

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
Кафедра кібербезпеки та математичного моделювання

СТАНДАРТИЗАЦІЯ, СЕРТИФІКАЦІЯ ЗАСОБІВ ТА КОМПЛЕКСІВ ЗАХИСТУ ІНФОРМАЦІЇ

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт
для здобувачів
другого (магістерського) рівня вищої освіти
освітньо-професійної програми «Кібербезпека»
спеціальності 125 Кібербезпека та захист інформації

Обговорено і рекомендовано
на засіданні кафедри
кібербезпеки та математичного
моделювання
Протокол №2
від 13 лютого 2024 р.

Чернігів 2024

Стандартизація, сертифікація засобів та комплексів захисту інформації. Методичні вказівки до виконання лабораторних робіт для здобувачів другого (магістерського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. – Чернігів: НУ «Чернігівська політехніка», 2024 – 94 с.

Укладачі: ХОРОШКО ВОЛОДИМИР ОЛЕКСІЙОВИЧ, професор кафедри безпеки інформаційних технологій Національного авіаційного університету, доктор технічних наук, професор
ТКАЧ ЮЛІЯ МИКОЛАЇВНА, завідувач кафедри кібербезпеки та математичного моделювання, доктор педагогічних наук, професор.
ШЕЛЕСТ МИХАЙЛО ЄВГЕНОВИЧ, професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук, професор;

Відповідальний за випуск – ТКАЧ ЮЛІЯ МИКОЛАЇВНА,
завідувач кафедри кібербезпеки та
математичного моделювання,
доктор педагогічних наук, професор

Рецензент – МЕХЕД ДМИТРО БОРИСОВИЧ,
доцент кафедри кібербезпеки та математичного моделювання,
кандидат педагогічних наук, доцент

ЗМІСТ

Перелік прийнятих скорочень.....	4
Вступ	5
Розділ 1.....	8
1.1 Структура законодавства України	8
1.2 Законодавча база України.....	13
Закон України «Про інформацію».....	13
Закон України «Про державну таємницю»	20
Закон України «Про стандартизацію»	43
1.3 Державні та міжнародні стандарти, які діють в Україні.....	67
1.4. Нормативна база України у сфері захисту інформації.....	73
1.5. Сертифікація у сфері засобів та комплексів захисту інформації....	74
Розділ 2.....	81
Розділ 3.....	83
Лабораторна робота №1.....	83
Лабораторна робота №2.....	84
Лабораторна робота №3.....	85
Лабораторна робота №4.....	86
Лабораторна робота №5.....	87
Лабораторна робота №6.....	88
Лабораторна робота №7.....	89
Лабораторна робота №8.....	90
Лабораторна робота №9.....	91
Лабораторна робота №10.....	92
Лабораторна робота №11.....	93
Перелік використаних джерел.....	94

Перелік прийнятих скорочень

АС – автоматизована система.

ЕОТ – електронно-обчислювальна техніка.

ЗІ – захист інформації.

ЗМІ – засоби масової інформації.

ІАР – інформаційно-аналітична робота.

ІБ – інформаційна безпека.

ІзОД – інформація з обмеженим доступом.

ІС – інформаційна система.

ІТС – інформаційно-телекомунікаційна система.

КСЗІ – комплексна система захисту інформації.

ОС – операційна система.

ОТ – обчислювальна техніка.

ПЗ – програмне забезпечення.

ПК – персональний комп'ютер.

РСО – режимно-секретні органи.

СЗ – система захисту.

СЗІ – система захисту інформації.

ТЗІ – технічний захист інформації.

ТСЗІ – технічний система захисту інформації.

ICT – Information and Communication Technologies (інформаційно-комунікаційні технології).

ISO/IEC – International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

IDS – Intrusion Detection System (система виявлення вторгнень).

ITSM – IT Service Management (менеджмент послуг в IT).

Вступ

За умов розбудови інформаційного простору України та входження до світового інформаційного простору надзвичайної гостроти та актуальності набувають питання забезпечення інформаційної безпеки держави.

Важливу роль інформаційної безпеки відведено з розумінням того, що:

- інформаційна безпека є не тільки однією із головних складових національної безпеки України, а й не від'ємною компонентною усіх інших її складових;
- Інформаційні стратегії в сучасних умовах набувають важливого, а іноді й вирішального значення у випадку реалізації рівня стратегій співробітництва або відіграють своєрідної інформаційної зброї;
- Руйнування та дезорганізації інформаційної інфраструктури держави прирівнюються за наслідками до застосування зброї масового знищення.

Для підвищення ефективності захисту інформації необхідно розробити певний системний підхід до цієї проблеми, який полягає у проведенні ряду заходів за такими напрямками: 1) Розробка нормативно-правових документів, що визначають етапи проведення, критерії оцінки та ефективності заходів щодо охорони інформації; 2) Визначення порядку проведення робіт і надання послуг у галузі інформаційної безпеки; 3) Створення вітчизняної інфраструктури, розробки, виробництва, впровадження та експлуатації засобів охорони інформації; 4) Підготовка та перепідготовка національних кадрів для роботи у сфері охорони інформації.

У рамках діяльності в галузі ТЗІ розроблені правові та нормативні документи щодо відносин у галузі у сфері охорони інформації.

Розроблені нормативно-правові акти вже передбачають та реалізують заходи у галузі технічного захисту інформації повністю відповідають таким основним напрямкам Державної політики, які відповідають Законам України.

Однією з найважливіших складових частин правового забезпечення системи інформаційної безпеки є стандартизація та сертифікація технічних засобів захисту та контролю їх ефективності у сфері технічного захисту інформації.

Впорядкування та розвиток існуючих, а також створення нової законодавчої бази в галузі інформаційних відносин потребує системного підходу.

На сам перед, необхідно вирішити:

- Правове вирішення інформації, як стратегічно важливого для держави ресурсу;

- Визначення взаємозв'язаної системи інформаційних масивів держави різного рівня та призначення, а також державних органів, відповідальних за формування, збереження, використання та захист цих масивів;

- Визначення прав, обов'язків, гарантій забезпечення прав і відповідальності суб'єктів інформаційних відносин у різних прикладних галузях; Стандартизація та сертифікація окремих видів інформаційної діяльності та продукції;

- Чіткого законодавчого визначення виду, типу, обсягу інформації з обмеженим доступом, визначення процедур до такої інформації та зняття обмежень, визначення прав, обов'язків і відповідальності суб'єктів інформаційних відносин у питаннях категорювання такої інформації, її використання;

- Створення загальної системи забезпечення інформаційної безпеки та охорони інформації.

- Однією з найважливіших складових частин правового забезпечення системи захисту інформації є стандартизація та сертифікація, які повинні відповідати основним принципам і положенням міжнародних, міждержавних, регіональних та національних системам інших держав, не вступаючи в протиріччя з інтересами України, і враховуючи такі завдання;

- Створення пакета основоположних стандартів організаційно-методичних та термінологічного забезпечення системи технічного захисту інформації у всіх сферах діяльності держави;

- Стандартизацію та сертифікацію вимог із захисту інформації про озброєння, військову техніку та військово-промислові об'єкти;

- Стандартизацію та сертифікацію та ліцензування вимог із захисту інформації в автоматизованих системах і мережах, у засобах обчислювальної техніки та орг техніки;

- Нормативне та метрологічне забезпечення стандартизації та сертифікації та ліцензування технічних засобів інформації та контролю їх ефективності.

Для гарантованого досягнення мети при вирішенні завдань інформаційно безпеки в країні повинно створюватись система стандартизації та сертифікації засобів захисту інформації, яка керується центрами, в компетенцію яких входили б окремі напрямки інформаційної безпеки. Такі центри повинні бути оснащені сучасними технічними засобами та нормативною документацією. Очевидно, що дослідження при виборі перспективних шляхів розвитку матеріально-технічного забезпечення системи інформаційної безпеки, створення стандартів, які покладенні в основу розробки унікальних засобів захисту інформації під час створення систем захисту, а також створення захищених

інформаційних технологій призначених для впровадження у інформаційно аналітичні системи держави.

Метою курсу є ознайомлення існуючої бази у сфері інформаційних відносин, завдання та повноваження органів влади, які реалізують державну політику інформаційної безпеки відносно стандартизації та сертифікації об'єктів та систем захисту інформації, які відіграють важливу роль у загальній структурі системи державної безпеки. Проблеми захисту власних інформаційних ресурсів і контрольованості свого інформаційного простору особливо загострилось на сьогоднішньому етапі функціонування нашої держави, що пов'язано з агресією Росії.

Розділ 1 Загальні теоретичні вказівки

1.1 Структура законодавства України

Право – це сукупність загальнообов’язкових правил і норм поведінки, які встановлені або санкціоновані державою по відношенню до певних сфер життя та діяльності державних органів, підприємств (організацій) та населення.

Правовий захист інформації – це спеціальні правові акти, правила, процедури та заходи, які забезпечують захист інформації на правовій основі.

Правовий захист інформації як ресурс признаний на міждержавному, державному рівні та визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом та ліцензіями на їхній захист. На державному рівні правовий захист регулюється державними та відомчими актами (рис. 1).



Рис. 1 Система нормативно-правових документів в Україні, що регламентують питання захисту інформації

В Україні такими правовими (актами, нормами) є:

- Конституція;
- закони України;
- адміністративне, кримінальне право, викладені у відповідних кодексах.

Відомчі нормативні акти визначаються:

- наказами;
- розпорядженнями;

- положеннями;
- інструкціями, що видаються відомствами, організаціями і підприємствами, діючими у рамках певних структур.

Сучасні умови вимагають і визначають необхідність комплексного підходу до формування законодавства із захисту інформації, його складу і змісту, співвідношення його з усією системою законів і правових актів України.



Рис. 2 Структура законодавства України в області захисту інформації

Вимоги інформаційної безпеки повинні органічно включатися в усі рівні законодавства, у тому числі і в (рис. 2):

- *конституційне законодавство* – норми, що стосуються питань інформатизації та захисту інформації, які входять до конституційного законодавства як складові елементи;
- *основні загальні закони та кодекси* – норми з питань інформатизації та захисту інформації;
- *закони з організації державної системи управління* – закони стосовно окремих структур господарства, економіки, системи державних органів та визначення їх статусу, які включають окремі норми з питань захисту інформації;

- *спеціальні закони* – сукупність законів, які закладають основи правового забезпечення інформаційної безпеки;

- *підзаконні нормативні акти* – стандарти, загальнодержавні та відомчі нормативні документи, що орієнтовані на забезпечення захисту інформації.

Спираючись на державні правові акти і враховуючи відомчі інтереси на рівні конкретної організації, розробляються власні нормативно-правові документи, орієнтовані на забезпечення інформаційної безпеки. До таких документів відносяться:

- положення про збереження конфіденційної інформації;

- перелік відомостей, що становлять конфіденційну інформацію;

- інструкція про порядок допуску співробітників до відомостей, що становлять конфіденційну інформацію;

- положення про спеціальне діловодство і документообіг;

- перелік відомостей, дозволених до публікації в пресі;

- положення про роботу з іноземними фірмами та їх представниками;

- зобов'язання співробітника про збереження конфіденційної інформації;

- пам'ятка співробітникові про збереження комерційної таємниці та ін.

Конфіденційна інформація – інформація з обмеженим доступом, яка містить відомості, що перебувають у володінні, користуванні або розпорядженні фізичних чи юридичних осіб або держави, та порядок доступу до якої обмежується ними. Вона може бути:

- *особиста* – відомості про факти, події і обставини приватного життя громадян, які дозволяють ідентифікувати його особу (персональні дані), за винятком відомостей, що підлягають поширенню в ЗМІ у встановленому Законом порядку;

- *судово-слідча* – відомості, які складають таємницю слідства і судочинства;

- *службова* – службові відомості, доступ до яких обмежений органами державної влади (службова таємниця);

- *професійна таємниця* – відомості, пов'язані з професійною діяльністю, доступ до яких обмежений Законами (лікарська, нотаріальна, адвокатська таємниця, таємниця листування, телефонних переговорів та ін.);

- *комерційна, банківська* – відомості, пов'язані з комерційною (банківською) діяльністю, доступ до яких обмежений Законом (комерційна, банківська таємниця);

- *виробнича* – відомості про суть винаходу, моделі або промислового зразка до офіційної публікації інформації про них.

Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Таблиця 1 Основні параметри комерційної таємниці

Визначення	Зміст
СУБ'ЄКТ	Підприємства, організації, колективи, громадяни
ОБ'ЄКТ	Поняття застосоване до широкого спектру інтелектуальної і промислової власності
ХАРАКТЕРИСТИКИ	Активний ресурс Конфіденційна інформація Особлива форма власності Товар ринкової новизни
ЦІННІСТЬ	Реально (потенційно) створює переваги в конкурентній боротьбі
ВИМОГИ	Потенційно корисна Не загальновідома
ТЕРМІН ДІЇ	Визначається життєвим циклом товару
ЗАХИСТ	Правовий Організаційний Інженерно-технічний

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці (*ст. 505 Цивільного кодексу України*).

Створюючи систему інформаційної безпеки, необхідно чітко розуміти, що без правового забезпечення захисту інформації будь-які подальші претензії до недобросовісного співробітника, клієнта, конкурента і посадовця виявляться просто безпідставними.

Якщо перелік відомостей конфіденційного характеру не доведений своєчасно до кожного співробітника (природно, якщо він допущений по посадових обов'язках) письмово, то співробітник, що вкрав важливу інформацію, порушуючи встановлений порядок роботи з нею, швидше за все розведе руками: звідки мені це знати!

В цьому випадку ніякі інстанції, аж до судових, не зможуть допомогти.

Правові норми забезпечення безпеки і захисту інформації на конкретному підприємстві відбиваються в сукупності засновницьких, організаційних і функціональних документів.

Правові вимоги забезпечення безпеки і захисту інформації відбиваються в **Статуті** у вигляді наступних положень:

- підприємство має право визначати склад, об'єм і порядок захисту відомостей конфіденційного характеру, вимагати від своїх співробітників забезпечення їх збереження і захисту від внутрішніх і зовнішніх загроз;

- підприємство зобов'язане забезпечити збереження конфіденційної інформації.

Це дозволяє адміністрації підприємства:

- створювати організаційні структури із захисту конфіденційної інформації;
- видавати нормативні та розпорядливі документи, які визначають порядок виділення відомостей конфіденційного характеру і механізми їх захисту;

- включати вимоги із захисту інформації в угоди з усіх видів господарської діяльності;

- вимагати захисту інтересів підприємства з боку державних і судових інстанцій;

- розпоряджатися інформацією, що являється власністю підприємства, в цілях отримання вигоди і недопущення економічного збитку колективу підприємства і власникові засобів виробництва;

- розробити «Перелік відомостей конфіденційної інформації».

Таким чином, правове регулювання потрібне для:

- вдосконалення механізму попередження протиправних дій по відношенню до інформаційних ресурсів;

- уточнення і закріплення завдань і правомірності окремих суб'єктів у сфері попереджувальної діяльності;

- охорони прав і законних інтересів громадян і організацій.

1.2 Законодавча база України

Закони України являють собою важливу ступень в організації правового забезпечення інформаційної безпеки держави. Цими документами є закони України про інформацію та про державну таємницю.

Закон України «Про інформацію»

Цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

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 напрямками 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.

{Частина друга статті 6 із змінами, внесеними згідно із Законом [№ 720-IX від 17.06.2020](#)}

Стаття 7. Охорона права на інформацію

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

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

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

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

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

Стаття 8. Мова інформації

1. Мову інформації визначають [Закон України](#) "Про забезпечення функціонування української мови як державної", інші закони України та міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

{Стаття 8 в редакції Закону [№ 2704-VIII від 25.04.2019](#)}

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;
інші види інформації.

Стаття 17. Правова інформація

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

2. Джерелами правової інформації є [Конституція України](#), інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

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

Стаття 18. Статистична інформація

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

2. Офіційна державна статистична інформація підлягає систематичному оприлюдненню.

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

4. Правовий режим державної статистичної інформації визначається [Законом України](#) "Про державну статистику", іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

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.

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

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

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

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

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

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

{Пункт 4 частини четвертої статті 21 в редакції Закону [№ 317-VIII від 09.04.2015](#)}

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

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

{Частину четверту статті 21 доповнено пунктом 5-1 згідно із Законом [№ 1405-VIII від 02.06.2016](#)}

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

Розділ III

ДІЯЛЬНІСТЬ ЖУРНАЛІСТІВ, ЗАСОБІВ МАСОВОЇ ІНФОРМАЦІЇ, ЇХ ПРАЦІВНИКІВ

Стаття 22. Масова інформація та її засоби

1. Масова інформація - інформація, що поширюється з метою її доведення до необмеженого кола осіб.

2. Засоби масової інформації - засоби, призначені для публічного поширення друкованої або аудіовізуальної інформації.

Стаття 26. Акредитація журналістів, працівників засобів масової інформації

1. З метою створення сприятливих умов для здійснення журналістами, працівниками засобів масової інформації професійної діяльності суб'єкт владних повноважень може здійснювати їх акредитацію.

Усі дії, пов'язані з акредитацією, мають ґрунтуватися на принципах відкритості, рівності, справедливості з метою забезпечення права громадськості на одержання інформації через засоби масової інформації. Відсутність акредитації не може бути підставою для відмови в допуску журналіста, працівника засобу масової інформації на відкриті заходи, що проводить суб'єкт владних повноважень.

2. Акредитація журналіста, працівника засобу масової інформації здійснюється безоплатно на підставі його заяви або подання засобу масової інформації.

У заяві, поданій журналістом, працівником засобу масової інформації, зазначаються його прізвище, ім'я та по батькові, адреса, номер засобу зв'язку, адреса електронної пошти (за наявності). До заяви додаються копії документів, що посвідчують особу та засвідчують її професійну належність.

У поданні засобу масової інформації зазначаються його повне найменування, дата і номер реєстрації, адреса, адреса електронної пошти (за наявності), номер засобу зв'язку, прізвище, ім'я та по батькові журналіста, працівника засобу масової інформації, щодо якого вноситься подання. До подання додаються копії документів, що посвідчують особу.

В акредитації не може бути відмовлено в разі подання усіх документів, передбачених цією частиною.

Суб'єкт владних повноважень може встановлювати спрощений порядок акредитації.

3. Порядок акредитації, визначений суб'єктом владних повноважень, підлягає оприлюдненню.

