**1. ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА, ДЕРЖАВНІ ТА МІЖНАРОДНІ ВИМОГИ, ПРАКТИКИ І СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА/АБО КІБЕРБЕЗПЕКИ**

***1.1. Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки.***

*1.1.1. ЗУ «Про інформацію», «Про науково-технічну інформацію»*

ЗУ Про інформацію

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

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

документ - матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

суб'єкт владних повноважень - орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень.

Стаття 2. Основні принципи інформаційних відносин

1. Основними принципами інформаційних відносин є:

гарантованість права на інформацію;

відкритість, доступність інформації, свобода обміну інформацією;

достовірність і повнота інформації;

свобода вираження поглядів і переконань;

правомірність одержання, використання, поширення, зберігання та захисту інформації;

захищеність особи від втручання в її особисте та сімейне життя.

Стаття 3. Державна інформаційна політика

1. Основними напрямами державної інформаційної політики є:

забезпечення доступу кожного до інформації;

забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

створення умов для формування в Україні інформаційного суспільства;

забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

створення інформаційних систем і мереж інформації, розвиток електронного урядування;

постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

забезпечення інформаційної безпеки України;

сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Стаття 4. Суб'єкти і об'єкт інформаційних відносин

1. Суб'єктами інформаційних відносин є:

фізичні особи;

юридичні особи;

об'єднання громадян;

суб'єкти владних повноважень.

2. Об'єктом інформаційних відносин є інформація.

**Стаття 5.** Право на інформацію

1. Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

**Стаття 6.**Гарантії права на інформацію

1. Право на інформацію забезпечується:

створенням механізму реалізації права на інформацію;

створенням можливостей для вільного доступу до статистичних даних, архівних, бібліотечних і музейних фондів, інших інформаційних банків, баз даних, інформаційних ресурсів;

обов'язком суб'єктів владних повноважень інформувати громадськість та медіа про свою діяльність і прийняті рішення;

обов'язком суб'єктів владних повноважень визначити спеціальні підрозділи або відповідальних осіб для забезпечення доступу запитувачів до інформації;

здійсненням державного і громадського контролю за додержанням законодавства про інформацію;

встановленням відповідальності за порушення законодавства про інформацію.

2. Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

**Стаття 7.**Охорона права на інформацію

1. Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації.

2. Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом.

Суб'єкт інформаційних відносин може вимагати усунення будь-яких порушень його права на інформацію.

3. Забороняється вилучення і знищення друкованих видань, експонатів, інформаційних банків, документів з архівних, бібліотечних, музейних фондів, крім встановлених законом випадків або на підставі рішення суду.

4. Право на інформацію, створену в процесі діяльності фізичної чи юридичної особи, суб'єкта владних повноважень або за рахунок фізичної чи юридичної особи, Державного бюджету України, місцевого бюджету, охороняється в порядку, визначеному законом.

**Стаття 8.**Мова інформації

1. Мову інформації визначають [Закон України](https://zakon.rada.gov.ua/laws/show/2704-19) "Про забезпечення функціонування української мови як державної", інші закони України та міжнародні договори, згода на обов’язковість яких надана Верховною Радою України.

**Стаття 9.**Основні види інформаційної діяльності

1. Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

**Розділ II**  
**ВИДИ ІНФОРМАЦІЇ**

**Стаття 10.**Види інформації за змістом

За змістом інформація поділяється на такі види:

інформація про фізичну особу;

інформація довідково-енциклопедичного характеру;

інформація про стан довкілля (екологічна інформація);

інформація про товар (роботу, послугу);

науково-технічна інформація;

податкова інформація;

правова інформація;

статистична інформація;

соціологічна інформація;

критична технологічна інформація;

*{Статтю 10 доповнено новим абзацом згідно із Законом*[*№ 1882-IX від 16.11.2021*](https://zakon.rada.gov.ua/laws/show/1882-20#n406)*}*

інші види інформації.

**Стаття 11.**Інформація про фізичну особу

1. Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

2. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом.

Центральний орган виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, під час здійснення повноважень щодо верифікації та моніторингу державних виплат не потребує згоди фізичних осіб на отримання та обробку персональних даних.

*{Частину другу статті 11 доповнено абзацом третім згідно із Законом*[*№ 1774-VIII від 06.12.2016*](https://zakon.rada.gov.ua/laws/show/1774-19#n219)*; в редакції Закону*[*№ 324-IX від 03.12.2019*](https://zakon.rada.gov.ua/laws/show/324-20#n169)*}*

**Стаття 12.**Інформація довідково-енциклопедичного характеру

1. Інформація довідково-енциклопедичного характеру - систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище.

2. Основними джерелами інформації довідково-енциклопедичного характеру є: енциклопедії, словники, довідники, рекламні повідомлення та оголошення, путівники, картографічні матеріали, електронні бази та банки даних, архіви різноманітних довідкових інформаційних служб, мереж та систем, а також довідки, що видаються уповноваженими на те органами державної влади та органами місцевого самоврядування, об'єднаннями громадян, організаціями, їх працівниками та автоматизованими інформаційно-комунікаційними системами.

*{Частина друга статті 12 із змінами, внесеними згідно із Законом*[*№ 1089-IX від 16.12.2020*](https://zakon.rada.gov.ua/laws/show/1089-20#n2381)*}*

3. Правовий режим інформації довідково-енциклопедичного характеру визначається законодавством та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

**Стаття 13.**Інформація про стан довкілля (екологічна інформація)

1. Інформація про стан довкілля (екологічна інформація) - відомості та/або дані про:

стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими;

фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми);

стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля;

інші відомості та/або дані.

2. Правовий режим інформації про стан довкілля (екологічної інформації) визначається законами України та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

3. Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, не може бути віднесена до інформації з обмеженим доступом.

**Стаття 14.**Інформація про товар (роботу, послугу)

1. Інформація про товар (роботу, послугу) - відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).

2. Інформація про вплив товару (роботи, послуги) на життя та здоров'я людини не може бути віднесена до інформації з обмеженим доступом.

3. Правовий режим інформації про товар (роботу, послугу) визначається законами України про захист прав споживачів, про рекламу, іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

**Стаття 15.**Науково-технічна інформація

1. Науково-технічна інформація - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

2. Правовий режим науково-технічної інформації визначається [Законом України](https://zakon.rada.gov.ua/laws/show/3322-12) "Про науково-технічну інформацію", іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

3. Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України.

**Стаття 16.**Податкова інформація

1. Податкова інформація - сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому [Податковим кодексом України](https://zakon.rada.gov.ua/laws/show/2755-17).

2. Правовий режим податкової інформації визначається [Податковим кодексом України](https://zakon.rada.gov.ua/laws/show/2755-17) та іншими законами.

**Стаття 17.**Правова інформація

1. Правова інформація - будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

2. Джерелами правової інформації є [Конституція України](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80), інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення медіа, публічні виступи, інші джерела інформації з правових питань.

3. З метою забезпечення доступу до законодавчих та інших нормативних актів фізичним та юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття.

**Стаття 18.**Статистична інформація

1. Статистична інформація - документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

2. Офіційна державна статистична інформація підлягає систематичному оприлюдненню.

3. Держава гарантує суб'єктам інформаційних відносин відкритий доступ до офіційної державної статистичної інформації, за винятком інформації, доступ до якої обмежений згідно із законом.

4. Правовий режим офіційної державної статистичної інформації визначається [Законом України](https://zakon.rada.gov.ua/laws/show/2524-20) "Про офіційну статистику", іншими законами України та міжнародними договорами України, згода на обов’язковість яких надана Верховною Радою України.

*{Частина четверта статті 18 в редакції Закону*[*№ 2524-IX від 16.08.2022*](https://zakon.rada.gov.ua/laws/show/2524-20#n354)*}*

**Стаття 19.**Соціологічна інформація

1. Соціологічна інформація - будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо.

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

**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.

*{Закон доповнено статтею 19***-1***згідно із Законом*[*№ 1882-IX від 16.11.2021*](https://zakon.rada.gov.ua/laws/show/1882-20#n409)*}*

**Стаття 20.**Доступ до інформації

1. За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом.

2. Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом.

**Стаття 21.** Інформація з обмеженим доступом

1. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

2. Конфіденційною є інформація про фізичну особу, інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, а також інформація, визнана такою на підставі закону. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, якщо інше не встановлено законом.

*{Абзац перший частини другої статті 21 в редакції Закону*[*№ 2718-IX від 03.11.2022*](https://zakon.rada.gov.ua/laws/show/2718-20#n392)*}*

Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

3. Порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законами.

4. До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов’язаних з політичними репресіями, Голодомором 1932-1933 років в Україні та іншими злочинами, вчиненими особами, які брали участь або сприяли реалізації російської імперської політики, представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

*{Пункт 4 частини четвертої статті 21 в редакції Законів*[*№ 317-VIII від 09.04.2015*](https://zakon.rada.gov.ua/laws/show/317-19#n132)*,*[*№ 3005-IX від 21.03.2023*](https://zakon.rada.gov.ua/laws/show/3005-20#n126)*}*

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

5**-1**) щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов’язковому оприлюдненню відповідно до закону;

*{Частину четверту статті 21 доповнено пунктом 5***-1***згідно із Законом*[*№ 1405-VIII від 02.06.2016*](https://zakon.rada.gov.ua/laws/show/1405-19#n315)*}*

6) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

**Розділ IV**  
**ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ІНФОРМАЦІЮ**

**Стаття 27.**Відповідальність за порушення законодавства про інформацію

1. Порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно із законами України.

**Стаття 28.**Неприпустимість зловживання правом на інформацію

1. Інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

**Стаття 29.**Поширення суспільно необхідної інформації

1. Інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

2. Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо.

**Стаття 30.**Звільнення від відповідальності

1. Ніхто не може бути притягнутий до відповідальності за висловлення оціночних суджень.

2. Оціночними судженнями, за винятком наклепу, є висловлювання, які не містять фактичних даних, критика, оцінка дій, а також висловлювання, що не можуть бути витлумачені як такі, що містять фактичні дані, зокрема з огляду на характер використання мовно-стилістичних засобів (вживання гіпербол, алегорій, сатири). Оціночні судження не підлягають спростуванню та доведенню їх правдивості.

Якщо особа вважає, що оціночні судження або думки принижують її гідність, честь чи ділову репутацію, а також інші особисті немайнові права, вона вправі скористатися наданим їй законодавством правом на відповідь, а також на власне тлумачення справи у тому самому медіа з метою обґрунтування безпідставності поширених суджень, надавши їм іншу оцінку. Якщо суб'єктивну думку висловлено в брутальній, принизливій чи непристойній формі, що принижує гідність, честь чи ділову репутацію, на особу, яка таким чином та у такий спосіб висловила думку або оцінку, може бути покладено обов'язок відшкодувати завдану моральну шкоду.

*{Абзац другий частини другої статті 30 із змінами, внесеними згідно із Законом*[*№ 2849-IX від 13.12.2022*](https://zakon.rada.gov.ua/laws/show/2849-20#n2440)*}*

3. Суб'єкти інформаційних відносин звільняються від відповідальності за розголошення інформації з обмеженим доступом, якщо суд встановить, що ця інформація є суспільно необхідною.

4. Додаткові підстави звільнення від відповідальності медіа та журналістів встановлюються [Законом України](https://zakon.rada.gov.ua/laws/show/2849-20) "Про медіа" та іншими законами України.

*{Частина четверта статті 30 в редакції Закону*[*№ 2849-IX від 13.12.2022*](https://zakon.rada.gov.ua/laws/show/2849-20#n2441)*}*

**Стаття 31.**Відшкодування матеріальної та моральної шкоди

1. У разі якщо порушенням права на свободу інформації особі завдано матеріальної чи моральної шкоди, вона має право на її відшкодування за рішенням суду.

2. Суб'єкти владних повноважень як позивачі у справах про захист честі, гідності та ділової репутації вправі вимагати в судовому порядку лише спростування недостовірної інформації про себе і не мають права вимагати відшкодування моральної (немайнової) шкоди. Це не позбавляє посадових і службових осіб права на захист честі, гідності та ділової репутації в суді.

ЗУ Про науково-технічну інформацію

**ЗАГАЛЬНІ ПОЛОЖЕННЯ**

**Стаття 1.** Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

науково-технічна інформація - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

*{Абзац другий статті 1 в редакції Закону*[*№ 2938-VI від 13.01.2011*](https://zakon.rada.gov.ua/laws/show/2938-17)*}*

науково-інформаційна діяльність - це сукупність дій, спрямованих на задоволення потреб громадян, юридичних осіб і держави у науково-технічній інформації, що полягає в її збиранні, аналітично-синтетичній обробці, фіксації, зберіганні, пошуку і поширенні;

інформаційні ресурси науково-технічної інформації - це систематизоване зібрання науково-технічної літератури і документації (книги, брошури, періодичні видання, патентна документація, нормативно-технічна документація, промислові каталоги, конструкторська документація, звітна науково-технічна документація з науково-дослідних і дослідно-конструкторських робіт, депоновані рукописи, переклади науково-технічної літератури і документації), зафіксовані на паперових чи інших носіях;

довідково-інформаційний фонд - це сукупність упорядкованих первинних документів і довідково-пошукового апарату, призначених для задоволення інформаційних потреб;

довідково-пошуковий апарат - це сукупність упорядкованих вторинних документів, створюваних для пошуку першоджерел;

інформаційні ресурси спільного користування - це сукупність інформаційних ресурсів державних органів науково-технічної інформації, наукових, науково-технічних бібліотек, а також комерційних центрів, фірм, організацій, які займаються науково-технічною діяльністю і з власниками яких укладено договори про їх спільне використання;

аналітично-синтетична обробка науково-технічної інформації - це процес обробки інформації шляхом аналізу і синтезу змісту документів з метою одержання необхідних відомостей, а також шляхом їх класифікації, оцінки, співставлення і узагальнення;

інформаційний ринок - це система економічних, організаційних і правових відносин щодо продажу і купівлі інформаційних ресурсів, технологій, продукції та послуг.

**Стаття 2.** Об’єкт відносин у сфері науково-технічної інформації

Об’єктом відносин у сфері науково-технічної інформації є вітчизняна і зарубіжна науково-технічна інформація.

*{Частина перша статті 2 із змінами, внесеними згідно із Законом*[*№ 2938-VI від 13.01.2011*](https://zakon.rada.gov.ua/laws/show/2938-17)*}*

Науково-технічна інформація охоплює отримувані в процесі науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності результати, зафіксовані у формі, яка забезпечує їх відтворення, використання та поширення.

Науково-технічна інформація є суспільним надбанням, необхідною умовою продуктивної інтелектуальної діяльності, зокрема наукової і технічної творчості.

Науково-технічна інформація, що є продуктом інтелектуальної творчої праці, становить об’єкт права інтелектуальної власності, а відносини щодо її придбання, зберігання, переробки, використання і поширення регулюються чинним законодавством.

**Стаття 3.** Суб’єкти відносин у сфері науково-технічної інформації

1. Суб’єктами відносин, що регулюються цим Законом, є державні органи, органи місцевого і регіонального самоврядування, юридичні особи та громадяни України, міжнародні організації, іноземні юридичні особи і громадяни та особи без громадянства.

2. Фізичні та юридичні особи у сфері дії цього Закону виступають як творці і накопичувачі науково-технічної інформації, власники, виробники, зберігачі і споживачі інформаційної продукції та послуг, а також як посередники у сфері науково-інформаційної діяльності.

**Стаття 4.** Законодавство України у сфері науково-технічної інформації

Відповідно до [Конституції](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80) законодавство України у сфері науково-технічної інформації складається з [Закону України](https://zakon.rada.gov.ua/laws/show/2657-12) "Про інформацію", цього Закону та інших актів законодавства.

