МІНІСТЕРСТВО РОЗВИТКУ ЕКОНОМІКИ, ТОРГІВЛІ ТА СІЛЬСЬКОГО ГОСПОДАРСТВА УКРАЇНИ
(Мінекономіки)
вул. М. Грушевського 12/2, м. Київ, 01008, тел. (044)200-47-53, факс (044)253-63-71
E-mail: meconomy@me.gov.ua, http://www.me.gov.ua, код ЄДРПОУ 37508596

На № _____ від _____

Державна регуляторна служба України

Щодо розгляду проекту Закону України

Відповідно до статті 21 Закону України "Про засади державної регуляторної політики у сфері господарської діяльності" та на виконання рішення Ради національної безпеки і оборони України від 29.12.2016 "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури", уведеного в дію Указом Президента України від 16.01.2017 № 8, Мінекономіки розроблено проект Закону України "Про критичну інфраструктуру та її захист".

Просимо розглянути та погодити зазначений проект Закону у п'ятиденний строк.

Додатки: 1. Проект Закону України на 29 арк.;
2. Пояснювальна записка на 4 арк.;
3. Порівняльна таблиця на 6 арк.;
4. Аналіз регуляторного впливу на 18 арк.;
5. Підтвердження оприлюднення проекту на 1 арк.

Міністр **Ігор ПЕТРАШКО**

Сугак О. В. 200-47-73*3938

ПРОЕКТ

ЗАКОН УКРАЇНИ

Про критичну інфраструктуру та її захист

Цей Закон встановлює принципи та напрями розбудови державної системи захисту критичної інфраструктури, визначає правові та організаційні засади забезпечення її діяльності і є складовою частиною законодавства України у сфері національної безпеки.

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення основних термінів

1. У цьому Законі терміни вживаються в такому значенні:

1) акт несанкціонованого втручання — діяння, що створило загрозу безпечному функціонуванню об'єкта критичної інфраструктури та призвело до одного або декількох з таких наслідків: порушило його безперервність і стійкість; створило реальні чи потенційні загрози національній безпеці;

2) безпека критичної інфраструктури — стан захищеності критичної інфраструктури, за якого забезпечується функціональність, безперервність роботи, цілісність і стійкість об'єктів критичної інфраструктури;

3) державна система захисту критичної інфраструктури – це сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади, органів місцевого самоврядування, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури;

4) життєво важливі послуги — послуги, надання яких забезпечується державними установами, підприємствами та організаціями будь-якої форми власності і збої та переривання у наданні яких призводять до швидких негативних наслідків для національної безпеки;

5) життєво важливі функції — функції, що виконуються органами державної влади, державними установами, підприємствами та організаціями будь-якої форми власності, порушення яких призводить до швидких негативних наслідків для національної безпеки;

6) захист критичної інфраструктури — всі види діяльності, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації;

7) категорія критичності об'єкта критичної інфраструктури — ступінь важливості об'єкта критичної інфраструктури, класифікована залежно від його впливу на виконання важливих функцій та(або) надання життєво важливих послуг;

8) категоризація об’єктів інфраструктури — процес віднесення об’єктів інфраструктури до категорій критичності об’єктів інфраструктури;

9) кризова ситуація — порушення або загроза порушення штатного режиму функціонування критичної інфраструктури чи окремого її об’єкта, реагування на яке потребує залучення додаткових сил і ресурсів;

10) критична інфраструктура — сукупність об’єктів, які є стратегічно важливими для економіки і національної безпеки, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам;

11) критична технологічна інформація — дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об’єктів критичної інфраструктури;

12) об’єкт критичної інфраструктури — визначений у встановленому законодавством порядку складовий елемент критичної інфраструктури, функціональність, безперервність, цілісність і стійкість якого забезпечують реалізацію життєво важливих послуг та функцій;

13) оператор критичної інфраструктури — підприємство, установа, організація, юридична та/або фізична особа-підприємець, якому/якій на правах власності, оренди або на інших законних підставах належать об’єкти критичної інфраструктури та який/яка відповідає за їх поточне функціонування;

14) охорона об’єктів критичної інфраструктури — комплекс режимних, інженерних, інженерно-технічних та інших заходів, які організовуються і проводяться суб’єктами державної системи захисту критичної інфраструктури з метою запобігання та/або недопущення чи припинення протиправних дій (чи актів несанкціонованого втручання) на об’єктах критичної інфраструктури;

15) паспорт безпеки — документ встановленої форми, який містить структуровані дані про об’єкт критичної інфраструктури та визначає комплекс заходів, що вживаються оператором критичної інфраструктури з метою захисту цього об’єкта від усіх видів загроз (відомості, що містяться у паспорті безпеки, можуть бути віднесені до відомостей, що становлять службову інформацію, державну або комерційну таємницю);

16) проектна загроза об’єкту критичної інфраструктурі - документ встановленої форми, який визначає властивості, характеристики реальних і потенційних загроз об’єкту критичної інфраструктурі, на унеможливлення яких (з урахуванням ймовірності їх реалізації) повинна бути спланована система захисту критичної інфраструктури;

17) рівень критичності об’єкта критичної інфраструктури — відносна міра важливості об’єкта, якою враховується його вплив на можливість виконання життєво важливих функцій та надання життєво важливих послуг;

18) режим функціонування критичної інфраструктури — визначені умови та вимоги до функціонування критичної інфраструктури залежно від стану і динаміки розвитку ситуації (штатний режим функціонування; режим запобігання виникнення кризової ситуації; режим функціонування в кризовій ситуації; режим відновлення);

19) реєстр об’єктів критичної інфраструктури – перелік найбільш важливої для життєдіяльності суспільства та держави критичної інфраструктури, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості та здійснюється моніторинг їх дотримання;

20) сектор критичної інфраструктури – сукупність об’єктів критичної інфраструктури, які належать до одного сектору економіки та/або мають спільну функціональну спрямованість;

21) стійкість критичної інфраструктури – стан критичної інфраструктури, за якого забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду;

22) секторальний орган у сфері захисту критичної інфраструктури - державні органи, визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури у окремому секторі критичної інфраструктури;

23) функціональний орган у сфері захисту критичної інфраструктури – державні органи, які визначені відповідальними за функціонування окремих державних систем захисту та реагування;

24) цифрова послуга – послуга інформаційного суспільства, яка зазвичай надається дистанційно, за допомогою засобів комунікацій та за індивідуальним запитом особи, яка є отримувачем послуги, та для цілей цього Закону відноситься до одного з таких видів послуг, як електронний торговий майданчик, електронна пошукова система, послуга хмарних обчислень).

2. Інші терміни вживаються у значенні, наведеному в Кодексі цивільного захисту України, Кримінальному кодексі України, Законах України “Про національну безпеку України”, “Про боротьбу з тероризмом”, “Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання”, “Про об’єкти підвищеної небезпеки”, “Про основні засади забезпечення кібербезпеки України”, “Про інформацію”, “Про оперативно-розшукову діяльність”, “Про контррозвідувальну діяльність”, “Про правовий режим надзвичайного стану”, “Про правовий режим воєнного стану”.

Стаття 2. Правова основа діяльності у сфері захисту критичної інфраструктури

1. Правову основу діяльності у сфері захисту критичної інфраструктури становлять Конституція України, міжнародні договори, що стосуються захисту критичної інфраструктури, згода на обов’язковість яких надана Верховною Радою України, цей Закон, інші закони України, а також інші нормативно-правові акти, що прийняті на виконання цього Закону.

Стаття 3. Сфера застосування цього Закону

1. Цей Закон унормовує діяльність у сфері захисту критичної інфраструктури у мирний час та в умовах надзвичайного стану. Діяльність у сфері захисту критичної інфраструктури в умовах воєнного стану регулюється іншими законами України.

Розділ II
ОСНОВНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 4. Засади державної політики захисту критичної інфраструктури

1. Забезпечення захисту критичної інфраструктури є складовою частиною забезпечення національної безпеки України.

2. Державна політика у сфері захисту критичної інфраструктури ґрунтується на засадах:

1) визнання необхідності забезпечення безперервності та стійкості функціонування критичної інфраструктури;

2) визначення законодавчих вимог до захисту критичної інфраструктури;

3) визначення повноважень та засад відповідальності суб'єктів державної системи захисту критичної інфраструктури;

4) створення умов, спрямованих на мінімізацію реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів;

5) створення умов швидкого відновлення функціонування критичної інфраструктури у випадку реалізованих загроз, кризових ситуацій;

6) створення системи виявлення загроз критичній інфраструктурі;

7) запровадження взаємодії держави, суб'єктів господарювання, експертного середовища та населення з питань забезпечення захисту та стійкості критичної інфраструктури;

8) забезпечення міжнародного співробітництва у сфері захисту критичної інфраструктури.

3. Державна політика у сфері захисту критичної інфраструктури спрямовується на формування комплексу організаційних, нормативно-правових, інженерно-технічних, експлуатаційних, наукових та інших заходів, спрямованих на забезпечення безпеки та стійкості критичної інфраструктури.

Стаття 5. Мета та завдання державної політики у сфері захисту критичної інфраструктури

1. Метою державної політики у сфері захисту критичної інфраструктури є забезпечення безперебійного та стійкого функціонування об'єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх

функціонування, прогнозування та запобігання кризовим ситуаціям на об’єктах критичної інфраструктури, підвищення рівня їх захисту, безпеки та стійкості до загроз будь-якого типу.

2. До завдань формування і реалізації державної політики захисту критичної інфраструктури належать:

1) забезпечення безпеки, стійкості та цілісності критичної інфраструктури;

2) попередження кризових ситуацій, що порушують стале функціонування критичної інфраструктури;

3) створення та забезпечення функціонування державної системи захисту критичної інфраструктури, у тому числі шляхом визначення Уповноваженого органу у справах захисту критичної інфраструктури України, а також компетенції і повноважень у сфері захисту критичної інфраструктури інших суб’єктів державної системи захисту критичної інфраструктури;

4) розроблення нормативно-правової бази з питань забезпечення безпеки та стійкості об’єктів критичної інфраструктури;

5) розроблення та реалізація державних цільових програм із захисту критичної інфраструктури;

6) розроблення комплексу заходів з виявлення, запобігання та ліквідації наслідків інцидентів на об’єктах критичної інфраструктури;

7) встановлення обов’язкових вимог із забезпечення безпеки об’єктів критичної інфраструктури, їхньої захищеності на всіх етапах життєвого циклу, в тому числі під час створення, прийняття в експлуатацію, модернізації;

8) аналіз викликів та загроз, що впливають на стійкість критичної інфраструктури, оцінка стану її захищеності;

9) розроблення методології аналізу результативності державної політики у сфері захисту критичної інфраструктури.

Стаття 6. Основні принципи функціонування державної системи захисту критичної інфраструктури

1. До основних принципів функціонування державної системи захисту критичної інфраструктури належать:

1) єдність методологічних засад;

2) координованість;

3) державно-приватна взаємодія;

4) конфіденційність комерційної інформації;

5) міжнародне співробітництво.

Стаття 7. Рівні управління державної системи захисту критичної інфраструктури

1. Державна система захисту критичної інфраструктури має такі рівні управління:

1) державний рівень, управління на якому здійснюється Президентом України, Радою національної безпеки і оборони України, Кабінетом Міністрів України, Уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень, згідно з цим Законом;

2) регіональний та галузевий рівень, управління на якому здійснюється органами державної влади, які визначені у встановленому законодавством порядку відповідальними за формування та реалізації державної політики у сфері захисту критичної інфраструктури у окремому секторі критичної інфраструктури та відповідальними за функціонування окремих державних систем захисту та реагування;

3) місцевий рівень, управління на якому здійснюється місцевими органами виконавчої влади (військовими у разі утворення) адміністраціями, органами місцевого самоврядування, об'єднаними територіальними громадами, в межах повноважень, покладених на них цим Законом;

4) об'єктовий рівень, управління на якому здійснюється оператором критичної інфраструктури на підставі нормативно-правових та регуляторних актів у сфері захисту критичної інфраструктури.

Розділ ІІІ
КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ

Стаття 8. Об'єкти критичної інфраструктури

1. Віднесення об'єктів критичної інфраструктури та включення до Реєстру об'єктів критичної інфраструктури здійснюється в порядку встановленому Кабінетом Міністрів України.

2. Віднесення об'єктів до критичної інфраструктури визначається за сукупністю критеріїв, що визначають їх важливість для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський фактор чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму.

