ЗАКОН УКРАЇНИ

Про критичну інфраструктуру

Цей Закон визначає правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури і є складовою законодавства у сфері національної безпеки.

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення основних термінів

1. У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) безпека критичної інфраструктури – стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури;

2) життєво важливі функції та/або послуги – функції та/або послуги, реалізація яких забезпечується органами державної влади, органами місцевого самоврядування, установами, суб'єктами господарювання та організаціями будь-якої форми власності, збої, переривання та порушення надання яких призводять до швидких негативних наслідків для національної безпеки;

3) захист критичної інфраструктури – всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і 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;

4) ідентифікація об'єкта критичної інфраструктури – процедура віднесення об'єкта інфраструктури до об'єктів критичної інфраструктури;

5) інцидент безпеки критичної інфраструктури (далі – інцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки несанкціонованого втручання в функціонування об'єкта критичної інфраструктури, які становлять загрозу його безпеці, системі управління технологічними процесами об'єкта критичної інфраструктури, створюють ймовірність порушення штатного режиму функціонування такого об'єкта (у тому числі зриву та/або блокування роботи, та/або несанкціонованого управління його ресурсами), ставлять під загрозу його захищеність;

6) категоризація об'єктів інфраструктури – віднесення об'єктів інфраструктури до категорій критичності об'єктів інфраструктури;

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

8) 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;

9) критична інфраструктура – сукупність об'єктів критичної інфраструктури;

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

11) 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;

12) 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;

13) об'єкти критичної інфраструктури – 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;

14) оператор критичної інфраструктури – юридична особа будь-якої форми власності та/або фізична особа – підприємець, що на правах власності, оренди або на інших законних підставах здійснює управління об'єктом критичної інфраструктури та відповідає за його поточне функціонування;

15) 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 (актів несанкціонованого втручання) на об'єктах критичної інфраструктури;

16) паспорт безпеки – документ встановленої форми, який містить відомості про об'єкт критичної інфраструктури, а також комплекс заходів, що вживаються для захисту цього об'єкта від визначених для нього видів загроз (відомості, що містяться у паспорті безпеки, є інформацією з обмеженим доступом);

17) проектна загроза об'єкту критичної інфраструктури – документ встановленої форми, який визначає властивості, характеристики реальних і потенційних загроз об'єкту критичної інфраструктури, на зниження ймовірності реалізації яких має бути спрямовано функціонування системи захисту критичної інфраструктури;

18) реєстр об'єктів критичної інфраструктури – автоматизована система, що містить перелік найбільш важливої для життєдіяльності суспільства та держави критичної інфраструктури, щодо якої встановлюються особливі вимоги із забезпечення її безпеки та стійкості і здійснюється моніторинг їх дотримання;

19) 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 у кризовій ситуації; режим відновлення);

20) 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;

21) сектор критичної інфраструктури – сукупність об'єктів критичної інфраструктури, які належать до одного сектору (галузі) економіки та/або мають спільну функціональну спрямованість;

22) секторальний орган у сфері захисту критичної інфраструктури – державний орган, визначений законодавством відповідальним за забезпечення формування та реалізації державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури;

23) 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;

24) функціональний орган у сфері захисту критичної інфраструктури – державний орган, визначений відповідальним за функціонування окремих державних систем захисту та реагування.

Стаття 2. Законодавство про критичну інфраструктуру та її захист

1. Законодавство про критичну інфраструктуру та її захист складають Конституція України, цей Закон, інші закони України, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України, інші нормативно-правові акти, прийняті на виконання цього Закону.

Стаття 3. Сфера застосування цього Закону

1. Цей Закон регулює відносини у сфері функціонування та захисту критичної інфраструктури в цілому та її об'єктів у мирний час.

2. Особливості захисту та правового режиму об'єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, особливого періоду регулюються законами України "Про правовий режим воєнного стану", "Про правовий режим надзвичайного стану", "Про функціонування єдиної транспортної системи України в особливий період" та "Про оборону України".

3. Окремим законом регулюються відносини щодо забезпечення кіберзахисту та кібербезпеки об'єктів критичної інфраструктури.

Розділ II
ОСНОВНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 4. Засади державної політики у сфері 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 та стійкості критичної інфраструктури;

2) визначення законодавчих вимог до принципів, пріоритетів, стратегічних завдань, підходів щодо захисту критичної інфраструктури;

3) визначення суб'єктів національної системи захисту критичної інфраструктури, їх повноважень та засад відповідальності, порядку взаємодії;

4) створення умов та впровадження заходів, спрямованих на ефективне зниження і контроль за ризиками безпеки, на зниження ризику 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, взаємодії суб'єктів господарювання та населення з питань забезпечення захисту та стійкості критичної інфраструктури;

7) забезпечення міжнародного співробітництва у сфері захисту критичної інфраструктури;

8) створення умов швидкого відновлення надання життєво важливих функцій та послуг у разі реалізації загроз і порушення функціонування 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 у сфері захисту критичної інфраструктури належать:

1) запобігання проявам несанкціонованого втручання в її функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури;

2) попередження кризових ситуацій, що порушують безпеку критичної інфраструктури;

3) 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;

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

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

6) розроблення комплексу заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об'єктах критичної інфраструктури;

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

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

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

10) підготовка, перепідготовка, підвищення кваліфікації, тренування працівників національної системи захисту критичної інфраструктури;

