ПРОЕКТ

Вноситься
народними депутатами України

Лук’янчук Р.В.
Кожем’якін А.А.
Бухарєв В.В.
Паламарчук М.П.
Король В.М.
Семенуха Р.С.
Поляков М.А.
Бабенко В.Б.
Сочка О.О.

ЗАКОН УКРАЇНИ

Про основні засади забезпечення
кібербезпеки України

Цей Закон визначає правові та організаційні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, основні принципи та напрями забезпечення кібербезпеки України.

Розділ I

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

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

1) кібератака — несанкціоновані дії, що здійснюються за допомогою інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційній (автоматизованій), телекомунікаційній, інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи;

2) кібербезпека — стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі;

3) кіберзагроза — наявні та потенційно можливі явища і чинники, що загрожують кібербезпеці;

4) кіберзахист — сукупність заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру, спрямованих на забезпечення кібербезпеки;

5) кіберзлочин — суспільно небезпечне винне діяння у кіберпросторі, передбачене законодавством України про кримінальну відповідальність;

6) кіберзлочинність — сукупність кіберзлочинів;

7) кіберінцидент — надзвичайна подія, пов’язана з реалізацією або можливістю реалізації кібератаки;

8) кібероборона — сукупність політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, спрямованих на захист інформаційного суверенітету та забезпечення обороноздатності держави у кіберпросторі;

9) кіберпростір — середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем;

10) кібертероризм — терористична діяльність, що провадиться у кіберпросторі або з його використанням;

11) критична інформаційна інфраструктура — сукупність об’єктів критичної інформаційної інфраструктури держави;

12) національний сегмент кіберпростору (кіберпростір України) — кіберпростір, що належить до юрисдикції України;

13) об’єкт критичної інформаційної інфраструктури — інформаційна (автоматизована), телекомунікаційна, інформаційно-телекомунікаційна система, порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України;

14) суб’єкти забезпечення кібербезпеки — державні органи, органи місцевого самоврядування, органи управління Збройних Сил України та інших військових формувань, утворених відповідно до законів України, правоохоронні органи, а також підприємства, установи та організації незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки національного сегмента кіберпростору, у тому числі забезпеченням кіберзахисту в рамках надання інформаційних та/або телекомунікаційних послуг;

15) суб’єкти забезпечення кібербезпеки постійної готовності — державні органи або їх підрозділи, що входять до складу національної системи кібербезпеки, сили та засоби яких спеціально виділені для перебування у постійній готовності до реагування на кіберзагрози та оперативного виконання завдань забезпечення кібербезпеки.

Стаття 2. Правова основа забезпечення кібербезпеки України

1. Правову основу забезпечення кібербезпеки України становлять Конституція України, Кримінальний кодекс України, Кодекс України про адміністративні правопорушення, цей та інші закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання законів інші нормативно-правові акти України.

Розділ II

ОРГАНІЗАЦІЙНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Стаття 3. Основні принципи забезпечення кібербезпеки

1. Діяльність із забезпечення кібербезпеки ґрунтується на принципах:

верховенства права, законності та неухильного додержання прав і свобод людини і громадянина;

пріоритетності для держави захисту особистої інформації людини і громадянина;

комплексного підходу до впровадження правових, організаційних, технічних та інформаційних заходів;

пріоритетності запобіжних заходів;

невідворотності відповідальності за вчинення кіберзлочинів та інших правопорушень, які вчиняються з використанням інформаційно-телекомунікаційних систем та їх ресурсів, забезпечення відновлення порушених прав і законних інтересів, відшкодування збитків, шкоди, завданої кіберзлочинами або відповідними правопорушеннями;

взаємодії держави та приватного сектору у виробленні нових рішень у сфері кібербезпеки та участі інституцій громадянського суспільства у забезпеченні кібербезпеки держави;

відповідальності суб'єктів забезпечення кібербезпеки за належне функціонування об'єктів кіберзахисту;

дієвості, комплексності і постійності заходів із захисту інформації та інформаційних ресурсів в кіберпросторі;

співпраці на міжнародному рівні з метою вироблення єдиних підходів та ефективної взаємодопомоги з питань протидії кіберзагрозам.

Стаття 4. Основні напрями забезпечення кібербезпеки України

1. Кібербезпека України забезпечується шляхом проведення виваженої державної політики відповідно до прийнятих в установленому порядку доктрин, концепцій, стратегій і програм.

