ПРОЕКТ

ЗАКОН УКРАЇНИ

Про забезпечення безпеки і стійкості критичної інфраструктури

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) проектна загроза критичній інфраструктурі - документ визначеної форми, який визначає властивості та характеристики реальних й потенційних загроз критичній інфраструктурі, на захист від яких має бути спланована система захисту критичної інфраструктури;

17) 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;

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

19) Реєстр критичної інфраструктури – перелік найбільш важливої для життєдіяльності суспільства та держави критичної інфраструктури, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості та здійснюється державний контроль за їх дотриманням;

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

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

22) секторальний орган у сфері захисту критичної інфраструктури - суб’єкт державної системи захисту критичної інфраструктури, визначений відповідальним за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури у окремому секторі критичної інфраструктури;

23) функціональний орган у сфері захисту критичної інфраструктури - суб’єкт державної системи захисту критичної інфраструктури, який визначений відповідальними за функціонування окремих державних систем захисту та реагування.

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 безпеку секретної інформації”, “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 II
ОСНОВНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 4. Засади державної політики захисту критичної інфраструктури

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

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

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

2) визначення законодавчих вимог до захисту критичної інфраструктури;

3) 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, безпеки та стійкості цих об'єктів загроз будь-якого типу.

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) єдність методологічних засад;

2) координованість;

3) державно-приватна взаємодія;

4) конфіденційність комерційної інформації, безпека та охорона секретної інформації;

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 Президентом України, Радою національної безпеки і оборони України, Кабінетом Міністрів України, Уповноваженим органом у сфері захисту критичної інфраструктури України, органами державної влади відповідно до розподілу повноважень, згідно з цим Законом;

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

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

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

Розділ ІІІ
КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ

Стаття 8. Об’єкти критичної інфраструктури

1. Об’єкти критичної інфраструктури визначаються та включаються до Реєстру критичної інфраструктури в порядку встановленому Кабінетом Міністрів України.

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

До таких критеріїв належать:

1) 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 9. Сектори критичної інфраструктури

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

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

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

4. Даним законом встановлюється вимога щодо формування та реалізації політики у сфері захисту критичної інфраструктури забезпечення наступних життєво-важливих функцій та послуг:

- урядування та надання найважливіших державних послуг;

- енергозабезпечення;

- водозабезпечення;

- продовольче забезпечення;

- охорона здоров'я;

- зв'язок та комунікації;

- фінансові та банківські послуги;

- транспортне забезпечення;

- оборона та правопорядок;

- цивільний захист.

Стаття 10. Категоризація об'єктів критичної інфраструктури

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

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

3. Секторальні органами у сфері захисту критичної, складають та ведуть секторальні переліки об'єктів критичної інфраструктури визначених категорій.

Стаття 11. Складення та ведення Реєстру критичної інфраструктури

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

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

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

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

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

6. Щодо об'єктів критичної інфраструктури включених до Реєстру критичної інфраструктури встановлюється вимога погодження зміни права власності та зміни цільового призначення чи режиму його функціонування відповідно до вимог цього Закону. Порядок погодження зміни права власності та зміни цільове призначення чи режиму функціонування об'єкта критичної інфраструктури встановлюються Кабінетом Міністрів України.

7. Реєстр критичної інфраструктури є документом обмеженого доступу щодо якого застосовуються вимоги Закону України «Про безпеку секретної інформації».

Стаття 12. Паспортизація об'єктів критичної інфраструктури

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

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

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

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

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

6. Паспорт безпеки є документом обмеженого доступу щодо якого застосовуються вимоги Закону України «Про безпеку секретної інформації».

Розділ IV
ДЕРЖАВНА СИСТЕМА ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

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

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

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

3. З метою формування єдиних методологічних підходів та координації діяльності суб'єктів державної системи захисту критичної інфраструктури створюється та функціонує Уповноважений орган у справах захисту критичної інфраструктури України.

4. 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.

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

3. Обмін інформацією в рамках функціонування державної системи захисту критичної інфраструктури здійснюється з врахуванням вимог Закону України «Про безпеку секретної інформації».

