МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ
(Мінекономрозвитку)
вул. М. Грушевського, 12/2 м. Київ 01008 тел. 253-93-94, факс 253-63-71
Web: http://www.me.gov.ua , e-mail: meconomy@me.gov.ua , код згідно з ЄДРПОУ 37508596

_____ № _____ На № _____ від _____

Державна регуляторна служба України

Щодо проекту Закону України
"Про критичну інфраструктуру
та її захист"

Відповідно до Закону України "Про засади державної регуляторної політики у сфері господарської діяльності" Мінекономрозвитку надсилає на погодження проект Закону України "Про критичну інфраструктуру та її захист".

У проекті Закону враховано зауваження та пропозиції Державної регуляторної служби України, надіслані листом від 04.09.2018 № 8814/0/20-18, а також рекомендації, отримані під час консультацій щодо доопрацювання аналізу регуляторного впливу до проекту Закону.

Просимо розглянути та погодити зазначений проект Закону у **триденний строк**.

Додатки: 1. Проект Закону України на 30 арк.
2. Аналіз регуляторного впливу на 13 арк.
3. Копія оприлюдненого повідомлення про оприлюднення проекту Закону України на 1 арк.
4. Витяг доповнень до плану діяльності з підготовки проектів регуляторних актів у сфері господарської діяльності на 2018 рік (з офіційного веб-сайту Мінекономрозвитку) на 2 арк.

Перший віце-прем'єр-міністр України –
Міністр **Степан КУБІВ**

Молочко Володимир
253-93-25

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 І
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів і понять

1. У цьому Законі наведені нижче терміни вживаються у 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 й стійкість критичної інфраструктури;

3) державна система захисту критичної інфраструктури - система суб'єктів із забезпечення реалізації державної політики у сфері захисту критичної інфраструктури;

4) життєво важливі послуги - послуги, що забезпечуються державними установами, підприємствами та організаціями будь-якої форми власності, 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 випадку їх реалізації;

7) категорія критичності об'єкту інфраструктури - відносна міра (відносне мірило) важливості об'єкта критичної інфраструктури, в залежності від ступеня його впливу на здійснення життєво важливих функцій та надання життєво важливих послуг;

8) категоризація об'єктів інфраструктури - 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 вимагає 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 національних інтересів;

13) оператор критичної інфраструктури - державний орган, підприємство, установа, організація, юридична та/або фізична особа, 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 визначеної форми, який містить структуровані дані про об'єкт критичної інфраструктури та визначає комплекс заходів, що вживаються оператором 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) рівень критичності - відносна міра важливості об'єктів критичної інфраструктури, якою враховується вплив раптового припинення функціонування або функціонального збою на безпеку постачання, забезпечення суспільства важливими товарами і послугами;

17) 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);

18) сектор критичної інфраструктури - сукупність об'єктів критичної інфраструктури, які належать до одного сектору економіки та/або мають спільну функціональну спрямованість;

19) 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;

20) суб'єкти державної системи захисту критичної інфраструктури - органи державної влади, органи місцевого самоврядування, Збройні Сили України та інші військові формування, утворені відповідно до законів України, правоохоронні органи, а також підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки об'єктів критичної інфраструктури.

2. Інші терміни вживаються у значеннях, наведених у Кодексі цивільного захисту України, Кримінальному кодексі України, Законах України "Про основи національної безпеки 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 державну таємницю", "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, акти Президента, Кабінету Міністрів України, а також інші нормативно-правові акти, що прийняті на виконання цього Закону.

Стаття 3. Сфера застосування Закону

1. 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 ІІ.
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 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) встановлення повноважень та 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 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.

4. Державна політика захисту критичної інфраструктури на тимчасово окупованих територіях здійснюється відповідно до Законів України "Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях", "Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України".

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 України, запобігання проявам актів несанкціонованого втручання, прогнозування та запобігання кризовим ситуаціям з негативним впливом на об'єкти критичної інфраструктури, а також підвищення рівня захисту, удосконалення заходів безпеки та стійкості цих об'єктів від існуючих загроз.

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

1) забезпечення безпеки, стійкості та цілісності критичної інфраструктури України;

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

3) створення та організація 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 правового регулювання безпеки на об'єктах 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 України;

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, введення до експлуатації, модернізації;

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

9) встановлення науково-обґрунтованих підходів до 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) координованість;

2) єдність методологічних засад;

3) державно-приватна взаємодія;

4) забезпечення конфіденційності;

5) міжнародне співробітництво.

Стаття 7. Рівні управління державної системи захисту критичної інфраструктури

1. Державна система захисту критичної інфраструктури включає в себе такі рівні управління:

1) загальнодержавний рівень, який здійснюється Кабінетом Міністрів України, Уповноваженим органом у справах захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень, згідно з цим Законом;

2) регіональний та галузевий рівень, який здійснюється органами державної влади, які визначені у встановленому законодавством порядку відповідальними за відповідні сектори критичної інфраструктури та їх захист;

3) місцевий рівень, що здійснюється місцевими органами виконавчої влади в межах повноважень, покладених на них цим Законом;

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

РОЗДІЛ ІІ.
КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ

Стаття 8. Об'єкти критичної інфраструктури

1. До об'єктів критичної інфраструктури можуть бути віднесені підприємства, установи, організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, централізованого водовідведення, постачання теплової енергії, гарячої води, електричної енергії і газу, виробництва продуктів, харчування, охорони здоров'я;

3) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

4) підлягають охороні та обороні в умовах надзвичайного стану і особливого періоду;

5) є об'єктами підвищеної небезпеки;

6) є об'єктами, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру;

7) є об'єктами, порушення функціонування яких призведе до кризової ситуації регіонального значення.

Стаття 9. Критерії віднесення об'єктів до критичної інфраструктури

1. 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, а саме:

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

2) завдання значної шкоди нормальним умовам життєдіяльності населення;

3) уразливість цих об'єктів, тяжкість настання 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 ВВП, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного значення; обороноздатності; іміджу країни;

4) 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;

5) тривалість ліквідації таких наслідків та дією подальшого негативного впливу на інші сектори держави;

6) вплив на функціонування суміжних секторів критичної інфраструктури.

Стаття 10. Категоризація об'єктів критичної інфраструктури

1. Для визначення рівня вимог до забезпечення захисту об'єктів критичної інфраструктури, повноважень та відповідальності суб'єктів державної системи захисту критичної інфраструктури, в межах секторів здійснюється категоризація об'єктів критичної інфраструктури, на які поширюється сфера дії цієї системи:

1) I категорія критичності – критично важливі об'єкти – об'єкти, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру. Зазначені об'єкти включаються до Національного переліку об'єктів критичної інфраструктури, формуються вимоги щодо забезпечення їх захисту;

2) II категорія критичності – життєво важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення. Зазначені об'єкти включаються до Національного переліку об'єктів критичної інфраструктури, формуються вимоги щодо розмежування завдань й повноважень органів державної влади та операторів критичної інфраструктури, спрямованих на забезпечення їх захисту та відновлення функціонування;

3) III категорія критичності – важливі об'єкти, пріоритетом захисту яких є забезпечення швидкого відновлення функцій за рахунок диверсифікації та резервів. Відповідальність за стійкість функціонування об'єктів несуть оператори при встановлених законодавством вимогах щодо взаємодії із органами державної влади;

4) IV категорія критичності – необхідні об'єкти, безпосередній захист яких є відповідальністю оператора, який має мати план реагування на кризову ситуацію.

