**Додаток до листа Телекомпалати України від 20.01.2021 №2565**

**Порівняльна таблиця**

**пропозицій та зауважень до**

**проекту Закону України “Про критичну інфраструктуру”**

|  |  |  |
| --- | --- | --- |
| **Запропонована редакція** | **Зауваження та пропозиції ТелПУ** | **Обгрунтування/Коментарі** |
| Цей Закон визначає правові та організаційні засади функціонування та захисту критичної інфраструктури і є складовою законодавства України у сфері національної безпеки. |  |  |
| **Розділ І ЗАГАЛЬНІ ПОЛОЖЕННЯ** |  |  |
| **Стаття 1. Визначення основних термінів** |  |  |
| 1. У цьому Законі терміни вживаються в такому значенні: |  |  |
| 1) безпека критичної інфраструктури — стан захищеності критичної інфраструктури, за якого забезпечується функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури; |  |  |
| 2) життєво важливі функції — функції та послуги, надання яких забезпечується органами державної влади, органами місцевого самоврядування, установами, суб’єктами господарювання та організаціями будь-якої форми власності, збої, переривання та порушення надання призводить до швидких негативних наслідків для національної безпеки; | 2) життєво важливі функції — функції та послуги, надання яких забезпечується органами державної влади, органами місцевого самоврядування, установами, суб’єктами господарювання та організаціями будь-якої форми власності, **~~збої,~~ переривання** та порушення надання призводить до швидких негативних наслідків для національної безпеки; | «збої, переривання та порушення надання» – в чому різниця? |
| 3) захист критичної інфраструктури — всі види діяльності, зокрема, формування перед або під час створення, функціонування і відновлення, реорганізації об’єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об’єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації; | захист критичної інфраструктури — всі види діяльності**~~, зокрема, формування~~ ,** **що виконуються** перед або під час створення, функціонування, **~~і~~** відновлення, реорганізації об’єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об’єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації; | Редакційно |
| 4) категорія критичності(критерії) об’єкта критичної інфраструктури — ступінь (відносний рівень) важливості об’єкта критичної інфраструктури, класифікована залежно від його впливу на виконання життєво важливих функцій та(або) надання життєво важливих послуг; |  |  |
| 5) категоризація об’єктів інфраструктури — віднесення об’єктів інфраструктури до категорій критичності об’єктів інфраструктури; |  |  |
| 6) 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; |  |  |
| 7) критична інфраструктура — об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам; |  |  |
| 8) критична технологічна інформація — дані, що обробляються (приймаються, передаються, зберігаються) в інформаційно-телекомунікаційних системах об’єктів критичної інфраструктури, які безпосередньо впливають на його функціонування; |  |  |
| 9) оператор критичної інфраструктури — юридична особа будь-якої форми власності та/або фізична особа- підприємець, який/яка на правах власності, оренди або на інших законних підставах здійснює управління об'єктом критичної інфраструктури та відповідає за його поточне функціонування; |  |  |
| 10) національна система захисту критичної інфраструктури – сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення), органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури; |  |  |
| 11) несанкціоноване втручання — незаконні дії, що створили загрозу безпечному функціонуванню об’єкта критичної інфраструктури та призвели до одного або декількох з таких наслідків: порушили його безперервність і стійкість; створили реальні чи потенційні загрози для населення, суспільства, соціально-економічного стану, національної безпеки і оборони України; |  |  |
| 12) охорона об’єктів критичної інфраструктури — комплекс режимних, інженерних, інженерно-технічних та інших заходів (крім заходів із захисту інформації та кіберзахисту об’єктів критичної інформаційної інфраструктури), які організовуються і проводяться суб’єктами національної системи захисту критичної інфраструктури з метою запобігання та/або недопущення чи припинення протиправних дій (чи актів несанкціонованого втручання) на об’єктах критичної інфраструктури; |  |  |
| 13) паспорт безпеки — документ встановленої форми, який містить відомості про об’єкт критичної інфраструктури, а також комплекс заходів, що вживаються для захисту цього об’єкту від визначених для нього видів загроз (відомості, що містяться у паспорті безпеки, є інформацією з обмеженим доступом); |  |  |
| 14) проектна загроза об’єкту критичної інфраструктурі - документ встановленої форми, який визначає властивості, характеристики реальних і потенційних загроз об’єкту критичної інфраструктурі, на унеможливлення яких (з урахуванням ймовірності їх реалізації) повинна бути спланована система захисту критичної інфраструктури; |  |  |
| 15) рівень критичності об’єкта критичної інфраструктури — відносна міра важливості об’єкта, якою враховується його вплив на можливість виконання життєво важливих функцій та надання життєво важливих послуг; |  |  |
| 16) режим функціонування критичної інфраструктури — визначені оператором умови та вимоги до функціонування критичної інфраструктури залежно від стану і динаміки розвитку ситуації (штатний режим функціонування; режим функціонування в кризовій ситуації; режим відновлення); |  |  |
| 17) реєстр об’єктів критичної інфраструктури – перелік найбільш важливої для життєдіяльності суспільства та держави критичної інфраструктури, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості та здійснюється моніторинг їх дотримання; |  |  |
| 18) сектор критичної інфраструктури — сукупність об’єктів критичної інфраструктури, які належать до одного сектору (галузі) економіки та/або мають спільну функціональну спрямованість; |  |  |
| 19) стійкість критичної інфраструктури — стан критичної інфраструктури, за якого забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду. |  |  |
| 20) секторальний орган у сфері захисту критичної інфраструктури - державний орган, визначений законодавством відповідальним за забезпечення формування та реалізації публічної політики у сфері захисту критичної інфраструктури у окремому секторі критичної інфраструктури; |  |  |
| 21) функціональний орган у сфері захисту критичної інфраструктури – державний орган, який визначений відповідальним за функціонування окремих державних систем захисту та реагування. |  |  |
| 2. Інші терміни вживаються у значенні, наведеному в Кодексі цивільного захисту України, Кримінальному кодексі України, Кримінально-процесуальному кодексі України, Законах України “Про національну безпеку України”, “Про боротьбу з тероризмом”, “Про фізичний захист ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання”, “Про об’єкти підвищеної небезпеки”, “Про основні засади забезпечення кібербезпеки України”, “Про інформацію”, “Про оперативно-розшукову діяльність”, “Про контррозвідувальну діяльність”, “Про правовий режим надзвичайного стану”, “Про правовий режим воєнного стану”, “Про державну таємницю”. |  |  |
|  |  |  |
| **Стаття 2. Правова основа діяльності у сфері захисту критичної інфраструктури** |  |  |
| 1. Правову основу діяльності у сфері захисту критичної інфраструктури становлять Конституція України, міжнародні договори, що стосуються захисту критичної інфраструктури, згода на обов’язковість яких надана Верховною Радою України, цей Закон, інші закони України, а також інші нормативно-правові акти, що прийняті на виконання цього Закону. |  |  |
|  |  |  |
| **Стаття 3. Сфера застосування цього Закону** |  |  |
| 1. Цей Закон унормовує діяльність у сфері захисту критичної інфраструктури у мирний час. |  |  |
| Діяльність у сфері захисту критичної інфраструктури в умовах надзвичайного, воєнного стану, особливого періоду регулюється відповідними законами України “Про правовий режим воєнного стану”, “Про правовий режим надзвичайного стану” та “**Про оборону**”. | Діяльність у сфері захисту критичної інфраструктури в умовах надзвичайного, воєнного стану, особливого періоду регулюється відповідними законами України “Про правовий режим воєнного стану”, “Про правовий режим надзвичайного стану” та “Про оборону **України**”. | Редакційна правка |
| Окремим законом регулюються відносини, що виникають при здійсненні заходів, спрямованих на забезпечення кіберзахисту та кібербезпеки об'єктів критичної інфраструктури. |  |  |
|  |  |  |
| **Розділ II** |  |  |
| **ОСНОВНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ** |  |  |
| **ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ** |  |  |
| **Стаття 4. Засади державної політики захисту критичної інфраструктури** |  |  |
| 1. Захист критичної інфраструктури є складовою частиною забезпечення національної безпеки України. |  |  |
| 2. Державна політика у сфері захисту критичної інфраструктури ґрунтується на засадах: |  |  |
| 1) визнання необхідності забезпечення безпеки критичної інфраструктури; |  |  |
| 2) визначення законодавчих вимог до принципів, пріоритетів, стратегічних завдань, підходів захисту критичної інфраструктури; |  |  |
| 3) визначення суб'єктів національної системи захисту критичної інфраструктури, їх повноважень та засад відповідальності, порядку взаємодії суб’єктів; |  |  |
| 4) створення умов, спрямованих на мінімізацію реалізації можливих загроз, ліквідацію та/або мінімізацію наслідків реалізованих загроз, кризових ситуацій та інших їх видів; |  |  |
| 5) створення системи раннього виявлення загроз критичній інфраструктурі; |  |  |
| 6) запровадження державно-приватного партнерства, суб’єктів господарювання та населення з питань забезпечення захисту та стійкості критичної інфраструктури; |  |  |
| 7) 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, ресурсних, інформаційно-аналітичних та методологічних  заходів, спрямованих на забезпечення безпеки критичної інфраструктури. |  |  |
| **Стаття 5. Мета та завдання державної політики у сфері захисту критичної інфраструктури** |  |  |
| 1. Метою державної політики у сфері захисту критичної інфраструктури є забезпечення безпеки об’єктів критичної інфраструктури, запобігання проявам несанкціонованого втручання в їх функціонування, прогнозування та запобігання кризовим ситуаціям на об’єктах критичної інфраструктури~~.~~ |  |  |
| 2. До завдань формування і реалізації державної політики захисту критичної інфраструктури належать: |  |  |
| 1. забезпечення безпеки та захисту критичної інфраструктури; |  |  |
| 1. попередження кризових ситуацій, що порушують безпеку критичної інфраструктури; |  |  |