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 та стійкості критичної інфраструктури;

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

Стаття 15. Режими функціонування державної системи захисту критичної інфраструктури

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

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

2) режим готовності та запобігання реалізації загроз — суб'єктами державної системи захисту критичної інфраструктури: проводиться перевірка та переведення системи захисту до готовності забезпечити захист та реагування на випадок реалізації загрози. Функціонування інфраструктури здійснюється відповідно до проектного цільового призначення;

3) режим реагування на виникнення кризової ситуації — суб'єктами державної системи захисту критичної інфраструктури із застосуванням заходів реагування на кризову ситуацію.

Функціонування інфраструктури відбувається в режимі кризової ситуації, вводяться обмеження на режими роботи об’єктів інфраструктури, економічні умови господарювання, доступу до об’єктів;

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

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

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

Стаття 16. Уповноважений орган у сфері захисту критичної інфраструктури

1. Уповноважений орган у сфері захисту критичної інфраструктури забезпечує координацію діяльності суб’єктів державної системи захисту критичної інфраструктури.

2. Уповноважений орган у сфері захисту критичної інфраструктури:

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

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

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

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

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

6) готує Оцінку ризиків критичній інфраструктурі національного рівня;

7) погоджує проектні загрози критичній інфраструктурі секторального рівня;

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

9) забезпечує обмін інформацією між суб’єктами державної системи захисту критичної інфраструктури.

10) надає пропозиції Кабінету Міністрів України щодо:

- Національного плану захисту та забезпечення стійкості критичної інфраструктури;

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

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

11) розробляє та подає на затвердження Ради національної безпеки і оборони України:

- Проектну загрозу критичній інфраструктурі національного рівня;

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

13) здійснює інші повноваження, передбачені цим Законом.

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

Стаття 17. Функціональні органи у сфері захисту критичної інфраструктури

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

1) Єдина державна система цивільного захисту;
2) Державна системою фізичного захисту з питань захищеності та охорони ядерних установок, ядерних матеріалів, запобігання диверсіям, крадіжкам або будь-якому іншому неправомірному вилученню радіоактивних матеріалів;
3) Єдина державна система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків;
4) Національна система кібербезпеки;
5) Органи сектору безпеки (спеціальні та правоохоронні органи);
6) Органи сектору оборони (Збройні сили України та система територіальної оборони).

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

1) беруть участь, у встановленому законодавством порядку, у реагуванні на кризові ситуації, пов'язані із забезпеченням безпеки та стійкості критичної інфраструктури;
2) готують пропозиції щодо включення об'єктів інфраструктури до Реєстру критичної інфраструктури;
3) формують перелік об'єктів критичної інфраструктури, що належать до сфери їх управління;
4) надають секторальним органам у сфері захисту критичної інфраструктури, власникам та операторам інфраструктури консультації щодо загроз критичній інфраструктурі та заходів щодо їх нейтралізації;
5) здійснюють іншу діяльність для захисту критичної інфраструктури в межах повноважень, визначеними законами, що регулюють діяльність суб'єктів захисту критичної інфраструктури, зокрема:
   - розробку та затвердження вимог законодавства у відповідних сферах щодо забезпечення захисту критичної інфраструктури;
   - забезпечення оцінки загроз та ризиків критичній інфраструктурі у відповідних сферах;
   - участь у проведенні оцінки загроз та ризиків критичній інфраструктурі на загальнодержавному рівні;
   - формування пропозицій до національної та секторальних проектних загроз;
   - організацію взаємодії та обміну інформацією із іншими суб'єктами державної системи захисту критичної інфраструктури;
   - контроль за дотриманням вимог законодавства у відповідних сферах.

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

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

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

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

6) 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 у захищені зони об’єктів 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, погодженні 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 державної системи захисту критичної інфраструктури;

15) відряджає співробітників 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 органами та установами іноземних держав, міжнародними організаціями 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, 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, 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. 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 25. Секторальні органи у сфері захисту критичної інфраструктури

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

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

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

2) здійснюють категоризацію критичної інфраструктури в межах визначених секторів критичної інфраструктури, формують переліки об’єктів критичної інфраструктури відповідно до секторальної специфіки та вимог секторального законодавства.