До таких критеріїв належать:

1) виконання функцій із забезпечення життєво важливих національних інтересів;

2) існування викликів і загроз, що можуть виникати щодо об'єктів критичної інфраструктури;

3) ймовірність завдання значної шкоди нормальним умовам життєдіяльності населення;

4) уразливість цих об’єктів, тяжкість можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода: здоров’ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам державного значення; обороноздатності; іміджу країни;

5) масштабність негативних наслідків для держави, які: вплинуть на діяльність стратегічно важливих об’єктів для кількох секторів життєзабезпечення чи призведуть до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначаться на діяльності ряду інших секторів;

6) тривалість ліквідації таких наслідків та дія подальшого негативного впливу на інші сектори держави;

7) вплив на функціонування суміжних секторів критичної інфраструктури.

Стаття 9. Сектори критичної інфраструктури

1. Для організації ефективного забезпечення безпеки і стійкості критичної інфраструктури, з врахуванням специфіки забезпечення окремих життєво важливих функцій та послуг, визначаються сектори критичної інфраструктури.

2. Для секторів критичної інфраструктури визначаються особливості реалізації державної політики у сфері захисту критичної інфраструктури. Формування та реалізацію державної політики у відповідних секторах здійснюють секторальні органи у сфері захисту критичної інфраструктури.

3. Перелік секторів критичної інфраструктури та суб’єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах державної системи захисту критичної інфраструктури, визначається Кабінетом Міністрів України.

4. Вимогами щодо формування та реалізації державної політики у сфері захисту критичної інфраструктури є забезпечення таких життєво-важливих функцій та послуг:

- урядування та надання найважливіших державних послуг;

- енергозабезпечення;

- водопостачання та водовідведення;

- продовольче забезпечення;

- охорона здоров’я;

- інформаційні, комунікаційні та цифрові послуги;

- фінансові та банківські послуги;

- транспортне забезпечення;

- оборона;

- правопорядок;

- постачання теплової енергії.

Стаття 10. Категоризація об’єктів критичної інфраструктури

1. Для визначення рівня вимог до забезпечення захисту об’єктів критичної інфраструктури відповідно до рівня їх важливості для забезпечення окремих життєво важливих функцій та послуг, в межах секторів критичної інфраструктури здійснюється категоризація об’єктів критичної інфраструктури.

2. Категоризація об’єктів критичної інфраструктури здійснюється секторальними органами у сфері захисту критичної інфраструктури відповідно до секторальної специфіки та вимог секторального законодавства.

3. Секторальні органи у сфері захисту критичної інфраструктури складають та ведуть секторальні переліки об’єктів критичної інфраструктури.

Стаття 11. Складення та ведення Реєстру об’єктів критичної інфраструктури

1. Для цілей узгодження дій суб’єктів державної системи захисту критичної інфраструктури щодо важливої критичної інфраструктури формується Реєстр об’єктів критичної інфраструктури.

2. Збирання, узагальнення, попередній аналіз даних щодо об’єктів критичної інфраструктури та пропозиції щодо внесення таких об’єктів до Реєстру об’єктів критичної інфраструктури в межах визначених секторів здійснюється секторальними органами у сфері захисту критичної інфраструктури.

3. Реєстр об’єктів критичної інфраструктури формується та ведеться Уповноваженим органом у сфері захисту критичної інфраструктури на основі пропозицій суб’єктів державної системи захисту критичної інфраструктури.

4. Після внесення об’єкта до Реєстру об’єктів критичної інфраструктури секторальні органи у сфері захисту критичної інфраструктури повідомляють про це оператора об’єкта критичної інфраструктури для забезпечення його паспортизації та захисту об’єкта критичної інфраструктури відповідно до вимог цього Закону.

5. Порядок ведення Реєстру об’єктів критичної інфраструктури, внесення об’єктів до Реєстру, та надання інформації з нього встановлюються Кабінетом Міністрів України.

6. Відомості, що містяться у Реєстрі об’єктів критичної інфраструктури, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до законодавства у сфері захисту інформації та безпеки секретної інформації.

Стаття 12. Паспортизація об’єктів критичної інфраструктури

1. З метою проведення аналізу можливих основних загроз та потенційних негативних наслідків для об’єктів критичної інфраструктури, запобігання та попередження виникнення таких загроз для критичної інфраструктури оператори об’єктів критичної інфраструктури готують і подають на погодження до відповідних секторальних органів у сфері захисту критичної інфраструктури, Служби безпеки України та суб’єкта, на якого покладено забезпечення фізичної охорони, паспорт безпеки на кожний об'єкт критичної інфраструктури.

2. Паспорт безпеки на об’єкт критичної інфраструктури містить процедури ідентифікації об’єкта та заходи щодо його захисту й безпеки, а також визначає перелік відповідальних осіб, до завдань яких належить зв’язок та обмін інформацією з суб’єктами державної системи захисту критичної інфраструктури.

3. Паспорт безпеки розробляється (переглядається) з врахуванням вимог національної та секторальної проектних загроз.

4. Порядок розроблення паспорта безпеки на об’єкт критичної інфраструктури, його наповнення, зміст і строки подання встановлюються Кабінетом Міністрів України.

5. Оператор критичної інфраструктури несе відповідальність за достовірність даних, наведених у паспорті безпеки, своєчасність внесення до нього змін.

6. Відомості, що містяться у Паспорті безпеки є інформацією з обмеженим доступом, захист якої забезпечується відповідно до законодавства у сфері захисту інформації та безпеки секретної інформації.

Розділ IV
ДЕРЖАВНА СИСТЕМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 13. Формування та реалізація державної політики у сфері захисту критичної інфраструктури

1. Кабінет Міністрів України забезпечує проведення державної політики у сфері захисту критичної інфраструктури України, організовує та забезпечує необхідними силами, засобами і ресурсами функціонування державної системи захисту критичної інфраструктури.

2. Формування та реалізацію державної політики в окремих секторах критичної інфраструктури здійснюють секторальні та функціональні органи у сфері захисту критичної інфраструктури, відповідно до визначених законом повноважень.

3. Формування єдиних методологічних підходів та координації діяльності суб’єктів державної системи захисту критичної інфраструктури забезпечує Уповноважений орган у справах захисту критичної інфраструктури України.

4. Формування національної мережі ситуаційно-кризових центрів (інформаційно-аналітичних, диспетчерських), функцію яких здійснюють структурні підрозділи суб'єктів державної системи захисту критичної інфраструктури.

5. Для забезпечення обміну інформацією та взаємодії суб'єктів державної системи захисту критичної інфраструктури Кабінет Міністрів України затверджує Регламент обміну інформацією.

6. Обмін інформацією в рамках функціонування державної системи захисту критичної інфраструктури здійснюється з врахуванням вимог Закону України "Про державну таємницю".

Стаття 14. Суб'єкти державної системи захисту критичної інфраструктури

1. Суб'єктами державної системи захисту критичної інфраструктури є:

1) Кабінет Міністрів України;

1) Уповноважений орган у сфері захисту критичної інфраструктури України;

2) міністерства та інші центральні органи виконавчої влади;

3) Служба безпеки України;

4) правоохоронні та розвідувальні органи;

5) Збройні Сили України, інші військові формування, утворені відповідно до законів України;

6) місцеві державні (військові, у разі утворення) адміністрації;

7) органи місцевого самоврядування;

8) оператори критичної інфраструктури незалежно від форми власності;

9) підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки та стійкості критичної інфраструктури.

Стаття 15. Режими функціонування державної системи захисту критичної інфраструктури

1. Забезпечення захисту та стійкості критичної інфраструктури здійснюється в таких режимах її функціонування:

1) штатний режим — суб'єктами державної системи захисту критичної інфраструктури щодо оцінки можливих загроз та інформування щодо них. Функціонування інфраструктури здійснюється відповідно до проектного цільового призначення;

2) режим готовності та запобігання реалізації загроз — секторальними та функціональними органами у сфері захисту критичної інфраструктури: проводиться перевірка та переведення системи захисту до готовності забезпечити захист та

реагування на випадок реалізації загрози. Функціонування інфраструктури здійснюється відповідно до проектного цільового призначення;

3) режим реагування на виникнення кризової ситуації — суб'єктами державної системи захисту критичної інфраструктури із застосуванням заходів реагування на кризову ситуацію. Функціонування інфраструктури відбувається в режимі кризової ситуації, вводяться обмеження на режими роботи об'єктів інфраструктури, економічні умови господарювання, доступу до об'єктів;

4) режим відновлення штатного функціонування — суб'єктами державної системи захисту критичної інфраструктури: застосовуються заходи щодо повернення параметрів функціонування критичної інфраструктури до штатного режиму. Функціонування інфраструктури здійснюється з обмеженнями відповідно до визначених термінів ліквідації наслідків кризи.

2. Для кожного режиму функціонування критичної інфраструктури відповідальними за сектори критичної інфраструктури розробляються плани взаємодії з іншими суб'єктами державної системи захисту, який погоджується у встановленому законодавством порядку.

3. Рішення щодо оголошення режимів функціонування критичної інфраструктури та запровадження окремих правових станів приймається секторальними органами у сфері захисту критичної інфраструктури, відповідальним за сектор критичної інфраструктури.

Стаття 16. Уповноважений орган у сфері захисту критичної інфраструктури

1. Уповноважений орган у сфері захисту критичної інфраструктури:

1) координує діяльність міністерств та інших центральних та місцевих органів виконавчої влади у сфері захисту критичної інфраструктури;

2) узагальнює пропозиції суб'єктів державної системи захисту критичної інфраструктури, формує та веде Реєстр об'єктів критичної інфраструктури;

3) взаємодіє з операторами критичної інфраструктури з питань забезпечення захисту об'єктів, включених до Реєстру об'єктів критичної інфраструктури;

4) здійснює оцінку захищеності об'єктів критичної інфраструктури, внесених до Реєстру об'єктів критичної інфраструктури;

5) проводить із залученням секторальних та функціональних органів у сфері захисту критичної інфраструктури оцінку загроз критичній інфраструктурі на державному рівні та оцінку загроз національній безпеці внаслідок реалізації загроз критичній інфраструктурі;

6) готує Оцінку ризиків критичній інфраструктурі національного рівня;

7) погоджує проектні загрози критичній інфраструктурі секторального рівня;

8) готує рекомендації щодо визначення вимог до забезпечення захисту та стійкості секторів критичної інфраструктури відповідно категорій об'єктів критичної інфраструктури;

9) надає пропозиції Кабінету Міністрів України щодо:

- Національного плану захисту та забезпечення стійкості критичної інфраструктури;

- порядку розроблення, форми та змісту паспорту безпеки об'єкта критичної інфраструктури;

- порядку розроблення, форми та змісту планів заходів щодо захисту критичної інфраструктури, які приймаються на державному рівні;

10) розробляє та подає на затвердження Ради національної безпеки і оборони України Проектну загрозу критичній інфраструктурі національного рівня;

11) готує висновки та рекомендації власнику/оператору критичної інфраструктури щодо зміни права власності, цільового призначення чи режиму функціонування об'єкта критичної інфраструктури;

12) здійснює інші повноваження, передбачені цим Законом.

3. Виконання функцій Уповноваженого органу у сфері захисту критичної інфраструктури, покладається на Апарат Ради національної безпеки і оборони України.

Стаття 17. Функціональні органи у сфері захисту критичної інфраструктури

1. До переліку окремих державних систем захисту та реагування із якими державна система захисту критичної інфраструктури здійснює взаємодію та обмін інформацією входять:

1) Єдина державна система цивільного захисту;
2) Державна система фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів інших джерел іонізуючого випромінювання;
3) Єдина державна система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків;
4) Національна система кібербезпеки;
5) Органи сектору безпеки (спеціальні та правоохоронні органи);
6) Органи сектору оборони (Збройні Сили України та система територіальної оборони).

2. Органи державної влади, які визначені відповідальними за функціонування окремих державних систем:

1) беруть участь, у встановленому законодавством порядку, у реагуванні на кризові ситуації, пов'язані із забезпеченням безпеки та стійкості критичної інфраструктури;
2) готують пропозиції щодо включення об'єктів інфраструктури до Реєстру об'єктів критичної інфраструктури;

3) формують перелік об’єктів критичної інфраструктури, що належать до сфери їх управління;

4) надають секторальним органам у сфері захисту критичної інфраструктури, власникам та операторам інфраструктури консультації щодо загроз критичній інфраструктурі та заходів щодо їх нейтралізації;

5) здійснюють іншу діяльність для захисту критичної інфраструктури в межах повноважень, визначеними законами, що регулюють діяльність суб’єктів захисту критичної інфраструктури, зокрема:

- забезпечення оцінки загроз та ризиків критичній інфраструктурі у відповідних сферах;
- участь у проведенні оцінки загроз та ризиків критичній інфраструктурі на загальнодержавному рівні;
- формування пропозицій до національної та секторальних проектних загроз;
- організацію взаємодії та обміну інформацією із іншими суб’єктами державної системи захисту критичної інфраструктури;
- моніторинг рівня безпеки об’єктів критичної інфраструктури у відповідних сферах.

