням необхідних ресурсів

1)Прийняття ризиків за результатами аналізу (не потребують додаткових заходів для мінімізації наслідків та ймовірності їх настання)

2)Уникнення ризиків (зокрема, припинення діяльності об'єкта, співпраці з постачальниками, використання ресурсів, тощо);

3)Пом'якшення ризиків, включаючи
забезпечення ресурсами об'єктового плану заходів щодо забезпечення безпеки та стійкості критичної інфраструктури;
формування переліку альтернативних заходів протидії ризикам;

4)Передачу ризиків (зокрема, страхування наслідків або угода про спільну відповідальність за наслідки з постачальником)**:**

~~[4)] створення моделі загроз безпеці об'єкта критичної інфраструктури;~~

~~[5)] визначення підходів до обробки кожного ідентифікованого ризику безпеки;~~

~~[6)] визначення прийнятних (не потребують додаткових заходів для мінімізації наслідків та ймовірності їх настання) та неприйнятних ризиків безпеки;~~

~~[7)] формування переліку альтернативних заходів протидії ризикам;~~

~~[8)] визначення найбільш ефективного заходу протидії ризикам безпеки, зокрема з урахуванням необхідних ресурсів;~~

[9)] **Ввизначення супутніх ризиків безпеки, які можуть виникнути у зв'язку із запровадженням додаткових заходів протидії ризикам безпеки та проведення їх аналізу.**~~;~~

В результаті прийняті рішення про обробку ризиків є основою для підготовки об’єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, а також планів захисту об’єкта критичної інфраструктури, що є невід’ємною складовою паспорта безпеки на об’єкт критичної інфраструктури.~~підготовки об’єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, а також планів захисту об’єкта критичної інфраструктури, що є невід’ємною складовою паспорта безпеки на об’єкт критичної інфраструктури.~~

16.[18.] **Моніторинг та перегляд актуальності ризиків безпеки передбачає забезпечення оператора критичної інфраструктури актуальною, об’єктивною та достовірною інформацією з питань, що відносяться до управління ризиками безпеки.**

Перегляд актуальності ризиків безпеки проводиться не рідше ніж раз на три роки шляхом:

перевірки актуальності інформації щодо стану захищеності об’єкта критичної інфраструктури, яка зазначена в паспорті безпеки на об’єкт критичної інфраструктури;

прогнозування виникнення нових інцидентів, ступеня вразливості об’єкта критичної інфраструктури та результатів наслідків впливу;

відстеження загальної ситуації в системі управління ризиками безпеки.

17.[19.] **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, 2022 р., № 84, ст. 5184).**

Звітування

18.[20.] **Секторальні органи у сфері захисту критичної інфраструктури подають уповноваженому органу у сфері захисту критичної інфраструктури України звіт про виконання вимог за формою згідно з додатком 1 до 15 лютого кожного року за попередній.**

19.[21.] **Оператори критичної інфраструктури подають секторальним органам у сфері захисту критичної інфраструктури звіт про виконання вимог за формою згідно з додатком 2 до 30 січня кожного року за попередній.**

Домен: Аналіз, спрямування та моніторинг **Ціль корпоративного управління: EDM03 — Забезпечена оптимізація ризиків**	**Сфера діяльності:** **Модель ядра COBIT**
Опис	
Забезпечити, що ризик апетит та толерантність до ризику є зрозумілі, викладені та поширені, та що ризик для цінності організації, пов'язаний з використанням I&T, ідентифікований та керований.	
Задача	
Забезпечити, що ризик організації, пов'язаний з I&T, не перевищує ризик апетит та рівень толерантності до ризику організації, вплив ризику I&T на цінність організації ідентифікований та керований, а можливості для виникнення випадків невідповідності мінімізуються.	
Ціль корпоративного управління підтримує досягнення набору початкових та цілей узгодження організації:: :	

Цілі організації		**Цілі узгодження**
EG02 Керовані бізнес-ризики EG06 Безперервність і доступність послуг бізнесу		AG02 Керовані ризики, пов’язані з I&T AG07 Безпека інформації, інфраструктури обробки і прикладних програм, приватність
Приклад метрик для цілей організації		**Приклад метрик для цілей узгодження**
EG02 a. Відсоток критичних цілей бізнесу та послуг, які охоплено оцінюванням ризику Співвідношення значних інцидентів, які не були ідентифіковані під час оцінювання ризиків, до загальної кількості інцидентів. b. Частота оновлення профілю ризику.		AG02 a. Частота оновлення профілю ризику b. Відсоток оцінки ризиків організації, що включає ризики, пов’язані з I&T c. Число значних інцидентів, пов’язаних з I&T, які не були ідентифіковані під час оцінювання ризиків
EG06 a. Кількість переривань обслуговування клієнтів або бізнес-процесів, що спричинили значні інциденти b. Комерційна вартість інцидентів Кількість робочих годин, втрачених через незаплановані переривання в обслуговуванні c. Відсоток скарг як функція узгоджених цільових показників доступності послуги		AG07 a. Кількість інцидентів, пов’язаних з порушенням конфіденційності, які призвели до фінансових збитків, порушення безперервності діяльності або публічного осудження b. Кількість інцидентів, пов’язаних з порушенням доступності, які призвели до фінансових збитків, порушення безперервності діяльності або публічного осудження c. c. Кількість інцидентів, пов’язаних з порушенням цілісності, які призвели до фінансових збитків, порушення безперервності діяльності або публічного осудження

A. Складова: Процес	
Практика корпоративного управління	**Приклад метрик**
EDM03.01 Оцінити управління ризиками Постійно вивчати та оцінювати вплив ризику на поточне та майбутнє використання I&T в організації. Проаналізувати, чи ризик апетит організації є належним та забезпечити, що ризик для цінності організації, пов'язаний з використанням I&T, ідентифікований та керований	a. Рівень неочікуваного впливу на організацію. b. Відсоток ризику I&T, який перевищує рівень толерантності до ризику організації c. Частота оновлення оцінок факторів ризику

Діяльність	Рівень спроможності
1. Зрозуміти організацію та її контекст, пов'язаний з ризиком I&T.	2
2. Визначити ризик-апетит організації, тобто, рівень ризику, пов’язаного з I&T, який організація готова прийняти в інтересах досягнення цілей організації.	
3. Визначити рівні толерантності з урахуванням ризик апетиту, тобто, тимчасово допустимі відхилення від ризик апетиту.	
4. Визначити ступінь узгодження стратегії щодо ризику I&T зі стратегією щодо ризиків організації, та переконатися, що ризик апетит є нижчим ризику, який організація може прийняти.	
5. Проактивно оцінювати фактори ризику I&T попередньо до прийняття стратегічних рішень організації та забезпечити, що розгляд ризиків є частиною процесу прийняття стратегічних рішень організації.	3
6. Оцінити діяльність з управління ризиками для забезпечення узгодженості зі здатністю організації приймати збитки, пов’язані з I&T, та толерантність керівництва до цього	
7. Залучати та утримувати необхідні навички та персонал для управління ризиками I&T.	

Пов`язані настанови (стандарти, загальні принципи, нормативні вимоги)	Детальне посилання
COSO Enterprise Risk Management, June 2017	Strategy and Objective-Setting—Principles 6 and 7; 9. Review and Revision—Principle 16
Практика корпоративного управління	**Приклад метрик**
EDM03.02 Спрямовувати управління ризиками Керувати впровадженням практик з управління ризиками для забезпечення достатньої впевненості у тому, що практики управління ризиком I&T є належними та що фактичний ризик I&T не перевищує ризик апетит, встановлений радою.	a. Рівень узгодженості між ризиком I&T та ризиком організації b. Відсоток проєктів організації, що враховують ризик I&T.