**Розділ II**  
**ПРАВОВИЙ РЕЖИМ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ**

**Стаття 5.** Право на науково-технічну інформацію

1. Усі громадяни України, юридичні особи, державні органи, органи місцевого і регіонального самоврядування відповідно до [Конституції України](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80) і цього Закону мають право на відкриту науково-технічну інформацію, яке передбачає можливість вільного її одержання, зберігання, використання і поширення під час здійснення наукової, науково-дослідної, виробничої, громадської та іншої діяльності, що не забороняється чинним законодавством.

2. Режим доступу до відкритої науково-технічної інформації та інформації з обмеженим доступом регулюється чинним законодавством.

**Стаття 6.** Права на науково-технічну інформацію

1. Права на науково-технічну інформацію охороняються відповідно до закону.

2. Підставою виникнення прав на науково-технічну інформацію є створення науково-технічної інформації своїми силами і за свій рахунок; виконання договору про створення науково-технічної інформації; виконання будь-якого договору, що містить умови переходу прав на інформацію до іншої особи.

3. Права на науково-технічну інформацію, створену кількома особами, визначаються договором, укладеним між творцями цієї інформації.

4. Права на науково-технічну інформацію, створену за рахунок коштів державного бюджету, визначаються державою шляхом прийняття загальних рішень і шляхом укладення договорів між державним органом, що здійснює фінансування, і виконавцем робіт із створення науково-технічної інформації.

Права на науково-технічну інформацію, що належали фізичним та юридичним особам, можуть переходити до держави в разі передачі її до відповідних державних банків даних, фондів або архівів на договірній основі.

*{Стаття 6 в редакції Закону*[*№ 1170-VII від 27.03.2014*](https://zakon.rada.gov.ua/laws/show/1170-18#n87)*}*

**Стаття 7.** Відносини між особами, яким належать права на науково-технічну інформацію, її споживачами і посередниками

1. Споживач науково-технічної інформації несе відповідальність за дотримання прав особи, якій належать права на цю інформацію. Споживач науково-технічної інформації не має права передачі одержаної науково-технічної інформації третій особі, якщо це не обумовлено договором з особою, якій належать права на науково-технічну інформацію.

Якщо споживач науково-технічної інформації одержав від особи, якій належать права на цю інформацію, або через посередника інформацію, що не відповідає умовам договору між ними, він має право вимагати безоплатного усунення недоліків у погоджений строк.

У разі відмови особи, якій належать права на цю інформацію, або посередника добровільно задовольнити законні вимоги споживача спір вирішується в суді.

2. Особа, якій належать права на інформацію, здійснює свої права щодо науково-технічної інформації самостійно або через посередника. Відносини між особою, якій належать права на інформацію, і посередником регулюються договором.

*{Стаття 7 із змінами, внесеними згідно із Законом*[*№ 762-IV від 15.05.2003*](https://zakon.rada.gov.ua/laws/show/762-15)*; в редакції Закону*[*№ 1170-VII від 27.03.2014*](https://zakon.rada.gov.ua/laws/show/1170-18#n87)*}*

**Розділ III**  
**НАЦІОНАЛЬНА СИСТЕМА НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ**

**Стаття 8.** Визначення та склад національної системи науково-технічної інформації

1. Основною метою національної системи науково-технічної інформації є задоволення потреб громадян, юридичних осіб і держави в науково-технічній інформації.

Національна система науково-технічної інформації - це організаційно-правова структура, за допомогою якої формується державна інформаційна політика, а також здійснюється координація робіт по створенню, користуванню, зберіганню та поширенню національних ресурсів науково-технічної інформації з урахуванням інтересів національної безпеки.

2. Національна система науково-технічної інформації складається з:

спеціалізованих державних підприємств, установ, організацій, державних органів науково-технічної інформації, наукових і науково-технічних бібліотек, об’єднаних загальносистемними зв’язками та обов’язками;

підприємств будь-яких організаційно-правових форм, заснованих на приватній чи колективній власності, предметом діяльності яких є інформаційне забезпечення народного господарства і громадян України.

Діяльність складових частин національної системи науково-технічної інформації здійснюється на основі договірно-обумовленого поділу праці в її збиранні, накопичуванні, переробці, зберіганні, поширенні та використанні.

3. Структура національної системи науково-технічної інформації, завдання і функції її основних інформаційних ланок щодо виконання загальносистемних зобов’язань, їх права і обов’язки визначаються положеннями, що затверджуються спеціально уповноваженим центральним органом державної виконавчої влади, який здійснює управління у сфері науково-технічної інформації.

4. Відносини між національною системою науково-технічної інформації України та системами науково-технічної інформації інших держав будуються на основі угод і договорів.

**Стаття 9.** Основні завдання національної системи науково-технічної інформації

Основними завданнями національної системи науково-технічної інформації є:

формування на основі вітчизняних і зарубіжних джерел довідково-інформаційних фондів, включаючи бази і банки даних, та інформаційне забезпечення юридичних та фізичних осіб;

одержання, обробка, зберігання, поширення і використання інформації, одержаної в процесі науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності юридичних та фізичних осіб;

організація надходження до України, обробка, зберігання і поширення зарубіжної науково-технічної інформації на основі вивчення світового інформаційного ринку;

підготовка аналітичних матеріалів, необхідних для прийняття державними органами, органами місцевого і регіонального самоврядування рішень з питань науково-технічного, економічного і соціального розвитку країни;

аналітично-синтетична обробка першоджерел, реферування опублікованих і не опублікованих на території України джерел науково-технічної та економічної інформації, створення на цій основі і поширення інформаційної продукції та послуг;

розроблення і впровадження сучасних технологій в науково-інформаційну діяльність;

організація пропаганди і сприяння широкому використанню досягнень науки і техніки, передового виробничого досвіду;

створення загальнодоступної мережі бібліотек, інформаційних центрів громадського користування як бази для освіти, виробництва та наукових досліджень, системи реалізації прав громадян на культурний та фаховий розвиток.

**Стаття 10.** Інформаційні ресурси національної системи науково-технічної інформації

1. Інформаційні ресурси національної системи науково-технічної інформації становлять сукупність довідково-інформаційних фондів з необхідним довідково-пошуковим апаратом і відповідними технічними засобами зберігання, обробки і передачі, що є у володінні, розпорядженні, користуванні державних органів і служб науково-технічної інформації, наукових і науково-технічних бібліотек, комерційних центрів, підприємств, установ і організацій.

2. Інформаційні ресурси науково-технічної інформації, що є власністю держави, визнаються державними ресурсами науково-технічної інформації. Їх розподіл між різними державними органами, службами, установами та порядок обміну може регулюватися на рівні загальнодержавних та відомчих рішень через уповноважені на те структури.

3. У поповненні інформаційних ресурсів національної системи науково-технічної інформації беруть участь фізичні і юридичні особи України незалежно від форм власності. При цьому законодавством України можуть встановлюватись обов’язкові норми їх участі (крім тієї, що реалізується на договірних засадах). Використання органами і службами науково-технічної інформації переданих їм підприємствами і організаціями матеріалів і технічної документації провадиться на умовах, встановлюваних підприємствами і організаціями - власниками цих матеріалів, крім випадків, коли законодавством не передбачено інше. Органи і служби науково-технічної інформації, яким передається така інформація, гарантують захист прав інтелектуальної власності, додержання комерційної таємниці, захист законних інтересів юридичних та фізичних осіб - творців інформації про науково-технічні досягнення.

4. Використання в процесі створення ресурсів науково-технічної інформації творів літератури, мистецтва і науки допускається за умов додержання авторського права. Це положення поширюється також на програмне забезпечення обчислювальної техніки і автоматизованих інформаційних систем.

**Стаття 11.** Державна реєстрація, облік і використання результатів науково-технічної діяльності

1. Результати науково-дослідної, дослідно-конструкторської, проектно-технологічної та іншої науково-технічної діяльності, фінансування якої повністю або частково здійснюється за рахунок коштів державного бюджету, підлягають обов’язковій реєстрації та обліку.

[Порядок реєстрації та обліку](https://zakon.rada.gov.ua/laws/show/z0312-09) визначається спеціально уповноваженим центральним органом виконавчої влади, що здійснює управління в сфері науково-технічної інформації.

2. Права на результати науково-дослідних, дослідно-конструкторських, проектно-технологічних та інших робіт, що проводяться за рахунок власних коштів юридичних та фізичних осіб, належать цим особам і реєструються ними на добровільних засадах в державному органі науково-технічної інформації з наступним поширенням звітних матеріалів самостійно або через відповідні служби науково-технічної інформації на договірній основі.

*{Частина друга статті 11 із змінами, внесеними згідно із Законом*[*№ 1170-VII від 27.03.2014*](https://zakon.rada.gov.ua/laws/show/1170-18#n99)*}*

3. Відомості про всі зареєстровані в Україні результати науково-технічної діяльності з зазначенням місцезнаходження звітної документації та умов їх передачі розповсюджуються за запитом заінтересованих осіб та організацій органами і службами науково-технічної інформації, відповідальними за реєстрацію цих результатів, крім випадків обмежень, пов’язаних із державною чи комерційною таємницею.

**Стаття 12.** Організація надходження та використання зарубіжної науково-технічної інформації

Придбання зарубіжної науково-технічної літератури і документації, баз і банків даних, необхідних для формування державних ресурсів науково-технічної інформації, здійснюється як за безвалютним обміном, так і за рахунок інвалютних коштів органів і служб науково-технічної інформації. Для створення ресурсів зарубіжної науково-технічної інформації державних органів і наукових організацій, що фінансуються з бюджету, валютні кошти щорічно передбачаються в державному бюджеті цільовим призначенням.

**Розділ IV**  
**РИНОК НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ**

**Стаття 13.** Науково-технічна інформація як об’єкт товарних відносин

Інформаційна продукція та послуги органів науково-технічної інформації, а також підприємств, установ, організацій, окремих громадян, які здійснюють науково-інформаційну діяльність, можуть бути об’єктами товарних відносин, що регулюються чинним законодавством.

Ціни на інформаційну продукцію та послуги встановлюються договорами, за винятком випадків, передбачених цим Законом.

**Стаття 14.** Формування ринку науково-технічної інформації

1. Органи науково-технічної інформації, підприємства, організації, громадяни, що здійснюють науково-інформаційну діяльність і вільно реалізують свою інформаційну продукцію та інформаційні послуги, є товаровиробниками, які беруть участь у створенні ринку на загальних підставах незалежно від форм власності.

2. Товаровиробник має право вчиняти будь-які дії стосовно реалізації своєї продукції, що не суперечать чинному законодавству.

3. Підприємства, установи і організації незалежно від форм власності, що здійснюють науково-інформаційну діяльність, є вільними у виборі постачальників інформації, форм відносин з ними, методів і видів інформування, а також номенклатури інформаційної продукції та послуг, крім випадків, коли власники цих підприємств, установ і організацій встановлюють певні вимоги щодо номенклатури продукції, сфери інформаційного обслуговування тощо.

**Стаття 15.** Умови надання інформаційної продукції та послуг

1. Державні органи та служби науково-технічної інформації, які організують використання державних ресурсів науково-технічної інформації, здійснюють її пошук і передачу на безприбуткових засадах. У наукових і науково-технічних бібліотеках, які фінансуються з бюджету, науково-технічна інформація, що не потребує спеціального тематичного пошуку або копіювання, надається безплатно.

2. Огляди, аналітичні і фактографічні довідки, інші види інформаційної продукції, що готуються на основі аналізу, оцінки та узагальнення науково-технічної інформації (за винятком державних замовлень), реалізуються на комерційних засадах.

Без отримання прибутку здійснюється репродукування друкованих творів у галузі науки і техніки з науковою, навчальною і освітньою метою відповідно до чинного законодавства.

3. Державні органи та служби науково-технічної інформації, інші інформаційні центри, фірми, підприємства, установи і організації, які формують ресурси науково-технічної інформації за рахунок власних коштів, надають інформаційну продукцію і послуги на комерційних засадах.

4. У ході здійснення купівлі-продажу інформаційної продукції повинні гарантуватись охорона прав інтелектуальної власності, державної та комерційної таємниці, законні права та інтереси власника і виробника інформаційної продукції і послуг.

**Стаття 16.** Відносини виробників і споживачів науково-технічної інформації

Відносини між державними органами і службами науково-технічної інформації, підприємствами, установами і організаціями будь-яких форм власності, які здійснюють науково-інформаційну діяльність, і споживачами інформації будуються на основі контрактів (договорів) та на інших формах угод, передбачених чинним законодавством. Контракт (договір) є основним документом, що регламентує відносини між виробником і споживачем інформації.

На контрактній (договірній) основі можуть також здійснюватись інформаційне забезпечення, наукові дослідження і розробки для органів державної влади, крім випадків, коли діючими законами передбачено безплатне надання інформації цим органам.

Розрахунки з зарубіжними партнерами здійснюються на договірних умовах і в порядку, встановленому законодавством.

**Розділ V**  
**ДЕРЖАВНА ПОЛІТИКА У СФЕРІ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ**

**Стаття 17.** Державна підтримка науково-інформаційної діяльності

1. Держава з метою створення та розвитку національної системи науково-технічної інформації забезпечує:

створення державних мереж первинного збирання, обробки та зберігання усіх видів науково-технічної інформації;

проведення заходів для поширення і підвищення якісного рівня інформаційної продукції та послуг;

фінансову, в тому числі валютну, підтримку надходження науково-технічної інформації до державних органів і служб науково-технічної інформації, наукових і науково-технічних бібліотек, створення їх мереж і відповідного технічного забезпечення;

підготовку кадрів у сфері інформатики і науково-інформаційної діяльності через систему навчальних закладів вищої та середньої освіти, підвищення рівня інформаційної підготовки спеціалістів народного господарства;

вільну конкуренцію між органами науково-технічної інформації, іншими підприємствами та організаціями усіх форм власності, які здійснюють науково-інформаційну діяльність;

захист суб’єктів відносин в галузі науково-технічної інформації від прояву недобросовісної конкуренції та монополізму в будь-яких сферах науково-інформаційної діяльності.

*{Абзац сьомий частини першої статті 17 із змінами, внесеними згідно із Законом*[*№ 1294-IV від 20.11.2003*](https://zakon.rada.gov.ua/laws/show/1294-15)*}*

2. Держава сприяє відкритості та загальнодоступності науково-технічної інформації.

Обмеження щодо доступу, поширення та використання інформації, яка є державною або іншою таємницею, що охороняється законом, визначаються законами України.

3. Держава підтримує міжнародне співробітництво у сфері науково-технічної інформації, створює для цього правові і економічні умови та сприяє здійсненню суб’єктами науково-інформаційної діяльності вільних і рівноправних відносин з міжнародними організаціями і установами, якщо це не суперечить чинному законодавству України.

4. Держава сприяє формуванню, зберіганню і ефективному використанню державних ресурсів науково-технічної інформації шляхом:

створення реєстраційно-облікового механізму, який забезпечує збирання, обробку і поширення відомостей про виконані за рахунок коштів державного бюджету наукові дослідження і розробки, дисертації та інші види науково-технічних робіт, про нові види продукції, бази і банки даних;

проведення пільгової податкової та фінансово-кредитної політики щодо послуг з надання науково-технічної інформації споживачеві та передачі інформації про науково-технічні досягнення державним органам і службам науково-технічної інформації;

виділення коштів і матеріально-технічних засобів для роботи над створенням і розвитком державних ресурсів науково-технічної інформації та їх використанням, а також для міжгалузевого обміну інформацією про науково-технічні досягнення;

створення механізму зберігання інформаційних ресурсів, баз і банків даних, сформованих в державних організаціях та органах управління, їх відповідної передачі іншим установам в разі ліквідації або реорганізації;

впровадження економічних механізмів створення і підтримки підприємств, заснованих на приватній чи колективній власності, які здійснюють інформаційну діяльність, та їх інтеграції в національну систему науково-технічної інформації.