4) розробляють та затверджують:

- вимоги до забезпечення захисту та стійкості секторів критичної інфраструктури відповідно категорій об’єктів критичної інфраструктури;

- проектні загрози критичній інфраструктурі секторального рівня;

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

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

5) затверджують:

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

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

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

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

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

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

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

11) запроваджують:

- галузеві програми з протидії загрозам внутрішніх порушників, зокрема завдяки заходам, спрямованим на досягнення високого рівня культури безпеки (фізичної та технічної);13) здійснюють

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

- функціонування відповідних систем обміну інформацією, моніторингу безпекових умов на об’єктах критичної інфраструктури;

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

Стаття 26. 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 у кризовій ситуації з метою підтримання життєво-важливих функцій та надання життєво-важливих, планів відновлення функціонування критичної інфраструктури.

Стаття 27. Оператори критичної інфраструктури

1. Основними завданнями операторів критичної інфраструктури є:

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

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

3) проведення оцінки ризиків на об'єктах критичної інфраструктури та обмін інформацією про ризики та загрози з іншими суб'єктам державної системи захисту критичної інфраструктури державного, місцевого та приватного секторів;

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

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

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

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

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

9) негайне інформування органів Національної поліції України, Служби безпеки України, підрозділів Національної гвардії України, інших державних органів про інциденти, пов'язані з 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) 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 забезпечують розробку та затвердження, у встановленому законодавством порядку:

1) корпоративних вимог щодо організації захисту КІ;

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

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

4) Паспортів безпеки об’єктів критичної інфраструктури.

3. Оператори критичної інфраструктури мають право:

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

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

4.Оператори критичної інфраструктури зобов’язані:

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

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

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

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

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

Розділ V
ОРГАНІЗАЦІЙНІ ЗАСАДИ ДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 28. 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.

Стаття 29. 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 захищеності об'єкта критичної інфраструктури вимогам законодавства, достовірності наданої інформації визначеним суб'єктам державної системи захисту критичної інфраструктури, надання методичної допомоги операторам об'єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури.

3. Контроль за рівнем безпеки об'єктів критичної інфраструктури здійснюється шляхом оцінки захищеності об'єктів критичної інфраструктури. Оцінка захищеності об'єктів критичної інфраструктури проводиться суб'єктами державної системи захисту критичної інфраструктури, відповідно до їх повноважень визначених законодавством.

4. Контроль за дотриманням операторами критичної інфраструктури вимог законодавства, виконання висновків та рекомендацій Уповноваженого органу у сфері захисту критичної інфраструктури, достовірності наданої, в межах вимог даного закону, інформації здійснюється визначеними суб'єктам державної системи захисту критичної інфраструктури.

5. Порядок проведення контролю визначається Кабінетом Міністрів України.

Стаття 30. 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 31. 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.

2. 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 32. Погодження зміни права власності, цільового призначення чи режиму функціонування об’єкта критичної інфраструктури

1. Щодо об’єктів критичної інфраструктури включених до Реєстру критичної інфраструктури встановлюється вимога погодження зміни права власності та зміни цільового призначення чи режиму його функціонування.

2. Власник/оператор об’єкта критичної інфраструктури включеного до Реєстру критичної інфраструктури подає заявку до Уповноваженого органу у справах захисту критичної інфраструктури щодо намірів передати право власності на об’єкт критичної інфраструктури чи змінити цільове призначення, режим його функціонування.

3. Уповноважений орган у справах захисту критичної інфраструктури створює комісію щодо розгляду заявки власника/оператора об’єкта критичної інфраструктури із залученням відповідних секторальних та функціональних органів у сфері захисту критичної інфраструктури, а також представників власника/оператора критичної інфраструктури.

4. За результатами розгляду заявки власника/оператора об’єкта критичної інфраструктури Уповноважений орган у справах захисту критичної інфраструктури надає висновки та рекомендації власнику/оператору критичної інфраструктури.

5. Власник/оператор об’єкта критичної інфраструктури розглядає надані висновки та враховує рекомендації перед ініціюванням процесу зміни права власності, цільового призначення чи режиму функціонування об’єкта критичної інфраструктури.

6. У випадку незгоди щодо наданих висновків та рекомендацій власник/оператор об’єкта критичної інфраструктури має право їх оскарження шляхом звернення до Кабінету Міністрів України.

7. У випадку порушення власником/оператором критичної інфраструктури висновків та рекомендації наданих Уповноваженим органам у справах захисту критичної інфраструктури, відповідним секторальним органом у сфері захисту критичної інфраструктури запроваджується оперативний контроль за об’єктом критичної інфраструктури на період до прийняття рішення Кабінетом Міністрів України.

