Запропоновані зміни до Проекту Закону України “Про основні засади забезпечення кібербезпеки України” (**версія від ГО «ІСАКА Київ» від вересня 2015**)

Розділ І

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Статтю 1 викласти в такій редакції.

Стаття 1. Визначення термінів

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

1) Комп’ютерна система - будь-який пристрій або група взаємно поєднаних або пов’язаних пристроїв, один чи більш з яких, відповідно до певної програми, виконує автоматичну обробку даних;

2) Комп’ютерні дані – будь-яке представлення фактів, інформації або концепції у формі, яка є придатною для обробки у комп’ютерні системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп’ютерною системою;

3) Постачальник послуг - будь-яка державна або приватна установа, яка надає користувачам своїх послуг можливість комунікацій за допомогою комп'ютерної системи, та будь-яка інша установа, яка обробляє або зберігає комп'ютерні дані від імені такої комунікаційної послуги або користувачів такої послуги;

4) Дані про рух інформації - будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, що складала частину ланцюга комунікації, і які зазначають походження, кінцевий пункт, маршрут, час, дату, розмір і тривалість комунікації або тип основної послуги;

5) Кібернетичний простір (кіберпростір) - це віртуальний простір, який створюється за допомогою апаратного і програмного забезпечення, інформаційних систем, електромагнітного спектра (включаючи телекомунікаційні мережі та Інтернет) і відповідних фізичних інфраструктур, а також користувачів та відносин між ними;

6) Кібернетична безпека (кібербезпека) – стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави при використанні кіберпростору;

7) Кібернетична загроза (кіберзагроза) – наявні та потенційно можливі явища і чинники, що загрожують кібербезпеці;

8) Кібернетичний злочин (кіберзлочин) – суспільно небезпечне винне діяння з використанням кіберпростору, передбачене законодавством України про кримінальну відповідальність;

9) Кібернетична злочинність (кіберзлочинність) – сукупність кіберзлочинів;

10) Кібернетичний тероризм (кібертероризм) – злочини, що вчиняються з терористичною метою з використанням кібернетичного простору.

11) Кібернетична атака (кібератака) – несанкціоновані дії в кіберпросторі, спрямовані на порушення конфіденційності, цілісності і доступності інформації;

12) Кібернетичний інцидент (кіберінцидент) – подія, пов’язана з реалізацією або спробою реалізації кібератаки в кіберпросторі;

13) Кібернетичний захист (кіберзахист) – сукупність заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру, спрямованих на забезпечення кібербезпеки, включаючи попередження кібернетичних загроз, протистояння кібератакам, та відновлення та усунення наслідків кібернетичних інцидентів;

14) Національний сегмент кіберпростору (кіберпростір України) – кіберпростір, що належить до юрисдикції України;

15) Об’єкт критичної інформаційної інфраструктури (об’єкти киберзахисту) – елемент(и) національного сегменту кіберпростору, порушення сталого функціонування яких(ого) матиме негативний вплив на стан національної безпеки і оборони України, включаючи також економічну безпеку держави та здоров’я громадян

16) Суб’єкти забезпечення кібербезпеки – юридичні та фізичні особи які здійснюють діяльність, пов’язану із забезпеченням безпеки національного сегмента кіберпростору, у тому числі в рамках надання безоплатних інформаційних та/або телекомунікаційних послуг;

17) 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 вирішення завдань забезпечення кібербезпеки.

18) Система забезпечення кібербезпеки – внутрішня організація роботи суб’єктів забезпечення кібербезпеки, у тому числі їх організаційна структура, процеси, вимоги до культури та етики, професіоналізму, компетенції виконавців, інфраструктура, послуги та програмні додатки для підтримки діяльності системи, політики, методології, процедури, інструкції, облік та керування інформацією (даними).

19) Національна система кібербезпеки – сукупність суб’єктів забезпечення кібербезпеки та суб’єктів кібербезпеки постійної готовності , а також взаємоузгоджених заходів кіберзахисту, що здійснюються ними.

