# ТЕМА 2. ЗАКОНОДАВЧІ ТА НОРМАТИВНО-ПРАВОВА БАЗА УКРАЇНИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА/АБО КІБЕРБЕЗПЕКИ

**Закон України «Про освіту». Стаття 42. Академічна доброчесність.**

**1.1. Закон України «Про інформацію».**

**1.2. Закон України «Про науково-технічну інформацію».**

**1.3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».**

**1.4. Закон України «Про основні засади забезпечення кібербезпеки України».**

**1.5. Закон України «Про державну таємницю».**

**1.6. Закон України «Про захист персональних даних».**

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

**1.8. ДСТУ 3396.0,1,2-97**

**1.9. ДСТУ ISO/IEC 15408-1:2017**

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

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

**1.12. Закон України «Про доступ до публічної інформації».**

**1.13. Загрози, яким підлягає інформація.**

**1.14. Стратегії реалізації загроз.**

**1.15. Основні міри протидії загрозам безпеці, принципи побудови систем захисту, основні механізми захисту.**

**1.16. Перелік основних задач, які повинні вирішуватися системою комп'ютерної безпеки.**

**1.17. Основні принципи побудови систем захисту інформаційно-комунікаційних систем (ІКС).**

**Закон України «Про освіту»**

**Стаття 42. Академічна доброчесність**

1. **Академічна доброчесність** – це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

2. **Дотримання академічної доброчесності педагогічними, науково-педагогічними та науковими працівниками передбачає:**

– посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

– дотримання норм законодавства про авторське право і суміжні права;

– надання достовірної інформації про методики і результати досліджень, джерела використаної інформації та власну педагогічну (науково-педагогічну, творчу) діяльність;

– контроль за дотриманням академічної доброчесності здобувачами освіти;

– об’єктивне оцінювання результатів навчання.

3. **Дотримання академічної доброчесності здобувачами освіти передбачає**:

– самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);

– посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

– дотримання норм законодавства про авторське право і суміжні права;

– надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

4. **Порушенням академічної доброчесності вважається**:

– **академічний плагіат –** оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

– **самоплагіат** – оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

– **фабрикація –** вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

– **фальсифікація –** свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

– **списування –** виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання;

– **обман –** надання завідомо неправдивої інформації щодо власної освітньої (наукової, творчої) діяльності чи організації освітнього процесу; формами обману є, зокрема, академічний плагіат, самоплагіат, фабрикація, фальсифікація та списування;

– **хабарництво –** надання (отримання) учасником освітнього процесу чи пропозиція щодо надання (отримання) коштів, майна, послуг, пільг чи будь-яких інших благ матеріального або нематеріального характеру з метою отримання неправомірної переваги в освітньому процесі;

– **необ’єктивне оцінювання –** свідоме завищення або заниження оцінки результатів навчання здобувачів освіти;

– надання здобувачам освіти під час проходження ними оцінювання результатів навчання допомоги чи створення перешкод, не передбачених умовами та/або процедурами проходження такого оцінювання;

– вплив у будь-якій формі (прохання, умовляння, вказівка, погроза, примушування тощо) на педагогічного (науково-педагогічного) працівника з метою здійснення ним необ'єктивного оцінювання результатів навчання.

5. **За порушення академічної доброчесності педагогічні, науково-педагогічні та наукові працівники закладів освіти можуть бути притягнені до такої академічної відповідальності:**

– відмова у присудженні ступеня освітньо-наукового чи освітньо-творчого рівня чи присвоєнні вченого звання;

– позбавлення присудженого ступеня освітньо-наукового чи освітньо-творчого рівня чи присвоєного вченого звання;

– відмова в присвоєнні або позбавлення присвоєного педагогічного звання, кваліфікаційної категорії;

– позбавлення права брати участь у роботі визначених законом органів чи займати визначені законом посади.

6. **За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності**:

– повторне проходження оцінювання (контрольна робота, іспит, залік тощо);

– повторне проходження відповідного освітнього компонента освітньої програми;

– відрахування із закладу освіти (крім осіб, які здобувають загальну середню освіту);

– позбавлення академічної стипендії;

– позбавлення наданих закладом освіти пільг з оплати навчання.

7. **Види академічної відповідальності** (у тому числі додаткові та/або деталізовані) учасників освітнього процесу за конкретні порушення академічної доброчесності визначаються спеціальними законами та/або внутрішніми положеннями закладу освіти, що мають бути затверджені (погоджені) основним колегіальним органом управління закладу освіти та погоджені з відповідними органами самоврядування здобувачів освіти в частині їхньої відповідальності.

8. **Порядок виявлення та встановлення фактів порушення академічної доброчесності** визначається уповноваженим колегіальним органом управління закладу освіти з урахуванням вимог цього Закону та спеціальних законів.

Кожна особа, стосовно якої порушено питання про порушення нею академічної доброчесності, має такі права:

– ознайомлюватися з усіма матеріалами перевірки щодо встановлення факту порушення академічної доброчесності, подавати до них зауваження;

– особисто або через представника надавати усні та письмові пояснення або відмовитися від надання будь-яких пояснень, брати участь у дослідженні доказів порушення академічної доброчесності;

– знати про дату, час і місце та бути присутньою під час розгляду питання про встановлення факту порушення академічної доброчесності та притягнення її до академічної відповідальності;

– оскаржити рішення про притягнення до академічної відповідальності до органу, уповноваженого розглядати апеляції, або до суду.

9. **Форми та види академічної відповідальності закладів освіти** визначаються спеціальними законами.

10. **За дії (бездіяльність), що цим Законом визнані порушенням академічної доброчесності, особа може бути притягнута до інших видів відповідальності з підстав та в порядку, визначених законом**.

**Інформаційна безпека** (англ. *Information Security*, а також – англ. *InfoSec*) – Практика запобігання несанкціонованого доступу, використання, розкриття, спотворення, зміни, дослідження, запису або знищення інформації. Це універсальне поняття застосовується незалежно від форми, яку можуть набувати дані (електронна або, наприклад, фізична). Основне завдання інформаційної безпеки – збалансований захист конфіденційності, цілісності та доступності даних, з урахуванням доцільності застосування і без будь-яких збитківпродуктивності організації. Це досягається, в основному, за допомогою багатоетапного процесу управління ризиками, який дозволяє ідентифікувати основні засоби та нематеріальні активи, джерела загроз, уразливості, потенційний ступінь впливу та можливості управління ризиками. Цей процес супроводжується оцінкою ефективності плану управління ризиками.

**Комп'ютерна безпека** – розділ інформаційної безпеки, що характеризує неможливість виникнення шкоди комп'ютера, що перевищує величину прийнятної шкоди для нього від усіх виявлених та вивчених джерел його відмов у певних умовах роботи та на заданому інтервалі часу. Комп'ютерна безпека – заходи безпеки для захисту обчислювальних пристроїв (комп'ютери, смартфони та інші), а також комп'ютерних мереж (приватних та публічних мереж, включаючи Інтернет). Поле діяльності системних адміністраторів охоплює всі процеси та механізми, за допомогою яких цифрове обладнання, інформаційне поле та послуги захищаються від випадкового чи несанкціонованого доступу, зміни або знищення даних, і набуває все більшого значення у зв'язку з зростаючою залежністю від комп'ютерних систем у розвиненій спільноті.

**Кібербезпека** – розділ інформаційної безпеки, в рамках якого вивчають процеси формування, функціонування та еволюції кібероб'єктів, для виявлення джерел кібернебезпеки, що утворюються при цьому, визначення їх характеристик, а також їх класифікацію та формування нормативних документів, виконання яких має гарантувати захист кібероб'єктів від усіх виявлених і вивчених джерел кібернебезпеки. Кібербезпека – процес використання заходів безпеки для забезпечення конфіденційності, цілісності та доступності даних. Системний адміністратор забезпечує захист активів, включаючи дані локальної мережі комп'ютерів та серверів. Крім того, під охорону беруться безпосередньо будівлі та, найголовніше, персонал. Метою забезпечення кібербезпеки є захист даних (як у процесі передачі та/або обміну так і тих, що знаходяться на зберіганні). З метою безпеки даних можуть бути застосовані і контрзаходи. Деякі

з цих заходів включають (але не обмежуються) контроль доступу, навчання персоналу, аудит та звітність, оцінку ймовірних ризиків, тестування на проникнення та вимогу авторизації.

## 1.1. Закон України «Про інформацію»

Цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, та складається з наступних розділів і статей.

**Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ**

**Стаття 1.** Визначення термінів

**Стаття 2.** Основні принципи інформаційних відносин

**Стаття 3.** Державна інформаційна політика

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

**Стаття 5.** Право на інформацію

**Стаття 6.** Гарантії права на інформацію

**Стаття 7.** Охорона права на інформацію

**Стаття 8.** Мова інформації

**Стаття 9.** Основні види інформаційної діяльності

**Розділ II. ВИДИ ІНФОРМАЦІЇ**

**Стаття 10.** Види інформації за змістом

**Стаття 11.** Інформація про фізичну особу

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

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

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

**Стаття 15.** Науково-технічна інформація

**Стаття 16.** Податкова інформація

**Стаття 17.** Правова інформація

**Стаття 18.** Статистична інформація

**Стаття 19.** Соціологічна інформація

**Стаття 19.** Критична технологічна інформація

**Стаття 20.** Доступ до інформації

**Стаття 21.** Інформація з обмеженим доступом

**Розділ III. ДІЯЛЬНІСТЬ ЖУРНАЛІСТІВ, ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ, ЇХ ПРАЦІВНИКІВ**

**Стаття 22.** Масова інформація та її засоби

**Стаття 23.** Інформаційна продукція та інформаційна послуга

**Стаття 24.** Заборона цензури та заборона втручання в професійну діяльність журналістів і засобів масової інформації

**Стаття 25.** Гарантії діяльності засобів масової інформації та журналістів

**Стаття 26.** Акредитація журналістів, працівників засобів масової інформації

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

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

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

**Стаття 29.** Поширення суспільно необхідної інформації

**Стаття 30.** Звільнення від відповідальності

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

**Розділ I. 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 засоби масової інформації 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 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;
– 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.