11) 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

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

1) єдність методологічних засад;

2) координованість;

3) державно-приватне партнерство;

4) безпека, захист та охорона інформації з обмеженим доступом;

5) 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, іншими центральними органами виконавчої влади та державними органами, Національним банком України;

2) регіональний та галузевий рівні, управління на яких здійснюється центральними та місцевими органами виконавчої влади, визначеними в установленому законом порядку відповідальними за забезпечення формування та реалізацію державної політики у сфері захисту критичної інфраструктури в окремому секторі критичної інфраструктури та відповідальними за функціонування окремих державних систем захисту та реагування;

3) місцевий рівень, управління на якому здійснюється місцевими органами виконавчої влади (військово-цивільними адміністраціями – у разі створення), органами місцевого самоврядування в межах повноважень, покладених на них цим Законом;

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

Розділ III
КРИТИЧНА ІНФРАСТРУКТУРА УКРАЇНИ

Стаття 8. Віднесення об'єктів до критичної інфраструктури

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

Віднесення банків, інших об'єктів, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких

здійснює Національний банк України, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури здійснюється в порядку, встановленому Національним банком України.

Віднесення об'єктів до критичної інфраструктури, що здійснюють діяльність на ринках послуг, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, здійснюється в порядку, встановленому такими державними органами.

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 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 таких 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); державному суверенітету (зниження обороноздатності, дискредитація іміджу країни, дестабілізація системи державного управління та унеможливлення виконання державою своїх функцій); економіці (вплив на внутрішній валовий продукт, розмір економічних втрат, як прямих, так і непрямих); природним ресурсам загальнодержавного та місцевого значення;

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 позначаться на діяльності ряду інших секторів;

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

7) вплив на функціонування суміжних секторів критичної інфраструктури.

4. Об'єкти критичної інфраструктури, що не можуть належати:

фізичним і юридичним особам – громадянам та/або резидентам держави, визнаної Верховною Радою України державою-агресором, або кінцевими бенефіціарними власниками яких є громадяни держави, визнаної Україною державою-агресором або державою-окупантом;

юридичним особам, зареєстрованим згідно із законодавством держав, включених FATF до списку держав, що не співпрацюють у сфері протидії відмиванню доходів, одержаних злочинним шляхом, а також юридичним особам, 50 і більше відсотків статутного капіталу яких належать прямо або опосередковано таким особам, протягом року підлягають відчуженню.

Стаття 9. Сектори критичної інфраструктури

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

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

Секторальні органи у сфері захисту критичної інфраструктури складають та ведуть секторальні переліки об'єктів 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 (далі – Перелік), визначається Кабінетом Міністрів України. У разі необхідності внесення змін до Переліку Кабінет Міністрів України переглядає та змінює його виходячи з критеріїв критичності, визначених цим Законом.

4. До життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема:

1) урядування та надання найважливіших публічних (адміністративних) послуг;

2) енергозабезпечення (у тому числі постачання теплової енергії);

3) водопостачання та водовідведення;

4) продовольче забезпечення;

5) охорона здоров'я;

6) фармацевтична промисловість;

7) виготовлення вакцин, стале функціонування біолабораторій;

8) інформаційні послуги;

9) електронні комунікації;

10) фінансові послуги;

11) транспортне забезпечення;

12) оборона, державна безпека;

13) правопорядок, здійснення правосуддя, тримання під вартою;

14) цивільний захист населення та територій, служби порятунку;

15) космічна діяльність, космічні технології та послуги;

16) хімічна промисловість;

17) дослідницька діяльність.

Стаття 10. Категоризація об'єктів критичної інфраструктури

1. Для визначення рівня вимог щодо забезпечення захисту об'єктів критичної інфраструктури відповідно до рівня їх важливості для забезпечення окремих життєво важливих функцій у межах секторів критичної інфраструктури здійснюється категоризація об'єктів критичної інфраструктури відповідно до категорій критичності, визначених цим Законом.

2. Установлюються такі категорії критичності об'єктів критичної інфраструктури:

1) 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 державного значення;

2) II категорія критичності – життєво важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації регіонального значення;

3) III категорія критичності – важливі об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації місцевого значення;

4) IV категорія критичності – необхідні об'єкти, порушення функціонування яких призведе до виникнення кризової ситуації локального значення.

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

4. Секторальні органи разом з операторами критичної інфраструктури здійснюють категоризацію об'єктів критичної інфраструктури своїх секторів (підсекторів) критичної інфраструктури відповідно до Методики категоризації об'єктів критичної інфраструктури, що затверджується Кабінетом Міністрів України, а в банківській та фінансовій системах – Національним банком України, у сферах, державне регулювання та нагляд за діяльністю яких здійснюють державні органи, – такими державними органами.

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 (далі – Реєстр).

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

3. Реєстр формується та ведеться уповноваженим органом у сфері захисту критичної інфраструктури України на основі пропозицій суб'єктів національної системи захисту критичної інфраструктури.

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

5. Порядок ведення Реєстру, включення об'єктів до Реєстру, доступу та надання інформації з нього визначається Кабінетом Міністрів України.

6. Інформація про об'єкти критичної інфраструктури, що міститься в Реєстрі, є відкритою, загальнодоступною та безоплатною, крім інформації з обмеженим доступом. Розпорядник забезпечує цілодобовий доступ до відкритої інформації Реєстру на своєму офіційному веб-сайті.