2. Категоризація об'єктів критичної інфраструктури, в межах визначених секторів критичної інфраструктури здійснюється відповідальними за сектори суб'єктами державної системи захисту критичної інфраструктури.

3. Суб'єкти державної системи захисту критичної інфраструктури, визначені відповідальними за сектори критичної інфраструктури, складають та ведуть Переліки об'єктів критичної інфраструктури.

4. До об'єктів інфраструктури I та II категорії критичності встановлюються обов'язкові вимоги щодо організації захисту критичної інфраструктури.

5. До об'єктів інфраструктури III категорії критичності встановлюються рекомендаційні вимоги щодо рівня організації захисту та стійкості інфраструктури.

Стаття 11. Складання та ведення Національного переліку об'єктів критичної інфраструктури

1. Для цілей узгодження дій суб'єктів державної системи захисту критичної інфраструктури з організації захисту найбільш важливих об'єктів інфраструктури формується Національний перелік об'єктів критичної інфраструктури.

2. Збирання, узагальнення, попередній аналіз даних щодо об'єктів критичної інфраструктури та пропозиції щодо внесення таких об'єктів до Національного переліку об'єктів критичної інфраструктури в межах визначених секторів здійснюється відповідальними за сектори суб'єктами державної системи захисту критичної інфраструктури.

3. Національний перелік об'єктів критичної інфраструктури формується та ведеться Уповноваженим органом у справах захисту критичної інфраструктури на основі пропозицій суб'єктів державної системи захисту критичної інфраструктури, направлених на розгляд Уповноваженого органу.

4. Після внесення об'єкту до Національного переліку об'єктів критичної інфраструктури відповідальний за сектор суб'єкт державної системи захисту критичної інфраструктури повідомляє про це оператора об'єкта критичної інфраструктури для здійснення паспортизації об'єкта критичної інфраструктури.

5. Порядок ведення Національного переліку об'єктів критичної інфраструктури, внесення об'єктів до цього переліку, та надання інформації з Національного переліку встановлюються Кабінетом Міністрів України за поданням Уповноваженого органу у справах захисту критичної інфраструктури України.

6. З метою розподілення функцій із захисту об'єктів критичної інфраструктури між суб'єктами державної системи захисту критичної інфраструктури Кабінетом Міністрів України затверджується перелік секторів критичної інфраструктури та встановлюються суб'єкти державної системи захисту критичної інфраструктури, які є відповідальними за сектори.

7. Для забезпечення належного рівня захисту критичної інфраструктури відповідальні за сектори суб'єкти державної системи захисту критичної інфраструктури можуть залучати, у тому числі на договірних засадах, для охорони об'єктів критичної інфраструктури інших суб'єктів державної системи захисту критичної інфраструктури відповідно до їхніх повноважень, встановлених цим Законом та іншими нормативними актами, що регулюють діяльність таких суб'єктів державної системи захисту критичної інфраструктури.

8. Залучення суб'єктів державної системи захисту критичної інфраструктури до захисту об'єктів критичної інфраструктури здійснюється після розроблення, складання та узгодження з визначеними органами та службами паспортів безпеки на об'єкти критичної інфраструктури.

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 відповідальних за сектори суб'єктів 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. Розроблення паспорта безпеки, порядок його наповнення, зміст та строки подання встановлюються Кабінетом Міністрів України.

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

РОЗДІЛ ІІІ.
ДЕРЖАВНА СИСТЕМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 13. Органи, що забезпечують формування та реалізацію державної політики у сфері захисту критичної інфраструктури

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

2. Для створення системи інформаційно-аналітичної підтримки процесу прийняття рішень щодо забезпечення захисту та стійкості критичної інфраструктури створюється та функціонує національна мережа ситуаційно-кризових центрів (інформаційно-аналітичних, диспетчерських), функцію яких здійснюють структурні підрозділи суб'єктів державної системи захисту критичної інфраструктури.

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

Стаття 14. Суб'єкти державної системи захисту критичної інфраструктури

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

1) Уповноважений орган у справах 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 адміністрації;

7) оператори критичної інфраструктури;

8) громадські організації, населення.

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;

2) режим готовності та запобігання реалізації загроз - суб'єктами державної системи захисту критичної інфраструктури: проводиться перевірка та переведення системи захисту до готовності забезпечити захист та реагування на випадок реалізації загрози;

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.

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.

Рішення щодо оголошення режимів функціонування критичної інфраструктури та запровадження окремих правових станів приймається суб'єктом, відповідальним за сектор критичної інфраструктури.

Стаття 16. Уповноважений орган у справах захисту критичної інфраструктури

1. З метою формування і реалізації державної політики у сфері захисту критичної інфраструктури створюється та функціонує Уповноважений орган у справах захисту критичної інфраструктури України.

2. Уповноважений орган у справах захисту критичної інфраструктури:

1) координує діяльність міністерств та інших центральних органів виконавчої влади у сфері захисту та безпеки об'єктів критичної інфраструктури України;

2) взаємодіє з операторами критичної інфраструктури з питань забезпечення захисту об'єктів критичної інфраструктури;

3) здійснює оцінку захищеності об'єктів критичної інфраструктури, внесених до Національного переліку об'єктів критичної інфраструктури;

4) проводить перевірку на правильність віднесення об'єктів до критичної інфраструктури;

5) проводить із залученням суб'єктів державної системи захисту критичної інфраструктури, які визначені відповідальними за сектори критичної інфраструктури, оцінку загроз критичній інфраструктурі на загальнодержавному рівні;

6) веде Національний перелік об'єктів критичної інфраструктури України;

7) розробляє та подає на затвердження Кабінету Міністрів України:

Національний план захисту та забезпечення стійкості критичної інфраструктури;

перелік секторів критичної інфраструктури та суб'єктів державної системи захисту критичної інфраструктури, які є відповідальними за ці сектори;

порядок розроблення, форму та зміст паспорту безпеки об'єкта критичної інфраструктури;

порядок розроблення, форму та зміст планів заходів щодо захисту критичної інфраструктури, які приймаються на загальнодержавному рівні;

пропозиції щодо оголошення зміни режимів функціонування державної системи захисту критичної інфраструктури;

типові вимоги щодо забезпечення захисту та стійкості об'єктів критичної інфраструктури відповідно до категорій критичності;

8) звертається до Національної академії наук України, Національного інституту стратегічних досліджень, інших наукових установ, закладів вищої освіти щодо проведення наукової та науково-технічної діяльності з питань забезпечення захисту та стійкості об'єктів критичної інфраструктури;

9) здійснює інші повноваження, передбачені цим Законом та Положенням про Уповноважений орган у справах захисту критичної інфраструктури України.

3. Положення про Уповноважений орган у справах захисту критичної інфраструктури України затверджується Кабінетом Міністрів України.