**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.

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

**Стаття 19.** 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.

**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, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

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

**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.

## 1.2. Закон України «Про науково-технічну інформацію»

Цей Закон визначає основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни та складається з наступних розділів і статей.

**Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ**

**Стаття 1.** Визначення термінів

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

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

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

Метою Закону є створення в Україні правової бази для одержання та використання науково-технічної інформації.

Законом регулюються правові і економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного співробітництва в цій галузі.

Дія Закону поширюється на підприємства, установи, організації незалежно від форм власності, а також громадян, які мають право на одержання, використання та поширення науково-технічної інформації. Дія Закону не поширюється на інформацію, що містить державну та іншу охоронювану законом таємницю.

**Розділ І. 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;

**– 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 фон**д – 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.

**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.

## 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 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.

## 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.

**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.

## 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.

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.

## 1.3. Закон України «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) та складається з наступних статей.

**Стаття 1.** Визначення термінів
**Стаття 2.** Об'єкти захисту в системі
**Стаття 3.** Суб'єкти відносин
**Стаття 4.** Доступ до інформації в системі
**Стаття 5.** Відносини між володільцем інформації та власником системи
**Стаття 6.** Відносини між власником системи та користувачем
**Стаття 7.** Відносини між власниками систем
**Стаття 8.** Умови обробки інформації в системі
**Стаття 9.** Забезпечення захисту інформації в системі
**Стаття 10.** Повноваження державних органів у сфері захисту інформації в системах
**Стаття 11.** Відповідальність за порушення законодавства про захист інформації в системах
**Стаття 12.** Міжнародні договори

**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;

**– 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;

**– 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, визначається Кабінетом Міністрів України.

**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;

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.

**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, встановленому Кабінетом Міністрів України.

**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.

**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.

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.

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

Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

**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.

## 1.4. Закон України «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, та складається з наступних статей.

**Стаття 1.** Визначення термінів

**Стаття 2.** Принципи застосування Закону

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

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

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

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

**Стаття 7.** Принципи забезпечення кібербезпеки

**Стаття 8.** Національна система кібербезпеки

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

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

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

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

**Стаття 13.** Фінансове забезпечення заходів кібербезпеки

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

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

**Стаття 1.** Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

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

– **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;

– **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;

– **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;

– **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;

– **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;

– **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;

– **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;

– **кіберзлочинність** – сукупність кіберзлочинів;

– **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;

– **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;

– **кіберрозвідка** – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

– **кібертероризм** – терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

– **кібершпигунство** – шпигунство, що здійснюється у кіберпросторі або з його використанням;

– **критична інформаційна інфраструктура** – сукупність об'єктів критичної інформаційної інфраструктури;

– **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;

– **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;

– **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;

– **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;

– **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;

– **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;

– **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;

– **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.

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

1. **Об'єктами кібербезпеки** є:

– конституційні права і свободи людини і громадянина;

– суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

– держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

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

– об'єкти критичної інфраструктури.

2. **Об’єктами кіберзахисту** є:

– 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;

– об’єкти критичної інформаційної інфраструктури;

– 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 критичної інформаційної інфраструктури, перелік таких об’єктів та порядок їх внесення до державного реєстру об’єктів критичної інформаційної інфраструктури, а також порядок 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 покладаються на Національний банк України.

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

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

– міністерства та інші центральні органи виконавчої влади;

– місцеві державні адміністрації;

– органи місцевого самоврядування;

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

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

– Національний банк України;

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

– 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:

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

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

– здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

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

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

– 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 "Про критичну інфраструктуру".

2. Критерії та порядок віднесення об’єктів до об’єктів критичної інфраструктури, перелік таких об’єктів, загальні вимоги до їх кіберзахисту, 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.

**Стаття 7.** Принципи забезпечення кібербезпеки

1. **Забезпечення кібербезпеки в Україні ґрунтується на принципах**:

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

– забезпечення національних інтересів України;

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

– 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;

– 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;

– пріоритетності запобіжних заходів;

– невідворотності покарання за вчинення кіберзлочинів;

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

– 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;

– 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.**

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

1. **Завданнями CERT-UA** є:

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

– надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

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

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

– 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;

– 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;

– опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

– 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 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.

## 1.5. Закон України «Про державну таємницю»

Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України, та складається з наступних розділів і статей.

**Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ**

**Стаття 1.** Визначення термінів

**Стаття 2.** Законодавство України про державну таємницю

**Стаття 3.** Сфера дії Закону

**Стаття 4.** Державна політика щодо державної таємниці

**Стаття 5.** Компетенція державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

**Стаття 6.** Реалізація прав на секретну інформацію та її матеріальні носії

**Стаття 7.** Фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею

**Розділ II. ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ**

**Стаття 8.** Інформація, що може бути віднесена до державної таємниці

**Стаття 9.** Державні експерти з питань таємниць

**Стаття 10.** Порядок віднесення інформації до державної таємниці

**Стаття 11.** Рішення державного експерта з питань таємниць

**Стаття 12.** Звід відомостей, що становлять державну таємницю

**Стаття 13.** Строк дії рішення про віднесення інформації до державної таємниці

**Стаття 14.** Зміна ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці

**Розділ III. ЗАСЕКРЕЧУВАННЯ ТА РОЗСЕКРЕЧУВАННЯ МАТЕРІАЛЬНИХ НОСІЇВ ІНФОРМАЦІЇ**

**Стаття 15.** Засекречування та розсекречування матеріальних носіїв інформації

**Стаття 16.** Строк засекречування матеріальних носіїв інформації

## Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

**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, 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**, – 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.

**Стаття 5.** Компетенція державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

Президент України, забезпечуючи національну безпеку, видає укази та розпорядження з питань охорони державної таємниці, віднесених цим Законом та іншими законами до його повноважень.

Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері охорони державної таємниці.

Кабінет Міністрів України спрямовує та координує роботу міністерств, інших органів виконавчої влади щодо забезпечення здійснення державної політики у сфері охорони державної таємниці.

Центральні та місцеві органи виконавчої влади, Рада міністрів Автономної Республіки Крим та органи місцевого самоврядування здійснюють державну політику у сфері охорони державної таємниці в межах своїх повноважень, передбачених законом.

Спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці є Служба безпеки України.

Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій.

**Стаття 6.** Реалізація прав на секретну інформацію та її матеріальні носії

Володілець секретної інформації або власник матеріальних носіїв такої інформації реалізує свої права з урахуванням обмежень, установлених в інтересах національної безпеки України відповідно до цього Закону.

**Розділ ІІ. ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ**

**Стаття 8.** Інформація, що може бути віднесена до державної таємниці

**До державної таємниці у порядку, встановленому цим Законом, відноситься інформація**:

1) **у сфері оборони**:

– про зміст стратегічних і оперативних планів та інших документів бойового управління, підготовку та проведення військових операцій, стратегічне та мобілізаційне розгортання військ, а також про інші найважливіші показники, які характеризують організацію, чисельність, дислокацію, бойову і мобілізаційну готовність, бойову та іншу військову підготовку, озброєння та матеріально-технічне забезпечення Збройних Сил України та інших військових формувань;

– про дислокацію, характеристики пунктів управління, зміст заходів загальнодержавного та регіонального, у разі необхідності міського і районного рівня, щодо приведення у готовність єдиної державної системи цивільного захисту населення і територій до виконання завдань в особливий період та про організацію системи зв'язку (оповіщення) в особливий період, можливості населених пунктів, регіонів і окремих об'єктів щодо евакуації, розосередження населення і забезпечення його життєдіяльності; забезпечення виробничої діяльності об'єктів національної економіки у воєнний час;

– про геодезичні, гравіметричні, картографічні та гідрометеорологічні дані і характеристики, які мають значення для оборони країни;

– про застосування систем озброєння, підготовку та проведення військових операцій;

– про винаходи, дослідження і розробку нових зразків озброєння в інтересах забезпечення національної безпеки і оборони та про результати таких досліджень і розробок;

– про заходи та показники розвитку Збройних Сил України та їх спроможностей;

– про склад, завдання та матеріально-технічне забезпечення розвідувального органу Міністерства оборони України та зібрану і створену ним інформацію в результаті його діяльності;

– про особовий склад Сил спеціальних операцій Збройних Сил України, а також осіб, які співпрацюють або раніше співпрацювали на конфіденційній

основі із Силами спеціальних операцій Збройних Сил України, фінансування та матеріально-технічне забезпечення руху опору, засоби, зміст, плани, організацію, завдання, форми, методи і результати ведення руху опору, оперативний резерв та мережу осередків руху опору;

2) **у сфері економіки, науки і техніки**:

– про зміст мобілізаційних планів державних органів та органів місцевого самоврядування, мобілізаційні потужності, заходи мобілізаційної підготовки і мобілізації та обсяги їх фінансування, запаси та обсяги постачання стратегічних видів сировини і матеріалів, а також зведені відомості про номенклатуру та рівні накопичення, загальні обсяги поставок, відпуску, закладення, освіження, розміщення і фактичні запаси державного матеріального резерву;

– про використання транспорту, зв'язку, потужностей інших галузей та об'єктів інфраструктури держави в інтересах забезпечення її безпеки;

– про плани, обсяги та інші найважливіші характеристики добування, виробництва та реалізації окремих стратегічних видів сировини і продукції;

– про державні запаси дорогоцінних металів монетарної групи, коштовного каміння, валюти та інших цінностей, операції, пов'язані з виготовленням грошових знаків і цінних паперів, їх зберіганням, охороною і захистом від підроблення, обігом, обміном або вилученням з обігу, а також про інші особливі заходи фінансової діяльності держави;

– про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, предметом яких є створення новітніх складних зразків озброєння, військової або спеціальної техніки та інші роботи, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України;

– про найменування, загальну кількість, вартість озброєння, військової техніки, боєприпасів, запасних частин та матеріалів до них, що закуповуються для потреб військових формувань (правоохоронних органів);

– про кількість, строки поставок військовим формуванням чи правоохоронним органам, спеціальним формуванням Міністерства внутрішніх справ України для забезпечення їх боєздатності основних видів пального (мастильних матеріалів), речового майна та продовольства;

– про факт та предмет закупівлі товарів, робіт і послуг оборонного призначення для забезпечення Збройних Сил України та інших військових формувань та правоохоронних органів (крім випадків, якщо окрема інформація про закупівлю таких товарів, робіт і послуг оборонного призначення, що закуповуються відповідно до Закону України "Про оборонні закупівлі", становить державну таємницю. У такому разі окрема інформація розміщується у додатку до тендерної документації).