**Стаття 18.** Державне управління у сфері науково-технічної інформації

Кабінет Міністрів України визначає орган державного управління, який забезпечує організацію діяльності у сфері науково-технічної інформації, здійснює функціональне управління національною системою науково-технічної інформації, формує і реалізує політику в цій сфері.

**Стаття 19.** Відповідальність за порушення законодавства України про науково-технічну інформацію

Порушення законодавства України про науково-технічну інформацію тягне за собою відповідальність згідно з чинним законодавством.

**Розділ VI**  
**МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ НАУКОВО-ТЕХНІЧНОЇ ІНФОРМАЦІЇ**

**Стаття 20.** Міжнародна інформаційна діяльність

Міжнародне співробітництво у сфері науково-технічної інформації та міжнародна інформаційна діяльність регулюються згідно з чинним законодавством.

**Стаття 21.** Міждержавний обмін науково-технічною інформацією

1. Міждержавний обмін науково-технічною інформацією здійснюється відповідно до угод, підписаних Україною.

2. Держава забезпечує відкритий і рівноправний доступ своїх громадян і громадян держав - партнерів за угодами до інформаційних ресурсів спільного користування.

3. Уряд України визначає національний інформаційний центр, який координує міждержавний обмін науково-технічною інформацією.

**Стаття 22.** Діяльність іноземних фізичних та юридичних осіб в Україні у сфері науково-технічної інформації

Іноземні юридичні та фізичні особи, а також особи без громадянства можуть інвестувати розвиток сфери науково-технічної інформації України відповідно до чинного законодавства.

**Стаття 23.** Забезпечення суверенітету України у сфері науково-технічної інформації

Суверенітет України у сфері науково-технічної інформації забезпечується:

організацією та державною підтримкою власних інформаційних систем і наданням для них можливостей шукати, фіксувати, отримувати, оброблювати і поширювати в інтересах суспільства науково-технічну інформацію, вироблену в Україні або в інших країнах світу;

встановленням власності держави на ресурси науково-технічної інформації, що формуються за рахунок коштів бюджету;

створенням і розвитком національної системи науково-технічної інформації;

організацією доступу інших держав до інформаційних ресурсів України на основі укладання угод та договорів про їх спільне використання, ліцензуванням і квотуванням науково-технічної інформації, яка може бути використана за межами України для виготовлення зброї, військової техніки, наукоємної продукції;

організацією належної системи охорони та зберігання інформації.

*1.1.2 ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України»*

ЗУ Про захист інформації в інформаційно-телекомунікаційних системах

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі - система).

**Стаття 1.**Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;

виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

володілець інформації - фізична або юридична особа, якій належать права на інформацію;

*{Абзац четвертий статті 1 в редакції Закону*[*№ 1170-VII від 27.03.2014*](https://zakon.rada.gov.ua/laws/show/1170-18#n290)*}*

власник системи - фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-комунікаційна система - сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі (далі - користувач) - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

електронна комунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації;

резервна копія державних інформаційних ресурсів - копія інформації, яка міститься в державних інформаційних ресурсах, що перебувають у володінні або розпорядженні органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, державних підприємств, установ та організацій, та є критичною для їх сталого функціонування, створюється, записується, обробляється або зберігається у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів з метою подальшого відновлення цієї інформації;

*{Частину першу статті 1 доповнено абзацом двадцятим згідно із Законом*[*№ 2130-IX від 15.03.2022*](https://zakon.rada.gov.ua/laws/show/2130-20#n7)*}*

резервування державних інформаційних ресурсів та систем - сукупність заходів, спрямованих на забезпечення створення резервної копії (резервних копій) та зберігання державних інформаційних ресурсів та систем з метою забезпечення безперервності їх роботи та подальшого відновлення інформації, що міститься в державних інформаційних ресурсах та системах, а також інсталяційних копій програмного забезпечення та операційних систем (та/або їх образів), в яких здійснюється їх обробка. [Перелік видів державних інформаційних ресурсів та систем, щодо яких може здійснюватися резервне копіювання](https://zakon.rada.gov.ua/laws/show/1500-2022-%D0%BF#n94), визначається Кабінетом Міністрів України.

*{Частину першу статті 1 доповнено абзацом двадцять першим згідно із Законом*[*№ 2130-IX від 15.03.2022*](https://zakon.rada.gov.ua/laws/show/2130-20#n7)*}*

Інші терміни вживаються у значенні, наведеному в законах України ["Про інформацію"](https://zakon.rada.gov.ua/laws/show/2657-12) та ["Про технічні регламенти та оцінку відповідності"](https://zakon.rada.gov.ua/laws/show/124-19).

*{Статтю 1 доповнено частиною другою згідно із Законом* [*№ 681-IX від 04.06.2020*](https://zakon.rada.gov.ua/laws/show/681-20#n6)*}*

*{Стаття 1 із змінами, внесеними згідно із Законом*[*№ 1089-IX від 16.12.2020*](https://zakon.rada.gov.ua/laws/show/1089-20#n2341)*}*

**Стаття 2.**Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

**Стаття 3.**Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

володільці інформації;

власники системи;

користувачі;

спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи;

*{Абзац п'ятий частини першої статті 3 в редакції Закону*[*№ 879-VI від 15.01.2009*](https://zakon.rada.gov.ua/laws/show/879-17)*}*

*{Абзац шостий частини першої статті 3 виключено на підставі Закону*[*№ 767-VII від 23.02.2014*](https://zakon.rada.gov.ua/laws/show/767-18#n252)*}*

*{Частину другу статті 3 виключено на підставі Закону*[*№ 1170-VII від 27.03.2014*](https://zakon.rada.gov.ua/laws/show/1170-18#n292)*}*

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи.

**Стаття 4.**Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації.

Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом.

*{Частина третя статті 4 із змінами, внесеними згідно із Законом*[*№ 1170-VII від 27.03.2014*](https://zakon.rada.gov.ua/laws/show/1170-18#n293)*}*

**Стаття 5.**Відносини між володільцем інформації та власником системи

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із володільцем інформації, якщо інше не передбачено законом.

Власник системи на вимогу володільця інформації надає відомості щодо захисту інформації в системі.

Протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування володільці інформації - власники (держателі) державних інформаційних ресурсів можуть укладати договори про технічне адміністрування відповідних реєстрів з іноземними компаніями, організаціями - постачальниками послуг з надання хмарних ресурсів (надавачами хмарних послуг), утвореними відповідно до законодавства інших держав, та/або їх зареєстрованими (акредитованими або легалізованими) відповідно до законодавства України філіями, представництвами та іншими відокремленими підрозділами з місцезнаходженням на території України в [порядку](https://zakon.rada.gov.ua/laws/show/1500-2022-%D0%BF#n59), встановленому Кабінетом Міністрів України.

*{Статтю 5 доповнено частиною третьою згідно із Законом*[*№ 2130-IX від 15.03.2022*](https://zakon.rada.gov.ua/laws/show/2130-20#n10)*}*

**Стаття 6.**Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

**Стаття 7.**Відносини між власниками систем

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

**Стаття 8.**Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством.

*{Частина друга статті 8 із змінами, внесеними згідно із Законами*[*№ 1170-VII від 27.03.2014*](https://zakon.rada.gov.ua/laws/show/1170-18#n294)*,* [*№ 681-IX від 04.06.2020*](https://zakon.rada.gov.ua/laws/show/681-20#n9)*}*

Підтвердження відповідності та проведення державної експертизи засобів технічного і криптографічного захисту інформації здійснюються в порядку, встановленому законодавством. Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації, та засоби технічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації або сертифікат відповідності, виданий органом з оцінки відповідності, який акредитовано:

національним органом України з акредитації;

чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності.

*{Частина третя статті 8 в редакції Закону*[*№ 681-IX від 04.06.2020*](https://zakon.rada.gov.ua/laws/show/681-20#n11)*}*

Державні інформаційні ресурси та інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, крім державної таємниці, службової інформації та інформації з державних і єдиних реєстрів, створення та забезпечення функціонування яких визначені законом, можуть оброблятися в системі без застосування комплексної системи захисту інформації у разі виконання всіх таких умов:

підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іноземної держави, якщо і національний орган України з акредитації, і національний орган з акредитації іноземної держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності;

використання для захисту інформації в системі засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації або документ про відповідність, виданий за результатами сертифікації таких засобів відповідно до [Закону України](https://zakon.rada.gov.ua/laws/show/124-19) "Про технічні регламенти та оцінку відповідності";

жодний з елементів системи не розташований, а власник такої системи або його офіційний представник не є юридичною особою (її представником), зареєстрованою на територіях України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на території держави, визнаної Верховною Радою України державою-агресором, на території держави, щодо якої застосовані санкції відповідно до [Закону України](https://zakon.rada.gov.ua/laws/show/1644-18) "Про санкції", або на території держави, яка входить до митного союзу з такими державами;

власник системи або його представник, який надає послуги з використанням системи, елементи якої розміщуються поза межами України, є юридичною особою, зареєстрованою в Україні, або має свого офіційного представника в Україні;

виконання особливих вимог, встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, що обробляються.

*{Статтю 8 доповнено частиною четвертою згідно із Законом*[*№ 681-IX від 04.06.2020*](https://zakon.rada.gov.ua/laws/show/681-20#n15)*;  із змінами, внесеними згідно із Законом*[*№ 1882-IX від 16.11.2021*](https://zakon.rada.gov.ua/laws/show/1882-20#n401)*; в редакції Закону*[*№ 2801-IX від 01.12.2022*](https://zakon.rada.gov.ua/laws/show/2801-20#n196)*}*

Власники систем для забезпечення належного функціонування систем та захисту інформації, що обробляється в них:

створюють резервні копії державних інформаційних ресурсів та систем із дотриманням встановлених для таких ресурсів та систем вимог щодо їх захисту, цілісності та конфіденційності;

забезпечують створення резервних копій державних інформаційних ресурсів та систем на окремих фізичних носіях у зашифрованому вигляді та їх подальшу передачу (переміщення) для зберігання в установленому законодавством порядку, у тому числі за межами України (зокрема в закордонних дипломатичних установах України), протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування;

забезпечують в установленому законодавством порядку передачу (переміщення) державних інформаційних ресурсів та їх резервних копій для розміщення на хмарних ресурсах та/або в центрах обробки даних, розташованих за межами України, протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування.

*{Статтю 8 доповнено частиною п'ятою згідно із Законом*[*№ 2130-IX від 15.03.2022*](https://zakon.rada.gov.ua/laws/show/2130-20#n12)*}*

[Порядок передачі, зберігання, функціонування та доступу до державних інформаційних ресурсів та їх резервних копій](https://zakon.rada.gov.ua/laws/show/1500-2022-%D0%BF#n12) встановлюється Кабінетом Міністрів України.

*{Статтю 8 доповнено частиною шостою згідно із Законом*[*№ 2130-IX від 15.03.2022*](https://zakon.rada.gov.ua/laws/show/2130-20#n12)*}*

Розміщення систем та зберігання резервних копій державних інформаційних ресурсів та систем на територіях України, на яких органи державної влади України тимчасово не здійснюють свої повноваження, територіях держав, визнаних Верховною Радою України державами-агресорами, територіях держав, щодо яких застосовані санкції відповідно до [Закону України](https://zakon.rada.gov.ua/laws/show/1644-18) "Про санкції", та територіях держав, які входять до митних та воєнних союзів з такими державами, забороняється.

*{Статтю 8 доповнено частиною сьомою згідно із Законом*[*№ 2130-IX від 15.03.2022*](https://zakon.rada.gov.ua/laws/show/2130-20#n12)*}*

**Стаття 9.**Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

*{Частина друга статті 9 із змінами, внесеними згідно із Законом*[*№ 1170-VII від 27.03.2014*](https://zakon.rada.gov.ua/laws/show/1170-18#n295)*}*

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

*{Частина третя статті 9 із змінами, внесеними згідно із Законом*[*№ 879-VI від 15.01.2009*](https://zakon.rada.gov.ua/laws/show/879-17)*}*

**Стаття 10.**Повноваження державних органів у сфері захисту інформації в системах

[Вимоги](https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF) до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

*{Частину другу статті 10 виключено на підставі Закону*[*№ 879-VI від 15.01.2009*](https://zakon.rada.gov.ua/laws/show/879-17)*}*

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

*{Абзац перший частини третьої статті 10 в редакції Закону*[*№ 879-VI від 15.01.2009*](https://zakon.rada.gov.ua/laws/show/879-17)*}*

розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

*{Частину третю статті 10 доповнено абзацом згідно із Законом*[*№ 1180-VI від 19.03.2009*](https://zakon.rada.gov.ua/laws/show/1180-17)*}*

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

*{Частина четверта статті 10 із змінами, внесеними згідно із Законом*[*№ 879-VI від 15.01.2009*](https://zakon.rada.gov.ua/laws/show/879-17)*}*

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

*{Стаття 10 із змінами, внесеними згідно із Законом*[*№ 1089-IX від 16.12.2020*](https://zakon.rada.gov.ua/laws/show/1089-20#n2342)*}*

**Стаття 11.**Відповідальність за порушення законодавства про захист інформації в системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

**Стаття 12.**Міжнародні договори

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору.

**Стаття 13.**Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2006 року.

2. Нормативно-правові акти до приведення їх у відповідність із цим Законом діють у частині, що не суперечить цьому Закону.

3. Кабінету Міністрів України та Національному банку України в межах своїх повноважень протягом шести місяців з дня набрання чинності цим Законом:

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

забезпечити приведення міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

ЗУ Про основні засади забезпечення кібербезпеки України

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

**Стаття 1.** Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

2) інформація про інцидент кібербезпеки - відомості про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

3) інцидент кібербезпеки (далі - кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

4) кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;

5) кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

6) кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів;

7) кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

8) кіберзлочин (комп’ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

9) кіберзлочинність - сукупність кіберзлочинів;

10) кібероборона - сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

11) кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

12) кіберрозвідка - діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

13) кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

14) кібершпигунство - шпигунство, що здійснюється у кіберпросторі або з його використанням;

15) критична інформаційна інфраструктура - сукупність об’єктів критичної інформаційної інфраструктури;

*{Пункт 16 частини першої статті 1 виключено на підставі Закону*[*№ 1882-IX від 16.11.2021*](https://zakon.rada.gov.ua/laws/show/1882-20#n447)*}*

17) Національна телекомунікаційна мережа - сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв’язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

18) національні електронні інформаційні ресурси (далі - національні інформаційні ресурси) - систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

18**-1**) Національний центр резервування державних інформаційних ресурсів - організована сукупність об’єктів, створених з метою забезпечення надійності та безперебійності роботи державних інформаційних ресурсів, кіберзахисту, зберігання національних електронних інформаційних ресурсів, резервного копіювання інформації та відомостей національних електронних інформаційних ресурсів державних органів, військових формувань, утворених відповідно до законів, підприємств, установ та організацій;

*{Частину першу статті 1 доповнено пунктом 18***-1***згідно із Законом*[*№ 1907-IX від 18.11.2021*](https://zakon.rada.gov.ua/laws/show/1907-20#n587)*}*

19) об’єкт критичної інформаційної інфраструктури - комунікаційна або технологічна система об’єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об’єкта критичної інфраструктури;

20) система управління технологічними процесами (далі - технологічна система) - автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

21) системи електронних комунікацій (далі - комунікаційні системи) - системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв’язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв’язку, комп’ютери, інша комп’ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних;

22) система активної протидії агресії у кіберпросторі - сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак;

*{Частину першу статті 1 доповнено пунктом 22 згідно із Законом*[*№ 2470-IX від 28.07.2022*](https://zakon.rada.gov.ua/laws/show/2470-20#n21)*}*

23) активна протидія агресії у кіберпросторі - дії, спрямовані на підвищення рівня кіберзахисту шляхом нейтралізації кібератак держави-агресора, його систем і мереж, а також джерел походження кіберзагроз та кібератак, які використовуються для завдання шкоди національній безпеці України.