Стаття 18. Служба безпеки України

1. Служба безпеки України у сфері захисту критичної інфраструктури:

1) бере участь у формуванні та реалізації державної політики у сфері захисту критичної інфраструктури;

2) бере участь у контрдиверсійних заходах із захист об’єктів критичної інфраструктури, здійснює їх контррозвідувальне забезпечення, захист економічного та науково-технічного потенціалу об’єктів критичної інфраструктури, обмін інформацією з питань оцінки загроз та реагування на загрози і кризові ситуації, а також ліквідації їх наслідків, пов’язаних із протиправною діяльністю спеціальних служб іноземних держав, негативного впливу окремих організацій, груп та осіб, а також розробляє заходи реагування на них у взаємодії з іншими суб’єктами державної системи захисту критичної інфраструктури;

3) здійснює заходи з попередження, виявлення, запобігання та припинення проявів фінансування тероризму з використанням об’єктів критичної інфраструктури;

4) бере участь у перевірці походження інвестицій з метою недопущення спроб використання об’єктів критичної інфраструктури у фінансуванні терористичної та іншої протиправної діяльності;

5) попереджує та протидіє актам несанкціонованого втручання в діяльність об’єктів критичної інфраструктури;

6) контролює у межах компетенції здійснення на об’єктах критичної інфраструктури заходів з попередження, виявлення, запобігання та припинення витоку інформації з обмеженим доступом, втрати її матеріальних носіїв, локалізації можливих наслідків, а також виявлення та усунення існуючих для цього передумов;

7) здійснює контррозвідувальне забезпечення процесу укладання і реалізації операторами (власниками) об’єктів критичної інфраструктури угод, спрямованих на підвищення рівня надійності, стійкості та безпечного функціонування об’єктів критичної інфраструктури;

8) бере участь у розробленні категоризації, визначенні критеріїв та порядку оцінки стану безпеки та захищеності об’єктів критичної інфраструктури;

9) здійснює спеціальну перевірку осіб для допуску у захищені зони об’єктів критичної інфраструктури;

10) подає органам державної влади, органам місцевого самоврядування, підприємствам, установам, організаціям усіх форм власності обов’язкові для розгляду пропозиції з питань захисту критичної інфраструктури та обов’язкові до виконання запити про діяльність об’єктів критичної інфраструктури, вимоги щодо дотримання законодавства;

11) бере участь у перевірці та оцінці захищеності об’єктів критичної інфраструктури, погодженні паспортів безпеки на кожний об'єкт;

12) бере участь у встановленому законодавством порядку у реагуванні на кризові ситуації, пов’язані з безпекою, захистом, стійкістю і цілісністю критичної інфраструктури;

13) використовує для своєї діяльності інформацію щодо критичної інфраструктури, отриману від Уповноваженого органу у сфері захисту критичної інфраструктури й інших суб’єктів державної системи захисту критичної інфраструктури;

14) відряджає співробітників Служби безпеки України до Уповноваженого органу у сфері захисту критичної інфраструктури та об’єктів критичної інфраструктури незалежно від форм власності;

15) ініціює застосування та притягнення до відповідальності посадових і службових осіб, операторів об’єктів критичної інфраструктури за невжиття заходів із безпечного функціонування об’єктів критичної інфраструктури та діяння, що не забезпечують вимоги їх режимно-охоронного захисту, стійкість, цілісність та відновлення у випадку відмов, атак та настання інших кризових ситуацій;

16) створює бази даних щодо загроз і уразливості об’єктів критичної інфраструктури;

17) здійснює міжнародне співробітництво і взаємодіє з органами та установами іноземних держав, міжнародними організаціями у рамках надання міжнародно-правової допомоги у сфері захисту критичної інфраструктури та вживає заходів для забезпечення виконання міжнародних зобов’язань України у рамках захисту критичної інфраструктури;

18) здійснює аналітичну обробку інформації, проводить контррозвідувальні, оперативно-розшукові, пошукові та адміністративно-правові заходи, спрямовані на боротьбу з кібертероризмом і кібершпигунством стосовно об’єктів критичної інформаційної інфраструктури;

19) бере участь у розслідуванні кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури, забезпечує реагування на кіберінциденти у сфері державної безпеки;

20) здійснює іншу діяльність для захисту критичної інфраструктури в межах повноважень, визначених законами, що регулюють діяльність суб'єктів захисту критичної інфраструктури.

Стаття 19. Міністерство внутрішніх справ України

1. Міністерство внутрішніх справ України у сфері захисту критичної інфраструктури:

1) бере участь у формуванні та реалізації державної політики у сфері захисту критичної інфраструктури;

2) здійснює взаємодію з іншими суб'єктами державної системи захисту критичної інфраструктури;

3) бере участь у заходах із забезпечення стійкості об'єктів критичної інфраструктури, посилення їх захисту від злочинних дій, терористичних актів та кібератак, розвитку державно-приватної взаємодії стосовно загроз критичній інфраструктурі та створення ефективної системи управління її безпекою.

Стаття 20. Центральний орган виконавчої влади, який реалізує державну політику у сфері цивільного захисту

1. Центральний орган виконавчої влади, який реалізує державну політику у сфері цивільного захисту, у сфері захисту критичної інфраструктури:

1) бере участь в реалізації державної політики у сфері захисту критичної інфраструктури шляхом захисту населення і територій від надзвичайних ситуацій, запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, гасіння пожеж, здійснення державного нагляду (контролю) за додержанням і виконанням вимог законодавства у сфері цивільного захисту, пожежної та техногенної безпеки;

2) реалізує заходи державної політики у сфері захисту критичної інфраструктури щодо впровадження інженерно-технічних заходів цивільного захисту на об'єктах критичної інфраструктури;

3) бере участь у межах компетенції в оцінці захищеності об'єктів критичної інфраструктури;

4) здійснює заходи щодо постійного та обов'язкового на договірній основі аварійно-рятувального обслуговування суб'єктів господарювання та окремих територій, на яких існує небезпека виникнення надзвичайних ситуацій та віднесених до об'єктів критичної інфраструктури аварійно-рятувальними службами, що пройшли атестацію в установленому порядку;

5) у взаємодії з Міністерством внутрішніх справ України, Службою безпеки України забезпечує організацію захисту від терористичних посягань об’єктів аварійно-рятувальних служб, які залучаються і виконують свої функції на об’єктах критичної інфраструктури у разі виникнення надзвичайних ситуацій.

Стаття 21. Національна гвардія України

1. Національна гвардія України у сфері захисту критичної інфраструктури забезпечує:

1) охорону об’єктів критичної інфраструктури, переліки яких визначаються Кабінетом Міністрів України;

2) участь у ліквідації наслідків кризових ситуацій на об’єктах критичної інфраструктури.

Стаття 22. Національна поліція України

1. Національна поліція України у сфері захисту критичної інфраструктури забезпечує:

1) протидію злочинним посяганням на об’єкти критичної інфраструктури, які загрожують безпеці громадян і порушують функціонування систем життєзабезпечення;

2) здійснення на договірних засадах охорони об’єктів критичної інфраструктури, переліки яких визначаються Кабінетом Міністрів України;

3) захист об’єктів критичної інфраструктури, інтересів суспільства і держави від злочинних посягань у кіберпросторі, здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів проти об’єктів критичної інфраструктури;

4) проведення спільно зі Службою безпеки України перевірки та оцінки захищеності об’єктів критичної інфраструктури, охорону яких покладено на Національну поліцію України.

Стаття 23. Збройні Сили України

1. Збройні Сили України у сфері захисту критичної інфраструктури забезпечують:

1) організацію захисту військових об’єктів Збройних Сил України від терористичних загроз, підготовку до застосування військ (сил) Збройних Сил України, у разі вчинення терористичного акту в повітряному просторі або територіальному морі України;

2) проведення заходів з підвищення рівня живучості та вибухопожежобезпеки арсеналів, баз та складів Збройних Сил України;

3) виконання завдань з протиповітряного прикриття об’єктів критичної інфраструктури.

Стаття 24. Державна спеціальна служба транспорту

1. Державна спеціальна служба транспорту у сфері захисту критичної інфраструктури забезпечує:

1) організацію, планування і проведення робіт з технічного прикриття та відбудови об’єктів критичної інфраструктури національної транспортної системи України;

2) охорону державних об’єктів критичної інфраструктури національної транспортної системи України в умовах надзвичайного стану та в особливий період, перелік яких визначається Кабінетом Міністрів України.

Стаття 25. Державна служба спеціального зв’язку та захисту інформації України

1. Державна служба спеціального зв’язку та захисту інформації України у сфері захисту критичної інфраструктури:

1) бере участь у формуванні та реалізує державну політику щодо захисту критичної технологічної інформації, кіберзахисту об’єктів критичної інформаційної інфраструктури, здійснює державний контроль у цій сфері;

2) забезпечує впровадження аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації);

3) координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на вразливість;

4) забезпечує формування та функціонування державного реєстру об’єктів критичної інформаційної інфраструктури, що функціонують на об’єктах критичної інфраструктури;

5) формує загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, веде перелік об’єктів критичної інформаційної інфраструктури та здійснює заходи щодо його оновлення та актуалізації;

6) координує діяльність суб’єктів забезпечення кібербезпеки щодо кіберзахисту об’єктів критичної інфраструктури;

7) інформує про кіберзагрози та відповідні методи захисту від них;

8) надає операторам об’єктів критичної інфраструктури консультативну та практичну допомогу з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо їх об’єктів;

9) здійснює обмін інформацією між органами державної влади і приватним сектором щодо кіберзагроз об’єктам критичної інфраструктури;

10) здійснює міжнародне співробітництво з питань кібербезпеки об’єктів критичної інфраструктури, забезпечує впровадження міжнародних ініціатив у сфері кібербезпеки об’єктів критичної інфраструктури, що відповідають національним інтересам України.

Стаття 26. Секторальні органи у сфері захисту критичної інфраструктури

1. Державні органи, які визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури у окремому секторі критичної інфраструктури:

1) створюють у своєму складі структурні підрозділи з питань захисту критичної інфраструктури;

2) збирають, узагальнюють та здійснюють попередній аналіз даних щодо критичної інфраструктури та її функціонування;

3) спільно з операторами критичної інфраструктури здійснюють категоризацію об'єктів критичної інфраструктури своїх секторів критичної інфраструктури, формують секторальні переліки об'єктів критичної інфраструктури, подають інформацію до Реєстру об'єктів критичної інфраструктури;

4) розробляють та затверджують:

- вимоги до захисту об'єктів критичної інфраструктури відповідно до їх категорій;

- проектні загрози критичній інфраструктурі секторального рівня;

- плани взаємодії функціональних органів у сфері захисту критичної інфраструктури у відповідних секторах для всіх режимів функціонування критичної інфраструктури;

- плани взаємодії та підтримання життєво-важливих функцій та надання життєво-важливих послуг, на випадок порушення функціонування об'єктів критичної інфраструктури;

5) затверджують:

- Проектні загрози критичній інфраструктурі об'єктового рівня у відповідних секторах;

- Паспорти безпеки об'єктів критичної інфраструктури, наданих операторами у відповідних секторах;

6) беруть участь, у встановленому законодавством порядку, в реагуванні на кризові ситуації, пов'язані з безпекою, захистом та стійкістю об'єктів критичної інфраструктури;

7) здійснюють попередження про загрози операторів критичної інфраструктури та надають інформаційної, консультативної, експертної, технологічної допомоги операторам критичної інфраструктури, користувачам їх послуг (населенню) задля попередження, реагування, мінімізації можливого впливу загроз;

8) розробляють та впроваджують, норми і регламенти захисту критичної інфраструктури у відповідних секторах критичної інфраструктури;

9) здійснюють:

- перевірку та оцінку захищеності об'єктів критичної інфраструктури;

- підготовку пропозицій до Проектної загрози критичній інфраструктурі національного рівня та Оцінку ризиків критичній інфраструктури національного рівня;

- організацію системи підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури.