7. Для посадових осіб суб'єктів національної системи захисту критичної інфраструктури, визначених статтею 14 цього Закону, інформація з Реєстру у зв'язку із здійсненням ними повноважень, передбачених законом, надається за суб'єктом права чи за об'єктом критичної інфраструктури в електронній формі шляхом безпосереднього доступу до Реєстру, за умови ідентифікації

відповідної посадової особи у порядку, встановленому Законом України "Про електронні довірчі послуги".

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, відповідного функціонального органу 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 і безпеки, а також визначає перелік посад та відповідальних осіб, до завдань яких належать зв'язок та обмін інформацією з суб'єктами національної системи захисту критичної інфраструктури.

3. Паспорт безпеки розробляється (переглядається) з урахуванням визначених проектних загроз. Погодження паспорта безпеки на об'єкт критичної інфраструктури здійснюється безоплатно для усіх операторів об'єктів критичної інфраструктури незалежно від форми власності.

4. Вимоги до порядку розроблення та погодження паспорта безпеки на об'єкт критичної інфраструктури, його наповнення, зміст, порядок і строки подання встановлюються Кабінетом Міністрів України.

5. Національний банк України визначає з урахуванням вимог цього Закону порядок розроблення паспорта безпеки на об'єкти критичної інфраструктури, зміст і строки подання його банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, платіжними організаціями, учасниками платіжних систем, операторами послуг платіжної інфраструктури.

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

7. 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, визначає уповноважений орган з питань захисту критичної інфраструктури України.

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:

1) Кабінет Міністрів України;

2) Апарат Ради національної безпеки і оборони України;

3) Центральна виборча комісія;

4) Національний банк України;

5) Національна комісія з цінних паперів та фондового ринку, Національна комісія, що здійснює державне регулювання у сфері зв'язку та

інформатизації, Національна комісія, що здійснює державне регулювання у сферах енергетики та комунальних послуг;

6) Адміністрація Державної служби спеціального зв'язку та захисту інформації України;

7) Фонд державного майна України, інші центральні органи виконавчої влади із спеціальним статусом;

8) уповноважений орган у сфері захисту критичної інфраструктури України;

9) центральний орган виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту;

10) секторальні та функціональні органи, інші міністерства та центральні органи виконавчої влади;

11) Служба безпеки України;

12) правоохоронні та розвідувальні органи, суб'єкти оперативно-розшукової та контррозвідувальної діяльності;

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

14) місцеві органи виконавчої влади (військово-цивільні адміністрації – у разі утворення);

15) органи місцевого самоврядування;

16) оператори критичної інфраструктури;

17) 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 стосовно 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, доступ 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. Суб'єктами національної системи захисту критичної інфраструктури розробляється план взаємодії з іншими суб'єктами національної системи захисту, який погоджується з уповноваженим органом у сфері захисту критичної інфраструктури України та затверджується Кабінетом Міністрів України і переглядається раз на три роки. У плані взаємодії можуть бути визначені особливості взаємодії для режимів функціонування національної системи захисту критичної інфраструктури.

3. Рішення про оголошення режимів функціонування критичної інфраструктури приймається секторальними органами у сфері захисту критичної інфраструктури, відповідальними за сектор критичної інфраструктури.

Стаття 16. Уповноважений орган у сфері захисту критичної інфраструктури України

1. Уповноважений орган у сфері захисту критичної інфраструктури України забезпечує формування та реалізує державну політику у сфері захисту критичної інфраструктури, здійснює функціональне управління національною системою захисту критичної інфраструктури, забезпечує координацію діяльності міністерств та операторів критичної інфраструктури з питань забезпечення стійкості та захисту об'єктів критичної інфраструктури.

Діяльність уповноваженого органу у сфері захисту критичної інфраструктури України спрямовує, координує та контролює Міністр Кабінету Міністрів України.

2. Уповноважений орган у сфері захисту критичної інфраструктури України:

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;

3) взаємодіє з секторальними, функціональними органами у сфері захисту критичної інфраструктури та операторами критичної інфраструктури з питань забезпечення захисту об'єктів, включених до Реєстру;

4) організовує здійснення оцінки захищеності об'єктів критичної інфраструктури, внесених до Реєстру, аналізує та оцінює загальний стан їх захищеності;

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

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 до категорій об'єктів критичної інфраструктури;

9) надає пропозиції Кабінету Міністрів України щодо:

Національного плану захисту та забезпечення стійкості критичної інфраструктури;

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

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

10) розробляє та затверджує Проектні загрози критичній інфраструктурі національного рівня, що становлять інформацію з обмеженим доступом;

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

12) забезпечує функціонування системи обміну інформацією між суб'єктами національної системи захисту критичної інфраструктури;

13) створює бази даних щодо загроз і вразливостей критичній інфраструктурі;

14) забезпечує координацію секторальних органів, підготовку пропозицій до проектів стратегічних документів щодо забезпечення безпеки та стійкості, здійснення захисту критичної інфраструктури – Стратегії національної безпеки України, Стратегії кібербезпеки України та Стратегії громадської безпеки та цивільного захисту України;

15) бере участь у розробленні нової галузі знань, програм навчання, підвищення кваліфікації, робочих і навчальних програм з питань забезпечення стійкості та захисту критичної інфраструктури;

16) здійснює міжнародне співробітництво, забезпечує дотримання і виконання зобов'язань, взятих відповідно до міжнародних договорів України з питань захисту критичної інфраструктури, налагоджує і підтримує зв'язки з міжнародними організаціями, іноземними державами, їх правоохоронними органами і спеціальними службами;

17) здійснює інші повноваження, передбачені цим Законом.