8. Оперативний контроль за функціонуванням об’єкта критичної інфраструктури відповідним секторальним органом у сфері захисту критичної інфраструктури здійснюється виключно для забезпечення штатного функціонування об’єкта критичної інфраструктури на період оскарження власником/оператором критичної інфраструктури висновків та рекомендації Уповноваженого органу у справах захисту критичної інфраструктури.

9. Кабінет Міністрів України, у період не більше 30 днів, приймає мотивоване рішення на звернення власника/оператора критичної інфраструктури щодо оскарження висновків та рекомендацій Уповноваженого органу у справах захисту критичної інфраструктури.

10. У разі погодження Кабінетом Міністрів України зміни права власності, цільового призначення чи режиму функціонування об'єкта критичної інфраструктури Уповноважений орган у справах захисту критичної інфраструктури інформує відповідних суб'єктів державної системи захисту критичної інфраструктури про необхідність перегляду планів та заходів забезпечення життєво-важливих функцій та надання життєво-важливих послуг з врахуванням нових загроз безпеці та стійкості критичної інфраструктури.

11. Порядок оскарження висновків та рекомендацій Уповноваженого органу у справах захисту критичної інфраструктури та Порядок запровадження оперативного контролю за функціонуванням об'єкта критичної інфраструктури затверджується Кабінетом Міністрів України.

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

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

Стаття 34. Фінансування заходів у сфері захисту критичної інфраструктури

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

2. Для забезпечення захисту критичної інфраструктури можуть створюватись, у визначеному законодавством порядку, окремі цільові механізми фінансування:

1) залучення власних та інвестиційних ресурсів операторами критичної інфраструктури в рамках державно-приватного партнерства;

2) врахування у тарифах (цінах) на послуги (продукцію) та звільнення від оподаткування частини видатків операторів критичної інфраструктури, здійснених на виконання визначених цим Законом вимог щодо захисту об'єктів критичної інфраструктури включених до Реєстру критичної інфраструктури;

3) створення ринкового механізму страхування ризиків у сфері захисту критичної інфраструктури.

3. Виключний перелік заходів захисту критичної інфраструктури щодо яких застосовуються вищезазначені цільові механізми фінансування затверджуються Кабінетом Міністрів України.

Стаття 35. Міжнародне співробітництво у сфері захисту критичної інфраструктури

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

2. Україна відповідно до міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення захисту критичної інфраструктури, зокрема у проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України "Про

порядок направлення підрозділів Збройних Сил України до інших держав” та “Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України”.

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

Розділ VI
ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

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

2. Внести 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) 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;

3) 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.”;

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

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

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

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

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

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

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

частину першу статті 15 після слів “Про мобілізаційну підготовку та мобілізацію” доповнити словами “Про забезпечення безпеки і стійкості критичної інфраструктури”.

7) статтю 7 Закону України «Про страхування» (Відомості Верховної Ради України (ВВР), 1996, № 18, ст. 78) доповнити пунктами 48 та 49 такого змісту:

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

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

8) у Законі України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403):

пункт 16) статті 1 вилучити:

абзац 24 статті 1 доповнити реченням «Термін «об’єкт критичної інфраструктури» вживаються в цьому Законі у значенні, визначеному Законом України "Про забезпечення безпеки і стійкості критичної інфраструктури".

пункт 1 статті 6 вилучити;

пункті 2 статті 6 викласти у такій редакції:

«Порядок віднесення об’єктів до об’єктів критичної інфраструктури та формування Реєстру критичної інфраструктури здійснюється відповідно до Закону України «Про забезпечення безпеки і стійкості критичної інфраструктури».

Загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а в банківській системі України - Національним банком України»

9) у Законі України «Про Про Раду національної безпеки і оборони України» (Відомості Верховної Ради України (ВВР), 1998, № 35, ст.237):

статтю 8 після другого абзацу доповнити новим абзацом такого змісту:

“забезпечує функцію Уповноваженого органу у сфері захисту критичної інфраструктури”.

У зв’язку з цим абзаци 3 - 5 статті 8 вважати відповідно абзацами 4 – 6.

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