- підготовку щорічного звіту щодо забезпечення захисту критичної інфраструктури у відповідному секторі;

10) подають операторам об’єктів критичної інфраструктури обов'язкові для розгляду пропозиції з питань захисту критичної інфраструктури та обов’язкові до виконання вимоги щодо усунення причин і умов, які порушують цілісність і стійкість критичної інфраструктури;

11) розробляють та затверджують галузеві програми з протидії загрозам внутрішніх порушників, зокрема завдяки заходам, спрямованим на досягнення високого рівня культури безпеки (фізичної та технічної);

12) здійснюють:

- збір, аналіз та узагальнення даних щодо об’єктів критичної інфраструктури та загроз їх функціонуванню;

- функціонування відповідних систем обміну інформацією, моніторингу рівня безпеки об’єктів критичної інфраструктури;

- організацію функціонування системи обміну інформацією та взаємодії у відповідних секторах критичної інфраструктури, між суб’єктами державної системи захисту критичної інфраструктури.

Стаття 27. Місцеві (військові, у разі утворення) органи виконавчої влади

1. Місцеві органи виконавчої влади у сфері захисту критичної інфраструктури забезпечують:

1) розробку місцевих програм забезпечення захисту та стійкості критичної інфраструктури, програм підвищення стійкості громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг або для здійснення життєво важливих функцій;

2) розробку та погодження із заінтересованими органами місцевих планів взаємодії залучених суб’єктів у кризовій ситуації з метою підтримання життєво-важливих функцій та надання життєво-важливих, планів відновлення функціонування критичної інфраструктури.

Стаття 28. Оператори критичної інфраструктури

1. Основними завданнями операторів критичної інфраструктури є:

1) забезпечення захисту об’єктів критичної інфраструктури, зокрема створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки;

2) розробка та оновлення об’єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, а також заходів кіберзахисту;

3) проведення оцінки ризиків на об’єктах критичної інфраструктури та обмін інформацією про ризики та загрози з іншими суб’єктам державної системи захисту критичної інфраструктури;

4) створення окремого структурного підрозділу або визначення відповідальної особи за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб’єктами державної системи захисту критичної інфраструктури;

5) оперативне припинення протиправних дій, фізичних атак, спрямованих на відключення або пошкодження роботи операційних систем або систем забезпечення фізичної безпеки об’єкта критичної інфраструктури;

6) організація заходів з реагування на інциденти, кризові ситуації, а також ліквідації їх наслідків на об’єктах критичної інфраструктури у взаємодії з іншими суб’єктами державної системи захисту критичної інфраструктури;

7) забезпечення відновлення функціонування об’єктів критичної інфраструктури в разі виникнення аварій та інших небезпечних подій, вчинення протиправних дій;

8) участь у заходах з захисту повітряного простору над визначеними об’єктами критичної інфраструктури;

9) негайне інформування органів Національної поліції України, Служби безпеки України, підрозділів Національної гвардії України, інших державних органів про інциденти, пов’язані з порушеннями систем фізичної безпеки та кібербезпеки;

10) забезпечення постійного зв’язку з відповідальними за реагування та з іншими компетентними організаціями та установами;

11) забезпечення постійної взаємодії з підприємствами, які забезпечують централізоване водопостачання, централізоване водовідведення, постачання теплової енергії, енергопостачання, телекомунікаційні мережі, транспорт, медичну допомогу, безпеку та численні інші послуги, від яких залежить процес реагування на кризові ситуації та відновлення функціонування об’єктів критичної інфраструктури;

12) створення необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків;

13) проведення навчань та тренінгів, підготовку та перевірку персоналу, який відповідає за охорону, безпеку та захист об’єктів критичної інфраструктури;

14) захист інформації про системи управління, зв’язку, фізичну та кібернетичну безпеку, забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про об’єкти критичної інфраструктури;

15) забезпечення захисту персоналу об’єктів критичної інфраструктури у разі виникнення надзвичайних ситуацій.

2. Оператори критичної інфраструктури забезпечують розробку та затвердження, у встановленому законодавством порядку:

1) корпоративних вимог щодо організації захисту об’єктів критичної інфраструктури;

2) посадових інструкцій осіб, відповідальних за організацію та забезпечення захисту об’єктів критичної інфраструктури;

3) проведення навчань та тренінгів, підготовку та перевірку персоналу, який відповідає за охорону, безпеку та захист об’єктів критичної інфраструктури;

4) Паспортів безпеки об’єктів критичної інфраструктури.

3. Оператори критичної інфраструктури мають право:

1) отримувати в установленому порядку від уповноважених органів державної влади інформацію, що стосується забезпечення безпеки об’єктів критичної інфраструктури, що належать їм на праві власності або іншій законній підставі;

2) самостійно розробляти заходи щодо забезпечення безпеки об'єктів критичної інфраструктури, що не суперечать вимогам цього Закону та прийнятих відповідно до нього нормативно-правових актів.

4.Оператори критичної інфраструктури зобов’язані:

1) забезпечити захист об’єктів критичної інфраструктури, що належать їм на праві власності або на іншій законній підставі;

2) виконувати у встановлені терміни запити (вимоги) щодо надання інформації про об’єкти критичної інфраструктури;

3) невідкладно інформувати відповідальних суб’єктів державної системи захисту критичної інфраструктури (секторальні та функціональні органи, урядовий центр безпеки і стійкості) про інциденти, що сталися на об'єктах критичної інфраструктури, які належать їм на праві власності або іншій законній підставі;

4) невідкладно інформувати Уповноважений орган у сфері захисту критичної інфраструктури про наміри змінити цільове призначення, режим функціонування чи намір передати право власності на об’єкт критичної інфраструктури та виконувати надані йому висновки та рекомендації;

5) виконувати вимоги цього Закону та інших нормативно-правових актів, які регулюють діяльність об'єктів критичної інфраструктури.

Розділ V
ОРГАНІЗАЦІЙНІ ЗАСАДИ ДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 29. Планування заходів щодо забезпечення стійкості та захисту об’єктів критичної інфраструктури

1. Для організації функціонування державної системи захисту критичної інфраструктури Кабінетом Міністрів України, центральними органами виконавчої влади, місцевими органами виконавчої влади (військовими у разі утворення) адміністраціями, органами місцевого самоврядування, об'єднаними територіальними громадами розробляються та затверджуються відповідні плани та програми реагування на кризові ситуації.

2. На державному рівні розробляється Національний план захисту та забезпечення стійкості критичної інфраструктури, який затверджується Кабінетом Міністрів України.

3. На галузевому та регіональному рівнях органи державної влади розробляють і затверджують галузеві плани та програми з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань та тренувань.

4. Національна поліція України, Національна гвардія України, Служба безпеки України, Збройні Сили України та інші складові сектору безпеки і оборони у межах компетенції здійснюють планування відповідних заходів із захисту критичної інфраструктури.

5. На місцевому рівні:

Органи місцевого самоврядування, об'єднані територіальні громади забезпечують розробку, затвердження і виконання місцевих програм підвищення стійкості громад до кризових ситуацій, викликаних припиненням надання чи погіршенням якості важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій. Ці програми включають заходи з забезпечення захисту та стійкості критичної інфраструктури, взаємодії суб'єктів державної системи захисту критичної інфраструктури, а також відновлення функціонування об'єктів критичної інфраструктури.

6. На об'єктовому рівні:

оператори критичної інфраструктури на кожному об'єкті критичної інфраструктури розробляють та забезпечують виконання об'єктового плану заходів щодо захисту і забезпечення стійкості критичної інфраструктури, який включає заходи з фізичного захисту, протидії загрозам, забезпечення інформаційної безпеки та кібербезпеки на об'єктах критичної інфраструктури.

Стаття 30. Здійснення моніторингу рівня безпеки об'єктів критичної інфраструктури

1. Моніторинг рівня безпеки об'єктів критичної інфраструктури здійснюється шляхом оцінки захищеності об'єктів критичної інфраструктури. Оцінка захищеності об'єктів критичної інфраструктури проводиться секторальними та функціональними органами у сфері захисту критичної інфраструктури, відповідно до їх повноважень визначених законом.

2. Метою здійснення моніторингу є встановлення відповідності стану захищеності об’єкта критичної інфраструктури вимогам законодавства, достовірності наданої інформації визначеним суб’єктам державної системи захисту критичної інфраструктури, надання методичної допомоги операторам об’єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури.

3. За результатами проведення моніторингу секторальними та функціональними органами у сфері захисту критичної інфраструктури готуються пропозиції щодо удосконалення системи захисту критичної інфраструктури.

4. Порядок здійснення моніторингу рівня безпеки об’єктів критичної інфраструктури затверджується Кабінетом Міністрів України.

Стаття 31. Взаємодія державної системи захисту критичної інфраструктури з іншими системами захисту у сфері національної безпеки

1. Для забезпечення стійкості критичної інфраструктури до загроз усіх видів, реалізації національних інтересів, функціонування суспільства та забезпечення соціально-економічного розвитку державна система захисту критичної інфраструктури взаємодіє з іншими системами захисту у сфері національної безпеки:

1) з єдиною державною системою запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків, з територіальною та функціональною підсистемами, структурними підрозділами суб’єктів боротьби з тероризмом та Міжвідомчою координаційною комісією Антитерористичного центру при Службі безпеки України з питань боротьби з тероризмом та реагування на загрозу вчинення або вчинення терористичних актів;

2) з національною системою кібербезпеки, Ситуаційним центром забезпечення кібербезпеки Служби безпеки України з питань кібератак та кіберінцидентів, що загрожують сталому функціонуванню об’єктів критичної інформаційної інфраструктури;

3) з правоохоронними органами у сфері протидії злочинності;

4) з об’єднаною цивільно-військовою системою організації повітряного руху України, Українським центром планування використання повітряного простору та регулювання повітряного руху, Командуванням Повітряних Сил, Збройних Сил України з питань:

захисту повітряного простору, протиповітряної оборони важливих державних об’єктів та визначених об’єктів критичної інфраструктури;

взаємодії з припинення протиправних дій повітряних суден, які можуть використовуватися для вчинення терористичних актів у повітряному просторі України проти об’єктів критичної інфраструктури та важливих державних об’єктів;

5) з єдиною державною системою цивільного захисту, з постійно діючими функціональними і територіальними підсистемами та їх ланками, з Державною комісією з питань техногенно-екологічної безпеки та надзвичайних ситуацій та комісіями з питань техногенно-екологічної безпеки та надзвичайних ситуацій

Автономної Республіки Крим, областей, м. Києва та Севастополя, з питань попередження, реагування та ліквідації на кризові ситуації на об’єктах критичної інфраструктури;

6) з державною системою фізичного захисту з питань захищеності та охорони ядерних установок, ядерних матеріалів, запобігання диверсіям, крадіжкам або будь-якому іншому неправомірному вилученню радіоактивних матеріалів.

2. Взаємодія між державними системами захисту здійснюється у разі загрози виникнення або виникнення:

1) протиправних дій, захоплення об’єктів критичної інфраструктури або важливих державних об’єктів, які загрожують безпеці громадян і порушують функціонування систем життєзабезпечення;

2) диверсій, терористичних актів, викрадення, навмисного знищення, пошкодження майна та інших дій на об’єктах критичної інфраструктури та важливих державних об’єктах, внаслідок яких загинули люди або заподіяно значну матеріальну шкоду;

3) масштабних кібератак, актів кібертероризму проти систем управління, операційних та інших систем об’єктів критичної інфраструктури;

4) надзвичайних ситуацій або інших небезпечних подій на об’єктах критичної інфраструктури та важливих державних об’єктах;

5) аварій та технічних збоїв, кризових ситуацій на об’єктах критичної інфраструктури, що створюють загрозу життю та здоров’ю персоналу цих об’єктів та місцевого населення;

6) інших загроз національній безпеці, стійкості та безпеці критичної інфраструктури.