20) Галузевий регулятор з кібербезпеки – державний або недержавний орган, створений для розробки вимог та рекомендацій забезпечення кібербезпеки у відповідній (державній або недержавній) галузі;

21) Галузеві центри реагування з кібербезпеки – спеціальні структурні підрозділи галузевих регуляторів з кібербезпеки, які уповноважені забезпечувати реагування на інциденти кібербезпеки та відновлення сталого функціонування кібернетичного простору, виконувати обмін інформацією з суб’єктами забезпечення кібербезпеки та суб’єктами забезпечення кібербезпеки постійної готовності щодо загроз та атак кібербезпеки;

22) Незалежні аудитори та/або експерти – міжнародні аудиторські організації, або експерти, професійний рівень яких підтверджено відповідними сертифікатами міжнародного зразку в галузі аудиту інформаційної безпеки, забезпечення кібербезпеки, управління інформаційними технології;

23) Використання терористами кіберпростору - специфічні дії терористичних організацій та їх послідовників в кіберпросторі, спрямовані на пропаганду, збір пожертв, радикалізацію та залучення волонтерів, комунікацію та інші дії для реалізації мети терористичних дій;

24) Кібернетична операція (кібероперація) – комплекс заходів в інформаційному просторі, котрі проводяться під час військових, розвідувальних, правоохоронних дій, та підтримують досягнення їх мети.

25) Військові дії в кіберпросторі (кібервійна) – сукупність узгоджених і взаємопов’язаних за метою, завданнями, місцем і часом спільних дій військових та інших формувань, спрямованих на досягнення воєнно-технологічної переваги у кіберпросторі;

Статтю 2 викласти в такій редакції.

Стаття 2. Правова основа забезпечення кібербезпеки України

1. Правову основу забезпечення кібернетичної безпеки України становлять Конституція України, Кримінальний кодекс України, Кодекс України про адміністративні правопорушення, *Конвенція про кіберзлочинність*, цей та інші закони України, міжнародні договори, згода на обов’язковість яких надана Верховною Радою України, *конвенції, ратифіковані Верховною Радою України*, а також видані на виконання законів інші нормативно-правові акти України.

Розділ ІІ

ОРГАНІЗАЦІЙНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ  
КІБЕРБЕЗПЕКИ УКРАЇНИ

Статтю 3 викласти в такій редакції.

### 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;
* *відповідності актуальним потребам підприємств та громадян;*
* *дієвості, постійності та комплексного підходу до впровадження правових, організаційних, технічних та інформаційних заходів забезпечення кібербезпеки;*
* *ефективності роботи систем забезпечення кібербезпеки;*
* пріоритетності запобіжних заходів;
* *невідворотності відповідальності за вчинення кіберзлочинів;*
* *забезпечення відновлення порушених прав і законних інтересів, відшкодування збитків, шкоди, завданої кіберзлочинами;*
* *партнерства держави, приватного сектору та участі інституцій громадянського суспільства як суб’єктів у забезпеченні кібербезпеки держави;*
* відповідальності суб'єктів забезпечення кібербезпеки за належне функціонування об’єктів кіберзахисту;
* *розділення функцій виконання заходів із підвищення кібернетичної безпеки та контролю їх дієвості;*
* *ефективного контролю з боку громадянського суспільства за діяльністю суб'єктів забезпечення кібернетичної безпеки та аудиту кібернетичної безпеки;*
* співпраці на міжнародному рівні з метою вироблення єдиних підходів та ефективної взаємодопомоги з питань протидії кіберзагрозам;
* *пріоритетного використання міжнародних підходів, настанов та стандартів щодо впровадження та контролю кібернетичної безпеки;*
* *використання ризик-орієнтованого та фінансово-економічно обґрунтованого підходу до використання ресурсів, необхідних для впровадження кібернетичної безпеки (збалансованість ризиків та відповідних механізмів кіберзахисту);*
* *постійного підвищення рівня освіченості широких верств населення щодо ризиків та механізмів забезпечення кібернетичної безпеки, їх прав та обов’язків;*
* *ефективності системи кібернетичної безпеки по всій території України, у тому числі у зонах стихійного лиха, військових та антитерористичних дій, тимчасово окупованої території України;*
* *відповідальності керівництва держави за ефективність національної системи кібернетичного захисту;*
* координації заходів, які здійснюються для забезпечення кібербезпеки суб’єктами забезпечення кібербезпеки відповідно до їх призначення (специфіки діяльності) та повноважень;
* співробітництва структур державного і приватного секторів на національному та міжнародному рівнях з метою забезпечення адекватної відповіді кіберзагрозам;
* пріоритетності 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;

Статтю 4 викласти в такій редакції.