2. Основними напрямами державної політики у сфері кібербезпеки України є:

створення захищеного національного сегмента кіберпростору, що сприятиме підтриманню відкритого суспільства і забезпечуватиме безпечне використання цього простору суспільством;

запобігання втручанню у внутрішні справи України і нейтралізація посягань на її інформаційні ресурси з боку інших держав;

посилення обороноздатності держави у кіберпросторі;

боротьба з кіберзлочинністю та кібертероризмом;

зниження рівня уразливості об'єктів кіберзахисту;

забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки;

дотримання міжнародних зобов'язань щодо боротьби з кіберзлочинністю та кібертероризмом.

3. Вибір конкретних засобів і шляхів забезпечення кібербезпеки України обумовлюється необхідністю своєчасного вжиття заходів, адекватних характеру і масштабам реальних та потенційних кіберзагроз життєво важливим інтересам людини і громадянина, суспільства і держави.

4. Основними напрямами забезпечення кібербезпеки України є:

розвиток інформаційної інфраструктури держави, забезпечення безпечного функціонування об'єктів критичної інформаційної інфраструктури;

розвиток міжнародного співробітництва у сфері кібербезпеки;

зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби з проявами кіберзлочинності та кібертероризму;

забезпечення ефективного застосування Збройних Сил України для адекватної відповіді реальним та потенційним кіберзагрозам національному сегменту кіберпростору;

розвиток пріоритетних напрямів науки і техніки як основи створення високих інформаційних технологій;

підтримка виробників продукції та послуг у сфері кібербезпеки на засадах стимулювання вітчизняних виробників;

адаптація законодавства України до норм ЄС, створення нормативно-правових та економічних передумов для розвитку інформаційної інфраструктури держави, підвищення її стійкості до кібератак, спроможності держави більш ефективно захищати національні інтереси у кіберпросторі;

забезпечення неухильного дотримання власниками об'єктів критичної інформаційної інфраструктури вимог законодавства у сфері захисту

державних інформаційних ресурсів, криптографічного та технічного захисту інформації, захисту персональних даних;

підвищення рівня обізнаності суспільства щодо ризиків, викликів і загроз у кіберпросторі.

5. Головними принципами діяльності у сфері кібербезпеки України є:

координація заходів, які здійснюються для забезпечення кібербезпеки суб'єктами забезпечення кібербезпеки відповідно до їх призначення (специфіки діяльності) та повноважень;

взаємодія структур державного і приватного секторів на національному та міжнародному рівні з метою забезпечення адекватної відповіді кіберзагрозам;

пріоритетність завдань і зосередження зусиль на забезпеченні кібербезпеки об'єктів критичної інформаційної інфраструктури;

застосування новітніх технологій та передового досвіду для поліпшення стану кіберзахисту об'єктів критичної інформаційної інфраструктури.

Стаття 5. Об'єкти кіберзахисту

1. Об'єктами кіберзахисту є об'єкти критичної інформаційної інфраструктури та інші інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом.

2. Об'єкти критичної інформаційної інфраструктури потребують першочергового (пріоритетного) захисту від кібератак.

Порядок віднесення об'єктів до критичної інформаційної інфраструктури та перелік таких об'єктів затверджуються Кабінетом Міністрів України.

Стаття 6. Забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури

1. Кіберзахист об'єктів критичної інформаційної інфраструктури здійснюється відповідно до законодавства та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України.

2. Відповідальність за забезпечення кіберзахисту об'єкта критичної інформаційної інфраструктури покладається на його власника.

Власник об'єкта критичної інформаційної інфраструктури незалежно від форми власності зобов'язаний:

надавати суб'єктам забезпечення кібербезпеки постійної готовності в установленому Кабінетом Міністрів України порядку відомості про об'єкти критичної інформаційної інфраструктури;

утворювати у своїй структурі підрозділ забезпечення кібербезпеки або уповноважувати окремих осіб на виконання функцій такого підрозділу та забезпечувати їх функціонування;

негайно інформувати спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації про спроби вчинення та/або вчинення стосовно об'єктів критичної інформаційної інфраструктури кібератак та інших несанкціонованих дій, а також здійснювати заходи щодо блокування, усунення або локалізації їх негативних наслідків.

3. Захист об'єктів критичної інформаційної інфраструктури від кібератак забезпечується відповідно до вимог законодавства у сфері захисту інформації.

Стаття 7. Національна система кібербезпеки

1. Національна система кібербезпеки — це сукупність усіх суб'єктів забезпечення кібербезпеки, а також взаємоузгоджених заходів кіберзахисту, що здійснюються ними.

Національна система кібербезпеки забезпечує захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі.

2. Основою національної системи кібербезпеки є суб'єкти забезпечення кібербезпеки постійної готовності.

Координація діяльності суб'єктів забезпечення кібербезпеки постійної готовності здійснюється Радою національної безпеки і оборони України в межах повноважень, визначених законодавством.