4. Суб'єкти владних повноважень, що здійснили акредитацію журналістів, працівників засобів масової інформації, зобов'язані сприяти провадженню ними професійної діяльності; завчасно сповіщати їх про місце і час проведення сесій, засідань, нарад, брифінгів та інших публічних заходів; надавати їм інформацію, призначену для засобів масової інформації; а також сприяти створенню умов для здійснення запису і передачі інформації, проведення інтерв'ю, отримання коментарів посадових осіб.

5. У разі якщо захід проводиться відповідно до міжнародних або інших спеціальних протоколів, можуть встановлюватися особливі умови допуску журналістів. Такі особливі умови оприлюднюються на офіційному веб-сайті відповідного суб'єкта владних повноважень до проведення заходу.

6. Журналіст, працівник засобу масової інформації зобов'язаний дотримуватися встановлених суб'єктом владних повноважень правил внутрішнього трудового розпорядку, не перешкоджати діяльності його службових та посадових осіб.

7. Суб'єкти владних повноважень, що акредитували журналіста, працівника засобу масової інформації, приймають рішення про припинення акредитації у разі:

подання ним відповідної заяви;

неодноразового грубого порушення ним обов'язків, визначених цією статтею;

звернення засобу масової інформації, за поданням якого здійснена акредитація.

8. У рішенні про припинення акредитації зазначаються посадова особа чи службова особа (суб'єкт владних повноважень), яка прийняла відповідне рішення, дата прийняття рішення, підстава для прийняття рішення та порядок його оскарження. Письмове повідомлення про припинення акредитації видається або надсилається засобу масової інформації або журналістові, працівникові засобу масової інформації протягом п'яти робочих днів з дня прийняття відповідного рішення.

9. Рішення про припинення акредитації може бути оскаржено до суду в установленому порядку.

Розділ IV

ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ІНФОРМАЦІЮ

Стаття 28. Неприпустимість зловживання правом на інформацію

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

Стаття 30. Звільнення від відповідальності

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

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

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

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

4. Додаткові підстави звільнення від відповідальності засобів масової інформації та журналістів встановлюються законами України ["Про друковані засоби масової інформації \(пресу\) в Україні"](#), ["Про телебачення і радіомовлення"](#), ["Про інформаційні агентства"](#) та іншими.

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.

Розділ I

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 державною;

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 обґрунтування 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 2. Законодавство України про державну таємницю

Відносини у сфері охорони державної таємниці регулюються [Конституцією України](#), законами України "[Про інформацію](#)" та "[Про доступ до публічної інформації](#)", цим Законом, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України та іншими нормативно-правовими актами.

{Стаття 2 із змінами, внесеними згідно із Законом [№ 1170-VII від 27.03.2014](#)}

Стаття 3. Сфера дії Закону

Дія цього Закону поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші державні органи, в тому числі територіальні органи центрального органу виконавчої влади, що реалізує державну митну політику, та центрального органу виконавчої влади, що реалізує державну податкову політику, утворені як відокремлені підрозділи центрального органу виконавчої влади без статусу юридичної особи, Верховну Раду Автономної Республіки Крим, Раду міністрів Автономної Республіки Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі - державні органи, органи місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці.

{Частина перша статті 3 із змінами, внесеними згідно із Законом [№ 440-IX від 14.01.2020](#)}

Передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим Законом. У разі, якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші, ніж передбачені цим Законом, правила охорони таємниці іноземної держави чи міжнародної організації, то застосовуються правила міжнародного договору України.

Стаття 4. Державна політика щодо державної таємниці

Державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики визначає Верховна Рада України.

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, встановлених в інтересах національної безпеки України відповідно до цього Закону.

Якщо внаслідок обмеження прав на секретну інформацію або її матеріальні носії заподіюється шкода особі, якій належать такі права, відшкодування здійснюється за рахунок держави в порядку та розмірах, що визначаються в договорі між такою особою і державним органом (органами), якому (яким) державним експертом з питань таємниць надається право приймати рішення щодо суб'єктів, які мають доступ до цієї інформації та її матеріальних носіїв. Зазначеним договором також визначаються порядок та умови охорони державної таємниці, зокрема режим секретності під час користування і розпорядження секретною інформацією та її матеріальними носіями, обумовлюється згода особи на реалізацію прав щодо інформації або її матеріальних носіїв з урахуванням обмежень, встановлених відповідно до цього Закону, взяття особою на себе зобов'язання щодо збереження державної таємниці та ознайомлення її з мірою відповідальності за порушення законодавства про державну таємницю.

Якщо особа, якій належать права на секретну інформацію або її матеріальні носії, відмовляється від укладення договору чи порушує його, за рішенням суду ця інформація або її матеріальні носії можуть бути вилучені за умови попереднього і повного відшкодування їх вартості особі, якій належали відповідні права.

{Стаття 6 в редакції Закону [№ 1170-VII від 27.03.2014](#)}

Розділ II

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;

{Абзац третій пункту 1 частини першої статті 8 виключено на підставі Закону [№ 808-IX від 17.07.2020](#)}

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;

{Абзац четвертий пункту 1 частини першої статті 8 в редакції Закону [№ 2432-VI від 06.07.2010](#)}

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

про застосування систем озброєння, підготовку та проведення військових операцій;

{Пункт 1 частини першої статті 8 доповнено абзацом шостим згідно із Законом [№ 808-IX від 17.07.2020](#)}

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

{Пункт 1 частини першої статті 8 доповнено абзацом сьомим згідно із Законом [№ 808-IX від 17.07.2020](#)}

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

{Пункт 1 частини першої статті 8 доповнено абзацом восьмим згідно із Законом [№ 808-IX від 17.07.2020](#)}

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

{Пункт 1 частини першої статті 8 доповнено абзацом дев'ятим згідно із Законом [№ 808-IX від 17.07.2020](#)}

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;

{Абзац другий пункту 2 частини першої статті 8 в редакції Закону [№ 2432-VI від 06.07.2010](#)}

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

{Абзац четвертий пункту 2 частини першої статті 8 виключено на підставі Закону [№ 808-IX від 17.07.2020](#)}

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;

{Абзац сьомий пункту 2 частини першої статті 8 із змінами, внесеними згідно із Законом [№ 808-IX від 17.07.2020](#)}

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

{Пункт 2 частини першої статті 8 доповнено абзацом восьмим згідно із Законом [№ 808-IX від 17.07.2020](#)}

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;

{Пункт 2 частини першої статті 8 доповнено абзацом дев'ятим згідно із Законом [№ 808-IX від 17.07.2020](#)}

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).

{Пункт 2 частини першої статті 8 доповнено абзацом десятим згідно із Законом [№ 808-IX від 17.07.2020](#)}

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

{Пункт 2 частини першої статті 8 доповнено абзацом одинадцятим згідно із Законом [№ 808-IX від 17.07.2020](#)}

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;

{Пункт 3 частини першої статті 8 доповнено абзацом п'ятим згідно із Законом [№ 808-IX від 17.07.2020](#)}

4) у сфері державної безпеки та охорони правопорядку:

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

{Абзац другий пункту 4 частини першої статті 8 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

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;

{Абзац третій пункту 4 частини першої статті 8 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

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;

{Абзац одинадцятий пункту 4 частини першої статті 8 із змінами, внесеними згідно із Законом [№ 4652-VI від 13.04.2012](#)}

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".

{Частина друга статті 8 із змінами, внесеними згідно із Законом [№ 1170-VII від 27.03.2014](#)}

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;

{Абзац другий частини четвертої статті 8 із змінами, внесеними згідно із Законом [№ 1170-VII від 27.03.2014](#)}

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;

{Абзац шостий частини четвертої статті 8 в редакції Закону [№ 1170-VII від 27.03.2014](#)}

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

{Абзац сьомий частини четвертої статті 8 в редакції Закону [№ 1170-VII від 27.03.2014](#)}

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.

{Статтю 10 доповнено частиною четвертою згідно із Законом [№ 808-IX від 17.07.2020](#)}

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.

{Статтю 10 доповнено частиною п'ятою згідно із Законом [№ 808-IX від 17.07.2020](#)}

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.

{Частина перша статті 12 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

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.

{Частина друга статті 12 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Зразки форм рішень державних експертів з питань таємниць, порядок та механізм формування Зводу відомостей, що становлять державну таємницю, і його опублікування визначаються Кабінетом Міністрів України.

{Частина третій статті 12 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

На підставі та в межах [Зводу відомостей, що становлять державну таємницю](#), з метою конкретизації та систематизації даних про секретну інформацію державні органи створюють галузеві або відомчі розгорнуті переліки відомостей, що становлять державну таємницю, а також можуть створювати міжгалузеві або міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю. Підприємства, установи та організації незалежно від форм власності, що провадять діяльність, пов'язану із державною таємницею, за ініціативою та погодженням із замовником робіт, пов'язаних з державною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю. Такі переліки погоджуються із Службою безпеки України, затверджуються державними експертами з питань таємниць та реєструються у Службі безпеки України.

Розгорнуті переліки відомостей, що становлять державну таємницю, не можуть суперечити [Зводу відомостей, що становлять державну таємницю](#).

У разі включення до [Зводу відомостей, що становлять державну таємницю](#), або до розгорнутих переліків цих відомостей інформації, яка не відповідає категоріям і вимогам, передбаченим [статтею 8](#) цього Закону, або порушення встановленого порядку віднесення інформації до державної таємниці заінтересовані громадяни та юридичні особи мають право оскаржити відповідні рішення до суду. З метою недопущення розголошення державної таємниці судовий розгляд скарг може проводитися в закритих засіданнях відповідно до закону.

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.

{Частина друга статті 13 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Президент України з власної ініціативи або на підставі пропозицій державних експертів з питань таємниць чи за зверненням державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян може встановлювати більш тривалі строки дії рішень про віднесення інформації до державної таємниці, ніж строки, передбачені частиною першою цієї статті.

Установлення строку дії рішення про віднесення інформації до державної таємниці, прийняття рішення про його продовження здійснюються з дотриманням вимог [статті 6](#) Закону України "Про доступ до публічної інформації".

{Статтю 13 доповнено частиною четвертою згідно із Законом [№ 1170-VII від 27.03.2014](#)}

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](#).

{Частина перша статті 14 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Інформація вважається державною таємницею з більш високим чи нижчим ступенем секретності або такою, що не становить державної таємниці, з часу опублікування відповідних змін до [Зводу відомостей, що становлять державну таємницю](#).

Розділ III

ЗАСЕКРЕЧУВАННЯ ТА РОЗСЕКРЕЧУВАННЯ МАТЕРІАЛЬНИХ НОСІВ 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.

{Частина перша статті 15 в редакції Закону [№ 2432-VI від 06.07.2010](#); із змінами, внесеними згідно із Законом [№ 1170-VII від 27.03.2014](#)}

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.

{Частина друга статті 15 в редакції Закону [№ 2432-VI від 06.07.2010](#)}

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

Забороняється надавати грифи секретності, передбачені цим Законом, матеріальним носіям іншої таємної інформації, яка не становить державної таємниці, або конфіденційної інформації.

Перелік посад, перебування на яких дає посадовим особам право надавати матеріальним носіям секретної інформації грифи секретності, затверджується керівником державного органу, органу місцевого самоврядування, підприємства, установи, організації, що провадить діяльність, пов'язану з державною таємницею.

{Частина п'ята статті 15 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Ступені секретності науково-дослідних, дослідно-конструкторських і проектних робіт та інших секретних товарів, робіт і послуг, щодо яких здійснюється закупівля та які виконуються в інтересах забезпечення національної безпеки та оборони держави, встановлюються шляхом винесення відповідного висновку державним експертом з питань таємниць, який виконує свої функції у сфері діяльності замовника, разом з підрядником.

{Частина шоста статті 15 із змінами, внесеними згідно із Законами [№ 2432-VI від 06.07.2010](#), [№ 808-IX від 17.07.2020](#)}

Після закінчення встановлених строків засекречування матеріальних носіїв інформації та у разі підвищення чи зниження визначеного державним експертом з питань таємниць ступеня секретності такої інформації або скасування рішення про віднесення її до державної таємниці керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, у яких здійснювалося засекречування матеріальних носіїв інформації, або керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, які є їх правонаступниками, чи керівники вищого рівня зобов'язані протягом шести місяців забезпечити зміну грифа секретності або розсекречування цих матеріальних носіїв секретної інформації та письмово повідомити про це керівників державних органів, органів місцевого самоврядування, підприємств, установ, організацій, яким були передані такі матеріальні носії секретної інформації.

Стаття 16. Строк засекречування матеріальних носіїв інформації

Строк засекречування матеріальних носіїв інформації має відповідати строку дії рішення про віднесення інформації до державної таємниці, встановленого рішенням державного експерта з питань таємниць.

Перебіг строку засекречування матеріальних носіїв інформації починається з часу надання їм грифа секретності.

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 19. Єдині вимоги до матеріальних носіїв секретної інформації

Єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передачі та транспортування матеріальних носіїв секретної інформації встановлюються Кабінетом Міністрів України.

Стаття 20. Дозвільний порядок провадження діяльності, пов'язаної з державною таємницею, та режим секретності

Державні органи, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов'язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею.

Надання дозволу здійснюється на підставі заявок державних органів, органів місцевого самоврядування, підприємств, установ і організацій та результатів спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею. З метою визначення наявності умов для провадження діяльності, пов'язаної з державною таємницею, Служба безпеки України може створювати спеціальні експертні комісії, до складу яких включати фахівців державних органів, органів місцевого самоврядування, підприємств, установ і організацій за погодженням з їх керівниками. Результати спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, оформляються відповідним актом.

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, надається державним органам, органам місцевого самоврядування, підприємствам, установам, організаціям за результатами спеціальної експертизи за умови, що вони:

відповідно до компетенції, державних завдань, програм, замовлень, договорів (контрактів) беруть участь у діяльності, пов'язаній з державною таємницею;

мають приміщення для проведення робіт, пов'язаних з державною таємницею, сховища для зберігання засекречених документів та інших матеріальних носіїв секретної інформації, що відповідають вимогам щодо забезпечення секретності зазначених робіт, виключають можливість доступу до них сторонніх осіб, гарантують збереження носіїв секретної інформації;

додержуються передбачених законодавством вимог режиму секретності робіт та інших заходів, пов'язаних з використанням секретної інформації, порядку допуску осіб до державної таємниці, прийому іноземних громадян, а також порядку здійснення технічного та криптографічного захисту секретної інформації;

{Абзац четвертий частини третьої статті 20 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

мають режимно-секретний орган, якщо інше не передбачено цим Законом.

Керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, що провадять діяльність, пов'язану з державною таємницею, мають бути обізнані з чинним законодавством про державну таємницю.

Термін дії дозволу на провадження діяльності, пов'язаної з державною таємницею, встановлюється Службою безпеки України і не може перевищувати 5 років. Його тривалість залежить від обсягу робіт (діяльності), що здійснюються державним органом, органом місцевого самоврядування, підприємством, установою, організацією, ступеня секретності та обсягу пов'язаних з цими роботами (діяльністю) відомостей, що становлять державну таємницю, а також категорії режиму секретності.

{Частина п'ята статті 20 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, не надається, якщо відсутні умови для провадження такої діяльності, передбачені цією статтею, а також якщо керівник підприємства, установи, організації не є громадянином України або не має допуску до державної таємниці.

{Статтю 20 доповнено новою частиною згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, може бути скасований або його дія може бути зупинена Службою безпеки України на підставі акта проведеної нею перевірки, висновки якого містять дані про недодержання державним органом, органом місцевого самоврядування, підприємством, установою, організацією умов, передбачених цією статтею.

{Частина сьома статті 20 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Державним органам, органам місцевого самоврядування, підприємствам, установам, організаціям, що провадять діяльність, пов'язану з державною таємницею, за результатами

спеціальної експертизи надаються відповідні категорії режиму секретності (перша, друга або третя), що зазначаються Службою безпеки України у дозволах на провадження діяльності, пов'язаної з державною таємницею.

{Частина восьма статті 20 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Державні органи, органи місцевого самоврядування, підприємства, установи і організації, яким надано зазначений у цій статті дозвіл, набувають права на доступ до конкретної секретної інформації згідно з рішенням державних органів, уповноважених державним експертом з питань таємниць приймати такі рішення. За погодженням з цими органами здійснюється передача секретної інформації або її матеріальних носіїв державним органам, органам місцевого самоврядування, підприємствам, установам і організаціям, які мають дозвіл на провадження діяльності, пов'язаної з державною таємницею.

Порядок надання, переоформлення, зупинення та поновлення дії або скасування дозволу на провадження діяльності, пов'язаної з державною таємницею, форма акта спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, форма дозволу на провадження діяльності, пов'язаної з державною таємницею, та категорії режиму секретності встановлюються Кабінетом Міністрів України.

{Частина десята статті 20 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

У разі виникнення кризової ситуації, що загрожує національній безпеці України, оголошення рішення про проведення мобілізації та (або) введення правового режиму воєнного стану надання спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею, органам військового управління, військовим частинам, установам і організаціям Збройних Сил України, інших військових формувань, правоохоронних органів спеціального призначення, Державної спеціальної служби транспорту, Державної служби спеціального зв'язку та захисту інформації України, що відмобілізуються, доукомплектовуються, заново формуються, здійснюється у десятиденний термін.

{Статтю 20 доповнено частиною одинадцятою згідно із Законом [№ 1169-VII від 27.03.2014](#)}

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.

{Частина перша статті 21 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Створення, реорганізація чи ліквідація РСО здійснюються за погодженням із Службою безпеки України. У своїй роботі РСО взаємодіють з органами Служби безпеки України.

До складу режимно-секретного органу входять підрозділи режиму, секретного діловодства та інші підрозділи, що безпосередньо забезпечують охорону державної таємниці, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації.

{Частина третя статті 21 в редакції Законів [№ 1169-VII від 27.03.2014](#), [№ 374-VIII від 12.05.2015](#)}

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях із значним обсягом робіт, пов'язаних з державною таємницею, вводиться посада заступника керівника з питань режиму, на якого покладаються обов'язки та права керівника РСО.

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях з незначним обсягом робіт, пов'язаних з державною таємницею, де штатним розписом не передбачено створення РСО, облік і зберігання секретних документів, а також заходи щодо забезпечення режиму секретності здійснюються особисто їх керівниками або спеціально призначеним наказом керівника працівником після створення необхідних умов, що забезпечують режим секретності. На них поширюються обов'язки та права працівників РСО.

Призначення осіб на посади заступників керівників з питань режиму, начальників РСО та їх заступників, а також видання наказу про покладення на окремого працівника обов'язків щодо забезпечення режиму секретності здійснюється за погодженням з органами Служби безпеки України та РСО вищестоящих державних органів, органів місцевого самоврядування, підприємств, установ і організацій.