– Інформація не може бути повторно віднесена до державної таємниці після розсекречення та оприлюднення;

3) **у сфері зовнішніх відносин**:

– про директиви, плани, вказівки делегаціям і посадовим особам з питань зовнішньополітичної і зовнішньоекономічної діяльності України, спрямовані на забезпечення її національних інтересів і безпеки;

– про військове, науково-технічне та інше співробітництво України з іноземними державами, якщо розголошення відомостей про це завдаватиме шкоди національній безпеці України;

– про експорт та імпорт озброєння, військової і спеціальної техніки, окремих стратегічних видів сировини і продукції;

– про зміст секретної інформації, що отримується від іноземної держави чи міжнародної організації;

4) **у сфері державної безпеки та охорони правопорядку**:

– про особовий склад органів, що здійснюють оперативно-розшукову діяльність або розвідувальну чи контррозвідувальну;

– про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової, розвідувальної і контррозвідувальної діяльності; про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність; про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють оперативно-розшукову, розвідувальну і контррозвідувальну діяльність;

– про організацію та порядок здійснення охорони адміністративних будинків та інших державних об'єктів, посадових та інших осіб, охорона яких здійснюється відповідно до Закону України "Про державну охорону органів державної влади України та посадових осіб";

– про систему урядового та спеціального зв'язку;

– про організацію, зміст, стан і плани розвитку криптографічного захисту секретної інформації, зміст і результати наукових досліджень у сфері криптографії;

– про системи та засоби криптографічного захисту секретної інформації, їх розроблення, виробництво, технологію виготовлення та використання;

– про державні шифри, їх розроблення, виробництво, технологію виготовлення та використання;

– про організацію режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, державні програми, плани та інші заходи у сфері охорони державної таємниці;

– про організацію, зміст, стан і плани розвитку технічного захисту секретної інформації;

– про результати перевірок, здійснюваних згідно з законом прокурором у порядку відповідного нагляду за додержанням законів, та про зміст матеріалів оперативно-розшукової діяльності, досудового розслідування та судочинства з питань, зазначених у цій статті сфер;

– про інші засоби, форми і методи охорони державної таємниці.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності "особливої важливості", "цілком таємно" та "таємно" лише за умови, що вони належать до категорій, зазначених у частині першій цієї статті, і їх розголошення завдаватиме шкоди інтересам національної безпеки України та з дотриманням вимог статті 6 Закону України "Про доступ до публічної інформації".

Забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

**Не відноситься до державної таємниці інформація**:

– про стан довкілля, про якість харчових продуктів і предметів побуту, про вплив товару (роботи, послуги) на життя та здоров’я людини;

– про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

– 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;

– про факти порушень прав і свобод людини і громадянина;

– про незаконні дії державних органів, органів місцевого самоврядування та їх посадових і службових осіб;

– інша інформація, доступ до якої відповідно до законів та міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України, не може бути обмежено.

**Стаття 9.** Державні експерти з питань таємниць

Державний експерт з питань таємниць здійснює відповідно до вимог цього Закону віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування.

**Стаття 10.** Порядок віднесення інформації до державної таємниці

Віднесення інформації до державної таємниці здійснюється мотивованим рішенням державного експерта з питань таємниць за його власною ініціативою, за зверненням керівників відповідних державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян.

Державний експерт з питань таємниць відносить інформацію до державної таємниці з питань, прийняття рішень з яких належить до його компетенції згідно з посадою. У разі, якщо прийняття рішення про віднесення інформації до державної таємниці належить до компетенції кількох державних експертів з питань таємниць, воно за ініціативою державних експертів або за пропозицією Служби безпеки України приймається колегіально та ухвалюється простою більшістю голосів. При цьому кожен експерт має право викласти свою думку.

Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи зміни до нього у порядку, встановленому цим Законом.

**Інформація відноситься до державної таємниці з урахуванням таких принципів**:

– дотримання балансу інтересів національної безпеки, демократичних принципів відкритості та прозорості;

– вільного обігу інформації;

– презумпції публічності інформації до її віднесення в установленому законодавством порядку до державної таємниці.

У разі невідповідності інформації вимогам, встановленим цим Законом, забороняється віднесення її до державної таємниці. Засекречуванню підлягає інформація, а не документ. Якщо документ містить державну таємницю, для ознайомлення надається інформація, доступ до якої не обмежений.

**Стаття 11.** Рішення державного експерта з питань таємниць

У рішенні державного експерта з питань таємниць про віднесення інформації до державної таємниці зазначаються:

– інформація, яка має становити державну таємницю, та її відповідність категоріям і вимогам, передбаченим статтею 8 цього Закону та статтею 6 Закону України "Про доступ до публічної інформації";

– підстави для віднесення інформації до державної таємниці;

– критерії віднесення інформації до державної таємниці, зокрема:

– визначення рівня та опис загрози та шкоди національній безпеці (національним інтересам) у разі невіднесення інформації до державної таємниці;

– визначення дати або події розсекречування інформації;

– ступінь секретності зазначеної інформації;

– обсяг фінансування заходів, необхідних для охорони такої інформації;

– державний орган, орган місцевого самоврядування, підприємство, установа, організація чи громадянин, який вніс пропозицію про віднесення цієї інформації до державної таємниці, та державний орган (органи), якому надається право визначати коло суб'єктів, які матимуть доступ до цієї інформації;

– строк, протягом якого діє рішення про віднесення інформації до державної таємниці.

**Стаття 12.** Звід відомостей, що становлять державну таємницю

Звід відомостей, що становлять державну таємницю, формує Служба безпеки України на підставі рішень державних експертів з питань таємниць. Зазначений Звід та зміни до нього набирають чинності з моменту опублікування в офіційних виданнях України.

Зміни до Зводу відомостей, що становлять державну таємницю, вносяться не пізніше трьох місяців з дня одержання Службою безпеки України відповідного рішення державного експерта з питань таємниць.

**Стаття 13.** Строк дії рішення про віднесення інформації до державної таємниці

Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, та інших обставин. **Він не може перевищувати для інформації із ступенем секретності "особливої важливості" – 30 років, для інформації "цілком таємно" – 10 років, для інформації "таємно" – 5 років.**

Після закінчення передбаченого частиною першою цієї статті строку дії рішення про віднесення інформації до державної таємниці державний експерт з питань таємниць приймає рішення про скасування рішення про віднесення її до державної таємниці або приймає рішення про продовження строку дії

зазначеного рішення в межах строків, встановлених частиною першою цієї статті.

**Стаття 14.** Зміна ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці

Підвищення або зниження ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці здійснюються на підставі рішення державного експерта з питань таємниць або на підставі рішення суду у випадках, передбачених статтею 12 цього Закону, та оформляються Службою безпеки України шляхом внесення відповідних змін до Зводу відомостей, що становлять державну таємницю.

## Розділ III. ЗАСЕКРЕЧУВАННЯ ТА РОЗСЕКРЕЧУВАННЯ МАТЕРІАЛЬНИХ НОСІЇВ ІНФОРМАЦІЇ

**Стаття 15.** Засекречування та розсекречування матеріальних носіїв інформації

Засекречування матеріальних носіїв інформації здійснюється шляхом надання на підставі Зводу відомостей, що становлять державну таємницю (розгорнутих переліків відомостей, що становлять державну таємницю), відповідному документу, виробу або іншому матеріальному носію інформації грифа секретності посадовою особою, яка готує або створює документ, виріб або інший матеріальний носій інформації. Засекречування документів здійснюється лише в частині відомостей, що становлять державну таємницю. У разі подання запиту на документ, частина якого засекречена, доступ до такого документа забезпечується в частині, що не засекречена.

**Гриф секретності кожного матеріального носія секретної інформації повинен відповідати ступеню секретності інформації, яка у ньому міститься, згідно із Зводом відомостей, що становлять державну таємницю,** – **"особливої важливості", "цілком таємно" або "таємно"**. Реквізити кожного матеріального носія секретної інформації складаються із:

– грифа секретності;

– номера примірника;

– статті Зводу відомостей, що становлять державну таємницю, на підставі якої здійснюється засекречення;

– найменування посади та підпису особи, яка надала гриф секретності.

Якщо реквізити, зазначені у частині другій цієї статті, неможливо нанести безпосередньо на матеріальний носій секретної інформації, вони мають бути зазначені у супровідних документах.

## Розділ IV. ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ

**Стаття 18.** Основні організаційно-правові заходи щодо охорони державної таємниці

З метою охорони державної таємниці впроваджуються:

– єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

– дозвільний порядок провадження державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею;

– обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

– обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;

– особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею;

– режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею;

– спеціальний порядок допуску та доступу громадян до державної таємниці;

– технічний та криптографічний захисти секретної інформації.

**Стаття 21.** Режимно-секретні органи

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що провадять діяльність, пов'язану з державною таємницею, з метою розроблення та здійснення заходів щодо забезпечення режиму секретності, постійного контролю за їх додержанням створюються на правах окремих структурних підрозділів режимно-секретні органи (далі – РСО), які підпорядковуються безпосередньо керівнику державного органу, органу місцевого самоврядування, підприємства, установи, організації.