Діяльність	Рівень спроможності
1. Керувати втіленням стратегії ризику I&T в практики управління ризиками та операційну діяльність.	2
2. Керувати розробленням планів комунікацій стосовно ризику (який охоплює всі рівні організації).	
3. Керувати впровадженням відповідних механізмів для швидкого реагування на зміни ризику та звітувати негайно керівникам відповідних рівнів на базі узгоджених принципів ескалації (про що звітувати, коли, де та як).	
4. Надати вказівки, що ризик, можливості, питання та занепокоєння можуть бути ідентифіковані і та повідомлені відповідній стороні будь-ким у будь-який час. Ризиком необхідно управляти у відповідності до опублікованих політик та процедур, та здійснювати ескалацію відповідним особам, які здійснюють прийняття рішень.	
5. Визначити ключові цілі та показники процесів корпоративного та операційного управління ризиками, які необхідно моніторити, та затвердити підходи, методи, методики та процеси для отримання та звітування про інформацію щодо вимірювання.	3

A. Складова: Процес *(продовження)*	
Пов`язані настанови (стандарти, загальні принципи, нормативні вимоги)	**Детальне посилання**
CMMI Cybermaturity Platform, 2018 RS.AS Apply Risk Management Strategy; BC.RO Determine Strategic Risk	CMMI Cybermaturity Platform, 2018 RS.AS Apply Risk Management Strategy; BC.RO Determine Strategic Risk
ISF, The Standard of Good Practice for Information Security 2016 IR1.1 Information Risk Assessment—Management Approach	ISF, The Standard of Good Practice for Information Security 2016 IR1.1 Information Risk Assessment—Management Approach
King IV Report on Corporate Governance for South Africa, 2016 Part 5.4: Governance functional areas—Principle 11	King IV Report on Corporate Governance for South Africa, 2016 Part 5.4: Governance functional areas—Principle 11
National Institute of Standards and Technology Special Publication	National Institute of Standards and Technology Special Publication
Практика корпоративного управління	**Приклад метрик**
EDM03.03 Моніторити управління ризиками. Здійснювати моніторинг ключових цілей та показників процесів управління ризиками. Визначити, як будуть ідентифікуватися, та відслідковуватися відхилення або проблеми, та буде здійснюватися звітування для вжиття заходів відновлення.	a. Кількість ідентифікованих та керованих зон потенційних I&T ризику b. Відсоток критичних ризиків, які було успішно пом'якшено c. Відсоток заходів щодо ризиків I&T, які було вжито вчасно.

Діяльність	**Рівень спроможності**
1. Звітувати про будь-які питання щодо управління ризиками раді або виконавчому комітету.	2
2. Здійснювати моніторинг того, в якій мірі здійснюється управління профілем ризику в межах порогових значень ризик апетиту та рівнів толерантності організації.	3
3. Здійснювати моніторинг ключових цілей та показників процесів корпоративного та операційного управління ризиками у порівнянні з цільовими цілями, аналізувати причини будь-яких відхилень, та ініціювати заходи відновлення для усунення першопричин.	4
4. Сприяти здійсненню ключовими зацікавленими сторонами перегляду прогресу організації щодо досягнення ідентифікованих цілей.	

Пов`язані настанови (стандарти, загальні принципи, нормативні вимоги)	**Детальне посилання**
COSO Enterprise Risk Management, June 2017 9. Review and Revision—Principle 17	COSO Enterprise Risk Management, June 2017 9. Review and Revision—Principle 17
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 7); 3.5 Assessment (Task 1); 3.6 Authorization (Task 1)
The Open Group IT4IT Reference Architecture, Version 2.0 6. Requirement to Deploy (R2D) Value Stream; 7. Request to Fulfill (R2F)	The Open Group IT4IT Reference Architecture, Version 2.0 6. Requirement to Deploy (R2D) Value Stream; 7. Request to Fulfill (R2F)

B. Складова: Організаційні структури								
Ключові практики корпоративного управління	**Рада**	**Виконавчий комітет**	**Виконавчий директор, CEO**	**Директор з ризиків, CRO**	**І ІТ-директор, CIO**	**Рада корпоративного управління I&T**	**Комітет з ризиків**	**Директор з інформаційної безпеки,CISO**
EDM03.01 Оцінити управління ризиками.	A	R	R	R	R	R	R	
EDM03.02 Спрямовувати управління ризиками.	A	R	R	R	R	R	R	
EDM03.03 Моніторити управління ризиками.	A	R	R	R	R	R	R	R

Пов`язані настанови (стандарти, загальні принципи, нормативні вимоги)	**Детальне посилання**
COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principle
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance

C. Складова: Інформаційні потоки та елементи (див. також пункт 3.6)				
Практика корпоративного управління	**Входи**		**Виходи**	
	Від	**Опис**	**Опис**	**Куди**
EDM03.01 Оцінити управління ризиками.	APO12.01	Проблеми та фактори ризику, які виникають	Настанова щодо ризик апетиту	APO04.01; APO12.03
	Поза межами COBIT	Принципи ризиком організації (ERM)	Оцінка діяльності з управління ризиками	APO12.01
			Затверджені рівні толерантності до ризику	APO12.03
EDM03.02 Спрямовувати управління ризиками.	APO12.03	Агрегований профіль ризику, включаючи статус заходів з ризиком	Затверджений процес управління оцінюванням ризику	APO12.01
	Поза межами COBIT	Профілі управління ризиком організації (ERM) та плани пом`якшення ризиків	Ключові цілі, моніторинг яких має здійснювати для управління ризиком	APO12.01
			Політики з управління ризиками	APO12.01
EDM03.03 Моніторити управління ризиками.	APO12.02	Результати аналізу ризиків	Коригуючі дії для усунення відхилень в управлінні ризиками	APO12.06
	APO12.04	• Звіти щодо аналізу ризиків та профілю ризиків для зацікавлених сторін • Результати аналізу ризиків третіми сторонами • Можливості для прийняття більшого ризику	Питання управління ризиками для ради	EDM05.01

Пов`язані настанови (стандарти, загальні принципи, нормативні вимоги)	**Детальне посилання**
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 7): Inputs and Outputs; 3.5 Assessment (Tasks 1, 2): Inputs 2, and Outputs; 3.6 Authorization (Task 1): Inputs and Outputs

D. Складова: Люди, навички та компетенції		
Навички	**Пов`язані настанови (стандарти, загальні принципи, нормативні вимоги)**	**Детальне посилання**
Управління бізнес ризиками	Skills Framework for the Information Age V6, 2015	BURM
Управління ризиками	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Складова: Політики та процедури			
Відповідна політика	**Опис політики**	**Пов`язані настанови**	**Детальне посилання**
Політика управління ризиками організації	Визначає корпоративне та операційне управління ризиком організації на стратегічному, тактичному та операційному рівнях, у відповідності до цілей бізнесу. Перекладає принципи та політику корпоративного управління організацією у принципи та політику корпоративного управління ризиком, та розробляє діяльність з управління управління ризиком.	National Institute of Standards and Technology Special Publication800- 53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-1)

F. Складова: Культура, етика та поведінка		
Ключові елементи культури	**Пов`язані настанови**	**Детальне посилання**
Просувати культуру обізнаності щодо I&T ризиків на всіх рівнях організації та уповноважити організацію здійснювати проактивну ідентифікацію, звітування та ескалацію ризиків I&T, можливостей та потенційних наслідків для бізнесу. Вище керівництво задає напрямок та демонструє помітну та щиру підтримку практик щодо ризику. Додатково, керівництво має чітко визначати ризик апетит та забезпечити належний рівень обговорення як частину повсякденної діяльності. Бажана поведінка включає заохочення працівників порушувати питання або негативні результати та демонструвати прозорість стосовно ризику I&T. Власники бізнесу мають приймати відповідальність за ризики I&T, коли це необхідно, та демонструвати справжні зобов'язання щодо управління ризиками I&T шляхом надання відповідних ресурсів.	COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principles 3 and 4

G. Складова: Послуги, інфраструктура та прикладні програми
• Система управління ризиками

Домен: Узгодження, планування та організація **Цілі операційного управління: APO12 — Керований ризик**	**Сфера діяльності:** **Модель ядра COBIT**

Опис

Постійно ідентифікувати, оцінювати та зменшувати ризик, пов’язаний з I&T, в межах рівнів толерантності, визначених виконавчим керівництвом організації.