3. Організація взаємодії між суб’єктами державної системи захисту критичної інфраструктури здійснюється шляхом:

1) оперативного обміну інформацією щодо виконання завдань з захисту критичної інфраструктури;

2) проведення спільних оперативних нарад керівного складу центральних та територіальних органів Національної поліції України, Служби безпеки України, Національної гвардії України, Збройних сил України, та інших заінтересованих державних органів;

3) здійснення спільних заходів з захисту критичної інфраструктури за планами, що розробляються на загальнодержавному, галузевому, регіональному місцевому та об’єктовому рівнях;

4) проведення спільних командно-штабних, тактико-спеціальних навчань, спільних тренувань та занять з захисту, охорони, оборони, припинення злочинних дій та кібератак проти систем та об’єктів критичної інфраструктури;

5) регулярного уточнення розрахунків сил та засобів, що залучаються до спільного виконання завдань з захисту об’єктів критичної інфраструктури та важливих державних об’єктів;

6) спільних заходів з припинення протиправних дій проти об’єктів критичної інфраструктури або важливих державних об’єктів, що загрожує безпеці громадян і порушує їх функціонування;

7) участі у реагуванні та ліквідації наслідків інцидентів, кризових ситуацій на об’єктах критичної інфраструктури;

8) координації дій з підтримання або відновлення правопорядку в місцях розташування об’єктів критичної інфраструктури у разі виникнення кризових ситуацій;

9) здійснення інших заходів, передбачених законодавством.

Стаття 32. Державно-приватна взаємодія у сфері захисту критичної інфраструктури

1. Державно-приватна взаємодія у сфері захисту критичної інфраструктури здійснюється шляхом:

1) обміну інформацією між державними органами, органами місцевого самоврядування, операторами критичної інфраструктури, громадськими організаціями, об’єднаннями, організаціями роботодавців, а також громадянами щодо загроз критичній інфраструктурі та реагування на кризові ситуації;

2) визначення повноважень та відповідальності державних органів й операторів критичної інфраструктури у сфері забезпечення безпеки та стійкості критичної інфраструктури;

3) визначення порядку взаємодії між державними органами та операторами критичної інфраструктури у різних режимах функціонування об’єктів критичної інфраструктури;

4) створення системи підготовки кадрів у сфері захисту критичної інфраструктури;

5) підвищення комплексних знань, навичок і умінь персоналу та керівного складу операторів критичної інфраструктури, персоналу суб’єктів господарювання, які провадять діяльність, пов’язану із забезпеченням безпеки об’єктів критичної інфраструктури, з питань реагування на кризові ситуації на таких об’єктах;

6) залучення експертного потенціалу, наукових установ, професійних об’єднань та громадських організацій до підготовки галузевих проектів та нормативно-правових актів у сфері захисту критичної інфраструктури;

7) залучення до виконання завдань по забезпеченню сталого функціонування об’єктів критичної інфраструктури суб’єктів господарювання, які провадять діяльність, пов’язану із забезпеченням безпеки об’єктів критичної інфраструктури, громадських об’єднань та професійних організацій;

8) надання державними органами консультативної та практичної допомоги операторам критичної інфраструктури з питань реагування на кризові ситуації на об’єктах критичної інфраструктури;

9) організації забезпечення захисту персоналу об’єктів критичної інфраструктури від можливих загроз;

10) забезпечення резервування основних ресурсів для функціонування критичної інфраструктури у різних режимах;

11) організації системи оповіщення населення та суб’єктів господарювання про інциденти та кризові ситуації на об’єктах критичної інфраструктури.

2. Державно-приватна взаємодія у сфері захисту критичної інфраструктури здійснюється з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об’єктів критичної інфраструктури та окремих видів діяльності.

Стаття 33. Відповідальність за порушення законодавства у сфері захисту критичної інфраструктури

1. Органи державної влади, органи місцевого самоврядування, їхні посадові і службові особи, оператори об’єктів критичної інфраструктури, винні у порушенні законодавства у сфері захисту критичної інфраструктури, несуть відповідальність згідно із законом.

Стаття 34. Фінансування заходів у сфері захисту критичної інфраструктури

1. Джерелами фінансування робіт і заходів із забезпечення захисту критичної інфраструктури є кошти державного і місцевих бюджетів, власні кошти суб’єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Стаття 35. Міжнародне співробітництво у сфері захисту критичної інфраструктури

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері захисту критичної інфраструктури з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною злочинністю та тероризмом.

2. Україна відповідно до міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення захисту критичної інфраструктури, зокрема у проведенні спільних навчань суб’єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України “Про порядок направлення підрозділів Збройних Сил України до інших держав” та “Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України”.

3. Відповідно до законодавства України у сфері зовнішніх зносин суб’єкти державної системи захисту критичної інфраструктури у межах своїх повноважень можуть здійснювати міжнародну співпрацю безпосередньо на двосторонній або багатосторонній основі.

Розділ VI
ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності через шість місяців з дня його опублікування.

2. Внести до законів України такі зміни:

1) абзац четвертий частини першої статті 5 Закону України “Про оперативно-розшукову діяльність” (Відомості Верховної Ради України, 1992 р., № 22, ст. 303; 2006 р., № 14, ст. 116) після слів “захисту національної державності” доповнити словами “, контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, контррозвідувального захисту критичної інфраструктури”;

2) пункт 2 частини першої статті 6 Закону України “Про контррозвідувальну діяльність” (Відомості Верховної Ради України, 2003 р., № 12, ст. 89) після абзацу третього доповнити новим абзацом четвертим такого змісту:

“контррозвідувального захисту критичної інфраструктури;”.

У зв’язку з цим абзаци четвертий — сьомий вважати відповідно абзацами п’ятим — восьмим;

3) у Законі України “Про інформацію” (Відомості Верховної Ради України, 2011 р., № 32, ст. 313; 2015 р., № 26, ст. 29; 2016 р., № 28, ст. 533; 2017 р., № 2, ст. 25; 2019 р., № 21, ст. 81; 2020 р., № 11, ст. 63):

статтю 10 після абзацу десятого доповнити новим абзацом одинадцятим такого змісту:

“критична технологічна інформація;”.

У зв’язку з цим абзац одинадцятий вважати абзацом дванадцятим;

доповнити Закон статтею 19^1 такого змісту:

“Стаття 19^1. Критична технологічна інформація

1. Критична технологічна інформація — дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об’єктів критичної інфраструктури.

2. Правовий режим критичної технологічної інформації визначається законами та міжнародними договорами України, згода на обов’язковість яких надана Верховною Радою України.

3. Критична технологічна інформація за режимом доступу належить до інформації з обмеженим доступом та підлягає захисту згідно із законом.”;

4) пункт 5 частини першої статті 20 Закону України “Про Кабінет Міністрів України” (Відомості Верховної Ради України, 2014 р., № 13, ст. 222) після абзацу сьомого доповнити новим абзацом такого змісту:

“забезпечує проведення державної політики у сфері захисту критичної інфраструктури України;”.

У зв’язку з цим абзаци восьмий і дев’ятий вважати відповідно абзацами дев’ятим і десятим;

5) частину другу статті 6 Закону України “Про охоронну діяльність” (Відомості Верховної Ради України, 2013 р., № 2, ст. 8) викласти в такій редакції:

“Перелік об’єктів критичної інфраструктури, охорона яких здійснюється державними органами, підприємствами та організаціями, затверджується Кабінетом Міністрів України.”;

6) у Законі України “Про правовий режим воєнного стану” (Відомості Верховної Ради України, 2015 р., № 28, ст. 250):

частину першу статті 1 після слів “забезпечення національної безпеки” доповнити словами “, захисту критичної інфраструктури”;

частину першу статті 15 після слів “Про мобілізаційну підготовку та мобілізацію” доповнити словами “Про критичну інфраструктуру та її захист”.

7) статтю 7 Закону України “Про страхування” (Відомості Верховної Ради України, 2002 р., № 7, ст. 50 із наступними змінами) доповнити пунктами 48 та 49 такого змісту:

“48) страхування цивільної відповідальності операторів критичної інфраструктури за шкоду, яку може бути заподіяно припиненням функціонування та/або аваріями на об'єктах критичної інфраструктури, зумовленими невиконанням операторами критичної інфраструктури вимог законодавства у сфері захисту критичної інфраструктури;

49) страхування об'єктів критичної інфраструктури від пошкодження внаслідок впливу стихійних лих або техногенних катастроф та від протиправних дій третіх осіб.“

8) у Законі України “Про основні засади забезпечення кібербезпеки України” (Відомості Верховної Ради України, 2017 р., № 45, ст.403):

у статті 1:

пункт 16 виключити;

абзац двадцять третій доповнити реченням “Термін “об’єкт критичної інфраструктури” вживаються в цьому Законі у значенні, визначеному Законом України “Про критичну інфраструктуру та її захист”.

у статті 6:

пункт 1 виключити;

пункт 2 викласти у такій редакції:

“Порядок віднесення об’єктів до об’єктів критичної інфраструктури та формування Реєстру об’єктів критичної інфраструктури здійснюється відповідно до Закону України “Про критичну інфраструктуру та її захист”.

3. Кабінету Міністрів України у тримісячний строк з дня набрання чинності цим Законом:

1) забезпечити прийняття нормативно-правових актів, необхідних для реалізації цього Закону;

2) привести власні нормативно-правові акти у відповідність із цим Законом;

3) забезпечити приведення міністерствами та іншими центральними і місцевими органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

Голова
Верховної Ради України

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
до проекту Закону України
“Про критичну інфраструктуру та її захист”

І. Визначення проблеми.

Останніми роками у світі відбувається зростання загроз тероризму, екстремізму та сепаратизму, збільшення кількості надзвичайних ситуацій техногенного та природного характеру та кібератак на державні установи, компанії, підприємства. Зазначене відбувається і все це відбувається на тлі процесів подальшого ускладнення і розгалуження взаємозв’язків і взаємовпливів при забезпеченні життєдіяльності сучасної держави, її національної безпеки і оборони. Вплив перерахованих чинників значно підвищує уразливість об’єктів і систем, життєво-важливих для забезпечення повсякденного функціонування кожної сучасної держави.

Серед інструментів адекватного реагування на цей безпековий виклик одним із основних є запровадження та постійне удосконалення державних систем, спеціально призначених для забезпечення захисту (безпеки) та стійкості критичної інфраструктури.

Водночас варто зазначити, що на сьогодні основним критерієм віднесення різних об’єктів, систем і мереж (фізичних та віртуальних) до критичної інфраструктури є надзвичайна важливість об’єкта для безпечного та сталого повсякденного життя країни. Тобто мова йде про об’єкти, знищення або вихід з ладу (повний або частковий) яких може призвести до швидких тяжких наслідків для населення, суспільства і держави в цілому, а тому їх захист має бути забезпечений у першу чергу.

На сьогодні в державі готовність до реагування на комплексні загрози та ризики до цього часу забезпечується за умов наявності цілої низки державних/національних систем захисту, безпеки та кризового реагування, за функціонування яких несуть відповідальність окремі державні органи, що створює умови для домінування відомчих підходів, під впливом яких уповноважені державні органи проявляють схильність опікуватися лише певним спектром загроз та ризиків.

Ще однією характерною ознакою існуючого стану речей у цій сфері є те, що в Україні об’єкти, системи і мережі, які відповідно до світової практики прийнято відносити до критичної інфраструктури, “розпорошені” по більш ніж 10 різноманітних переліках і списках об’єктів, включаючи “особливо важливі”; “важливі”; такі, які підлягають “охороні та обороні” або “обов’язковій охороні”; “об’єкти підвищеної небезпеки”, “радіаційно-небезпечні об’єкти” тощо.

Зазначена ситуація неминуче створює міжвідомчі бар’єри для опрацювання питань, які перебувають поза межами конкретних систем, і це, зокрема, перешкоджає урахуванню загроз та ризиків, реалізація яких може викликати так звані каскадні ефекти, тобто випадки, коли надзвичайні та кризові ситуації, які можуть мати місце в одній галузі (одному секторі критичної інфраструктури) спричиняють швидкий негативний вплив на інші галузі, сектори і сегменти національної економіки, національної безпеки та оборони.

Аналіз існуючої ситуації у сфері захисту об’єктів, що мають бути віднесені до критичної інфраструктури, показує, що відомчі оцінки стосовно достатньої урегульованості процедур і механізмів координації дій, взаємодії та обміну інформацією між системами у діючому правовому полі не зовсім відповідають дійсному стану речей, і це особливо яскраво проявляється у випадках ситуацій,

пов’язаних з проблематикою реагування на реалізацію комплексних загроз. У наступних розділах представлене обґрунтування цього висновку.