**Стаття 22.** Допуск громадян до державної таємниці

Залежно від ступеня секретності інформації встановлюються такі форми допуску до державної таємниці:

**– форма 1 – для роботи з секретною інформацією, що має ступені секретності "особливої важливості", "цілком таємно" та "таємно";**

**– форма 2 – для роботи з секретною інформацією, що має ступені секретності "цілком таємно" та "таємно";**

**– форма 3 – для роботи з секретною інформацією, що має ступінь секретності "таємно",**

**а також такі терміни дії допусків:**

**– для форми 1 – 5 років;**

**– для форми 2 – 7 років;**

**– для форми 3 – 10 років.**

**Стаття 28.** Обов'язки громадянина щодо збереження державної таємниці

**Громадянин, якому надано допуск до державної таємниці, зобов'язаний**:

– не допускати розголошення будь-яким способом державної таємниці, яка йому довірена або стала відомою у зв'язку з виконанням службових обов'язків;

– не брати участі в діяльності політичних партій та громадських організацій, діяльність яких заборонена в порядку, встановленому законом;

– не сприяти іноземним державам, іноземним організаціям чи їх представникам, а також окремим іноземцям та особам без громадянства у

провадженні діяльності, що завдає шкоди інтересам національної безпеки України;

– виконувати вимоги режиму секретності;

– повідомляти посадових осіб, які надали йому доступ до державної таємниці, та відповідні режимно-секретні органи про виникнення обставин, передбачених статтею 23 цього Закону, або інших обставин, що перешкоджають збереженню довіреної йому державної таємниці, а також повідомляти у письмовій формі про свій виїзд з України;

– додержуватися інших вимог законодавства про державну таємницю.

**Стаття 29.** Обмеження прав у зв'язку з допуском та доступом до державної таємниці

Громадянин, якому було надано допуск та доступ до державної таємниці у порядку, встановленому законодавством, і який реально був обізнаний з нею, може бути обмежений у праві виїзду на постійне місце проживання в іноземну державу до розсекречування відповідної інформації, але **не більш як на п'ять років з часу припинення діяльності, пов'язаної з державною таємницею**.

Не обмежується виїзд у держави, з якими Україна має міжнародні договори, що передбачають такий виїзд і згода на обов'язковість яких надана Верховною Радою України.

На громадянина також поширюються обмеження свободи інформаційної діяльності, що випливають з цього Закону.

**Стаття 35.** Технічний та криптографічний захисти секретної інформації

Технічний та криптографічний захисти секретної інформації здійснюються в порядку, встановленому Президентом України.

**Стаття 36.** Оперативно-розшукові заходи щодо охорони державної таємниці

Оперативно-розшукові заходи щодо охорони державної таємниці здійснюються відповідно до Закону України "Про оперативно-розшукову діяльність".

## Розділ V. КОНТРОЛЬ ЗА ЗАБЕЗПЕЧЕННЯМ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА НАГЛЯД ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

**Стаття 37.** Контроль за забезпеченням охорони державної таємниці

Керівники державних органів, органів місцевого самоврядування, підприємств, установ і організацій зобов'язані здійснювати постійний контроль за забезпеченням охорони державної таємниці.

Контроль за додержанням законодавства про державну таємницю в системі Служби безпеки України здійснюється відповідно до Закону України "Про Службу безпеки України".

## Розділ VI. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

**Стаття 39.** Відповідальність за порушення законодавства про державну таємницю

Посадові особи та громадяни, винні у:

– розголошенні державної таємниці;

– втраті документів та інших матеріальних носіїв секретної інформації;

– недодержанні встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

– засекречуванні інформації, зазначеної у частинах третій і четвертій статті 8 цього Закону;

– навмисному невіднесенні до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України, а також необгрунтованому заниженні ступеня секретності або необгрунтованому розсекречуванні секретної інформації;

– безпідставному засекречуванні інформації, у тому числі з порушенням вимог Закону України "Про доступ до публічної інформації";

– наданні грифа секретності матеріальним носіям інформації, яка не становить державної таємниці, або ненаданні грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставному скасуванні чи зниженні грифа секретності матеріальних носіїв секретної інформації;

– порушенні встановленого законодавством порядку надання допуску та доступу до державної таємниці;

– порушенні встановленого законодавством режиму секретності та невиконанні обов'язків щодо збереження державної таємниці;

– невжитті заходів щодо забезпечення охорони державної таємниці та незабезпеченні контролю за охороною державної таємниці;

– провадженні діяльності, пов'язаної з державною таємницею, без одержання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщенні державних замовлень на виконання робіт, доведенні мобілізаційних завдань, пов'язаних з державною таємницею, в державних органах, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею;

– недодержанні вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства і проведення роботи з ними;

– невиконанні норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї інформації або просочення її технічними каналами,

несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно із законом.

## 1.6. Закон України «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.

**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;

– **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;

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

– **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;

– **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;

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

– **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;

– **суб'єкт персональних даних** – фізична особа, персональні дані якої обробляються;

– **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.

**Стаття 4. Суб'єкти відносин, пов'язаних із персональними даними**

1. **Суб'єктами** відносин, пов'язаних із персональними даними, є:

– суб'єкт персональних даних;

– володілець персональних даних;

– розпорядник персональних даних;

– третя особа;

– Уповноважений Верховної Ради України з прав людини (далі – Уповноважений).

2. **Володільцем чи розпорядником персональних даних** можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, які обробляють персональні дані відповідно до закону.

3. **Розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування,** крім цих органів, може бути лише підприємство державної або комунальної форми власності.

4. **Володілець персональних даних може доручити** обробку персональних даних розпоряднику персональних даних відповідно до договору, укладеного в письмовій формі.

5. **Розпорядник персональних даних** може обробляти персональні дані лише з метою і в обсязі, визначених у договорі.

**Стаття 5. Об'єкти захисту**

1. **Об'єктами захисту є персональні дані**.

2. Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою**. Не є конфіденційною інформацією персональні дані,** що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень.

3. **Персональні дані, зазначені у декларації особи**, уповноваженої на виконання функцій держави або місцевого самоврядування, оформленій за формою, визначеною відповідно до Закону України "Про запобігання корупції", **не належать до інформації з обмеженим доступом, крім відомостей, визначених Законом України "Про запобігання корупції".**

**Не належить до інформації з обмеженим доступом інформація про отримання у будь-якій формі фізичною особою** бюджетних коштів, державного чи комунального майна, структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага керівника, заступника керівника

юридичної особи публічного права, керівника, заступника керівника, члена наглядової ради державного чи комунального підприємства або державної чи комунальної організації, що має на меті одержання прибутку, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради господарського товариства, у статутному капіталі якого більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді, крім випадків, передбачених статтею 6 Закону України "Про доступ до публічної інформації".

**Не належить до інформації з обмеженим доступом інформація про фізичних осіб, які мають податковий борг, яка публікується на офіційному веб-порталі центрального органу виконавчої влади, що реалізує державну податкову політику, відповідно до вимог пункту 35.4 статті 35 Податкового кодексу України.**

Законом може бути заборонено віднесення інших відомостей, що є персональними даними, до інформації з обмеженим доступом.

**Стаття 6. Загальні вимоги до обробки персональних даних**

1. Мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних.

Обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки.

У разі зміни визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, для подальшої обробки даних володілець персональних даних повинен отримати згоду суб’єкта персональних даних на обробку його даних відповідно до зміненої мети, якщо інше не передбачено законом.

2. Персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їх обробки.

3. Склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки.

4. Первинними джерелами відомостей про фізичну особу є: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.

5. Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб’єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.

6. Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

7. Якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим.

8. Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися.

Подальша обробка персональних даних в історичних, статистичних чи наукових цілях може здійснюватися за умови забезпечення їх належного захисту.

**Стаття 7. Особливі вимоги до обробки персональних даних**

1. Забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних.

2. Положення частини першої цієї статті не застосовується, якщо обробка персональних даних:

1) здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;

2) необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;

3) необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;

4) здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних;

5) необхідна для обґрунтування, задоволення або захисту правової вимоги;

6) необхідна в цілях охорони здоров'я для:

– встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, моніторингу відповідності встановленим умовам надання таких послуг функціонування електронної системи охорони здоров'я за умови, що такі дані обробляються медичним працівником, фахівцем з реабілітації або іншою особою закладу охорони здоров'я, реабілітаційного закладу чи фізичною особою – підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов'язки щодо забезпечення захисту персональних даних та поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, працівниками закладу, що здійснює державний санітарно-епідеміологічний нагляд та діяльність у галузі громадського здоров'я, який одержав ліцензію на провадження господарської діяльності з медичної

практики, на яких покладено обов’язки щодо забезпечення захисту персональних даних;

– контролю якості надання медичних послуг за умови, що такі дані обробляються працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері контролю якості надання медичних послуг;

– обміну інформацією про фінансування медичних послуг та послуг у сфері охорони здоров’я за умови, що такі дані обробляються працівниками Фонду соціального страхування України, Пенсійного фонду України, Фонду соціального захисту осіб з інвалідністю, центрального органу виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, на яких покладено обов’язки щодо забезпечення захисту персональних даних.

**$6^{-1}$) необхідна в цілях забезпечення ведення військового обліку призовників, військовозобов’язаних та резервістів (в обсягах даних, зазначених у статті 7 Закону України "Про Єдиний державний реєстр призовників, військовозобов’язаних та резервістів");**

7) стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом;

8) стосується даних, які були явно оприлюднені суб'єктом персональних даних.

**Стаття 8. Права суб'єкта персональних даних**

1. Особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

2. **Суб'єкт персональних даних має право:**

– знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

– отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

– на доступ до своїх персональних даних;

– отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних;

– пред’являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

– пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

– на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання

відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

– звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду;

– застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

– вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

– відкликати згоду на обробку персональних даних;

– знати механізм автоматичної обробки персональних даних;

– на захист від автоматизованого рішення, яке має для нього правові наслідки.

**Стаття 9. Повідомлення про обробку персональних даних**

1. Володілець персональних даних повідомляє Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, упродовж тридцяти робочих днів з дня початку такої обробки.

Види обробки персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, та категорії суб’єктів, на яких поширюється вимога щодо повідомлення, визначаються Уповноваженим.