Задача

Інтегрувати управління ризиком організації, пов’язаним з I&T із загальним управлінням ризиком організації (ERM) та забезпечити баланс між витратами та вигодою управління ризиками організації, пов’язаним з I&T

Ціль операційного управління підтримує досягнення набору основних цілей організації та цілей узгодження:

Цілі організації		**Цілі узгодження**
EG02 Керовані бізнес-ризики EG06 Безперервність та доступність бізнес-послуг	➡	AG02 Керовані ризики, пов'язані з I&T AG07 Безпека інформації, інфраструктури обробки і прикладних програм, приватність
Приклад метрик для цілей організації		**Приклад метрик для цілей узгодження**
EG02 a. Відсоток критичних цілей бізнесу та послуг, які охоплені оцінюванням ризику b. Відношення значних інцидентів, які не були ідентифіковані під час оцінки ризиків, до загальної кількості інцидентів c. Частота оновлення профілю ризику		AG02 a. Частота оновлення профілю ризику b. Відсоток оцінок ризику організації, включаючи ризики, пов'язані з I&T c. Кількість значних інцидентів, пов'язаних з I&T, які не були ідентифіковані під час оцінки ризиків
EG06 a. Число збоїв в послугах чи бізнес процесах клієнтів, що призвели до виникнення значних інцидентів b. Витрати бізнесу через інциденти c. Кількість годин обслуговування бізнес-процесу, втрачених через незаплановані збої в наданні послуг d. Відсоток скарг як функція цільових показників доступності послуг		AG07 a. Число інцидентів, пов’язаних з порушенням конфіденційності, які призвели до фінансових збитків, порушення безперервності бізнесу або публічного осудження b. Число інцидентів, пов’язаних з порушенням доступності, які призвели до фінансових збитків, порушення безперервності бізнесу або публічного осудження c. Число інцидентів, пов’язаних з порушенням цілісності, які призвели до фінансових збитків, порушення безперервності бізнесу або публічного осудження

A. Складова: Процес	
Практика операційного управління	**Приклад метрик**
APO12.01 Збирати дані. Визначити та зібрати відповідні дані для забезпечення ефективного виявлення ризиків, пов'язаних з I&T, їх аналізу та звітування.	a. Кількість подій зі збитками з ключовими характеристиками, які занесено у репозиторії b. Відсоток аудитів, подій та трендів, які занесено у репозиторії. c. Відсоток критичних систем із відомими проблемами

Діяльність	Рівень спроможності
1. Впровадити та супроводжувати методику для збирання, класифікації та аналізу даних, пов'язаних з I&T ризиком.	2
2. Фіксувати відповідні та суттєві дані, пов'язані з I&T ризиком, щодо внутрішнього та зовнішнього середовищ діяльності організації.	
3. Адаптувати або визначити таксономію ризиків для узгодженого визначення категорій сценаріїв, які стосуються ризиків, впливу та імовірності.	3
4. Фіксувати дані щодо подій ризику, які спричинили або можуть спричинити вплив на бізнес відповідно до категорій впливу, визначених у таксономії ризиків. Збирати відповідні дані з пов'язаних питань, інцидентів, проблем та розслідувань.	
5. Дослідити та проаналізувати історичні дані щодо I&T ризику та статистику щодо збитків з зовнішніх доступних даних та трендів, галузевих аналогів, використовуючи галузеві журнали подій, бази даних та галузеві домовленості щодо спільного розкриття подій.	4
6. Для подібних класів подій, впорядкувати зібрані дані та виділити фактори впливу. Визначити спільні фактори впливу для множинних подій.	
7. Визначити специфічні умови, які існували або були відсутні на момент виникнення подій ризику, та спосіб, у який умови вплинули на частоту виникнення подій та величину збитків через них.	
8. Здійснити періодичний аналіз подій та факторів ризику для виявлення нових або виникаючих питань, пов'язаних з ризиками, та поглибити розуміння пов'язаних внутрішніх та зовнішніх факторів ризику.	

Пов'язані настанови (стандарти, загальні принципи, нормативні вимоги)	Детальне посилання
CMMI Data Management Maturity Model, 2014	Supporting Processes – Risk Management
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 10
ISO/IEC 27005:2011(E)	8.2 Risk identification; 12. Information security risk monitoring and review
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 7)

Практика операційного управління	Приклад метрик
APO12.02 Аналізувати ризик. Розробити обґрунтоване бачення на фактичний ризик I&T, в підтримку рішень стосовно ризиків	• Кількість виявлених сценаріїв для ризику I&T • Час з моменту останнього оновлення сценаріїв для ризику I&T

Діяльність	Рівень спроможності
1. Визначити відповідний обсяг для здійснення аналізу ризиків, враховуючи всі фактори ризику та /або критичність активів для бізнесу.	3
2. Створити та регулярно оновлювати сценарії для ризику I&T; можливу величну збитків, пов'язаних з I&T; та сценарії стосовно репутаційного ризику, включаючи комплексні сценарії послідовних та/або випадкових типів загроз та подій. Сформувати очікування стосовно специфічної контрольної діяльності та можливостей щодо виявлення.	
3. Оцінити частоту (або імовірність) та величину втрат або вигід, пов'язаних зі сценаріями для ризику I&T. Прийняти до уваги всі фактори ризику, які можуть бути застосовані, та оцінити відомі операційні контролі.	
4. Порівняти поточну величину ризику (можливу величну збитків, пов'язаних з I&T) з ризик апетитом та прийнятними рівнями толерантності. Виявити неприйнятний чи підвищений ризик.	
5. Запропонувати заходи реагування на ризик, який перевищує ризик апетит та рівні толерантності.	
6. Визначити високорівневі вимоги для проєктів або програм, які будуть реалізовувати обрані заходи реагування на ризик. Визначити вимоги та очікування стосовно відповідних ключових контролів для заходів з пом'якшення ризику.	
7. Здійснити валідацію результатів аналізу ризиків та аналізу впливу негативних факторів на бізнес (BIA) перед тим, як використовувати їх для подальшого прийняття рішень. Підтвердити, що аналіз узгоджується з вимогами організації та перевірити, що оцінки були належним чином відкалібровані та ретельно перевірені на предмет упередженості.	4
8. Проаналізувати витрати та вигоди від потенційних варіантів заходів реагування на ризик, таких як уникнути, зменшити/пом'якшити, передати/розподілити, та прийняти та використати/скористатися. Підтвердити оптимальний захід реагування на ризик.	5

A. Складова: Процес *(продовження)*	
Пов'язані настанови (стандарти, загальні принципи, нормативні вимоги)	**Детальне посилання**
CMMI Data Management Maturity Model, 2014	Supporting Processes—Risk Management
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 11
ISF, The Standard of Good Practice for Information Security 2016	IR2.1 Risk Assessment Scope; IR2.2 Business Impact Assessment
ISO/IEC 27001:2013/Cor.2:2015(E)	8.2 Information security risk assessment
ISO/IEC 27005:2011(E)	8.3 Risk analysis
National Institute of Standards and Technology Framework for ImprovingCritical Infrastructure Cybersecurity v1.1, April 2018	ID.RA Risk Assessment
National Institute of Standards and Technology Special Publication800-37, Revision 2 (Draft), May 2018	3.6 Authorization (Task 3)
National Institute of Standards and Technology Special Publication800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-3)
Практика операційного управління	**Приклад метрик**
APO12.03 Супроводжувати профіль ризику. Супроводжувати перелік відомих ризиків та характеристик ризику, включаючи очікувану частоту, потенційний вплив та заходи реагування. Задокументувати пов'язані ресурси, можливості та поточну контрольну діяльність, пов'язану з цими ризиками.	a. Повнота характеристик та значень в профілі ризику b. Відсоток ключових бізнес процесів, включених в профіль ризику.