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

Стаття 17. Функціональні органи у сфері захисту критичної інфраструктури

1. Органи державної влади, визначені відповідальними за функціонування окремих державних систем захисту та реагування:

1) беруть участь у встановленому законодавством порядку в реагуванні на кризові ситуації, пов'язані із забезпеченням безпеки та стійкості критичної інфраструктури;

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

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

4) надають власникам та операторам інфраструктури консультації щодо ризиків і загроз критичній інфраструктурі та заходів щодо їх нейтралізації;

5) здійснюють іншу діяльність для забезпечення стійкості та захисту критичної інфраструктури в межах повноважень, що регулюють діяльність суб'єктів захисту критичної інфраструктури, зокрема:

організовують проведення оцінки загроз та ризиків критичній інфраструктурі у відповідних сферах;

беруть участь у проведенні оцінки загроз та ризиків критичній інфраструктурі на загальнодержавному рівні;

формують пропозиції щодо національних та секторальних проектних ризиків і загроз;

забезпечують організацію взаємодії та обміну інформацією з іншими суб'єктами національної системи захисту критичної інфраструктури;

здійснюють моніторинг рівня безпеки об'єктів критичної інфраструктури у відповідних сферах.

Стаття 18. Особливості діяльності окремих органів, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури

1. Діяльність Національного банку України, уповноваженого органу у сфері захисту критичної інфраструктури України, центрального органу виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту, Служби безпеки України, Національної гвардії України, Національної поліції України, Збройних Сил України, Державної спеціальної служби транспорту та Державної служби спеціального зв'язку та захисту інформації України 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 у цій статті органів.

Стаття 19. Секторальні органи у сфері захисту критичної інфраструктури

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

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

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

3) спільно з операторами критичної інфраструктури здійснюють категоризацію об'єктів критичної інфраструктури своїх секторів критичної

інфраструктури, формують секторальні переліки об'єктів критичної інфраструктури, подають інформацію до Реєстру;

4) розробляють та затверджують:

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

б) проектні 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 важливих функцій на випадок порушення функціонування об'єктів критичної інфраструктури;

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

6) затверджують проектні загрози критичній інфраструктурі об'єктового рівня у відповідних секторах;

7) погоджують паспорти безпеки об'єктів критичної інфраструктури, надані операторами у відповідних секторах;

8) 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 інфраструктурі 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;

ґ) участь у встановленому законодавством порядку в реагуванні на кризові ситуації, пов'язані з безпекою, захистом та стійкістю об'єктів критичної інфраструктури, а також у створенні умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури;

д) 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;

9) надають операторам об'єктів критичної інфраструктури рекомендації з питань захисту критичної інфраструктури та обов'язкові до виконання вимоги щодо усунення причин і умов, які порушують стійкість критичної інфраструктури;

10) виконують:

а) збір, аналіз та узагальнення даних щодо об'єктів критичної інфраструктури та загроз їх функціонуванню;

б) заходи із функціонування відповідних систем обміну інформацією, моніторингу рівня безпеки об'єктів критичної інфраструктури;

11) організовують функціонування системи обміну інформацією та взаємодії у відповідних секторах критичної інфраструктури між суб'єктами національної системи захисту критичної інфраструктури;

12) готують пропозиції до стратегічних документів щодо забезпечення стійкості та захисту критичної інфраструктури.

2. Секторальні органи у сфері захисту критичної інфраструктури щороку відповідно до строків та форми звіту, затверджених Кабінетом Міністрів України, подають інформацію уповноваженому органу у сфері захисту критичної інфраструктури України.

Стаття 20. 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:

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

2) розроблення, затвердження та погодження із заінтересованими органами:

а) місцевих планів взаємодії залучених суб'єктів у кризовій ситуації з метою підтримання життєво важливих функцій та надання життєво важливих послуг, планів відновлення функціонування критичної інфраструктури;

б) програм навчання населення для забезпечення захисту в разі виникнення режиму реагування на виникнення кризової ситуації та режиму відновлення штатного функціонування.

Стаття 21. Завдання, права та обов'язки операторів 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) розроблення, оновлення та забезпечення виконання об'єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури, правил управління ризиками безпеки, 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'єктами національної системи захисту критичної інфраструктури, а також створення умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо 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 реагування на протиправні дії, фізичні атаки, спрямовані на відключення або пошкодження роботи операційних систем чи 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 із захисту повітряного простору над визначеними об'єктами критичної інфраструктури;

9) негайне інформування уповноваженого органу у сфері захисту критичної інфраструктури України, 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, а також інформування Служби безпеки України про загрози та ризики диверсій, терористичних актів, актів кібертероризму проти систем управління, операційних та інших систем об'єктів критичної інфраструктури, надзвичайних ситуацій або інших небезпечних подій на важливих державних об'єктах;

10) забезпечення постійного зв'язку з відповідальними за реагування на протиправні дії та з іншими компетентними організаціями та установами;

11) забезпечення постійної взаємодії з підприємствами, які забезпечують централізоване водопостачання, централізоване водовідведення, постачання теплової енергії, енергопостачання, функціонування електронних комунікаційних мереж, транспортне обслуговування, медичну допомогу,

безпеку та інші послуги, від яких залежить процес реагування на кризові ситуації та відновлення функціонування об'єктів критичної інфраструктури;

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

13) проведення навчань та тренінгів, підготовка та перевірка персоналу, який відповідає за охорону, безпеку та захист об'єктів критичної інфраструктури;

14) захист інформації про системи управління, зв'язку, фізичну безпеку 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 розроблення 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 про забезпечення безпеки об'єктів критичної інфраструктури;

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

3) отримувати від уповноваженого органу у сфері захисту критичної інфраструктури України консультації щодо застосування законодавства у сфері захисту критичної інфраструктури та вжиття необхідних заходів для захисту критичної інфраструктури.