Стаття 17. Служба безпеки України

1. Служба безпеки України:

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

2) здійснює контррозвідувальне забезпечення, контртерористичний та контрдиверсійний захист об'єктів критичної інфраструктури, захист її економічного та науково-технічного потенціалу, 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, екстремізму, сепаратизму з використанням об'єктів критичної інфраструктури;

4) бере участь у перевірці інвестицій та походження капіталу, що спрямовується на фінансування критичної інфраструктури, на предмет дотримання їх операторами інтересів національної безпеки держави;

5) вживає заходів з попередження та протидії актам несанкціонованого втручання в діяльність об'єктів критичної інфраструктури, фінансування критичної інфраструктури не в інтересах національної безпеки,

6) отримує у визначеному законом порядку доступ до автоматизованих інформаційних і довідкових систем, реєстрів та банків даних, держателем (адміністратором) яких є органи державної влади, оператори об'єктів критичної інфраструктури;

7) 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;

8) бере участь в обмеженні та блокуванні доступу до об'єктів та ресурсів, які використовуються для організації, підготовки, вчинення, фінансування, сприяння або приховування акту несанкціонованого втручання в діяльність критичної інфраструктури, а також в інших передбачених законами України випадках у порядку, встановленому законодавством;

9) проводить перевірку угод на постачання товарів, робіт і послуг на об'єкти критичної інфраструктури та персоналу компаній-підрядників на предмет завдання шкоди національній безпеці України;

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

11) здійснює спеціальну перевірку осіб для допуску на об'єкти критичної інфраструктури;

12) 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;

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

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

15) використовує для своєї діяльності інформацію щодо критичної інфраструктури, отриману від Уповноваженого органу у справах захисту критичної інфраструктури України й інших суб'єктів захисту критичної інфраструктури;

16) знайомиться в органах державної влади, органах місцевого самоврядування, в операторів об'єктів критичної інфраструктури із документами та іншими матеріальними носіями інформації, необхідними для попередження, виявлення та недопущення актів несанкціонованого втручання в діяльність об'єктів критичної інфраструктури, у тому числі такими, що містять інформацію з обмеженим доступом;

17) направляє військовослужбовців Служби безпеки України для роботи на штатних посадах в Уповноваженому органі у справах захисту критичної

інфраструктури України, на об'єкти критичної інфраструктури незалежно від форм власності в інтересах їх захисту;

18) ініціює застосування та притягнення до відповідальності посадових осіб операторів об'єктів критичної інфраструктури, за невжиття заходів із безпечного функціонування об'єктів критичної інфраструктури та вчинення (або невчинення) ними дій, які призводять до послаблення їх режимно-охоронного захисту, стійкості, цілісності та не забезпечують їх відновлення у випадку відмов, атак та настання інших кризових ситуацій;

19) створює бази даних щодо загроз і уразливості об'єктів критичної інфраструктури;

20) вживає заходів для забезпечення виконання міжнародних зобов'язань України у рамках захисту критичної інфраструктури;

21) здійснює міжнародне співробітництво і взаємодіє з іноземними державними та спеціальними правоохоронними органами у рамках надання міжнародно-правової допомоги у сфері захисту критичної інфраструктури;

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

23) 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;

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

2. Служба безпеки України здійснює діяльність у сфері захисту критичної інфраструктури через свої структурні органи (управління, відділи, підрозділи, служби), яким делеговані відповідні повноваження.

Стаття 18. Міністерство внутрішніх справ України

1. Міністерство внутрішніх справ України:

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

2) забезпечує координацію у сфері захисту критичної інфраструктури центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України та 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 19. 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:

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 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 аварійно-рятувального обслуговування об'єктів критичної інфраструктури аварійно-рятувальними службами;

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 при виникненні надзвичайних ситуацій;

6) бере участь у межах компетенції у розробленні нормативно-правових та інших нормативних актів у сфері захисту критичної інфраструктури.

Стаття 20. 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.

Стаття 21. Національна поліція України

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

1) протидію злочинним посяганням на об'єкти критичної інфраструктури або важливих державних об'єктів, 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 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 II, III та IV категорії критичності, охорону яких покладено на Національну поліцію України, а також погодження паспортів безпеки на кожний такий об'єкт.

Стаття 22. Міністерство оборони України

1. Міністерство оборони України у сфері захисту критичної інфраструктури забезпечує:

1) організацію захисту від терористичних посягань об'єктів Збройних Сил, озброєння, військової техніки, матеріально-технічних засобів, що знаходяться у військових частинах або зберігаються у визначених місцях, підготовку і застосування військ (сил) Збройних Сил у разі вчинення терористичного акту в повітряному просторі чи територіальних водах України;

2) участь у веденні антитерористичних операцій на військових об'єктах;

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

4) виконання завдань з протиповітряного прикриття важливих об'єктів держави, перелік яких визначається Кабінетом Міністрів України.

Стаття 23. Державна спеціальна служба транспорту

1. Державна спеціальна служба транспорту у мирний та в особливий період у сфері захисту критичної інфраструктури забезпечує:

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

2) охорону державних об'єктів національної транспортної системи України, перелік яких визначається Кабінетом Міністрів України.

Стаття 24. Центральний орган виконавчої влади, який забезпечує формування та реалізує державну політику в електроенергетичному, ядерно-промисловому, вугільно-промисловому, торфодобувному, нафтогазовому та нафтогазопереробному комплексах, а також забезпечує формування державної політики у сфері нагляду (контролю) у галузях електроенергетики та теплопостачання

1. Центральний орган виконавчої влади, який забезпечує формування та реалізує державну політику в електроенергетичному, ядерно-промисловому, вугільно-промисловому, торфодобувному, нафтогазовому та нафтогазопереробному комплексах, а також забезпечує формування державної політики у сфері нагляду (контролю) у галузях електроенергетики та теплопостачання у сфері захисту критичної інфраструктури у межах своєї компетенції:

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

2) здійснює обмін інформацією з питань оцінки загроз та реагування на загрози і кризові ситуації, а також ліквідації їх наслідків у взаємодії з іншими суб'єктами державної системи захисту критичної інфраструктури;

3) забезпечує здійснення заходів щодо запобігання, виявлення і припинення терористичних актів та злочинів терористичної спрямованості на об'єктах, що належать до його сфери управління;

4) приймає участь у міжнародному співробітництві з питань захисту критичної інфраструктури

5) створює у своєму складі структурний підрозділ з питань захисту критичної інфраструктури;

6) готує пропозиції щодо включення інфраструктурних об'єктів до критичної інфраструктури;

7) збирає, узагальнює та здійснює попередній аналіз даних щодо об'єктів критичної інфраструктури та їх функціонування у енергетичному секторі;

8) забезпечує функціонування відповідних систем обміну інформацією, моніторингу безпекових умов на об'єктах критичної інфраструктури у енергетичному секторі;

9) бере участь у встановленому законодавством порядку, у реагуванні на кризові ситуації, пов'язані з безпекою, захистом та стійкістю критичної інфраструктури у енергетичному секторі;

10) здійснює раннє оповіщення (попередження про загрози) операторів критичної інфраструктури та надає інформаційну, консультативну, експертну і технологічну допомогу операторам критичної інфраструктури у енергетичному секторі, користувачам їх послуг (населенню) задля попередження, реагування та мінімізації можливого впливу загроз;

11) розробляє й упроваджує стандарти, норми і регламенти захисту критичної інфраструктури у енергетичному секторі критичної інфраструктури;

12) здійснює перевірки та оцінки захищеності об'єктів критичної інфраструктури у енергетичному секторі;

13) подає операторам об'єктів критичної інфраструктури обов'язкові для розгляду пропозиції з питань захисту критичної інфраструктури у енергетичному секторі та обов'язкові до виконання вимоги щодо усунення причин і умов, які порушують цілісність і стійкість критичної інфраструктури;

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

15) приймає участь у погодженні та обліку паспортів безпеки об'єктів критичної інфраструктури у енергетичному секторі, а також у визначенні ризиків для адміністративно-територіальних одиниць.