Діяльність	**Рівень спроможності**
1. Інвентаризувати бізнес процеси та задокументувати їх залежність від процесів операційного управління I&T послугами та ресурсів інфраструктури IT. Ідентифікувати підтримуючий персонал, прикладні програми, інфраструктуру, споруди та обладнання, критичну документацію на паперових носіях, підрядників, постачальників та аутсорсерів.	2
2. Визначити та узгодити, які I&T послуги та ресурси інфраструктури IT мають важливе значення для підтримання функціонування бізнес процесів. Проаналізувати залежності та виявити слабкі зв'язки.	
3. Згрупувати поточні сценарії для ризиків за категорією, напрямком бізнесу та функціональною областю.	
4. Регулярно збирати всю інформацію щодо профілю ризику та консолідувати її у агрегований профіль ризику.	3
5. Зібрати інформацію стосовно плану заходів щодо реагування на ризик для включення у профіль ризику I&T організації.	
6. Базуючись на всій інформації щодо профілю ризику, визначити ряд ключових індикаторів, які дозволять швидко виявляти та моніторити поточний ризик та тренди щодо ризику.	4
7. Зібрати інформацію стосовно подій ризику I&T, які відбулися, для включення у профіль ризику I&T організації.	

Пов'язані настанови (стандарти, загальні принципи, нормативні вимоги)	**Детальне посилання**
CMMI Cybermaturity Platform, 2018	RS.DT Define Organizational Risk Tolerance
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 12
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-7)

A. Складова: Процес *(продовження)*	
Практика операційного управління	**Приклад метрик**
APO12.04 Сформулювати ризик Своєчасно повідомити інформацію про поточний стан ризиків та можливостей, пов'язаних з I&T, всім зацікавленим сторонам, яких це стосується, для вжиття належних заходів реагування.	a. Рівень задоволеності зацікавлених сторін наданою звітністю щодо ризику b. Повнота звітності щодо профілю ризику (включаючи інформацію відповідно до вимог зацікавлених сторін) c. Використання звітності щодо ризику керівництвом під час прийняття рішень

Діяльність	**Рівень спроможності**
1. Звітувати про результати аналізу ризиків всім зацікавленим сторонам, яких це стосується, в строки та формати, які приносять користь для підтримки рішень, що приймаються в організації. Де можливо, включити імовірності та діапазони втрат або вигід разом з рівнями конфіденційності для забезпечення керівництва можливістю управління балансом між ризиком та доходом	3
2. Ознайомити осіб, які приймають рішення, з найгіршим та найбільш імовірним сценаріями, можливою величною збитків, пов'язаних з I&T та суттєвими репутаційними, законодавчими та нормативними аспектами, або будь-якими іншими категоріями впливу відповідно до таксономії ризиків.	
3. Звітувати про поточний профіль ризику всім зацікавленим сторонам. Включити інформацію про ефективність процесу управління ризиками, ефективність контролів, відмінностей, невідповідностей, надлишкам, статусу заходів щодо відновлення та їх впливу на профіль ризику.	
4. На періодичній основі, для сфер з рівним співвідношенням між відносним ризиком та допустимим ступенем ризику, визначити можливості, пов'язані з I&T, які дозволять прийняти більший ризик та сприятимуть зростанню та доходності.	
5. Переглянути результати об'єктивних оцінок з боку третіх сторін та внутрішнього аудити та переглядів щодо забезпечення впевненості у якості. Включити їх у профіль ризику. Переглянути виявлені відмінності та можливу величну збитків, пов'язаних з I&T, для визначення потреби у додатковому аналізі ризиків.	4

Пов'язані настанови (стандарти, загальні принципи, нормативні вимоги)	**Детальне посилання**
CMMI Cybermaturity Platform, 2018	RS.CR Determine Critical Infrastructure Requirements
COSO Enterprise Risk Management, June 2017	10. Information, Communication, and Reporting—Principle 19
ISO/IEC 27005:2011(E)	11. Information security risk communication and consultation
National Institute of Standards and Technology Framework for ImprovingCritical Infrastructure Cybersecurity v1.1, April 2018	ID.RM Risk Management Strategy
National Institute of Standards and Technology Special Publication800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-32)

Практика операційного управління	**Приклад метрик**
APO12.05 Визначити програму дій з управління ризиками Управляти можливостями зменшення ризику до прийнятного рівня на портфельній основі.	a. Кількість суттєвих інцидентів, які не було виявлено та включено у програму дій з управління ризиками. b. Відсоток пропозицій стосовно проєктів з управління ризиками, відхилених через недостатність врахування інших пов'язаних ризиків.

Діяльність	**Рівень спроможності**
1. Супроводжувати перелік контролів, які існують для пом'якшення ризику та дозволяють приймати ризик у відповідності до ризик апетиту та рівнів толерантності. Класифікувати контролі та прив'язати їх до специфічних сценаріїв для ризику I&T, а також агрегованих сценаріїв для ризику I&T.	2
2. Визначити, чи кожна структура в межах організації здійснює моніторинг ризику та приймає відповідальність за діяльність в межах індивідуальних та портфельних рівнів толерантності.	3
3. Визначити збалансований перелік пропозицій щодо проєктів для зменшення ризику та/або проєктів, які дозволяють організації реалізувати стратегічні можливості, враховуючи витрати, переваги, вплив на поточний профіль ризику та вимоги.	

A. Складова: Процес *(продовження)*	
Пов'язані настанови (стандарти, загальні принципи, нормативні вимоги)	**Детальне посилання**
CMMI Data Management Maturity Model, 2014	HITRUST CSF version 9, September 2017
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 14
HITRUST CSF version 9, September 2017	03.01 Risk Management Program
Практика операційного управління	**Приклад метрик**
APO12.06 Реагувати на ризик. Своєчасно реагувати на події ризику, які реалізувалися, зі застосуванням ефективних заходів для обмеження величини збитків.	a. Кількість заходів, які не зменшують залишковий ризик b. Відсоток планів заходів, що стосуються ризику I&T, які виконуються як передбачалося.

Діяльність	**Рівень спроможності**
1. Готувати, супроводжувати та тестувати плани, які визначають конкретні кроки для випадків, коли подія ризику може спричинити суттєвий операційний або технологічний інцидент з суттєвим впливом на бізнес. Забезпечити, що плани включають шляхи ескалації в межах організації	3
2. Застосувати відповідний план реагування для пом'якшення наслідків у разі реалізації ризику у формі інциденту.	
3. Класифікувати інциденти та порівняти можливу величну збитків, пов'язаних з I&T, з порогами толерантності до ризику. Проінформувати осіб, які приймають рішення, стосовно впливу на бізнес в межах звітування та оновлення профілю ризику.	4
4. Вивчити минулі несприятливі події / втрати та упущені можливості, та визначити їх причини.	
5. Проінформувати відповідних осіб, які приймають рішення, про першопричини, вимоги щодо додаткових заходів реагування на ризик та вдосконалень процесу. Забезпечити, що причини, вимоги щодо заходів реагування та вдосконалень процесу включені у процеси управління ризиками.	5

Пов'язані настанови (стандарти, загальні принципи, нормативні вимоги)	**Детальне посилання**
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 13
ISF, The Standard of Good Practice for Information Security 2016	IR2.9 Risk Treatment
ISO/IEC 27001:2013/Cor.2:2015(E)	6.1 Action to address risk and opportunities
ISO/IEC 27005:2011(E)	9. Information security risk treatment
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.6 Authorization (Task 4)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-9, PM-31)

B. Складова: Організаційні структури																	
Ключові практики операційного управління	**Директор з ризиків, CRO**	**IT-директор, CIO**	**Технічний директор, CTO**	**Цифровий директор, CDO**	**Комітет з ризиків**	**Директор з інформаційної безпеки, CISO**	**Власники бізнес процесів**	**Відділ управління проєктами, PMO**	**Функція управління даними**	**Головний архітектор**	**Головний з розробки**	**Головний з IT-операційної діяльності**	**Головний з IT-адміністрування**	**Керівник сервісів**	**Керівник з інформаційної безпеки**	**Керівник з безперервної діяльності**	**Директор з приватності**
APO12.01 Збирати дані.	A	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
APO12.02 Аналізувати ризик.	A	R			R		R										
APO12.03 Супроводжувати профіль ризику.	A	R			R		R										
APO12.04 Сформулювати ризик	A	R			R		R										
APO12.05 Визначити програму дій з управління ризиками	A	R			R		R										
APO12.06 Реагувати на ризик.	R	A	R	R		R	R	R		R	R	R	R	R	R	R	R
Пов'язані настанови (стандарти, загальні принципи, нормативні вимоги)	**Детальне посилання**																
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 1); Appendix A: Roles and Responsibilities																