РСО комплектуються спеціалістами, яким надано допуск до державної таємниці із ступенем секретності "цілком таємно", якщо характер виконуваних робіт не вимагає допуску до державної таємниці із ступенем секретності "особливої важливості". Якщо державний орган, орган місцевого самоврядування, підприємство, установа або організація не провадить діяльність із секретною інформацією, що має ступені секретності "цілком таємно" та "особливої важливості", РСО такого органу, підприємства, установи або організації комплектується спеціалістами, яким надано допуск до державної таємниці зі ступенем секретності "таємно".

{Частина сьома статті 21 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Основними завданнями РСО є:

- а) недопущення необґрунтованого допуску та доступу осіб до секретної інформації;
- б) своєчасне розроблення та реалізація разом з іншими структурними підрозділами державних органів, органів місцевого самоврядування, підприємств, установ і організацій заходів, що забезпечують охорону державної таємниці;
- в) запобігання розголошенню секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодінню секретною інформацією іноземними державами, іноземними юридичними

особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуску та доступу до неї;

г) виявлення та закриття каналів просочення секретної інформації в процесі діяльності державних органів, органів місцевого самоврядування, підприємства, установи, організації;

д) забезпечення запровадження заходів режиму секретності під час виконання всіх видів робіт, пов'язаних з державною таємницею, та під час здійснення зовнішніх відносин;

е) організація та ведення секретного діловодства;

{Пункт "е" частини восьмої статті 21 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

є) здійснення контролю за станом режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та на підпорядкованих їм об'єктах.

PCO мають право:

а) вимагати від усіх працівників державного органу, органу місцевого самоврядування, підприємства, установи та організації, а також відряджених неухильного виконання вимог законодавства щодо забезпечення охорони державної таємниці;

б) брати участь у розгляді проектів штатних розписів державного органу, органу місцевого самоврядування, підприємства, установи та організації та підвідомчих їм установ, підприємств у частині, що стосується PCO, вносити пропозиції щодо структури та чисельності працівників цих органів;

в) брати участь у проведенні атестації працівників, що виконують роботи, пов'язані з державною таємницею, а також у розгляді пропозицій щодо виплати в установленому нормативними актами порядку компенсації за роботу в умовах режимних обмежень;

г) залучати спеціалістів державного органу, органу місцевого самоврядування, підприємства, установи та організації до здійснення заходів щодо охорони державної таємниці;

д) здійснювати перевірки стану й організації роботи з питань захисту державної таємниці і забезпечення режиму секретності у підрозділах державного органу, органу місцевого самоврядування, підприємства, установи та організації, а також у підвідомчих їм установах та підприємствах, давати відповідні рекомендації;

е) здійснювати перевірки додержання режиму секретності на робочих місцях працівників, що мають допуск до державної таємниці, вмісту спецсховищ (приміщень, сейфів, металевих шаф, спецчемоданів, спецпапок тощо), наявності документів, виробів та інших матеріальних носіїв секретної інформації;

є) порушувати перед керівником державного органу, органу місцевого самоврядування, підприємства, установи та організації питання про призначення службових розслідувань за фактами порушень режиму секретності та секретного діловодства, про притягнення осіб до відповідальності згідно з законом, а також давати рекомендації щодо обов'язкових для виконання вказівок керівникам підрозділів державного органу, органу місцевого самоврядування, підприємства,

установи та організації та підвідомчих їм установ, підприємств з питань забезпечення режиму секретності;

ж) брати участь у службових розслідуваннях, у встановленому порядку вимагати від працівників державного органу, органу місцевого самоврядування, підприємства, установи та організації письмових пояснень щодо фактів розголошення ними секретних відомостей, втрати матеріальних носіїв секретної інформації, інших порушень режиму секретності;

з) вносити пропозиції керівникові державного органу, органу місцевого самоврядування, підприємства, установи та організації про припинення робіт, пов'язаних з державною таємницею, в структурних підрозділах, якщо умови для їх виконання не відповідають вимогам режиму секретності; опечатувати приміщення, де ведуться такі роботи або зберігаються матеріальні носії секретної інформації;

и) одержувати від громадян, яким оформляються документи на допуск до державної таємниці, анкетні дані;

і) використовувати засоби зв'язку та вести в установленому порядку поштово-телеграфне листування з іншими державними органами, органами місцевого самоврядування, підприємствами, установами і організаціями та їх РСО з питань забезпечення режиму секретності;

ї) мати печатку з найменуванням РСО, а також інші печатки та штампи установленої форми.

Передача функцій РСО будь-яким іншим підрозділам державного органу, органу місцевого самоврядування, підприємства, установи та організації не допускається.

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;

{Абзац сьомий частини першої статті 22 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

для форми 3 - 10 років.

{Абзац восьмий частини першої статті 22 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Допуск до державної таємниці надається дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої, наукової чи науково-технічної

діяльності або навчання, органами Служби безпеки України після проведення їх перевірки. Порядок надання допуску до державної таємниці визначається Кабінетом Міністрів України.

{Частина друга статті 22 в редакції Закону [№ 2432-VI від 06.07.2010](#)}

В окремих випадках, які визначаються міністерствами, іншими центральними органами виконавчої влади, за погодженням із Службою безпеки України громадянам України віком від 16 років може надаватися допуск до державної таємниці із ступенями секретності "цілком таємно" та "таємно", а віком від 17 років - також до державної таємниці із ступенем секретності "особливої важливості".

Для розгляду питання про надання громадянам допуску до державної таємниці державними органами, органами місцевого самоврядування, підприємствами, установами, організаціями, де працюють, проходять службу або навчаються громадяни, оформляються документи, які надсилаються до органів Служби безпеки України. Перелік та форми таких документів, а також порядок їх надання визначаються Кабінетом Міністрів України.

{Частина четверта статті 22 із змінами, внесеними згідно із Законами [№ 293-VI від 21.05.2008](#), [№ 2592-VI від 07.10.2010](#); в редакції Закону [№ 2432-VI від 06.07.2010](#)}

Допуск до державної таємниці під час застосування до боржника судових процедур банкрутства у встановленому законодавством порядку надається органами Служби безпеки України арбітражному керуючому (розпоряднику майна, керуючому санацією, ліквідатору) після проведення його перевірки за поданням державного органу, органу місцевого самоврядування, підприємства, установи, організації, до сфери управління якого (якої) належить боржник або який (яка) є замовником робіт, пов'язаних з державною таємницею.

{Статтю 22 доповнено новою частиною згідно із Законом [№ 4212-VI від 22.12.2011](#)}

Якщо потреба громадянина у відомостях, що становлять державну таємницю, не пов'язана з місцем роботи, служби або навчання, документи про надання допуску до державної таємниці можуть оформлятися за місцем провадження діяльності, пов'язаної з державною таємницею.

{Частина статті 22 із змінами, внесеними згідно із Законом [№ 2978-VI від 03.02.2011](#)}

Надання допуску передбачає:

визначення необхідності роботи громадянина із секретною інформацією;

перевірку громадянина у зв'язку з допуском до державної таємниці;

взяття громадянином на себе письмового зобов'язання щодо збереження державної таємниці, яка буде йому довірена;

одержання у письмовій формі згоди громадянина на передбачені законом обмеження прав у зв'язку з його допуском до державної таємниці;

ознайомлення громадянина з мірою відповідальності за порушення законодавства про державну таємницю.

{Частину статті 22 виключено на підставі Закону [№ 2432-VI від 06.07.2010](#)}

Стаття 23. Відмова у наданні допуску до державної таємниці

Допуск до державної таємниці не надається у разі:

1) відсутності у громадянина обгрунтованої необхідності в роботі із секретною інформацією;

2) сприяння громадянином діяльності іноземної держави, іноземної організації чи їх представників, а також окремих іноземців чи осіб без громадянства, що завдає шкоди інтересам національної безпеки України, або участі громадянина в діяльності політичних партій та громадських організацій, діяльність яких заборонена у порядку, встановленому законом;

3) відмови громадянина взяти на себе письмове зобов'язання щодо збереження державної таємниці, яка буде йому довірена, а також за відсутності його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці;

4) наявності у громадянина судимості за тяжкі або особливо тяжкі злочини, не погашеної чи не знятої в установленому порядку;

{Пункт 4 частини першої статті 23 в редакції Закону [№ 2432-VI від 06.07.2010](#)}

5) наявності у громадянина психічних розладів, які можуть завдати шкоди охороні державної таємниці, відповідно до переліку, затвердженого Міністерством охорони здоров'я України і Службою безпеки України.

{Пункт 5 частини першої статті 23 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

У наданні допуску до державної таємниці може бути відмовлено також у разі:

1) повідомлення громадянином під час оформлення допуску недостовірних відомостей про себе;

2) постійного проживання громадянина за кордоном або оформлення ним документів на виїзд для постійного проживання за кордоном;

3) невиконання громадянином обов'язків щодо збереження державної таємниці, яка йому довірена або довірялася раніше.

Громадянина, якому відмовлено у допуску до державної таємниці, якщо виконання трудових чи службових обов'язків вимагає доступу до державної таємниці, а переміщення на інше робоче місце чи іншу посаду неможливе, може бути в передбаченому законодавством порядку переведено на іншу роботу або службу, не пов'язану з державною таємницею, чи звільнено.

{Статтю 23 доповнено частиною третьою згідно із Законом [№ 2978-VI від 03.02.2011](#)}

Стаття 24. Перевірка громадян у зв'язку з допуском їх до державної таємниці

Перевірка громадян у зв'язку з їх допуском до державної таємниці здійснюється органами Служби безпеки України у строк до одного місяця у порядку, встановленому цим Законом і [Законом України "Про оперативно-розшукову діяльність"](#).

{Частина перша статті 24 із змінами, внесеними згідно із Законом [№ 2978-VI від 03.02.2011](#); в редакції Закону [№ 1169-VII від 27.03.2014](#)}

У ході перевірки органами Служби безпеки України з'ясовуються наявність чи відсутність обставин, передбачених [пунктами 2 і 4 частини першої](#) та [частиною другою статті 23](#) цього Закону. За результатами перевірки органи Служби безпеки України надсилають протягом п'яти робочих

днів з дня її закінчення до державних органів, органів місцевого самоврядування, підприємств, установ, організацій, що звернулися з приводу надання громадянам допуску до державної таємниці, повідомлення про надання або відмову в наданні такого допуску.

{Частина друга статті 24 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Наявність чи відсутність обставин, передбачених [пунктами 1, 3 і 5](#) частини першої статті 23 цього Закону, з'ясовується державним органом, органом місцевого самоврядування, підприємством, установою, організацією, що оформляє документи на допуск.

{Частина третя статті 24 із змінами, внесеними згідно із Законом [№ 2978-VI від 03.02.2011](#)}

Повідомлення органів Служби безпеки України про відмову в наданні громадянам допуску до державної таємниці мають містити посилання на відповідні положення [статті 23](#) цього Закону. Відмова не виключає повторного звернення державних органів, органів місцевого самоврядування, підприємств, установ, організацій з цього приводу в разі зміни обставин, за яких у наданні допуску до державної таємниці було відмовлено.

{Частина четверта статті 24 в редакції Закону [№ 2432-VI від 06.07.2010](#)}

У разі виникнення кризової ситуації, що загрожує національній безпеці України, оголошення рішення про проведення мобілізації та (або) введення правового режиму воєнного стану допуск до державної таємниці громадянам України, які призиваються на військову службу, а також військовослужбовцям та працівникам Збройних Сил України, інших військових формувань, правоохоронних органів спеціального призначення, Державної спеціальної служби транспорту, Державної служби спеціального зв'язку та захисту інформації України, які переміщуються на посади, зайняття яких передбачає наявність допуску до державної таємниці, надається у десятиденний термін. Порядок проведення перевірки громадян у зв'язку з їх допуском до державної таємниці визначається Кабінетом Міністрів України.

{Статтю 24 доповнено частиною п'ятою згідно із Законом [№ 1169-VII від 27.03.2014](#)}

Стаття 27. Доступ громадян до державної таємниці

Доступ до державної таємниці надається дієздатним громадянам України, яким надано допуск до державної таємниці та які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання.

Рішення про надання доступу до конкретної секретної інформації (категорії секретної інформації) та її матеріальних носіїв приймають керівники державних органів, органів місцевого самоврядування, підприємств, установ та організацій, у яких виконуються роботи, пов'язані з державною таємницею, або зберігаються матеріальні носії секретної інформації.

{Частина друга статті 27 в редакції Закону [№ 2432-VI від 06.07.2010](#)}

Керівники державних органів, за винятком осіб, передбачених частиною шостою цієї статті, органів місцевого самоврядування, підприємств, установ та організацій доступ до державної таємниці у сфері, що стосується діяльності державного органу, органу місцевого самоврядування,

підприємства, установи та організації, отримують за посадою після надання їм допуску до державної таємниці за відповідною формою.

{Статтю 27 доповнено новою частиною згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Порядок надання доступу до державної таємниці особам, залученим до конфіденційного співробітництва з оперативними підрозділами правоохоронних та інших спеціально уповноважених органів, які проводять оперативно-розшукову, розвідувальну або контррозвідувальну діяльність, визначається керівниками зазначених органів за погодженням із Службою безпеки України. У Службі безпеки України такий порядок надання доступу до державної таємниці визначається Головою Служби безпеки України.

{Статтю 27 доповнено новою частиною згідно із Законом [№ 2432-VI від 06.07.2010](#)}

Відмова надати громадянину України доступ до конкретної секретної інформації та її матеріальних носіїв можлива лише у разі відсутності підстав, передбачених частиною першою цієї статті, та може бути оскаржена в порядку, встановленому [частиною другою](#) статті 25 цього Закону.

Президентові України, Голові Верховної Ради України, Прем'єр-міністрові України та іншим членам Кабінету Міністрів України, Голові Верховного Суду, Голові Конституційного Суду України, Генеральному прокурору, Голові Служби безпеки України, Голові та іншим членам Рахункової палати, народним депутатам України доступ до державної таємниці усіх ступенів секретності надається за посадою після взяття ними письмового зобов'язання щодо збереження державної таємниці.

{Частина статті 27 із змінами, внесеними згідно із Законами [№ 1519-IV від 19.02.2004](#), [№ 293-VI від 21.05.2008](#), [№ 576-VIII від 02.07.2015](#), [№ 1798-VIII від 21.12.2016](#), [№ 2509-VIII від 12.07.2018](#)}

[Іноземцям та особам без громадянства доступ до державної таємниці](#) надається у виняткових випадках на підставі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, або письмового розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України.

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;

{Абзац шостий статті 28 із змінами, внесеними згідно із Законом [№ 2432-VI від 06.07.2010](#)}
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 31. Обмеження на оприлюднення секретної інформації

Під час підготовки матеріалів для опублікування, поширення у пресі та інших засобах масової інформації або переміщення їх через державний кордон державні органи, органи місцевого самоврядування, підприємства, установи, організації та громадяни з метою охорони секретної інформації зобов'язані керуватися законами України "[Про інформацію](#)" та "[Про доступ до публічної інформації](#)", цим Законом та іншими нормативно-правовими актами про державну таємницю.

{Частина перша статті 31 із змінами, внесеними згідно із Законом [№ 1170-VII від 27.03.2014](#)}

Контроль за додержанням законодавства про державну таємницю з метою запобігання її поширенню у пресі та інших засобах масової інформації здійснює центральний орган виконавчої влади з питань інформаційної політики.

Стаття 32. Обмеження щодо передачі державної таємниці іноземній державі чи міжнародній організації

Секретна інформація до скасування рішення про віднесення її до державної таємниці та матеріальні носії такої інформації до їх розсекречування можуть бути передані іноземній державі чи міжнародній організації лише на підставі міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, або письмового мотивованого розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України.

Стаття 35. Технічний та криптографічний захисти секретної інформації

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

Крім цих законів ще використовуються щодо забезпечення захисту інформації в Україні такі закони:

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України», Закон України «Про національну безпеку України», Закон України «Про електронні довірчі послуги».

Закон України «Про стандартизацію»

Цей Закон установлює правові та організаційні засади стандартизації в Україні і спрямований на забезпечення формування та реалізації державної політики у відповідній сфері.

Розділ I

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

1. У цьому Законі терміни вживаються в такому значенні:

- 1) європейський стандарт - регіональний стандарт, прийнятий європейською організацією стандартизації;
- 2) заінтересована сторона - будь-яка фізична або юридична особа, яка має безпосередній або опосередкований інтерес щодо діяльності у сфері стандартизації та/або застосування її результатів;
- 3) каталог - документ, що містить систематизований звід або перелік будь-яких об'єктів та дає змогу віднайти кожний об'єкт за певним позначенням. Каталог може містити характеристики, показники та інші дані щодо об'єктів, внесених до нього;
- 4) кодекс усталеної практики - нормативний документ, що містить рекомендації щодо практик чи процедур проектування, виготовлення, монтажу, технічного обслуговування або експлуатації обладнання, конструкцій чи виробів;
- 5) коментарі - зауваження і пропозиції до проектів національних стандартів та кодексів усталеної практики;
- 6) консенсус - загальна згода, що характеризується відсутністю серйозних заперечень з суттєвих питань у більшості заінтересованих сторін та досягається в результаті процедури, спрямованої на врахування думки всіх сторін і зближення розбіжних поглядів. Консенсус не обов'язково є одностайним;
- 7) міждержавний стандарт - регіональний стандарт, передбачений Угодою про проведення узгодженої політики в галузі стандартизації, метрології і сертифікації від 13 березня 1992 року та прийнятий Міждержавною радою із стандартизації, метрології і сертифікації;

8) міжнародна організація стандартизації - організація, що займається стандартизацією, членство в якій відкрите для відповідних національних органів усіх держав;

9) міжнародна стандартизація - стандартизація, участь у якій відкрита для відповідних органів усіх держав;

10) міжнародний стандарт - стандарт, прийнятий міжнародною організацією із стандартизації і доступний для широкого кола користувачів;

{Пункт 10 частини першої статті 1 із змінами, внесеними згідно із Законом № 124-VIII від 15.01.2015}

11) національна стандартизація - стандартизація, що здійснюється на рівні однієї держави;

12) національний орган стандартизації - орган стандартизації, визнаний на національному рівні, що має право бути національним членом відповідних міжнародних та регіональних організацій стандартизації;

13) національний стандарт - стандарт, прийнятий національним органом стандартизації та доступний для широкого кола користувачів;

14) нормативний документ - документ, що встановлює правила, настанови чи характеристики щодо діяльності або її результатів;

15) перевірка - розгляд нормативного документа з метою встановлення необхідності його подальшого застосування, перегляду чи скасування;

16) перегляд - внесення всіх необхідних змін до змісту та оформлення нормативного документа, результатом якого є прийняття нового нормативного документа;

17) регіональна організація стандартизації - організація, що займається стандартизацією, членство в якій відкрите для відповідних національних органів держав лише одного географічного, політичного або економічного простору;

18) регіональна стандартизація - стандартизація, участь у якій відкрита для відповідних органів держав лише одного географічного, політичного або економічного простору;

19) регіональний стандарт - стандарт, прийнятий регіональною організацією стандартизації і доступний для широкого кола користувачів;

20) стандарт - нормативний документ, заснований на консенсусі, прийнятий визнаним органом, що встановлює для загального і неодноразового використання правила, настанови або характеристики щодо діяльності чи її результатів, та спрямований на досягнення оптимального ступеня впорядкованості в певній сфері;

21) стандартизація - діяльність, що полягає в установленні положень для загального та неодноразового використання щодо наявних чи потенційних завдань і спрямована на досягнення оптимального ступеня впорядкованості в певній сфері;

22) технічні умови - нормативний документ, що встановлює технічні вимоги, яким повинна відповідати продукція, процес або послуга, та визначає процедури, за допомогою яких може бути встановлено, чи дотримані такі вимоги.