*{Частину першу статті 1 доповнено пунктом 23 згідно із Законом*[*№ 2470-IX від 28.07.2022*](https://zakon.rada.gov.ua/laws/show/2470-20#n21)*}*

Терміни ["національна безпека"](https://zakon.rada.gov.ua/laws/show/964-15#n9), ["національні інтереси"](https://zakon.rada.gov.ua/laws/show/964-15#n11), ["загрози національній безпеці"](https://zakon.rada.gov.ua/laws/show/964-15#n12) вживаються в цьому Законі у значенні, визначеному Законом України "Про основи національної безпеки України". Термін ["об’єкт критичної інфраструктури"](https://zakon.rada.gov.ua/laws/show/1882-20#n20) вживається в цьому Законі у значенні, визначеному Законом України "Про критичну інфраструктуру".

*{Частина друга статті 1 із змінами, внесеними згідно із Законом*[*№ 1882-IX від 16.11.2021*](https://zakon.rada.gov.ua/laws/show/1882-20#n448)*}*

Термін ["платіжний ринок"](https://zakon.rada.gov.ua/laws/show/1591-20#n83) вживається в цьому Законі у значенні, наведеному в Законі України "Про платіжні послуги".

*{Статтю 1 доповнено частиною третьою згідно із Законом*[*№ 1591-IX від 30.06.2021*](https://zakon.rada.gov.ua/laws/show/1591-20#n1480)*- вводиться в дію з 01.08.2022}*

**Стаття 2.** Принципи застосування Закону

1. Цей Закон не поширюється на:

1) відносини та послуги, пов’язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;

2) діяльність, пов’язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов’язані з функціонуванням таких мереж і ресурсів;

4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем).

2. Застосування законодавства у сфері кібербезпеки та прийняття суб’єктами владних повноважень рішень на виконання норм цього Закону здійснюються з додержанням принципів:

1) мінімально необхідного регулювання, згідно з яким рішення (заходи) суб’єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом;

2) об’єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов’язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки;

3) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;

4) прозорості, згідно з яким рішення (заходи) суб’єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб’єктам, яких вони стосуються, до набрання ними чинності (їх застосування);

5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;

6) недискримінації, згідно з яким рішення, дії та бездіяльність суб’єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов’язків особи, який є:

відмінним від обсягу прав та обов’язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

таким, як і обсяг прав та обов’язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

7) еквівалентності вимог до забезпечення кібербезпеки об’єктів критичної інфраструктури, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем об’єктів критичної інфраструктури, що належать до одного сектору економіки та/або які здійснюють аналогічні функції.

Зазначені принципи застосовуються без переваги будь-якого з них з урахуванням мети і завдань цього Закону.

**Стаття 3.**Правові основи забезпечення кібербезпеки України

1. Правову основу забезпечення кібербезпеки України становлять [Конституція України](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80), закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, [Конвенція про кіберзлочинність](https://zakon.rada.gov.ua/laws/show/994_575), інші міжнародні договори, згода на обов’язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

2. Якщо міжнародним договором України, згоду на обов’язковість якого надано Верховною Радою України, передбачено інші правила, ніж встановлені цим Законом, застосовуються положення міжнародного договору України.

**Стаття 4.**Об’єкти кібербезпеки та кіберзахисту

1. Об’єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об’єкти критичної інфраструктури.

2. Об’єктами кіберзахисту є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об’єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

3. [Порядок формування переліку об’єктів](https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n16) критичної інформаційної інфраструктури, перелік таких об’єктів та порядок їх внесення до державного реєстру об’єктів критичної інформаційної інфраструктури, а також [порядок](https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#n61) формування та забезпечення функціонування державного реєстру об’єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України.

Повноваження щодо формування та забезпечення функціонування реєстру об’єктів критичної інформаційної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, регулювання та нагляд за діяльністю на яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг покладаються на Національний банк України.

*{Абзац другий частини третьої статті 4 із змінами, внесеними згідно із Законом*[*№ 1953-IX від 14.12.2021*](https://zakon.rada.gov.ua/laws/show/1953-20#n1465)*}*

**Стаття 5.**Суб’єкти забезпечення кібербезпеки

1. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

2. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб’єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення [Стратегії кібербезпеки України](https://zakon.rada.gov.ua/laws/show/96/2016#n11).

3. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури (крім об’єктів критичної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг).

*{Частина третя статті 5 із змінами, внесеними згідно із Законом*[*№ 1953-IX від 14.12.2021*](https://zakon.rada.gov.ua/laws/show/1953-20#n1466)*}*

4. Суб’єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об’єктів критичної інфраструктури;

8) суб’єкти господарювання, громадяни України та об’єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов’язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

5. Суб’єкти забезпечення кібербезпеки у межах своєї компетенції:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

**Стаття 6.** Об’єкти критичної інфраструктури

1. Віднесення об’єктів до об’єктів критичної інфраструктури та формування Реєстру об’єктів критичної інфраструктури здійснюються відповідно до [Закону України](https://zakon.rada.gov.ua/laws/show/1882-20) "Про критичну інфраструктуру".

*{Частина перша статті 6 в редакції Закону*[*№ 1882-IX від 16.11.2021*](https://zakon.rada.gov.ua/laws/show/1882-20#n449)*; зміни до пункту 1 частини першої статті 6, прийняті Законом*[*№ 1591-IX від 30.06.2021*](https://zakon.rada.gov.ua/laws/show/1591-20#n1483)*- вводиться в дію з 01.08.2022, внести неможливо (відсутній пункт 1)*}

2. Критерії та порядок віднесення об’єктів до об’єктів критичної інфраструктури, перелік таких об’єктів, [загальні вимоги до їх кіберзахисту](https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8), у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а щодо банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг - Національним банком України.

*{Частина друга статті 6 в редакції Законів*[*№ 1882-IX від 16.11.2021*](https://zakon.rada.gov.ua/laws/show/1882-20#n449)*,*[*№ 1591-IX від 30.06.2021*](https://zakon.rada.gov.ua/laws/show/1591-20#n1485)*- вводиться в дію з 01.08.2022}*

3. Вимоги і [порядок проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури](https://zakon.rada.gov.ua/laws/show/257-2023-%D0%BF#n11) встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України.

Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов’язковим залученням представників основних суб’єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

4. Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об’єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об’єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об’єктів критичної інфраструктури.

5. Обмін інформацією про інциденти кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог [Закону України](https://zakon.rada.gov.ua/laws/show/2297-17) "Про захист персональних даних".

**Стаття 7.**Принципи забезпечення кібербезпеки

1. Забезпечення кібербезпеки в Україні ґрунтується на принципах:

1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

2) забезпечення національних інтересів України;

3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід’ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

6) пріоритетності запобіжних заходів;

7) невідворотності покарання за вчинення кіберзлочинів;

8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

**Стаття 8.**Національна система кібербезпеки

1. Національна система кібербезпеки є сукупністю суб’єктів забезпечення кібербезпеки та взаємопов’язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури.

2. Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до [Конституції](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80) і законів України виконують в установленому порядку такі основні завдання:

1) Державна служба спеціального зв’язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, активної протидії агресії у кіберпросторі, кіберзахисту об’єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб’єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA;

*{Пункт 2 частини другої статті 8 із змінами, внесеними згідно із Законом*[*№ 2470-IX від 28.07.2022*](https://zakon.rada.gov.ua/laws/show/2470-20#n24)*}*

2) Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

*{Пункт 2 частини другої статті 8 із змінами, внесеними згідно із Законом*[*№ 720-IX від 17.06.2020*](https://zakon.rada.gov.ua/laws/show/720-20#n421)*}*

3) Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об’єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки;

*{Пункт 3 частини другої статті 8 із змінами, внесеними згідно із Законом*[*№ 720-IX від 17.06.2020*](https://zakon.rada.gov.ua/laws/show/720-20#n422)*}*

4) Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб’єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану;

5) розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

6) Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту для банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об’єктах критичної інфраструктури в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторах платіжних систем та/або учасниках платіжних систем, технологічних операторах платіжних послуг.

*{Пункт 6 частини другої статті 8 в редакції Закону*[*№ 1591-IX від 30.06.2021*](https://zakon.rada.gov.ua/laws/show/1591-20#n1487)*- вводиться в дію з 01.08.2022}*

3. Функціонування національної системи кібербезпеки забезпечується шляхом:

1) вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

3) встановлення обов’язкових вимог інформаційної безпеки об’єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об’єкти критичної інформаційної інфраструктури;

4) формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

5) залучення експертного потенціалу наукових установ, професійних та громадських об’єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

6) проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

7) функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

8) розвитку мережі команд реагування на комп’ютерні надзвичайні події;

9) розвитку та вдосконалення системи технічного і криптографічного захисту інформації;

10) забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;

11) створення та забезпечення функціонування Національної телекомунікаційної мережі;

12) обміну інформацією про інциденти кібербезпеки між суб’єктами забезпечення кібербезпеки у порядку, визначеному законодавством;

13) впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

14) підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов’язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об’єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

15) впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем;

16) встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

17) державно-приватної взаємодії у запобіганні кіберзагрозам об’єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

18) періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;

19) стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

20) розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

21) здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях;

*{Пункт 21 частини третьої статті 8 із змінами, внесеними згідно із Законом*[*№ 720-IX від 17.06.2020*](https://zakon.rada.gov.ua/laws/show/720-20#n423)*}*

22) здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;

23) обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб’єктів господарювання, які перебувають під контролем держави, визнаної Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб’єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері;

24) розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення;

25) проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки.

4. [Порядок](https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#n15) функціонування Національної телекомунікаційної мережі, критерії, [правила](https://zakon.rada.gov.ua/laws/show/1358-2020-%D0%BF#n148) та вимоги щодо надання послуг, їх тарифікації для користувачів бюджетної сфери, відшкодування витрат державного бюджету на утримання Національної телекомунікаційної мережі затверджуються Кабінетом Міністрів України.

5. Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об’єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об’єктів кіберзахисту, системи взаємодії команд реагування на комп’ютерні надзвичайні події, а також у взаємодії з іншими суб’єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

6. Органи державної влади, військові формування, утворені відповідно до законів України, державні підприємства, установи та організації з метою усунення можливих наслідків кіберінцидентів та кібератак створюють резервні копії національних електронних інформаційних ресурсів, що перебувають у їх володінні або розпорядженні та є критичними для їх сталого функціонування, та передають їх на зберігання до Національного центру резервування державних інформаційних ресурсів, крім тих, передача яких обмежена законодавством. Порядок передачі, збереження і доступу до зазначених копій визначається Кабінетом Міністрів України.

Національний центр резервування державних інформаційних ресурсів забезпечує:

1) безперервність роботи відповідного національного електронного інформаційного ресурсу, резервного копіювання інформації та відомостей національного електронного інформаційного ресурсу через єдині основний та резервний захищені центри обробки даних (дата-центри), призначені для обробки національних електронних інформаційних ресурсів, резервного копіювання національних електронних інформаційних ресурсів;

2) надійне функціонування серверного обладнання, системи зберігання даних, активного мережевого обладнання, архітектурно-технічних рішень щодо резервного копіювання й дублювання інформаційних систем, постійно працюючої інженерної інфраструктури;

3) здійснення обов’язкового контролю за статистичними даними роботи з фізичного захисту об’єктів, системи управління та моніторингу інформаційних систем, комплексу організаційних заходів;

4) розроблення, створення (побудову), модернізацію, розвиток, впровадження та супроводження програмного забезпечення інформаційної системи (платформи) для побудови та ведення реєстрів;

5) переміщення протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування резервних копій національних електронних інформаційних ресурсів до електронних комунікаційних мереж закордонних дипломатичних установ України в порядку, встановленому Кабінетом Міністрів України.

*{Частину шосту статті 8 доповнено пунктом 5 згідно із Законом*[*№ 2130-IX від 15.03.2022*](https://zakon.rada.gov.ua/laws/show/2130-20#n19)*}*

*{Статтю 8 доповнено частиною шостою згідно із Законом*[*№ 1907-IX від 18.11.2021*](https://zakon.rada.gov.ua/laws/show/1907-20#n589)*}*

**Стаття 9.**Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA

1. Завданнями CERT-UA є:

1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

2) надання власникам об’єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об’єктів;

3) організація та проведення практичних семінарів з питань кіберзахисту для суб’єктів національної системи кібербезпеки та власників об’єктів кіберзахисту;

4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

7) взаємодія з українськими командами реагування на комп’ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки кіберпростору;

8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об’єктів кіберзахисту;

9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

2. Забезпечення функціонування CERT-UA здійснює Державна служба спеціального зв’язку та захисту інформації України у межах штатної чисельності та виділених обсягів фінансування.

**Стаття 10.**Державно-приватна взаємодія у сфері кібербезпеки

1. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:

1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об’єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

4) партнерства та координації команд реагування на комп’ютерні надзвичайні події;

5) залучення експертного потенціалу, наукових установ, професійних об’єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;

6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;

8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;

10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;

11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

2. Державно-приватна взаємодія у сфері кібербезпеки застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об’єктів та окремих видів діяльності.

**Стаття 11.**Сприяння суб’єктам забезпечення кібербезпеки України

Державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об’єднання громадян зобов’язані сприяти суб’єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об’єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків.

**Стаття 12.**Відповідальність за порушення законодавства у сфері кібербезпеки

Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення кримінального правопорушення, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.

*{Стаття 12 із змінами, внесеними згідно із Законом*[*№ 720-IX від 17.06.2020*](https://zakon.rada.gov.ua/laws/show/720-20#n424)*}*

**Стаття 13.**Фінансове забезпечення заходів кібербезпеки

Джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є кошти державного і місцевих бюджетів, власні кошти суб’єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

**Стаття 14.**Міжнародне співробітництво у сфері кібербезпеки

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

2. Україна відповідно до міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення кібербезпеки, 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"](https://zakon.rada.gov.ua/laws/show/1518-14) та ["Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України"](https://zakon.rada.gov.ua/laws/show/1479-14).

3. Відповідно до законодавства України у сфері зовнішніх зносин суб’єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.

4. Інформацію з питань, пов’язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов’язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору.

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

1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному [Конституцією України](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80).

Парламентський контроль за дотриманням законодавства про захист персональних даних та доступ до публічної інформації у сфері кібербезпеки здійснюється Уповноваженим Верховної Ради України з прав людини.

2. Контроль за діяльністю із забезпечення кібербезпеки суб’єктів сектору безпеки і оборони, інших державних органів здійснюється Президентом України та Кабінетом Міністрів України в порядку, визначеному [Конституцією](https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80) і законами України.

3. Незалежний аудит діяльності основних суб’єктів національної кібербезпеки, визначених [частиною другою](https://zakon.rada.gov.ua/laws/show/2163-19#n108) статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави проводиться щороку згідно з міжнародними стандартами аудиту.

Звіти про результати проведення незалежного аудиту діяльності основних суб’єктів національної кібербезпеки, визначених [частиною другою](https://zakon.rada.gov.ua/laws/show/2163-19#n108) статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави за попередній рік подаються Президентові України, Верховній Раді України та Кабінету Міністрів України у сорокап’ятиденний строк після закінчення календарного року.

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 інформатизації та зв’язку, на своїх засіданнях розглядають звіти основних суб’єктів національної кібербезпеки, визначених [частиною другою](https://zakon.rada.gov.ua/laws/show/2163-19#n108) статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо ефективності системи забезпечення кібербезпеки держави.