С. Складова: Інформаційні потоки та елементи (див. також пункт 3.6)				
Практика операційного управління	**Вхід**		**Вихід**	
APO12.01 Збирати дані.	**Від**	**Опис**	**Опис**	**Куди**
	APO02.02	Відмінності та ризики, пов'язані з поточними спроможностями	Виникаючі проблеми з ризиками та факторами	APO01.01; APO02.02; EDM03.01
	APO02.05	Ініціативи щодо оцінювання ризику	Дані щодо подій ризику та факторів впливу	Внутрішній
	APO10.04	Виявлений ризик, пов'язаний з наданням послуг підрядником		Внутрішній
	DSS02.07	Статус інцидентів та звіти щодо трендів		
	EDM03.01	Оцінювання діяльності щодо управління ризиками		
	EDM03.02	• Політики з управління ризиками • Ключові цілі, які є предметом моніторингу для управління ризиками • Погоджений процес для визначення управління ризиками		
APO12.02 Аналізувати ризик.	DSS04.02	Аналіз впливу негативних факторів на бізнес організації (BIAs)	Результати аналізу ризиків	APO01.01; APO02.02; EDM03.03; BAI01.08; BAI11.06
	DSS05.01	Оцінювання потенційних загроз	Сценарії, пов'язані з ризиком I&T	Внутрішній
	Поза межами COBIT	Рекомендаційні вказівки щодо загроз	Обсяг для здійснення аналізу ризиків	Внутрішній
APO12.03 Супроводжувати профіль ризику.	APO10.04	Виявлений ризик, пов'язаний з наданням послуг підрядником	Агрегований профіль ризику, включаючи статус заходів реагування на ризик	APO02.02; EDM03.02
	DSS05.01	Оцінювання потенційних загроз	Задокументовані сценарії, які стосуються ризиків, в розрізі напрямків бізнесу та функцій	Внутрішній
	EDM03.01	• Настанови щодо ризик-апетиту • Погоджені рівні толерантності до ризику		Внутрішній
APO12.04 Сформулювати ризик			Звіти для зацікавлених сторін щодо аналізу ризиків та профілю ризиків	APO10.04; EDM03.03; EDM05.02; MEA04.05
			Результати оцінювання ризиків третіми сторонами	APO10.04; EDM03.03; MEA02.01
			Можливості для прийняття більшого ризику	EDM03.03
APO12.05 Визначити програму дій з управління ризиками			Пропозиції стосовно проєктів для зменшення ризику	APO02.02; APO13.02
APO12.06 Реагувати на ризик.	EDM03.03	Коригуючі заходи стосовно для усунення ризику відхилень в управлінні ризиками	Повідомлення щодо впливу ризику	APO01.02; APO08.04; DSS04.02
			Першопричини, що пов'язані з ризиками	DSS02.03; DSS03.01; DSS03.02; DSS03.03; DSS03.05; DSS04.02; MEA02.04; MEA04.04; MEA04.06
			План реагування на інциденти, пов'язані з ризиками	DSS02.05

C. Складова: Інформаційні потоки та елементи (див. також пункт 3.6) (*продовження*).	
Пов'язані настанови (стандарти, загальні принципи, нормативні вимоги)	**Детальне посилання**
COSO Enterprise Risk Management, June 2017	10. Information, Communication, and Reporting—Principle 20
SF, The Standard of Good Practice for Information Security 2016	IR1.3 Information Risk Assessment—Supporting Material
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 7): Inputs and Outputs; 3.6 Authorization (Task 3, 4): Inputs and Outputs
PMBOK Guide Sixth Edition, 2017	Part 1: 11. Project risk management: Inputs and Outputs

D. Складова: Люди, навички та компетенції		
Навички	**Пов'язані настанови (стандарти, загальні принципи, нормативні вимоги)**	**Детальне посилання**
Управління бізнес-ризиками	Skills Framework for the Information Age V6, 2015	BURM
Забезпечення впевненості в інформації	Skills Framework for the Information Age V6, 2015	INAS
Управління ризиками	e-Competence Framework (e-CF)—A common European Framework for ICT Professionals in all industry sectors—Part 1: Framework, 2016	E. Manage—E.3. Risk Management

E. Складова: Політики та процедури			
Відповідна політика	**Опис політики**	**Пов'язані настанови**	**Детальне посилання**
Політика управління ризиком організації	Визначає корпоративне управління ризиком організації на стратегічному, тактичному та операційному рівнях, у відповідності до цілей бізнесу. Перекладає корпоративне управління організацією в принципи корпоративного управління ризиками та політики, та визначає діяльність з управління ризиками.	National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-1)
Політика управління ризиком шахрайства організації	Визначає захист бренду організації, репутації та активів у випадку виникнення втрат чи пошкоджень в результаті шахрайства або неправомірної поведінки. Направляє працівників щодо повідомлень про підозрілу діяльність та роботу з чутливою інформацією та відомостями. Заохочує культуру протидії шахрайству та сприяє обізнаності щодо ризику.	National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	

F. Складова: Культура, етика та поведінка		
Ключові елементи культури	**Пов'язані настанови**	**Детальне посилання**
Для підтримання прозорої та загальної культури управління ризиками, вищі керівники повинні задавати напрямок та демонструвати явну та щиру підтримку впровадження практик управління ризиками в організації. Керівництво повинно заохочувати відкриту комунікацію та відповідальність бізнесу за бізнес ризик, пов'язаний з I&T. Бажана поведінка включає приведення політик до визначеного ризик-апетиту, звітування про тренди щодо ризиків вищому керівництву та органам, що відповідають за управління ризиками, заохочуючи ефективне управління ризиками, та проактивний моніторинг ризику та прогрес у впровадженні плану заходів стосовно ризиків.	ISF, The Standard of Good Practice for Information Security 2016	IR1.2 Information Risk Assessment

G. Складова: Послуги, інфраструктура та прикладні програми
• Послуги щодо антикризового управління • Інструменти для керування, ризику та комплаєнсу (GRC) • Інструменти для аналізу ризику • Послуги щодо отримання інформації для цілей управління ризиками

Сторінка навмисно залишена порожньою

Додаток №1 до листа від 25.08.2023 № 69/23

Порівняльна таблиця
пропозицій та зауважень Асоціації «Телас» до розробленого Адміністрацією Держспецзв'язку проекту постанови Кабінету Міністрів України «Про затвердження Вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності»

Загальний коментар:

Аналіз регуляторного впливу (надалі – АРВ) містить недоліки та потребує доопрацювання.

1. В АРВ вказується:

***Зазначена проблема не може бути розв'язана за допомогою ринкових механізмів**, оскільки вона стосується управління ризиками безпеки на об'єктах критичної інфраструктури, крім банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжних організації, учасників платіжних систем, операторів послуг платіжної інфраструктури, державне регулювання, нагляд за діяльністю яких здійснює Національний банк України.*

Не враховується той факт, що комерційний сектор самостійно витрачає суттєві кошти для зниження ризиків без регулювання з боку держави.

2. В оцінці впливу на сферу інтересів суб'єктів господарювання зазначається, що документ не потребує додаткових витрат. Будь-які рішення потребують витрат. Наприклад, документ передбачає, що план оператора критичної інфраструктури має передбачати визначення відповідної інфраструктури (альтернативне місце розташування), яка розташована щонайменше на відстані 50 кілометрів від існуючої інфраструктури та придатна для забезпечення життєво важливих функцій та / або послуг.

Загалом, документ потребує доопрацювання розробником разом з представниками заінтересованих індустрій з метою врахування дій та підходів, які вчиняються бізнесом самостійно та прибирання з документу зайвої зарегульованості.