2. Терміни "розумне пристосування" та "універсальний дизайн" вживаються у значенні, наведеному в Законі України "Про ратифікацію Конвенції про права осіб з інвалідністю і Факультативного протоколу до неї", термін "технічний регламент" вживається у значенні, наведеному в Законі України "Про стандарти, технічні регламенти та процедури оцінки відповідності", а термін "продукція" - у значенні, наведеному в Законі України "Про підтвердження відповідності".

{Частина друга статті 1 із змінами, внесеними згідно із Законом № 2581-VIII від 02.10.2018}

Стаття 2. Сфера дії Закону

1. Цей Закон регулює відносини, пов'язані з діяльністю у сфері стандартизації та застосуванням її результатів.

2. Дія цього Закону не поширюється на санітарні заходи безпечності харчових продуктів, ветеринарно-санітарні та фітосанітарні заходи, будівельні норми, авіаційні правила України, розроблені відповідно до нормативних актів Європейського агентства з безпеки польотів, які визначають стандарти та вимоги для сертифікації, нагляду та експлуатації повітряних суден та є нормативно-технічними документами, лікарські засоби, військові стандарти, стандарти медичної допомоги, бухгалтерського обліку, оцінки майна, освіти та інші соціальні стандарти, передбачені законодавством.

{Частина друга статті 2 із змінами, внесеними згідно із Законами № 2742-VIII від 06.06.2019, № 2026-IX від 27.01.2022}

Стаття 3. Законодавство України у сфері стандартизації

1. Законодавство України у сфері стандартизації складається з цього Закону, чинних міжнародних договорів України та інших нормативно-правових актів, що регулюють відносини у відповідній сфері.

Стаття 4. Мета стандартизації та основні принципи державної політики у сфері стандартизації

1. Метою стандартизації в Україні є:

1) забезпечення відповідності об'єктів стандартизації своєму призначенню;

2) керування різноманітністю, застосовність, сумісність, взаємозамінність об'єктів стандартизації;

3) забезпечення раціонального виробництва шляхом застосування визнаних правил, настанов і процедур;

4) забезпечення охорони життя та здоров'я;

5) забезпечення прав та інтересів споживачів;

6) забезпечення безпечності праці;

7) збереження навколишнього природного середовища і економія всіх видів ресурсів;

8) усунення технічних бар'єрів у торгівлі та запобігання їх виникненню, підтримка розвитку і міжнародної конкурентоспроможності продукції.

2. Державна політика у сфері стандартизації базується на збалансованому застосуванні таких принципів:

1) забезпечення участі фізичних і юридичних осіб у розробленні національних стандартів та кодексів усталеної практики;

2) відкритості та прозорості процедур розроблення і прийняття національних стандартів та кодексів усталеної практики з урахуванням інтересів усіх заінтересованих сторін;

3) неупередженого прийняття національних стандартів та кодексів усталеної практики на засадах консенсусу;

4) добровільного застосування національних стандартів та кодексів усталеної практики, якщо інше не передбачено нормативно-правовими актами;

5) відповідності національних стандартів та кодексів усталеної практики законодавству;

6) адаптації до сучасних досягнень науки і техніки, сприяння впровадженню інновацій та підвищення конкурентоспроможності продукції вітчизняних виробників;

7) доступності національних стандартів та кодексів усталеної практики, а також інформації про них для користувачів;

8) пріоритетності прийняття в Україні міжнародних і регіональних стандартів та кодексів усталеної практики як національних;

9) дотриманні міжнародних та регіональних правил і процедур стандартизації;

10) участі в міжнародній та регіональній стандартизації;

11) прийняття і дотримання суб'єктами стандартизації Кодексу добродійної практики з розробки, прийняття та застосування стандартів відповідно до Угоди Світової

організації торгівлі про технічні бар'єри у торгівлі, що є додатком до Марракеської Угоди про заснування Світової організації торгівлі від 15 квітня 1994 року.

Стаття 5. Об'єкти стандартизації

1. Об'єктами стандартизації є:

- 1) матеріали, складники, обладнання, системи, їх сумісність;
- 2) правила, процедури, функції, методи, діяльність чи її результати, включаючи продукцію, персонал, системи управління;
- 3) вимоги до термінології, позначення, фасування, пакування, маркування, етикетування тощо.

Стаття 6. Нормативні документи

1. Залежно від рівня суб'єкта стандартизації, що приймає нормативні документи, вони поділяються на:

- 1) національні стандарти та кодекси усталеної практики, прийняті національним органом стандартизації;
- 2) стандарти, кодекси усталеної практики та технічні умови, прийняті підприємствами, установами та організаціями, що здійснюють стандартизацію.

Стаття 7. Мова національних стандартів та кодексів усталеної практики

1. Національні стандарти та кодекси усталеної практики приймаються державною мовою або в разі потреби однією з мов відповідних міжнародних або регіональних організацій стандартизації.

Розділ II

ОРГАНІЗАЦІЯ СТАНДАРТИЗАЦІЇ

Стаття 8. Суб'єкти стандартизації

1. Суб'єктами стандартизації є:

- 1) центральний орган виконавчої влади, що забезпечує формування державної політики у сфері стандартизації;
- 2) центральний орган виконавчої влади, що реалізує державну політику у сфері стандартизації;
- 3) національний орган стандартизації;
- 4) технічні комітети стандартизації;
- 5) підприємства, установи та організації, що здійснюють стандартизацію.

Стаття 9. Центральний орган виконавчої влади, що забезпечує формування державної політики у сфері стандартизації

1. До повноважень центрального органу виконавчої влади, що забезпечує формування державної політики у сфері стандартизації, належить:

- 1) забезпечення нормативно-правового регулювання у сфері стандартизації;
- 2) визначення пріоритетних напрямів розвитку у сфері стандартизації;
- 3) інформування та надання роз'яснень щодо реалізації державної політики у сфері стандартизації;
- 4) узагальнення практики застосування законодавства у сфері стандартизації, розроблення пропозицій щодо його вдосконалення та внесення на розгляд в установленому порядку проектів законодавчих актів, актів Президента України, Кабінету Міністрів України;
- 5) погодження програми робіт з національної стандартизації.

2. Центральний орган виконавчої влади, що забезпечує формування державної політики у сфері стандартизації, виконує інші повноваження згідно із законами.

Стаття 10. Центральний орган виконавчої влади, що реалізує державну політику у сфері стандартизації

1. До повноважень центрального органу виконавчої влади, що реалізує державну політику у сфері стандартизації, належить:

- 1) вжиття обґрунтованих заходів для прийняття і дотримання суб'єктами стандартизації Кодексу добросовісної практики з розробки, прийняття та застосування стандартів відповідно до Угоди Світової організації торгівлі про технічні бар'єри у торгівлі, що є додатком до Марракеської Угоди про заснування Світової організації торгівлі від 15 квітня 1994 року;

- 2) здійснення контролю за дотриманням національним органом стандартизації процедур у сфері стандартизації відповідно до принципів, норм і вимог, установлених цим Законом та іншими нормативно-правовими актами.

2. Центральний орган виконавчої влади, що реалізує державну політику у сфері стандартизації, виконує інші повноваження згідно із законами.

Стаття 11. Національний орган стандартизації

1. Функції національного органу стандартизації виконує державне підприємство, що не підлягає приватизації, утворене центральним органом виконавчої влади, що реалізує державну політику у сфері стандартизації.

Національний орган стандартизації не може мати на меті одержання прибутку від своєї діяльності.

2. До повноважень національного органу стандартизації належить:

- 1) організація та координація діяльності щодо розроблення, прийняття, перевірки, перегляду, скасування та відновлення дії національних стандартів, кодексів ustalеної практики та змін до них відповідно до цього Закону;

2) прийняття, скасування та відновлення дії національних стандартів, кодексів ustalеної практики та змін до них відповідно до цього Закону;

3) вжиття заходів щодо гармонізації національних стандартів та кодексів ustalеної практики з відповідними міжнародними, регіональними стандартами та кодексами ustalеної практики;

4) розроблення за погодженням з центральним органом виконавчої влади, що реалізує державну політику у сфері стандартизації, національних стандартів та змін до них щодо:

процедур розроблення, прийняття, перевірки, перегляду, скасування та відновлення дії національних стандартів, кодексів ustalеної практики та змін до них;

критеріїв, форми і процедур розгляду пропозицій щодо проведення робіт з національної стандартизації;

процедур створення, діяльності та припинення діяльності технічних комітетів стандартизації;

5) забезпечення відповідності національних стандартів та кодексів ustalеної практики законодавству;

6) забезпечення адаптації національних стандартів та кодексів ustalеної практики до сучасних досягнень науки і техніки;

7) підготовка та затвердження програми робіт з національної стандартизації;

8) прийняття рішень щодо створення та припинення діяльності технічних комітетів стандартизації, визначення сфери їх діяльності;

9) координація діяльності технічних комітетів стандартизації;

10) участь у підготовці міжнародних, регіональних стандартів та кодексів ustalеної практики, що розробляються відповідними міжнародними та регіональними організаціями стандартизації, членом яких є національний орган стандартизації чи з якими він співпрацює згідно з положеннями таких організацій або відповідними договорами, а також забезпечення врахування інтересів України під час провадження зазначеної діяльності;

11) забезпечення та сприяння співробітництву у сфері стандартизації між виробниками, постачальниками, споживачами продукції та відповідними державними органами;

12) заохочення суб'єктів малого і середнього підприємництва до участі в розробленні національних стандартів та кодексів ustalеної практики, забезпечення доступу зазначених суб'єктів до текстів таких документів;

13) підготовка щорічного звіту про свою діяльність, внесення його після схвалення керівною радою на розгляд до центрального органу виконавчої влади, що забезпечує

формування державної політики у сфері стандартизації, та оприлюднення на офіційному веб-сайті не пізніше п'яти робочих днів з дня схвалення цього звіту керівною радою, але не пізніше 1 квітня наступного за звітним року.

3. Національний орган стандартизації виконує інші функції та повноваження згідно із законами та статутом.

4. Статут національного органу стандартизації та зміни до нього затверджуються центральним органом виконавчої влади, що реалізує державну політику у сфері стандартизації.

Стаття 12. Керівник національного органу стандартизації

1. Національний орган стандартизації очолює керівник, який призначається на посаду та звільняється з посади керівником центрального органу виконавчої влади, що реалізує державну політику у сфері стандартизації.

2. Керівник національного органу стандартизації призначається на посаду за пропозицією керівної ради.

3. Керівником національного органу стандартизації може бути громадянин України, який проживає в Україні останні п'ять років, має повну вищу освіту, загальний стаж роботи на керівних посадах не менш як три роки, досвід роботи у сфері стандартизації не менш як п'ять років та в якого відсутня не погашена або не знята судимість за вчинення кримінального правопорушення.

{Частина третя статті 12 із змінами, внесеними згідно із Законом № 720-IX від 17.06.2020}

4. Керівник національного органу стандартизації є членом керівної ради, не може бути обраний її головою (заступником голови) або головувати на її засіданнях.

Стаття 13. Керівна рада

1. Керівна рада є дорадчо-наглядним органом національного органу стандартизації та формується на паритетних засадах з представників:

1) центрального органу виконавчої влади, що забезпечує формування державної політики у сфері стандартизації, інших центральних органів виконавчої влади та державних органів;

2) наукових установ, навчальних закладів, науково-технічних та інженерних товариств (спілок);

3) громадських об'єднань суб'єктів господарювання (у тому числі суб'єктів малого і середнього підприємництва), організацій роботодавців та їх об'єднань;

4) громадських організацій споживачів (об'єднань споживачів);

5) інших громадських об'єднань та професійних спілок.

Члени керівної ради виконують свої обов'язки на громадських засадах.

2. Голова керівної ради та його заступники обираються керівною радою.

3. До повноважень керівної ради належить:

1) підготовка пропозицій щодо:

формування державної політики у сфері стандартизації;

здійснення контролю за дотриманням національним органом стандартизації процедур у сфері стандартизації;

процедур у сфері стандартизації;

приєднання до міжнародних та регіональних організацій стандартизації, укладення договорів про співробітництво та проведення робіт у сфері стандартизації з національними органами стандартизації інших держав;

2) схвалення проектів:

рішень щодо створення та припинення діяльності технічних комітетів стандартизації, визначення сфери їх діяльності;

програми робіт з національної стандартизації;

щорічного звіту про діяльність національного органу стандартизації;

3) моніторинг та оцінка діяльності технічних комітетів стандартизації;

4) здійснення нагляду за виконанням національним органом стандартизації його повноважень.

4. Організаційне забезпечення діяльності керівної ради здійснюється національним органом стандартизації.

5. Положення про керівну раду та її склад затверджуються центральним органом виконавчої влади, що забезпечує формування державної політики у сфері стандартизації.

Стаття 14. Комісія з апеляцій

1. Будь-яка заінтересована сторона або технічний комітет стандартизації має право звернутися до комісії з апеляцій шляхом подання апеляції, якщо вважає, що рішенням, дією чи бездіяльністю національного органу стандартизації були порушені процедури у сфері стандартизації.

Предметом апеляції не може бути зміст національного стандарту, кодексу ustalеної практики чи його проекту.

Подання апеляції не обмежує права заявника на звернення до суду.

2. У разі якщо комісія з апеляцій визнає, що рішення, дія чи бездіяльність національного органу стандартизації порушує процедури у сфері стандартизації, вона приймає рішення про підтримання апеляції, в якому рекомендує національному органу стандартизації усунути виявлені порушення.

Рішення комісії з апеляцій надається сторонам у письмовій формі.

3. Рішення комісії з апеляцій може бути оскаржене в судовому порядку.

4. Комісія з апеляцій не має статусу юридичної особи.

До складу комісії з апеляцій не можуть входити працівники національного органу стандартизації. Член комісії з апеляцій не може брати участь у розгляді апеляції в разі, якщо він перебував або перебуває у службовій чи іншій залежності від осіб, які є сторонами апеляції, або за наявності інших обставин, що викликають сумнів у неупередженості такого члена.

5. Комісія з апеляцій подає на розгляд керівної ради щорічний звіт про свою діяльність.

6. Положення про комісію з апеляцій, її склад та порядок розгляду апеляцій затверджує центральний орган виконавчої влади, що забезпечує формування державної політики у сфері стандартизації.

Стаття 15. Технічні комітети стандартизації

1. Технічним комітетом стандартизації є форма співробітництва заінтересованих юридичних та фізичних осіб з метою організації і виконання робіт з міжнародної, регіональної, національної стандартизації у визначених сферах діяльності та за закріпленими об'єктами стандартизації.

Технічні комітети стандартизації не мають статусу юридичної особи.

2. До роботи в технічних комітетах стандартизації залучаються уповноважені представники органів виконавчої влади, інших державних органів, органів місцевого самоврядування, суб'єктів господарювання та їх громадських об'єднань, організацій роботодавців та їх об'єднань, наукових установ та навчальних закладів, науково-технічних та інженерних товариств (спілок), громадських організацій споживачів (об'єднань споживачів), інших громадських об'єднань, професійних спілок, провідних науковців і фахівців.

Технічні комітети стандартизації формуються з урахуванням принципу представництва всіх заінтересованих сторін.

Членство в технічних комітетах стандартизації є добровільним.

3. До повноважень технічних комітетів стандартизації належить:

1) участь у роботі відповідних технічних комітетів стандартизації міжнародних і регіональних організацій стандартизації;

2) розроблення і погодження національних стандартів, кодексів усталеної практики та змін до них;

3) участь у формуванні програми робіт з національної стандартизації;

4) перевірка і перегляд національних стандартів та кодексів усталеної практики, розробниками яких вони є;

5) погодження і надання пропозицій щодо скасування та відновлення дії національних стандартів, кодексів усталеної практики та змін до них.

4. У разі відсутності технічного комітету стандартизації, сфера діяльності якого поширюється на певні об'єкти стандартизації:

1) робочі групи, утворені національним органом стандартизації, до складу яких входять представники заінтересованих сторін, розробляють міжнародні, регіональні, національні стандарти та кодекси усталеної практики на відповідні об'єкти стандартизації;

2) національний орган стандартизації погоджує, проводить перевірку, переглядає, розробляє зміни до національних стандартів та кодексів усталеної практики і приймає рішення щодо їх скасування та відновлення дії.

5. Роз'яснення щодо положень національних стандартів та кодексів усталеної практики надають відповідні технічні комітети стандартизації, а в разі їх відсутності - національний орган стандартизації.

6. Положення про технічні комітети стандартизації затверджує національний орган стандартизації.

7. Організаційне забезпечення діяльності технічних комітетів стандартизації здійснюють їх секретаріати.

Функції секретаріату технічного комітету стандартизації покладаються національним органом стандартизації на організацію, що є юридичною особою - резидентом України та офіційно заявить про намір виконувати функції секретаріату і підтвердить спроможність організаційно, технічно та фінансово забезпечити його діяльність.

Національний орган стандартизації може виконувати функції секретаріату технічних комітетів стандартизації.

8. Технічні комітети стандартизації не можуть мати на меті одержання прибутку від своєї діяльності.