| 1. створення, впровадження, розвиток та забезпечення функціонування національної системи захисту критичної інфраструктури, у тому числі шляхом створення Уповноваженого органу у сфері захисту критичної інфраструктури України, а також визначення повноважень у сфері захисту критичної інфраструктури інших суб’єктів національної системи захисту критичної інфраструктури; |  |  |
| 1. розроблення нормативно-правової та нормативно-технічної бази з питань забезпечення безпеки об’єктів критичної інфраструктури; |  |  |
| 1. розроблення та реалізація державних цільових програм із захисту критичної інфраструктури; |  |  |
| 1. розроблення комплексу заходів з виявлення, запобігання та ліквідації наслідків інцидентів на об’єктах критичної інфраструктури; |  |  |
| 1. 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; |  |  |
| 1. аналіз викликів та загроз, що впливають на стійкість критичної інфраструктури, оцінка стану її захищеності; |  |  |
| 1. розроблення методології аналізу результативності державної політики у сфері захисту критичної інфраструктури; |  |  |
| 1. підготовка, перепідготовка, підвищення кваліфікації, тренування співробітників державної системи захисту критичної інфраструктури |  |  |
| 1. забезпечення взаємодії національної системи захисту критичної інфраструктури з відповідними міжнародними системами, насамперед європейськими та євроатлантичними. |  |  |
|  |  |  |
| **Стаття 6. Основні принципи функціонування національної системи захисту критичної інфраструктури** |  |  |
| До основних принципів функціонування національної системи захисту критичної інфраструктури належать: |  |  |
| 1. єдність методологічних засад; |  |  |
| 1. координованість; |  |  |
| 1. державно-приватне партнерство; |  |  |
| 1. безпека, захист та охорона інформації з обмеженим доступом; |  |  |
| 1. міжнародне співробітництво. |  |  |
|  |  |  |
| **Стаття 7. Рівні управління національною системою захисту критичної інфраструктури** |  |  |
| 1. Національна система захисту критичної інфраструктури має 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; |  |  |
| 1. регіональний та галузевий рівень, управління на якому здійснюється органами державної влади та органами місцевого самоврядування (регіональні), які визначені у встановленому законодавством порядку відповідальними за формування та реалізацію публічної політики у сфері захисту критичної інфраструктури у окремому секторі критичної інфраструктури та відповідальними за функціонування окремих державних систем захисту та реагування; |  |  |
| 1. місцевий рівень, управління на якому здійснюється місцевими органами виконавчої влади (військово-цивільними адміністраціями - у разі створення), органами місцевого самоврядування в межах повноважень, покладених на них цим Законом; |  |  |
| 1. 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. Віднесення об’єктів до критичної інфраструктури здійснюється в порядку встановленому Кабінетом Міністрів України. |  |  |
| 2. Віднесення об’єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх (соціальну, політичну, економічну, екологічну, значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку), зокрема, 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. |  |  |
| 3. До таких критеріїв належать: |  |  |
| 1. виконання функцій із забезпечення життєво важливих національних інтересів; |  |  |
| 2. існування викликів і загроз, що можуть виникати щодо об’єктів критичної інфраструктури; |  |  |
| 3. ймовірність завдання значної шкоди нормальним умовам життєдіяльності населення; |  |  |
| 4. уразливість цих об’єктів, тяжкість можливих негативних наслідків, внаслідок чого буде заподіяна значна шкода: здоров’ю населення (визначається кількістю постраждалих, загиблих та осіб, які отримали значні травми, а також чисельністю евакуйованого населення); соціальній сфері (руйнація систем соціального захисту населення і надання соціальних послуг, втрата спроможності держави задовольнити критичні потреби суспільства); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного та місцевого значення; обороноздатності; іміджу країни; |  |  |
| 5. масштабність негативних наслідків для держави, які: впливають на діяльність стратегічно важливих об’єктів для кількох секторів життєзабезпечення чи призводять до втрати унікальних національно значущих активів, систем і ресурсів, матимуть тривалі наслідки для держави і позначається на діяльності ряду інших секторів; |  |  |
| 6. тривалість ліквідації таких наслідків та дія подальшого негативного впливу на інші сектори держави; |  |  |
| 7. вплив на функціонування суміжних секторів критичної інфраструктури. |  |  |
| **Стаття 9. Сектори критичної інфраструктури** |  |  |
| 1. Для організації ефективного забезпечення безпеки і стійкості критичної інфраструктури, з урахуванням специфіки забезпечення окремих життєво важливих функцій та послуг, визначаються сектори критичної інфраструктури. |  |  |
|  |  |  |
| 2. Для секторів критичної інфраструктури визначаються особливості реалізації публічної політики у сфері захисту критичної інфраструктури. Формування та реалізацію державної політики у відповідних секторах здійснюють секторальні органи у сфері захисту критичної інфраструктури. |  |  |
|  |  |  |
| 3. Перелік секторів критичної інфраструктури та суб’єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах національної системи захисту критичної інфраструктури, визначається Кабінетом Міністрів України виходячи з переліку життєво-важливих функцій визначеного цим Законом та іншими законами, що визначають повноваження секторальних органів. |  |  |
| У разі необхідності внесення змін до Переліку секторів критичної інфраструктури та суб’єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах національної системи захисту критичної інфраструктури, Кабінет Міністрів України переглядає цей Перелік та змінює його також виходячи з критеріїв критичності визначених цим законом. | У разі необхідності внесення змін до Переліку секторів критичної інфраструктури та суб’єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах національної системи захисту критичної інфраструктури, Кабінет Міністрів України переглядає цей Перелік та змінює його також виходячи з критеріїв критичності визначених цим законом.  **Перелік секторів критичної інфраструктури та суб’єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах національної системи захисту критичної інфраструктури підлягає перегляду Кабінетом Міністрів України не частіше одного разу на рік .**  **Внесення суб’єктів до Переліку секторів критичної інфраструктури та суб’єктів, відповідальних за формування та реалізацію державної політики у відповідних секторах національної системи захисту критичної інфраструктури відбувається, у тому числі, за ініціативи суб’єктів господарювання.** | Можливо необхідно встановити терміни періодичності перегляду критеріїв? Наприклад, 1 раз на рік (на 3 роки). |
|  |  |  |
| 4. До життєво важливих функцій порушення яких призводить до негативних наслідків для національної безпеки України відносяться, **~~зокрема:~~** | 4. До життєво важливих функцій порушення яких призводить до негативних наслідків для національної безпеки України відносяться: | Навести вичерпний перелік |
| 1. урядування та надання найважливіших публічних (адміністративних) послуг; |  |  |
| 1. енергозабезпечення ( в тому числі постачання теплової енергії); |  |  |
| 1. водопостачання та водовідведення; |  |  |
| 1. продовольче забезпечення; |  |  |
| 1. сільське господарство; |  |  |
| 1. охорона здоров’я; |  |  |
| 1. фармацевтична промисловість; |  |  |
| 1. виготовлення вакцин, стале функціонування біолабораторій; |  |  |
| 1. інформаційні та електронні комунікаційні послуги; | **Виключити.** | Поняття «інформаційні послуги» надзвичайно широке, формально під це поняття підпадає, наприклад, будь-яка консультація.  **Пропонуємо виключити, оскільки вказані послуги не передбачені** Директивою Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу.  **Також, звертаємо увагу, що функціонування системи зв’язку забезпечується НЦУ, а не через систему критичної інфраструктури.** |
| 1. електронні комунікації, зокрема мобільний зв'язок, радіозв'язок, супутниковий зв'язок та навігація; | 1. **забезпечення функціонування точок обміну трафіком (IXP), підтримка системи доменних імен (DNS) в Інтернеті, хмарні обчислення.** | **Включити лише ті послуги, що передбачені** Директивою Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. |
| 1. фінансові та банківські послуги; |  |  |
| 1. транспортне забезпечення; |  |  |
| 1. оборона; |  |  |
| 1. правопорядок, здійснення правосуддя, тримання під вартою; |  |  |
| 1. цивільний захист населення, служби порятунку; |  |  |
| 1. космічна діяльність, космічні технології та послуги; |  |  |
| 1. хімічна промисловість; |  |  |
| 1. дослідницька діяльність. |  |  |
|  |  |  |
| **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, в межах секторів критичної інфраструктури здійснюється категоризація об’єктів критичної інфраструктури відповідно до категорій критичності, визначених цим Законом. |  |  |
| 2. Категоризація об’єктів критичної інфраструктури здійснюється секторальними органами у сфері захисту критичної інфраструктури відповідно до секторальної специфіки та вимог секторального законодавства. |  |  |
| 3. Секторальні органи у сфері захисту критичної інфраструктури складають та ведуть секторальні переліки об’єктів критичної інфраструктури. |  |  |
| 4. Встановлюються такі категорії критичності об’єктів критичної інфраструктури: |  |  |
| I категорія критичності - особливо важливі об’єкти, які мають загальнодержавне значення, значний вплив на інші об’єкти критичної інфраструктури та порушення функціонування яких призведе до виникнення кризової ситуації національного значення; |  |  |
| II категорія критичності - життєво важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення; |  |  |
| III категорія критичності - важливі об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення; |  |  |
| IV категорія критичності - необхідні об’єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення. |  |  |
| 5. Секторальні органи разом з операторами основних послуг здійснюють категоризацію об’єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури відповідно до [Методики категоризації об’єктів критичної інфраструктури](https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#n45), яка затверджується Кабінетом Міністрів України. |  |  |
| **Стаття 11. Реєстр об’єктів критичної інфраструктури** |  |  |
| 1. Для цілей узгодження дій суб’єктів національної системи захисту критичної інфраструктури формується Реєстр об’єктів критичної інфраструктури. |  |  |