### 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 забезпечення 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 світових, європейських та регіональних системах забезпечення кібербезпеки;
* дотримання міжнародних зобов’язань щодо боротьби з кіберзлочинністю та кібертероризмом;
* протидія використанню терористами Інтернет;створення можливостей в державних органах для проведення кібернетичних операцій;
* забезпечення контролю придбання та використання програмного та апаратного забезпечення, послуг в державних органах та на об’єктах критичної інфраструктури з точки зору зменшення ризиків кібернетичної безпеки;
* обмеження використання іноземних веб-додатків співробітниками українських державних органів (поштових скриньок, соціальних мереж, використання лічильників, банерів, та інших елементів кіберпростору); встановлення пріоритетності використання послуг для державних органів та об’єктів критичної інфраструктури, що знаходяться в національному сегменті кіберпростору;
* запровадження ризик-орієнтованої методології управління заходами кібернетичної безпеки;
* врахування галузевих особливостей при створенні галузевих нормативних документів з кібернетичної безпеки;
* запровадження механізму громадського контролю ефективності (аудиту) заходів кібернетичної безпеки а також відповідних видатків, спрямованих на забезпечення кібербезпеки на (в) об’єктах критичної інформаційної інфраструктури, (включаючи такі заходи, зміст яких є державною таємницею) та забезпечення прав громадян під час реалізації цих заходів.
* стимулювання розвитку співробітництва в сфері забезпечення кібербезпеки на національному і міжнародному рівнях;
* адаптація законодавства України до загальноприйнятих міжнародних норм, 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 виконання на об’єктах 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 і загроз у кіберпросторі;
* введення до класифікатора професій професії "Аудитор інформаційних технологій" та «спеціаліст з кібернетичної безпеки»;створення стандартів аудиту кібербезпеки на об’єктах критичної інформаційної інфраструктури;запровадження заходів, що забезпечують контрольоване державою безперервне розповсюдження інформації у зонах військових дій, надзвичайного стану, антитерористичних операцій, стихійних лих та інших постраждалих районах;запровадження програми обов’язкової атестації держслужбовців, що відповідають за безпеку національного кіберпростору, на володіння сучасними практиками кібербезпеки;
* впровадження системи управління системою забезпечення кібербезпеки відповідно до міжнародних стандартів та кращих світових практик на об’єктах критичної інформаційної інфраструктури та в органах державної влади;
* розробка програми навчання та підготовки спеціалістів із проведення кібернетичних операцій та ведення військових дій в кіберпросторі;
* впровадження стандартів безпечної конфігурації та використання програмного забезпечення на об’єктах критичної інформаційної інфраструктури та в органах державної влади.

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 та держави.

Статтю 5 викласти в такій редакції

### Стаття 5. Об’єкти кіберзахисту

1. Об’єктами кіберзахисту державних органів є таки об’єкти, які визначені «Порядком визначення об’єктів кіберзахисту державних органів». Перелік цих об’єктів затверджуються Кабінетом Міністрів України.
2. Галузеві регулятори з кібербезпеки визначають об'єкти критичної інфраструктури на підприємствах у галузях, які вони регулюють.
3. Галузі, що містять об’єкти кіберзахисту є:

* енергетика (генерація, передача та розподіл, включаючи ядерні та інші електростанції, транспортні та розподільні мережі та ін.);
* хімічна промисловість;
* газовидобування, транспортування, зберігання та розподіл;
* інфраструктура та транспорт;
* телекомунікації;
* фінансовий сектор;
* медіа сектор;
* промисловість;
* сільське господарство та виготовлення продуктів харчування;
* охорона здоров’я;
* водні ресурси, водоочисні споруди та дамби;
* воєнно-промисловий комплекс.