Стаття 25. Центральний орган виконавчої влади, що забезпечує формування та реалізує державну політику у сферах автомобільного, залізничного, морського та річкового транспорту, надання послуг поштового зв'язку

1. Центральний орган виконавчої влади, що забезпечує формування та реалізує державну політику у сферах автомобільного, залізничного, морського та річкового транспорту, надання послуг поштового зв'язку:

1) забезпечує формування державної політики з питань захисту об'єктів критичної інфраструктури галузі транспорту на основі постійного аналізу стану їх захищеності;

2) забезпечує нормативно-правове регулювання державної політики у сферах, які належать до його компетенції, розробляє та впроваджує галузеві стандарти і норми з питань захисту об'єктів та/або елементів критичної інфраструктури об'єктів національної транспортної системи;

3) забезпечує підготовку пропозицій щодо включення об'єктів (елементів) національної транспортної системи до переліку об'єктів (елементів) критичної інфраструктури у галузі транспорту;

4) координує навчання працівників об'єктів критичної інфраструктури у галузі транспорту;

5) здійснює моніторинг, постійний аналіз стану справ та оцінювання результатів реалізації державної політики з питань захисту об'єктів (елементів) критичної інфраструктури у галузі транспорту, розробляє пропозиції щодо її покращення та щодо варіантів розв'язання виявлених проблем, здійснює оцінку їх переваг і ризиків;

6) розробляє пропозиції щодо формування державної політики за результатами проведеного аналізу, узгодження інтересів, цілей та шляхів розв'язання проблем;

7) бере участь у заходах з інформування громадськості з питань захисту критичної інфраструктури;

8) здійснює заходи щодо адаптації законодавства України до законодавства Європейського Союзу відповідно до зобов'язань України в рамках Угоди про асоціацію, вивчає європейський досвід з питань захисту критичної інфраструктури у галузі транспорту;

9) бере участь у міжнародному співробітництві з питань захисту критичної інфраструктури, здійснює координацію залучення, надання та використання міжнародної фінансової допомоги з питань захисту критичної інфраструктури у галузі транспорту;

10) бере участь у встановленому порядку в реагуванні на кризові ситуації, пов'язані з вчиненням актів несанкціонованого втручання;

11) надає консультативну, експертну допомогу операторам критичної інфраструктури з питань захисту критичної інфраструктури у галузі транспорту;

12) бере участь у погодженні та обліку паспортів безпеки об'єктів критичної інфраструктури у галузі транспорту.

Стаття 26. 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) забезпечує формування та реалізацію державної політики щодо 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 комунікаційних систем, систем управління технологічними процесами, 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 27. Центральний орган виконавчої влади, який реалізує державну політику із здійснення державного нагляду (контролю) у сфері охорони навколишнього природного середовища, раціонального використання, відтворення і охорони природних ресурсів

1. Центральний орган виконавчої влади який реалізує державну політику із здійснення державного нагляду (контролю) у сфері охорони навколишнього природного середовища, раціонального використання, відтворення і охорони природних ресурсів забезпечує:

реалізацію державної політики із здійснення державного нагляду (контролю) у сфері охорони навколишнього природного середовища, раціонального використання, відтворення і охорони природних ресурсів;

здійснення в межах повноважень, передбачених законом, державного нагляду (контролю) за додержанням вимог природоохоронного законодавства, зокрема на об'єктах критичної інфраструктури для оцінки їх захищеності від можливого виникнення надзвичайних, аварійних, техногенно-екологічних ситуацій та природних явищ, які можуть заподіяти державі значні обсяги збитків, пов'язані із забрудненням, пошкодженням чи знищенням її природних ресурсів;

участь, у встановленому законодавством порядку, у реагуванні на кризові ситуації, шляхом проведення кризового моніторингу об'єктів навколишнього природного середовища від початку виникнення їх аварійного забруднення до відновлення показників їх природного стану;

використання, у межах повноважень, інформації щодо критичної інфраструктури, отриманої від Уповноваженого органу у справах захисту критичної інфраструктури України й інших суб'єктів захисту критичної інфраструктури;

надання операторам критичної інфраструктури обов'язкових для розгляду вимог з питань захисту критичної інфраструктури та обов'язкових для виконання запитів про діяльність об'єктів критичної інфраструктури та приписів про усунення причин та умов, які порушують стійкість критичної інфраструктури;

надання пропозицій у межах компетенції, до встановлення категорій критичності об'єктів критичної інфраструктури, визначення критеріїв та порядку оцінки стану безпеки та захищеності об'єктів критичної інфраструктури;

доступ до автоматизованих інформаційних та довідкових систем, реєстрів та банків даних, держателем (адміністратором) яких є органи державної влади, оператори об'єктів критичної інфраструктури;

підготовку пропозицій щодо включення інфраструктурних об'єктів до критичної інфраструктури.

Стаття 28. Інші центральні органи виконавчої влади

1. Інші центральні органи виконавчої влади у сфері захисту критичної інфраструктури:

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

2) готують пропозиції щодо включення інфраструктурних об'єктів до критичної інфраструктури;

3) формують перелік об'єктів критичної інфраструктури, що належать до сфери їх управління і потребують першочергового захисту у разі ускладнення ситуації, виникнення загрози, у тому числі зумовленої терористичними загрозами;

4) здійснюють іншу діяльність для захисту критичної інфраструктури в межах повноважень, визначеними законами, що регулюють діяльність суб'єктів захисту критичної інфраструктури.

2. Інші центральні органи виконавчої влади здійснюють діяльність у сфері захисту критичної інфраструктури через свої територіальні органи та/або підприємства, установи та організації, що належать до сфери їх управління.

Стаття 29. Органи виконавчої влади, які визначені відповідальними за відповідні сектори критичної інфраструктури

1. Органи виконавчої влади, які визначені відповідальними за відповідні сектори критичної інфраструктури:

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

2) готують пропозиції щодо включення інфраструктурних об'єктів до критичної інфраструктури;

3) збирають, узагальнюють та здійснюють попередній аналіз даних щодо об'єктів критичної інфраструктури та їх функціонування;

4) розробляють та затверджують вимоги до забезпечення захисту та стійкості секторів критичної інфраструктури; загрози критичній інфраструктурі

у відповідних секторах; плани взаємодії суб'єктів державної системи захисту критичної інфраструктури у відповідних секторах для всіх режимів функціонування критичної інфраструктури;

5) забезпечують функціонування відповідних систем обміну інформацією, моніторингу безпекових умов на об'єктах критичної інфраструктури;

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

7) здійснюють раннє оповіщення (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 й упроваджують стандарти, норми і регламенти захисту критичної інфраструктури у відповідних секторах критичної інфраструктури;

9) здійснюють перевірки та оцінки захищеності об'єктів критичної інфраструктури;

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) запроваджують галузеві програми з протидії загрозам внутрішніх порушників, у т.ч. завдяки заходам, спрямованим на досягнення високого рівня культури безпеки (фізичної та технічної);

12) приймають участь у погодженні та обліку паспортів безпеки об'єктів критичної інфраструктури, а також у визначенні ризиків для адміністративно-територіальних одиниць;

13) здійснюють організацію системи підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури тощо.