| 2. Збирання, узагальнення, попередній аналіз даних щодо об’єктів критичної інфраструктури та пропозиції щодо включення таких об’єктів до Реєстру об’єктів критичної інфраструктури в межах визначених секторів здійснюється секторальними органами у сфері захисту критичної інфраструктури. |  |  |
| 3. Реєстр об’єктів критичної інфраструктури формується та ведеться Уповноваженим органом у сфері захисту критичної інфраструктури на основі пропозицій суб’єктів національної системи захисту критичної інфраструктури. |  |  |
| 4. Після включення об’єкта до Реєстру об’єктів критичної інфраструктури секторальні органи у сфері захисту критичної інфраструктури повідомляють про це оператора об’єкта критичної інфраструктури для забезпечення його паспортизації та захисту об’єкта критичної інфраструктури відповідно до вимог цього Закону. |  |  |
| 5. Порядок ведення Реєстру об’єктів критичної інфраструктури, включення об’єктів до Реєстру, та надання інформації з нього визначається Кабінетом Міністрів України. |  |  |
| 6. Відомості, що містяться у Реєстрі об’єктів критичної інфраструктури, є інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом. |  |  |
|  |  |  |
| **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, 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 інформацію про ідентифікацію об’єкта та заходи щодо його захисту й безпеки, а також визначає перелік посад та відповідальних осіб, до завдань яких належить зв’язок та обмін інформацією з суб’єктами національної системи захисту критичної інфраструктури. |  |  |
| 3. Паспорт безпеки розробляється (переглядається) з урахуванням визначених національних та секторальних проектних ризиків та загроз. |  |  |
| Погодження паспорту безпеки на об’єкт критичної **інфраструктур** здійснюється безоплатно для усіх операторів об’єктів критичної інфраструктури незалежно від форми власності. | Інфраструктур**и** (ред.правка) | Редакційно |
| 4. **Порядок розроблення паспорта** безпеки на об’єкт критичної інфраструктури, його наповнення, зміст, порядок і строки подання встановлюються Кабінетом Міністрів України. | 4. Порядок розроблення паспорта безпеки на об’єкт критичної інфраструктури, його наповнення, зміст, порядок і строки подання, **його погодження та підстави для відмови у такому погодженні** встановлюються Кабінетом Міністрів України. | Має бути й порядок погодження, та підстави для відмови у такому погодженню, а не тільки розроблення. |
| Національним банком України з урахуванням вимог цього Закону визначається Порядок розроблення паспорта безпеки на об’єкти критичної інфраструктури, його наповнення, зміст і строки подання для банківської **системі** України, суб’єктів переказу коштів, страховими, лізингових та фінансових компаній, кредитним спілкам, ломбардів та бюро кредитних історій. | Систем**и** | Редакційно |
| 5. Оператор критичної інфраструктури несе відповідальність за достовірність даних, наведених у паспорті безпеки, своєчасність внесення до нього змін. |  |  |
| 6. Відомості, що містяться у паспорті безпеки є інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом. |  |  |
| **Розділ IV** |  |  |
| **НАЦІОНАЛЬНА 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 національної системи захисту критичної інфраструктури. |  |  |
| 2. Формування та реалізацію державної політики в окремих секторах критичної інфраструктури здійснюють секторальні та функціональні органи у сфері захисту критичної інфраструктури, відповідно до визначених законом повноважень. |  |  |
| 3. З метою формування і реалізації державної політики у сфері захисту критичної інфраструктури, координації діяльності суб’єктів національної системи захисту критичної інфраструктури створюється та функціонує Уповноважений орган у сфері захисту критичної інфраструктури України. |  |  |
| 4. Для забезпечення обміну інформацією та взаємодії суб’єктів національної системи захисту критичної інфраструктури Кабінет Міністрів України затверджує Регламент обміну інформацією. |  |  |
| 5. Обмін інформацією в рамках функціонування національної системи захисту критичної інфраструктури здійснюється відповідно до вимог законодавства у сфері захисту інформації. |  |  |
|  |  |  |
| **Стаття 14. Суб’єкти національної системи захисту критичної інфраструктури** |  |  |
| 1. Суб’єктами національної системи захисту критичної інфраструктури є: |  | Некоректний перелік державних органів, оскільки наприклад, для ЦВК та СБУ не передбачено повноважень у даній сфері ані чинним законодавством, ані цим Проектом Які функції та повноваження кожного суб’єкту? В даному випадку необхідно передбачити повноваження для кожного з них.  . |
| 1) Кабінет Міністрів України; |  |  |
| 2) Національний банк України; |  |  |
| 3) Центральна виборча комісія; | виключити | Оскільки, у проекті Закону не передбачено повноважень у даній сфері. |
| 4) Уповноважений орган у сфері захисту критичної інфраструктури України; |  |  |
| 5) секторальні та функціональні органи, інші міністерства та центральні органи виконавчої влади; |  |  |
| 6) Служба безпеки України; | виключити | Оскільки, у проекті Закону не передбачено повноважень у даній сфері. |
| 7) правоохоронні та розвідувальні органи; |  |  |
| 8) Збройні Сили України, інші військові формування, утворені відповідно до законів України; |  |  |
| 9) місцеві органи виконавчої влади (військово-цивільні адміністрації - у разі утворення); |  |  |
| 10) органи місцевого самоврядування. Забезпечення вимог законодавства щодо захисту критичної інфраструктури органами місцевого самоврядування відбувається відповідно до Закону України “Про органи місцевого самоврядування”; |  |  |
| 11) оператори критичної інфраструктури; |  |  |
| 12) підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки та стійкості критичної інфраструктури. |  |  |
|  |  |  |
| **Стаття 15. Режими функціонування національної системи захисту критичної інфраструктури** |  |  |
| 1. Забезпечення захисту та стійкості критичної інфраструктури здійснюється в таких режимах її функціонування: |  |  |
| 1) штатний режим — суб’єктами національної системи захисту критичної інфраструктури щодо оцінки можливих загроз та інформування щодо них. Функціонування інфраструктури здійснюється відповідно до проектного цільового призначення; |  |  |
| 2) режим готовності та запобігання реалізації загроз — секторальними та функціональними органами у сфері захисту критичної інфраструктури: проводиться перевірка та переведення системи захисту до готовності забезпечити захист та реагування на випадок реалізації загрози. Функціонування інфраструктури здійснюється відповідно до проектного цільового призначення; |  |  |
| 3) режим реагування на виникнення кризової ситуації — суб’єктами національної 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 національної 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 національної системи захисту, який погоджується з Уповноваженим органом у сфері захисту критичної інфраструктури. |  |  |
| 3. Рішення щодо оголошення режимів функціонування критичної інфраструктури приймається секторальними органами у сфері захисту критичної інфраструктури, відповідальним за сектор критичної інфраструктури. |  |  |
|  |  |  |
| **Стаття 16. Уповноважений орган у сфері захисту критичної інфраструктури** |  |  |
| 1. Уповноваженим органом у сфері захисту критичної інфраструктури є Національна комісія з питань захисту критичної інфраструктури центральний орган виконавчої влади зі спеціальним статусом, який забезпечує формування та реалізує державну політику у сфері захисту критичної інфраструктури, здійснює функціональне управління національною системою захисту критичної інфраструктури; забезпечує здійснення координації діяльності міністерств та операторів критичної інфраструктури з питань забезпечення захисту об’єктів критичної інфраструктури. |  |  |
| Діяльність Уповноваженого органу спрямовує, координує та контролює Міністр Кабінету Міністрів України. |  |  |
| 2. Уповноважений орган у сфері захисту критичної інфраструктури: |  |  |
| 1) координує діяльність міністерств, інших центральних та місцевих органів виконавчої влади (військово-цивільних адміністрацій – у разі утворення) у сфері захисту критичної інфраструктури; |  |  |
| 2) узагальнює пропозиції суб’єктів національної системи захисту критичної інфраструктури, формує та веде Реєстр об’єктів критичної інфраструктури; |  |  |
| 3) взаємодіє з секторальними, функціональними органами у сфері захисту критичної інфраструктури та операторами критичної інфраструктури з питань забезпечення захисту об’єктів, включених до Реєстру об’єктів критичної інфраструктури; |  |  |
| 4) здійснює оцінку захищеності об’єктів критичної інфраструктури, внесених до Реєстру об’єктів критичної інфраструктури; |  |  |
| 5) проводить із залученням секторальних та функціональних органів у сфері захисту критичної інфраструктури оцінку загроз критичній інфраструктурі на національному рівні та оцінку загроз національній безпеці внаслідок **реалізації загроз** критичній інфраструктурі; | 5) проводить із залученням секторальних та функціональних органів у сфері захисту критичної інфраструктури оцінку загроз критичній інфраструктурі на національному рівні та оцінку загроз національній безпеці внаслідок **завдання шкоди** критичній інфраструктурі; | Редакційно |
| 6) готує щорічну оцінку ризиків і загроз критичній інфраструктурі національного рівня; |  |  |
| 7) погоджує проектні ризики та 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; |  |  |
| 8) надає пропозиції Кабінету Міністрів України щодо: |  |  |
| Національного плану захисту та забезпечення стійкості критичної інфраструктури; |  |  |
| порядку розроблення, форми та змісту паспорту безпеки об’єкта критичної інфраструктури; |  |  |
| порядку розроблення, форми та змісту планів заходів щодо захисту критичної інфраструктури, які приймаються на державному рівні; |  |  |
| 9) розробляє та затверджує Проектні ризики та загрози критичній інфраструктурі національного рівня; |  |  |
| 10) готує висновки та рекомендації власнику/оператору критичної інфраструктури щодо зміни права власності, цільового призначення чи режиму функціонування об’єкта критичної інфраструктури; |  |  |
| 11) забезпечує функціонування системи обміну інформацією між суб’єктами національної системи захисту критичної інфраструктури; |  |  |
| 12) створює бази даних щодо загроз і уразливості об’єктів критичної інфраструктури; |  |  |
| 13) здійснює міжнародне співробітництво, забезпечує дотримання і виконання зобов’язань, узятих за міжнародними договорами України з питань захисту критичної інфраструктури, налагоджує і підтримує зв’язки з міжнародними організаціями, іноземними державами, їх правоохоронними органами і спеціальними службами; |  |  |