Статтю 6 викласти в такій редакції

### Стаття 6. Захист об’єктів кіберзахисту

1. Захист об’єктів кіберзахисту від кібератак забезпечується відповідно до вимог міжнародних стандартів та кращих практик із кібербезпеки (NIST Framework for Improving Critical Infrastructure Cybersecurity або відповідних стандартів та кращих практик) та нормативних документів, розроблених Галузевими регуляторами з кібербезпеки.
2. Відповідальність за впровадження кіберзахисту об’єкта кібербезпеки покладається на його власника та уповноваженний ним орган (наглядова рада).
3. Власник об’єкта кібербезпеки незалежно від форми власності зобов’язаний:

* проводити незалежні аудити ефективності системи кіберзахисту з залученням незалежних аудиторів та/або експертів які мають рівень квалификації, підтверджений сертифікатами міжнародного зразка з кібербезпеки, інформаційної безпеки або аудиті інформаційних технологій;
* надавати суб’єктам забезпечення кібербезпеки постійної готовності, в установленому законодавством України порядку, відомості про власні об’єкти критичної інформаційної інфраструктури;
* призначити члена наглядової ради (в разі, якщо підприємство має наглядову раду), та керівника підприємства або його заступника, відповідальним за кібербезпеку;створити в своїй структурі підрозділ забезпечення кібербезпеки або уповноважувати окремих осіб чи організації виконувати функції такого підрозділу та забезпечувати їх функціонування. Такий підрозділ має підпорядковуватися безпосередньо особі, відповідальній за кібербезпеку;
* створити в своїй структурі підрозділ внутрішнього аудиту кібербезпеки, або уповноважувати окремих осіб чи організації виконувати функції такого підрозділу, забезпечити їх функціонування. Такий підрозділ має підпорядковуватися безпосередньо керівнику організації, звітувати власнику та/або уповноваженому ним органу,та галузевому регулятору з кібербезпеки відповідної галузі;
* організувати негайне інформування галузевого центра реагування та обміну інформацією з кібербезпеки та відповідного цій галузі суб’єкта забезпечення кібербезпеки постійної готовності про спроби вчинення кібератак та інших несанкціонованих дій стосовно об’єктів кібербезпеки, а також здійснювати заходи щодо блокування, усунення або локалізації їх негативних наслідків.

1. Незалежні аудитори та експерти звітують власникам об’єктів критичної інформаційної інфраструктури, відповідальним за кібербезпеку на підприємстві, галузевим регуляторам з кібербезпеки відповідних галузей та суб’єктам забезпечення кібербезпеки постійної готовності щодо результатів аудиту.

Статтю 7 викласти в такій редакції

### Стаття 7. Національна система кібербезпеки

1. Національна система кібербезпеки забезпечує захист життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі.
2. Основою національної системи кібербезпеки є всі суб’єкти забезпечення кібербезпеки.
3. Оперативне управління та координація діяльності суб’єктів забезпечення кібербезпеки здійснюється Національним центром кібернетичної безпеки при Президентові України.
4. Вищі навчальні та наукові заклади проводять підготовку фахівців та фундаментальні дослідження у напрямках кібернетичної безпеки