Стаття 16. Підприємства, установи та організації, що здійснюють стандартизацію

1. Підприємства, установи та організації мають право у відповідних сферах діяльності та з урахуванням своїх господарських і професійних потреб організовувати та виконувати роботи із стандартизації, зокрема:

1) розробляти, приймати, перевіряти, переглядати та скасовувати стандарти, кодекси ustalеної практики, технічні умови і зміни до них, установлювати процедури їх розроблення, прийняття, перевірки, перегляду, скасування та застосування;

2) застосовувати прийняті ними стандарти, кодекси ustalеної практики та технічні умови;

3) брати участь у роботі спеціалізованих міжнародних та регіональних організацій стандартизації відповідно до положень про такі організації;

4) створювати та вести фонди нормативних документів і видавати каталоги нормативних документів для забезпечення своєї діяльності та інформаційного обміну;

5) видавати і розповсюджувати прийняті ними стандарти, кодекси ustalеної практики та технічні умови, документи відповідних спеціалізованих міжнародних організацій стандартизації, членами яких вони є чи з якими співпрацюють на підставі положень про такі організації або відповідних договорів.

2. Стандарти, кодекси ustalеної практики та технічні умови, прийняті підприємствами, установами та організаціями, застосовуються на добровільній основі.

3. Право власності на стандарти, кодекси ustalеної практики і технічні умови, прийняті підприємствами, установами та організаціями, і видані ними каталоги належать відповідним підприємствам, установам та організаціям.

Розділ III

ОСНОВНІ ЗАСАДИ, ПРОЦЕДУРИ РОЗРОБЛЕННЯ І ПРИЙНЯТТЯ ТА ЗАСТОСУВАННЯ НАЦІОНАЛЬНИХ СТАНДАРТІВ, КОДЕКСІВ УСТАЛЕНОЇ ПРАКТИКИ ТА ЗМІН ДО НИХ

Стаття 17. Основні засади розроблення національних стандартів, кодексів ustalеної практики та змін до них

1. Національні стандарти, кодекси ustalеної практики та зміни до них розробляються у спосіб, що не створює технічних бар'єрів у торгівлі та запобігає їх виникненню.

2. Національні стандарти, кодекси ustalеної практики та зміни до них розробляються на основі:

1) міжнародних стандартів, кодексів ustalеної практики та змін до них, якщо вони вже прийняті або перебувають на завершальній стадії розроблення, або відповідних їх частин, крім випадків, якщо такі стандарти, кодекси та зміни є неефективними або невідповідними, зокрема з огляду на недостатній рівень захисту, суттєві кліматичні чи географічні фактори або технологічні проблеми;

2) регіональних стандартів, кодексів усталеної практики та змін до них або відповідних їх частин у разі, якщо міжнародні стандарти, кодекси усталеної практики та зміни до них не можуть бути використані з причин, зазначених у пункті першому цієї частини;

3) стандартів, кодексів усталеної практики та змін до них або відповідних їх частин держав, що є членами відповідних міжнародних чи регіональних організацій стандартизації та з якими укладено відповідні міжнародні договори України про співробітництво і проведення робіт у сфері стандартизації;

4) наукових досягнень, знань і практики.

Національний орган зі стандартизації зобов'язаний приймати національні стандарти у сфері електронних комунікацій та радіочастотного спектра, що є ідентичні стандартам Європейського інституту телекомунікаційних стандартів та застосовуються для надання презумпції відповідності технічному регламенту радіообладнання, виключно методом перекладу державною мовою.

{Частина другу статті 17 доповнено абзацом шостим згідно із Законом № 1089-IX від 16.12.2020}

3. У разі якщо міжнародні стандарти, кодекси усталеної практики та зміни до них, визначені частиною другою цієї статті, не беруться за основу для національного стандарту, кодексу усталеної практики та змін до них, національний орган стандартизації надає письмове пояснення на запит заінтересованої сторони.

4. У разі прийняття європейського стандарту як національного забезпечується ідентичність національного стандарту відповідному європейському стандарту. З дня набрання чинності національним стандартом, що є ідентичним європейському стандарту, повинен бути скасований національний стандарт, положення якого суперечать положенням відповідного національного стандарту, що є ідентичним європейському стандарту.

5. Національні стандарти та кодекси усталеної практики повинні бути точними, чіткими та структурно уніфікованими, а їх положення у відповідних випадках повинні стосуватися експлуатаційних характеристик продукції, а не її конструктивних чи описових характеристик.

6. Національні стандарти та кодекси усталеної практики викладаються в такий спосіб, щоб їх неможливо було використовувати з метою введення в оману споживачів продукції, якої стосується національний стандарт та кодекс усталеної практики, або надавати перевагу виробнику продукції чи продукції залежно від місця її виготовлення.

7. З метою реалізації особами з інвалідністю прав та свобод людини і громадянина під час розроблення національних стандартів та кодексів усталеної практики враховуються

потреби осіб з інвалідністю та/або застосовуються принципи розумного пристосування та універсального дизайну.

{Частина сьома статті 17 із змінами, внесеними згідно із Законом № 2581-VIII від 02.10.2018}

Стаття 18. Пропозиції щодо проведення робіт з національної стандартизації

1. Заінтересовані сторони подають національному органу стандартизації пропозиції щодо проведення робіт з національної стандартизації, які стосуються розроблення, перегляду, скасування національних стандартів, кодексів усталеної практики та змін до них.

2. Пропозиції щодо проведення робіт з національної стандартизації розглядаються відповідним технічним комітетом стандартизації з урахуванням пріоритетних напрямів розвитку стандартизації та вимог, установлених у частині другій статті 17 цього Закону.

3. Національний орган стандартизації письмово повідомляє сторони, яка подала пропозицію щодо проведення робіт з національної стандартизації, про включення такої пропозиції до програми робіт з національної стандартизації або про відмову в її включенні до програми із зазначенням підстав для відмови не пізніше ніж через 60 календарних днів з дня отримання відповідної пропозиції.

4. Національний стандарт, кодекс усталеної практики та зміни до них вважаються такими, що перебувають на стадії розроблення, з дня прийняття рішення про включення пропозиції щодо їх розроблення до програми робіт з національної стандартизації до дня їх прийняття національним органом стандартизації.

Стаття 19. Підготовка програми робіт з національної стандартизації

1. Національний орган стандартизації готує програму робіт з національної стандартизації, до якої включаються роботи з розроблення, перегляду, скасування національних стандартів, кодексів усталеної практики та змін до них.

2. Програма робіт з національної стандартизації складається для координації виконання відповідних робіт.

3. Національний орган стандартизації повинен вживати заходів для уникнення дублювання робіт із стандартизації, що виконуються відповідними міжнародними або регіональними організаціями стандартизації.

4. Програма робіт з національної стандартизації повинна містити для кожного національного стандарту, кодексу усталеної практики та змін до них інформацію про етап, досягнутий у їх розробленні, і посилання на міжнародні чи регіональні стандарти та кодекси усталеної практики, взяті за основу.

5. Національний орган стандартизації повинен щонайменше один раз на шість місяців оприлюднювати програму робіт з національної стандартизації із зазначенням свого

найменування та адреси, а також назв конкретних національних стандартів та кодексів усталеної практики, що розробляються, переглядаються, скасовуються та до яких вносяться зміни. Повідомлення про оприлюднення програми робіт з національної стандартизації публікуються в офіційному друкованому виданні національного органу стандартизації та не пізніше п'яти робочих днів з дня оприлюднення програми розміщуються на офіційному веб-сайті.

6. Після оприлюднення програми робіт з національної стандартизації національний орган стандартизації повинен повідомити про це відповідні міжнародні чи регіональні організації стандартизації, членом яких він є, з використанням їх форми звітності.

Стаття 20. Повідомлення про проекти національних стандартів, кодексів усталеної практики та зміни до них, запити щодо коментарів

1. Після розроблення першої редакції проекту національного стандарту, кодексу усталеної практики чи змін до них національний орган стандартизації оприлюднює повідомлення про такий проект у своєму офіційному друкованому виданні та не пізніше п'яти робочих днів з дня завершення розроблення його першої редакції розміщує зазначене повідомлення на офіційному веб-сайті. У повідомленні зазначаються:

1) позначення та назва проекту національного стандарту, кодексу усталеної практики чи змін до нього;

2) усі відхилення проекту національного стандарту, кодексу усталеної практики чи змін до них від відповідного міжнародного, регіонального стандарту, кодексу усталеної практики чи змін до них;

3) адреса та строк подання коментарів усіма заінтересованими сторонами;

4) інформація про спосіб отримання проекту національного стандарту, кодексу усталеної практики чи змін до них.

2. Коментарі до проектів національних стандартів, кодексів усталеної практики чи змін до них надаються протягом 60 календарних днів з дня оприлюднення інформації, визначеної частиною першою цієї статті, крім термінових питань оборони держави, охорони здоров'я, безпеки навколишнього природного середовища та підготовки проекту національного стандарту для розроблення відповідного технічного регламенту.

3. Коментарі заінтересованих сторін щодо проектів національних стандартів, кодексів усталеної практики чи змін до них розглядаються відповідним технічним комітетом стандартизації або робочою групою, яка розробляє проект національного стандарту, кодексу усталеної практики чи змін до них.

4. Відповіді на коментарі щодо проектів національних стандартів, кодексів усталеної практики чи змін до них, отримані від органів стандартизації інших держав, міжнародних

або регіональних організацій стандартизації, що дотримуються Кодексу добросовісної практики з розробки, прийняття та застосування стандартів відповідно до Угоди Світової організації торгівлі про технічні бар'єри у торгівлі, що є додатком до Марракеської Угоди про заснування Світової організації торгівлі від 15 квітня 1994 року, надаються в стислий строк, але не пізніше строку прийняття. Відповідь повинна містити пояснення щодо необхідності відхилення від міжнародного або регіонального стандарту, кодексу усталеної практики чи змін до них.

5. Розробник проектів національних стандартів, кодексів усталеної практики чи змін до них після закінчення строку подання коментарів розглядає їх та враховує в остаточному проекті або обґрунтовано відхиляє.

Стаття 21. Прийняття і скасування національних стандартів, кодексів усталеної практики та змін до них

1. Проекти національних стандартів, кодексів усталеної практики та змін до них не підлягають погодженню з центральними органами виконавчої влади, іншими державними органами.

2. Міжнародні та регіональні стандарти, кодекси усталеної практики та зміни до них приймаються як національні стандарти, кодекси усталеної практики та зміни до них національним органом стандартизації.

3. У разі досягнення консенсусу щодо проекту національного стандарту, кодексу усталеної практики та змін до них національний орган стандартизації приймає їх та визначає строк набрання ними чинності з урахуванням періоду підготовчих заходів.

4. За пропозиціями заінтересованих сторін національний орган стандартизації у разі необхідності встановлює строк одночасної дії прийнятого національного стандарту чи кодексу усталеної практики та чинного національного стандарту чи кодексу усталеної практики на один і той самий об'єкт стандартизації.

5. У разі якщо технічний комітет стандартизації погоджує пропозиції щодо скасування національних стандартів та кодексів усталеної практики, національний орган стандартизації приймає рішення із зазначеного питання.

6. Інформація про прийняті і скасовані протягом календарного місяця національні стандарти, кодекси усталеної практики, зміни до них та ті з них, дію яких відновлено, оприлюднюється наступного календарного місяця в офіційному друкованому виданні національного органу стандартизації та розміщується не пізніше п'яти робочих днів з дня завершення звітного місяця на офіційному веб-сайті.

Стаття 22. Перевірка національних стандартів та кодексів усталеної практики

1. Національний орган стандартизації організує та координує діяльність з проведення перевірки національних стандартів та кодексів ustalеної практики на відповідність законодавству, потребам виробників та споживачів, рівню розвитку науки і техніки, інтересам держави, вимогам міжнародних, регіональних стандартів та кодексів ustalеної практики.

Національні стандарти та кодекси ustalеної практики перевіряються не рідше одного разу на п'ять років з дня їх прийняття.

Стаття 23. Застосування національних стандартів та кодексів ustalеної практики

1. Національні стандарти та кодекси ustalеної практики застосовуються безпосередньо чи шляхом посилання на них в інших документах.

2. Національні стандарти та кодекси ustalеної практики застосовуються на добровільній основі, крім випадків, якщо обов'язковість їх застосування встановлена нормативно-правовими актами.

3. Національний орган стандартизації забезпечує розміщення на своєму офіційному веб-сайті текстів національних стандартів та кодексів ustalеної практики, обов'язковість застосування яких встановлена нормативно-правовими актами, а також національних стандартів (крім національних стандартів, гармонізованих з міжнародними і європейськими стандартами та національними стандартами інших країн), розроблених за рахунок бюджетних коштів, у тридцятиденний строк з дня офіційного опублікування таких актів з наданням безоплатного доступу та можливості їх пошуку за датою прийняття та/або номером, назвою, контекстом, галуззю економічної діяльності та іншими параметрами пошуку, визначеними Кабінетом Міністрів України.

{Частина третя статті 23 із змінами, внесеними згідно із Законами № 124-VIII від 15.01.2015, № 199-IX від 17.10.2019; в редакції Законів № 850-IX від 02.09.2020, № 2254-IX від 12.05.2022}

{Частина четверту статті 23 виключено на підставі Закону № 2742-VIII від 06.06.2019}

Розділ IV

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ТА ПРАВО ВЛАСНОСТІ НА НАЦІОНАЛЬНІ СТАНДАРТИ, КОДЕКСИ УСТАЛЕНОЇ ПРАКТИКИ ТА КАТАЛОГИ І ВИКОРИСТАННЯ КОШТІВ, ОДЕРЖАНИХ ВІД ЇХ РЕАЛІЗАЦІЇ

Стаття 24. Інформаційне забезпечення

1. Національні стандарти, кодекси ustalеної практики, зміни до них та розроблені національним органом стандартизації каталоги видаються, відтворюються та розповсюджуються національним органом стандартизації.

2. Видання, відтворення і розповсюдження документів міжнародних та регіональних організацій стандартизації, членом яких є національний орган стандартизації, здійснюються зазначеним органом відповідно до правил таких організацій.

3. Для подання інформації заінтересованим сторонам національний орган стандартизації формує та веде національний фонд нормативних документів, функціонує як Національний інформаційний центр міжнародної інформаційної мережі (ISONET), складає та веде каталог національних стандартів та кодексів ustalеної практики.

4. Інформаційні послуги надаються національним органом стандартизації на договірних засадах шляхом видання, відтворення та розповсюдження офіційних текстів національних стандартів, кодексів ustalеної практики та змін до них, розроблених національним органом стандартизації каталогів, іншої друкованої продукції щодо прийнятих національних стандартів, кодексів ustalеної практики та змін до них, а також стандартів, кодексів ustalеної практики, документів та змін до них відповідних міжнародних та регіональних організацій стандартизації, членом яких є національний орган стандартизації чи з якими він співпрацює відповідно до положень таких організацій або відповідних договорів, інших інформаційних та довідкових видань з питань стандартизації, а також шляхом їх розповсюдження інформаційними мережами в порядку ініціативи та на замовлення.

Стаття 25. Право власності на національні стандарти, кодекси ustalеної практики та каталоги

1. Право власності на національні стандарти, кодекси ustalеної практики та розроблені національним органом стандартизації каталоги належить державі.

2. Національний стандарт та кодекс ustalеної практики можуть розроблятися на продукцію, що є об'єктом стандартизації та одночасно об'єктом інтелектуальної або промислової власності, якщо національний орган стандартизації отримав дозвіл від власника прав на продукцію в установленому законом порядку.

3. Забороняється повністю чи частково видавати, відтворювати з метою розповсюдження і розповсюджувати як офіційні видання будь-які національні стандарти, кодекси ustalеної практики та розроблені національним органом стандартизації каталоги або їх частини на будь-яких носіях інформації без дозволу національного органу стандартизації чи уповноваженої ним особи.

4. У разі видання, відтворення чи розповсюдження національного стандарту, кодексу ustalеної практики та розробленого національним органом стандартизації каталогу або їх частини без дозволу національного органу стандартизації зазначений орган не несе відповідальності за невідповідність тексту розповсюджуваного документа його офіційному тексту чи за наслідки, спричинені застосуванням розповсюдженого документа.

5. Національний орган стандартизації має право на відшкодування збитків, завданих йому недозволеним виданням, відтворенням та розповсюдженням національного стандарту, кодексу ustalеної практики та розробленого національним органом стандартизації каталогу або їх частини, відповідно до закону.

Стаття 26. Використання коштів, одержаних від реалізації стандартів, кодексів ustalеної практики та каталогів

1. Кошти, одержані від реалізації національних, регіональних, міжнародних стандартів, кодексів ustalеної практики та розроблених національним органом стандартизації каталогів, у повному обсязі спрямовуються на виконання робіт з національної стандартизації та розвиток науково-технічної бази.

Розділ V

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО ТА ФІНАНСУВАННЯ РОБІТ ІЗ СТАНДАРТИЗАЦІЇ

Стаття 27. Міжнародне співробітництво у сфері стандартизації

1. Центральний орган виконавчої влади, що забезпечує формування державної політики у сфері стандартизації, вживає заходів щодо адаптації законодавства України у сфері стандартизації до законодавства Європейського Союзу.

2. Центральний орган виконавчої влади, що забезпечує формування державної політики у сфері стандартизації, та національний орган стандартизації в межах своїх повноважень здійснюють співробітництво у зазначеній сфері з відповідними органами інших держав.

3. Центральний орган виконавчої влади, що забезпечує формування державної політики у сфері стандартизації, представляє інтереси України в міжурядових організаціях стандартизації, укладає міжнародні договори України про співробітництво та проведення робіт у сфері стандартизації з такими організаціями та відповідними урядовими і міжурядовими органами інших держав відповідно до Закону України "Про міжнародні договори України".

Національний орган стандартизації представляє інтереси України в міжнародних та регіональних організаціях стандартизації, приймає рішення про приєднання до них, укладає

договори про співробітництво та проведення робіт у сфері стандартизації з національними органами стандартизації інших держав.

Національний орган стандартизації вживає заходів щодо виконання зобов'язань, узятих за результатами участі в міжнародних та регіональних організаціях стандартизації.

4. У разі якщо міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Законом, застосовуються правила міжнародних договорів.

Стаття 28. Джерела фінансування

1. Роботи із стандартизації фінансуються їх замовниками.

2. Джерелами фінансування є:

- 1) кошти Державного бюджету України;
- 2) кошти, передбачені на виконання програм і проектів;
- 3) власні та залучені кошти суб'єктів господарювання;
- 4) інші не заборонені законодавством джерела фінансування.

3. Забезпечення участі центральних органів виконавчої влади та національного органу стандартизації в роботі керівних органів міжнародних, регіональних та міжурядових організацій стандартизації та сплата членських внесків до таких організацій здійснюються за рахунок коштів Державного бюджету України.