Стаття 30. Місцеві 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 доступу до життєво важливих ресурсів;

2) розробку та погодження із заінтересованими органами місцевих планів взаємодії залучених суб'єктів, планів відновлення функціонування критичної інфраструктури.

Стаття 31. 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 захисту і забезпечення безпеки 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 державного, місцевого та приватного секторів;

4) вжиття оперативних заходів у разі отримання інформації про загрозу проникнення на територію об'єкта;

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/збоїв, вчинення протиправних дій або впливу природних явищ;

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 будь-якими 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) призначення відповідальних осіб за захист та фізичну та кібернетичну безпеку на об'єктах, 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.

2. 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.

3. Оператори критичної інфраструктури зобов'язані:

1) забезпечити захист, в тому числі фізичний і кіберзахист, об'єктів критичної інфраструктури, що належать їм на праві власності або на іншій законній підставі;

2) направляти у встановлені терміни до контролюючих суб'єктів захисту критичної інфраструктури відомості про виконання заходів, що містяться в приписі за результатами проведеної перевірки та оцінки захищеності об'єктів критичної інфраструктури;

3) невідкладно інформувати відповідальних за сектори суб'єктів захисту критичної інфраструктури про інциденти, що сталися на об'єктах критичної інфраструктури, які належать їм на праві власності або іншій законній підставі;

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

5) забезпечувати безперешкодний доступ контролюючих суб'єктів захисту критичної інфраструктури до об'єкту критичної інфраструктури, при реалізації ними повноважень, передбачених цим Законом та іншими нормативно-правовими актами;

6) сприяти іншим суб'єктам захисту критичної інфраструктури у виявленні, попередженні і припиненні актів несанкціонованого втручання, а також в ліквідації їх наслідків, встановлення причин і умов їх вчинення;

7) забезпечувати цілісність і сталу експлуатацію об'єктів критичної інфраструктури з додержанням мінімально можливого ризику;

8) забезпечувати виконання технічних умов (регламентів), порядку встановлення і експлуатації, а також збереження технічних засобів систем виявлення, попередження та ліквідації наслідків кібератак на інформаційні ресурси об'єктів критичної інфраструктури;

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

РОЗДІЛ IV.
ОРГАНІЗАЦІЙНІ ЗАСАДИ ДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 32. Організаційні засади захисту критичної інфраструктури

1. Захист критичної інфраструктури включає в себе:

1) визначення секторів критичної інфраструктури, встановлення відповідальних суб'єктів захисту критичної інфраструктури за визначені сектори;

2) встановлення категоризації об'єктів критичної інфраструктури для визначення рівня вимог до забезпечення захисту критичної інфраструктури, повноважень та відповідальності суб'єктів;

3) складання та ведення Національного переліку об'єктів критичної інфраструктури;

4) паспортизацію об'єктів критичної інфраструктури;

5) визначення режимів функціонування критичної інфраструктури та розроблення планів реагування на кризові ситуації;

6) взаємодію та обмін інформацією між суб'єктами державної системи захисту критичної інфраструктури та визначення рівня доступу до такої інформації третіх осіб;

7) здійснення контролю за рівнем безпеки об'єктів критичної інфраструктури та їх стійкості;

8) встановлення шляхів взаємодії між органами державної влади та приватним сектором в сфері захисту критичної інфраструктури;

9) запровадження критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури;

10) запровадження методології проведення оцінки загроз об'єкту критичної інфраструктури та реагування на них, зокрема щодо аварій і технічних збоїв, небезпечних природних явищ, зловмисних дій, тощо;

11) реалізацію заходів, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем, захист технологічної інформації, що циркулює на об'єктах критичної інфраструктури.

Стаття 33. Планування заходів щодо забезпечення стійкості та захисту об'єктів критичної інфраструктури

1. Для організації діяльності державної системи захисту критичної інфраструктури Кабінетом Міністрів України, центральними органами виконавчої влади, місцевими державними адміністраціями, органами місцевого самоврядування, операторами розробляються та затверджуються відповідні плани та програми реагування на кризові ситуації.

2. На загальнодержавному рівні:

1) розробляється Національний план захисту та забезпечення стійкості критичної інфраструктури, який затверджується Кабінетом Міністрів України;

2) встановлюються вимоги до планування заходів щодо захисту критичної інфраструктури, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об'єктів критичної інфраструктури, плани проведення навчань та тренувань.

3. На галузевому та регіональному рівнях органами державної влади розробляються і затверджуються галузеві плани та програми з протидії загрозам критичній інфраструктурі.

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

5. На місцевому рівні:

Органи місцевого самоврядування 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 доступу до життєво важливих ресурсів. Ці програми включають заходи з забезпечення захисту та стійкості критичної інфраструктури, взаємодії суб'єктів системи захисту критичної інфраструктури, а також відновлення функціонування об'єктів критичної інфраструктури.

6. На об'єктовому рівні:

оператори 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.

7. Заходи щодо кіберзахисту об'єктів критичної інфраструктури на всіх рівнях, а також захист технологічної інформації, що циркулює в автоматизованих системах об'єктів критичної інфраструктури, здійснюються відповідно до законодавства у сфері захисту інформації та кібербезпеки.

Повноваження суб'єктів державної системи захисту критичної інфраструктури щодо забезпечення кібербезпеки та кіберзахисту об'єктів критичної інфраструктури визначаються законодавством у сфері захисту інформації та кібербезпеки.

Стаття 34. Здійснення контролю за рівнем безпеки об'єктів критичної інфраструктури та їх стійкості

1. Контроль за рівнем безпеки об'єктів критичної інфраструктури здійснюється шляхом оцінки захищеності об'єктів критичної інфраструктури.

2. Метою здійснення контролю є встановлення відповідності стану безпеки об'єкта критичної інфраструктури параметрам, задекларованим оператором об'єкта критичної інфраструктури у паспорті безпеки на відповідний об'єкт, надання методичної допомоги операторам об'єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури.

3. Оцінка захищеності об'єктів критичної інфраструктури проводиться визначеними цим Законом суб'єктами державної системи захисту об'єктів критичної інфраструктури.

4. Порядок проведення контролю визначається Кабінетом Міністрів України.

Стаття 35. 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 при загрозі виникнення або виникненні:

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) техногенних або природних катастроф та аварій 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;

9) здійснення інших заходів, передбачених законодавством.