Статтю 8 викласти в такій редакції

*Стаття 8. Суб’єкти забезпечення кібербезпеки*

1. *Національний центр кібернетичної безпеки при Президентові України:*

* *розробляє Стратегію забезпечення кібернетичної безпеки України;*
* *затверджує перелік Галузевих регуляторів з кібербезпеки та Суб’єктів забезпечення кібербезпеки постійної готовності;*
* *здійснює управління та координацію роботи Суб’єктів забезпечення кібернетичної безпеки постійної готовності;*
* *координує проведення кібернетичних операцій за участю Суб’єктів забезпечення кібернетичної безпеки постійної готовності та Галузевих центрів реагування з кібербезпеки;*
* *розробляє рекомендації з кібербезпеки за участю Галузевих регуляторів з кібербезпеки;*
* *структура, повноваження, організація діяльності, питання кадрового, фінансового та іншого ресурсного забезпечення Національного центру кібернетичної безпеки при Президентові України регулюються «Положенням про Національний центр кібернетичної безпеки при Президентові України».*
* *організовує розгортання та функціонування системи оперативної взаємодії між суб’єктами забезпечення кібербезпеки постійної готовності, галузевими центрами реагування з кібербезпеки;*
* *проводить аналіз стану кібербезпеки і можливих кіберзагроз національній безпеці України та узагальнює міжнародний досвід щодо формування та реалізації державної політики у сфері кібербезпеки;*
* *визначає стратегічні напрями державної політики у сфері кібербезпеки*
* *визначає методику та процес управління ризиками кібербезпеки на національному рівні, а також цільові показники прийнятного рівня ризиків, якості та ефективності заходів кібернетичної безпеки;*
* *визначає, відповідно до законодавства України, загальнодержавні методологію, стандарти, моделі процесів, вимоги до управління кібернетичною безпекою, ризиками кібернетичних атак, технічних засобів забезпечення кібернетичної безпеки, налаштувань безпеки для програмного і апаратного забезпечення інформаційних систем, центрів обробки даних, кваліфікації спеціалістів із кібернетичної безпеки, штатних структур із забезпечення кібербезпеки;*
* *координує проведення інвентаризації та класифікації даних органів держаної влади та об’єктів критичної інформаційної інфраструктури;*
* *координує проведення заходів із підвищення рівня обізнаності та культури кібернетичної безпеки;*
* *готує пропозиції та розробляє спільно з суб’єктами забезпечення кібербезпеки постійної готовності сценарії реагування на кіберзагрози, рекомендації щодо протидії ним;*
* *формує пропозиції щодо підготовки кадрів у сфері кібербезпеки;*
* *координує розробку 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 вищих органів державної влади у сфері кібербезпеки.*

1. *Рада національної безпеки і оборони України:*

* *узгоджує Стратегію забезпечення кібернетичної безпеки України;*
* *аналізує стан кібербезпеки і можливі кіберзагрози національній безпеці України та узагальнює міжнародний досвід щодо формування та реалізації політики у сфері кібербезпеки;*
* *аналізує звіти Національного центру кібернетичної безпеки при Президентові України щодо стану виконання державними органами галузевих програм і заходів, пов'язаних із реалізацією державної політики у сфері кібербезпеки та використовує їх у своєї роботі.*

1. *Галузеві регулятори з кібербезпеки:*

* *відповідають за розробку галузевих рекомендацій, вимог, стандартів та нормативних документів, які обов’язкові до виконання у відповідній галузі;*
* *забезпечують контроль виконання вимог, стандартів та нормативних документів за допомогою залучення незалежних аудиторів або експертів, які проводять перевірки їх виконання;*
* *звітують Національному центру кібернетичної безпеки при Президентові України щодо стану кібербезпеки відповідної галузі.*

1. *Міністерство внутрішніх справ України:*

* *бере участь у формуванні та реалізації державної політики у сфері кібербезпеки;*
* *створює і забезпечує функціонування підрозділу з протидії кіберзлочинності;*
* *розроблює 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 при 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 зі збору та обліку інформації про кіберінциденти, кіберзагрози і результати діяльності з протидії кіберзлочинності, узагальнює і надає таку інформацію суб'єктам забезпечення кібербезпеки постійної готовності відповідно до їх повноважень;*
* *у встановленому законом України порядку забезпечує 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;*
* *проводить профілактику кіберзлочинів та бере участь у профілактиці злочинів, які вчиняються з використанням інформаційно-телекомунікаційних систем та їх ресурсів;*
* *проводить у встановленому законом порядку кібернетичні операції для протидії використанню інформаційно-телекомунікаційних систем та їх ресурсів у злочинах;*
* *проводить у встановленому законом порядку дослідження інформаційно-телекомунікаційних систем та їх ресурсів для протидії злочинам.*

1. *Міністерство оборони України:*

* *бере участь у формуванні та реалізації державної політики кібербезпекиу воєнній сфері і сфері оборони;*
* *здійснює аналіз воєнно-політичної обстановки та визначає рівень воєнної загрози національній безпеці України через використання кіберпростору;*
* *здійснює аналіз, прогнозування та оцінку рівня кіберзагроз воєнного характеру;*
* *здійснює планування та реалізацію 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, під час проведення антитерористичних операції, окупації 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.*