Основні суб’єкти національної кібербезпеки, визначені [частиною другою](https://zakon.rada.gov.ua/laws/show/2163-19#n108) статті 8 цього Закону, подають один раз на рік звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати проведення незалежного аудиту їхньої діяльності.

За результатами розгляду звітів основних суб’єктів національної кібербезпеки Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв’язку, може порушити питання про розгляд цих питань Верховною Радою України.

ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

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

2. Внести зміни до таких законів України:

1) [статтю 7](https://zakon.rada.gov.ua/laws/show/679-14#n109) Закону України "Про Національний банк України" (Відомості Верховної Ради України, 1999 р., № 29, ст. 238 із наступними змінами) доповнити пунктами 32 і 33 такого змісту:

"32) визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб’єктів переказу коштів, здійснює контроль за їх виконанням; утворює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України;

33) забезпечує формування та ведення переліку об’єктів критичної інфраструктури, а також 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 інфраструктури та об’єктів критичної інформаційної інфраструктури, забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки у банківській системі України";

2) у [Законі України "Про оборону України"](https://zakon.rada.gov.ua/laws/show/1932-12) (Відомості Верховної Ради України, 2000 р., № 49, ст. 420; 2011 р., № 4, ст. 27; 2015 р., № 16, ст. 110; 2016 р., № 33, ст. 564):

а) [статтю 3](https://zakon.rada.gov.ua/laws/show/1932-12#n168) після абзацу дев’ятнадцятого доповнити новим абзацом такого змісту:

"здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії".

У зв’язку з цим абзац двадцятий вважати абзацом двадцять першим;

б) друге речення [частини другої](https://zakon.rada.gov.ua/laws/show/1932-12#n189) статті 4 доповнити словами "у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі";

*{Підпункт 3 пункту 2 розділу втратив чинність на підставі Закону*[*№ 912-IX від 17.09.2020*](https://zakon.rada.gov.ua/laws/show/912-20#n442)*}*

*{Підпункт 4 пункту 2 розділу втратив чинність на підставі Закону*[*№ 2469-VIII від 21.06.2018*](https://zakon.rada.gov.ua/laws/show/2469-19#n355)*}*

5) [абзац шостий](https://zakon.rada.gov.ua/laws/show/3160-15) статті 3 Закону України "Про Службу зовнішньої розвідки України" (Відомості Верховної Ради України, 2006 р., № 8, ст. 94) після слів "національній безпеці України" доповнити словами "у тому числі у кіберпросторі";

6) у [Законі України "Про Державну службу спеціального зв’язку та захисту інформації України"](https://zakon.rada.gov.ua/laws/show/3475-15) (Відомості Верховної Ради України, 2014 р., № 25, ст. 890, № 29, ст. 946):

а) [частину першу статті 2](https://zakon.rada.gov.ua/laws/show/3475-15#n31) та [абзац другий частини першої статті 3](https://zakon.rada.gov.ua/laws/show/3475-15#n35) після слів "криптографічного та технічного захисту інформації" доповнити словом "кіберзахисту";

б) у [частині першій](https://zakon.rada.gov.ua/laws/show/3475-15#n126) статті 14:

пункт 39 після слів "забезпечення функціонування" доповнити словом "урядової";

доповнити пунктами 85-92 такого змісту:

"85) формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах;

86) координація діяльності суб’єктів забезпечення кібербезпеки щодо кіберзахисту;

87) забезпечення створення та функціонування Національної телекомунікаційної мережі;

88) впровадження організаційно-технічної моделі кіберзахисту, здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;

89) інформування про кіберзагрози та відповідні методи захисту від них;

90) забезпечення впровадження системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки, їх атестації (переатестації);

91) координація, організація та проведення аудиту захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на вразливість;

92) забезпечення функціонування Державного центру кіберзахисту".

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

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

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

забезпечити перегляд і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів, що суперечать цьому Закону.

*1.1.3. ЗУ «Про державну таємницю». «Про захист персональних даних*

ЗУ Про державну таємницю

**Стаття 1.**Визначення термінів

У цьому Законі терміни вживаються у такому значенні:

державна таємниця (далі також - секретна інформація) - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;

віднесення інформації до державної таємниці - процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обгрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до [Зводу відомостей, що становлять державну таємницю](https://zakon.rada.gov.ua/laws/show/z0052-21#n13), та з опублікуванням цього Зводу, змін до нього;

гриф секретності - реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації;

державний експерт з питань таємниць - посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування;

допуск до державної таємниці - оформлення права громадянина на доступ до секретної інформації;

доступ до державної таємниці - надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;

засекречування матеріальних носіїв інформації - введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

[Звід відомостей, що становлять державну таємницю](https://zakon.rada.gov.ua/laws/show/z0052-21#n13), - акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених цим Законом сферах;

категорія режиму секретності - категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях;

криптографічний захист секретної інформації - вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

матеріальні носії секретної інформації - матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо;

охорона державної таємниці - комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;

режим секретності - встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці;

розсекречування матеріальних носіїв секретної інформації - зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

спеціальна експертиза щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, - експертиза, що проводиться з метою визначення в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, передбачених цим Законом, для провадження діяльності, пов'язаної з державною таємницею;

ступінь секретності ("особливої важливості", "цілком таємно", "таємно") - категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою;

технічний захист секретної інформації - вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

ЗУ Про захист персональних даних

**Стаття 1. Сфера дії Закону**

Цей Закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.

Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

*{Частину третю статті 1 виключено на підставі Закону*[*№ 383-VII від 03.07.2013*](https://zakon.rada.gov.ua/laws/show/383-18#n30)*}*

*{Частину четверту статті 1 виключено на підставі Закону*[*№ 383-VII від 03.07.2013*](https://zakon.rada.gov.ua/laws/show/383-18#n30)*}*

*{Стаття 1 в редакції Закону*[*№ 5491-VI від 20.11.2012*](https://zakon.rada.gov.ua/laws/show/5491-17#n6)*}*

**Стаття 2. Визначення термінів**

У цьому Законі нижченаведені терміни вживаються в такому значенні:

база персональних даних - іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;

володілець персональних даних - фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

*{Абзац третій статті 2 із змінами, внесеними згідно із Законом*[*№ 5491-VI від 20.11.2012*](https://zakon.rada.gov.ua/laws/show/5491-17#n13)*; в редакції Закону*[*№ 383-VII від 03.07.2013*](https://zakon.rada.gov.ua/laws/show/383-18#n32)*}*

згода суб’єкта персональних даних - добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб’єкта персональних даних може бути надана під час реєстрації в інформаційно-комунікаційній системі суб’єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки;

*{Абзац четвертий статті 2 в редакції Закону*[*№ 1262-VII від 13.05.2014*](https://zakon.rada.gov.ua/laws/show/1262-18#n14)*; із змінами, внесеними згідно із Законами*[*№ 675-VIII від 03.09.2015*](https://zakon.rada.gov.ua/laws/show/675-19#n222)*,*[*№ 1089-IX від 16.12.2020*](https://zakon.rada.gov.ua/laws/show/1089-20#n2360)*}*

*{Абзац п'ятий статті 2 виключено на підставі Закону*[*№ 383-VII від 03.07.2013*](https://zakon.rada.gov.ua/laws/show/383-18#n34)*}*

знеособлення персональних даних - вилучення відомостей, які дають змогу прямо чи опосередковано ідентифікувати особу;

*{Абзац шостий статті 2 із змінами, внесеними згідно із Законом*[*№ 5491-VI від 20.11.2012*](https://zakon.rada.gov.ua/laws/show/5491-17#n16)*}*

картотека - будь-які структуровані персональні дані, доступні за визначеними критеріями, незалежно від того, чи такі дані централізовані, децентралізовані або розділені за функціональними чи географічними принципами;

*{Статтю 2 доповнено терміном згідно із Законом*[*№ 5491-VI від 20.11.2012*](https://zakon.rada.gov.ua/laws/show/5491-17#n19)*}*

обробка персональних даних - будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем;

*{Абзац статті 2 в редакції Закону*[*№ 5491-VI від 20.11.2012*](https://zakon.rada.gov.ua/laws/show/5491-17#n17)*}*

одержувач - фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа;

*{Статтю 2 доповнено терміном згідно із Законом*[*№ 5491-VI від 20.11.2012*](https://zakon.rada.gov.ua/laws/show/5491-17#n19)*}*

персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

розпорядник персональних даних - фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця;

*{Абзац одинадцятий статті 2 із змінами, внесеними згідно із Законом*[*№ 5491-VI від 20.11.2012*](https://zakon.rada.gov.ua/laws/show/5491-17#n22)*}*

суб’єкт персональних даних - фізична особа, персональні дані якої обробляються;

*{Абзац дванадцятий статті 2 в редакції Закону*[*№ 383-VII від 03.07.2013*](https://zakon.rada.gov.ua/laws/show/383-18#n35)*}*

третя особа - будь-яка особа, за винятком суб’єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних.

*{Абзац тринадцятий статті 2 в редакції Закону*[*№ 383-VII від 03.07.2013*](https://zakon.rada.gov.ua/laws/show/383-18#n35)*}*

*1.1.4. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури*

**АГАЛЬНІ ВИМОГИ**  
**до кіберзахисту об’єктів критичної інфраструктури**

*{У тексті Загальних вимог слова “інформаційно-телекомунікаційні системи” в усіх відмінках замінено словами “інформаційно-комунікаційні системи” у відповідному відмінку згідно з Постановою КМ*[*№ 991 від 02.09.2022*](https://zakon.rada.gov.ua/laws/show/991-2022-%D0%BF#n25)*}*

1. Ці Загальні вимоги визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання підприємствами, установами та організаціями, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури.

2. У цих Загальних вимогах терміни вживаються у такому значенні:

критичні бізнес/операційні процеси об’єкта критичної інфраструктури - процеси організації функціонування об’єктів критичної інфраструктури, реалізація загроз на які призводить до виведення з ладу або порушення функціонування самого об’єкта критичної інфраструктури та відповідно справляє негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіює майнову шкоду та/або становить загрозу для суспільства, життя і здоров’я людей; для організації функціонування цього процесу можуть використовуватися декілька інформаційно-комунікаційних систем;

система інформаційної безпеки - сукупність організаційних та технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури з метою запобігання кіберінцидентам, виявлення та захисту від кібератак, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, запобігання порушенню режиму функціонування та/або недоступності служб (функцій) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, порушенню функціонування компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури; забезпечення спостережності за діями користувачів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та функціонуванням засобів захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

політика інформаційної безпеки - політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об’єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки.

Інші терміни вживаються у значенні, наведеному в Законах України [“Про основні засади забезпечення кібербезпеки України”](https://zakon.rada.gov.ua/laws/show/2163-19), “[Про захист інформації в інформаційно-комунікаційних системах](https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#n3)”, [Правилах забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах](https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF), затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 (Офіційний вісник України, 2006 p., № 13, ст. 878).

*{Абзац п'ятий пункту 2 із змінами, внесеними згідно з Постановою КМ*[*№ 991 від 02.09.2022*](https://zakon.rada.gov.ua/laws/show/991-2022-%D0%BF#n23)*}*

3. Кіберзахист об’єкта критичної інфраструктури забезпечується шляхом впровадження на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю.

4. Кіберзахист об’єкта критичної інфраструктури є складовою частиною робіт із створення (модернізації) та експлуатації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

5. Кіберзахист об’єкта критичної інфраструктури забезпечується власником та/або керівником об’єкта критичної інфраструктури відповідно до цих Загальних вимог та законодавства в сфері захисту інформації та кібербезпеки.

6. У випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог повинні бути враховані під час створення (модернізації) на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури комплексної системи захисту інформації, а їх відповідність перевіряється під час її державної експертизи в сфері технічного захисту інформації.

Створення комплексної системи захисту інформації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та її державна експертиза здійснюються відповідно до вимог законодавства в сфері захисту інформації та охорони державної таємниці.

7. У випадку, якщо на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури не обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, положення цих Загальних вимог враховуються під час створення (модернізації) системи інформаційної безпеки об’єкта критичної інфраструктури. Виконання Загальних вимог перевіряється під час незалежного аудиту інформаційної безпеки на об’єкті критичної інфраструктури.

Створення системи інформаційної безпеки об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури здійснюється відповідно до вимог технічного завдання на створення системи інформаційної безпеки.

Технічне завдання формується за результатами оцінки ризиків, які зазначаються в звіті за результатами оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури. Методичною основою для оцінки ризиків на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури є стандарт ДСТУ ISO/IEC 27005.

Власник та/або керівник об’єкта критичної інфраструктури організовує проведення незалежного аудиту інформаційної безпеки на об’єкті критичної інфраструктури згідно з вимогами законодавства в сфері захисту інформації та кібербезпеки.

8. Власник та/або керівник об’єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA (у разі наявності - галузевої команди реагування на комп’ютерні надзвичайні події), а також функціонального підрозділу контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Центрального управління СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

9. Державні органи отримують доступ до Інтернету через систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту, через постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних із створеними комплексними системами захисту інформації з підтвердженою відповідністю, або через власні системи захищеного доступу до Інтернету із створеними комплексними системами захисту інформації з підтвердженою відповідністю. Ця вимога не поширюється на інформаційно-комунікаційні системи закордонних дипломатичних установ України.

*{Пункт 9 із змінами, внесеними згідно з Постановою КМ*[*№ 991 від 02.09.2022*](https://zakon.rada.gov.ua/laws/show/991-2022-%D0%BF#n24)*}*

10. Власник та/або керівник об’єкта критичної інфраструктури з метою усунення можливих наслідків кіберінцидентів та кібератак забезпечує створення резервних копій інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та критичних бізнес/операційних процесів об’єкта критичної інфраструктури для оперативного їх відновлення у разі пошкодження або знищення.

Державні органи для збереження резервних копій своїх інформаційних ресурсів та їх оперативного відновлення використовують основний та резервний захищений дата-центр збереження державних електронних інформаційних ресурсів Державного центру кіберзахисту.

11. Державні органи з метою здійснення захищеного інформаційного обміну, зберігання резервних копій інформаційних ресурсів, підключення до системи захищеного доступу державних органів до Інтернету Державного центру кіберзахисту використовують ресурси Національної телекомунікаційної мережі.

12. Організаційні та технічні заходи з кіберзахисту, які впроваджуються на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, повинні забезпечувати:

формування на об’єкті критичної інфраструктури загальної політики інформаційної безпеки;

управління доступом користувачів та адміністраторів до об’єктів захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

ідентифікацію та автентифікацію користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

реєстрацію подій компонентами об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та їх періодичний аудит;

мережевий захист компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

доступність та відмовостійкість компонентів та інформаційних ресурсів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

визначення умов використання змінних (зовнішніх) пристроїв та носіїв інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

визначення умов використання програмного та апаратного забезпечення об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;

визначення умов розміщення компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури.

Перелік базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури, які повинні бути впроваджені під час створення комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, наведено у [додатку](https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n49).

Перелік базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури може бути доповнено відповідно до технології обробки інформації на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури, особливостей функціонування та програмно-апаратного складу об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, складу інформаційних ресурсів та компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, які підлягають захисту, тощо.

Під час доповнення переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури для кожної загрози об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури передбачаються захід або комплекс заходів, що забезпечують блокування однієї чи декількох загроз або знижують ризик її реалізації, та враховуються умови функціонування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури. У разі коли перелік мінімальних заходів не дає можливості забезпечити блокування (нейтралізацію) усіх загроз об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, повинні бути визначені додаткові заходи, які ці загрози блокують.

