ПРОЕКТ

Вноситься
Кабінетом Міністрів України

В. ГРОЙСМАН

“ ” 2019 р.

# *ЗАКОН УКРАЇНИ*

Про критичну інфраструктуру та її захист

---

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

## Розділ I
## ЗАГАЛЬНІ ПОЛОЖЕННЯ

### Стаття 1. Визначення основних термінів

1. У цьому Законі терміни вживаються в такому значенні:

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

2) безпека критичної інфраструктури – стан захищеності критичної інфраструктури, за якого забезпечується функціональність, безперервність роботи, цілісність і стійкість критичної інфраструктури;

3) державна система захисту критичної інфраструктури – система суб’єктів із забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури;

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

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

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

7) категорія критичності об'єкта інфраструктури – відносний рівень важливості об'єкта критичної інфраструктури залежно 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 потребує залучення додаткових сил і ресурсів;

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

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

12) об'єкт критичної інфраструктури – визначений у встановленому законодавством порядку складовий елемент критичної інфраструктури, функціональність, безперервність, цілісність і стійкість якого забезпечують реалізацію життєво важливих 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.

2. Інші терміни вживаються у значенні, наведеному в Кодексі цивільного захисту України, Кримінальному кодексі України, Законах України “Про національну безпеку України”, “Про боротьбу з тероризмом”, “Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання”, “Про об’єкти підвищеної небезпеки”, “Про основні засади забезпечення кібербезпеки України”, “Про інформацію”, “Про 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 цього Закону

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

## Розділ 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 у сфері захисту критичної інфраструктури ґрунтується на засадах:

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

2) визначення законодавчих вимог до захисту критичної інфраструктури;

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

4. Державна політика у сфері 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, прийняття в експлуатацію, 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, управління на якому здійснюється Кабінетом Міністрів України, Уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень, згідно з цим Законом;

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

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

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

## Розділ III
## КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ

### Стаття 8. Об’єкти критичної інфраструктури

1. До об’єктів критичної інфраструктури відносяться підприємства, установи, організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, оборонно-промислового комплексу, 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 харчових продуктів, 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.

До таких критеріїв належать:

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 можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода: здоров’ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам 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 дія 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) І 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) ІІ 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) ІІІ 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 – об’єкти, безпосередній захист яких є відповідальністю оператора, який повинен 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. Складення 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 сфері захисту критичної інфраструктури на основі пропозицій суб’єктів державної системи захисту критичної інфраструктури, направлених на розгляд Уповноваженого органу.

4. Після внесення об’єкта 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 сфері 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 нормативно-правовими 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. Порядок розроблення паспорта безпеки на об ’ єкт, його наповнення, зміст і 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 IV
## ДЕРЖАВНА СИСТЕМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

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

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

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

3. 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.

### Стаття 14. Суб'єкти державної системи захисту критичної інфраструктури

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

1) Уповноважений орган у сфері захисту критичної інфраструктури України;

2) міністерства та інші центральні органи виконавчої влади;

3) Служба безпеки України;

4) правоохоронні та розвідувальні органи;

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

6) місцеві державні адміністрації;

7) органи місцевого самоврядування;

8) оператори критичної інфраструктури незалежно від форми власності;

9) підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки об’єктів критичної інфраструктури, у тому числі суб’єкти охоронної діяльності;

10) громадські організації, об’єднання та організації роботодавців.

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

### 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.

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

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

Стаття 16. Уповноважений орган у сфері захисту критичної інфраструктури

1. Уповноважений орган у сфері захисту критичної інфраструктури:

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

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 сфері захисту критичної інфраструктури.

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

Стаття 17. Служба безпеки України

1. Служба безпеки України у сфері захисту критичної інфраструктури:

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

2) здійснює контррозвідувальний, 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 походження інвестицій з метою недопущення спроб використання об’єктів критичної інфраструктури у фінансуванні терористичної та іншої протиправної діяльності;

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

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

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

10) здійснює спеціальну перевірку осіб для допуску на об’єкти критичної інфраструктури;

11) 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;

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

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

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

15) відряджає військовослужбовців Служби безпеки України для роботи на штатних посадах в Уповноваженому органі у сфері захисту критичної інфраструктури, на об’єкти критичної інфраструктури незалежно від форм власності в інтересах їх захисту;

16) 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;

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

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

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

20) здійснює аналітичну обробку інформації, проводить контррозвідувальні, оперативно-розшукові, пошукові та адміністративно-правові заходи, спрямовані на боротьбу з кібертероризмом і

кібершпигунством стосовно об’єктів критичної інформаційної інфраструктури;

21) 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;

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

Стаття 18. Міністерство внутрішніх справ України

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

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

2) 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, у сфері захисту критичної інфраструктури:

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

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

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

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

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

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 важливі державні об’єкти, які загрожують безпеці громадян і порушують функціонування систем життєзабезпечення;

2) здійснення на договірних засадах охорони об’єктів критичної інфраструктури ІІ категорії критичності, 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.