2. Повідомлення про обробку персональних даних подається за формою та в порядку, визначеними Уповноваженим.

3. Володілець персональних даних зобов’язаний повідомляти Уповноваженого про кожну зміну відомостей, що підлягають повідомленню, упродовж десяти робочих днів з дня настання такої зміни.

4. Інформація, що повідомляється відповідно до цієї статті, підлягає оприлюдненню на офіційному веб-сайті Уповноваженого в порядку, визначеному Уповноваженим.

**Стаття 10. Використання персональних даних**

1. Використання персональних даних передбачає будь-які дії володільця щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюються за згодою суб'єкта персональних даних чи відповідно до закону.

2. Використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних. Володільцю забороняється розголошувати відомості стосовно суб'єктів персональних даних, доступ до персональних даних яких надається іншим суб'єктам відносин, пов'язаних з такими даними.

3. **Використання персональних даних працівниками суб'єктів відносин, пов'язаних з персональними даними, повинно здійснюватися лише відповідно до їхніх професійних чи службових або трудових обов'язків.** Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків,

передбачених законом. Таке зобов'язання чинне після припинення ними діяльності, пов'язаної з персональними даними, крім випадків, установлених законом.

4. **Відомості про особисте життя фізичної особи не можуть використовуватися як чинник, що підтверджує чи спростовує її ділові якості.**

5. **Стаття 11. Підстави для обробки персональних даних**

1. Підставами для обробки персональних даних є:

– згода суб’єкта персональних даних на обробку його персональних даних;

– дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;

– укладення та виконання правочину, стороною якого є суб’єкт персональних даних або який укладено на користь суб’єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб’єкта персональних даних;

– захист життєво важливих інтересів суб’єкта персональних даних;

– необхідність виконання обов’язку володільця персональних даних, який передбачений законом;

– необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб’єкта персональних даних у зв’язку з обробкою його даних переважають такі інтереси.

**Стаття 12. Збирання персональних даних**

1. Збирання персональних даних є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу.

2. Суб’єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані:

– в момент збору персональних даних, якщо персональні дані збираються у суб’єкта персональних даних;

– в інших випадках протягом тридцяти робочих днів з дня збору персональних даних.

**Стаття 13. Накопичення та зберігання персональних даних**

1. Накопичення персональних даних передбачає дії щодо поєднання та систематизації відомостей про фізичну особу чи групу фізичних осіб або внесення цих даних до бази персональних даних.

2. Зберігання персональних даних передбачає дії щодо забезпечення їх цілісності та відповідного режиму доступу до них.

**Стаття 14. Поширення персональних даних**

1. Поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних.

2. Поширення персональних даних без згоди суб’єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і

лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту, прав людини та для проведення Всеукраїнського перепису населення.

3. Виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані.

4. Сторона, якій передаються персональні дані, повинна попередньо вжити заходів щодо забезпечення вимог цього Закону.

**Стаття 15. Видалення або знищення персональних даних**

1. Персональні дані видаляються або знищуються в порядку, встановленому відповідно до вимог закону.

2. Персональні дані підлягають видаленню або знищенню у разі:

– закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом;

– припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом;

– видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого;

– набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

3. Персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню у встановленому законодавством порядку.

4. Персональні дані, зібрані під час виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом, видаляються або знищуються відповідно до вимог закону.

**Стаття 16. Порядок доступу до персональних даних**

1. Порядок доступу до персональних даних третіх осіб визначається умовами згоди суб’єкта персональних даних на обробку цих даних, наданої володільцю персональних даних, або відповідно до вимог закону. Порядок доступу третіх осіб до персональних даних, які перебувають у володінні розпорядника публічної інформації, визначається Законом України "Про доступ до публічної інформації", крім даних, що отримує від інших органів центральний орган виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, під час здійснення верифікації та моніторингу державних виплат.

2. Доступ до персональних даних третій особі не надається, якщо зазначена особа відмовляється взяти на себе зобов'язання щодо забезпечення виконання вимог цього Закону або неспроможна їх забезпечити.

3. Суб'єкт відносин, пов'язаних з персональними даними, подає запит щодо доступу (далі – запит) до персональних даних володільцю персональних даних.

4. **У запиті зазначаються**:

– прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка подає запит (для фізичної особи – заявника);

– найменування, місцезнаходження юридичної особи, яка подає запит, посада, прізвище, ім'я та по батькові особи, яка засвідчує запит; підтвердження

того, що зміст запиту відповідає повноваженням юридичної особи (для юридичної особи – заявника);

– прізвище, ім'я та по батькові, а також інші відомості, що дають змогу ідентифікувати фізичну особу, стосовно якої робиться запит;

– відомості про базу персональних даних, стосовно якої подається запит, чи відомості про володільця чи розпорядника персональних даних;

– перелік персональних даних, що запитуються;

– мета та/або правові підстави для запиту.

5. **Строк вивчення запиту** на предмет його задоволення не може **перевищувати десяти робочих днів з дня його надходження**.

Протягом цього строку володілець персональних даних доводить до відома особи, яка подає запит, що запит буде задоволено або відповідні персональні дані не підлягають наданню, із зазначенням підстави, визначеної у відповідному нормативно-правовому акті.

**Запит задовольняється протягом тридцяти календарних дні**в з дня його надходження, якщо інше не передбачено законом.

6. Суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними, за умови надання інформації, визначеної у пункті 1 частини четвертої цієї статті, крім випадків, установлених законом.

**Стаття 17. Відстрочення або відмова у доступі до персональних даних**

1. Відстрочення доступу суб'єкта персональних даних до своїх персональних даних не допускається.

2. Відстрочення доступу до персональних даних третіх осіб допускається у разі, якщо необхідні дані не можуть бути надані протягом тридцяти календарних днів з дня надходження запиту. При цьому загальний термін вирішення питань, порушених у запиті, не може перевищувати сорока п'яти календарних днів.

Повідомлення про відстрочення доводиться до відома третьої особи, яка подала запит, у письмовій формі з роз'ясненням порядку оскарження такого рішення.

**У повідомленні про відстрочення зазначаються:**

**–** прізвище, ім'я та по батькові посадової особи;

– дата відправлення повідомлення;

– причина відстрочення;

– строк, протягом якого буде задоволено запит.

3. Відмова у доступі до персональних даних допускається, якщо доступ до них заборонено згідно із законом.

**У повідомленні про відмову зазначаються:**

– прізвище, ім'я, по батькові посадової особи, яка відмовляє у доступі;

– дата відправлення повідомлення;

– причина відмови.

**Стаття 18. Оскарження рішення про відстрочення або відмову в доступі до персональних даних**

1. Рішення про відстрочення або відмову у доступі до персональних даних може бути оскаржено до Уповноваженого Верховної Ради України з прав людини або суду.

2. Якщо запит зроблено суб'єктом персональних даних щодо даних про себе, обов'язок доведення в суді законності відмови у доступі покладається на володільця персональних даних, до якого подано запит.

**Стаття 19. Оплата доступу до персональних даних**

1. Доступ суб'єкта персональних даних до даних про себе здійснюється безоплатно.

2. Доступ інших суб'єктів відносин, пов'язаних з персональними даними, до персональних даних певної фізичної особи чи групи фізичних осіб може бути платним у разі додержання умов, визначених цим Законом. Оплаті підлягає робота, пов'язана з обробкою персональних даних, а також робота з консультування та організації доступу до відповідних даних.

4. Органи державної влади та органи місцевого самоврядування мають право на безперешкодний і безоплатний доступ до персональних даних відповідно до їх повноважень.

**Стаття 20. Зміни і доповнення до персональних даних**

1. Володільці чи розпорядники персональних даних зобов'язані вносити зміни до персональних даних на підставі вмотивованої письмової вимоги суб'єкта персональних даних.

2. Володільці чи розпорядники персональних даних зобов’язані вносити зміни до персональних даних також за зверненням інших суб’єктів відносин, пов’язаних із персональними даними, якщо на це є згода суб’єкта персональних даних чи відповідна зміна здійснюється згідно з приписом Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого чи за рішенням суду, що набрало законної сили.

3. Зміна персональних даних, які не відповідають дійсності, проводиться невідкладно з моменту встановлення невідповідності.

**Стаття 21. Повідомлення про дії з персональними даними**

1. Про передачу персональних даних третій особі володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, якщо цього вимагають умови його згоди або інше не передбачено законом.

2. Повідомлення, зазначені у частині першій цієї статті, не здійснюються у разі:

– передачі персональних даних за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом;

– виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом;

– здійснення обробки персональних даних в історичних, статистичних чи наукових цілях;

– повідомлення суб’єкта персональних даних відповідно до вимог частини другої статті 12 цього Закону.

3. Про зміну, видалення чи знищення персональних даних або обмеження доступу до них володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, а також суб'єктів відносин, пов'язаних із персональними даними, яким ці дані було передано.

**Стаття 22. Контроль за додержанням законодавства про захист персональних даних**

1. Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснюють такі органи:

– уповноважений;

– суди.

**Стаття 24. Забезпечення захисту персональних даних**

1. Володільці, розпорядники персональних даних та треті особи зобов’язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.

2. В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці.

Інформація про зазначений структурний підрозділ або відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення.

3. Структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці:

– інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;

– взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

4. Фізичні особи-підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист персональних даних, якими вони володіють, згідно з вимогами закону.

**Стаття 28. Відповідальність за порушення законодавства про захист персональних даних**

Порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом.

## 1.7. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури

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-телекомунікаційних 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.

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.

## 1.8. ДСТУ 3396.0,1,2-97

**ДСТУ 3396.0-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення**

Цей стандарт установлює об'єкт захисту, мету, основні організаційно-технічні положення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів з 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.

**ДСТУ 3396.1-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт**

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.

**ДСТУ 3396.2-97. Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення**

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.