Стаття 29. Витрати на виконання робіт із стандартизації

1. Витрати суб'єктів господарювання, пов'язані з розробленням стандартів, кодексів ustalеної практики, у тому числі національних, та технічних умов, участю в роботі міжнародних та регіональних організацій стандартизації, належать до витрат, пов'язаних з науково-технічним забезпеченням їх господарської діяльності.

2. Витрати бюджетних установ, пов'язані з розробленням стандартів, кодексів ustalеної практики, у тому числі національних, та технічних умов, відшкодовуються за рахунок коштів, передбачених на утримання таких установ.

3. Замовниками послуг з виконання робіт з національної стандартизації за рахунок коштів Державного бюджету України є центральні органи виконавчої влади, а єдиним надавачем таких послуг - національний орган стандартизації.

4. Державна закупівля послуг з виконання робіт з національної стандартизації за рахунок коштів Державного бюджету України здійснюється відповідно до Закону України "Про публічні закупівлі".

{Частина четверта статті 29 із змінами, внесеними згідно із Законом № 114-IX від 19.09.2019}

5. Методика визначення трудомісткості та вартості робіт з національної стандартизації встановлюється центральним органом виконавчої влади, що забезпечує формування державної політики у сфері стандартизації.

Розділ VI

ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності через шість місяців з дня його опублікування, крім: підпункту 4 пункту 5 розділу VI "Прикінцеві та перехідні положення", який набирає чинності через два роки з дня опублікування цього Закону;

абзаців тринадцятого - сімнадцятого підпункту 1 та підпункту 5 пункту 5, пунктів 2 та 6 розділу VI "Прикінцеві та перехідні положення", які набирають чинності з дня, наступного за днем опублікування цього Закону.

2. Міждержавні стандарти (ГОСТ), що діяли на момент набрання чинності Угодою про проведення узгодженої політики в галузі стандартизації, метрології і сертифікації від 13 березня 1992 року, та республіканські стандарти Української Радянської Соціалістичної Республіки (РСТ УРСР) застосовуються як національні стандарти до їх заміни на національні стандарти чи скасування в Україні.

3. Стандарти, кодекси усталеної практики та технічні умови, прийняті центральними органами виконавчої влади до набрання чинності цим Законом, а також галузеві стандарти (ОСТ) та прирівняні до них інші нормативні документи колишнього Союзу Радянських Соціалістичних Республік, галузеві стандарти України (ГСТУ) (далі - галузеві нормативні документи) застосовуються до їх заміни на технічні регламенти, національні стандарти, кодекси усталеної практики чи скасування в Україні, але не більш як 15 років з дня набрання чинності цим Законом.

Протягом 15 років з дня набрання чинності цим Законом центральні органи виконавчої влади мають право у відповідних сферах діяльності та в межах своїх повноважень:

перевіряти, переглядати та скасовувати галузеві нормативні документи;

установлювати процедури перевірки, перегляду та скасування галузевих нормативних документів;

брати участь у роботі спеціалізованих міжнародних та регіональних організацій, що здійснюють стандартизацію у відповідних сферах діяльності, членами яких вони є чи з якими співпрацюють на підставі правил таких організацій або відповідних договорів;

видавати і розповсюджувати галузеві нормативні документи, каталоги галузевих нормативних документів, документи спеціалізованих міжнародних та регіональних організацій, що здійснюють стандартизацію у відповідних сферах діяльності, членами яких

вони є чи з якими співпрацюють на підставі правил таких організацій або відповідних договорів, а також делегувати зазначені повноваження іншим особам.

Центральні органи виконавчої влади мають право замовляти послуги з виконання робіт щодо перевірки галузевих нормативних документів і розроблення пропозицій щодо внесення до них змін та їх скасування відповідними технічними комітетами стандартизації з додержанням вимог частин першої і другої статті 28 та частин першої і другої статті 29 цього Закону. Закупівля зазначених послуг за рахунок коштів Державного бюджету України здійснюється відповідно до Закону України "Про публічні закупівлі".

{Абзац сьомий пункту 3 розділу VI "Прикінцеві та перехідні положення" із змінами, внесеними згідно із Законом № 114-IX від 19.09.2019}

Інформація про скасовані галузеві нормативні документи та зміни до них оприлюднюється відповідно до процедур, установлених відповідними центральними органами виконавчої влади.

Галузеві нормативні документи застосовуються на добровільній основі, крім випадків, якщо обов'язковість їх застосування встановлена нормативно-правовими актами.

Центральні органи виконавчої влади забезпечують розміщення на офіційних веб-сайтах текстів галузевих нормативних документів, обов'язковість застосування яких встановлена нормативно-правовими актами, з безоплатним доступом до них.

Право власності на галузеві нормативні документи та видані центральними органами виконавчої влади каталоги належить державі. Від імені держави права власника на такі документи здійснюють відповідні центральні органи виконавчої влади.

4. Визнати таким, що втратив чинність, Закон України "Про стандартизацію" (Відомості Верховної Ради України, 2001 р., № 31, ст. 145; 2006 р., № 12, ст. 101; 2014 р., № 4, ст. 61).

5. Внести зміни до таких законодавчих актів України:

1) у Господарському кодексі України (Відомості Верховної Ради України, 2003 р., №№ 18-22, ст. 144):

абзац четвертий частини другої статті 12 викласти в такій редакції:

"технічне регулювання";

у статті 15:

частину першу викласти в такій редакції:

"1. У сфері господарювання застосовуються технічні регламенти, стандарти, кодекси усталеної практики та технічні умови";

у частині другій:

абзац перший після слів "Застосування стандартів" доповнити словами "кодексів усталеної практики";

абзац другий викласти в такій редакції:

"суб'єктів господарювання, якщо обов'язковість застосування стандартів чи кодексів усталеної практики встановлено нормативно-правовими актами";

абзац третій доповнити словами "чи кодекси усталеної практики";

в абзаці сьомому частини третьої статті 19 слово "стандартів" виключити;

у статті 259:

у частині четвертій слова "державної системи класифікації техніко-економічної та соціальної інформації" замінити словами "національної системи класифікації";

частину п'яту викласти в такій редакції:

"5. Складовою частиною національної системи класифікації є національні класифікатори. Національні класифікатори та процедури їх розроблення затверджує центральний орган виконавчої влади, що забезпечує формування державної політики у сфері економічного розвитку";

частину шосту виключити;

2) абзац четвертий частини першої статті 15 Закону України "Про захист прав споживачів" (Відомості Верховної Ради України, 2006 р., № 7, ст. 84; 2010 р., № 9, ст. 84) виключити;

{Підпункт 3 пункту 5 розділу VI втратив чинність на підставі Закону № 124-VIII від 15.01.2015}

4) у частині другій статті 9 Закону України "Про регулювання містобудівної діяльності" (Відомості Верховної Ради України, 2011 р., № 34, ст. 343; 2013 р., № 48, ст. 682; 2014 р., № 1, ст. 4) слова і цифри "а також національних стандартів і кодексів усталеної практики за класами 91 і 93 Українського класифікатора нормативних документів (крім позицій, що стосуються лічильників, машин та устаткування), утворює та припиняє діяльність технічних комітетів стандартизації у цій сфері" виключити;

5) у Декреті Кабінету Міністрів України від 10 травня 1993 року № 46-93 "Про стандартизацію і сертифікацію" (Відомості Верховної Ради України, 1993 р., № 27, ст. 289):

у пункті 1 статті 15 слово "обов'язковим" виключити;

в абзаці другому статті 16 слово "державним" замінити словом "національним".

6. Кабінету Міністрів України у шестимісячний строк з дня опублікування цього Закону:

забезпечити утворення або визначення державного підприємства, що не підлягає приватизації і виконує функції національного органу стандартизації;

затвердити нормативно-правові акти, що впливають із цього Закону;
подати на розгляд Верховної Ради України пропозиції щодо внесення змін до законодавчих актів України у зв'язку з прийняттям цього Закону;
привести свої нормативно-правові акти у відповідність із цим Законом;
забезпечити приведення міністерствами, іншими центральними органами виконавчої влади своїх нормативно-правових актів у відповідність із цим Законом.

1.3 Державні та міжнародні стандарти, які діють в Україні

Після законодавчої бази державні стандарти являють собою важливу основу у організації відносин у сфері інформаційної безпеки.

Основними документами є ДСТУ 3396.0-96 та ДСТУ 3396.1-96:

ДСТУ 3396.0-96

Державний стандарт України ДСТУ 3396.0-96 отримав чинність від 01.01.1997 р. та установлює об'єкт захисту, мету, основні організаційно-технічні положення технічного захисту інформації, неправомірний доступ до якої може завдати шкоди громадянам, організаціям та державі.

Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян, 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.

Цей стандарт складається із таких частин:

- галузь використання;
- нормативні посилання;
- загальні положення;
- побудова системи захисту інформації;
- нормативні документи з ТЗІ.

Загальні положення Стандарту установлюють важливі положення щодо ТЗІ.

Об'єктом технічного захисту є інформація, що становить державну або іншу передбачену законодавством України таємницю, конфіденційна інформація, що є державною власністю чи передана державі у володіння, користування, розпорядження.

Носіями інформації з обмеженим доступом ІзОД можуть бути фізичні поля, сигнали, хімічні речовини, що утворюються в процесі інформаційної діяльності, виробництва й експлуатації продукції різного призначення.

Середовищем поширення носіїв ІзОД можуть бути лінії зв'язку, сигналізації, керування, енергетичні мережі, інженерні комунікації і споруди, повітряне, водне та інше середовища, ґрунт, тощо.

Витік або порушення цілісності ІзОД можуть бути результатом реалізації загроз безпеці інформації.

Мета ТЗІ може бути досягнута побудовою системи ЗІ, що є організованою сукупністю методів і засобів забезпечення ТЗІ.

Технічний захист інформації здійснюється поетапно:

- 1 етап – визначення й аналіз загроз;
- 2 етап – розроблення системи захисту інформації;
- 3 етап – реалізація плану захисту інформації;
- 4 етап - контроль функціонування та керування системою захисту інформації.

Відповідно розділ "Побудова системи захисту інформації" складається з таких підрозділів:

- визначення й аналіз загроз;
- розроблення системи захисту інформації ;
- реалізація плану захисту інформації;
- контроль функціонування та керування системою захисту інформації.

На першому етапі необхідно здійснити аналіз об'єкта захисту, ситуаційного плану, умов функціонування підприємства, установи, організації, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати засадничі дані для побудови окремої моделі загроз.

На другому етапі слід здійснити розроблення плану ТЗІ, що містить організаційні, первинні технічні та основні технічні заходи захисту ІзОД, визначити зони безпеки інформації.

Організаційні заходи регламентують порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ для всіх періодів життєвого циклу об'єкта захисту.

Первинні технічні заходи передбачають захист інформації блокуванням загроз без використання засобів ТЗІ.

Основні технічні заходи передбачають захист інформації з використанням засобів забезпечення ТЗІ.

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

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

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

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

Керування системою захисту інформації полягає у адаптації заходів ТЗІ до поточного завдання захисту інформації. За фактами зміни умов здійснення або виявлення нових загроз заходи ТЗІ реалізуються у найкоротший строк.

У разі потреби підвищення рівня захисту інформації необхідно виконати роботи, передбачені 1, 2 та 3 етапами побудови системи захисту інформації.

Крім того, стандарт визначає порядок проведення робіт із стандартизації та нормування у галузі ТЗІ, порядок розроблення, оформлення, погодження, затвердження, реєстрації, видання, впровадження, перевірки, перегляду, зміни та скасування нормативних документів.

ДСТУ 3396.1-96

Державний стандарт України ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт" отримав чинність від 01.07.1997 року і має наступні розділи:

- галузь використання;
- нормативні посилення;
- загальні положення;
- організація проведення обстеження;
- організація розроблення системи захисту інформації;
- реалізація організаційних заходів захисту;
- реалізація первинних технічних заходів захисту;
- реалізація основних технічних заходів захисту;
- приймання, визначення повноти та якості робіт.

Також стандарт має додаток, у якому наведений склад засобів забезпечення технічного захисту інформації.

Цей стандарт установлює вимоги до порядку проведення робіт з ТЗІ.

У розділі "Загальні положення" визначається здатність системи захисту інформації протистояти впливу загроз.

Можливі такі варіанти постановки задач захисту інформації:

- досягнення необхідного рівня захисту ІЗОД за мінімальних затрат і допустимого рівня обмежень видів інформаційної діяльності;
- досягнення найбільш можливого рівня захисту ІЗОД за доступних затрат і заданого рівня обмежень видів інформаційної діяльності;
- досягнення максимального рівня захисту ІЗОД за необхідних затрат і мінімального рівня обмежень видів інформаційної діяльності.

Захист інформації, яка не є державною таємницею, забезпечується, як правило, застосуванням першого чи другого варіанту.

Захист інформації, яка становить державну таємницю, забезпечується застосуванням третього варіанту.

Зміст та послідовність робіт з протидії загрозам або їхньої нейтралізації повинні відповідати зазначеним в ДСТУ 3396.0-96 етапам функціонування системи захисту інформації і полягають в:

- проведення обстеження підприємства, установи, організації;
- розробленні і реалізації організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення ТЗІ;
- прийманні робіт у ТЗІ;
- атестації систем забезпечення інформаційної діяльності на відповідність вимогам нормативних документів системи ТЗІ.

Розділ "Організація розроблення системи захисту інформації" вимагає, що на підставі матеріалів обстеження та окремої моделі загроз необхідно визначити головні задачі захисту інформації і скласти технічне завдання на розроблення системи захисту інформації.

Технічне завдання повинно включати основні розділи:

- вимоги до систем захисту інформації;
- вимоги до складу проектної та експлуатаційної документації;
- етапи виконання робіт;
- порядок внесення змін і доповнень до розділів технічного завдання;
- вимоги до порядку проведення випробування системи захисту.

Основою функціонування системи захисту інформації є план ТЗІ, що повинен містити такі документи:

- перелік розпорядчих, організаційно-методичних НД ТЗІ, а також вказівки щодо їхнього застосування;
- інструкції про порядок реалізації організаційних, первинних технічних та основних технічних заходів захисту;
- інструкції, що встановлюють обов'язки, права та відповідальність персоналу;
- календарний план ТЗІ.

Шостий розділ "Реалізація організаційних заходів захисту" визначає, що організаційні заходи захисту інформації – комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації

діяльності персоналу і порядку функціонування систем забезпечення інформаційної діяльності та систем забезпечення ТЗІ.

Оперативне вирішення задач ТЗІ досягається організацією керування системою захисту інформації.

Сьомий розділ – це розділ "Реалізація первинних технічних заходів захисту".

У процесі реалізації первинних технічних заходів потрібно забезпечити:

–блокування каналів витоку інформації;

–блокування несанкціонованого доступу до інформації чи її носіїв;

–перевірку справності та працездатності технічних засобів забезпечення інформаційної діяльності.

Усі заходи здійснюються відповідно до нормативних та експлуатаційних документів, а також згідно діючих вказівок, методик та цього розділу стандарту.

Вибір засобів забезпечення ТЗІ зумовлюється фрагментним або комплексним способом захисту інформації. Засоби ТЗІ застосовують автономно або спільно з механічними засобами забезпечення інформаційної діяльності для пасивного або активного приховування ІзОД.

Порядок атестації встановлюється НД ТЗІ.

Крім цих стандартів використовується:

–ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. формування та перевіряння";

–ДСТУ 3918-1999 (ISO/IEC 1207:1995) "Інформаційні технології. Процеси життєвого циклу програмного забезпечення";

–ДСТУ ISO/IEC TR 13335-1:2003 "Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій";

–ДСТУ ISO/IEC TR 13335-2:2003 "Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 2. Керування та планування безпеки інформаційних технологій";

–ДСТУ ISO/IEC TR 13335-3:2003 "Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій";

–ДСТУ ISO/IEC TR 13335-4:2005 "Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 4. Вибір засобів захисту";

–ДСТУ ISO/IEC TR 13335-5:2005 "Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 5. Настанова з керування мережею безпеки";

– ДСТУ ISO/IEC 27001-2015 "Інформаційні технології. Методи захисту. Система управління інформаційною безпекою";

– ДСТУ ISO/IEC 27002-2015 "Інформаційні технології. Методи захисту. Звіт практик щодо заходів інформаційної безпеки";

– ДСТУ ISO/IEC 27005-2019 "Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки".

В Україні крім державних стандартів використовуються і міжнародні стандарти в сфері інформаційної безпеки:

– ISO / IEC 18043:2006 "Інформаційні технології. Методи захисту. Вибір, застосування та операції систем виявлення вторгнення";

– *ISO/IEC TR 18044:2004 "Інформаційна технологія. Методи і засоби забезпечення безпеки МЕНЕДЖМЕНТ інцидентами інформаційної безпеки"*;

– ISO/IEC 18045:2008: "Інформаційні технології - Методи забезпечення безпеки - Методика оцінки безпеки інформаційних технологій";

– ISO / IEC 17799: 2000 (BS 7799-1: 2000) "Управління інформаційною безпекою - Інформаційні технології";

1.4. Нормативна база України у сфері захисту інформації.

Крім державних та міжнародних стандартів для забезпечення захисту інформації використовуються нормативні документи з технічного захисту інформації, які допомагають в роботі по виконанню поставлених завдань:

- НД ТЗІ 1.6-005-2013 "Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці";
- НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу";
- НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі ";
- НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу";
- НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу";
- НД ТЗІ 2.5-008-2002 "Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2";
- НД ТЗІ 3.3-001-07 "Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації".

1.5. Сертифікація у сфері засобів та комплексів захисту інформації

Міжнародний досвід свідчить про те, що необхідним інструментом гарантуючим відповідність якості продукції вимогам нормативно-технічної документації (НТД) є сертифікація. Сертифікат від лат. Certim – робити.

Сертифікація в загально прийнятій міжнародній термінології визначається, як установлення відповідальності. Національні законодавчі акти різних країн конкретизують: відповідність чому встановлюється та хто встановлює цю відповідність.

Сертифікація – це документальне підтвердження відповідності продукції визначеним вимогам, конкретним стандартам, чи технічним умовам.

Сертифікація продукції являє собою комплекс засобів або дій, проведених з метою підтвердження за допомогою сертифіката відповідності (документа), що продукція відповідає визначеним стандартам чи іншим НТД.

Багато закордонних фірм витрачають великі кошти і час на доведення споживачу, що їхня продукція має високу якість, так з закордонних джерел величезні витрати на ці роботи складають близько одного – 2,5% усіх затрат підприємств виготовлювачів.