| 14) здійснює інші повноваження, передбачені цим Законом. |  |  |
| 3. Положення про Уповноважений орган у сфері захисту критичної інфраструктури затверджується Кабінетом Міністрів України. |  |  |
| **Стаття 17. Статус та система органів Національної комісії** |  |  |
| 1. Національна комісія є постійно діючим державним колегіальним органом, підпорядкованим і підзвітним Кабінету Міністрів України, здійснює свою діяльність самостійно, незалежно від будь-яких інших органів держави. |  |  |
| 2. Систему органів Національної комісії становлять Національна комісія як колегіальний орган та його апарат. |  |  |
| 3. Національна комісія як колегіальний орган утворюється у складі Голови Національної комісії та шести його членів, набуває повноважень з моменту призначення більше половини його загального кількісного складу. |  |  |
| 4. Структура та гранична чисельність працівників Національної комісії затверджується Головою Національної комісії з урахуванням видатків, передбачених у Державному бюджеті України. Штатний розпис апарату Національної комісії затверджується Головою Національної комісії за погодженням із Міністерством фінансів України. |  |  |
| 5. Голова та члени Національної комісії, працівники апарату Національної комісії є державними службовцями і мають відповідні службові повноваження відповідно до цього Закону та Закону України «Про державну службу». |  |  |
| **Стаття 18. Призначення, звільнення та термін повноважень керівництва Національної комісії** |  |  |
| 1. Голова та члени Національної комісії призначаються на посади та |  |  |
| звільняються з посад Кабінетом Міністрів України. |  |  |
| 2. Термін повноважень Голови та членів Національної комісії становить шість років. Одна й та ж особа не може бути Головою та/або членом Національної комісії більше двох термінів **підряд**. | 2. Термін повноважень Голови та членів Національної комісії становить шість років. Одна й та ж особа не може бути Головою та/або членом Національної комісії більше двох термінів **поспіль**. |  |
| 3. У разі відсутності Голови Національної комісії або неможливості здійснення ним своїх повноважень з інших причин його обов’язки та повноваження виконує член Комісії відповідно до встановленого Головою Національної комісії розподілу обов’язків та повноважень. |  |  |
| 4. Повноваження Голови та членів Національної комісії припиняються у разі: |  |  |
| 1) відмови Голови або члена Національної комісії від подальшого виконання обов’язків шляхом подання заяви про складення своїх повноважень; |  |  |
| 2) набрання законної сили обвинувальним вироком суду щодо Голови або члена Національної комісії; |  |  |
| 3) набрання законної сили рішенням суду про визнання особи, яка обіймає посаду Голови або члена Національної комісії, безвісно відсутньою або про оголошення її померлою; |  |  |
| 4) смерті особи, яка обіймає посаду Голови або члена Національної комісії. |  |  |
| Кабінет Міністрів приймає рішення про звільнення з посади Голови або члена Національної комісії до закінчення строку, на який його було обрано, у разі: |  |  |
| 1) порушення вимог щодо несумісності діяльності; |  |  |
| 2) засудження за умисне кримінальне правопорушення, вчинене з використанням свого посадового становища, або притягнення до відповідальності за вчинення адміністративного корупційного правопорушення, пов’язаного з порушенням обмежень, передбачених законодавством про запобігання і протидії корупції; |  |  |
| 3) припинення громадянства України; |  |  |
| 4) неспроможності протягом більше чотирьох місяців **підряд** виконувати обов’язки через незадовільний стан здоров’я чи втрату працездатності. | 4) неспроможності протягом більше чотирьох місяців **поспіль** виконувати обов’язки через незадовільний стан здоров’я чи втрату працездатності. |  |
| 5. Голова та члени Національної комісії набувають повноваження або припиняють їх з моменту набрання чинності рішенням Кабінету Міністрів України про їх призначення або звільнення. |  |  |
| **Стаття 19. Колегіальні рішення Національної комісії** |  |  |
| 1. Основною формою роботи Національної комісії як колегіального органу є засідання, які проводяться за рішенням Голови Національної комісії. |  |  |
| 2. Засідання Національної комісії є правомочним, якщо на ньому присутні більше половини її загального кількісного складу. |  |  |
| 3. Рішення Національної комісії приймаються більшістю голосів від її загального кількісного складу. Голова та член Національної комісії мають по одному голосу кожен. |  |  |
| 4. Рішення Національної комісії приймаються на засіданнях, які проводяться у формі відкритих або закритих слухань. У разі розгляду питань, що мають важливе суспільне значення, засідання проводяться у формі відкритих слухань, у яких мають право брати участь оператори критичної інфраструктури, представники функціональних та секторальнх орагнів, представники громадських об’єднань, засоби масової інформації. |  |  |
| 5. Перелік питань, з яких рішення приймаються колегіально, визначаються наказом Національної комісії. |  |  |
| 6. Рішення Національної комісії можуть бути оскаржені в установленому законодавством порядку. |  |  |
| 7. Рішення Національної комісії, які є нормативно-правовими актами, підлягають державній реєстрації в установленому законодавством порядку та не потребують узгодження з іншими органами державної влади, крім випадків, передбачених законом. |  |  |
| 8. Національна комісія веде реєстр всіх прийнятих рішень та забезпечує вільний доступ до них, крім рішень з обмеженим доступом, на своєму офіційному веб сайті у затвердженому ним порядку. |  |  |
| 9. Національна комісія щорічно подає Верховній Раді України звіт про свою діяльність. |  |  |
| **Стаття 20. Апарат Національної комісії** |  |  |
| 1. Організаційно-технічну та іншу роботу щодо забезпечення діяльності |  |  |
| Національної комісії як колегіального органу здійснює його апарат. Положення про апарат Національної комісії затверджує Голова Національної комісії. |  |  |
| 2. Апарат очолює керівник, який призначається на посаду та звільняється з посади Головою Національної комісії. Керівник апарату призначається на строк дії повноважень Голови Національної комісії та є підзвітним і підконтрольним безпосередньо Голові Національної комісії. Керівник апарату може мати не більше одного заступника. |  |  |
| 3. Обов’язки керівника апарату та його заступника визначаються Національною комісією. |  |  |
| **Стаття 21. Функціональні органи у сфері захисту критичної інфраструктури** |  |  |
| 1. Органи державної влади, які визначені відповідальними за функціонування окремих державних систем захисту та реагування: |  |  |
| беруть участь, у встановленому законодавством порядку, у реагуванні на кризові ситуації, пов’язані із забезпеченням безпеки та стійкості критичної інфраструктури; |  |  |
| готують пропозиції щодо включення об’єктів інфраструктури до Реєстру об’єктів критичної інфраструктури; |  |  |
| формують перелік об’єктів критичної інфраструктури, що належать до сфери їх управління; |  |  |
| надають секторальним органам у сфері захисту критичної інфраструктури, власникам та операторам інфраструктури консультації щодо загроз критичній інфраструктурі та заходів щодо їх нейтралізації; |  |  |
| здійснюють іншу діяльність для захисту критичної інфраструктури в межах повноважень, що регулюють діяльність суб’єктів захисту критичної інфраструктури, зокрема: |  |  |
| **організовує проведення** оцінки загроз та ризиків критичній інфраструктурі у відповідних сферах; |  |  |
| участь у проведенні оцінки загроз та ризиків критичній інфраструктурі на загальнодержавному рівні; |  |  |
| формування пропозицій до національних та секторальних проектних ризиків та загроз; |  |  |
| організацію взаємодії та обміну інформацією із іншими суб’єктами національної системи захисту критичної інфраструктури; |  |  |
| моніторинг рівня безпеки об’єктів критичної інфраструктури у відповідних сферах. |  |  |
| 2. До переліку окремих державних **та національних** систем захисту та реагування із якими національна система захисту критичної інфраструктури здійснює взаємодію та обмін інформацією входять: |  |  |
| 1. Єдина державна система цивільного захисту; |  |  |
| 2. Державна система фізичного захисту ядерних установок, ядерних матеріалів, радіоактивних відходів інших джерел іонізуючого випромінювання; |  |  |
| 3. Єдина державна система запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків; |  |  |
| 4. Національна система кібербезпеки; |  |  |
| 5. Сили безпеки (правоохоронні та розвідувальні органи, державні органи спеціального призначення з правоохоронними функціями, сили цивільного захисту та інші органи, на які Конституцією та законами України покладено функції із забезпечення національної безпеки України); |  |  |
| 6. Сили оборони – Збройні Сили України, а також інші утворені відповідно до законів України військові формування, правоохоронні та розвідувальні органи, органи спеціального призначення з правоохоронними функціями, на які Конституцією та законами України покладено функції із забезпечення оборони держави; |  |  |
|  |  |  |
| **Стаття 22. Особливості діяльності окремих органів на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури** |  |  |
| Діяльність Національного банку України, центрального органу виконавчої влади, який реалізує державну політику у сфері цивільного захисту, у сфері захисту критичної інфраструктури, Служби безпеки України, Національної гвардії України, Національної поліції України, Збройний сил України, Державної спеціальної служби транспорту та Державної служби спеціального зв’язку та захисту інформації України щодо (з питань) формування та/або реалізації державної політики у сфері захисту критичної інфраструктури здійснюється в рамках визначених цим Законом та у порядку, встановленому законами України, що регламентують правові засади організації та діяльності зазначених (перерахованих у цій статті) органів. |  |  |
|  |  |  |
| **Стаття 23. Секторальні органи у сфері захисту критичної інфраструктури** |  |  |
|  |  |  |
| 1. Державні органи, які визначені відповідальними за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури у окремому секторі критичної інфраструктури здійснюють наступні завдання: |  |  |
| 1. створюють у межах штатної чисельності у своєму складі структурні підрозділи з питань захисту критичної інфраструктури; |  |  |
| 1. збирають, узагальнюють та здійснюють попередній аналіз даних щодо критичної інфраструктури та її функціонування; |  |  |