## 1.9. ДСТУ ISO/IEC 15408-1:2017

**ISO/IEC 15408-1:2022. Інформаційна безпека, кібербезпека та захист конфіденційності. Критерії оцінки IT-безпеки. Частина 1. Вступ і загальна модель**

Цей документ встановлює загальні концепції та принципи оцінювання безпеки IT і визначає загальну модель оцінювання, що надається різними частинами стандарту, який у цілому призначений для використання в якості основи для оцінки властивостей безпеки IT-продуктів.

Цей документ містить огляд усіх частин серії ISO/IEC 15408. Він описує різні частини серії ISO/IEC 15408; визначає терміни та скорочення, які слід використовувати в усіх частинах стандарту; встановлює основну концепцію мети оцінювання (TOE); описує контекст оцінювання та описує аудиторію, якій адресовані критерії оцінювання. Дано вступ до основних концепцій безпеки, необхідних для оцінки IT-продуктів.

Цей документ представляє:

– ключові поняття профілів захисту (PP), модулів PP, конфігурацій PP, пакетів, цілей безпеки (ST) і типів відповідності;

– опис організації компонентів безпеки по всій моделі;

– різні операції, за допомогою яких функціональні компоненти та компоненти гарантії, наведені в ISO/IEC 15408-2 та ISO/IEC 15408-3, можуть бути налаштовані шляхом використання дозволених операцій;

– загальну інформацію про методи оцінювання, наведені в ISO/IEC 18045;

– настанова щодо застосування ISO/IEC 15408-4 для розробки методів оцінювання (EM) і діяльності з оцінювання (EA), виведених із ISO/IEC 18045;

– загальну інформацію про попередньо визначені рівні гарантії оцінювання (EAL), визначені в ISO/IEC 15408-5;

– інформація щодо обсягу схем оцінювання.

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

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.

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

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 Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України нових послуг.

## 1.12. Закон України «Про доступ до публічної інформації»

Цей Закон визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес, та складається з наступних розділів і статей.

**Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ**

**Стаття 1. Публічна інформація**

**Стаття 2. Мета і сфера дії Закону**

**Стаття 3. Гарантії забезпечення права на доступ до публічної інформації**

**Стаття 4. Принципи забезпечення доступу до публічної інформації**

## Розділ І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

### Стаття 1. Публічна інформація

1. **Публічна інформація** – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом.

2. Публічна інформація є відкритою, крім випадків, встановлених законом.

**Стаття 3. Гарантії забезпечення права на доступ до публічної інформації**

1. **Право на доступ до публічної інформації** гарантується:

– обов'язком розпорядників інформації надавати та оприлюднювати інформацію, крім випадків, передбачених законом;

– визначенням розпорядником інформації спеціальних структурних підрозділів або посадових осіб, які організовують у встановленому порядку доступ до публічної інформації, якою він володіє;

– максимальним спрощенням процедури подання запиту та отримання інформації;

– доступом до засідань колегіальних суб'єктів владних повноважень, крім випадків, передбачених законодавством;

– здійсненням парламентського, громадського та державного контролю за дотриманням прав на доступ до публічної інформації;

– юридичною відповідальністю за порушення законодавства про доступ до публічної інформації.

**Стаття 4. Принципи забезпечення доступу до публічної інформації**

1. Доступ до публічної інформації відповідно до цього Закону здійснюється на принципах:

– прозорості та відкритості діяльності суб'єктів владних повноважень;

– вільного отримання, поширення та будь-якого іншого використання інформації, що була надана або оприлюднена відповідно до цього Закону, крім обмежень, встановлених законом;

– рівноправності, незалежно від ознак раси, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак.

**Розділ II. ПОРЯДОК ДОСТУПУ ДО ІНФОРМАЦІЇ**

**Стаття 5. Забезпечення доступу до інформації**

1. Доступ до інформації забезпечується шляхом:

1) систематичного та оперативного оприлюднення інформації:

– в офіційних друкованих виданнях;

– на офіційних веб-сайтах в мережі Інтернет;

– на єдиному державному веб-порталі відкритих даних;

– на інформаційних стендах;

– будь-яким іншим способом;

2) надання інформації за запитами на інформацію.

**Стаття 6. Публічна інформація з обмеженим доступом**

**1. Інформацією з обмеженим доступом є:**

**– конфіденційна інформація;**

**– таємна інформація;**

**– службова інформація.**

2. Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

– виключно 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;

– розголошення інформації може завдати істотної шкоди цим інтересам;

– шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

3. Інформація з обмеженим доступом має надаватися розпорядником інформації, якщо він правомірно оприлюднив її раніше.

4. Інформація з обмеженим доступом має надаватися розпорядником інформації, якщо немає законних підстав для обмеження у доступі до такої інформації, які існували раніше.

6. Не належать до інформації з обмеженим доступом відомості, зазначені у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, поданій відповідно до Закону України "Про запобігання корупції", крім випадків, визначених зазначеним Законом.

7. Не належить до інформації з обмеженим доступом інформація про структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага керівника, заступника керівника юридичної особи публічного права, керівника, заступника керівника, члена наглядової ради державного чи комунального підприємства або державної чи комунальної організації, що має на меті одержання прибутку, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради господарського товариства, у статутному капіталі якого більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді.

8. Обмеженню доступу підлягає інформація, а не документ. Якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений.

**Стаття 7. Конфіденційна інформація**

1. **Конфіденційна інформація** – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Не може бути віднесена до конфіденційної інформація, зазначена в частині першій і другій статті 13 цього Закону.

**Стаття 8. Таємна інформація**

1. **Таємна інформація** – інформація, доступ до якої обмежується відповідно до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

**Стаття 9. Службова інформація**

1. Відповідно до вимог частини другої статті 6 цього Закону до службової може належати така інформація:

– що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або

здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

– зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

2. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф **"для службового користування"**. Доступ до таких документів надається відповідно до частини другої статті 6 цього Закону.

**Стаття 10. Доступ до інформації про особу**

1. Кожна **особа має право**:

– знати у період збирання інформації, але до початку її використання, які відомості про неї та з якою метою збираються, як, ким і з якою метою вони використовуються, передаються чи поширюються, крім випадків, встановлених законом;

– доступу до інформації про неї, яка збирається та зберігається;

– вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання якої здійснюється з порушенням вимог закону;

– на ознайомлення за рішенням суду з інформацією про інших осіб, якщо це необхідно для реалізації та захисту прав та законних інтересів;

– на відшкодування шкоди у разі розкриття інформації про цю особу з порушенням вимог, визначених законом.

2. Обсяг інформації про особу, що збирається, зберігається і використовується розпорядниками інформації, має бути максимально обмеженим і використовуватися лише з метою та у спосіб, визначений законом.

3. Розпорядники інформації, які володіють інформацією про особу, зобов'язані:

– надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом;

– використовувати її лише з метою та у спосіб, визначений законом;

– вживати заходів щодо унеможливлення несанкціонованого доступу до неї інших осіб;

4) виправляти неточну та застарілу інформацію про особу самостійно або на вимогу осіб, яких вона стосується.

4. Зберігання інформації про особу не повинно тривати довше, ніж це необхідно для досягнення мети, задля якої ця інформація збиралася.

5. Відмова особі в доступі до інформації про неї, приховування, незаконне збирання, використання, зберігання чи поширення інформації можуть бути оскаржені.

**Стаття 10.** Публічна інформація у формі відкритих даних

1. **Публічна інформація у формі відкритих даних** – це публічна інформація у форматі, що дозволяє її автоматизоване оброблення електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання.

## Розділ ІІІ. СУБ'ЄКТИ ВІДНОСИН У СФЕРІ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ

### Стаття 12. Визначення та перелік суб'єктів

1. **Суб'єктами** відносин у сфері доступу до публічної інформації є:

– **запитувачі інформації** – фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень;

– **розпорядники інформації** – суб'єкти, визначені у статті 13 цього Закону;

– **структурний підрозділ або відповідальна особа з питань доступу до публічної інформації розпорядників інформації**.

### Стаття 13. Розпорядники інформації

1. **Розпорядниками інформації** для цілей цього Закону визнаються:

– **суб'єкти владних повноважень** – органи державної влади, інші державні органи, органи місцевого самоврядування, органи влади Автономної Республіки Крим, інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання;

– **юридичні особи, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим**, – стосовно інформації щодо використання бюджетних коштів;

– **особи, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг**, – стосовно інформації, пов'язаної з виконанням їхніх обов'язків;

– **суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями**, – стосовно інформації щодо умов постачання товарів, послуг та цін на них;

– **юридичні особи публічного права, державні/комунальні підприємства або державні/комунальні організації, що мають на меті одержання прибутку, господарські товариства, у статутному капіталі яких більше 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді**, – щодо інформації про структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага їх керівника, заступника керівника, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради.

### Стаття 14. Обов'язки розпорядників інформації

1. Розпорядники інформації зобов'язані:

– оприлюднювати інформацію, передбачену цим та іншими законами;

– систематично вести облік документів, що знаходяться в їхньому володінні;

– вести облік запитів на інформацію;

– визначати спеціальні місця для роботи запитувачів з документами чи їх копіями, а також надавати право запитувачам робити виписки з них, фотографувати, копіювати, сканувати їх, записувати на будь-які носії інформації тощо;

– мати спеціальні структурні підрозділи або призначати відповідальних осіб для забезпечення доступу запитувачів до інформації та оприлюднення інформації;

– надавати та оприлюднювати достовірну, точну та повну інформацію, а також у разі потреби перевіряти правильність та об’єктивність наданої інформації і оновлювати оприлюднену інформацію.

## Розділ IV. РЕАЛІЗАЦІЯ ПРАВА НА ДОСТУП ДО ІНФОРМАЦІЇ ЗА ІНФОРМАЦІЙНИМ ЗАПИТОМ

### Стаття 19. Оформлення запитів на інформацію

1. **Запит на інформацію** – це прохання особи до розпорядника інформації надати публічну інформацію, що знаходиться у його володінні.

2. Запитувач має право звернутися до розпорядника інформації із запитом на інформацію незалежно від того, стосується ця інформація його особисто чи ні, без пояснення причини подання запиту.