4. Оператори критичної інфраструктури зобов'язані:

1) забезпечити захист об'єктів критичної інфраструктури;

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 на іншій законній підставі;

3) завчасно, але не менше ніж за 30 календарних днів до дати зміни стану об'єкта критичної інфраструктури або його частини, інформувати уповноважений орган у сфері захисту критичної інфраструктури України про наміри змінити цільове призначення, режим функціонування чи намір передати права на об'єкт критичної інфраструктури та виконувати надані їм висновки та рекомендації;

4) щороку надавати інформацію про виконання повноважень відповідно до цього Закону за формою, визначеною Кабінетом Міністрів України.

Розділ V
ОРГАНІЗАЦІЙНІ ЗАСАДИ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стаття 22. 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 розробляються та затверджуються відповідні плани та програми реагування на кризові ситуації.

Кабінет Міністрів України встановлює вимоги щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності, крім банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури, державне регулювання, нагляд за діяльністю яких здійснює Національний банк України, та встановлює вимоги щодо управління ризиками безпеки.

2. На державному рівні розробляється Національний план захисту та забезпечення безпеки та 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 розроблення, затвердження і виконання місцевих програм підвищення стійкості територіальних громад до кризових ситуацій, викликаних припиненням надання чи погіршенням якості важливих для їх життєдіяльності послуг або припиненням здійснення життєво важливих функцій. Такі програми включають заходи із забезпечення безпеки 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, ефективного зниження та контролю за ризиками безпеки, забезпечення безпеки інформації та кібербезпеки на об'єктах критичної інфраструктури.

7. Плани та програми, затверджені відповідно до цієї статті, є обов'язковими до виконання всіма суб'єктами національної системи захисту критичної інфраструктури.

Стаття 23. Здійснення моніторингу рівня безпеки об'єктів критичної інфраструктури

1. Моніторинг рівня безпеки об'єктів критичної інфраструктури здійснюється шляхом проведення оцінки стану захищеності об'єктів критичної інфраструктури.

Оцінка стану 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 рівня безпеки готуються пропозиції щодо удосконалення системи захисту об'єктів критичної інфраструктури, оцінки стану безпеки об'єктів критичної інфраструктури секторальними та функціональними органами у сфері захисту критичної інфраструктури. Пропозиції щодо удосконалення системи захисту об'єктів критичної інфраструктури, підготовлені за результатами моніторингу оцінки стану захищеності, є інформацією з обмеженим доступом.

4. Порядок здійснення моніторингу оцінки стану безпеки об'єктів критичної інфраструктури та його періодичність затверджуються Кабінетом Міністрів України.

Стаття 24. Взаємодія національної системи захисту критичної інфраструктури з іншими системами захисту у сфері національної безпеки

1. Для забезпечення безпеки і 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, а також з контррозвідувальними та розвідувальними органами у сфері забезпечення державної безпеки;

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, що 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, 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 таких об'єктів та місцевого населення.

3. Організація взаємодії між суб'єктами національної системи захисту критичної інфраструктури здійснюється шляхом:

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

2) проведення спільних оперативних нарад керівного складу уповноваженого органу у сфері захисту критичної інфраструктури України, 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 із 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 із 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 із 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 загрожують безпеці громадян і порушують функціонування таких об'єктів;

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 25. Державно-приватне партнерство у сфері захисту критичної інфраструктури

1. Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється 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;

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

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

4) створення системи підготовки кадрів для сфери захисту критичної інфраструктури;

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

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

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

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

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

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

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

12) 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;

13) створення механізмів для саморегулювання, обміну інформацією між операторами об'єктів критичної інфраструктури у певному секторі;

14) створення та підтримки розвитку систем сертифікації та оцінки відповідності у секторах критичної інфраструктури.

2. Державно-приватне партнерство у сфері захисту критичної інфраструктури здійснюється з урахуванням установлених 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 можуть створюватися консультативно-дорадчі органи, об'єднання та мережі у порядку, встановленому законодавством.

Стаття 26. Проведення незалежного аудиту діяльності національної системи захисту критичної інфраструктури

1. Незалежна зовнішня оцінка діяльності уповноваженого органу у сфері захисту критичної інфраструктури України здійснюється шляхом проведення щорічного зовнішнього аудиту його діяльності. Зовнішній аудит діяльності уповноваженого органу у сфері захисту критичної інфраструктури України проводиться Рахунковою палатою.

2. Незалежна зовнішня оцінка діяльності національної системи захисту критичної інфраструктури здійснюється один раз на три роки Рахунковою

палатою у визначеному нею порядку на підставі міжнародних стандартів оцінки.