1. *Генеральний штаб Збройних Сил України:*
2. *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;*
3. *здійснює розробку стратегії бойових дій і операцій в кіберпросторі;*
4. *здійснює керівництво обороною держави в кіберпросторі під час воєнного стану та в особливий період;*
5. *здійснює загальне керівництво та координацію дій суб’єктів кібернетичної безпеки у сфері кібернетичної оборони держави та боротьби з кібернетичною агресією;*
6. *бере участь у забезпеченні кібербезпеки системи управління державою та контролює її стан в особливий період;*
7. *здійснює міжнародне військове співробітництво, бере участь у виконанні спільних планових та оперативних дій у рамках міжнародних угод та договорів щодо кібербезпеки та кібероборони;*
8. *здійснює керівництво та забезпечує функціонування центрів захисту інформації та кібербезпеки в інтересах Міністерства оборони України та Збройних Сил України;*
9. *розробляє та впроваджує комплекс організаційних, режимних і технічних заходів щодо запобігання кібератакам на воєнні об’єкти, військову техніку та озброєння;*
10. *провадить в кіберпросторі розвідувальну та інформаційно-аналітичну діяльність з метою підтримання бойової готовності Збройних Сил України, для чого має у своєму складі відповідний структурний підрозділ;*
11. *організовує підготовку Збройних Сил України до виконання дій та завдань у кіберпросторі, здійснює координацію і контроль підготовки інших військових формувань, утворених відповідно до законів України, правоохоронних органів та центрального органу виконавчої влади з питань організації спеціального зв’язку та захисту інформації до виконання завдань з кібернетичної оборони України;*
12. *організовує розробку та впровадження заходів з досягнення Збройними Силами України військово-технологічної переваги у кіберпросторі;*
13. *бере участь у формуванні та реалізації державної політики кібербезпеки у воєнній сфері і сфері оборони;*
14. *прогнозує тенденції розвитку форм і способів воєнних дій у кіберпросторі та пов’язаних з ним засобів збройної боротьби;*
15. *здійснює розробку та реалізує стратегію воєнної безпеки національного сегмента кіберпростору;*
16. *здійснює стратегічне планування застосування суб’єктів забезпечення кібербезпеки для оборони держави в кіберпросторі;*
17. *бере участь в організації та контролює підготовку об’єктів критичної інформаційної інфраструктури держави і національної системи кібербезпеки до оборони;*
18. *організовує використання національної системи кібербезпеки в інтересах оборони, здійснює відповідно до закону управління та регулювання в сфері використання ресурсу кібернетичної безпеки, виділеного для цілей оборони;*
19. *бере участь в організації контролю стану кібернетичної безпеки національного сегменту кіберпростору.*