3. Запит на інформацію може бути індивідуальним або колективним. Запити можуть подаватися в усній, письмовій чи іншій формі (поштою, факсом, телефоном, електронною поштою) на вибір запитувача.

4. Письмовий запит подається в довільній формі.

5. Запит на інформацію має містити:

– ім'я (найменування) запитувача, поштову адресу або адресу електронної пошти, а також номер засобу зв'язку, якщо такий є;

– загальний опис інформації або вид, назву, реквізити чи зміст документа, щодо якого зроблено запит, якщо запитувачу це відомо;

– підпис і дату за умови подання запиту в письмовій формі.

6. З метою спрощення процедури оформлення письмових запитів на інформацію особа може подавати запит шляхом заповнення відповідних форм запитів на інформацію, які можна отримати в розпорядника інформації та на офіційному веб-сайті відповідного розпорядника. Зазначені форми мають містити стислу інструкцію щодо процедури подання запиту на інформацію, її отримання тощо.

7. У разі якщо з поважних причин (інвалідність, обмежені фізичні можливості тощо) особа не може подати письмовий запит, його має оформити відповідальна особа з питань доступу до публічної інформації, обов'язково зазначивши в запиті своє ім'я, контактний телефон, та надати копію запиту особі, яка його подала.

### Стаття 20. Строк розгляду запитів на інформацію

1. Розпорядник інформації має надати відповідь на запит на інформацію **не пізніше п'яти робочих днів** з дня отримання запиту.

2. У разі якщо запит на інформацію стосується інформації, необхідної для захисту життя чи свободи особи, щодо стану довкілля, якості харчових продуктів і предметів побуту, аварій, катастроф, небезпечних природних явищ та інших надзвичайних подій, що сталися або можуть статись і загрожують безпеці громадян, відповідь має бути надана **не пізніше 48 годин** з дня отримання запиту.

3. Клопотання про термінове опрацювання запиту має бути обґрунтованим.

4. У разі якщо запит стосується надання великого обсягу інформації або потребує пошуку інформації серед значної кількості даних, розпорядник інформації може **продовжити строк розгляду запиту до 20 робочих днів** з обґрунтуванням такого продовження. Про продовження строку розпорядник інформації повідомляє запитувача в письмовій формі не пізніше п'яти робочих днів з дня отримання запиту.

**Стаття 21. Плата за надання інформації**

1. Інформація на запит надається безкоштовно.

2. У разі якщо задоволення запиту на інформацію передбачає виготовлення копій документів обсягом **більш як 10 сторінок, запитувач зобов'язаний відшкодувати фактичні витрати на копіювання та друк**.

3. Розмір фактичних витрат визначається відповідним розпорядником на копіювання та друк в межах граничних норм, встановлених Кабінетом Міністрів України. У разі якщо розпорядник інформації не встановив розміру плати за копіювання або друк, інформація надається безкоштовно.

4. При наданні особі інформації про себе та інформації, що становить суспільний інтерес, плата за копіювання та друк не стягується.

**Стаття 22. Відмова та відстрочка в задоволенні запиту на інформацію**

1. Розпорядник інформації має право відмовити в задоволенні запиту в таких випадках:

1) розпорядник інформації не володіє і не зобов'язаний відповідно до його компетенції, передбаченої законодавством, володіти інформацією, щодо якої зроблено запит;

2) інформація, що запитується, належить до категорії інформації з обмеженим доступом відповідно до частини другої статті 6 цього Закону;

3) особа, яка подала запит на інформацію, не оплатила передбачені статтею 21 цього Закону фактичні витрати, пов'язані з копіюванням або друком;

4) не дотримано вимог до запиту на інформацію, передбачених частиною п'ятою статті 19 цього Закону.

2. Відповідь розпорядника інформації про те, що інформація може бути одержана запитувачем із загальнодоступних джерел, або відповідь не за суттю запиту вважається неправомірною відмовою в наданні інформації.

3. Розпорядник інформації, який не володіє запитуваною інформацією, але якому за статусом або характером діяльності відомо або має бути відомо, хто нею володіє, зобов'язаний направити цей запит належному розпоряднику з одночасним повідомленням про це запитувача. У такому разі відлік строку розгляду запиту на інформацію починається з дня отримання запиту належним розпорядником.

4. У відмові в задоволенні запиту на інформацію має бути зазначено:

– прізвище, ім'я, по батькові та посаду особи, відповідальної за розгляд запиту розпорядником інформації;

– дату відмови;

– мотивовану підставу відмови;

– порядок оскарження відмови;

– підпис.

5. Відмова в задоволенні запиту на інформацію надається в письмовій формі.

6. Відстрочка в задоволенні запиту на інформацію допускається в разі, якщо запитувана інформація не може бути надана для ознайомлення в передбачені цим Законом строки у разі настання обставин непереборної сили. Рішення про відстрочку доводиться до відома запитувача у письмовій формі з роз'ясненням порядку оскарження прийнятого рішення.

7. У рішенні про відстрочку в задоволенні запиту на інформацію має бути зазначено:

– прізвище, ім'я, по батькові та посаду особи, відповідальної за розгляд запиту розпорядником інформації;

– дату надсилання або вручення повідомлення про відстрочку;

– причини, у зв'язку з якими запит на інформацію не може бути задоволений у встановлений цим Законом строк;

– строк, у який буде задоволено запит;

– підпис.

## 1.13. Загрози, яким підлягає інформація

Як показує аналіз, сучасні комп’ютерні системи підлягають наступним найбільш розповсюдженим загрозам:

– ненавмисні помилки користувачів, операторів, системних адміністраторів і інших осіб (65%)

– крадіжки і фальсифікація В більшості випадків, що розслідувалися, винними виявлялися штатні співробітники організацій, відмінно знайомі із режимом роботи і мірами захисту;

– “ображені співробітники” – нинішні і колишні, наприклад, шляхом вживляння “логічної бомби”, введення невірних даних, вилучення або модифікації даних;

– загрози від навколишньої середи (відключення зв’язку, пожежа і т.і.);

– дії хакерів і злочинців, що можуть здійснювати обман шляхом створення неправдивих або модифікованих справжніх документів (інформації).

## 1.14. Стратегії реалізації загроз

**В процесі реалізації загроз порушники і злочинці можуть реалізовувати наступні стратегії**:

1. Видавання себе за іншого користувача, щоб зняти з себе відповідальність.

2. Видавання себе за іншого користувача, щоб використовувати його повноваження з метою:

– формування неправдивої інформації;

– зміни істинної інформації;

– застосування неправдивого посвідчення для отримання несанкціонованого доступу (НСД);

– санкціонування неправдивих обмінів інформацією або іхнє підтвердження.

3. Відмова джерела від факту формування і передачі інформації.

4. Твердження джерела про те, що одержувачу була відправлена інформація, в тому числі в певний час, що насправді не була відправлена або відправлена в інший час.

5. Відмова отримувача від факту отримання інформації, хоча насправді вона була отримана, або неправдиве затвердження про час її отримання.

6. Твердження про те, що інформація отримана від певного користувача, хоча насправді вона сформована самим же порушником.

7. Отримання НСД, тобто порушення конфіденційності інформації, що захищається.

8. Несанкціоноване розширення (зміна) своїх повноважень.

9. Несанкціонована зміна повноважень інших осіб (обмеження або розширення).

10. Введення в систему або активізація вірусів або інших “шкідливих” програм з метою перехоплення ключів і паролів, а також модифікації (непомітно) документів.

11. Спроба завадити передачі повідомлень між іншими користувачами, в частковості, внесення до повідомлення прихованих завад для того, щоб це повідомлення при автентифікації було спростоване.

12. Модифікація програмного забезпечення, наприклад, шляхом додання нових функцій.

13. Підрив довіри до протоколу шляхом виклику порушень або примушення інших порушити протокол шляхом введення неправдивої інформації і т.і.

## 1.15. Основні міри протидії загрозам безпеці, принципи побудови систем захисту, основні механізми захисту

Перекриття більшості названих загроз може бути здійснено за рахунок формування і проведення в життя **політики безпеки** – набору законів, правил і норм поведінки, які визначають те, як ІКС обробляє, захищає і розповсюджує інформацію. За суттю **політика безпеки** – це активний компонент захисту, що включає в себе аналіз можливих загроз і вибір мір протидії. В практичному додатку політика безпеки являє собою сукупність документованих управлінських рішень, направлених на захист інформації і асоційованих з нею ресурсів. В результаті реалізації такої політики повинна бути створена система

захисту інформації, що являє собою комплекс організаційних, технічних засобів і заходів, юридичних, законодавчих норм, фізичних обмежень й т.і., які реалізуються комплексно на всіх етапах життєвого циклу інформаційної системи: від проектування – і до застосування в різноманітних умовах.

В системах захисту інформації (СЗІ) повинні реалізовуватися функції безпеки і механізми безпеки; вони повинні перекривати всі виявлені загрози, перераховані вище.

## 1.16. Перелік основних задач, які повинні вирішуватися системою комп'ютерної безпеки:

– керування доступом користувачів до ресурсів ІКС, з метою її захисту від неправомірного випадкового або навмисного втручання у роботу системи і несанкціонованого (із перевищенням наданих повноваженнь) доступу до її інформаційних, програмних і апаратних ресурсів із боку сторонніх осіб, а також осіб із числа персоналу організації і користувачів;

– захист даних, що передаються по каналам зв'язку;

– реєстрація, збір, збереження, опрацювання і видача даних про усі події, що відбувалися у системі і мали відношення до її безпеки;

– контроль роботи користувачів системи з боку адміністрації і оперативне оповіщення адміністратора безпеки про спроби несанкціонованого доступу до ресурсів системи;

– контроль і підтримка цілісністності критичних ресурсів системи захисту і середовища виконання прикладних програм;

– забезпечення замкнутого середовища перевіреного програмного забезпечення, із метою захисту від безконтрольного впровадження у систему потенційно небезпечних програм (у яких можуть міститись вредоносні закладки або небезпечні помилки) і засобів подолання системи захисту, а також від впровадження і поширення комп'ютерних вірусів;

– керування засобами системи захисту.