| 1. спільно з операторами критичної інфраструктури здійснюють категоризацію об’єктів критичної інфраструктури своїх секторів критичної інфраструктури, формують секторальні переліки об’єктів критичної інфраструктури, подають інформацію до Реєстру об’єктів критичної інфраструктури; |  |  |
| 1. розробляють та затверджують: |  |  |
| а) вимоги до захисту об’єктів критичної інфраструктури відповідно до їх категорій; |  |  |
| б) проектні ризики і загрози критичній інфраструктурі секторального рівня; |  |  |
| в) плани взаємодії функціональних органів у сфері захисту критичної інфраструктури у відповідних секторах для всіх режимів функціонування критичної інфраструктури; плани взаємодії та підтримання життєво важливі функцій, на випадок порушення функціонування об’єктів критичної інфраструктури; |  |  |
| г) галузеві програми з протидії загрозам внутрішніх порушників, зокрема завдяки заходам, спрямованим на досягнення високого рівня культури безпеки (фізичної та технічної); |  |  |
|  |  |  |
| 1. затверджують: |  |  |
| а) Проектні ризики і загрози критичній інфраструктурі об’єктового рівня у відповідних секторах; |  |  |
| б) Паспорти безпеки об’єктів критичної інфраструктури, наданих операторами у відповідних секторах; |  |  |
| в) розробляють та впроваджують, норми і регламенти захисту критичної інфраструктури у відповідних секторах критичної інфраструктури; |  |  |
| 1. здійснюють: |  |  |
| а) перевірку та оцінку захищеності об’єктів критичної інфраструктури; |  |  |
| б) підготовку пропозицій до проектних ризиків та загроз критичній інфраструктурі національного рівня та щорічної оцінки ризиків і загроз критичній інфраструктури національного рівня; |  |  |
| в) організацію системи підготовки персоналу, навчання та тренувань щодо забезпечення стійкості та захисту секторів критичної інфраструктури. |  |  |
| г) підготовку щорічного звіту щодо забезпечення захисту критичної інфраструктури у відповідному секторі; | г)підготовку щорічного звіту щодо забезпечення захисту критичної інфраструктури у відповідному секторі **за встановленою Кабінетом Міністрів України формою;** | Необхідно передбачити форму звіту. |
| д) 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 стійкість критичної інфраструктури~~**; | д) подають операторам об’єктів критичної інфраструктури обов'язкові для розгляду пропозиції з питань захисту критичної інфраструктури; | Цим законом не врегульовано питання виконання цих вимог. Крім того, не зрозуміло та не передбачено які це саме можуть бути вимоги. |
| е) беруть участь, у встановленому законодавством порядку, в реагуванні на кризові ситуації, пов’язані з безпекою, захистом та стійкістю об’єктів критичної інфраструктури; |  |  |
| є) попередження про загрози операторів критичної інфраструктури та надають інформаційну, консультативну, експертну, методичну допомогу операторам критичної інфраструктури, користувачам їх послуг (населенню) задля попередження, реагування, мінімізації можливого впливу загроз; |  |  |
| 1. виконують: |  |  |
| а) збір, аналіз та узагальнення даних щодо об’єктів критичної інфраструктури та загроз їх функціонуванню; |  |  |
| б) функціонування відповідних систем обміну інформацією, моніторингу рівня безпеки об’єктів критичної інфраструктури; |  |  |
| в) організацію функціонування системи обміну інформацією та взаємодії у відповідних секторах критичної інфраструктури, між суб’єктами національної системи захисту критичної інфраструктури. |  |  |
| 8. Секторальні органи у сфері захисту критичної інфраструктури щорічно, відповідно до строків та форми звіту, затвердженої Кабінетом Міністрів України, подають інформацію Уповноваженому органу. |  |  |
| **Стаття 24. Місцеві органи виконавчої влади та військово-цивільні адміністрації** |  |  |
| 1. Місцеві органи виконавчої влади (військово-цивільні адміністрації - у разі утворення) у сфері захисту критичної інфраструктури забезпечують: |  |  |
| розробку та затвердження 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; |  |  |
| розробку, затвердження 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 25. 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, планів локалізації та ліквідації наслідків аварій, а також заходів кіберзахисту; |  |  |
| 3) проведення оцінки ризиків на об’єктах критичної інфраструктури та обмін інформацією про ризики та загрози з іншими суб’єктам національної системи захисту критичної інфраструктури; |  |  |
| 4) створення окремого структурного підрозділу або визначення відповідальної особи за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб’єктами національної 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 національної 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 Уповноваженого органу, органів Національної поліції України, Служби безпеки України, підрозділів Національної гвардії України, інших державних органів про інциденти, пов’язані з порушеннями систем фізичної безпеки та кібербезпеки; | 9) негайне інформування Уповноваженого органу, **~~органів Національної поліції України, Служби безпеки України, підрозділів Національної гвардії України, інших державних органів про інциденти,~~ пов’язані з порушеннями систем фізичної безпеки та кібербезпеки** **відповідно до встановленого Порядку Уповноваженим органом;** | Інформування повинно відбуватися за так званим «принципом єдиного вікна», яким може бути Уповноважений орган. А в свою чергу Уповноважений орган вже в порядку взаємодії може повідомляти інші державні органи. |
| 10) забезпечення постійного зв’язку з відповідальними за реагування та з іншими компетентними організаціями та установами; | Виключити | Не відповідає принципу юридичної визначеності. |
| 11) забезпечення постійної взаємодії з підприємствами, які забезпечують централізоване водопостачання, централізоване водовідведення, постачання теплової енергії, енергопостачання, функціонування телекомунікаційних мереж, транспорт, медичну допомогу, безпеку та численні інші послуги, від яких залежить процес реагування на кризові ситуації та відновлення функціонування об’єктів критичної інфраструктури; | 11) забезпечення постійної взаємодії з підприємствами, які забезпечують централізоване водопостачання, централізоване водовідведення, постачання теплової енергії, енергопостачання, **функціонування електронних комунікаційних мереж,** транспорт, медичну допомогу, безпеку та численні інші послуги, від яких залежить процес реагування на кризові ситуації та відновлення функціонування об’єктів критичної інфраструктури; | Редакційно |
| 12) створення і використання необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків; | виключити |  |
| 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 кібербезпеку, забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про об’єкти критичної інфраструктури; |  |  |
| 15) забезпечення захисту персоналу об’єктів критичної інфраструктури, організація та здійснення евакуаційних заходів у разі виникнення надзвичайних ситуацій. |  |  |
| 2. Оператори критичної інфраструктури забезпечують розробку та затвердження, у встановленому законодавством порядку: |  |  |
| 1) вимог щодо організації захисту об’єктів критичної інфраструктури; |  |  |
| 2) посадових інструкцій осіб, відповідальних за організацію та забезпечення захисту об’єктів критичної інфраструктури; |  |  |
| 3) проведення навчань та тренінгів, підготовку та перевірку персоналу, який відповідає за охорону, безпеку та захист об’єктів критичної інфраструктури; |  |  |
| 4) Паспортів безпеки об’єктів критичної інфраструктури. |  |  |
| 3. Оператори критичної інфраструктури мають право: |  |  |
| 1) отримувати в установленому порядку від уповноважених органів державної влади інформацію, що стосується забезпечення безпеки об’єктів критичної інфраструктури, що належать їм на праві власності або іншій законній підставі; |  |  |
| 2) самостійно розробляти заходи щодо забезпечення безпеки об'єктів критичної інфраструктури, що не суперечать вимогам цього Закону та прийнятих відповідно до нього нормативно-правових актів. |  |  |
| 4. Оператори критичної інфраструктури зобов’язані: |  |  |
| 1) забезпечити захист об’єктів критичної інфраструктури, що належать їм на праві власності або на іншій законній підставі; |  |  |
| 2) невідкладно поінформувати відповідальних суб’єктів національної системи захисту критичної інфраструктури (секторальні та функціональні органи) про інциденти, що сталися на об'єктах критичної інфраструктури, які належать їм на праві власності або іншій законній підставі; |  |  |
| 3) невідкладно поінформувати 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; |  |  |
| 4) щорічно надавати інформацію про виконання повноважень відповідно до цього Закону, за формою, визначеною Кабінетом Міністрів України; | Потребує деталізації! | Кому конкретно? Уповноваженому органу, секторальному чи кому? В які чіткі строки має надаватися інформація? |
| 5) виконувати вимоги цього Закону та інших нормативно-правових актів, які регулюють діяльність об'єктів критичної інфраструктури. |  |  |
|  |  |  |
| **Розділ V** |  |  |
| **ОРГАНІЗАЦІЙНІ ЗАСАДИ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ** |  |  |
| **Стаття 26. Планування заходів щодо забезпечення стійкості та захисту об’єктів критичної інфраструктури** |  |  |
| 1. Для організації функціонування національної системи захисту критичної інфраструктури Кабінетом Міністрів України, центральними органами виконавчої влади, місцевими органами виконавчої влади (військово-цивільними адміністраціями - у разі створення), органами місцевого самоврядування та затверджуються відповідні плани та програми реагування на кризові ситуації. |  |  |
| 2. На державному рівні розробляється Національний план захисту та забезпечення стійкості критичної інфраструктури, який затверджується Кабінетом Міністрів України. |  |  |
| 3. На секторальному (галузевому) та регіональному рівнях органи державної влади розробляють і затверджують галузеві, регіональні плани та програми з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани взаємодії, плани відновлення об’єктів критичної інфраструктури, плани проведення навчань та тренувань. |  |  |
| 4. Національна поліція України, Національна гвардія України, Служба безпеки України, Збройні Сили України, Державна служба України з питань надзвичайних ситуацій та інші складові сектору безпеки і оборони у межах компетенції здійснюють планування відповідних заходів із захисту критичної інфраструктури. |  |  |
| 5. На місцевому рівні: |  |  |
| Місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення), 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 національної системи захисту критичної інфраструктури, а також відновлення функціонування об’єктів критичної інфраструктури. |  |  |