*7. Служба безпеки України:*

1. *бере участь у формуванні та реалізації державної політики у сфері кібербезпеки;*
2. *створює 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;*
3. *бере участь у розробленні критеріїв та порядку оцінки стану кіберзахисту об’єктів критичної інформаційної інфраструктури та має можливість брати участь у проведенні цієї оцінки;*
4. *вживає заходів з протидії кіберзагрозам державній безпеці або іншим життєво важливим інтересам держави;*
5. *створює і забезпечує функціонування підрозділу з протидії кібертероризму;*
6. *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;вживає заходів для забезпечення виконання міжнародних зобов’язань України у рамках протидії кіберзагрозам та використанню терористами кіберпростору;*
7. *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;*
8. *проводить профілактику кіберзлочниів та бере участь у профілактиці злочинів проти держави, які вчиняються з використанням інформаційно-телекомунікаційних систем та їх ресурсів;*
9. *проводить у встановленому законом порядку кібернетичні операції для протидії використанню інформаційно-телекомунікаційних систем та їх ресурсів у злочинах проти держави.*
10. *Державий орган, на який покладені завдання забезпечення державної системи урядового зв’язку, криптографічного та технічного захисту інформації в державних органах:*
11. *бере участь та реалізації державної політики у сфері кібербезпеки;*
12. *створює та забезпечує функціонування підрозділу з питань оперативного реагування на кіберінциденти, включаючи кіберінциденти в сфері автоматизації управління виробництвом та промислової автоматики;*
13. *забезпечує функціонування системи захищеного доступу органів державної влади до сервісів в кіберпросторі;*
14. *координує діяльність державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форми власності з питань попередження, виявлення та усунення наслідків кіберінцидентів;*
15. *вживає організаційно-технічних заходів зі збору та обліку інформації про кіберінциденти і кіберзагрози, узагальнює і надає таку інформацію суб'єктам забезпечення кібербезпеки постійної готовності відповідно до їх повноважень а також здійснює оперативне інформування та обмін інформацією про кіберінциденти і кіберзагрози із Галузевими центрами реагування та обміну інформацією з кібербезпеки;*
16. *розробляє порядок віднесення об’єктів до критичної інформаційної інфраструктури на основі кількісних та якісних показників, у відповідності до методик, розроблених організацією ENISA;*
17. *організовує та координує проведення щорічного загальнонаціонального випробування та навчання щодо надзвичайних ситуацій та інцидентів в сфері кібербезпеки;*
18. *принаймні два рази на рік проводить наради з Галузевими регуляторами з кібербезпеки та інформаційних технологій та Галузевими центрами реагування та обміну інформацією з кібербезпеки для обговорення поточного стану забезпечення кібербезпеки об’єктів критичної інфраструктури та поточних загроз;*
19. *активно залучає волонтерів та незалежних експертів, рівень кваліфікації яких підтверджено відповідними міжнародними сертифікатами, до роботи в державних органах в сфері кіберзахисту, та сприяє прискореному отриманню такими експертами необхідних дозволів та доступу до державної таємниці, якщо це необхідно;*
20. *проходить щорічний незалежний аудит за міжнародними стандартами щодо ефективності забезпечення кібербезпеки, та звітує відповідному комітету Верховної Ради стосовно результатів цього аудиту та стану забезпечення кібербезпеки держави;*
21. *здійснює міжнародне співробітництво і взаємодіє з компетентними органами інших держав у рамках надання міжнародної технічної допомоги з питань кіберзахисту;*
22. *розробляє технічні засоби та надає іншим державним органам допомогу для проведення кібернетичних операцій та криміналістичних досліджень;*
23. *підтримує реєстр ризиків кіберзагроз державного рівня та координує створення реєстрів ризиків у інших державних органах та розпорядниках критичної інфраструктури;*
24. *надає методологічну та іншу допомогу Галузевим центрам реагування на кібератаки, а також малому та середньому бізнесу щодо забезпечення кібербезпеки, реагування на інциденти та відновлення роботи систем.*
25. *Спеціально уповноважені законодавством України на здійснення розвідувальної діяльності органи:*

* *здійснюють розвідувальну діяльність щодо кіберзагроз, інших подій і обставин, що стосуються кібербезпеки;*
* *сприяють реалізації та захисту національних інтересів у кіберпросторі;*
* *приймають участь у забезпеченні реалізації інтересів держави, громадян, корінних народів та підприємств України у кіберпросторі.*

### Статтю 9 викласти в такій редакції

### Стаття 9. Взаємодія суб’єктів забезпечення кібербезпеки

1. Суб’єкти забезпечення кібербезпеки:

* взаємодіють з метою виявлення, запобігання і нейтралізації кіберзагроз, усунення передумов до їх виникнення та наслідків їх реалізації, проведення розслідувань кіберінцидентів;
* здійснюють інформаційний обмін з Національним центром кібернетичної безпеки при Президентові України;

1. Порядок взаємодії суб’єктів забезпечення кібербезпеки під час підготовки та здійснення кібероборони, запобігання, виявлення та усунення наслідків кібертероризму встановлюється Національним центром кібернетичної безпеки при Президентові України.

### 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.

### Статтю 12 викласти в такій редакції

### Стаття 12. Фінансове забезпечення заходів кібербезпеки України

1. Фінансування робіт та заходів щодо забезпечення кібербезпеки здійснюються:

* на державних підприємствах, установах та організаціях - за рахунок коштів Державного бюджету України;
* місцевих органів влади, комунальних підприємств – за рахунок місцевих бюджетів;
* інших – за власний рахунок.

# Розділ ІІІ

# 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

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

# Розділ IV

# КОНТРОЛЬ ЗА ЗАКОННІСТЮ ТА ДІЄВІСТЮ ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Статтю 15 викласти в такій редакції

### Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України

1. Комітет з Інформаційних Технологій Верховної Ради України, із залученням громадських організацій та незалежних експертів розробляє механізми громадського контролю ефективності заходів кібернетичної безпеки (включаючи такі заходи, зміст яких є державною таємницею) та забезпечення прав громадян під час реалізації цих заходів.