Зазвичай розрізняють зовнішню і внутрішню безпеку комп'ютерних систем. **Зовнішня безпека** включає захист ІКС від стихійного лиха (пожежі, повені і т.п.) і від проникнення у систему зловмисника ззовні з цілями розкрадання, одержання доступу до інформації або виводу системи з ладу. **Внутрішня безпека** – створення надійних і зручних механізмів регламентації діяльністі усіх її законних користувачів і обслуговуючого персоналу для примусу їх до безумовного дотримання встановлених в організації дисципліни доступу до ресурсів системи.

**Міри протидії погрозам безпеки. Класифікація мір забезпечення безпеки комп'ютерних систем**

За способом здійснення усі міри забезпечення безпеки комп'ютерних систем підрозділяються на: правові (законодавчі), морально-етичні, організаційні (адміністративні), фізичні і технічні (апаратурні і програмні).

До **правових** мір захисту відносяться діючі у країні закони, укази і нормативні акти, що регламентують правила роботи з інформацією

До **морально-етичних** мір протидії відносяться норми поводження, що традиційно склались або складаються у міру поширення ЕОМ у країні або суспільстві.

**Організаційні (**адміністративні) міри захисту – це міри організаційного характеру, що регламентують процес функціонування системи опрацювання даних, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів з системою таким чином, щоб найбільшою мірою утруднити або виключити можливість реалізації погроз безпеки.

**Фізичні** міри захисту засновані на застосуванні різного роду механічних, електро- або електронно-механічних пристроїв і споруджень, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонент системи і захищаємої інформації, а також технічні засоби візуального спостереження, зв'язку і охоронної сигналізації.

**Технічні** (апаратно-програмні) міри захисту засновані на використанні різних електронних пристроїв і спеціальних програм, що входять до складу ІКС і виконують (самостійно або в комплексі з іншими засобами) функції захисту (ідентифікацію й автентифікацію користувачів, розмежування доступу до ресурсів, реєстрацію подій, криптографічне закриття інформації і т.д.)

## 1.17. Основні принципи побудови систем захисту інформаційно-комунікаційних систем (ІКС)

Захист інформації в ІКС повинний ґрунтуватися на наступних основних принципах:

- системності,
- комплексності;
- безперервності захисту;
- розумної достатності;
- гнучкості керування і застосування:
- відкритості алгоритмів і механізмів захисту;
- простоти застосування захисних мір і засобів.

**Принцип системності**

Системний підхід припускає необхідність обліку усіх взаємозалежних, взаємодіючих і елементів, умов і чинників, які змінюються в ІКС, значимих для розуміння і рішення проблеми забезпечення безпеки ІКС.

**Принцип комплексності**

У розпорядженні фахівців із комп'ютерної безпеки є широкий спектр мір, методів і засобів захисту комп'ютерних систем. Комплексне їхнє використання припускає погоджене застосування різнорідних засобів при побудові цілісної

системи захисту, що перекриває всі істотні канали реалізації погроз і не має слабких місць на стиках окремих її компонентів**.**

**Принцип безперервності захисту**

Захист інформації – це безупинний цілеспрямований процес, що припускає прийняття відповідних мір на всіх етапах життєвого циклу ІКС, починаючи із самих ранніх стадій проектування, а не тільки на етапі її експлуатації**.**

**Розумна достатність**

Створити абсолютно неперебoрну систему захисту принципово неможливо. При достатній кількості методів і засобів можна перебороти будь-який захист. Тому має сенс вести мову тільки про деякий прийнятний рівень безпеки.

**Гнучкість системи захисту**

Для забезпечення можливості варіювання рівнем захищеності, засоби захисту повинні мати визначену гнучкість. Особливо важливим ця властивість є в тих випадках, коли установку засобів захисту необхідно здійснювати на працюючу систему, не порушуючи процесу її нормального функціонування.

**Відкритість алгоритмів і механізмів захисту**

Суть принципу відкритості алгоритмів і механізмів захисту перебуває в тому, що захист не повинний забезпечуватися тільки за рахунок таємності структурної організації й алгоритмів функціонування її підсистем

**Принцип простоти застосування засобів захисту**

Механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути зв'язане зі знанням спеціальних мов або з виконанням дій, що вимагають значних додаткових працезатрат при звичайній роботі законних користувачів, а також не повинно жадати від користувача виконання рутинних малозрозумілих йому операцій (введення кількох паролів і імен і т.д.).

**Основні механізми захисту комп'ютерних систем від проникнення з метою дезорганізації їхньої роботи і НСД до інформації**

Затвердимо ряд понять, необхідних надалі.

**1. Об'єкт** – пасивний компонент системи, одиниця ресурсу автоматизованої системи (пристрій, диск, каталог, файл і т.п.), доступ до якого регламентується правилами розмежування доступу.

**2. Суб'єкт** – активний компонент системи (користувач, процес, програма), дії якого регламентуються правилами розмежування доступу.

**3. Доступ до інформації** – ознайомлення з інформацією, (копіювання, тиражування), її модифікація (корректировка) або знищення (видалення).

**4. Доступ до ресурсу** – одержання суб'єктом можливості маніпулювати (використовувати, управляти, змінювати характеристики і т.п.) даним ресурсом.

**5. Правила розмежування доступу** – сукупність правил, що регламентують права доступу суб'єктів до об'єктів у деякій системі.

**6. Розмежування доступу до ресурсів ІКС** – це такий порядок використання ресурсів автоматизованої системи, при якому суб'єкти одержують доступ до об'єктів у суворій відповідності з установленими правилами.

**7. Авторизований суб'єкт доступу** – суб'єкт, якому надані відповідні права доступу до об'єктів системи (повноваження).

**8. Несанкціонований доступ (НСД) –** доступ суб'єкта до об'єкта в порушення встановлених у системі правил розмежування доступу.

**9. Несанкціонована дія** – дія суб'єкта в порушення встановлених у системі правил обробки інформації.

Для реалізації наведених вище мір захисту комп'ютерних систем використовуються **універсальні механізми захисту інформації**. До числа таких механізмів відносяться:

- ідентифікація (найменування і впізнання), автентифікація (підтвердження істинності) і авторизація (присвоєння повноважень) суб'єктів;
- контроль (розмежування) доступу до ресурсів системи;
- реєстрація й аналіз подій, що відбуваються в системі;
- контроль цілісності ресурсів системи.

Механізми ідентифікації, автентифікації й авторизації необхідні для підтвердження істинності суб'єкта, забезпечення його роботи в системі, і визначення законності прав суб'єкта на даний об'єкт або на визначені дії з ним.

**Ідентифікація** – це процес розпізнавання елемента системи, зазвичай за допомогою заздалегідь визначеного ідентифікатора або іншої унікальної інформації; кожний суб'єкт або об'єкт системи повинний бути однозначно ідентифікуємим.

**Автентифікація** – це перевірка істинності ідентифікації користувача, процесу, пристрою або іншого компоненту системи (звичайно здійснюється перед дозволом доступу); а також перевірка цілісності й авторства даних при їхньому збереженні або передачі для запобігання несанкціонованої модифікації.

**Авторизація** – це надання суб'єкту прав на доступ до об'єкта.

Приведемо приклад з доступом в онлайн-банкінг. Кожну дію користувача й системи розглянемо докладно.

Перебуваючи на сайті банку, користувач вирішує зайти в особистий кабінет, щоб зробити грошовий переказ. На сторінці особистого кабінету система спочатку просить ввести ідентифікатор. Це може бути логін, ім'я й прізвище, адреса електронної пошти або номер мобільного телефону.

*Який конкретно вид даних необхідно ввести – залежить від ресурсу. Дані, які вказувалися при реєстрації, необхідно ввести для одержання доступу. Якщо при реєстрації вказувалося кілька типів даних – і логін, і адреса електронної пошти, і номер мобільного, то система сама підкаже що їй конкретно потрібно.*

Введення цих даних необхідний для ідентифікації людини за монітором як користувача конкретно цього банку.

Якщо користувач як ідентифікатор увів «Олександр Ковальчук», і система знайшла у своїй базі запис про користувача з таким іменем, то ідентифікація завершилася.

Після ідентифікації випливає процес автентифікації, у якому користувачеві потрібно довести, що він є людиною, яка реєструвалася під іменем Олександр Ковальчук.

Для доказу необхідна наявність одного з типів автентифікаційних даних:

- Щось, властиве тільки користувачеві. Біометричні дані: сканери особи, відбитки пальців або сітківки ока.
- Щось, відоме тільки користувачеві. Сюди ставляться pin-коди, паролі, графічні ключі, секретні слова.
- Щось, наявне в користувача. У даній якості може виступати токен, тобто компактний пристрій, призначене для забезпечення інформаційної безпеки користувача, також використовується для ідентифікації власника. Найпростіші токени не вимагають фізичного підключення до комп'ютера – у них є дисплей, де відображається число, яке користувач уводить у систему для здійснення входу; більш складні підключаються до комп'ютерів за допомогою USB і Bluetooth-Інтерфейсів.

Найпоширеніший тип автентифікаційних даних – це пароль. Саме тому так важливо створювати й правильно зберігати свої паролі.

Після введення користувачем пароля система перевіряє: чи відповідає умовний пароль «Q45fp02@13» користувачеві з іменем Олександр Ковальчук. У такий спосіб відбувається автентифікація.

Якщо всі вірно, і пари логін-пароль вірні, то система надасть користувачеві доступ до його ресурсів і здійснення банківських операцій, тобто відбудеться авторизація.

Описані процеси завжди відбуваються тільки в такому порядку: ідентифікація, автентифікація, авторизація. Увесь ланцюжок втратить зміст, якщо, наприклад, сайт спочатку надасть доступ до коштів користувача, а потім буде уточнювати, чи він це насправді.

Процеси ідентифікації, автентифікації й авторизації характерні не тільки для онлайн-банкінгу, але й для електронної пошти, соціальних мереж і інших ресурсів.