Запропонована ДССЗЗІ редакція	Пропозиції та зауваження Асоціації «Телас»	Обґрунтування
КАБІНЕТ МІНІСТРІВ УКРАЇНИ		
ПОСТАНОВА		
від 2023 р. №		
Київ		
Про затвердження Вимог щодо управління ризиками безпеки на об’єктах критичної інфраструктури І категорії критичності		
Відповідно до абзацу другого частини першої статті 22 Закону України «Про критичну інфраструктуру» Кабінет Міністрів України **постановляє:**		
1. Затвердити Вимоги щодо управління ризиками безпеки на об’єктах критичної інфраструктури І категорії критичності (далі – Вимоги), що додаються.		
2. Установити, що починаючи з 1 січня 2024 року:		
секторальні органи у сфері захисту критичної інфраструктури щороку до 30 січня подають уповноваженому органу у сфері захисту критичної інфраструктури України звіт про виконання Вимог, за минулий рік;		

оператори критичної інфраструктури щороку до **15 січня** подають секторальним органам у сфері захисту критичної інфраструктури звіт про виконання Вимог, за минулий рік.	оператори критичної інфраструктури **I категорії критичності** щороку до **15 лютого** подають секторальним органам у сфері захисту критичної інфраструктури звіт про виконання Вимог, за минулий рік.	Звітувати повинні не всі оператори ОКІ, а лише ті, що віднесені до І категорії критичності. 15 січня – лише 2 робочі тижні після закінчення звітного періоду, а також період свят, а тому запропонованого строку може бути недостатньою формування та подання звіту. Пропонуємо збільшити термін.
3. Ця постанова набирає чинності з дня її опублікування **та застосовується** з 1 січня 2024 року.	3. Ця постанова набирає чинності з 1 січня 2024 року.	Некоректне формулювання.

Порівняльна таблиця
пропозицій та зауважень Асоціації «Телас» до розробленого Адміністрацією Держспецзв'язку проекту Вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності

Запропонована ДССЗЗІ редакція	Пропозиції та зауваження Асоціації «Телас»	Обґрунтування
ВИМОГИ		
щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності		
1. Цими вимогами встановлюються критерії щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності.	1. Цими вимогами встановлюються **методи** щодо управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності.	Критерій це підстава для оцінки, визначення або класифікації чогось. Вимоги мають встановлювати процес прийняття рішень і здійснення заходів, спрямованих на зміну ризику.
Управління ризиками безпеки на об'єктах критичної інфраструктури І категорії критичності здійснюється оператором критичної інфраструктури з метою забезпечення стійкості та захисту таких об'єктів.		
Дія цих вимог не поширюється на банки, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжні організації, учасників платіжних систем, операторів послуг платіжної інфраструктури, державне регулювання, нагляд за діяльністю яких здійснює		

Національний банк України та встановлює вимоги щодо управління ризиками безпеки.		
2. У цих вимогах терміни вживаються у таких значеннях:		
аналіз ризиків безпеки на об’єктах критичної інфраструктури (далі – аналіз ризиків безпеки) – визначення наслідків та їх ймовірностей стосовно ідентифікованих ризиків безпеки;		
вірогідність (likelihood) – ймовірність того, що щось станеться, незалежно від того, виміряно чи визначено об’єктивно чи суб’єктивно, якісно чи кількісно та описано за допомогою загальних термінів або математично, зокрема, ймовірність або частота протягом певного періоду часу;	вірогідність (likelihood) – ймовірність настання ризиків та/або потенційної події протягом певного періоду часу;	У запропонованому тлумаченні терміну повністю відсутня будь-яка визначеність і розуміння того, що саме означає цей термін.
джерело ризику – подія, зокрема: явище, інцидент, дія, бездіяльність або їх сукупність, які потенційно можуть спричинити ризик;		
ймовірність – числова характеристика можливості того, що потенційна подія відбудеться в умовах, які можуть бути відтворені необмежену кількість разів;		
європейська критична інфраструктура – це об’єкти критичної інфраструктури України, які надають життєво важливі функції та/або послуги більше ніж 6		

державам членам Європейського Союзу;		
ліміт ризику – обмеження, встановлені оператором критичної інфраструктури для контролю величини ризиків, які впливають на надання життєво важливих функцій та/або послуг об’єктом критичної інфраструктури;		
модель загроз безпеці об’єкта критичної інфраструктури – формалізований або неформалізований опис методів та засобів реалізації ризиків безпеки;		
наслідок – результат події, що впливає на діяльність оператора критичної інфраструктури щодо сталого функціонування об’єкта критичної інфраструктури;		
оцінка ризиків безпеки на об’єктах критичної інфраструктури (далі – оцінка ризиків безпеки) – процес ідентифікації, аналізу та оцінювання вагомості ризику з метою забезпечення ухвалення рішень, спрямованих на мінімізацію виникнення кризових ситуацій;		
потенційна подія – подія, яка може статися чи не статися, може бути джерелом ризику, мати один або більше випадків реалізації, мати кілька причин та/або наслідків;		
ризик – потенційна можливість виникнення небажаних наслідків, яка визначається вірогідністю, джерелами		

реалізації та пов'язаними з ними наслідками;		
ризик безпеки на об’єктах критичної інфраструктури (далі – ризик безпеки) – потенційна можливість порушення стану захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури;		
система управління ризиками безпеки на об’єктах критичної інфраструктури (далі – система управління ризиками безпеки) – це сукупність задокументованих і затверджених політики, правил, методик і процедур управління ризиками безпеки, які визначають порядок дій оператора критичної інфраструктури, спрямованих на здійснення систематичного процесу вимірювання, моніторингу, контролю, звітування та обробки ризиків безпеки, в тому числі Паспорт безпеки на об’єкт критичної інфраструктури;		
управління ризиками безпеки на об’єктах критичної інфраструктури (далі – управління ризиками безпеки) – процес прийняття рішень на підставі обробки ризиків безпеки та організації заходів, які направлені на зниження (виключення) ймовірності інциденту		

безпеки критичної інфраструктури та мінімізацію можливих наслідків такого інциденту.		
Інші терміни вживаються у значеннях, наведених у Законі України «Про критичну інфраструктуру».		
3. Метою створення системи управління ризиками безпеки є інтеграція управління ризиками у важливі види діяльності та функції критичної інфраструктури, включаючи прийняття рішень оператором критичної інфраструктури.		
4. Оператор критичної інфраструктури, у тому числі європейської критичної інфраструктури, у співпраці з секторальним органом у сфері захисту критичної інфраструктури розробляє плани захисту об’єкта критичної інфраструктури відповідно до проектних загроз критичній інфраструктурі національного рівня, проектних загроз критичній інфраструктури секторального рівня та проектних загроз критичній інфраструктурі об’єктового рівня, які є невід’ємною частиною Паспорту безпеки на об’єкт критичної інфраструктури, розробленого відповідно до Порядку розроблення та погодження паспорта безпеки на об’єкт	Виключити.	Дана вимога щодо паспортизації передбачена напряму у ЗУ «Про критичну інфраструктуру» та деталізована у Порядку розроблення та погодження паспорта безпеки на об’єкт критичної інфраструктури (постанова КМУ від 04.08.2023 № 818). Не доцільно дублювати ще в одному НПА.

критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від _____ № ____.		
5. Оператор критичної інфраструктури повинен забезпечити інтеграцію управління ризиками безпеки в усі організаційні заходи шляхом:		
налаштування та впровадження всіх компонентів системи управління ризиками безпеки (проєктування, впровадження, оцінка та постійне вдосконалення системи управління ризиками безпеки);		
розробка та затвердження регламентуючих документів (політики, регламенту, процедури), які встановлюють підхід до управління ризиками безпеки, плану або порядку дій;		
забезпечення необхідними ресурсами для управління ризиками безпеки;		
розподілу повноважень, відповідальності та підзвітності на відповідних рівнях в організації (рівень підрозділу з управління ризиками/головного ризик-менеджера (за наявності), керівника оператора критичної інфраструктури, вищих **статутних** органів управління (за наявності).	розподілу повноважень, відповідальності та підзвітності на відповідних рівнях в організації (рівень підрозділу з управління ризиками/головного ризик-менеджера (за наявності), керівника оператора критичної інфраструктури, вищих органів управління (за наявності).	Не існує такого поняття «статутний орган управління».