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 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:

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 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 та впроваджує 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) 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 у сфері захисту критичної інфраструктури:

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 у сфері захисту критичної інфраструктури, 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 ситуацій та інших небезпечних подій, 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 моніторингу об’єктів навколишнього природного середовища від початку виникнення їх забруднення до відновлення показників їх природного стану;

використання, у межах компетенції, інформації щодо критичної інфраструктури, отриманої від Уповноваженого органу у сфері захисту критичної інфраструктури 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;

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

8) розробляють та впроваджують 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, зокрема завдяки заходам, спрямованим на досягнення високого рівня культури безпеки (фізичної та технічної);

12) беруть 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 для здійснення життєво важливих функцій;

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 та інших небезпечних подій, вчинення протиправних дій;

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

9) негайне інформування органів Національної поліції України, Служби безпеки України, підрозділів Національної гвардії України, інших державних органів про інциденти, пов'язані з 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) сприяти суб’єктам захисту критичної інфраструктури, у тому числі шляхом надання доступу до об'єкту критичної інфраструктури, під час реалізації ними повноважень, передбачених цим Законом та іншими нормативно-правовими актами, з метою виявлення, попередження і припинення загроз безпеці об’єктів критичної інфраструктури;

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

7) 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;

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

## Розділ V
## ОРГАНІЗАЦІЙНІ ЗАСАДИ ДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

### Стаття 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 та інших небезпечних подій, 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 складові 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 здійснення життєво важливих функцій. 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 за поданням Уповноваженого органу у сфері захисту критичної інфраструктури 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 у разі загрози виникнення або виникнення:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

9) здійснення інших заходів, передбачених законодавством.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Розділ VI
## ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

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

2. Внести зміни до таких законів України:

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

2) 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; 2014 р., № 12, ст. 189):

частину першу статті 2 після слів “оборонного потенціалу України” доповнити словами “, критичної інфраструктури”;

друге речення частини першої статті 10 та частину першу статті 15 після слів “захисту національної державності” доповнити словами “, контррозвідувального захисту критичної інфраструктури”;

частину першу статті 24 доповнити пунктом $6^1$ такого змісту:

“$6^1$) здійснювати контррозвідувальний захист критичної інфраструктури;”;

3) пункт 4 частини першої статті 8 Закону України “Про державну таємницю” (Відомості Верховної Ради України, 1999 р., № 49, ст. 428; 2010 р., № 46, ст. 537; 2013 р., № 21, ст. 208; 2014 р., № 22, ст. 816) після абзацу третього доповнити новим 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 відповідно абзацами п’ятим – тринадцятим;

4) пункт 2 частини першої статті 6 Закону України “Про контррозвідувальну діяльність” (Відомості Верховної Ради України, 2003 р., № 12, ст. 89; 2014 р., № 12, ст. 178; 2016 р., № 19, ст. 214) після абзацу третього доповнити новим абзацом такого змісту:

“контррозвідувального захисту критичної інфраструктури;”.

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

5) абзац четвертий 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) викласти в такій редакції:

“контррозвідувального захисту критичної інфраструктури;”;

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

статтю 10 після абзацу десятого доповнити новим абзацом такого змісту:

“критична технологічна інформація;”.

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

доповнити Закон статтею $19^1$ такого змісту:

“Стаття $19^1$. Критична технологічна інформація

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

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

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

7) у статті 9 Закону України “Про доступ до публічної інформації” (Відомості Верховної Ради України, 2011 р., № 32, ст. 314):

частину першу доповнити пунктом $1^1$ такого змісту:

“$1^{1)}$ щодо об’єктів критичної інфраструктури та запроваджених заходів для їх захисту, яку не віднесено до державної таємниці;”;

частину третю після слів “іншими суб’єктами владних повноважень” доповнити словами “та об’єктами критичної інфраструктури”;

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

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

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

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

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

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

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

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

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

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

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

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

4) у шестимісячний строк з дня набрання чинності цим Законом забезпечити розроблення та внесення на розгляд Верховної Ради України законопроектів про стимулювання діяльності суб’єктів господарювання, які провадять діяльність, пов’язану із забезпеченням безпеки об’єктів критичної інфраструктури.

**Голова**
**Верховної Ради України**