| 6. На об’єктовому рівні: |  |  |
| оператори критичної інфраструктури на кожному об’єкті критичної інфраструктури розробляють та забезпечують виконання об’єктового плану заходів щодо захисту і забезпечення стійкості критичної інфраструктури, який включає заходи з фізичного захисту, протидії загрозам, забезпечення безпеки інформації та кібербезпеки на об’єктах критичної інфраструктури. |  |  |
| **Стаття 27. Здійснення моніторингу рівня безпеки об’єктів критичної інфраструктури** |  |  |
| 1. Моніторинг рівня безпеки об’єктів критичної інфраструктури здійснюється шляхом оцінки захищеності об’єктів критичної інфраструктури. Оцінка захищеності об’єктів критичної інфраструктури проводиться секторальними та функціональними органами у сфері захисту критичної інфраструктури, відповідно до їх повноважень визначених законом. |  |  |
| 2. Метою здійснення моніторингу є встановлення відповідності стану захищеності об’єкта критичної інфраструктури вимогам законодавства, достовірності наданої інформації визначеним суб’єктам національної системи захисту критичної інфраструктури, надання методичної допомоги операторам об’єктів критичної інфраструктури в удосконаленні системи захисту критичної інфраструктури. |  |  |
| 3. За результатами проведення моніторингу секторальними та функціональними органами у сфері захисту критичної інфраструктури готуються пропозиції щодо удосконалення системи захисту критичної інфраструктури. |  |  |
| 4. Порядок здійснення моніторингу рівня безпеки об’єктів критичної інфраструктури затверджується Кабінетом Міністрів України. | 4. Порядок, **періодичність та строк** здійснення моніторингу рівня безпеки об’єктів критичної інфраструктури затверджується **Кабінетом Міністрів України.** | Необхідно визначити строк та періодичність проведення моніторингу. |
|  |  |  |
| **Стаття 28. Взаємодія національної 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 національна 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; |  |  |
| 2) з національною системою захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах; |  |  |
| 3) з національною системою кібербезпеки; |  |  |
| 4) з правоохоронними органами у сфері протидії злочинності; |  |  |
| 5) з об’єднаною цивільно-військовою системою організації повітряного руху України; |  |  |
| 6) з єдиною державною системою цивільного захисту; |  |  |
| 7) з державною системою фізичного захисту з питань охорони і оборони важливих державних об’єктів, захищеності та охорони ядерних установок, ядерних матеріалів, радіоактивних відходів, інших джерел іонізуючого випромінювання державної власності, запобігання диверсіям, крадіжкам або будь-якому іншому неправомірному вилученню радіоактивних матеріалів, протидії незаконному використанню безпілотних літальних апаратів; |  |  |
| 8) із системою захисту персональних даних. |  |  |
| 2. Взаємодія між державними системами захисту здійснюється у разі загрози виникнення або виникнення: |  |  |
| 1) протиправних дій (у тому числі із застосуванням безпілотних літальних апаратів), 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 національної 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, Державної служби України з питань надзвичайних ситуацій 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, інцидентів та кібератак проти об’єктів критичної інформаційної 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 29. Державно-приватне партнерство у сфері захисту критичної інфраструктури** |  |  |
| 1. Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється шляхом: | 1. Державно-приватне партнерство у сфері захисту критичної інфраструктури **може здійснюватися** шляхом: |  |
| 1. обміну інформацією між державними органами, місцевими органами виконавчої влади (військово-цивільними адміністраціями – у разі утворення), органами місцевого самоврядування, операторами критичної інфраструктури, громадськими об’єднаннями, організаціями роботодавців, а також громадянами щодо загроз критичній інфраструктурі та реагування на кризові ситуації; | обміну інформацією між державними органами, місцевими органами виконавчої влади (військово-цивільними адміністраціями – у разі утворення), органами місцевого самоврядування, операторами критичної інфраструктури, громадськими об’єднаннями, **об’єднаннями підприємств,** організаціями роботодавців, а також громадянами щодо загроз критичній інфраструктурі та реагування на кризові ситуації; |  |
| 1. визначення повноважень та відповідальності державних органів й операторів критичної інфраструктури у сфері забезпечення безпеки та стійкості критичної інфраструктури; |  |  |
| 1. визначення порядку взаємодії між державними органами та операторами критичної інфраструктури у різних режимах функціонування об’єктів критичної інфраструктури; |  |  |
| 1. створення системи підготовки кадрів у сфері захисту критичної інфраструктури; |  |  |
| 1. 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; |  |  |
| 1. залучення експертного потенціалу наукових установ, професійних та громадських об’єднань до підготовки галузевих проектів та нормативно-правових актів у сфері захисту критичної інфраструктури; |  |  |
| 1. 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; |  |  |
| 1. надання державними органами консультативної та практичної допомоги операторам критичної інфраструктури з питань реагування на кризові ситуації на об’єктах критичної інфраструктури; |  |  |
| 1. організації забезпечення захисту персоналу об’єктів критичної інфраструктури від можливих загроз; |  |  |
| 1. забезпечення резервування основних ресурсів для функціонування критичної інфраструктури у різних режимах; | **Виключити** | Резервування – це додаткове навантаження на операторів. В чому партнерство з Державою?  Крім того, проектом не визначено порядок та об’єми такого резервування. |
| 1. організації системи оповіщення населення та суб’єктів господарювання про інциденти та кризові ситуації на об’єктах критичної інфраструктури; |  |  |
| 1. створення системи самооцінки віднесення об’єктів критичної інфраструктури за критеріями, визначеними цим Законом, створення інформаційних ресурсів для підвищення рівня знань із захисту об’єктів критичної інфраструктури; |  |  |
| 1. створення механізмів для саморегулювання, обміну інформацією між операторами об’єктів критичної інфраструктури у певному секторі; |  |  |
| 1. підтримки розвитку систем сертифікації та оцінки відповідності у секторах критичної інфраструктури; | **виключити** | З реакції положення не зрозуміло сертифікації чого саме передбачається. |
| 1. створення сприятливих умов для запровадження системи добровільного страхування від потенційних ризиків і загроз для об’єктів критичної інфраструктури. |  |  |
| 2. Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об’єктів критичної інфраструктури та окремих видів діяльності. |  |  |
| 3. З метою забезпечення ефективної взаємодії представників громадськості, органів виконавчої влади та реального сектору економіки у формуванні та реалізації єдиної державної політики у сферах забезпечення захисту національних інтересів України у кіберпросторі та захисту об'єктів критичної інфраструктури створюються консультативно-дорадчі органи, об’єднання та мережі. |  |  |
|  |  |  |
|  |  |  |
| **Стаття 30. Проведення незалежного аудиту діяльності національної системи захисту критичної інфраструктури** |  |  |
|  |  |  |
| 1. Незалежна зовнішня оцінка діяльності Уповноваженого органу у сфері захисту критичної інфраструктури здійснюється шляхом проведення щорічного зовнішнього аудиту його діяльності. Зовнішній аудит діяльності Уповноваженого органу проводиться Рахунковою палатою України. |  |  |
|  |  |  |
| 2. Незалежна зовнішня оцінка діяльності системи захисту критичної інфраструктури здійснюється один раз на три роки Рахунковою палатою України у визначеному нею порядку, на підставі міжнародних стандартів оцінки | виключити | Оцінка діяльності *системи захисту* Рахунковою палатою?  Під нагляд Рахункової палати підпадають в тому числі і приватні суб’єкти господарювання. |
|  |  |  |
| 3. Форма та зміст звіту про зовнішній аудит діяльності Уповноваженого органу затверджуються Кабінетом Міністрів України з урахуванням вимог цього Закону. |  |  |
|  |  |  |
| 4. Відшкодування витрат, пов’язаних із проведенням щорічного зовнішнього аудиту, здійснюється за рахунок Державного бюджету України. |  |  |
|  |  |  |
| **Стаття 31. Парламентський контроль у сфері захисту критичної інфраструктури** |  |  |
|  |  |  |
| 1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення у сфері захисту критичної інфраструктури здійснюється Верховною Радою України в порядку, визначеному Конституцією України. Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та Комітет Верховної Ради України, до предмета відання якого належать питання кібербезпеки об’єктів критичної інформаційної інфраструктури, на своїх засіданнях розглядають звіт Уповноваженого органу у сфері захисту критичної інфраструктури про результати незалежного аудиту діяльності щодо ефективності системи забезпечення захисту критичної інфраструктури. |  |  |
| 2. За результатами розгляду звіту Уповноваженого органу, Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, може порушити питання про розгляд цих питань Верховною Радою України. |  |  |
|  |  |  |
|  |  |  |
| **Стаття 32. Громадський контроль у сфері захисту критичної інфраструктури** |  |  |
|  |  |  |
| 1. Право громадського контролю у сфері захисту критичної інфраструктури реалізується громадянами України через громадські об’єднання, членами яких вони є, через депутатів місцевих рад, особисто шляхом звернення до Уповноваженого Верховної Ради України з прав людини або до державних органів у порядку, встановленому Конституцією України, Законом України "Про громадські об’єднання" та іншими законами України; участі у діяльності громадських радах при органах, що формують та забезпечують реалізацію державної політики у сфері забезпечення захисту критичної інфраструктури, проведення незалежного аудиту їх діяльності; права доступу до публічної частини звіту щодо забезпечення захисту об’єктів критичної інфраструктури. |  |  |
| Сфера громадського контролю може бути обмежена виключно Законами України "Про державну таємницю", “Про інформацію”. |  |  |
| **Стаття 33. Відповідальність за порушення законодавства у сфері захисту критичної інфраструктури** |  |  |
| 1. Центральні та місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення), інші державні органи, органи місцевого самоврядування, територіальні громади, їхні посадові і службові особи, оператори об’єктів критичної інфраструктури, винні у порушенні законодавства у сфері захисту критичної інфраструктури, несуть відповідальність згідно із законом. |  |  |