У разі, якщо оператором критичної інфраструктури не забезпечено створення та діяльність підрозділу з управління ризиками/головного ризик-менеджера, його функції виконує керівник оператора критичної інфраструктури.		
6. Підрозділ з управління ризиками/головний ризик-менеджер (за наявності) виконує такі функції з управління ризиками безпеки:		
1) забезпечує виконання заходів з метою ефективного функціонування системи управління ризиками безпеки;		
2) забезпечує своєчасне виявлення, вимірювання, моніторинг, контроль та звітування керівнику оператора критичної інфраструктури та/ або вищим **статутним** органам управління (за наявності) щодо суттєвих ризиків безпеки;	2) забезпечує своєчасне виявлення, вимірювання, моніторинг, контроль та звітування керівнику оператора критичної інфраструктури та/ або вищим органам управління (за наявності) щодо суттєвих ризиків безпеки;	Не існує такого поняття «статутний орган управління».
3) забезпечує моніторинг, контроль наближення величини ризиків безпеки до лімітів ризику та ініціює рішення керівника оператора критичної інфраструктури та/або вищих **статутних** органів управління (за наявності) щодо вжиття заходів для попередження, пом'якшення та/або уникнення ризиків безпеки;	3) забезпечує моніторинг, контроль наближення величини ризиків безпеки до лімітів ризику та ініціює рішення керівника оператора критичної інфраструктури та/або вищих органів управління (за наявності) щодо вжиття заходів для попередження, пом'якшення та/або уникнення ризиків безпеки;	Не існує такого поняття «статутний орган управління».
4) готує звіти щодо ризиків безпеки;		

5) розробляє та підтримує в актуальному стані методики, інструменти та моделі, що використовуються для аналізу впливу різних факторів ризиків;		
6) здійснює вимірювання ризиків;		
7) складає профіль ризиків безпеки об’єктів критичної інфраструктури оператора критичної інфраструктури;		
8) готує висновки щодо ідентифікованих і задокументованих ризиків безпеки;		
9) розробляє, бере участь у розробленні внутрішніх документів з питань управління ризиками безпеки.		
7. Ризики безпеки включають, зокрема:		
1) матеріальні ризики, до яких відносяться фізичні та природні ризики для частин активів, критичних для функціонування об’єкта критичної інфраструктури (фізичний доступ до об’єкта критичної інфраструктури, об’єктів інфраструктури, систем, їх частин), в тому числі аварія, катастрофа, епідемія, стихійне лихо, епізоотія, епіфітотія, пожежа, застосування засобів ураження, що призвели або можуть призвести до людських і матеріальних втрат, а також велике зараження людей і тварин;		
2) ризики кібербезпеки та інформаційної безпеки – ризики для	2) ризики кібербезпеки та інформаційної безпеки – ризики для	Згідно ЗУ «Про основні засади забезпечення кібербезпеки України»

інформаційних, комунікаційних та інформаційно-комунікаційних систем, їх частин, які забезпечують стале функціонування об’єкта критичної інфраструктури;	інформаційних, комунікаційних та інформаційно-комунікаційних систем, їх частин, які **включено в національний перелік як об’єкт критичної інформаційної інфраструктури та** забезпечують стале функціонування об’єкта критичної інфраструктури;	об’єкт критичної інформаційної інфраструктури - комунікаційна або технологічна система об’єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об’єкта критичної інфраструктури
3) ризики, пов’язані з людським капіталом – ризики, які створює персонал (працівники) об’єкта критичної інфраструктури;	3) ризики, пов’язані з людським **фактором** – ризики, які створює персонал (працівники) об’єкта критичної інфраструктури;	Пропонуємо визначати не людський капітал, а людський фактор, як вже застосовується у НПА які регулюють діяльність атомних станцій. Наприклад: Людський фактор - індивідуальні характеристики персоналу, які впливають на експлуатацію енергоблока атомної станції (позитивно чи негативно) (Наказ Держінспекції ядерного регулювання України Наказ № 411 від 12.07.2021)
4) ризики ланцюжка постачання – ризик зриву, злочинного або ненавмисного використання ланцюгів постачання, що призводить до порушення стійкості критичної інфраструктури.		
Оператор критичної інфраструктури визначає ризики безпеки з обов’язковим урахуванням визначеного цим пунктом Вимог переліком, а також інших		

суттєвих ризиків, які можуть впливати на забезпечення функціональності, безперервності роботи, відновлюваності, цілісності і стійкості критичної інфраструктури.		
8. Оператор критичної інфраструктури повинен розробити та затвердити об’єктовий план заходів щодо забезпечення безпеки та стійкості критичної інфраструктури (далі – план), який повинен включати, зокрема:		
визначення суттєвих ризиків;		
план мінімізації ризиків для запобігання інцидентів та критичних ситуацій, де має бути враховано ризики для активів критичної інфраструктури.		
9. Для забезпечення стійкості критичної інфраструктури оператор критичної інфраструктури:		
оцінює та визначає необхідний для сталого функціонування об’єкта критичної інфраструктури персонал (працівників) та здійснює бронювання військовозобов’язаних в порядку визначеному чинним законодавством;		
забезпечує підготовку та навчання персоналу;		
здійснює заходи щодо забезпечення належними умовами праці на об’єкті критичної інфраструктури, зокрема для тривалого перебування в робочих		

приміщеннях;		
визначає засоби зв'язку для оповіщення та інформування персоналу (працівників).		Потребує доопрацювання в частині уточнення про що саме має здійснюватися інформування персоналу
10. Оператор критичної інфраструктури повинен зазначити в плані та забезпечити:		
1) альтернативним робочим приміщенням (альтернативним місцем розташування) у разі відсутності постійних робочих приміщень. Для цього оператор критичної інфраструктури оцінює особливості об’єкта критичної інфраструктури;		
2) визначення відповідної інфраструктури (альтернативне місце розташування), яка розташована щонайменше на відстані 50 кілометрів від існуючої інфраструктури та придатна для забезпечення життєво важливих функцій та / або послуг;		
3) розроблення процедури переміщення персоналу (працівників) та технологічного обладнання (далі – обладнання) на альтернативні робочі місця, визначаючи необхідні засоби та заходи;		
4) визначення можливості залучення персоналу (працівників), обладнання та матеріально-технічних		

ресурсів, наявних в альтернативному місці;		
5) визначення обладнання та матеріально-технічних ресурсів, необхідних для надання життєво важливих функцій та/або послуг, включно з:		
переліком критичних елементів об’єкта критичної інфраструктури та матеріально-технічних засобів;		
визначенням альтернатив критичних елементів об’єкта критичної інфраструктури та матеріально-технічних засобів, можливостей заміни;		
забезпеченням безперебійності роботи у разі втрати обладнання та матеріально-технічних засобів;		
забезпеченням здійснення ремонтних робіт, оновлення, вдосконалення або створення альтернатив обладнання (включаючи зміну зовнішніх постачальників);		
своєчасним резервним копіюванням інформаційних, інформаційно-комунікаційних та інших систем і резервування обладнання для забезпечення доступу до даних, систем і процесів;		
дублюванням підключення електропостачання інформаційних систем та обладнання до системи		

автономного електропостачання;		
6) організацію зв’язку та енергопостачання на постійних та альтернативних робочих місцях;		
7) визначення ресурсів необхідних для сталого функціонування критичної інфраструктури, а також способів їх постачання;		
8) стабільність поставок, зокрема:		
визначити головних постачальників та їх географічне розташування з метою виявлення вразливостей у разі порушення ланцюгів постачання та визначення можливих альтернатив;		
розподілити ризики постачання, уникнувши залежності лише від одного іноземного постачальника;		
не залучати до ланцюгів постачання суб’єктів господарювання, до яких застосовано спеціальні економічні та інші обмежувальні заходи (санкції);		
визначити можливість надання переваги національним ланцюгам постачання та національним виробникам, переробникам і постачальникам послуг.		
9) визначення алгоритму дій під час кризової ситуації, включно з заходами:		
забезпечення надання життєво важливих функцій та/або послуг;		
визначення порядку зв’язку з персоналом (працівниками);		