Формування додаткових заходів із забезпечення кіберзахисту об’єктів критичної інфраструктури розробник комплексної системи захисту інформації (системи інформаційної безпеки) об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури здійснює з урахуванням вимог нормативних документів у сфері технічного захисту інформації, міжнародних стандартів з питань інформаційної безпеки.

13. У разі відсутності можливості виконання окремих вимог із забезпечення кіберзахисту, наведених у [додатку](https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n49), і/або неможливості їх застосування до окремих об’єктів захисту чи користувачів та адміністраторів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, у тому числі внаслідок їх можливого негативного впливу на функціонування об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, або неможливості їх здійснення на об’єкті критичної інформаційної інфраструктури об’єкта критичної інфраструктури через особливості функціонування, або відсутності складу компонентів об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні бути розроблені і впроваджені компенсуючі заходи, що забезпечують блокування (нейтралізацію) загроз об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури, або обґрунтовано виключені окремі вимоги з переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури.

Власник та/або керівник об’єкта критичної інфраструктури у ході розроблення організаційних і технічних заходів щодо забезпечення кіберзахисту об’єкта критичної інфраструктури обґрунтовує застосування компенсуючих заходів або виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури. При цьому під час проведення незалежного аудиту інформаційної безпеки об’єкта критичної інфраструктури або державної експертизи комплексної системи захисту інформації об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури має бути оцінена достатність і адекватність компенсуючих заходів, які застосовані для блокування (нейтралізації) загроз об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури та зменшення ризиків об’єкта критичної інфраструктури, або обґрунтованість виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури.

Рішення з обґрунтуванням щодо впровадження компенсуючих заходів або виключення окремих вимог з переліку базових вимог із забезпечення кіберзахисту об’єктів критичної інфраструктури оформлюється окремим рішенням за підписом власника та/або керівника об’єкта критичної інфраструктури.

14. Міністерства та інші центральні органи виконавчої влади можуть розробляти конкретизовані вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування об’єктів критичної інфраструктури, які відносяться до сфери їх управління. Такі вимоги з кіберзахисту погоджуються з Адміністрацією Держспецзв’язку.

СБУ має право подавати міністерствам та іншим центральним органам виконавчої влади обов’язкові для розгляду пропозиції щодо таких вимог з кіберзахисту.

*1.1.5. Державні Стандарти України в галузі інформаційної та/або кібербезпеки ДСТУ 3396.0,1,2-97 , ДСТУ ISO/ІЕС 15408-1:2017*

ДСТУ 3396.0,1,2-97

0

1 Галузь використання

Цей стандарт установлює об’єкт, мету, основні організаційнотехнічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ. Вимоги стандарту обов’язкові для підприємств та установ усіх форм власності і підпорядкування, громадян - суб’єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

2 Нормативні посилання

У цьому стандарті наведено посилання на такі документи: - ДСТУ 1.0-93 Державна система стандартизації України. Основні положення; - ДСТУ 1.2-93 Державна система стандартизації України. Порядок розроблення державних стандартів; - ДСТУ 1.3-93 Державна система стандартизації України. Порядок розроблення, побудови, викладу, оформлення, узгодження, затвердження, позначення та реєстрації технічних умов; - ДСТУ 1.4-93 Державна система стандартизації України. Стандарт підприємства. Основні положення; - ДСТУ 1.5-93 Державна система стандартизації України. Загальні вимоги до побудови, викладу, оформлення і змісту стандартів; - ДБН А.1.1-1-93 Система стандартизації та нормування в будівництві. Основні положення; - ДБН А.1.1-2-93 Система стандартизації та нормування в будівництві. Порядок розробки, вимоги до побудови, викладу та оформлення нормативних документів.

3 Загальні положення

3.1 Об’єктом технічного захисту є інформація, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження (далі - інформація з обмеженим доступом, ІзОД).

3.2 Об’єкт, мету і завдання ТЗІ визначають і встановлюють особи, які володіють, користуються, розпоряджаються ІзОД у межах прав і повноважень, наданих законами України, підзаконними актами та нормативними документами системи ТЗІ.

3.3 Носіями ІзОД можуть бути фізичні поля, сигнали, хімічні речовини, що утворюються в процесі інформаційної діяльності, виробництва й експлуатації продукції різного призначення (далі - інформаційна діяльність).

3.4 Середовищем поширення носіїв ІзОД можуть бути лінії зв’язку, сигналізації, керування, енергетичні мережі, прикінцеве і проміжне обладнання, інженерні комунікації і споруди, відгороджувальні будівельні конструкції, а також світлопроникні елементи будинків і споруд (отвори), повітряне, водне та інші середовища, грунт, рослинність тощо.

3.5 Витік або порушення цілісності IзОД (спотворення, модифікація, руйнування, знищення) можуть бути результатом реалізації загроз безпеці інформації (далі - загроза).

3.6 Метою ТЗІ є запобігання витоку або порушенню цілісності ІзОД. 3.7 Мета ТЗІ може бути досягнута побудовою системи захисту інформації, що є організованою сукупністю методів і засобів забезпечення ТЗІ. Технічний захист інформації здійснюється поетапно: 1 етап - визначення й аналіз загроз; 2 етап - розроблення системи захисту інформації; 3 етап - реалізація плану захисту інформації; 4 етап - контроль функціювання та керування системою захисту інформації. 2

4 Побудова системи захисту інформації

4.1 Визначення й аналіз загроз

4.1.1 На першому етапі необхідно здійснити аналіз об’єктів ТЗІ, ситуаційного плану, умов функціювання підприємства, установи, організації, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати засадничі дані для побудови окремої моделі загроз.

4.1.2 Джерелами загроз може бути діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб.

4.1.3 Загрози можуть здійснюватися: - технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали; - каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації; - несанкційованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

4.1.4 Опис загроз і схематичне подання шляхів їх здійснення складають окрему модель загроз.

4.2 Розроблення системи захисту інформації

4.2.1 На другому етапі слід здійснити розроблення плану ТЗІ, що містить організаційні, первинні технічні та основні технічні заходи захисту ІзОД, визначити зони безпеки інформації. Організаційні заходи регламентують порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу об’єкта ТЗІ. Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів ТЗІ. Основні технічні заходи передбачають захист інформації з використанням засобів забезпечення ТЗІ.

4.2.2 Для технічного захисту інформації слід застосовувати спосіб приховування або спосіб технічної дезінформації.

4.2.3 Заходи захисту інформації повинні: - бути відповідними загрозам; - бути розробленими з урахуванням можливої шкоди від їх реа-лізації і вартості захисних заходів та обмежень, що вносяться ними; 3 - забезпечувати задану ефективність захисту інформації на встановленому рівні протягом часу обмеження доступу до неї або можливості здійснення загроз.

4.2.4 Рівень захисту інформації означується системою кількісних та якісних показників, які забезпечують розв’язання завдання захисту інформації на основі норм та вимог ТЗІ.

4.2.5 Мінімально необхідний рівень захисту інформації забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі. Підвищення рівня захисту інформації досягається нарощуванням технічних заходів протидії безлічі загроз.

4.2.6 Порядок розрахунку та інструментального визначення зон безпеки інформації, реалізації заходів ТЗІ, розрахунку ефективності захисту та порядок атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) установлюються нормативними документами системи ТЗІ. 4.3 Реалізація плану захисту інформації

4.3.1 На третьому етапі слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту ІзОД, установити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, технічних засобів захисту інформації, робочих місць (приміщень) на відповідність вимогам безпеки інформації.

4.3.2 Технічний захист інформації забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації (далі - засоби ТЗІ) та контролю ефективності захисту, які мають cертифікат відповідності вимогам нормативних документів системи УкрСЕПРО або дозвіл на їх використання від уповноваженого Кабінетом Мі-ністрів України органу, а також застосуванням спеціальних інженернотехнічних споруд, засобів і систем (далі - засоби забезпечення ТЗІ).

4.3.3 Засоби ТЗІ можуть функціювати автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складових елементів.

4.3.4 Склад засобів забезпечення ТЗІ, перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, що володіють, користуються і розпоряджаються ІзОД самостійно або за рекомендаціями спеціалістів з ТЗІ згідно з нормативними документами системи ТЗІ.

4.3.5 Надання послуг з ТЗІ, атестацію та сервісне обслуговування засобів забезпечення ТЗІ можуть здійснювати юридичні і фізичні особи, що мають ліцензію на право проведення цих робіт, видану уповноваженим Кабінетом Міністрів України органом.

4.4 Контроль функціювання та керування системою захисту інформації

4.4.1 На четвертому етапі слід провести аналіз функціювання системи захисту інформації, перевірку виконання заходів ТЗІ, контроль ефективності захисту, підготувати та видати засадничі дані для керування системою захисту інформації.

4.4.2 Керування системою захисту інформації полягає у адаптації заходів ТЗІ до поточного завдання захисту інформації. За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізуються у найкоротший строк. 4.4.3 У разі потреби підвищення рівня захисту інформації необхідно виконати роботи, передбачені 1, 2 та 3 етапами побудови системи захисту інформації. 4.4.4 Порядок проведення перевірок і контролю ефективності захисту інформації встановлюється нормативними документами.

5 Нормативні документи системи ТЗІ

5.1 Нормативні документи розробляються в ході проведення комплексу робіт із стандартизації та нормування у галузі ТЗІ.

5.2 Нормативні документи повинні забезпечувати: - проведення єдиної технічної політики; - створення і розвиток єдиної термінологічної системи; - функціювання багаторівневих систем захисту інформації на основі взаємнопогоджених положень, правил, методик, вимог та норм; - функціювання систем сертифікації, ліцензування й атестації згідно з вимогами безпеки інформації; - розвиток сфери послуг у галузі ТЗІ; - установлення порядку розроблення, виготовлення, експлуатації засобів забезпечення ТЗІ та спеціальної контрольно-вимірювальної апа-ратури; - організацію проектування будівельних робіт у частині забезпечення ТЗІ; - підготовку та перепідготовку кадрів у системі ТЗІ.

5.3 Нормативні документи системи ТЗІ поділяються на: - нормативні документи із стандартизації у галузі ТЗІ; - державні стандарти та прирівняні до них нормативні документи; 5 - нормативні акти міжвідомчого значення, що реєструються у Міністерстві юстиції України; - нормативні документи міжвідомчого значення технічного характеру, що реєструються уповноваженим Кабінетом Міністрів органом; - нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

5.4 Порядок проведення робіт із стандартизації та нормування в галузі ТЗІ встановлюється ДСТУ 1.0, ДБН А.1.1-1, документами системи ТЗІ.

5.5 Порядок розроблення, оформлення, узгодження, затвердження, реєстрації, видання, впровадження, перевірки, перегляду, зміни та скасування нормативних документів установлюється ДСТУ 1.2, ДСТУ 1.3, ДСТУ 1.4, ДСТУ 1.5, ДБН А.1.1-2, документами системи ТЗІ.

1

1 Галузь використання

Цей стандарт установлює вимоги до порядку проведення робіт з технічного захисту інформації (ТЗІ). Вимоги стандарту обов`язкові для підприємств та установ усіх форм власності й підпорядкування, громадян-суб`єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

2 Нормативні посилання

У цьому стандарті наведено посилання на такий стандарт: ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

3 Загальні положення

3.1 Інформація з обмеженим доступом (ІзОД) в процесі інформаційної діяльності (ІД), основними видами якої є одержання, використання, поширення та зберігання ІзОД, може зазнавати впливу загроз її безпеці (далі - загроза), у результаті чого може відбутися її витік або порушення цілісності інформації. Схильність ІзОД до впливу загроз визначає її вразливість. Здатність системи захисту інформації протистояти впливу загроз визначає захищеність ІзОД.

3.2 Можливі такі варіанти захисту інформації: - досягнення необхідного рівня захисту ІзОД за мінімальних затрат і допустимого рівня обмежень видів ІД; - досягнення необхідного рівня захисту ІзОД за допустимих затрат і заданого рівня обмежень видів ІД; - досягнення максимального рівня захисту ІзОД за необхідних затрат і мінімального рівня обмежень видів ІД. Захист інформації, яка не є державною таємницею, забезпечується, як правило, застосуванням першого чи другого варіанту. Захист інформації, яка становить державну таємницю, забезпечується, як правило, застосуванням третього варіанту.

3.3 Зміст та послідовність робіт з протидії загрозам або їхньої нейтралізації повинні відповідати зазначеним в ДСТУ 3396.0-96 етапам функціювання системи захисту інформації і полягає в: - проведенні обстеження підприємства, установи, організації (далі - підприємство); - розробленні і реалізації організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення ТЗІ (додаток А); - прийманні робіт з ТЗІ; - атестації засобів (систем) забезпечення ІД на відповідність вимогам нормативних документів з ТЗІ.

3.4 Порядок проведення робіт з ТЗІ або окремих їхніх етапів установлюється наказом (розпорядженням) керівника підприємства. Роботи повинні виконуватися силами підприємства під керівництвом спеціалістів з ТЗІ. Для участі в роботах, подання методичної допомоги, оцінювання повноти та якості реалізації заходів захисту можуть залучатися спеціалісти з ТЗІ інших організацій, які мають ліцензію органа, уповноваженого Кабінетом Міністрів України.

4 Організація проведення обстеження

4.1 Метою обстеження підприємства є вивчення його ІД, визначення об`єктів захисту - ІзОД, виявлення загроз, їхній аналіз та побудова окремої моделі загроз.

4.2 Обстеження повинно бути проведено комісією, склад якої визначається відповідальною за ТЗІ особою і затверджується наказом керівника підприємства.

4.3 У ході обстеження необхідно: - провести аналіз умов функціювання підприємства, його розташування на місцевості (ситуаційного плану) для визначення можливих джерел загроз; - дослідити засоби забезпечення ІД, які мають вихід за межі контрольованої території; - вивчити схеми засобів і систем життєзабезпечення підприємства (електроживлення, уземлення, автоматизації, пожежної та охоронної сигналізацій), а також інженерних комунікацій та металоконструкцій; - дослідити інформаційні потоки, технологічні процеси передачі, одержання, використання, розповсюдження і зберігання (далі - оброблення) інформації і провести необхідні вимірювання; - визначити наявність та технічний стан засобів забезпечення ТЗІ; - перевірити наявність на підприємстві нормативних документів, які забезпечують функціювання системи захисту інформації, організацію проектування будівельних робіт з урахуванням вимог ТЗІ, а також нормативної та експлуатаційної документації, яка забезпечує ІД; - виявити наявність транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених у каналізацію) кабелів, кіл і проводів; - визначити технічні засоби і системи, застосування яких не обгрунтовано службовою чи виробничою необхідністю і які підлягають демонтуванню; 2 - визначити технічні засоби, що потребують переобладнання (перемонтування) та встановлення засобів ТЗІ.

4.4 За результатами обстеження слід скласти акт, який повинен бути затверджений керівником підприємства.

4.5 Матеріали обстеження необхідно використовувати під час розроблення окремої моделі загроз, яка повинна включати: - генеральний та ситуаційний плани підприємства, схеми розташування засобів і систем забезпечення ІД, а також інженерних комунікацій, які виходять за межі контрольованої території; - схеми та описи каналів витоку інформації, каналів спеціального впливу і шляхів несанкційованого доступу до ІзОД; - оцінку шкоди, яка передбачається від реалізації загроз.

5 Організація розроблення системи захисту інформації

5.1 На підставі матеріалів обстеження та окремої моделі загроз необхідно визначити головні задачі захисту інформації і скласти технічне завдання (ТЗ) на розроблення системи захисту інформації.

5.2 ТЗ повинно включати основні розділи: - вимоги до системи захисту інформації; - вимоги до складу проектної та експлуатаційної документації; - етапи виконання робіт; - порядок внесення змін і доповнень до розділів ТЗ; - вимоги до порядку проведення випробування системи захисту.