| 2. У разі **у** порушення законодавства у сфері захисту критичної інфраструктури, до суб'єктів перерахованих у частині першій цієї статті, можуть бути застосовані такі адміністративно-господарські санкції: | «у» - видалити | Редакційно |
| адміністративно-господарський штраф; |  | Потрібно передбачити порядок та чітку санкцію.  Проте, у цьому проекті це не передбачено.  Конкретизувати перелік порушень та міру відповідальності цим Законом та/або КупАП. |
| стягнення зборів (обов'язкових платежів); | Виключити | Застосовується у випадку порушення податкового законодавства. Як це пов’язано з порушенням порушення законодавства у сфері захисту критичної інфраструктури?  Крім того, не зрозуміло як буде використовуватись частина 2 на практиці. Мова йде про господарські договори?  Прохання роз’яснити або виключити, оскільки реальні штрафи передбачено у частині 3 і частина 2 не потрібна. |
| обмеження або зупинення діяльності суб'єкта господарювання. | виключити |  |
| 3. У разі порушення законодавства у сфері захисту критичної інфраструктури, що містить ознаки адміністративного правопорушення та/ або суспільно небезпечного діяння, яке містить склад кримінального правопорушення, такі особи мають бути притягнуті до відповідальності відповідно до законодавства України про кримінальну відповідальність, та/або до законодавства України про адміністративні правопорушення. |  | Виключити, або передбачити зміни до Кодексів окремим проектом який повинен бути поданий пакетом. |
|  |  |  |
| **Стаття 34. Фінансування заходів у сфері захисту критичної інфраструктури** |  |  |
| 1. Джерелами фінансування робіт і заходів із забезпечення захисту критичної інфраструктури є кошти державного і місцевих бюджетів, власні кошти суб’єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством. |  |  |
| **Стаття 35. Міжнародне співробітництво у сфері захисту критичної інфраструктури** |  |  |
| 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. |  |  |
| 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”. |  |  |
| Відповідно до законодавства України у сфері зовнішніх зносин суб’єкти національної системи захисту критичної інфраструктури у межах своїх повноважень можуть здійснювати міжнародну співпрацю безпосередньо на двосторонній або багатосторонній основі. |  |  |
| **Стаття 36. Страхування ризиків** |  |  |
| 1. Власники та/або керівники підприємств, установ та організацій, віднесених до об’єктів критичної інфраструктури забезпечують страхування ризику фінансових втрати, викликаних кризовою ситуацією відповідно до Закону України «Про страхування». | 1. Власники та/або керівники підприємств, установ та організацій, віднесених до об’єктів критичної інфраструктури забезпечують **добровільне** страхування ризику фінансових втрати, викликаних кризовою ситуацією відповідно до Закону України «Про страхування». |  |
| 2. Перелік об’єктів критичної інфраструктури, страхових ризиків, щодо яких здійснюється обов'язкове державне страхування ризику фінансових втрати, викликаних кризовою ситуацією, затверджується Кабінетом Міністрів України. |  |  |
| **Розділ VI** |  |  |
| **ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ** |  |  |
|  |  |  |
| 1. Цей Закон набирає чинності з дня, наступного за днем його опублікування та вводиться в дію через шість місяців з дня набрання ним чинності. |  |  |
| Через 3 роки з дня набрання чинності цим Законом набувають чинності положення: |  |  |
| про обов'язкове страхування об’єктів критичної інфраструктури, - частина друга статті 36 та абзац другий підпункту 20 пункту 2 цього Закон, |  |  |
| про запровадження адміністративно-господарської відповідальності у разі у порушення законодавства у сфері захисту критичної інфраструктури, - частина друга статті 33 цього Закону. |  |  |
| До приведення у відповідність із цим Законом законодавчі та інші нормативно-правові акти застосовуються в частині, що не суперечить цьому Закону. |  |  |
| 2. Внести до законів України такі зміни: |  |  |
| 1. **абзац четвертий частини першої статті 5 Закону України “Про оперативно- розшукову діяльність”** (Відомості Верховної Ради України, 1992 р., № 22, ст. 303 із наступними змінами) викласти в такій редакції: | **виключити** | **Виключити. Не предмет даного Проекту** |
| “Служби безпеки України – оперативними підрозділами Центрального управління та регіональних органів”; |  |  |
| 2) **пункт 2 частини першої статті 6 Закону України “Про контррозвідувальну діяльність”** (Відомості Верховної Ради України, 2003 р., № 12, ст. 89) після абзацу третього доповнити новим абзацом четвертим такого змісту: |  |  |
| “контррозвідувального захисту критичної інфраструктури;”. |  |  |
| У зв’язку з цим абзаци четвертий — сьомий вважати відповідно абзацами п’ятим — восьмим; |  |  |
| 3) **у Законі України “Про інформацію”** (Відомості Верховної Ради України, 2011 р., № 32, ст. 313; 2015 р., № 26, ст. 29; 2016 р., № 28, ст. 533; 2017 р., № 2, ст. 25; 2019 р., № 21, ст. 81; 2020 р., № 11, ст. 63): |  |  |
| статтю 10 після абзацу десятого доповнити новим абзацом одинадцятим такого змісту: |  |  |
| “критична технологічна інформація;”. |  |  |
| У зв’язку з цим абзац одинадцятий вважати абзацом дванадцятим; доповнити Закон статтею 19-1 такого змісту: |  |  |
| “Стаття 19-1. Критична технологічна інформація |  |  |
| Критична технологічна інформація — дані, що обробляються (приймаються, передаються, зберігаються) в системах управління технологічними процесами об’єктів критичної інфраструктури. |  |  |
| Правовий режим критичної технологічної інформації визначається законами та міжнародними договорами України, згода на обов’язковість яких надана Верховною Радою України. |  |  |
| Критична технологічна інформація за режимом доступу належить до інформації з обмеженим доступом та підлягає захисту згідно із законом.”; |  |  |
| 4) **пункт 5 частини першої статті 20 Закону України “Про Кабінет Міністрів України”** (Відомості Верховної Ради України, 2014 р., № 13, ст. 222) після абзацу сьомого доповнити новим абзацом такого змісту: |  |  |
| “забезпечує проведення державної політики у сфері захисту критичної інфраструктури України;”. |  |  |
| У зв’язку з цим абзаци восьмий і дев’ятий вважати відповідно абзацами дев’ятим і десятим; |  |  |
| **5) частину другу статті 6 Закону України “Про охоронну діяльність”** (Відомості Верховної Ради України, 2013 р., № 2, ст. 8) викласти в такій редакції: |  |  |
| “Перелік об’єктів критичної інфраструктури, охорона яких здійснюється державними органами, підприємствами та організаціями, затверджується Кабінетом Міністрів України.”; |  |  |
| **6) у Законі України “Про правовий режим воєнного стану”** (Відомості Верховної Ради України, 2015 р., № 28, ст. 250): |  |  |
| частину першу, абзаци перший та другий частини сьомої, друге речення частини восьмої статті 4 після слів «громадського порядку і безпеки» доповнити словами “захисту критичної інфраструктури»; |  |  |
| у частині першій статті 8: |  |  |
| у першому реченні пункту 1 слова «важливих об’єктів національної економіки» та другому реченні слова «об’єктів національної економіки» замінити словами |  |  |
| «важливих державних об’єктів національної економіки, об’єктів критичної інфраструктури» відповідно; |  |  |
| у першому реченні пункту 2 слова «та сфері забезпечення життєдіяльності населення» і «та системи забезпечення життєдіяльності населення» замінити словами |  |  |
| «, сфері забезпечення життєдіяльності населення та захисту критичної інфраструктури» і «, системи забезпечення життєдіяльності населення та захисту критичної інфраструктури» відповідно; |  |  |
| пункт 9 після слів «посягання на» доповнити словами «стійкість критичної інфраструктури,»; |  |  |
| у статті 15: |  |  |
| частину першу після слів «Про мобілізаційну підготовку та мобілізацію» доповнити словами «Про критичну інфраструктуру»; |  |  |
| у пункті 25 частини другої слова «об’єктів національної економіки» замінити словами «важливих державних об’єктів національної економіки, об’єктів критичної інфраструктури»; |  |  |
| у пункті 7 частини третьої слова «важливих об’єктів національної економіки» замінити словами «важливих державних об’єктів національної економіки, об’єктів критичної інфраструктури»; |  |  |
| **7) У Законі України “Про правовий режим надзвичайного стану”** (Відомості Верховної Ради України, 2000, № 23, ст.176): |  |  |
| у пункті 3 статті 16 слова «об’єктів, що забезпечують життєдіяльність населення та народного господарства» замінити словами «важливих об’єктів національної економіки та об’єктів критичної інфраструктури»; |  |  |
| **8) У Законі України “Про оборону” (**Відомості Верховної Ради України (ВВР), 1992, № 9, ст.106): |  |  |
| у частині першій статті 3: |  |  |
| у абзаці десятому після слів «єдиної державної системи цивільного захисту» додати слова «та національної системи захисту критичної інфраструктури»; |  |  |
| у абзаці тринадцятому після слів «підготовку національної економіки» додати слова «національної системи захисту критичної інфраструктури»; |  |  |
|  |  |  |
| у абзаці сьомому частини першої статті 9 слова «живучості об’єктів національної економіки та державного управління» замінити словами «живучості важливих об’єктів національної економіки, об’єктів критичної інфраструктури та державного управління»; |  |  |
|  |  |  |
| у абзаці третьому частини першої статті 13 слова «інших об'єктів інфраструктури» замінити на слова «інших об’єктів критичної інфраструктури». |  |  |
|  |  |  |
| **9) у Законі України "Про Збройні Сили України"** (Відомості Верховної Ради України, 2000 р., № 48, ст. 410 із наступними змінами): |  |  |
|  |  |  |
| у статті 1: |  |  |
|  |  |  |
| у частині четвертій: |  |  |
|  |  |  |
| після слів “до здійснення заходів правового режиму воєнного і надзвичайного стану,” доповнити словами “безпеки та захисту критичної інфраструктури,” |  |  |
| після слів “ліквідації надзвичайних ситуацій природного і техногенного характеру, ” доповнити словами “кризових ситуацій”; |  |  |
|  |  |  |
| після частини четвертої доповнити новою частиною п'ятою такого змісту: |  |  |
| “Збройні Сили України у сфері захисту критичної інфраструктури забезпечують організацію захисту військових об’єктів критичної інфраструктури Збройних Сил України від терористичних загроз, підготовку до застосування військ (сил) Збройних Сил України, у разі вчинення терористичного акту в повітряному просторі або територіальному морі України; проведення заходів з підвищення рівня захищеності, усунення ризиків і загроз вибухопожежобезпеки арсеналів, баз та складів Збройних Сил України; виконання завдань з протиповітряного прикриття важливих об’єктів держави (критичної інфраструктури), перелік яких визначається Кабінетом Міністрів України.” |  |  |