2. Всі Суб’єкти забезпечення кібербезпеки постійної готовності проходять щорічний незалежний аудит за міжнародними стандартами щодо ефективності забезпечення кібербезпеки, та звітує Комітету з Інформаційних Технологій Верховної Ради України та Суб’єктам забезпечення кібербезпеки постійної готовності стосовно результатів цього аудиту та стану забезпечення кібербезпеки держави.

# Розділ V

# ПРИКІНЦЕВІ ПОЛОЖЕННЯ

Розділ V викласти в такій редакції

1. Цей Закон набирає чинності з дня, наступного за днем його опублікування.
2. Внести зміни до таких законодавчих актів 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;”;*

1. У Законі України “Про телекомунікації” (Відомості Верховної Ради України, 2004 р., № 12, ст. 155, № 48, ст. 526; 2010 р., № 34, ст. 482, № 38, ст. 504):

назву статті 29 та частину першу викласти у такій редакції:

*Стаття 29. Оперативно-технічне управління телекомунікаційними мережами загального користування в період надзвичайних ситуацій, надзвичайного та воєнного стану*

*1. Управління телекомунікаційними мережами загального користування та відповідальність за забезпечення їх сталості в період надзвичайних ситуацій, надзвичайного та воєнного стану покладається на Генеральний Штаб Збройних Сил України».*

 у Законі України “Про правовий режим надзвичайного стану”:

частину першу статті 6 після пункту 4 доповнити новим пунктом такого змісту:

*«перелік заходів, пов’язаних з функціонуванням національного сегмента кібернетичного простору та об'єктів критичної інформаційної інфраструктури»;*

У зв’язку з цим пункти 5 та 6 вважати відповідно пунктами 6 та 7;

пункт 8 статті 18 викласти у такій редакції:

*“ особливі правила функціонування національного сегмента кібернетичного простору та об'єктів критичної інформаційної інфраструктури”;*

 абзац третій статті 1 Закону України “Про оборону” (Відомості Верховної Ради України, 1992, № 9, ст.106) 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;”.*

у статті 39:

назву статті викласти у такій редакції:

*“Стаття 39. Обов’язки операторів і провайдерів телекомунікацій ”;*

у частині другій:

абзац другий викласти у такій редакції:

*“Оператори, та провайдери телекомунікацій у встановленому законом порядку, за поданням прокуратури починають зберігати, а за рішенням суду надавати суб’єктам забезпечення кібернетичної безпеки постійної готовності інформацію для ідентифікації постачальників послуг і маршруту, яким було передано інформацію про з’єднання свого абонента. При цьому мають виконуватися наступні вимоги:*

*виконання вимог Конвенції про кіберзлочинність, ратифікованої Верховною Радою України;*

*принцип «пропорційності» - обсяг запиту на перехоплення інформації (та/або обмеження чи блокування доступу) має бути спів розмірний злочину, в якому звинувачують суб’єкта перехоплення інформації;*

*заборона вивідування інформації без надання відповідного обґрунтування;*

*обмеження терміну зберігання інформації – 60 днів, та обов’язкове знищення цієї інформації після закінчення цього терміну;*

*обов’язкове інформування всіх суб’єктів перехоплення інформації, що їх інформація перехоплювалася, після передачі доказової бази до суду;*

*розробка та впровадження організаційно-технічних можливостей для забезпечення громадського контролю та протидії зловживанню пов’язаному з перехопленням інформації державою та операторами зв’язку (включаючи обов’язкове автоматичне інформування прокуратори та судових інстанцій при включенні функцій зберігання чи перехоплення інформації в інформаційних та телекомунікаційних системах);*

*створення громадської комісії для контролю дій пов’язаних з перехопленням та вилученням цифрових даних;*

*можливість проникнення та криміналістичне дослідження інформаційних систем, які терористи використовують під час своєї діяльності;*

*заборона конфіскації серверів у операторів та провайдерів телекомунікацій.*

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

* привести свої 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.