5.3 Основою функціювання системи захисту інформації є план ТЗІ, що повинен містити такі документи: - перелік розпорядчих, організаційно-методичних, нормативних документів з ТЗІ, а також вказівки щодо їхнього застосування; - інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту; - інструкції, що встановлюють обов`язки, права та відповідальність персоналу; - календарний план ТЗІ.

5.4 ТЗ і план ТЗІ розробляють спеціалісти з ТЗІ, узгоджують із зацікавленими підрозділами (організаціями). Затверджує їх керівник підприємства.

6 Реалізація організаційних заходів захисту

6.1 Організаційні заходи захисту інформації - комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціювання засобів (систем) забезпечення ІД та засобів (систем) забезпечення ТЗІ.

6.2 У процесі розроблення і реалізації організаційних заходів потрібно: - визначити окремі задачі захисту ІзОД; - обгрунтувати структуру і технологію функціювання системи захисту інформації; - розробити і впровадити правила реалізації заходів ТЗІ; 3 - визначити і встановити права та обов`язки підрозділів та осіб, що беруть участь в обробленні ІзОД; - придбати засоби забезпечення ТЗІ та нормативні документи і забезпечити ними підприємство; - установити порядок упровадження захищених засобів оброблення інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ; - установити порядок контролю функціювання системи захисту інформації та її якісних характеристик; - визначити зони безпеки інформації; - установити порядок проведення атестації системи захисту інформаціїі, її елементів і розробити програми атестаційного випробування; - забезпечити керування системою захисту інформації.

6.3 Оперативне вирішення задач ТЗІ досягається організацією керування системою захисту інформації, для чого необхідно: - вивчати й аналізувати технологію проходження ІзОД у процесі ІД; - оцінювати схильність ІзОД до впливу загроз у конкретний момент часу; - оцінювати очікувану ефективність застосування засобів забезпечення ТЗІ; - визначати (за необхідності) додаткову потребу в засобах забезпечення ТЗІ; - здійснювати збирання, оброблення та реєстрацію даних, які відносяться до ТЗІ; - розробляти і реалізовувати пропозиції щодо коригування плану ТЗІ в цілому або окремих його елементів.

7 Реалізація первинних технічних заходів захисту

7.1 У процесі реалізації первинних технічних заходів потрібно забезпечити: - блокування каналів витоку інформації; - блокування несанкційованого доступу до інформації чи її носіїв; - перевірку справності та працездатності технічних засобів забезпечення ІД.

7.2 Блокування каналів витоку інформації може здійснюватися: - демонтуванням технічних засобів, ліній зв'язку, сигналізації та керування, енергетичних мереж, використання яких не пов'язано з життєзабезпеченням підприємства та обробленням ІзОД; - видаленням окремих елементів технічних засобів, які є середовищем поширення полів та сигналів, з приміщень, де циркулює ІзОД; - тимчасовим відключенням технічних засобів, які не беруть участі в обробленні ІзОД, від ліній зв'язку, сигналізації, керування та енергетичних мереж; - застосуванням способів та схемних рішень із захисту інформації, що не порушують основних технічних характеристик засобів забезпечення ІД.

7.3 Блокування несанкційованого доступу до інформації або її носіїв може здійснюватися: 4 - створенням умов роботи в межах установленого регламенту; - унеможливленням використання програмних, програмно-апаратних засобів, що не пройшли перевірки (випробування).

7.4 Перевірку справності та працездатності технічних засобів і систем забезпечення ІД необхідно проводити відповідно до експлуатаційних документів. Виявлені несправні блоки й елементи можуть сприяти витоку або порушенню цілісності інформації і підлягають негайній заміні (демонтуванню).

8 Реалізація основних технічних заходів захисту

8.1 У процесі реалізації основних технічних заходів захисту потрібно: - установити засоби виявлення та індикації загроз і перевірити їхню працездатність; - установити захищені засоби оброблення інформації, засоби ТЗІ та перевірити їхню працездатність; - застосувати програмні засоби захисту в засобах обчислювальної техніки, автоматизованих системах, здійснити їхнє функційне тестування і тестування на відповідність вимогам захищеності; - застосувати спеціальні інженерно-технічні споруди, засоби (системи).

8.2 Вибір засобів забезпечення ТЗІ зумовлюється фрагментарним або комплексним способом захисту інформації. Фрагментарний захист забезпечує протидію певній загрозі. Комплексний захист забезпечує одночасну протидію безлічі загроз.

8.3 Засоби виявлення та індикації загроз застосовують для сигналізації та оповіщення власника (користувача, розпорядника) ІзОД про витік інформації чи порушення її цілісності.

8.4 Засоби ТЗІ застосовуються автономно або спільно з технічними засобами забезпечення ІД для пасивного або активного приховування ІзОД. Для пасивного приховування застосовують фільтри-обмежувачі, лінійні фільтри, спеціальні абонентські пристрої захисту та електромагнітні екрани. Для активного приховування застосовують вузькосмугові й широкосмугові генератори лінійного та просторового зашумлення.

8.5 Програмні засоби застосовуються для забезпечення: - ідентифікації та автентифікації користувачів, персоналу і ресурсів системи оброблення інформації; - розмежування доступу користувачів до інформації, засобів обчислювальної техніки і технічних засобів автоматизованих систем; - цілісності інформації та конфігурації автоматизованих систем; - реєстрації та обліку дій користувачів; - маскування оброблюваної інформації; - реагування (сигналізації, відключення, зупинення робіт, відмови у запиті) на спроби несанкційованих дій.

8.6 Спеціальні інженерно-технічні споруди, засоби та системи застосовуються для оптичного, акустичного, електромагнітного та іншого екранування носіїв інформації. 5 До них належать спеціально обладнані світлопроникні, технологічні та санітарно-технічні отвори, а також спеціальні камери, перекриття, навіси, канали тощо.

8.7 Розміщення, монтування та прокладання спеціальних інженернотехнічних засобів і систем, серед них систем уземлення та електроживлення засобів забезпечення ІД, слід здійснювати відповідно до вимог нормативних документів з ТЗІ.

8.8 Технічні характеристики, порядок застосування та перевірки засобів забезпечення ТЗІ наводять у відповідній експлуатаційній документації.

9 Приймання, визначення повноти та якості робіт

9.1 За результатами виконання рекомендацій акта обстеження та реалізації заходів захисту ІзОД слід скласти у довільній формі акт приймання робіт з ТЗІ, який повинен підписати виконавець робіт, особа, відповідальна за ТЗІ, та затвердити керівник підприємства. Примітка. За потреби акт приймання робіт може бути погоджений із зацікавленими організаціями.

9.2 Для визначення повноти та якості робіт з ТЗІ слід провести атестацію. Атестація виконується організаціями, які мають ліцензії на право діяльності в галузі ТЗІ.

9.3 Об`єктами атестації є системи забезпечення ІД та їхні окремі елементи, де циркулює інформація, що підлягає технічному захисту.

9.4 У ході атестації потрібно: - установити відповідність об`єкта, що атестується, вимогам ТЗІ; - оцінити якість та надійність заходів захисту інформації; - оцінити повноту та достатність технічної документації для об`єкта атестації; - визначити необхідність внесення змін і доповнень до організаційнорозпорядчих документів тощо. Порядок атестації встановлюється нормативними документами системи ТЗІ.

2

**1 ГАЛУЗЬ ВИКОРИСТАННЯ**

Цей стандарт установлює терміни та визначення понять у сфері технічного захисту інформації (ТЗІ).

Терміни, регламентовані у цьому стандарті, обов’язкові для ви­користання в усіх видах організаційної та нормативної документації, а також для робіт зі стандартизації і рекомендовані для використан­ня у довідковій та навчально-методичній літературі, що належить до сфери технічного захисту інформації.

Терміни стандарту є обов’язковими для використання підпри­ємствами та установами усіх форм власності і підпорядкування, громадянами-суб'єктами підприємницької діяльності, міністерствами (ві­домствами), центральними і місцевими органами державної виконав­чої влади, військовими частинами усіх військових формувань, пред­ставництвами України за кордоном, які володіють, використовують та розпоряджаються інформацією, що становить державну чи іншу пе­редбачену законом таємницю або є конфіденційною інформацією, яка належить державі.

**2 ОСНОВНІ ПОЛОЖЕННЯ**

2.1 Для кожного поняття встановлено один стандартизований термін. Терміни-синоніми подано як довідкові, вони не є стандар­тизованими.

2.2 Узята в круглі дужки частина терміна може бути опущена в разі використання терміна в документах з технічного захисту ін­формації. Позначку, що вказує на галузь застосування багатозначні і ного терміна, подано в круглих дужках світлим шрифтом, після терміна. Позначка не е частиною терміна.

2.3 У разі необхідності подані визначення можна змінювати, вводячи до них похідні ознаки з уточненням значення вживаних тер­мінів. У випадках, коли в терміні містяться всі необхідні й достатні ознаки понять, замість їхнього визначення поставлено риску.

2.4 У стандарті як довідкові подано переклади термінів англій­ською (еn) та російською (ru) мовами, визначень — російською мовою.

2.5 У стандарті наведено абетковий покажчик термінів україн­ською мовою та абеткові покажчики англійських та російських пе­рекладів термінів.

2.6  Стандартизовані терміни набрано напівгрубим шрифтом, їхні короткі форми, подані абревіатурою, — прямим світлим, а си­ноніми — курсивом.

ДСТУ ISO/ІЕС 15408-1:2017

ДСТУ ISO/IEC 15408. Інформаційні технології. Методи захисту. Критерії оцінки. Безпека інформаційних технологій (ІТ) стоїть у ряду найактуальніших проблем інформатизації суспільства. Її розв’язання значною мірою визначається досконалістю відповідної нормативно-методичної бази. Дана доповідь присвячена одному з найбільш значущих в цьому плані документів – міжнародному стандарту ISO/IEC 15408 “Критерії оцінки безпеки інформаційних технологій ”

Стандарт ISO 15408 – один з найбільш поширених стандартів у галузі безпеки. У його створенні взяли участь організації зі США, Канади, Англії, Франції, Німеччини, Голландії. У стандарті, що отримав назву «Загальні критерії оцінки безпеки інформаційних технологій» (The Common Criteria for Information Technology Security Evaluation), докладно розглянуто загальні підходи, методи та функції забезпечення захисту інформації в організаціях.

Функції системи інформаційної безпеки забезпечують виконання вимог конфіденційності, цілісності, достовірності та доступності інформації. Всі функції представлені у вигляді чотирирівневої ієрархічної структури: клас – сімейство – компонент – елемент.

За аналогією представлені вимоги якості. Подібна градація дозволяє описати будь-яку систему інформаційної безпеки і зіставити створену модель з поточним станом справ.

У стандарті виділені 11 класів функцій: – аудит; – ідентифікація та автентифікація; – криптографічний захист; – конфіденційність; – передача даних; – захист даних користувача; – управління безпекою; – захист функцій безпеки системи; – використання ресурсів; – доступ до системи; – надійність засобів.

Оцінка інформаційної безпеки базується на моделях системи безпеки, що складаються з перерахованих у стандарті функцій. У ISO 15408 міститься ряд зумовлених моделей (так званих профілів), що описують стандартні модулі системи безпеки. З їх допомогою можна не створювати моделі поширених засобів захисту самостійно, винаходячи велосипед, а користуватися вже готовими наборами описів, цілей, функцій і вимог до цих засобів. Простим прикладом профілів може служити модель міжмережевого екрану.

Сертифікований профіль являє собою повний опис певної частини (або функції) системи безпеки. У ньому міститься аналіз внутрішнього і зовнішнього середовища об’єкта, вимоги до його функціональності і надійності, логічне обгрунтування його використання, можливості та обмеження розвитку об’єкта.

Стандарт ISO 15408 вигідно відрізняє відкритість. Описує ту чи іншу область системи безпеки профіль можна створити самостійно за допомогою розробленої в ISO 15408 структури документа. У стандарті визначена також послідовність дій для самостійного створення профілів.

Загальні критерії (ЗК) визначені у стандарті ISO 15408 дозволяють підвищити довіру до засобів захисту і самої інформації, що захищається за рахунок трьох основних якостей:

1. Можливості гнучкого завдання вимог до засобів захисту інформації з урахуванням їх призначення і умов застосування.

2. Більш повного і обґрунтованого набору вимог безпеки.

3. Наявності методології оцінки, що забезпечує об’єктивність і порівнянність результатів.

Загальні критерії являють собою набір з п’яти окремих взаємопов’язаних частин. До них відносяться: – Введення і загальна модель. – Функціональні вимоги безпеки. – Вимоги до надійності захисних механізмів. – Попереднє визначення профілі захисту. – Процедури реєстрації профілів захисту.

*1.1.6. Нормативні документи з технічного захисту інформації НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу» НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»*

НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу»

1 Галузь використання

Цей документ установлює терміни і визначення понять у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. Терміни, що установлюються цим документом, обов’язкові для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації. Для кожного поняття встановлено один термін. Застосування синонімів терміна не допускається. Для довідки наведені іноземні еквіваленти термінів, що запроваджуються, а також алфавітні покажчики термінів.

2 Нормативні посилання

Під час розробки цього нормативного документа використані наступні стандарти: - ДСТУ 2226-93. Автоматизовані системи. Терміни і визначення. - ДСТУ 2941-94. Системи обробки інформації. Розробка систем. Терміни і визначення. - ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення.

3 Позначення і скорочення

В цьому НД ТЗІ використовуються наступні позначення і скорочення: АС — автоматизована система; КЗЗ — комплекс засобів захисту; КС — комп’ютерна система; КСЗІ— комплексна система захисту інформації; НСД — несанкціонований доступ; ОС — обчислювальна система; ПЗ — програмне забезпечення; ПРД — правила розмежування доступу; ТЗІ — технічний захист інформації.

4 Терміни і визначення

4.1 Основні поняття

4.1.1 Обчислювальна система; ОС (computer system) — сукупність програмних-апаратних засобів, призначених для обробки інформації.

4.1.2 Автоматизована система; АС (automated system) — організаційнотехнічна система, що реалізує інформаційну технологію і об’єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється.

4.1.3 Комп’ютерна система; КС (computer system, target of evaluation) — 6 НД ТЗІ 1.1-003-99 сукупність програмно-апаратних засобів, яка подана для оцінки.

4.1.4 Політика безпеки інформації (information security policy) — сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

4.1.5 Загроза (threat) — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

4.1.6 Безпека інформації (information security) — стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

4.1.7 Захист інформації в АС (information protection, information security, computer system security) — діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

4.1.8 Комплексна система захисту інформації; КСЗІ — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

4.1.9 Комплекс засобів захисту; КЗЗ (trusted computing base; TCB) — сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

4.1.10 Захищена комп’ютерна система; захищена КС (trusted computer system, trusted computer product) — комп’ютерна система, яка здатна забезпечувати захист оброблюваної інформації від певних загроз.

4.1.11 Об’єкт комп’ютерної системи; об’єкт КС (product object, system object) — елемент ресурсу КС, що знаходиться під керуванням КЗЗ і характеризується певними атрибутами і поводженням.

4.1.12 Пасивний об’єкт (passive object) — об’єкт КС, який в конкретному акті доступу виступає як пасивний компонент системи, над яким виконується дія і/або який служить джерелом чи приймальником інформації.

4.1.13 Об’єкт-процес (process object) — виконувана в даний момент програма, яка повністю характеризується своїм контекстом (поточним станом регістрів обчислювальної системи, адресним простором, повноваженнями і т.ін.).

4.1.14 Користувач (user) — фізична особа, яка може взаємодіяти з КС через наданий їй інтерфейс.

4.1.15 Об’єкт-користувач (user object) — подання фізичного користувача в КС, що створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями і т. ін.).