Стаття 36. Державно-приватна взаємодія у сфері захисту критичної інфраструктури

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

1) створення системи своєчасного виявлення, запобігання та нейтралізації загроз критичній інфраструктурі, у тому числі із залученням волонтерських організацій;

2) підвищення комплексних знань, навичок і вмінь громадян, необхідних для реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо захисту критичної інфраструктури;

3) обміну інформацією між органами державної влади, приватним сектором і громадянами щодо загроз об'єктам критичної інфраструктури та кризових ситуацій на цих об'єктах;

4) залучення експертного потенціалу, наукових установ, професійних об'єднань та громадських організацій до підготовки ключових галузевих

проектів та нормативних документів у сфері захисту критичної інфраструктури;

5) надання консультативної та практичної допомоги з питань реагування на кризові ситуації на об'єктах критичної інфраструктури;

6) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки критичної інфраструктури;

7) запровадження механізму громадського контролю ефективності заходів з захисту критичної інфраструктури;

8) періодичного проведення спільних заходів з постачальниками бізнес-послуг, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері захисту критичної інфраструктури;

9) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань захисту критичної інфраструктури;

10) забезпечення постійної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, іншими підприємствами з метою виконання заходів з захисту критичної інфраструктури;

11) забезпечення сталого функціонування об'єктів критичної інфраструктури у різних режимах шляхом вирішення комплексу завдань щодо підтримки відповідного технологічного процесу та його безаварійної зупинки;

12) організації забезпечення захисту персоналу від можливих загроз;

13) забезпечення резервування основних ресурсів для функціонування об'єкта критичної інфраструктури у різних режимах;

14) оповіщення місцевого населення про інциденти та кризові ситуації на об'єктах критичної інфраструктури.

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

3. Органи державної влади та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та громадські об'єднання зобов'язані сприяти суб'єктам, повідомляти відомі їм дані щодо загроз національній безпеці або будь-яких інших кіберзагроз критичній інфраструктурі, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії злочинним діям, терористичним атакам та мінімізації їх наслідків.

Стаття 37. Відповідальність за порушення законодавства у сфері захисту критичної інфраструктури

1. Органи державної виконавчої влади, органи місцевого самоврядування, їхні посадові, оператори об'єктів критичної інфраструктури, винні у порушенні законодавства у сфері захисту критичної інфраструктури, несуть відповідальність згідно з законом.

Стаття 38. 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 39. 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.

ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

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

2. Внести зміни до таких законів України:

1) У Законі України "Про Кабінет Міністрів України" (Відомості Верховної Ради (ВВР), 2014, № 13, ст.222) пункт п'ятий частини першої статті 20 після абзацу сьомого доповнити абзацом такого змісту:

"забезпечує проведення державної політики у сфері захисту критичної інфраструктури України";

2) У Законі України "Про Службу безпеки України" (Відомості Верховної Ради України, 1992 р., № 27, ст. 382; 2004 р., № 32, ст. 394; 2006 р., № 14, ст. 116, № 30, ст. 258; 2011 р., № 10, ст. 63; 2012 р., № 29, ст. 333):

а) частину першу статті 2 після слів "оборонного потенціалу України," доповнити словами "критичної інфраструктури,";

б) частину першу статті 10 і частину першу статті 15 після слів "захисту національної державності," доповнити словами "контррозвідувального захисту критичної інфраструктури,";

в) частину першу статті 24 доповнити пунктом 6-1 такого змісту:

"6-1) здійснювати контррозвідувальний захист критичної інфраструктури;".

3) Абзац четвертий частини першої статті 5 Закону України "Про

оперативно-розшукову діяльність" (Відомості Верховної Ради України, 1992 р., № 22, ст. 303, № 39, ст. 572; 1993 р., № 11, ст. 83; 1998 р., № 26, ст. 149; 1999 р., № 4, ст. 35; 2001 р., № 10, ст. 44, № 14, ст. 72; 2002 р., № 33, ст. 236; 2003 р., № 27, ст. 209, № 30, ст. 247, № 45, ст. 357; 2004 р., № 8, ст. 66; 2005 р., № 10, ст. 187, № 25, ст. 335; 2006, № 14, ст. 116) після слів "захисту національної державності," доповнити словами "контррозвідувального захисту інтересів держави у сфері інформаційної безпеки, контррозвідувального захисту критичної інфраструктури,".

4) Пункт 2 частини першої статті 6 Закону України "Про контррозвідувальну діяльність" (Відомості Верховної Ради України, 2003 р., № 12, ст. 89, № 27, ст. 209; 2006 р., № 14, ст. 116; 2011 р., № 32, ст. 314; 2013 р., № 21, ст. 208; 2014 р., № 12, ст. 178; 2016 р., № 19, ст. 214) доповнити новим абзацом четвертим, виклавши його в такій редакції: "контррозвідувального захисту критичної інфраструктури;".

У зв'язку з цим абзаци четвертий – сьомий вважати абзацами п'ятим – восьмим відповідно.

5) В абзаці четвертому частини другої статті 1 Закону України "Про загальну структуру і чисельність Служби безпеки України" (Відомості Верховної Ради України, 2006 р., № 4, ст. 53, № 30, ст. 258; 2009 р., № 24, ст. 296; 2012 р., № 29, ст. 333) слова "контррозвідувального захисту економіки держави" замінити словами "контррозвідувального захисту критичної інфраструктури".

6) У Законі України "Про державну таємницю":

пункт 4 частини першої статті 8 після абзацу третього доповнити абзацом такого змісту:

"відомості про організацію, зміст, стан і плани забезпечення захисту об'єктів критичної інфраструктури".

У зв'язку з цим абзаци четвертий – дванадцятий вважати абзацами п'ятим – тринадцятим відповідно.

6) У Законі України "Про доступ до публічної інформації":

частину першу статті 9 після абзацу першого доповнити абзац такого змісту:

"2) щодо об'єктів критичної інфраструктури та запроваджених заходів їх захисту, яку не віднесено до державної таємниці";

частину третю статті 9 після слів "іншими суб'єктами владних повноважень" доповнити словами "та об'єктами критичної інфраструктури".

7) У Законі України "Про доступ до публічної інформації":

частину першу статті 9 після абзацу першого доповнити абзацом такого змісту:

"2) щодо об'єктів критичної інфраструктури та запроваджених заходів їх захисту, яку не віднесено до державної таємниці";

частину третю статті 9 після слів "іншими суб'єктами владних повноважень" доповнити словами "та об'єктами критичної інфраструктури".

8) У законі України "Про правовий режим воєнного стану" (Відомості Верховної Ради (ВВР), 2015, № 28, ст.250):

а) у частині першій статті 1 після слів “забезпечення національної безпеки” доповнити розділовими знаками та словами: “, захисту критичної інфраструктури,”:

б) у частині першій статті 15 після слів “Про мобілізаційну підготовку та мобілізацію” доповнити розділовими знаками та словами: “ “Про критичну інфраструктуру та її захист” ”.

9) У Законі України “Про інформацію” (Відомості Верховної Ради України, 2011 р., № 32, ст. 313):

а) статтю 10 після абзацу десятого доповнити новим абзацом такого змісту:

“критична технологічна інформація”.

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

б) доповнити статтею 191 такого змісту:

“Стаття 19-1. Критична технологічна інформація

1. Критична технологічна інформація - це 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. Технологічна інформація за режимом доступу відноситься до інформації з обмеженим доступом та підлягає захисту згідно із законодавством.”