| У зв'язку з цим частини п'яту - дев'яту, вважати частинами шостою - десятою; |  |  |
| **10) Статтю 7 Закону України "Про Національний банк України" (Відомості Верховної Ради України, 1999 р., № 29, ст. 238 із наступними змінами)** після пункту 35 доповнити новим пунктом такого змісту: |  |  |
| “36) здійснює формування та реалізацію державної політику у сфері захисту критичної інфраструктури щодо надання фінансових та банківських послуг установами та організаціями регулювання та нагляд за якими здійснює Національний банк та є секторальним органом у цій сфері; застосовує заходи впливу, у разі порушення банками, іншими установами та організаціями, регулювання та нагляд за діяльністю яких здійснює Національний банк, законодавства з питань захисту критичної інфраструктури, кіберзахисту та інформаційної безпеки; щорічно подає інформацію щодо забезпечення захисту критичної інфраструктури у власному секторі Уповноваженому органу, відповідно до строків та форми звіту погодженому з ним.»; |  |  |
| **11) у Законі України “Про основні засади забезпечення кібербезпеки України”** (Відомості Верховної Ради України, 2017 р., № 45, ст.403): |  |  |
| у статті 1: |  |  |
| пункт 16 виключити; |  |  |
| частину другу доповнити реченням такого змісту : |  |  |
| “Термін “об’єкт критичної інфраструктури” вживаються в цьому Законі у значенні, визначеному Законом України “Про критичну інфраструктуру”; |  |  |
| у статті 6: |  |  |
| частину першу виключити; |  |  |
| частину другу викласти у такій редакції: |  |  |
| “2. Віднесення об’єктів до об’єктів критичної інфраструктури та формування Реєстру об’єктів критичної інфраструктури здійснюється відповідно до Закону України “Про критичну інфраструктуру.”; |  |  |
| **12) у частині першій статті 23 Закону України "Про Національну поліцію" (Відомості Верховної Ради України, 2015 р., № 40-41, ст. 379; 2018 р., № 48, ст. 380):** |  |  |
| пункт 20 після слів “комунальної власності” доповнити словами “об’єктів критичної інфраструктури, перелік яких визначаються Кабінетом Міністрів України;”; |  |  |
| після пункту 24 доповнити новим пунктом 241  у такій редакції: |  |  |
| **“**241) здійснює у визначеному законом порядку протидію злочинним посяганням на об’єкти критичної інфраструктури, які загрожують безпеці громадян і порушують функціонування систем життєзабезпечення; захист об’єктів критичної інфраструктури, інтересів суспільства і держави від злочинних посягань у кіберпросторі, здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів проти об’єктів критичної інфраструктури;”. |  |  |
| **13) у частині першій статті 2 Закону України “Про Національну гвардію України”** (Відомості Верховної Ради України, 2014 р., № 17, ст. 594) після пункту 5 доповнити новим пунктом 51  у такій редакції: |  |  |
| 51) охорона об’єктів критичної інфраструктури, перелік яких визначається Кабінетом Міністрів України. Участь у ліквідації наслідків кризових ситуацій на об’єктах критичної інфраструктури, що нею охороняються; |  |  |
|  |  |  |
| **14) у Законі України "Про Службу безпеки України"** (Відомості Верховної Ради України, 1992 р., № 27, ст. 382 із наступними змінами): |  |  |
| частину другу статті 2 після слів “у сфері управління і економіки” доповнити словами “, критичної інфраструктури”; |  |  |
| у пункті 11 статті 24 після слів “їх оголошення” доповнити словами “безпеку та захисту критичної інфраструктури,”, а після слів “стихійного лиха” доповнити словами “кризових ситуацій”; |  |  |
| **15) У Кодексі цивільного захисту України** (Відомості Верховної Ради України, 2013 р., № 34-35, ст. 458): |  |  |
| доповнити частину другу статті 17 після пункту 53 новими пунктами такого змісту: |  |  |
| 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; |  |  |
| реалізує заходи державної політики у сфері захисту критичної інфраструктури щодо впровадження інженерно-технічних заходів цивільного захисту на об’єктах критичної інфраструктури; |  |  |
| бере участь у межах компетенції в оцінці захищеності об’єктів критичної інфраструктури; |  |  |
| 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; |  |  |
| 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;”. |  |  |
| У зв'язку з цим з пункту 54 вважати пунтом 59; |  |  |
| **16) У Законі України "Про Державну службу спеціального зв’язку та захисту інформації України"** (Відомості Верховної Ради України, 2014 р., № 25, ст. 890; 2017 р., № 45, ст. 403): |  |  |
| у частині першій статті 3: |  |  |
| у абзаці третьому після слів “довірчих послуг)” доповнити словами “захисту критичної **інформаційної** інфраструктури”; |  |  |
|  |  |  |
| доповнити після абзацу четвертого новими абзацами такого змісту: |  |  |
| реалізує державну політику щодо захисту критичної технологічної інформації, кіберзахисту об’єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; |  |  |
| визначає вимоги до захисту критичної технологічної інформації, формує загальні вимоги до кіберзахисту об’єктів критичної інфраструктури, веде перелік об’єктів критичної інформаційної інфраструктури, здійснює заходи щодо його оновлення та актуалізації; |  |  |
| здійснює інші завдання, передбачені законодавством у сфері забезпечення кібербезпеки та кіберзахисту.”; |  |  |
|  |  |  |
| **17) у статті 38 Закону України “Про місцеве самоврядування в Україні”** (Відомості Верховної Ради України, 1997 р., № 24, ст. 170) пункт «б» частини першої доповнити пунктом 21 такого змісту: |  |  |
| «21) забезпечення вимог законодавства щодо захисту критичної інфраструктури, відновлення функціонування важливих державних об’єктів національної економіки, об’єктів критичної інфраструктури та об’єктів, які забезпечують життєдіяльність населення, підвищення стійкості громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій, взаємодії між суб’єктами державної системи захисту критичної інфраструктури з урахуванням вимог Закону України “Про критичну інфраструктуру”.»; |  |  |
|  |  |  |
| **18) абзаци четвертий та п'ятий частини четвертої статті 8 Закону України “Про захист інформації в інформаційно-телекомунікаційних системах”** (Відомості Верховної Ради України, 2005 р., № 26, ст. 347; 2014 р., № 22, ст. 816) викласти у такій редакції: |  |  |
| “Жоден з елементів системи не може бути розташований, а власник такої системи або його офіційний представник не може бути юридичною особою (його представником), зареєстрованою на територіях України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України “Про санкції”, та на територіях держав, які входять до митних союзів з такими державами. |  |  |
| Власник системи або його представник, які надають послуги з використанням системи, елементи якої розміщуються поза межами України, має бути юридичною особою, зареєстрованою в Україні, або мати свого офіційного представника в Україні. |  |  |
| Виконання особливих вимог, встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, що обробляються.”; |  |  |
| **19) статтю 25 Закону України “Про місцеві державні адміністрації” (Відомості Верховної Ради України, 1999 р., № 20-21, ст.190) доповнити пунктом 24 такого змісту:** |  |  |
| «24) забезпечення вимог законодавства щодо захисту критичної інфраструктури, відновлення функціонування важливих державних об’єктів національної економіки, об’єктів критичної інфраструктури та об’єктів, які забезпечують життєдіяльність населення, підвищення стійкості громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій, взаємодії між суб’єктами державної системи захисту критичної інфраструктури.». |  |  |
| **20) У Законі України "Про страхування"** (Відомості Верховної Ради України, 2002 р., № 7, ст. 50 із наступними змінами) : |  |  |
| частину четверту статті 6 після пункту 22 доповнити новим пунктом такого змісту: |  |  |
| “22-1) страхування ризику фінансових втрат, викликаних кризовою ситуацією на об’єкті критичної інфраструктури; ”; |  |  |
| частину першу статті 7 після пункту 49 доповнити новим пунктом 50 такого змісту: |  |  |
| «50) страхування ризику фінансових втрат, викликаних кризовою ситуацією на об’єкті критичної інфраструктури віднесеному до Переліку, що затверджується Кабінетом Міністрів України відповідно до Закону України “Про критичну інфраструктуру”; |  |  |
| 21)  **Абзац перший частини першої статті 73 Закону України “Про банки і банківську діяльність”** (Відомості Верховної Ради України, 2001 р., № 5-6, ст. 30 із наступними змінами) після слів “масового знищення,” доповнити словами “законодавства з питань захисту критичної інфраструктури, кіберзахисту та інформаційної безпеки,”. |  |  |
| 3. Кабінету Міністрів України у тримісячний строк з дня набрання чинності цим Законом: |  |  |
| забезпечити прийняття нормативно-правових актів, необхідних для реалізації цього Закону; |  |  |
| привести власні нормативно-правові акти у відповідність із цим Законом; |  |  |
| забезпечити приведення міністерствами, іншими центральними і місцевими органами виконавчої влади (військово-цивільними адміністраціями – у разі утворення) їх нормативно-правових актів у відповідність із цим Законом; |  |  |
| створити Національну комісію з питань захисту критичної інфраструктури; |  |  |
| забезпечити проведення конкурсу з відбору Голови та членів Національної комісії з питань захисту критичної інфраструктури, у порядку, визначеному Законом України “Про державну службу” до введення його в дію. |  |  |
| 3. Перша щорічна незалежна зовнішня оцінка діяльності Уповноваженого органу у сфері захисту критичної інфраструктури має бути проведення після першого повного календарного року його діяльності починаючи відлік часу з календарного року, у якому Уповноважений орган приступив до здійснення власних повноважень. |  |  |
| Перша незалежна зовнішня оцінка діяльності системи захисту критичної інфраструктури має бути проведення після спливу перших трьох календарних років діяльності Уповноваженого органу у сфері захисту критичної інфраструктури. |  |  |
| 4. Кабінет Міністрів щорічно починаючи з наступного дня за днем набрання чинності цим Законом, забезпечити перегляд нормативно -правових акти у сфері захисту об'єктів критичної інфраструктури та кіберзахисту за результатами проведених науково-дослідних робіт, щодо впливу новітніх і проривних технологій на формування нових індикаторів потенційних та ризиків загроз об'єктам критичної інфраструктури та кібербезпеці, надавати відповідні рекомендації. |  |  |