Варто зазначити, що у провідних країнах світу ефективна взаємодія систем реагування на загрози, небезпеки і ризики є важливим елементом забезпечення національної безпеки. Наприклад, у США для характеристики здатності систем взаємодіяти широко використовується спеціальний термін “interoperability”, а забезпечення оптимальної здатності систем, персоналу та обладнання отримувати та надавати: функціональну підтримку, дані, інформацію та послуги визначено як найбільш важлива вимога для Міністерства внутрішньої безпеки США при реагуванні на інциденти. Натомість, у законодавстві України щодо національної безпеки такий або аналогічний за змістом терміни відсутні.

На сьогодні в Україні діють відокремлено такі державні системи:

- Єдина державна система цивільного захисту (далі – ЄДСЦЗ);
- Єдина система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (далі – ЄСЗРПТА);
- Державна система фізичного захисту (далі – ДСФЗ).

Параметри функціонування деяких систем безпеки та кризового реагування:

ЄДСЦЗ режими функціонування	ДСФЗ умови функціонування	ЄСЗРПТА рівні терористичних загроз
режим повсякденного функціонування	нормальне функціонування	сірий (можлива загроза) за наявності факторів (умов), що сприяють вчиненню терористичного акту
підвищена готовність	підвищена готовність	синій (потенційна загроза) за наявності інформації, що потребує підтвердження, про підготовку до вчинення терористичного акту
надзвичайна ситуація	функціонування у кризовій ситуації	жовтий (імовірна загроза) за наявності достовірної (підтвердженої) інформації про підготовку до вчинення терористичного акту
надзвичайний стан	відновлення нормального функціонування	червоний (реальна загроза) у разі вчинення терористичного акту

У запропонованій таблиці можна побачити такі аспекти функціонування державної системи захисту критичної інфраструктури:

1. Положення про внесені у таблицю системи використовують різні терміни для опису функціонування у різних умовах, а саме – “режими”, “умови” та “рівні”.

2. Фактично про майже повний збіг можна говорити лише для двох перших режимів/умов для ЄДСЦЗ та ДСФЗ, які, при цьому, можна вважати найпростішими з точки зору планування і організації діяльності та забезпечення готовності до них.

3. Для ЄСЗРПТА, на відміну від двох інших систем, відсутній режим, який можна було б поставити у відповідність режимам “повсякденного” або “нормального” функціонування.

4. З ускладненням режимів невідповідності критеріїв їх запровадження можуть суттєво збільшуватися (це твердження пояснюється нижче на прикладі).

Наведемо приклад того, як у випадку конкретної загрози на сьогодні діють зазначені вище системи.

У разі надходження підтвердженої інформації про загрозу теракту на одній з українських АЕС. У такому випадку настання серйозних наслідків для життя і здоров'я населення, окремих осіб можливе не тільки в результаті застосування терористами стрілецької зброї та вибухівки, але й в результаті пошкодження технологічного обладнання на реакторних та інших небезпечних технологічних установках, тобто з точки зору ядерної, радіаційної, техногенної та екологічної безпеки, впливу на соціально-політичну ситуацію в країні.

При цьому, відповідно до положень про внесені до таблиці системи, при отриманні вказаної інформації вони функціонують таким чином: ДСФЗ – функціонування у кризовій ситуації; ЄДСЦЗ – у режимі повсякденного функціонування; ЄСЗРПТА – у режимі, що відповідає передостанньому "жовтому рівню" шкали терористичної загрози.

Водночас, ЄДСЦЗ не залишається поза процесом реагування на таку комплексну загрозу, але при цьому неузгодженості можуть призвести до зайвих витрат часу, ресурсів, неминучих збоїв та плутанини в діях, у т.ч. щодо розподілу (передачі) відповідальності на різних етапах реагування, що, у свою чергу, в результаті, може стати причиною тяжких наслідків, включаючи втрати людських життів.

Таким чином, національна нормативно-правова база в її теперішньому вигляді не може бути надійною основою для розробки і реалізації планів і процедур координації дій, взаємодії та обміну інформацією між існуючими в Україні системами захисту, безпеки та кризового реагування.

Розробка дієвих планів і процедур координації дій, взаємодії та обміну інформацією потребує, щонайменше, прийняття спільної термінології, визначення співвідношень між режимами, рівнями та умовами функціонування систем, узгодження принципів управління комплексною кризою, яка пов'язана з дією кількох небезпечних факторів (у розглянутому випадку це тероризм і радіація) тощо.

Запровадження єдиних підходів, термінології, процедур і форматів координації дій, взаємодії та обміну інформацією на національному рівні має бути враховане при розробці та коригуванні документів оперативного і тактичного рівнів.

Іншим прикладом недостатнього рівня координації дій, взаємодії та обміну інформацією при реалізації загроз комплексного характеру може слугувати ситуація із хакерською атакою на сайт Міненерговугілля, яка мала місце наприкінці квітня 2018 року. При цьому спікер Національної поліції озвучив у ЗМІ позицію свого відомства щодо цієї кібератаки, заявивши, що воно готове надати допомогу міністерству, але лише у випадку офіційного звернення останнього. Такий підхід свідчить про відсутність на момент атаки процедур ефективної взаємодії.

Таким чином існуючі в Україні державні/національні системи захисту, безпеки і кризового реагування не спроможні забезпечити системний інтегрований підхід до захисту критичної інфраструктури від комбінацій фізичних загроз (природних, техногенних та соціально-політичних) і кіберзагроз, а чинна нормативно-правова база та фактори, що діють у рамках цих систем, не створюють достатніх можливостей для запровадження дієвих процедур і механізмів координації дій, взаємодії та обміну інформацією між системами.

На сучасному етапі реформування сектору безпеки і оборони держави слід вважати доцільним створення єдиної державної системи захисту критичної

інфраструктури на основі існуючих державних/національних систем захисту, безпеки та кризового реагування за умов досягнення якісно нового рівня координації дій та взаємодії між ними, що передбачає, зокрема, узгодження основних параметрів функціонування зазначених систем у т.ч. через запровадження єдиної термінології.

На короткострокову перспективу найважливішим завданням у рамках заходів, спрямованих на створення державної системи захисту критичної інфраструктури, слід вважати розробку і прийняття Закону України "Про критичну інфраструктуру та її захист" у запропонованій Мінекономрозвитку редакції та яка відповідає загальновизнаним в країнах-членах НАТО та ЄС підходам та національним інтересам України.

У проекті Закону України "Про критичну інфраструктуру та її захист" запропоновано вирішення таких проблем:

відсутність єдиної загальнодержавної системи захисту критичної інфраструктури;

недостатність та неузгодженість нормативно-правового регулювання з питань захисту систем і об'єктів критичної інфраструктури, зокрема відсутність спеціального закону про критичну інфраструктуру та її захист;

відсутність державного органу, відповідального за координацію дій у сфері захисту критичної інфраструктури;

відсутність розподілу повноважень, завдань і відповідальності центральних органів виконавчої влади та інших державних органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників (розпорядників) об'єктів критичної інфраструктури;

відсутність єдиних критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації;

відсутність єдиної методології проведення оцінки загроз критичній інфраструктурі, а також відсутність спеціального правоохоронного органу, відповідального за проведення аналізу та оцінки загроз критичній інфраструктурі внаслідок проведення іноземними державами економічної експансії та дискримінаційної політики, недопущення заподіяння шкоди економічному та науково-технічному потенціалу держави, а також організацію та вжиття відповідних заходів протидії.

Крім того, запропоновано єдині критерії віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації.

Метою формування паспортів безпеки об'єктів критичної інфраструктури є визначення загроз та оцінки можливих ризиків негативних наслідків їх прояву для об'єктів критичної інфраструктури, визначення напрямів забезпечення їх безпеки для подальшої розробки на цій основі заходів із запобігання та попередження прояву загроз для об'єктів критичної інфраструктури. Паспорти безпеки мають готуватися операторами об'єктів критичної інфраструктури і надаватися на погодження до відповідальних за сектори суб'єктів захисту критичної інфраструктури та Служби безпеки України.

Законопроект (проект регуляторного акту) розроблено Мінекономрозвитку на виконання доручення Кабінету Міністрів України від 21.02.2017 № 1835/4/1-17 до Указу Президента України від 16 січня 2017 року № 8/2017 "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури".

Основні групи (підгрупи), на які проблема має вплив:

Групи (підгрупи)	Так	Ні
Громадяни	Так	–
Держава	Так	–
Суб'єкти господарювання,	Так	–
у т.ч. суб'єкти малого підприємництва	–	Ні

Врегулювання зазначених проблемних питань не може бути здійснено за допомогою:

ринкових механізмів, оскільки такі питання регулюються виключно законодавчими актами;

діючих регуляторних актів, оскільки чинним законодавством порушені питання не врегульовані, а внесення відповідних змін до законодавства можливе лише шляхом прийняття цього регуляторного акта.

II. Цілі державного регулювання.

Метою проекту Закону України є врегулювання діяльності із захисту критичної інфраструктури у мирний час та в умовах надзвичайної ситуації. Діяльність із захисту критичної інфраструктури в умовах воєнного стану регулюється іншими законами України.

III. Визначення та оцінка альтернативних способів досягнення цілей.

1. Визначення альтернативних способів:

Вид альтернативи	Опис альтернативи
Альтернатива 1. Спосіб оцінюється як такий, що потребує вдосконалення	Відсутність регулювання або збереження status quo Залишити нормативне регулювання на рівні, що існує, та сподіватися на еволюційний розвиток відносин, які виникають між різними суб'єктами, які залучаються до захисту критичної інфраструктури.
Альтернатива 2. Спосіб оцінюється як такий, що потребує вдосконалення	Інший, відмінний від запропонованого способу (внесення змін до чинних законодавчих актів) Цей альтернативний спосіб не забезпечить врегулювання питання. Зокрема, в рамках існуючих державних систем захисту та реагування (єдиної державної системи цивільного захисту, єдиної державної системи запобігання, реагування і припинення терористичних актів і мінімізації їх наслідків, державної системи фізичного захисту, національної системи кібербезпеки) та відповідних законодавчих актів *неможливо*: – визначити єдиний державний орган, відповідальний за координацію дій у сфері захисту критичної інфраструктури від загроз будь-якого походження та спрямованості; – визначити повноваження, завдання і відповідальність центральних органів виконавчої влади та інших державних органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників (розпорядників) об'єктів критичної інфраструктури;

	– забезпечити ефективну координацію між суб'єктами державної системи захисту критичної інфраструктури; – забезпечити єдність методологічних засад у сфері оцінки загроз та ризиків критичній інфраструктурі, єдність критеріїв та методології віднесення об'єктів інфраструктури до критичної; – забезпечити розвиток державно-приватного партнерства у сфері захисту критичної інфраструктури та забезпечити заходи із захисту критичної інфраструктури джерелами фінансування.
Альтернатива 3. Обраний спосіб забезпечує досягнення цілей державного регулювання.	Обраний спосіб (прийняття законопроекту) Зазначений альтернативний спосіб досягнення цілей є найбільш прийнятним і ефективним, оскільки він відповідає потребам у розв'язанні визначених проблем та принципам державної регуляторної політики. Прийняття законопроекту дозволить: – визначити законодавчі вимоги до захисту критичної інфраструктури; – створити умови, спрямовані на мінімізацію можливості реалізації загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз критичній інфраструктурі усіх видів; – створити умови для швидкого відновлення функціонування критичної інфраструктури (у випадку реалізованих загроз, надзвичайних/кризових ситуацій); – визначити повноваження, завдання і відповідальність центральних органів виконавчої влади та інших державних органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників (розпорядників) об'єктів критичної інфраструктури; – забезпечити ефективну координацію між суб'єктами державної системи захисту критичної інфраструктури; – сприяти розвитку державно-приватного партнерства у сфері захисту критичної інфраструктури; – забезпечити розвиток міжнародного співробітництва у сфері захисту критичної інфраструктури.