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

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

привести свої нормативно-правові акти у відповідність із цим Законом;

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

С. Кубів

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проекту Закону України
"Про критичну інфраструктуру та її захист"

І. Визначення проблеми.

Світові тенденції до посилення загроз природного та техногенного характеру, підвищення рівня терористичних загроз, збільшення кількості та підвищення складності кібератак, а також пошкодження інфраструктурних об'єктів у східних та південних регіонах України внаслідок збройної агресії Російської Федерації зумовили актуалізацію питання захисту систем, об'єктів і ресурсів, які є критично важливими для життєдіяльності громадян, функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки.

З урахуванням потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми на загальнодержавному рівні створення державної системи захисту критичної інфраструктури (сукупності об'єктів, які є стратегічно важливими для економіки і безпеки держави, суспільства, населення та порушення функціонування яких може завдати шкоди життєво важливим національним інтересам України) є одним із пріоритетів у реформуванні сектору оборони і безпеки України.

Основними проблемами, які потребують розв'язання, є:

необхідність розвитку 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;

необхідність узгодження 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;

нерозвиненість державно-приватного партнерства у сфері захисту критичної інфраструктури та невизначеність джерел фінансування заходів із захисту критичної інфраструктури;

недостатній рівень міжнародного співробітництва у сфері захисту критичної інфраструктури.

Для вирішення цих проблемних питань доцільно прийняти окремий законодавчий акт, який забезпечить врегулювання відносин, пов'язаних із забезпеченням безперебійного та сталого функціонування об'єктів критичної

інфраструктури України, запобіганням проявам актів несанкціонованого втручання в їх роботу та інцидентів щодо них, прогнозуванням та запобіганням кризових ситуацій, які створюють негативний вплив на об'єкти критичної інфраструктури України, а також підвищенням рівня захисту, вдосконаленням заходів безпеки цих об'єктів від існуючих загроз будь-якого походження (природного та техногенного характеру, протиправних дій), забезпеченням їх стійкості.

Зазначений 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 quo)*	Вигоди відсутні. Ситуація залишиться на рівні, що існує. Відсутність законодавчого врегулювання відносин у сфері захисту критичної інфраструктури "консервує" ті проблемні питання, які є на сьогодні у цій сфері та залишаються невирішеними, що може створити загрози національній безпеці України.	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 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	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

	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; – 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.	інфраструктури, з прийняттям Закону, буде здійснюватись шляхом перерозподілу коштів в межах видатків, передбачених на кожен відповідний орган влади. Термін інтеграції та 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	Реалізація не потребує додаткових матеріальних та інших витрат з боку громадян.

	надання життєво-важливих послуг та функцій для суспільства та населення.	

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 середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 9 х рядок 10), гривень	1574995	7874975

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*	1	Збереження чинного регулювання не дає змоги досягнути поставлених цілей державного регулювання, не забезпечується вирішення визначених проблемних питань у

цио)		сфері захисту критичної інфраструктури, не забезпечується захист безперервності надання життєво-важливих послуг та функцій для держави, суспільства та населення.
Альтернатива 2. *(Інший, відмінний від запропонованого способу (внесення змін до чинних законодавчих актів)*	1	Така альтернатива не дає змоги 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 3.	1. Забезпечить виконання 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.	Прийняття законопроекту не пов'язане з додатковими витратами держави та громадян, а витрати суб'єктів господарювання перекриються вигодами від безперервності бізнесу.	Ціль прийняття регуляторного акта, визначена розділом 1 цього АРВ, буде досягнута повною мірою, проблема державного регулювання, 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.

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 Національного переліку об'єктів критичної інфраструктури; статтею 13 – координація діяльності органів виконавчої влади у сфері захисту критичної інфраструктури; статтею 14 – суб'єкти державної системи захисту критичної інфраструктури; статтею 32 – завдання, права та обов'язки операторів критичної інфраструктури, тощо.

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.

Результативність дії регуляторного акта здійснюватиметься за допомогою здійснення базового, повторного, періодичного відстежень.

Базове відстеження результативності здійснюватиметься після набрання чинності цим регуляторним актом, але не пізніше дня, з якого починається проведення повторного відстеження результативності цього акта.

Повторне відстеження результативності регуляторного акта здійснюється через рік з дня набрання ним чинності, але не пізніше двох років після набрання ним чинності.

Періодичне відстеження результативності регуляторного акта здійснюється раз на три роки, починаючи з дня виконання заходів із повторного відстеження.

У разі виявлення неврегульованих та проблемних питань під час проведення аналізу показників дії цього акта, ці питання будуть вирішені шляхом внесення відповідних змін.

Перший віце-прем'єр-міністр України – Міністр економічного розвитку і торгівлі України **Степан КУБІВ**

Повідомлення про оприлюднення проекту Закону України "Про критичну інфраструктуру та її захист"

20.07.2018 | 15:54 | Департамент стратегічного розвитку сектору оборони та безпеки

На виконання розпорядження Кабінету Міністрів України від 06.12.2017 № 1009 "Про схвалення Концепції створення державної системи захисту критичної інфраструктури", з метою визначення основних засад державної політики у сфері захисту критичної інфраструктури, врегулювання правових і господарських відносин, що виникають під час такої діяльності, повноважень державних органів у сфері захисту критичної інфраструктури Мінекономрозвитку розроблено проект Закону України "Про критичну інфраструктуру та її захист".

Електронну версію проекту Закону України розміщено у рубриці "Обговорення проектів документів", що міститься на головній сторінці веб-сайту Міністерства економічного розвитку і торгівлі України.