3. Форма та зміст звіту про зовнішній аудит діяльності уповноваженого органу у сфері захисту критичної інфраструктури України 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 27. Парламентський контроль у сфері захисту критичної інфраструктури

1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення 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 України про результати незалежного аудиту діяльності щодо ефективності системи забезпечення захисту критичної інфраструктури.

2. За результатами розгляду звіту уповноваженого органу у сфері захисту критичної інфраструктури України 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 28. Громадський нагляд у сфері захисту критичної інфраструктури

1. Право громадського нагляду 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 рад при органах, що формують та забезпечують реалізацію державної політики у сфері забезпечення захисту критичної інфраструктури, проведення незалежного аудиту їх діяльності, право доступу до публічної частини звіту щодо забезпечення захисту об'єктів критичної інфраструктури.

2. Доступ до інформації у сфері захисту критичної інфраструктури для реалізації громадського нагляду здійснюється у порядку, передбаченому Законом України "Про доступ до публічної інформації", та може бути обмежений виключно Законом України "Про державну таємницю".

Стаття 29. Відповідальність за порушення законодавства у сфері захисту критичної інфраструктури

1. Особи, винні у порушенні законодавства у сфері захисту критичної інфраструктури, несуть відповідальність згідно із законом.

Стаття 30. 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 операторів критичної інфраструктури, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Стаття 31. Міжнародне співробітництво у сфері захисту критичної інфраструктури

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

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

3. Відповідно до законодавства у сфері зовнішніх зносин суб'єкти національної системи захисту критичної інфраструктури у межах своїх повноважень здійснюють міжнародну співпрацю безпосередньо на двосторонній або багатосторонній основі.

Стаття 32. Страхування ризиків

1. Оператор критичної інфраструктури зобов'язаний забезпечити страхування ризику настання кризової ситуації.

2. Перелік об'єктів критичної інфраструктури, включених до Реєстру, страхових ризиків настання кризової ситуації на таких об'єктах, які підлягають страхуванню, а також мінімальний ліміт відповідальності (у разі страхування відповідальності перед третіми особами) затверджуються Кабінетом Міністрів України, а щодо об'єктів критичної інфраструктури у сфері фінансових послуг – погоджуються з Національним банком 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, крім частини другої статті 32 (щодо страхування об'єктів критичної інфраструктури), яка набирає чинності через три роки з дня набрання чинності цим Законом.

2. Внести зміни до таких законодавчих актів України:

1) частину другу статті 17 Кодексу цивільного захисту України (Відомості Верховної Ради України, 2013 р., № 34–35, ст. 458) після пункту 53 доповнити п'ятьма новими пунктами такого змісту:

"54) 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;

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

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

57) 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, віднесених до об'єктів критичної інфраструктури, аварійно-рятувальними службами, що пройшли атестацію в установленому порядку;

58) 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 в разі виникнення надзвичайних ситуацій".

У зв'язку з цим пункт 54 вважати пунктом 59;

2) 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:

"Служби безпеки України – оперативними підрозділами Центрального управління, регіональних органів та органів військової контррозвідки";

3) пункт "б" частини першої статті 38 Закону України "Про місцеве самоврядування в Україні" (Відомості Верховної Ради України, 1997 р., № 24, ст. 170 із наступними змінами) доповнити підпунктом 2^1 такого змісту:

"2^1) вжиття необхідних заходів 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 чи припиненням здійснення життєво важливих функцій, взаємодія між суб'єктами національної системи захисту критичної інфраструктури з урахуванням вимог Закону України "Про критичну інфраструктуру";

4) статтю 25 Закону України "Про місцеві державні адміністрації" (Відомості Верховної Ради України, 1999 р., № 20–21, ст. 190 із наступними змінами) доповнити пунктом 24 такого змісту:

"24) забезпечує захист 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, взаємодію між суб'єктами національної системи захисту критичної інфраструктури";

5) у статті 7 Закону України "Про Національний банк України" (Відомості Верховної Ради України, 1999 р., № 29, ст. 238 із наступними змінами):

пункт 33 викласти в такій редакції:

"33) забезпечує формування та ведення реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України, визначає критерії та порядок віднесення об'єктів у банківській системі України до

об'єктів критичної інформаційної інфраструктури, забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки у банківській системі України";

доповнити пунктом 33^1 такого змісту:

"33^1) забезпечує формування та реалізацію державної політики у сфері захисту критичної інфраструктури щодо банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, платіжних організацій, учасників платіжних систем, операторів послуг платіжної інфраструктури відповідно до закону, що визначає правові та організаційні засади функціонування і захисту критичної інфраструктури";

6) у пункті 3 статті 16 Закону України "Про правовий режим надзвичайного стану" (Відомості Верховної Ради України, 2000 р., № 23, ст. 176; 2013 р., № 15, ст. 99; 2014 р., № 12, ст. 178) слова "об'єктів, що забезпечують життєдіяльність населення та народного господарства" замінити словами "важливих об'єктів національної економіки та об'єктів критичної інфраструктури";

7) у Законі України "Про Збройні Сили України" (Відомості Верховної Ради України, 2000 р., № 48, ст. 410 із наступними змінами):

у статті 1:

частину четверту після слів "до здійснення заходів правового режиму воєнного і надзвичайного стану" доповнити словами "безпеки та захисту критичної інфраструктури", а після слів "ліквідації надзвичайних ситуацій природного і техногенного характеру" – словами "кризових ситуацій";