2. Оцінка вибраних альтернативних способів досягнення цілей:
Оцінка впливу на сферу інтересів держави:

Вид альтернативи	Вигоди	Витрати
Альтернатива 1. *(Відсутність регулювання або збереження status*	Вигоди відсутні. Ситуація залишиться на рівні, що існує. Відсутність законодавчого врегулювання відносин у сфері захисту	Можливо зменшення надходження коштів до державного бюджету у випадку реалізації загроз

quo)	критичної інфраструктури "консервує" ті проблемні питання, які є на сьогодні у цій сфері та залишаються невирішеними, що може створити загрози національній безпеці України.	об'єктам критичної інфраструктури, пошкодженні майна, а також збільшення видатків з держбюджету на необхідні заходи щодо відновлення порушених об'єктів критичної інфраструктури.
Альтернатива 2. *(Інший, відмінний від запропонованого способу (внесення змін до чинних законодавчих актів)*	Вигоди відсутні. Цей альтернативний спосіб не забезпечить врегулювання питання, оскільки не буде комплексно унормовано питання захисту об'єктів критичної інфраструктури та не буде створено ефективну систему захисту критичної інфраструктури.	Можливо зменшення надходження коштів до державного бюджету у випадку реалізації загроз об'єктам критичної інфраструктури, пошкодженні майна, а також збільшення видатків з держбюджету на необхідні заходи щодо відновлення порушених об'єктів критичної інфраструктури.
Альтернатива 3. *(Обраний спосіб забезпечує досягнення цілей державного регулювання)*	Вигоди значні. Прийняття регуляторного акта дозволить: – захистити інтереси держави та забезпечити державну безпеку шляхом підвищення безпеки та стійкості критичної інфраструктури до загроз будь-якого походження (природного та техногенного характеру, протиправних дій), що, у свою чергу, забезпечить національну безпеку; – розмежувати повноваження, завдання і відповідальність центральних органів виконавчої влади та інших державних органів у сфері захисту критичної інфраструктури; – визначити права, обов'язки та відповідальність власників (розпорядників) об'єктів критичної інфраструктури; – забезпечити ефективну координацію між суб'єктами державної системи захисту критичної інфраструктури; – сприяти розвитку державно-приватного партнерства у сфері захисту критичної інфраструктури та забезпечити заходи із захисту критичної інфраструктури джерелами фінансування;	Джерелами фінансування робіт і заходів із забезпечення захисту критичної інфраструктури є кошти державного і місцевих бюджетів. Водночас, організація належного захисту об'єктів критичної інфраструктури сприятиме зменшенню додаткового навантаження на державний бюджет щодо усунення наслідків порушення у роботі об'єктів критичної інфраструктури та відновлення їх функціонування. Функціонування структурних підрозділів з питань захисту критичної інфраструктури, з прийняттям Закону, буде здійснюватись шляхом перерозподілу коштів в межах видатків, передбачених на кожен відповідний орган влади. Термін інтеграції та

	– забезпечити єдність методологічних засад у сфері оцінки загроз та ризиків об'єктам критичної інфраструктурі різної форми власності, єдність критеріїв та методології віднесення об'єктів інфраструктури до критичної.	адаптації суб'єктів господарювання у державній системі захисту критичної інфраструктури пропонується встановити два роки.

У разі прийняття Закону, прогнозується підвищення захищеності об'єктів критичної інфраструктури в наслідок організації належного їх захисту, сприятиме зменшенню додаткового навантаження на державний бюджет щодо усунення наслідків порушення у роботі об'єктів критичної інфраструктури та відновлення їх функціонування.

Функціонування структурних підрозділів з питань захисту критичної інфраструктури, з прийняттям Закону, буде здійснюватись шляхом перерозподілу коштів в межах видатків передбачених на кожен відповідний орган влади.

Оцінка впливу на сферу інтересів громадян:

Вид альтернативи	Вигоди	Витрати
Альтернатива 1. *(Відсутність регулювання або збереження status quo)*	Вигоди відсутні. Ситуація залишиться на рівні, що існує. Ймовірне виникнення загроз безпеці життєдіяльності громадян, можливості втрати ними життєво-важливих послуг та функцій, які виконують об'єкти критичної інфраструктури.	Не передбачаються
Альтернатива 2. *(Інший, відмінний від запропонованого способу (внесення змін до чинних законодавчих актів)*	Вигоди відсутні. Ситуація залишиться на рівні, що існує. Ймовірне виникнення загроз безпеці життєдіяльності громадян, можливості втрати ними життєво-важливих послуг та функцій, які виконують об'єкти критичної інфраструктури.	Не передбачаються
Альтернатива 3. *(Обраний спосіб забезпечує досягнення цілей державного регулювання)*	Вигоди значні. Прийняття регуляторного акта дозволить підвищити безпеку та стійкість критичної інфраструктури до загроз будь-якого походження (природного та техногенного характеру, протиправних дій), що, у свою чергу сприятиме захисту життєдіяльності громадян, забезпечить безперервність надання життєво-важливих послуг та функцій для суспільства та населення.	Реалізація не потребує додаткових матеріальних та інших витрат з боку громадян.

Оцінка впливу на сферу інтересів суб'єктів господарювання:

Показник	Великі	Середні	Малі, мікро
Кількість суб'єктів господарювання, що підпадають під дію регулювання, одиниць (питома вага %)	245 суб'єктів господарювання, які можуть бути віднесені до об'єктів критичної інфраструктури та можуть підпадати під дію регулювання (18%)	1100 суб'єктів господарювання, які можуть бути віднесені до об'єктів критичної інфраструктури та можуть підпадати під дію регулювання (82%)	Відносяться до IV групи критичності, які не відносяться до критичної інфраструктури

Витрати
на одного суб'єкта господарювання великого і середнього підприємництва, які виникають внаслідок дії регуляторного акта

Порядковий номер	Витрати	За перший рік	За п'ять років
1	Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання/підвищення кваліфікації персоналу тощо, гривень	–	–
2	Податки та збори (зміна розміру податків/зборів, виникнення необхідності у сплаті податків/зборів), гривень	–	–
3	Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам, гривень	1071	5355
3.1.	*Витрати пов'язані із розробкою плану заходів із захисту критичної інфраструктури*	*504*	*2520*
3.2.	*Витрати пов'язані із веденням паспорту об'єкту критичної інфраструктури*	*567*	*2835*
4	Витрати, пов'язані з адмініструванням заходів державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/ приписів тощо), гривень	–	–
5	Витрати на отримання адміністративних послуг (дозволів, ліцензій, сертифікатів, атестатів, погоджень, висновків, проведення незалежних/обов'язкових експертиз, сертифікації, атестації тощо) та інших послуг (проведення наукових, інших експертиз, страхування тощо), гривень	–	–
6	Витрати на оборотні активи (матеріали, канцелярські товари тощо), гривень	100	500
7	Витрати, пов'язані із наймом додаткового персоналу, гривень	–	–
8	Інше (уточнити), гривень	–	–
9	РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8), гривень	1171	5855
10	Кількість суб'єктів господарювання великого та середнього підприємництва, на яких буде поширено регулювання, одиниць	1345	1345
11	Сумарні витрати суб'єктів господарювання великого та	1574995	7874975

	середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 9 х рядок 10), гривень		

Вид альтернативи	Вигоди	Витрати
Альтернатива 1. *(Відсутність регулювання або збереження status quo)*	Вигоди відсутні. Ситуація залишиться на рівні, що існує. Ризики для суб'єктів господарювання щодо можливості втрати бізнесу, не зменшаться.	Витрати відсутні.
Альтернатива 2. *(Інший, відмінний від запропонованого способу (внесення змін до чинних законодавчих актів)*	Вигоди відсутні. Ситуація залишиться на рівні, що існує. Ризики для суб'єктів господарювання щодо можливості втрати бізнесу, не зменшаться.	Зміни чи вдосконалення охоронно-режимних заходів, оплати праці персоналу, спроможного кваліфіковано, швидко й адекватно протистояти існуючим викликам та загрозам, відновлювати роботу після аварій і технічних збоїв, запобігати зловмисним діям (насамперед фізичним і кібернетичним), організовувати заходи з протистоянням природним лихам та небезпечним явищам.
Альтернатива 3. *(Обраний спосіб забезпечує досягнення цілей державного регулювання)*	Вигоди значні. Прийняття регуляторного акта дозволить підвищити безпеку та стійкість критичної інфраструктури до загроз будь-якого походження (природного та техногенного характеру, протиправних дій), що, у свою чергу, забезпечить безперервність бізнесу. Крім того, належний захист об'єктів критичної інфраструктури убезпечить суб'єктів господарювання від руйнівного впливу іноземних держав.	Витрати суб'єктів господарювання, які увійдуть до державної системи захисту критичної інфраструктури, залежатимуть від виділення (залучення) останніми коштів, що спрямовуватимуться на підтримання в робочому стані їх виробничих спроможностей, модернізацію матеріально-технічної бази, можливе перепрофілювання підприємства, потребою істотної зміни чи вдосконалення охоронно-режимних заходів, оплату праці персоналу, спроможного кваліфіковано, швидко й адекватно протистояти існуючим викликам та загрозам, відновлювати роботу після аварій і технічних збоїв, запобігати зловмисним діям (насамперед фізичним і

		кібернетичним), організовувати заходи з протистоянням природним лихам та небезпечним явищам. Такий підхід щодо розрахунку вигод і витрат з урахуванням вищенаведених критеріїв повинен бути диференційованим для кожного окремо взятого суб'єкта підприємницької діяльності. *Вигоди від безперервності бізнесу компенсують витрати на підвищення безпеки та стійкості.* Термін інтеграції та адаптації суб'єктів господарювання у державній системі захисту критичної інфраструктури пропонується встановити два роки.

Сумарні витрати за альтернативами

Альтернативами	Сума витрат, гривень
Альтернатива 1 (відсутність регулювання або збереження status quo)	**0**
Альтернатива 2 (внесення змін до чинних законодавчих актів)	**1574995**
Альтернатива 3 (прийняття Закону)	**1574995**

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей.

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотири-бальною системою оцінки)	Коментарі щодо присвоєння відповідного балу
Альтернатива 1. *(Відсутність регулювання або збереження status quo)*	1	Збереження чинного регулювання не дає змоги досягнути поставлених цілей державного регулювання, не забезпечується вирішення визначених проблемних питань у сфері захисту критичної інфраструктури, не забезпечується захист безперервності надання життєво важливих послуг та функцій для держави, суспільства та населення.
Альтернатива	1	Така альтернатива не дає змоги

2. *(Інший, відмінний від запропонованого способу (внесення змін до чинних законодавчих актів)*		досягнути поставлених цілей державного регулювання, значно збільшаться часові витрати на створення державної системи захисту критичної інфраструктури не забезпечується вирішення визначених проблемних питань у сфері захисту критичної інфраструктури, не забезпечується захист безперервності надання життєво важливих послуг та функцій для держави, суспільства та населення.	
Альтернатива 3. *(Обраний спосіб забезпечує досягнення цілей державного регулювання)*	4	Забезпечується розв'язання визначених проблем у сфері захисту критичної інфраструктури та повністю досягаються цілі державного регулювання, а саме: – визначаються законодавчі вимоги до захисту критичної інфраструктури; – створюються умови, спрямовані на мінімізацію можливості реалізації загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз критичній інфраструктурі усіх видів; – створюються умови для швидкого відновлення функціонування критичної інфраструктури (у випадку реалізованих загроз, надзвичайних/кризових ситуацій); – визначаються повноваження, завдання і відповідальність центральних органів виконавчої влади та інших державних органів у сфері захисту критичної інфраструктури, а також права, обов'язки та відповідальність власників (розпорядників) об'єктів критичної інфраструктури; – забезпечується ефективна координація між суб'єктами державної системи захисту критичної інфраструктури; – сприяння розвитку державно-приватного партнерства у сфері захисту критичної інфраструктури; – забезпечується розвиток міжнародного співробітництва у сфері захисту критичної інфраструктури.	
Рейтинг результативності	Вигоди (підсумок)	Витрати (Підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива	1. Забезпечить виконання	Прийняття законо-	Ціль прийняття

3.	положень Резолюції Ради безпеки ООН від 13 лютого 2018 р. № 2341 (2017); 2. Підвищить рівень захисту критичної інфраструктури. Шляхом нормативного врегулювання цієї сфери, визначення конкретних завдань і функцій відомств на національному, регіональному, місцевому та об'єктовому рівнях, сприятиме усуненню дублювання зусиль забезпечить оптимізацію бюджет них витрат; 3. Мінімізує виникнення та реалізацію загроз критичній інфраструктурі; шляхом запровадження належної взаємодії всіх суб'єктів захисту критичної інфраструктури, створення спільних підходів до оцінки загроз та ризиків на національному, секторальному та об'єктовому рівні. 4. Забезпечить умови для стійкого функціонування об'єктів критичної інфраструктури. Запровадить чіткі вимоги до заходів з планування, реагування та відновлення функціонування об'єктів критичної інфраструктури у разі кризових та надзвичайних ситуацій, терористичних актів, актів несанкціонованого втручання та кібератак.	проекту не пов'язане з додатковими витратами держави та громадян, а витрати суб'єктів господарювання перекриються вигодами від безперервності бізнесу.	регуляторного акта, визначена розділом 1 цього АРВ, буде досягнута повною мірою, проблема державного регу-лювання, викладена в АРВ, більше існувати не буде.
Альтернатива 2.	Вигоди відсутні	Витрати відсутні	Не дає змоги досягнути поставленої цілі державного регулювання та не сприяє розв'язанню проблеми, яка продовжить існувати.
Альтернатива 1.	Вигоди відсутні	Витрати відсутні	Не дає змоги досягнути поставленої цілі державного

			регулювання та не сприяє розв'язанню проблеми, яка продовжить існувати.