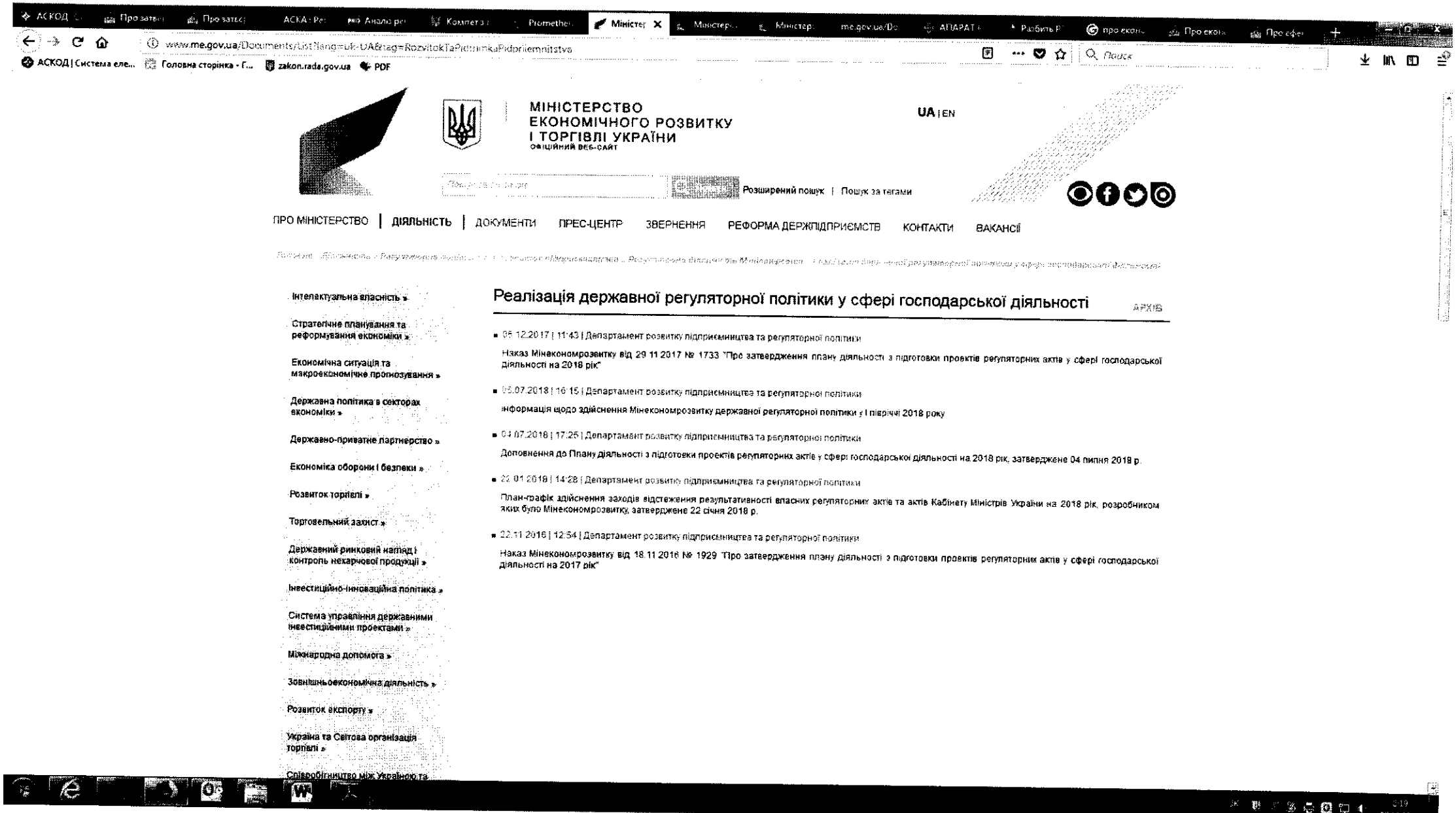
Зауваження та пропозиції до законопроекту просимо надсилати протягом одного місяця з дати його оприлюднення у паперовому та електронному виглядах:

Міністерство економічного розвитку і торгівлі України,

01008, м. Київ, вул. М. Грушевського, 12/2.

Контактна особа: Кушнір Ольга Василівна, тел. 253-93-25, вн. 200-47-73*3988;

e-mail : kushnir@me.gov.ua.



МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ
ОФІЦІЙНИЙ ВЕБ-САЙТ

UA | EN

Розширений пошук | Пошук за тегами

ПРО МІНІСТЕРСТВО | ДІЯЛЬНІСТЬ | ДОКУМЕНТИ | ПРЕС-ЦЕНТР | ЗВЕРНЕННЯ | РЕФОРМА ДЕРЖПІДПРИЄМСТВ | КОНТАКТИ | ВАКАНСІЇ

Інтелектуальна власність »
Стратегічне планування та реформування економіки »
Економічна ситуація та макроекономічне прогнозування »
Державна політика в секторах економіки »
Державно-приватне партнерство »
Економіка оборони і безпеки »
Розвиток торгівлі »
Торговельний захист »
Державний ринковий нагляд і контроль нехарчової продукції »
Інвестиційно-інноваційна політика »
Система управління державними інвестиційними проектами »
Міжнародна допомога »
Зовнішньоекономічна діяльність »
Розвиток експорту »
Україна та Світова організація торгівлі »
Співробітництво між Україною та

Реалізація державної регуляторної політики у сфері господарської діяльності

АРХІВ

- 05.12.2017 | 11:43 | Департамент розвитку підприємництва та регуляторної політики

  Наказ Мінекономрозвитку від 29.11.2017 № 1733 "Про затвердження плану діяльності з підготовки проектів регуляторних актів у сфері господарської діяльності на 2018 рік"

- 05.07.2018 | 16:15 | Департамент розвитку підприємництва та регуляторної політики

  Інформація щодо здійснення Мінекономрозвитку державної регуляторної політики у I півріччі 2018 року

- 04.07.2018 | 17:25 | Департамент розвитку підприємництва та регуляторної політики

  Доповнення до Плану діяльності з підготовки проектів регуляторних актів у сфері господарської діяльності на 2018 рік, затверджене 04 липня 2018 р.

- 22.01.2018 | 14:28 | Департамент розвитку підприємництва та регуляторної політики

  План-графік здійснення заходів відстеження результативності власних регуляторних актів та актів Кабінету Міністрів України на 2018 рік, розробником яких була Мінекономрозвитку, затверджене 22 січня 2018 р.

- 22.11.2016 | 12:54 | Департамент розвитку підприємництва та регуляторної політики

  Наказ Мінекономрозвитку від 18.11.2016 № 1929 "Про затвердження плану діяльності з підготовки проектів регуляторних актів у сфері господарської діяльності на 2017 рік"

Дата внесення доповнення у план 24 травня 2018 р.					
21	Проект постанови Кабінету Міністрів України «Про внесення зміни у додаток до постанови Кабінету Міністрів України від 20 грудня 2006 р. № 1765 «Про порядок встановлення та застосування	з метою підтвердження українського походження фотоелектричних модулів вітчизняного виробництва, що дозволить отримати конкурентну перевагу для вітчизняних виробників цієї	грудень	врегулювання питання отримання сертифіката походження на фотоелектричні модулі, сприяння вітчизняним виробникам цієї продукції збільшенню її обсягів реалізації, покращенню фінансово-економічного стану та, як наслідок, збільшення надходження до Державного	відділ розвитку машинобудів ної галузі, авіабудування та суднобудуван

	правила адвалерної частки та виконання виробничих і технологічних операцій»	продукції в Україні, пропонується включити код товарної підпозиції 8541 40 згідно з УКТЗЕД (прилади напівпровідникові фоточутливі, включаючи фотогальванічні елементи, зібрані або не зібрані у модуль або вмонтовані чи вмонтовані в панель; світловипромінювальні діоди) до переліку технологічних операцій, за якими визначається країна походження товару, затвердженого постановою Кабінету Міністрів України від 20 грудня 2006 р. № 1765		бюджету України за рахунок сплати податків та забезпечення створення нових робочих місць	ня (інд. 3803)
22	Проект Закону України «Про критичну інфраструктуру та її захист»	на виконання пункту 2 Плану організації виконання Указу Президента України від 16 січня 2017 р. № 8 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» до підпункту 2 пункту 1 зазначеного рішення Ради національної безпеки і оборони України розроблено проект Закону	грудень	створення державної системи захисту критичної інфраструктури, запровадить єдині підходи до організації управління об'єктами системи на державному та місцевому рівнях, визначить засади взаємодії залучених до захисту критичної інфраструктури державних органів та суб'єктів господарювання, суспільства та громадян	відділ стратегічного планування у секторі оборони та безпеки (інд. 2711)