До участі у здійсненні заходів, пов'язаних із виявленням, запобіганням і нейтралізацією кіберзагроз, залучаються інші суб'єкти забезпечення кібербезпеки, діяльність яких координується суб'єктами забезпечення кібербезпеки постійної готовності.

Стаття 8. Повноваження суб'єктів забезпечення кібербезпеки постійної готовності

1. Рада національної безпеки і оборони України:

виробляє стратегічні напрями державної політики у сфері кібербезпеки;

організовує розгортання та функціонування системи оперативної взаємодії між суб'єктами забезпечення кібербезпеки постійної готовності;

координує діяльність органів виконавчої влади, які є суб'єктами забезпечення кібербезпеки постійної готовності, щодо запобігання кіберзагрозам, усунення передумов їх настання та наслідків їх реалізації;

проводить аналіз стану кібербезпеки і можливих кіберзагроз національній безпеці України та узагальнює міжнародний досвід щодо формування та реалізації державної політики у сфері кібербезпеки;

готує пропозиції та розробляє разом із суб'єктами забезпечення кібербезпеки постійної готовності сценарії реагування на кіберзагрози, рекомендації щодо протидії ним;

проводить аналіз стану виконання державними органами галузевих програм і заходів, пов'язаних з реалізацією державної політики у сфері кібербезпеки;

формує пропозиції щодо підготовки кадрів у сфері кібербезпеки;

координує розроблення і готує пропозиції щодо:

визначення концептуальних підходів до формування державної політики у сфері кібербезпеки;

удосконалення системи правового, наукового і кадрового забезпечення кібербезпеки;

удосконалення системи оперативного інформаційно-аналітичного забезпечення органів державної влади у сфері кібербезпеки.

2. Міністерство внутрішніх справ України:

бере участь у формуванні та реалізації державної політики у сфері кібербезпеки;

створює у межах затвердженої чисельності і забезпечує функціонування підрозділу з протидії кіберзлочинності;

розробляє та реалізує комплекс організаційних і практичних заходів, спрямованих на боротьбу з кіберзлочинами та іншими правопорушеннями, які вчиняються з використанням інформаційно-телекомунікаційних систем та їх ресурсів;

створює і забезпечує належне функціонування цілодобової контактної мережі для надання невідкладної допомоги у розслідуванні кіберзлочинів;

вживає заходів для забезпечення виконання міжнародних зобов'язань України щодо боротьби з кіберзлочинністю;

здійснює міжнародне співробітництво і взаємодіє з компетентними органами інших держав у рамках надання міжнародно-правової допомоги у протидії кіберзлочинам;

вживає правових і організаційно-технічних заходів із збору та обліку інформації про кіберінциденти, кіберзлочини і результати діяльності з протидії кіберзлочинності, узагальнює і надає таку інформацію суб'єктам забезпечення кібербезпеки постійної готовності відповідно до їх повноважень;

забезпечує у встановленому Кабінетом Міністрів України порядку організацію та функціонування системи обмеження та блокування доступу до ресурсів, які використовуються для підготовки, вчинення або приховування кіберзлочинів, а також в інших передбачених законами України випадках.

3. Міністерство оборони України:

бере участь у формуванні та реалізації державної політики кібербезпеки у воєнній сфері і сфері оборони;

проводить аналіз воєнно-політичної обстановки та визначає рівень воєнної загрози національній безпеці України через використання кіберпростору;

проводить аналіз, прогнозування та оцінку рівня кіберзагроз воєнного характеру;

здійснює планування та виконання заходів щодо протидії і нейтралізації воєнно-політичних ризиків, викликів, загроз застосування воєнної сили проти національного сегмента кіберпростору;

бере участь у підготовці об’єктів критичної інформаційної інфраструктури держави до функціонування в особливий період та в умовах воєнного стану;

організовує взаємодію суб’єктів забезпечення кібербезпеки в інтересах забезпечення кібероборони;

забезпечує розширення можливостей Збройних Сил України з ведення воєнних операцій з використанням кіберпростору;

забезпечує розвиток інфраструктури кібербезпеки, фінансове і матеріально-технічне забезпечення заходів кібербезпеки у Збройних Силах України.