Рейтинг	Аргументи щодо переваги обраної альтернативи / причини відмови від альтернативи	Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта
Альтернатива 3.	Забезпечується підвищення безпеки та стійкості критичної інфраструктури до загроз будь-якого походження (природного та техногенного характеру, протиправних дій) та, у свою чергу, забезпечення безперервності надання життєво-важливих послуг та функцій для держави, суспільства та населення шляхом: – розмежування повноважень, завдань та відповідальності центральних органів виконавчої влади, інших державних органів у сфері захисту критичної інфраструктури; – визначення прав, обов'язків та відповідальності власників (розпорядників) об'єктів критичної інфраструктури; – забезпечення ефективної координації між суб'єктами державної системи захисту критичної інфраструктури; – розвитку державно-приватного партнерства у сфері захисту критичної; – забезпечення єдності методологічних засад у сфері оцінки загроз та ризиків об'єктам критичної інфраструктурі різної форми власності, єдності критеріїв та методології віднесення об'єктів інфраструктури до критичної.	Запропонований регуляторний акт у т.ч. сприятиме зменшенню ризиків, пов'язаних із гібридними загрозами, які збільшилися внаслідок агресії Російської Федерації, а також сприятиме зближенню українського законодавства до законодавства ЄС.
Альтернатива 1 та 2.	Такі альтернативи не дають змоги досягнути поставлених цілей державного регулювання. Відсутність законодавчого врегулювання відносин у сфері захисту критичної інфраструктури "консервує" ті проблемні питання, які є на сьогодні у цій сфері.	Х

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

Для розв'язання визначеної в АРВ проблеми Мінекономрозвитку розроблено

законопроект, прийняття якого дозволить створити умови для формування та ефективної реалізації державної політики у сфері захисту критичної інфраструктури.

У разі прийняття законопроекту будуть визначені:

- основні засади державної політики у сфері захисту критичної інфраструктури;
- засади правових і господарських відносин, що виникають під час такої діяльності;
- повноваження державних органів у сфері захисту критичної інфраструктури.

Розвиток законодавства у сфері забезпечення захисту критичної інфраструктури одночасно вирішить комплекс питань: дозволить визначити єдині критерії та методологію віднесення об'єктів інфраструктури до критичної інфраструктури, порядок їх паспортизації та категоризації; дозволить запровадити системний інтегрований підхід до захисту об'єктів критичної інфраструктури шляхом впровадження дієвих процедур і механізмів координації дій, взаємодії та обміну інформацією між системами, а також визначення єдиної термінології у цій сфері.

Для впровадження цього регуляторного акта Кабінету Міністрів України, державним органам необхідно буде у шестимісячний строк забезпечити приведення власних нормативно-правових актів у відповідність із Законом України "Про критичну інфраструктуру та її захист" та забезпечити прийняття нормативно-правових актів, що випливають з цього Закону.

Так, статтею 4 законопроекту визначено основні засади державної політики у сфері захисту критичної інфраструктури; статтею 7 – рівні управління державної системи захисту критичної інфраструктури; статтею 10 – категоризація об'єктів критичної інфраструктури; статтею 11 – складання та ведення Реєстру об'єктів критичної інфраструктури; статтею 14 – розроблення паспорта безпеки на об'єкт критичної інфраструктури; статтею 16 – визначення функцій Уповноваженого органу у сфері захисту критичної інфраструктури, тощо.

Для реалізації положень проекту Закону буде також запроваджено механізм паспортизації об'єктів критичної інфраструктури. У загальному випадку паспорт безпеки об'єкта критичної інфраструктури має включати інформацію щодо загальних відомостей про об'єкт, зв'язків з іншою інфраструктурою, природно-кліматичних і географічних умов місця розташування об'єкта критичної інфраструктури, відомості про речовини та матеріали, що використовуються на об'єкт критичної інфраструктури, аварійної готовності персоналу до дій в умовах НС, організації охорони та фізичного захисту об'єкта критичної інфраструктури, інженерно-технічних засобів охорони, характеристики основних джерел небезпеки, категорії критичності об'єкта критичної інфраструктури, присвоєна об'єкту.

Далі, з урахуванням актуальних загроз та завдань захисту критичної інфраструктури, паспорт безпеки об'єкта критичної інфраструктури, що може включати такі розділи:

1. Загальні відомості про об'єкт.
2. Основні споруди і технологічне обладнання.
3. Зв'язок з іншою інфраструктурою.
4. Природно-кліматичні умови.
5. Небезпечні технологічні процеси.
6. Характеристика основних загроз безпеці об'єктам критичної інфраструктури.
7. Аварійна готовність.

8. Організація охорони та фізичного захисту об’єктів критичної інфраструктури.

9. Оцінка вразливості об’єктів критичної інфраструктури.

10. Захист інформаційної інфраструктури.

11. Відповідність вимогам захисту об’єктів критичної інфраструктури.

При формуванні паспортів безпеки об’єктів критичної інфраструктури планується враховувати всі типи загроз, включаючи загрози природного та техногенного походження. При цьому серед усіх загроз різного походження для безпеки критичної інфраструктури найбільш актуальними можна виокремити такі:

– природні: повені, екстремальні погодні явища, лісові пожежі, землетруси, епідемії та пандемії, епізоотії;

– техногенні:

а) незловмисні: промислові аварії, ядерні/радіологічні аварії, аварії на транспорті, втрата критично важливої інфраструктури;

б) зловмисні: кібератаки, терористичні атаки.

Особливої уваги потребують взаємозв’язки та взаємозалежності між загрозами природного походження, коли виникнення одних небезпечних явищ призводить до формування нових через механізм каскадних ефектів. Усвідомлення каскадних ефектів сучасних загроз є досить складним через взаємозв’язок об’єктів інфраструктури та оточуючого її середовища.

Паспорт безпеки надасть можливість зробити висновки щодо відповідності об’єкта критичної інфраструктури необхідним вимогам захисту. Зокрема, що об’єкт за галузевою ознакою і видом діяльності відноситься до відповідної категорії з цивільного захисту, хімічної небезпеки або пожежо- та вибухонебезпечності. Крім того, даному об’єкту за сукупністю збитку, що може бути нанесений у результаті кризової ситуації і за ступенем критичності присвоюється відповідна категорія. Також має бути надана оцінка виконання вимог охорони об’єкта і захисту його елементів, інформація щодо наявності критичних елементів об’єкта, їх взаємовпливу і відповідності необхідному рівню захищеності.

Паспорт безпеки дозволить робити висновки щодо достатності сил і засобів для виконання заходів з фізичного захисту та антитерористичної захищеності об’єкта і визначати перелік додаткових заходів з удосконалення та усунення виявлених недоліків із зазначенням термінів їх виконання.

Паспортизація є одним із етапів проведення обліку об’єктів критичної інфраструктури. У свою чергу облік об’єктів критичної інфраструктури включатиме виконання комплексу заходів із забезпечення збору, накопичення та актуалізації необхідної інформації щодо характеристик об’єктів критичної інфраструктури, формування та адміністрування бази даних реєстру об’єктів критичної інфраструктури, інформаційний обмін та надання даних реєстру, розроблення програмного забезпечення для ведення реєстру об’єктів критичної інфраструктури. Враховуючи важливість інформації щодо об’єктів критичної інфраструктури для забезпечення національної безпеки держави, інформація, що використовується для обліку об’єктів критичної інфраструктури, може бути віднесена до інформації з обмеженим доступом або взагалі бути закритою.

Після проведення паспортизації має відбутися внесення даних паспорта безпеки об’єктів критичної інфраструктури до Переліку. Очевидно, що внесення об’єктів до Переліку об’єктів критичної інфраструктури має здійснювати Уповноважений орган у справах захисту критичної інфраструктури України за

поданням відповідальних за сектори критичної інфраструктури. При цьому важливим етапом обліку буде періодичне оновлення даних паспортів безпеки об'єктів критичної інфраструктури, що може відбуватися щорічно або кожні два роки з огляду на важливість і пріоритетність виконання завдань захисту критичної інфраструктури.

Паспорти безпеки об'єктів критичної інфраструктури мають готуватися операторами об'єктів критичної інфраструктури і надаватися на погодження до відповідальних за сектори суб'єктів захисту критичної інфраструктури.

При формуванні паспортів безпеки будуть враховуватись наявність в Україні декількох систем, що забезпечують захист від різних загроз. Система захисту критичної інфраструктури має забезпечити координацію різних систем і відомств через механізм узгодження і підтримки діяльності.

Організаційні заходи для впровадження регулювання

Для впровадження цього регуляторного акта необхідно забезпечити інформування громадськості про вимоги регуляторного акта шляхом його оприлюднення у засобах масової інформації та розміщення на сайті Верховної Ради України.

Реалізація цього регуляторного акта забезпечить вирішення визначених проблем, сприятиме поліпшенню умов функціонування стратегічних об'єктів інфраструктури України.

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 потребуватиме додаткових бюджетних витрат і ресурсів на адміністрування регулювання державними органами та не потребуватиме додаткових витрат суб'єктів господарювання, пов'язаних з виконанням вимог регуляторного акта.

VII. Обґрунтування запропонованого строку дії регуляторного акта.

Строк дії цього регуляторного акта встановлюється на необмежений термін з моменту набрання чинності, оскільки необхідність виконання положень регуляторного акта є постійною та спрямована на розбудову державної системи захисту критичної інфраструктури, визначення правових та організаційних засад забезпечення її діяльності у сфері національної безпеки.

VIII. Визначення показників результативності дії регуляторного акта.

До показників результативності дії регуляторного акта належать:

1. Кількість державних органів та їх територіальних органів, на яких поширюватиметься дія акта, відповідальних за формування і реалізацію державної політики у сфері захисту критичної інфраструктури.

2. Кількість суб'єктів господарювання, на яких поширюватиметься дія акта, які є операторами критичної інфраструктури та які відповідають за поточне функціонування об'єктів критичної інфраструктури.

3. Розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов'язаних з дією Закону.

4. Рівень поінформованості суб'єктів господарювання та (або) фізичних осіб із основними положеннями регуляторного акта – вище середнього, оскільки:

- зі змістом законопроекту та супровідних до нього документів можна

ознайомитися на офіційному веб-сайті Мінекономрозвитку (www.me.gov.ua);

- після схвалення законопроекту та подання його на розгляд Верховній Раді України в установленому порядку зі змістом законопроекту та супровідних до нього документів можна буде ознайомитися на Порталі Верховної Ради України у рубриці “Законотворчість”;

- після прийняття проекту Закону Верховною Радою України та його підписання Президентом України Закон буде розміщено на офіційному веб-сайті Верховної ради України;

5. Розмір коштів і час, що витрачатимуться суб’єктами господарювання та/або державними органами та їх територіальними органами, пов'язаними з виконанням вимог Закону.

6. Кількість об’єктів критичної інфраструктури, які забезпечено належним рівнем захисту.

7. Рівень захищеності об’єктів критичної інфраструктури.

8. Рівень заходів захисту об’єктів критичної інфраструктури.

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

Відстеження результативності регуляторного акта здійснюватиметься Мінекономіки.

Базове відстеження регуляторного акта здійснюватиметься після набрання ним чинності, але не пізніше дня, з якого починається проведення повторного відстеження його результативності.

Повторне відстеження результативності регуляторного акта здійснюється в межах строків, установлених статтею 10 Закону України “Про засади державної регуляторної політики у сфері господарської діяльності”, – через два роки після набрання чинності актом або більшістю його положень.

Періодичні відстеження результативності регуляторного акта будуть здійснюватися раз на кожні три роки, починаючи з дня закінчення заходів з повторного відстеження результативності цього акта.

Аналіз регуляторного впливу підготовлено департаментом економіки безпеки і оборони Міністерства розвитку економіки, торгівлі та сільського господарства України.

Міністр розвитку економіки, торгівлі та сільського господарства України **Ігор ПЕТРАШКО**

"____" _____ 2020 р.