визначення порядку та правил дій групи антикризового управління, а також механізм координації з секторальним органом у сфері захисту критичної інфраструктури, функціональними органами у сфері захисту критичної інфраструктури та уповноваженим органом у сфері захисту критичної інфраструктури України;		
визначення протоколу кризової комунікації, що включає засоби та заходи комунікації для структурних підрозділів оператора критичної інфраструктури та суб'єктів національної системи захисту критичної інфраструктури;		
визначення процедури оперативного реагування на інциденти шляхом впровадження процедур та протоколів кризового менеджменту.		
Підпункти 1-4 цього пункту зазначаються в плані та забезпечуються за можливості здійснення відповідних заходів.		
11. План повинен також передбачити перевірку та визначення ефективності системи управління ризиками безпеки, включаючи навчання у співпраці з секторальним органом у сфері захисту критичної інфраструктури, функціональними		

органами у сфері захисту критичної інфраструктури та уповноваженим органом у сфері захисту критичної інфраструктури України не рідше одного разу на три роки.		
12. План та зміни до плану затверджуються оператором критичної інфраструктури.		
13. Система управління ризиками безпеки повинна відповідати наступним вимогам:		
інтегрованість – управління ризиками є невід'ємною частиною всієї діяльності оператора критичної інфраструктури;		
структурованість і комплексність - підхід до управління ризиками сприяє послідовним і порівнюваним результатам;		
індивідуальність – структура та процес управління ризиками адаптовані та пропорційні зовнішньому та внутрішньому контексту оператора критичної інфраструктури, пов’язаному з його цілями;		
динамічність – реагування на зміну зовнішнього і внутрішнього контексту;		
належна поінформованість – вхідні дані для управління ризиками безпеки базуються на попередній та поточній інформації, а також на майбутніх очікуваннях;		

управління людським капіталом – професійні навички, знання, фізичні здібності та соціально-психологічні відносини персоналу, що впливають на стійке функціонування об’єктів критичної інфраструктури.	управління людським **фактором** – професійні навички, знання, фізичні здібності та соціально-психологічні відносини персоналу, що впливають на стійке функціонування об’єктів критичної інфраструктури.	Редакційно
14. Управління ризиками безпеки здійснюється у такому порядку:		
організація управління ризиками безпеки;		
оцінка ризиків безпеки;		
обробка ризиків безпеки;		
моніторинг та перегляд актуальності ризиків безпеки;		
обмін інформацією та взаємодія із суб’єктами національної системи захисту критичної інфраструктури.		
15. Організація управління ризиками безпеки включає:		
визначення вихідних даних щодо функціонування об'єкту критичної інфраструктури (область застосування, внутрішні і зовнішні чинники, критерії щодо управління ризиками безпеки);		
визначення суб’єктів національної системи захисту критичної інфраструктури, які виконують завдання/заходи щодо управління ризиками безпеки;		
формування структурованих та чітких		

підходів до організації управління ризиками безпеки та їх застосування;		
визначення методів, інструментів та механізмів, які використовуються в ході управління ризиками безпеки;		
ідентифікацію та планування ресурсів, необхідних для управління ризиками безпеки, зокрема людські, інформаційні, фінансові, матеріально-технічні;		
визначення засобів та заходів щодо забезпечення комунікації в ході управління ризиками безпеки, в тому числі взаємодія з суб'єктами національної системи захисту критичної інфраструктури;		
забезпечення узгодженості заходів щодо управління ризиками безпеки із заходами, що сплановані за іншими напрямами функціонування об'єкта критичної інфраструктури.		
Управління ризиками безпеки здійснюється із застосуванням різних методів якісного та/або кількісного характеру, у тому числі методів, наведених у ДСТУ IEC/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).	Управління ризиками безпеки здійснюється із застосуванням національних та міжнародних стандартів управління ризиками безпеки.	Зазначення конкретних стандартів звужує перелік вимог, яким повинні відповідати об'єкти критичної інфраструктури та збільшує ризики безпеки ОКІ.

Оцінка ризиків безпеки передбачає визначення вірогідності, джерел ризиків, характеристик інцидентів безпеки критичної інфраструктури, ймовірності та вагомості їх наслідків і сценаріїв розвитку, а також методів управління ризиками та їх ефективності.		
У ході оцінки ризиків безпеки проводяться:		
ідентифікація ризиків безпеки;		
аналіз ризиків безпеки;		
оцінка відповідності ризиків безпеки варіантам рішень щодо їх обробки, у тому числі планам захисту об’єктів критичної інфраструктури.		
16. Ідентифікація ризиків безпеки передбачає визначення всіх потенційно можливих інцидентів, які можуть мати негативний вплив на функціонування об’єкта критичної інфраструктури та документуванні показників (характеристик) та сценаріїв їх розвитку.		
Ідентифікація ризиків безпеки проводиться шляхом:		
складання переліку ризиків безпеки;		
формування сценаріїв розвитку інцидентів;		
ідентифікація найбільш вірогідних для даного об'єкта критичної інфраструктури показників ризику		

безпеки.		
17. Аналіз ризиків безпеки передбачає вивчення ідентифікованих ризиків безпеки щодо рівня їх потенційної загрози та можливого впливу на функціонування об’єкта критичної інфраструктури.		
Аналіз ризиків безпеки проводиться шляхом:		
визначення причин та джерел виникнення ризиків безпеки;		
визначення вірогідності та впливу ідентифікованих ризиків безпеки на підставі отриманих кількісних, якісних або комбінованих характеристик ризиків безпеки;		
ранжування (визначення пріоритетності) ризиків безпеки на підставі вивчення їх кількісних, якісних або комбінованих показників ризиків безпеки.		
Під час аналізу ризиків безпеки необхідно попередньо прийняти рішення, які ризики обробляти, при цьому відхилити незначні ризики, оброблення яких недоцільне.		
Аналіз ризиків безпеки здійснюється на основі аналізу досвіду суб’єктів національної системи захисту критичної інфраструктури, у разі наявності, та аналізу рішень прийнятих внаслідок інцидентів, які виникали раніше.		

18. Оцінка відповідності ризиків безпеки варіантам рішень щодо їх обробки передбачає визначення відповідності результатів аналізу ризиків безпеки рішенням, які можуть бути прийняті щодо управління такими ризиками.		
19. Обробка ризиків безпеки передбачає визначення завдань (заходів), які направлені на зниження (виключення) ймовірності інциденту критичної інфраструктури та мінімізацію можливих наслідків такого інциденту.		
Обробка ризиків безпеки проводиться шляхом:		
створення моделі загроз безпеці об’єкта критичної інфраструктури;		
визначення підходів до обробки кожного ідентифікованого ризику безпеки;		
визначення прийнятних (не потребують додаткових заходів для мінімізації наслідків та ймовірності їх настання) та неприйнятних ризиків безпеки;		
формування переліку альтернативних заходів протидії ризикам;		
визначення найбільш ефективного заходу протидії ризикам безпеки, зокрема з урахуванням необхідних ресурсів;		

визначення супутніх ризиків безпеки, які можуть виникнути у зв’язку із запровадженням додаткових заходів протидії ризикам безпеки та проведення їх аналізу;		
підготовки об’єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, а також планів захисту об’єкта критичної інфраструктури, що є невід’ємною складовою паспорта безпеки на об’єкт критичної інфраструктури.		
20. Моніторинг та перегляд актуальності ризиків безпеки передбачає забезпечення оператора критичної інфраструктури актуальною, об’єктивною та достовірною інформацією з питань, що відносяться до управління ризиками безпеки.		
Перегляд актуальності ризиків безпеки проводиться не рідше ніж раз на три роки шляхом:		
перевірки актуальності інформації щодо стану захищеності об’єкта критичної інфраструктури, яка зазначена в паспорті безпеки на об’єкт критичної інфраструктури;		
прогнозування виникнення нових інцидентів, ступеня вразливості об’єкта критичної інфраструктури та результатів		

наслідків впливу;		
відстеження загальної ситуації в системі управління ризиками безпеки.		
21. Обмін інформацією та взаємодія суб'єктів національної системи захисту критичної інфраструктури здійснюються відповідно до Регламенту обміну інформацією та плану взаємодії, затверджених Кабінетом Міністрів України від 14 жовтня 2022 р. № 1174.		