4. Генеральний штаб Збройних Сил України:

бере участь у формуванні та реалізації державної політики кібербезпеки у воєнній сфері і сфері оборони;

прогнозує тенденції розвитку форм і способів воєнних дій у кіберпросторі та пов’язаних з ним засобів збройної боротьби;

здійснює розроблення та реалізує стратегію воєнної безпеки національного сегмента кіберпростору;

обґрунтовує напрями розвитку форм і способів оборони держави та боротьби з агресією у кіберпросторі;

організовує та координує заходи щодо кібербезпеки у воєнній сфері і сфері оборони та здійснює контроль за їх виконанням;

здійснює стратегічне планування застосування суб'єктів забезпечення кібербезпеки для оборони держави в кіберпросторі;

організовує стратегічне розгортання систем та комплексів кібербезпеки Збройних Сил України та інших суб'єктів забезпечення кібербезпеки постійної готовності для оборони держави та боротьби з агресією у кіберпросторі;

здійснює розроблення стратегії бойових дій і операцій в кіберпросторі;

здійснює керівництво обороною держави в кіберпросторі під час воєнного стану та в особливий період;

бере участь в організації та здійснює контроль за підготовкою об'єктів критичної інформаційної інфраструктури держави і національної системи кібербезпеки до оборони;

бере участь у забезпеченні кібербезпеки системи управління державою та здійснює контроль за її станом в особливий період;

здійснює міжнародне військове співробітництво, бере участь у виконанні спільних планових та оперативних дій в рамках міжнародних угод та договорів щодо кібербезпеки та кібероборони;

здійснює керівництво та забезпечує функціонування центрів захисту інформації та кібербезпеки в інтересах Міністерства оборони України та Збройних Сил України;

розробляє та впроваджує комплекс організаційних, режимних і технічних заходів щодо запобігання кібератакам на воєнні об'єкти, військову техніку та озброєння.

5. Служба безпеки України:

бере участь у формуванні та реалізації державної політики у сфері кібербезпеки;

створює у межах затвердженої чисельності та забезпечує функціонування підрозділу з протидії кібертероризму та кіберзагрозам у сфері державної безпеки;

здійснює контррозвідувальний захист інтересів держави у сфері кібербезпеки та контррозвідувальне забезпечення суб'єктів кібербезпеки;

вживає заходів з протидії кіберзагрозам державній безпеці або іншим життєво важливим інтересам держави;

бере участь в обмеженні та блокуванні доступу до ресурсів, які використовуються для організації, підготовки, вчинення, фінансування,

сприяння або приховування кібертероризму, а також в інших передбачених законами України випадках;

бере участь у розробленні критеріїв та порядку оцінки стану кіберзахисту об’єктів критичної інформаційної інфраструктури та проведенні цієї оцінки;

вживає заходів для забезпечення виконання міжнародних зобов’язань України у рамках протидії кіберзагрозам;

здійснює міжнародне співробітництво і взаємодіє з компетентними органами інших держав у рамках надання міжнародно-правової допомоги у протидії кіберзагрозам державній безпеці або іншим життєво важливим інтересам держави.

6. Державна служба спеціального зв’язку та захисту інформації України:

бере участь у формуванні та реалізації державної політики у сфері кібербезпеки;

розробляє критерії та порядок оцінки стану кіберзахисту об’єктів критичної інформаційної інфраструктури, забезпечує її організацію та проведення;

здійснює державний контроль за станом захисту інформації, яка циркулює на об’єктах критичної інформаційної інфраструктури;

створює у межах затвердженої чисельності та забезпечує функціонування підрозділу з питань оперативного реагування на кіберінциденти;

забезпечує функціонування системи захищеного доступу державних органів до Інтернету;

координує діяльність державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форми власності з питань запобігання, виявлення та усунення наслідків кіберінцидентів;

вживає організаційно-технічних заходів із збору та обліку інформації про кіберінциденти і кіберзагрози, узагальнює і надає таку інформацію суб’єктам забезпечення кібербезпеки постійної готовності відповідно до їх повноважень;

за результатами аналізу кіберінцидентів координує діяльність операторів, провайдерів телекомунікацій з питань забезпечення збереження ними необхідних даних про відповідні кіберінциденти в інтересах суб’єктів забезпечення кібербезпеки постійної готовності;

здійснює міжнародне співробітництво і взаємодіє з компетентними органами інших держав у рамках надання міжнародної технічної допомоги з питань кіберзахисту.

7. Розвідувальні органи України провадять розвідувальну діяльність з метою забезпечення визначених законом державних органів розвідувальною інформацією щодо кіберзагроз національній безпеці України, інших подій і обставин, що стосуються кібербезпеки, сприяння реалізації та захисту національних інтересів у кіберпросторі, а також беруть участь у протидії зовнішнім загрозам національній безпеці у кіберпросторі.

Стаття 9. Взаємодія суб'єктів забезпечення кібербезпеки

1. Суб'єкти забезпечення кібербезпеки:

1) взаємодіють з метою виявлення, запобігання і нейтралізації кіберзагроз, усунення передумов до їх виникнення та наслідків їх реалізації;

2) здійснюють інформаційний обмін в режимі реального часу з Радою національної безпеки і оборони України.