У деяких випадках витрати навіть порівняні з витратами на дослідження самої якості. Це робиться не випадково, тому що сертифікація є дуже ефективним засобом розвитку торгово-економічних зв'язків країн, просування продукції підприємства на зовнішній і внутрішній ринок збуту, а також закріплення них на досить тривалий період часу. Саме все це визначило широке поширення сертифікації.

Сертифікація з'явилася в зв'язку з необхідністю захистити внутрішній ринок від продукції, непридатної до використання. Питання безпеки, захисту здоров'я і навколишнього середовища, змушують законодавчу базу з одного боку, встановлювати відповідальність постачальника (виробника, продавця і так далі) за введення в обіг недоброякісної продукції, а з іншого боку встановлювати обов'язкові до виконання мінімальні вимоги, що стосуються характеристик продукції, що вводиться в обіг. Це також відноситься до сфери захисту інформації.

До першого відносяться такі законодавчі акти, як наприклад Закон України “Про захист прав споживачів”, чи Закон “Про відповідальність за продукцію”, прийнятий у країнах Європейського Співтовариства. Закони, що встановлюють мінімальні вимоги по характеристиках, можуть відноситися в цілому до групи продукції чи до окремих її параметрів. Прикладом таких законів можуть стати закони “Про електромагнітну сумісність” та інше.

Таким чином встановлюється обмеження на введення в обіг продукції, що у цілому чи по яких-небудь параметрів підпадає під дію законодавчих актів. При цьому зазначають,

що продукція попадає законодавчо регульовану область. Якщо характеристики продукції в цілому і частково не підпадають під дію національних законів, то така продукція може вільно переміщатися в межах відповідного ринку, і при цьому зазначається, що продукція попадає в область, законодавчо нерегульовану.

Для введення в обіг продукції, що підпадає в законодавчу регульовану область, потрібно офіційне підтвердження того, що вона відповідає усім пред'явленим законодавством вимогам. Однією з форм такого підтвердження є сертифікація продукції, проведена незалежною третьою стороною (перша виготовлювач, друга споживач).

У випадку отримання позитивного результату у процесі сертифікації видається документ, який називається "сертифікат відповідності", що підтверджує відповідність продукції всім вимогам, установленим національним законодавством. Даний документ є допуском на ринок у законодавчо регульованій області.

Продукція законодавчо не регульованій області може безпосередньо переміщатися в середині ринку, і при цьому, до неї офіційно не пред'явлені вимоги по установленню відповідальності. Проте, у контрактній ситуації, споживач може зажадати від постачальника доказ відповідності продукції визначеним вимогам, наприклад, відповідності конкретному стандарту чи групі стандартів, відповідності специфічним вимогам, пред'явленим самим споживачем. У цьому випадку сертифікація третьою стороною також може виступати, як підтвердження виконання умов, що буде зафіксовано в сертифікаті відповідності конкретним, установленим споживачем вимогам.

Постачальник у законодавчо не регульованій області може проводити сертифікацію своєї продукції незалежною третьою стороною і за власною ініціативою. При цьому він запитує підтвердження відповідності своєї продукції характеристикам, обраним на свій розсуд. Постачальник може запросити установлення відповідності своєї продукції визначеним стандартом, визначеним технічним параметром, змісту паспорта чи рекламного матеріалу на виріб і так далі. Оскільки процедура сертифікації дуже дорога то вона може викликати або зниження прибутку постачальника, або збільшення вартості продукції, що у свою чергу може знизити її конкурентоздатність на ринку. Тому постачальник повинен чітко представляти механізм отримання вигоди з процедури сертифікації.

Відповідно визначені вісім схем сертифікації третьою стороною:

- Испити зразка продукції,
- Испити зразка продукції з наступним контролем на основі нагляду за заводськими зразками, за купованими на відповідному ринку,
- Испити зразка продукції з наступним контролем на основі нагляду за заводськими зразками,

- Испити зразка продукції на основі нагляду за зразками, придбаними на відповідному ринку й отриманими з заводу,
- Испити зразка продукції й оцінка заводського керування якістю з наступним контролем на основі нагляду за заводським керуванням якістю й іспитів зразків, отриманих із заводу і відкритого ринку,
- Тільки оцінка заводського керування якістю,
- Перевірка партії виробів,
- Стовідсотковий контроль.

Застосування Українськими підприємствами сертифікації продукції в ринкових умовах дає наступні переваги:

- Забезпечує довіру внутрішніх і закордонних споживачів до якості продукції,
- Полегшує і спрощує вибір необхідної продукції споживачеві,
- Забезпечує споживачу одержати об'єктивної інформації про якість продукції,
- Сприяє більш тривалому успіху і захисту конкуренції з виготовлювачами не сертифікованої продукції,
- Зменшує імпорт у країну аналогічної продукції,
- Запобігає надходженню в країну імпортової продукції невідповідного ринку якості,
- Стимулює поліпшення якості НТД шляхом встановлення в ній більш прогресивних вимог,
- Сприяє підвищенню організаційно-технічного рівня виробництва,
- Стимулює прискорення НТД.

Уся сертифікаційна діяльність здійснюється у відповідності системі, що має власні правила і керівні положення.

Для аналізу вартості величини засобів, затрачених на підтримку якості продукції, використовується різна інформація але перш ніж перейти до її збору варто визначити, яке призначення цієї інформації.

Мета збору даних у процесі вартісного аналізу якості може полягати в наступному:

- Виявлення конкурентоспроможності продукції на існуючих ринках,
- Визначення розмірів необхідних капіталовкладень,
- Виявлення взаємозв'язків витрат на якість продукції і результатів господарської діяльності підприємства,
- Зниження витрат на одиницю продукції при збереженні її колишньої якості,
- Зниження витрат на вироби при одночасному поліпшенні та інших властивостей,

- Визначення величини витрат по видах для зміни їхньої структури,
- Збільшення обсягу виробництва без зниження якості продукції з колишнього обсягу ресурсів за рахунок зменшення і ліквідації відходів,
- Аналіз відхилень від установлених вимог,
- Контроль продукції,
- Установлення ціни на продукцію та інше.

Звідки видно, що частина даних про якість, що стосується технічних особливостей виробу та його виробництва знаходиться на підприємстві – виготовлювачі, а інше – на конкуруючому підприємстві чи в сфері реалізації, тобто зовнішньому середовищі.

Дані для аналізу витрат на якість можуть бути первинними, як правило, це технічні та інші параметри виробів, що містяться в ТУ, ДСТУ, сертифікатах і інших документах, що підтверджують якість продукції і вторинними, що виходять у результаті обробки первинних.

Дані мають потребу в обробці. Для цього необхідно зареєструвати джерело інформації (дату, коли вона збиралася, працівника, що робив операцію, верстат на якому проводилася обробка, партію використовуваних матеріалів і т. п.). Реєструвати інформацію в таблицях, що полегшує і прискорює обчислення статистичних показників, використовуваних при прийнятті оперативних управлінських рішень і для подальшого більш глибокого статистико-математичного аналізу за взаємозв'язків і тенденцій.

На сьогодні сертифікати в Україні відсутні. Для засобів захисту інформації, програмного забезпечення та криптографічних систем надається висновок державної експертизи, а для комп'ютерної техніки комплексних систем захисту та приміщень видаються декларації.

Технічні, криптографічні, програмні та інші засоби призначенні для захисту, відомостей, які складають державну таємницю засобів, в яких вони реалізовані, а також засоби контролю ефективності захисту інформації, яку здійснюють ці засоби інформації, підлягають державній експертизі.

Вказані засоби підлягають обов'язковій державній експертизі, яка проводиться в рамках системи контролю відповідності встановленим нормам засобів захисту інформації.

Учасниками процесу державної експертизи є:

- Центральний орган по проведенню державної експертизи (ДЕ) засобів захисту інформації;
- Органи по проведенню ДЕ засобів ЗІ по відповідній продукції;

- Випробувальні лабораторії, які поводять випробовування засобів ЗІ відповідної продукції;

- Виробник – продавець, виробник.

Система ДЕ засобів ЗІ представляє собою сукупність учасників ДЕ, здійснюючих її по встановленим правилам.

Органи по ДЕ засобів ЗІ:

- Здійснює ДЕ засобів ЗІ, видає висновки ДЕ, декларації та ліцензії на застосування цих засобів та вносить їх у державний реєстр і веде їх облік;

- Припиняє або відміняє виданих ним висновків ДЕ та декларацій на застосування засобів Зі;

- Приймає рішення на проведення повторних ДЕ при змінах у технології виготовлення та конструкції засобів ЗІ, які пройшли ДЕ;

- Формує фонд нормативних документів, необхідних щодо проведення ДЕ;

- Надає виробнику за їх вимогою необхідну інформацію у межах своєї компетенції.

Випробовувані лабораторії проводять випробування засобів ЗІ та по їх результатам оформлюють висновки та протоколи, які направляють у відповідний орган та виробнику.

Випробувальна лабораторія есе відповідальність за повноту випробувань засобів ЗІ та достовірність їх результатів. Виробник:

- Виробляє або реалізує засоби ЗІ тільки при наявності висновка державної експертизи;

- Повідомляє орган ДЕ щодо змін у технології виготовлення та конструкції засобів Зі, що пройшли ДЕ;

- Надає дані супроводжувальних технічних документах відомості щодо проведення ДЕ та нормативних документах, яким засоби ЗІ повинні відповідати, а також забезпечити доведення цієї інформації до користувача;

- Застосовують висновок ДЕ, керуючись законодавством та правилами встановленими для даної системи ДЕ;

- Забезпечує безперешкодне виконання своїх обов'язків посадовим особам органів ДЕ та контроль за продукцією, яка пройшла ДЕ;

- Припиняє реалізацію засобів ЗІ при невідповідності їх вимогам нормативних документів або по закінченню строку дії висновка ДЕ, а також у випадку припинення дії висновка або його відміни.

Виробник повинен мати ДЕ (мати ліцензію) на відповідний вид діяльності. Виробник для отримання висновку ДЕ направляє у орган, який проводить ДЕ заяву на

проведення ДЕ, до якої можуть бути додані схеми проведення ДЕ, державні стандарти та інші нормативні та методологічні документи, вимоги, яким повинні відповідати засоби ЗІ.

Орган ДЕ у місячний термін, після отримання заяви на проведення ДЕ направляє виробнику рішення щодо проведення ДЕ з наданням схеми її проведення, випробувальної лабораторії, яка буде здійснювати випробовування засобів ЗІ, та нормативні документи, вимоги яких повинні відповідати випробувані засоби ЗІ, а при необхідності рішення о проведенні та термінах проведення перевірки виробництва засобів захисту.

Щодо визначення закордонних сертифікатів виробник направляє його копію та заяву на визначення сертифіката УДЕ, яка повідомляє виробнику щодо визначення сертифікату або необхідності проведення випробувань ДЕ в терміни не пізніше одного місяця з моменту отримання вказаних документів. Випробування закордонних засобів ЗІ та ДЕ проводиться по тим самим правилам, що і вітчизняні. Основними схемами ДЕ засобів ЗІ є:

- Щодо одиночних зразків засобів ЗІ – проведення випробувань цих зразків по захисту інформації;

- Щодо серійного виробництва засобів ЗІ – проведення типових випробувань засобів ЗІ на відповідність вимогам по захисту інформації та наступного інспекційного контролю за стабільністю характеристик засобів ЗІ, які пройшли ДЕ, визначаючи виконання цих вимог. Крім того допускається попередня перевірка виробництва спеціально розробленої програми.

Строк дії висновка ДЕ не може перевершувати п'ять років.

Випробування зразків ЗІ, ДЕ проводяться на зразках, технологіях виробництва та конструкція яких повинна відповідати зразкам, які поставляються користувачу.

У окремих випадках по узгодженню з ДЕ допускається проведення випробувань на випробувальній базі виробника. При цьому ДЕ визначає умови, які необхідні щодо забезпечення об'єктивних результатів випробувань.

Виробнику повинні бути надані можливості ознайомитись з умовами випробувань та зберігання зразків засобів ЗІ у випробувальній лабораторії.

ДЕ має право припиняти або анулювати дію висновка у наступних випадках:

- Зміни у нормативних та методичних документах з ЗІ у частині вимог до засобів ЗІ, методам випробувань і контролю;

- Зміни у технологіях виготовлення конструкції, комплектності засобів ЗІ та системи контролю їх якості;

- Відмова виробника забезпечувати безперешкодне виконання своїх повноважень особам, які здійснюють державний контроль та нагляд, інспекційний контроль за проведенням ДЕ засобами ЗІ, які пройшли ДЕ.

Інспекційний контроль за засобами ЗІ, які пройшли ДЕ, здійснюють органи, які проводили ДЕ цих засобів. Орган ДЕ, який здійснює Де засобів ЗІ, несе відповідальність в установленому законодавством порядку за виконання покладених на них обов'язків.

Схеми висновку державної експертизи засобів обчислювальної техніки та техніки захисту інформації

№	Схеми	Зміст висновку державної експертизи (ВДЕ)
1	Схема №1	ВДЕ одиночного виробу
2	Схема №2	ВДЕ серії продукції з зазначенням розміру виготовленої партії
3	Схема №3	ВДЕ серійної продукції та технічний нагляд над її виробництвом (термін дії ВДЕ до одного року, технічний нагляд здійснюється через пів року після видачі ВДЕ)
4	Схема №4	ВДЕ продукції, яка випускається серійно. Ця схема передбачає проведення атестації виробництва, ВДЕ випробовування зразків, взятих на підприємстві – виготовлення даної продукції, технічний огляд.
5	Схема №5	ВДЕ продукції, яка випускається серійно. Ця схема передбачає ВДЕ системи якості виробництва, ВДЕ випробовування зразків, взятих на підприємствах виробнику та технічний огляд.

Розділ 2

Основна мета лабораторних робіт – сприяння засвоєнню набутих знань, умінь і навичок із забезпечення інформаційної безпеки держави.

Навчальні заняття проводяться згідно з навчальним розкладом. Група приходить інструктаж за правилами техніки безпеки, пожежної безпеки та ділить на бригади по 2 або більше студентів. На першому навчальному занятті бригада отримує номер відповідно робочого місця.

До початку навчального заняття студент повинен вивчити порядок виконання роботи, ознайомитися з літературою, яка має відношення до неї.

Ступінь підготовки студента до виконання поточної роботи перевіряється викладачем. З метою самоконтролю при підготовці до виконання роботи, рекомендується відповісти на запитання, які наводяться в кінці кожної лабораторної роботи. Студент, який отримав незадовільну оцінку під час перевірки, до виконання роботи не допускається. Студент, який не здав попередню роботу, до наступної не допускається.

Звіт про лабораторну роботу оформляється на аркушах білого паперу формату А4 (210 x 297 мм) та зброшуровано таким чином, щоб аркуші були щільно стиснуті. Не допускається їх з'єднання скріпкою.

Текст звіту слід оформлювати українською мовою і він повинен мати такі береги: 30мм – лівий; 10мм – правий; 20мм – верхній та нижній.

Текст звіту про роботу виконується за допомогою комп'ютера та перетворений у візуальну форму подання електронного документа. Друкується на одній стороні аркуша через 1,5 міжрядковий інтервал, текст вирівнюється по ширині аркуша. Візуальною формою подання електронного документа є відображення даних, які він містить, на папері у формі, придатній для приймання його змісту людиною.

Сторінки тексту звіту про роботу слід нумерувати арабськими цифрами, додержуючись валової нумерації по всьому тексту. Номер сторінки

проставляється у правому верхньому березі сторінки без крапки в кінці. Титульна сторінка включається до загальної нумерації сторінок тексту звіту. Номер сторінки на титульному аркуші не проставляється.

Текст звіту про роботу повинен бути викладений стисло, грамотно, зрозуміло, без повторів та вживання слів і зворотів, які не несуть смислового навантаження і оформлений у вигляді поєднання суцільного тексту і таблиць при необхідності.

Текст звіту про роботу повинен містити:

- мету роботи;
- суть звіту про роботу;

- висновки.

Суть звіту про роботу – це викладення відомостей про предмет практичної роботи, котрий є необхідний і достатнім для розкриття сутності даної роботи (опис: теорії, методів роботи тощо) та її результатів.

При викладенні суті звіту особливу увагу приділяють новизні в роботу, а також питання безпеки інформації тощо.

Висновки вміщують безпосередньо після викладення суті звіту про роботу, починаючи з нової строки.

У висновках наводять оцінку одержаних результатів роботи.

Якщо текст висновків має різні смислові аспекти, або містить декілька висновків його треба розбити на розділи, підрозділи, пункти, підпункти, які нумерувати арабськими цифрами і друкують з абзацу.

Зразок оформлення титульної сторінки звіту про роботу наведено нижче.

Розділ 3
Лабораторні роботи

Лабораторна робота №1

Закони України «Про Державну службу спеціального зв'язку та захисту інформації України».

Мета роботи: Поглиблення знань щодо Закону України «Про Державну службу спеціального зв'язку та захисту інформації України».

Порядок виконання лабораторної роботи:

1. Включити персональний комп'ютер.
2. Отримати доступ до internet.
3. Завдання щодо виконання лабораторної роботи №1 знайти за номером бригади у табл. 3.1.
4. Знайти інформацію відповідно до завдання.
5. Обробити отриману інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3.1.

Завдання для виконання лабораторної роботи №1.

Номер бригади	Завдання
1	Знайти матеріали щодо Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», проаналізуйте їх і сформулюйте мету та задачі, які вирішує цей закон
2	Знайти матеріали щодо Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», проаналізуйте їх і визначте статус Державної служби
3	Знайти матеріали щодо Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», проаналізуйте їх і сформулюйте обов'язки Державної служби
4	Знайти матеріали щодо Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», проаналізуйте їх і сформулюйте права Державної служби
5	Знайти матеріали щодо Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», проаналізуйте їх і сформулюйте основні принципи діяльності Державної служби
6	Знайти матеріали щодо Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», проаналізуйте їх і визначте основні завдання Державної служби
7	Знайти матеріали щодо Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», проаналізуйте їх і визначте особливості застосування цього Закону України

Лабораторна робота №2 Закони України «Про стандартизацію»

Мета роботи: Поглиблення знань щодо Закону України «Про стандартизацію».

Порядок виконання лабораторної роботи:

1. Включити персональний комп'ютер.
2. Отримати доступ до internet.
3. Завдання щодо виконання лабораторної роботи №2 знайти за номером бригади у табл. 3.2.
4. Знайти інформацію відповідно до завдання.
5. Обробити отриману інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3.2.

Завдання для виконання лабораторної роботи №2.