4.1.16 Ідентифікатор об’єкта КС (object identifier) — унікальний атрибут об’єкта КС, що дозволяє однозначно виділити даний об’єкт серед подібних.

4.1.17 Потік інформації (information flow) — передавання інформації від одного до іншого об’єкта КС.

4.1.18 Доступ до інформації (access to information ) — вид взаємодії двох об’єктів КС, внаслідок якого створюється потік інформації від одного об’єкта до 7 НД ТЗІ 1.1-003-99 іншого і/або відбувається зміна стану системи.

4.1.19 Правила розмежування доступу; ПРД (access mediation rules) — частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об’єктів.

4.1.20 Тип доступу (access type) — суттєвість доступу до об’єкта, що характеризує зміст здійснюваної взаємодії, а саме: проведені дії, напрям потоків інформації, зміни в стані системи (наприклад, читання, запис, запуск на виконання, видаляння, дозапис).

4.1.21 Запит на доступ (access request) — звернення одного об’єкта КС до іншого з метою отримання певного типу доступу.

4.1.22 Санкціонований доступ до інформації (authorized access to information) — доступ до інформації, що не порушує ПРД.

4.1.23 Несанкціонований доступ до інформації; НСД до інформації (unauthorized access to information) — доступ до інформації, здійснюваний з порушенням ПРД. 4.1.24 Захист від несанкціонованого доступу; захист від НСД (protection from unauthorized access) — запобігання або істотне утруднення несанкціонованого доступу до інформації.

4.1.25 Право доступу (access right) — дозвіл або заборона здійснення певного типу доступу.

4.1.26 Повноваження (privilege) — права користувача або процесу на виконання певних дій, зокрема на одержання певного типу доступу до об’єктів.

4.1.27 Керування доступом (access control) — сукупність заходів з визначення повноважень і прав доступу, контролю за додержанням ПРД.

4.1.28 Розмежування доступу (access mediation) — сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі ПРД можливості надання доступу.

4.1.29 Авторизація (authorization) — надання повноважень; встановлення відповідності між повідомленням (пасивним об’єктом) і його джерелом (створившим його користувачем або процесом).

4.1.30 Авторизований користувач (authorized user) — користувач, що володіє певними повноваженнями.

4.1.31 Роль користувача (user role) — сукупність функцій щодо керування КС, КЗЗ і обробки інформації, доступних користувачеві.

4.1.32 Адміністратор (administrator, administrative user) — користувач, роль якого включає функції керування КС і/або КЗЗ. 4.1.33 Адміністратор безпеки (security administrator) — адміністратор, відповідальний за дотримання політики безпеки.

4.1.34 Порушник (user violator) — користувач, який здійснює несанкціонований доступ до інформації.

НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»

1 Галузь використання

Цей нормативний документ (далі — Критерії) — установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

1. Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2. Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

Критерії можуть застосовуватися до всього спектра комп'ютерних систем, включаючи однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, мережі, об'єктно-орієнтовані системи та ін.

Цей документ призначено для постачальників (розробників), споживачів (замовників, користувачів) комп'ютерних систем, які використовуються для обробки (в тому числі збирання, зберігання, передачі і т. ін.) критичної інформації, а також для органів, що здійснюють функції оцінювання захищеності такої інформації та контролю за її обробкою.

Цей документ відображає сучасний стан проблеми і підходів до її розв'язання. З розвитком нових тенденцій в галузі і за умови достатньої обгрунтованості документ є відкритим для включення до його складу Адміністрацією Державної служби спеціального зв'язку та захисту інформації України нових послуг.

2 Нормативні посилання

У цьому НД ТЗІ наведено посилання на такі нормативні документи: ДСТУ 3230-95. Управління якістю і забезпечення якості. Терміни і визначення.

ДСТУ 2853-94. Програмні засоби ЭОМ. Підготовка і проведення випробувань.

ДСТУ 2851-94. Програмні засоби ЭОМ. Документування результатів випробувань.

НД ТЗІ 1.1-004-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

3 Визначення

В цьому нормативному документі використовуються терміни і визначення,що відповідають встановленим нормативним документом ТЗІ 1.1-003-99“Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу“.

4 Позначення і скорочення

В цьому нормативному документі використовуються такі позначення і скорочення:

Загальні терміни:

АС — автоматизована система; КС — комп'ютерна система; КЗЗ — комплекс засобів захисту; НСД — несанкціонований доступ; ОС — обчислювальна система; ПЗ — програмне забезпечення; ПЗП — постійний запам’ятовуючий пристрій; ПРД — правила розмежування доступу;

Позначення послуг:

КД — довірча конфіденційність; КА — адміністративна конфіденційність; КО — повторне використання об'єктів; КК — аналіз прихованих каналів; КВ — конфіденційність при обміні; ЦД — довірча цілісність; ЦА — адміністративна цілісність; ЦО — відкат; ЦВ — цілісність при обміні; ДР — використання ресурсів; ДВ — стійкість до відмов; ДЗ — гаряча заміна; ДВ — відновлення після збоїв; НР — реєстрація; НИ — ідентифікація і автентифікація; НК — достовірний канал; НО — розподіл обов'язків; НЦ — цілісність КЗЗ; НТ — самотестування; НВ — автентифікація при обміні; НА — автентифікація відправника;

***1.2. Міжнародні стандарти в галузі інформаційної та /або кібербезпеки.***

*1.2.1. Регламенти ЄС в галузі кібербезпеки*

*Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»*

Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року "Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій" є важливим регуляторним актом Європейського Союзу, спрямованим на зміцнення кібербезпеки та забезпечення відповідного рівня захисту інформаційних технологій.

Основні положення регламенту включають:

Створення Агентства Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) з метою забезпечення високого рівня мережевої та інформаційної безпеки в Європейському Союзі.

Удосконалення координації та співпраці між державами-членами ЄС у сфері кібербезпеки.

Визначення процедур і вимог для сертифікації кібербезпеки інформаційно-комунікаційних технологій (ІКТ) в Європейському Союзі.

Забезпечення створення єдиного ринку для безпечних ІКТ-продуктів і послуг у Європейському Союзі.

Регламент спрямований на підвищення рівня кібербезпеки в ЄС шляхом створення більш ефективних механізмів координації, стандартизації та сертифікації в цій області.

*1.2.2. ISO 27001, ISO 27002, ISO 27003*

*ISO/IEC 15408- 2, ISO/IEC 15408-3*

ISO 27001

Стандарт ISO 27001

Стандарт ISO 27001 містить опис створення системи управління інформаційною безпекою організації. Реалізація багатьох положень цього стандарту залежить від специфіки організації. Сучасний бізнес має нагальну потребу ідентифікувати ризики та керувати ними. Технічні можливості постійно змінюються, технічні засоби ускладнюються, вимоги неухильно зростають. Стандарт ISO 27001 регламентує впорядкований підхід до вирішення проблем безпеки.

Стандарт ISO 27001 дає опис загальної моделі впровадження та функціонування системи управління інформаційною безпекою, а також заходів щодо її моніторингу та покращення.

Для цілей сертифікації на відповідність стандарту ISO 27001 поняття інформаційна безпека визначається як система заходів, що забезпечують захист інформації та інформаційних технологій, забезпечують конфіденційність, цілісність та доступність.

Стандарт ISO 27001 гармонізований з іншими стандартами систем управління, такими як стандарти серії ISO 9000 та серії ISO 14000, що дозволяє забезпечити узгоджене та цілісне впровадження та функціонування корпоративної системи управління.

ISO 27002

**ISO / IEC 27002**[[1]](https://uk.wikipedia.org/wiki/ISO/IEC_27002#cite_note-1) — стандарт [інформаційної безпеки](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0), опублікований організаціями [ISO](https://uk.wikipedia.org/wiki/%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B0_%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F_%D0%B7%D1%96_%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%97) і [IEC](https://uk.wikipedia.org/wiki/%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B0_%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D1%82%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D0%B0_%D0%BA%D0%BE%D0%BC%D1%96%D1%81%D1%96%D1%8F). Він має назву *Інформаційні технології* — *Технології безпеки* — *Практичні правила* [менеджменту інформаційної безпеки](https://uk.wikipedia.org/w/index.php?title=%D0%9C%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%BC%D0%B5%D0%BD%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8&action=edit&redlink=1) ([англ](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0). *Information technology — Security techniques — Code of practice for information security management*). До 2007 року цей стандарт називався [ISO / IEC 17799](https://uk.wikipedia.org/w/index.php?title=ISO_/_IEC_17799&action=edit&redlink=1). Стандарт розроблений в 2005 році на основі версії [ISO 17799](https://uk.wikipedia.org/w/index.php?title=ISO_17799&action=edit&redlink=1), опублікованій у [2000](https://uk.wikipedia.org/wiki/2000), яка була повною копією Британського стандарту [BS 7799-1: +1999](https://uk.wikipedia.org/w/index.php?title=BS_7799-1:_%2B1999&action=edit&redlink=1).

Стандарт надає кращі практичні поради з менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування систем менеджменту інформаційної безпеки. *Інформаційна безпека* визначається стандартом як «збереження конфіденційності (впевненості в тому, що інформація доступна тільки тим, хто уповноважений мати такий доступ), цілісності (гарантії точності і повноти інформації, а також методів її обробки) і доступності (гарантії того, що уповноважені користувачі мають доступ до інформації та пов'язаним з нею ресурсів)».

Поточна версія стандарту складається з наступних основних розділів:

* [Політика безпеки](https://uk.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%96%D1%82%D0%B8%D0%BA%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96) (*Security policy*)
* [Організація інформаційної безпеки](https://uk.wikipedia.org/w/index.php?title=%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%97_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8&action=edit&redlink=1) (*Organization of information security*)
* Управління ресурсами (*Asset management*)
* Безпека персоналу (*Human resources security*)
* Фізична безпека і безпека оточення (*Physical and environmental security*)
* Управління комунікаціями та операціями (*Communications and operations management*)
* Управління доступом (*Access control*)
* Придбання, розробка та підтримка систем (*Information systems acquisition, development and maintenance*)
* Управління інцидентами інформаційної безпеки (*Information security incident management*)
* Управління безперебійною роботою організації (*Business continuity management*)
* Відповідність нормативним вимогам (*Compliance*)

ISO 27003

**ISO / IEC 27003**[[1]](https://uk.wikipedia.org/wiki/ISO/IEC_27003#cite_note-1) — стандарт [інформаційної безпеки](https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0), опублікований організаціями [ISO](https://uk.wikipedia.org/wiki/%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B0_%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F_%D0%B7%D1%96_%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D1%96%D1%97) і [IEC](https://uk.wikipedia.org/wiki/%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B0_%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D1%82%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D0%B0_%D0%BA%D0%BE%D0%BC%D1%96%D1%81%D1%96%D1%8F). Він має назву *Інформаційні технології* — *Технології безпеки* — *Системи управління інформаційною безпекою. Керівництво* ([англ](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0). *Information technology -- Security techniques -- Information security management systems -- Guidance*).

Цей документ був підготовлений ISO/IEC JTC 1, підкомітет SC 27. Це друге видання ISO/IEC 27003 скасовує та замінює перше видання (ISO/IEC 27003:2010. Попереднє видання мало проектний підхід із послідовним впровадженням. Замість цього в новому виданні наводяться вказівки щодо вимог, незалежно від порядку, в якому вони виконуються. Структура стандарту тепер узгоджена зі структурою ISO/IEC 27001:2013.

ISO/IEC 27003 містить керівні вказівки щодо вимог до [системи управління інформаційною безпекою](https://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE%D1%8E_%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%BE%D1%8E) (СУІБ), як зазначено у стандарті ISO/IEC 27001, і надає рекомендації, можливості та дозволи щодо них. Цей документ не передбачає надання загальних рекомендацій з усіх аспектів інформаційної безпеки. Статті 4-10 цього документа відображають структуру ISO/IEC 27001:2013. Стандарт ISO/IEC 27003 не додає нових вимог до СУІБ та пов'язаних з ними термінів та визначень. Організації, що впроваджують СУІБ, не зобов'язані дотримуватися вказівок у цьому документі. СУІБ підкреслює важливість наступних етапів:

* розуміння потреб організації та необхідності встановлення політики інформаційної безпеки та цілей інформаційної безпеки;
* оцінка ризиків організації, пов'язаних з інформаційною безпекою;
* впровадження та керування процесами інформаційної безпеки, контролю та іншими заходами щодо ліквідації ризиків;
* моніторинг та перевірка продуктивності та ефективності СУІБ;
* впровадження постійного вдосконалення СУІБ.

ISO/IEC 15408- 2

ISO/IEC 15408 є міжнародним стандартом, також відомим як "Common Criteria for Information Technology Security Evaluation" (CC), що визначає процес оцінки безпеки інформаційних технологій. Цей стандарт розробляється спільно Міжнародною організацією зі стандартизації (ISO) та Міжнародним електротехнічним комітетом (IEC).

ISO/IEC 15408 складається з кількох частин. Одна з головних частин - ISO/IEC 15408-2, яка визначає процедури оцінки безпеки та встановлює вимоги до організацій, які проводять оцінку, і до виробників, які подають продукти на оцінку. Основні аспекти ISO/IEC 15408-2 включають:

Процес оцінки безпеки: Стандарт встановлює кроки, які потрібно виконати під час оцінки безпеки, включаючи визначення потреб замовника, вибір критеріїв оцінки, виконання самої оцінки, підготовку звіту тощо.

Компоненти оцінки: Стандарт визначає різні компоненти оцінки, такі як Замовник, Виробник, Завідувач, Оцінювач, Виробнича лабораторія тощо, і встановлює їхні обов'язки та відповідальність у процесі оцінки.

Вимоги до продуктів та сертифікатів: Стандарт встановлює вимоги до продуктів, які підлягають оцінці безпеки, та до сертифікатів, які видаються після успішної оцінки.

Методи оцінки: Стандарт також визначає методи, які можуть бути використані під час оцінки безпеки, включаючи аналіз документації, виконання тестів, аудит безпеки тощо.

ISO/IEC 15408-2 є важливим інструментом для забезпечення безпеки інформаційних технологій та допомагає стандартизувати процес оцінки безпеки на міжнародному рівні.

ISO/IEC 15408 - 3

ISO/IEC 15408-3 - це одна з частин міжнародного стандарту "Common Criteria for Information Technology Security Evaluation" (CC), який регулює процес оцінки безпеки інформаційних технологій. Ця частина стандарту визначає вимоги до безпеки та організаційних заходів безпеки, які повинні бути взяті до уваги під час розробки систем безпеки для інформаційних технологій.

Основні аспекти ISO/IEC 15408-3 включають:

Визначення безпеки системи: Стандарт встановлює процес визначення потреб замовника щодо безпеки системи та встановлює основні цілі безпеки для цієї системи.

Аналіз загроз і вразливостей: Вимагається проведення аналізу загроз і вразливостей для визначення потенційних загроз і шляхів їх нейтралізації.

Вимоги до захисту і заходи безпеки: Стандарт встановлює вимоги до захисту і описує заходи безпеки, які повинні бути реалізовані для досягнення поставлених цілей безпеки.

Організаційні заходи безпеки: Вимагається виконання організаційних заходів безпеки, таких як політики безпеки, навчання персоналу, управління ризиками та інші, для забезпечення ефективності заходів технічного захисту.

Управління життєвим циклом безпеки: Стандарт вимагає впровадження процесу управління життєвим циклом безпеки, що включає планування, розробку, впровадження, експлуатацію та вилучення заходів безпеки.

Вимоги до документування: Вимагається створення та підтримання відповідної документації, яка описує безпеку системи, заходи безпеки та здійснені організаційні заходи.

ISO/IEC 15408-3 є важливим інструментом для розробників інформаційних технологій та організацій, що стежать за безпекою, для забезпечення високого рівня безпеки в їхніх продуктах та системах.