2. Порядок взаємодії суб'єктів забезпечення кібербезпеки під час здійснення заходів кібероборони, протидії кібертероризму та кіберзлочинності, а також запобігання, виявлення та усунення наслідків кібератак, регламентується спільними нормативно-правовими актами суб'єктів забезпечення кібербезпеки.

Стаття 10. Сприяння забезпеченню кібербезпеки України

1. Громадяни України, державні органи, органи місцевого самоврядування, підприємства, установи та організації, їх посадові особи зобов'язані сприяти забезпеченню кібербезпеки України.

2. Підприємства, установи та організації, які провадять діяльність, пов'язану із забезпеченням кіберзахисту в рамках надання інформаційних та/або телекомунікаційних послуг, у межах своїх повноважень розробляють і здійснюють запобіжні, режимні, організаційні, виховні та інші заходи, необхідні для виконання завдань щодо кібербезпеки.

Стаття 11. Відповідальність за порушення законодавства у сфері кібербезпеки

1. Особи, винні у порушенні законодавства у сфері кібербезпеки, несуть відповідальність згідно із законодавством.

Стаття 12. Фінансове забезпечення заходів кібербезпеки України

1. Фінансування робіт та заходів щодо забезпечення кібербезпеки здійснюється за рахунок коштів Державного бюджету України та місцевих

бюджетів, коштів суб’єктів відносин, пов’язаних із забезпеченням кібербезпеки.

Розділ III

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ

Стаття 13. Засади міжнародного співробітництва у сфері кібербезпеки

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами і спеціальними службами, а також з міжнародними організаціями.

Стаття 14. Подання інформації

1. Інформація з питань, пов’язаних із забезпеченням кібербезпеки, боротьбою з кіберзлочинністю та кібертероризмом, подається іноземній державі на підставі укладених Україною міжнародних договорів.

Розділ IV

КОНТРОЛЬ ЗА ЗАКОННІСТЮ ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України

1. Контроль за діяльністю суб’єктів забезпечення кібербезпеки здійснюється в порядку, визначеному Конституцією та законами України.

Розділ V

ПРИКІНЦЕВІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності з дня, наступного за днем його опублікування.

2. Внести зміни до таких законів України:

1) абзац шостий статті 1 Закону України “Про оборону України” (Відомості Верховної Ради України, 1992 р., № 9, ст. 106 із наступними змінами) викласти у такій редакції:

“блокада портів, узбережжя або повітряного простору, порушення комунікацій, сталого функціонування об’єктів критичної інформаційної інфраструктури України збройними силами іншої держави або групи держав;”;

2) у Законі України “Про правовий режим надзвичайного стану” (Відомості Верховної Ради України, 2000 р., № 23, ст. 176):

частину першу статті 6 доповнити пунктом 4^1 такого змісту:

“4^1) перелік заходів, пов’язаних з функціонуванням національного сегмента кіберпростору та об’єктів критичної інформаційної інфраструктури;”;

пункт 8 частини першої статті 18 викласти у такій редакції:

“8) особливі правила функціонування національного сегмента кіберпростору та об’єктів критичної інформаційної інфраструктури;”;

3) у Законі України “Про телекомунікації” (Відомості Верховної Ради України, 2004 р., № 12, ст. 155 із наступними змінами):

у статті 1:

доповнити статтю з урахуванням алфавітного порядку терміном такого змісту:

“контент-провайдер — суб’єкт господарювання, який надає інформаційні та інші послуги через мережі операторів та провайдерів телекомунікацій;”;

визначення терміна “телекомунікаційна послуга (послуга)” після слів “провайдера телекомунікацій” доповнити словом “, контент-провайдера”;

у статті 39:

назву статті викласти у такій редакції:

“Стаття 39. Обов’язки операторів і провайдерів телекомунікацій та контент-провайдерів”;

у частині другій:

абзац перший після слів “провайдерів телекомунікацій” доповнити словом “, контент-провайдерів”;

абзац другий викласти у такій редакції:

“Оператори, провайдери телекомунікацій та контент-провайдери у встановленому законом порядку зберігають та надають інформацію для ідентифікації постачальників послуг і маршруту, яким було передано інформацію про з’єднання свого абонента, у порядку, встановленому законом.”;

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

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

видати нормативно-правові акти, що випливають із цього Закону;

забезпечити перегляд і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів,

що суперечать цьому Закону, видання зазначеними органами актів, що випливають із цього Закону.

Голова
Верховної Ради України