після частини четвертої доповнити новою частиною 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 відповідно частинами шостою – десятою;

8) у Законі України "Про оборону України" (Відомості Верховної Ради України, 2000 р., № 49, ст. 420 із наступними змінами):

у статті 3:

абзац десятий після слів "єдиної державної системи цивільного захисту" доповнити словами "об'єктів критичної інфраструктури";

абзац тринадцятий після слів "підготовку національної економіки" доповнити словами "об'єктів критичної інфраструктури";

в абзаці сьомому 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";

в абзаці третьому частини першої статті 13 слова "інших об'єктів інфраструктури" замінити словами "інших об'єктів критичної інфраструктури";

9) 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";

10) у Законі України "Про страхування" (Відомості Верховної Ради України, 2002 р., № 7, ст. 50 із наступними змінами):

частину четверту статті 6 доповнити пунктом 22^1 такого змісту:

"22^1) страхування ризику фінансових втрат, викликаних кризовою ситуацією на об'єкті критичної інфраструктури";

частину першу статті 7 доповнити пунктом 52 такого змісту:

"52) 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";

11) абзац четвертий частини четвертої статті 8 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" (Відомості Верховної Ради України, 2005 р., № 26, ст. 347; 2020 р., № 42, ст. 349) замінити двома новими абзацами такого змісту:

"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, який надає послуги з використанням системи, елементи якої розміщуються поза межами України, має бути юридичною особою, зареєстрованою в Україні, або мати свого офіційного представника в Україні".

У зв'язку з цим абзац п'ятий вважати абзацом шостим;

12) у Законі України "Про інформацію" (Відомості Верховної Ради України, 2011 р., № 32, ст. 313 із наступними змінами):

статтю 10 після абзацу десятого доповнити новим абзацом такого змісту:

"критична технологічна інформація".

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

доповнити статтею 19^1 такого змісту:

"Стаття 19^1. Критична технологічна інформація

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

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

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

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

"2. Перелік об'єктів критичної інфраструктури, охорона яких здійснюється державними органами, підприємствами та організаціями, затверджується Кабінетом Міністрів України";

14) пункт 5 частини першої статті 20 Закону України "Про Кабінет Міністрів України" (Відомості Верховної Ради України, 2014 р., № 13, ст. 222; 2021 р., № 29, ст. 234) після абзацу сьомого доповнити трьома новими абзацами такого змісту:

"забезпечує здійснення заходів із запобігання загрозам безпеці критичної інфраструктури та забезпечення безпеки критичної інфраструктури;

забезпечує планування відновлення функціонування критичної інфраструктури у випадках надзвичайних ситуацій, яким не можна запобігти;

забезпечує стійкість критичної інфраструктури до ідентифікованих загроз і небезпек".

У зв'язку з цим абзаци восьмий і дев'ятий вважати відповідно абзацами одинадцятим і дванадцятим;

15) частину першу статті 2 Закону України "Про Національну гвардію України" (Відомості Верховної Ради України, 2014 р., № 17, ст. 594 із наступними змінами) доповнити пунктом 5^1 такого змісту:

"5^1) 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";

16) у Законі України "Про Державну службу спеціального зв'язку та захисту інформації України" (Відомості Верховної Ради України, 2014 р., № 25, ст. 890 із наступними змінами):

у частині першій статті 3:

абзац третій після слів "довірчих послуг" доповнити словами "захисту критичної інформаційної інфраструктури";

доповнити абзацами п'ятим – сьомим такого змісту:

"реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснення державного контролю в цих сферах;

визначення вимог до захисту критичної технологічної інформації, формування загальних вимог до кіберзахисту об'єктів критичної інфраструктури, ведення переліку об'єктів критичної інформаційної інфраструктури, здійснення заходів щодо його оновлення та актуалізації;

виконання інших завдань, передбачених законодавством у сфері забезпечення кібербезпеки та кіберзахисту";

пункт 24 частини першої статті 14 після слів "захисту інформації" доповнити словами "кіберзахисту об'єктів критичної інфраструктури";

17) у Законі України "Про правовий режим воєнного стану" (Відомості Верховної Ради України, 2015 р., № 28, ст. 250; 2021 р., № 41, ст. 339):

частину першу, абзаци перший і другий частини сьомої, друге речення частини восьмої статті 4 після слів "громадської безпеки і порядку" доповнити словами "захисту критичної інфраструктури";

у частині першій статті 8:

у пункті 1 слова "об'єктів державного значення, об'єктів державного значення національної транспортної системи України" замінити словами "об'єктів критичної інфраструктури";

у пункті 2 слова "та сфері забезпечення життєдіяльності населення" і "та системи забезпечення життєдіяльності населення" замінити словами "та захисту критичної інфраструктури";

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 "важливих об'єктів національної економіки" замінити словами "об'єктів критичної інфраструктури";

у пункті 7 частини третьої слова "важливих об'єктів національної економіки" замінити словами "об'єктів критичної інфраструктури";

18) у частині першій статті 23 Закону України "Про Національну поліцію" (Відомості Верховної Ради України, 2015 р., № 40–41, ст. 379 із наступними змінами):

пункт 20 доповнити словами "а також об'єктів критичної інфраструктури, перелік яких визначається Кабінетом Міністрів України";

доповнити пунктом 24^1 такого змісту:

"24^1) 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";

19) у Законі України "Про основні засади забезпечення кібербезпеки України" (Відомості Верховної Ради України, 2017 р., № 45, ст. 403; із змінами, внесеними Законом України від 30 червня 2021 року № 1591–IX):

у статті 1:

пункт 16 частини першої виключити;

частину другу доповнити реченням такого змісту: "Термін "об'єкт критичної інфраструктури" вживається в цьому Законі у значенні, визначеному Законом України "Про критичну інфраструктуру";

частини першу і другу статті 6 викласти в такій редакції:

"1. Віднесення об'єктів до об'єктів критичної інфраструктури та формування Реєстру об'єктів критичної інфраструктури здійснюються відповідно до Закону України "Про критичну інфраструктуру".

2. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а в банківській системі України – Національним банком України";

20) частину четверту статті 3 Закону України "Про національну безпеку України" (Відомості Верховної Ради України, 2018 р., № 31, ст. 241) викласти в такій редакції:

"4. Державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями".

3. До приведення у відповідність із цим Законом законодавчі та інші нормативно-правові акти застосовуються в частині, що не суперечить цьому Закону.

4. Перша щорічна незалежна зовнішня оцінка діяльності уповноваженого органу у сфері захисту критичної інфраструктури України має бути проведена після першого повного календарного року його діяльності починаючи відлік часу з календарного року, у якому такий орган приступив до здійснення своїх повноважень.

Перша незалежна зовнішня оцінка діяльності національної системи захисту критичної інфраструктури має бути проведена після спливу перших трьох календарних років діяльності уповноваженого органу у сфері захисту критичної інфраструктури України.

5. Кабінету Міністрів України:

1) у тримісячний строк з дня набрання чинності цим Законом:

визначити уповноважений орган з питань захисту критичної інфраструктури України;

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

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

забезпечити приведення міністерствами, іншими центральними і місцевими органами виконавчої влади (військово-цивільними адміністраціями – в разі утворення) їх нормативно-правових актів у відповідність із цим Законом;

2) організувати та забезпечити виконання функцій уповноваженого органу з питань захисту критичної інфраструктури України в межах відповідних видатків на поточний рік державного органу, на який покладено такі повноваження;

3) під час підготовки проекту Державного бюджету України на 2022 рік та наступні роки врахувати видатки, необхідні для виконання повноважень (функцій) уповноваженого органу з питань захисту критичної інфраструктури України.

6. Кабінету Міністрів України протягом трьох років з дня набрання чинності цим Законом забезпечити проведення та завершення перевірки

структури власності об'єктів критичної інфраструктури з метою убезпечення належності таких об'єктів фізичним і юридичним особам – громадянам та/або резидентам держави, визнаної Верховною Радою України державою-агресором, або кінцевими бенефіціарними власниками яких є громадяни держави, визнаної Україною державою-агресором або державою-окупантом; юридичним особам, зареєстрованим згідно із законодавством держав, включених FATF до списку держав, що не співпрацюють у сфері протидії відмиванню доходів, одержаних злочинним шляхом, а також юридичним особам, 50 і більше відсотків статутного капіталу яких належать прямо або опосередковано таким особам.

7. Кабінету Міністрів України до 1 січня 2024 року поінформувати Верховну Раду України про стан виконання цього Закону.

8. Рекомендувати Центральній виборчій комісії, Антимонопольному комітету України, Національному банку України, Національній комісії з цінних паперів та фондового ринку, Національній комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, Національній комісії, що здійснює державне регулювання у сферах енергетики та комунальних послуг, протягом трьох місяців з дня набрання чинності цим Законом:

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

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

9. Центральному органу виконавчої влади у сфері освіти і науки спільно з уповноваженим органом у сфері захисту критичної інфраструктури України забезпечити проведення науково-дослідної роботи щодо доповнення Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, новою позицією у сфері забезпечення стійкості та захисту критичної інфраструктури та до 1 січня 2024 року поінформувати про результати Кабінет Міністрів України і подати проект відповідного рішення та пропозиції щодо програм навчання, підвищення кваліфікації, робочих і навчальних програм.

10. Уповноваженому органу у сфері захисту критичної інфраструктури України щороку починаючи з наступного дня за днем набрання чинності цим Законом забезпечити:

проведення науково-дослідних робіт щодо впливу новітніх і проривних технологій на формування нових індикаторів потенційних ризиків та загроз об'єктам критичної інфраструктури;

перегляд нормативно-правових актів у сфері захисту об'єктів критичної інфраструктури за результатами проведення науково-дослідних робіт;

підготовку рекомендацій для операторів об'єктів критичної інфраструктури за результатами проведення науково-дослідних робіт;

подання пропозицій щодо обсягів бюджетного фінансування для проведення уповноваженим органом у сфері захисту критичної інфраструктури України таких науково-дослідних робіт починаючи відлік часу з календарного року, у якому такий орган приступив до здійснення своїх повноважень;

постійне інформування про результати Кабінету Міністрів України.

11. Уповноваженому органу у сфері захисту критичної інфраструктури України протягом року з дня початку ним діяльності підготувати зміни до Закону України "Про критичну інфраструктуру" в частині визначення форм та розмірів штрафних санкцій до операторів об'єктів критичної інфраструктури, до Кодексу України про адміністративні правопорушення, Кримінального кодексу України в частині визначення видів правопорушень та відповідальності за них.

Президент України В. ЗЕЛЕНСЬКИЙ

м. К и ї в
16 листопада 2021 року
№ 1882–IX