Номер бригади	Завдання
1	Знайти матеріали щодо Закону України «Про стандартизацію», проаналізуйте їх і сформулюйте мету та задачі, які вирішує цей закон
2	Знайти матеріали щодо Закону України «Про стандартизацію», проаналізуйте їх і визначте яким чином визначається порядок створення, впровадження та використання стандартів у різних галузях економіки та громадського життя
3	Знайти матеріали щодо Закону України «Про стандартизацію», проаналізуйте їх і визначте мету та принципи на яких базується державна політика у сфері стандартизації
4	Знайти матеріали щодо Закону України «Про стандартизацію», проаналізуйте їх і визначте принципи організації стандартизації
5	Знайти матеріали щодо Закону України «Про стандартизацію», проаналізуйте їх і визначте основні засади, процедури розроблення і прийняття та застосування національних стандартів, кодексів усталеної практики та змін до них
6	Знайти матеріали щодо Закону України «Про стандартизацію», проаналізуйте їх і визначте інформаційне забезпечення та право власності на національні стандарти, кодекси усталеної практики та каталоги і використання коштів, одержаних від їх реалізації
7	Знайти матеріали щодо закону України «про стандартизацію», проаналізуйте їх і визначте особливості міжнародного співробітництва та фінансування робіт із стандартизації

Лабораторна робота №3
Закони України «Про електронні довірчі послуги»

Мета роботи: Поглиблення знань щодо Закону України «Про електронні довірчі послуги».

Порядок виконання лабораторної роботи:

1. Включити персональний комп'ютер.
2. Отримати доступ до internet.
3. Завдання щодо виконання лабораторної роботи №3 знайти за номером бригади у табл. 3.3.
4. Знайти інформацію відповідно до завдання.
5. Обробити отриману інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3.3.

Завдання для виконання лабораторної роботи №3.

Номер бригади	Завдання
1	Знайти матеріали щодо Закону України «Про електронні довірчі послуги», проаналізуйте їх і визначте вимоги до кваліфікованого надавача електронних довірчих послуг
2	Знайти матеріали щодо Закону України «Про електронні довірчі послуги», проаналізуйте їх і визначте вимоги до порядку проведення ідентифікації особи під час ідентифікації та видачі сертифікату відкритого ключа
3	Знайти матеріали щодо Закону України «Про електронні довірчі послуги», проаналізуйте їх і визначте вимоги до засобів та схем електронної ідентифікації
4	Знайти матеріали щодо Закону України «Про електронні довірчі послуги», проаналізуйте їх і визначте вимоги до засвідчувального центру
5	Знайти матеріали щодо Закону України «Про електронні довірчі послуги», проаналізуйте їх і визначте вимоги до центрального засвідчувального органу
6	Знайти матеріали щодо Закону України «Про електронні довірчі послуги», проаналізуйте їх і визначте вимоги щодо скасування, блокування та поновлення посиленого сертифікату відкритого ключа
7	Знайти матеріали щодо Закону України «Про електронні довірчі послуги», проаналізуйте їх і визначте правила діяльності центрального засвідчувального органу

Лабораторна робота №4

Декрет Кабінету Міністрів України «Про стандартизацію та сертифікацію».

Мета роботи: Поглиблення знань щодо Декрету Кабінету Міністрів України «Про стандартизацію та сертифікацію».

Порядок виконання лабораторної роботи:

1. Включити персональний комп'ютер.
2. Отримати доступ до internet.
3. Завдання щодо виконання лабораторної роботи №4 знайти за номером бригади у табл. 3.4.
4. Знайти інформацію відповідно до завдання.
5. Обробити отриману інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3.4.

Завдання для виконання лабораторної роботи №4.

Номер бригади	Завдання
1	Знайти матеріали щодо Декрету Кабінету Міністрів України «Про стандартизацію та сертифікацію», проаналізуйте їх і визначте види та методи сертифікації продукції
2	Знайти матеріали щодо Декрету Кабінету Міністрів України «Про стандартизацію та сертифікацію», проаналізуйте їх і визначте державну систему сертифікації
3	Знайти матеріали щодо Декрету Кабінету Міністрів України «Про стандартизацію та сертифікацію», проаналізуйте їх і визначте, що підлягає обов'язковій сертифікації
4	Знайти матеріали щодо Декрету Кабінету Міністрів України «Про стандартизацію та сертифікацію», проаналізуйте їх і визначте в чому полягає відповідальність органів сертифікації
5	Знайти матеріали щодо Декрету Кабінету Міністрів України «Про стандартизацію та сертифікацію», проаналізуйте їх і визначте принципи видачі сертифікату
6	Знайти матеріали щодо Декрету Кабінету Міністрів України «Про стандартизацію та сертифікацію», проаналізуйте їх і визначте принципи внесення у реєстр свідоцтва про видачу сертифікату
7	Знайти матеріали щодо Декрету Кабінету Міністрів України «Про стандартизацію та сертифікацію», проаналізуйте їх і визначте вимоги до змісту інформації про рішення щодо видачі сертифікату

Лабораторна робота №5
Вивчення стандартів України щодо забезпечення захисту інформації.

Мета роботи: Поглиблення теоретичних знань щодо вивчення стандартів України щодо забезпечення захисту інформації.

Порядок виконання лабораторної роботи:

1. Включити персональний комп'ютер.
2. Отримати доступ до internet.
3. Завдання щодо виконання лабораторної роботи №5 знайти за номером бригади у табл. 3.5.
4. Знайти інформацію відповідно до завдання.
5. Обробити отриману інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3.5.

Завдання для виконання лабораторної роботи №5.

Номер бригади	Завдання
1	Знайти матеріали з ДСТУ 3396.0-96 та ДСТУ 3396.1-96, проаналізувати їх та сформулювати недоліки та переваги
2	Знайти матеріали з ДСТУ 4145-2002, проаналізувати їх та сформулювати недоліки та переваги. Провести порівняльний аналіз цього стандарту з існуючими стандартами інших країн
3	Знайти матеріали з ДСТУ 3918-1999, проаналізувати їх та сформулювати недоліки та переваги. Провести порівняльний аналіз цього стандарту з існуючими стандартами інших країн
4	Знайти матеріали з ДСТУ 3396.0-96, проаналізувати їх та сформулювати недоліки та переваги. Провести порівняльний аналіз цього стандарту з існуючими стандартами інших країн
5	Знайти матеріали з ДСТУ 3396.1-96, проаналізувати їх та сформулювати недоліки та переваги. Провести порівняльний аналіз цього стандарту з існуючими стандартами інших країн

Лабораторна робота №6
Вивчення стандартів України групи ДСТУ ІСО/ІЕС TR 13335.

Мета роботи: Поглиблення теоретичних знань щодо вивчення стандартів України групи ДСТУ ІСО/ІЕС TR 13335.

Порядок виконання лабораторної роботи:

1. Включити персональний комп'ютер.
2. Отримати доступ до internet.
3. Завдання щодо виконання лабораторної роботи №6 знайти за номером бригади у табл. 3.6.
4. Знайти інформацію відповідно до завдання.
5. Обробити отриману інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3.6.

Завдання для виконання лабораторної роботи №6.

Номер бригади	Завдання
1	Знайти матеріали щодо стандарту України ДСТУ ІСО/ІЕС TR 13335-1:2003, проаналізувати їх та сформулювати їх недоліки та переваги
2	Знайти матеріали щодо стандарту України ДСТУ ІСО/ІЕС TR 13335-2:2003, проаналізувати їх та сформулювати їх недоліки та переваги
3	Знайти матеріали щодо стандарту України ДСТУ ІСО/ІЕС TR 13335-3:2003, проаналізувати їх та сформулювати їх недоліки та переваги
4	Знайти матеріали щодо стандарту України ДСТУ ІСО/ІЕС TR 13335-4:2005, проаналізувати їх та сформулювати їх недоліки та переваги
5	Знайти матеріали щодо стандарту України ДСТУ ІСО/ІЕС TR 13335-5:2005, проаналізувати їх та сформулювати їх недоліки та переваги
6	Знайти матеріали щодо стандартів України ДСТУ ІСО/ІЕС TR 13335-3:2003 та ДСТУ ІСО/ІЕС TR 13335-5:2005 проаналізувати їх та сформулювати їх відмінності та спільність
7	Знайти матеріали щодо стандартів України ДСТУ ІСО/ІЕС TR 13335-2:2003 та ДСТУ ІСО/ІЕС TR 13335-4:2005 проаналізувати їх та сформулювати їх відмінності та спільність

Лабораторна робота №7
Вивчення міжнародних стандартів, що забезпечують захист інформації та використовуються в Україні.

Мета роботи: Поглиблення теоретичних знань щодо вивчення міжнародних стандартів, що забезпечують захист інформації та використовуються в Україні.

Порядок виконання лабораторної роботи:

1. Включити персональний комп'ютер.
2. Отримати доступ до internet.
3. Завдання щодо виконання лабораторної роботи №7 знайти за номером бригади у табл. 3.7.
4. Знайти інформацію відповідно до завдання.
5. Обробити отриману інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3.7.

Завдання для виконання лабораторної роботи №7.

Номер бригади	Завдання
1	Знайти матеріали з ISO/IEC 27033-1, проаналізувати їх та сформулювати їх недоліки та переваги
2	Знайти матеріали з ISO/IEC 18043, проаналізувати їх та сформулювати їх недоліки та переваги
3	Знайти матеріали з ISO/IEC 18044, проаналізувати їх та сформулювати їх недоліки та переваги
4	Знайти матеріали з ISO/IEC 18045, проаналізувати їх та сформулювати їх недоліки та переваги
5	Знайти матеріали з ISO/IEC 17799-2000, проаналізувати їх та сформулювати їх недоліки та переваги
6	Знайти матеріали з ISO/IEC 27033-2, проаналізувати їх та сформулювати їх недоліки та переваги
7	Знайти матеріали з ISO/IEC 27033-5, проаналізувати їх та сформулювати їх недоліки та переваги

Лабораторна робота №8

Вивчення нормативних документів України щодо забезпечення захисту інформації.

Мета роботи: Поглиблення теоретичних знань щодо вивчення нормативних документів України щодо забезпечення захисту інформації.

Порядок виконання лабораторної роботи:

1. Включити персональний комп'ютер.
2. Отримати доступ до internet.
3. Завдання щодо виконання лабораторної роботи №8 знайти за номером бригади у табл. 3.8.
4. Знайти інформацію відповідно до завдання.
5. Обробити отриману інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3.8.

Завдання для виконання лабораторної роботи №8.

Номер бригади	Завдання
1	Знайти матеріали з НДТЗІ 1.1-002-99, проаналізувати їх та сформулювати їх недоліки та переваги
2	Знайти матеріали з НДТЗІ 1.4-001-2000, проаналізувати їх та сформулювати їх недоліки та переваги
3	Знайти матеріали з НДТЗІ 1.6-005-2013, проаналізувати їх та сформулювати їх недоліки та переваги
4	Знайти матеріали з НДТЗІ 2.5-008-2002, проаналізувати їх та сформулювати їх недоліки та переваги
5	Знайти матеріали з НДТЗІ 3.3-001-07, проаналізувати їх та сформулювати їх недоліки та переваги
6	Знайти матеріали з НДТЗІ 1.1-002-99 та НДТЗІ 1.4-004-2000 та сформулюйте їх відмінності та спільність
7	Знайти матеріали з НДТЗІ 1.6-005-2013 та НДТЗІ 2.5-008-2002 та сформулюйте їх відмінності та спільність

Лабораторна робота №9
Вивчення нормативних документів України групи 2.5.

Мета роботи: Поглиблення теоретичних знань щодо вивчення нормативних документів України групи 2.5.

Порядок виконання лабораторної роботи:

1. Включити персональний комп'ютер.
2. Отримати доступ до internet.
3. Завдання щодо виконання лабораторної роботи №9 знайти за номером бригади у табл. 3.9.
4. Знайти інформацію відповідно до завдання.
5. Обробити отриману інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3.9.

Завдання для виконання лабораторної роботи №9.

Номер бригади	Завдання
1	Знайти матеріали з НДТЗІ 2.5-004-99, проаналізувати їх та сформулювати їх недоліки та переваги
2	Знайти матеріали з НДТЗІ 2.5-005-99, проаналізувати їх та сформулювати їх недоліки та переваги
3	Знайти матеріали з НДТЗІ 2.5-004-99 та сформулюйте критерії оцінки захищеності комп'ютерних систем
4	Знайти матеріали з НДТЗІ 2.5-005-99, проаналізувати їх та сформулювати вимоги до класифікації автоматизованих систем
5	Знайти матеріали з НДТЗІ 2.5-005-99, проаналізувати їх та сформулювати вимоги до стандартних функціональних профілів захищеності
6	Знайти матеріали з НДТЗІ 2.5-004-99 та НДТЗІ 2.5-005-99 та сформулюйте їх відмінності та спільність відносно протидії несанкціонованому доступу
7	Знайти матеріали з НДТЗІ 2.5-004-99 та НДТЗІ 2.5-005-99 та сформулюйте їх відмінності та спільність відносно підвищення захищеності в комп'ютерних системах

Лабораторна робота №10

Методи та порядок проведення сертифікації у сфері захисту інформації в Україні.

Мета роботи: Поглиблення знань щодо методів та порядку проведення сертифікації у сфері захисту інформації в Україні.

Порядок виконання лабораторної роботи:

1. Включити персональний комп'ютер.
2. Отримати доступ до internet.
3. Завдання щодо виконання лабораторної роботи №10 знайти за номером бригади у табл. 3.10.
4. Знайти інформацію відповідно до завдання.
5. Обробити отриману інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3.10.

Завдання для виконання лабораторної роботи №10.

Номер бригади	Завдання
1	Знайти матеріали щодо сертифікації в Україні, проаналізуйте їх і сформулюйте задачі сертифікації
2	Знайти матеріали щодо сертифікації в Україні, проаналізуйте їх і визначте схеми сертифікації третьої сторони
3	Знайти матеріали щодо сертифікації в Україні, проаналізуйте їх і визначте мету збору даних у процесі аналізу якості продукції
4	Знайти матеріали щодо сертифікації в Україні, проаналізуйте їх і визначте вимоги до державної експертизи
5	Знайти матеріали щодо сертифікації в Україні, проаналізуйте їх і визначте основні схеми проведення державної експертизи засобів захисту інформації
6	Знайти матеріали щодо сертифікації в Україні, проаналізуйте їх і визначте вимоги до випробувальної лабораторії
7	Знайти матеріали щодо сертифікації в Україні, проаналізуйте їх і визначте вимоги до виробника засобів захисту інформації

Лабораторна робота №11
Міжнародний досвід у сфері сертифікації.

Мета роботи: Поглиблення знань щодо міжнародного досвіду у сфері сертифікації.

Порядок виконання лабораторної роботи:

1. Включити персональний комп'ютер.
2. Отримати доступ до internet.
3. Завдання щодо виконання лабораторної роботи №11 знайти за номером бригади у табл. 3.11.
4. Знайти інформацію відповідно до завдання.
5. Обробити отриману інформацію.
6. Оформити звіт.
7. Зробити висновки.

Таблиця 3.11.

Завдання для виконання лабораторної роботи №11.

Номер бригади	Завдання
1	Знайти матеріали щодо сертифікації у США, проаналізуйте їх і сформулюйте їх особливості
2	Знайти матеріали щодо сертифікації у Канаді, проаналізуйте їх і сформулюйте їх особливості
3	Знайти матеріали щодо сертифікації у Великобританії, проаналізуйте їх і сформулюйте їх особливості
4	Знайти матеріали щодо сертифікації у Німеччині, проаналізуйте їх і сформулюйте їх особливості
5	Знайти матеріали щодо сертифікації у Франції, проаналізуйте їх і сформулюйте їх особливості
6	Знайти матеріали щодо сертифікації у Польщі, проаналізуйте їх і сформулюйте їх особливості
7	Знайти матеріали щодо сертифікації у Італії, проаналізуйте їх і сформулюйте їх особливості

Перелік використаних джерел

1. Конституція України. Офіційне видання Верховної Ради України.
2. Сердюков В.В. Правові основи охорони інформації: підручник / В.В. Сердюков, О.М. Стаднік, З.Б. Живко; за ред. В.О. Хорошка. – Вид. 2-е, допов. і переробл. – К. : ДУІКТ, 2009. – 355 с.
3. Артемов В.Ю. Нормативно-правовий довідник з охорони інформації в Україні: в 6 т. Т. 1. Законодавча база охорони інформації / В.Ю. Артемов, О.С. Ленков, А.С. Пашков, О.М.Стаднік, В.О. Хорошко. – К., 2010. – 270 с.
4. Артемов В.Ю. Нормативно-правовий довідник з охорони інформації в Україні: в 6 т. Т. 2. Організаційно-правові засади охорони інформації / В.Ю. Артемов, О.С. Ленков, А.С. Пашков, О.М.Стаднік, В.О. Хорошко. – К., 2010. – 349 с.
5. Артемов В.Ю. Нормативно-правовий довідник з охорони інформації в Україні: в 6 т. Т. 3. Правові основи охорони інформації / В.Ю. Артемов, О.С. Ленков, А.С. Пашков, О.М.Стаднік, В.О. Хорошко. – К., 2010. – 319 с.
6. Інформаційна безпека (соціально-правові аспекти) : підручник / В.В. Остроухов, В.М. Петрик, М.М. Присяжнюк, Я.М. Жарков та ін.; за заг. ред. Є. Д. Скулиша. – К. : КНТ, 2010. – 776 с.
7. Ортинський В. Л. Економічна безпека підприємств, організацій та установ : Навчальний посібник / В.Л. Ортинський, І.С. Керницький, З.Б. Живко. – К. : Правова єдність, 2009. – 544 с.
8. Грайворонський М.В. Безпека інформаційно-комунікаційних систем. / Грайворонський М.В., Новіков О.М.– К.: Видавнича група ВНУ, 2009. – 608 с.
9. Головань С.М. Нормативно-правове забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Л.М. Щербак ; [під ред. В.О. Хорошка] – Луганськ : Вид. "Ноулідж". – 2012. – 480 с.
10. Дудикевич В.Б. Правові основи захисту інформації: конспект лекцій / В.Б. Дудикевич, В.С. Зачепило, В.В. Хома – Львів: Видавництво Національного університету "Львівська політехніка", 2002, – 67 с.
11. Бобало Ю.Я., Горбатий І.В., Кіселичник М.Л. та інші. Інформаційна безпека – Львів: Вид. Львівської політехніки, 2019. – 580 с.
12. Іванченко Є.В. Забезпечення інформаційної держави / Є.В. Іванченко, І.С. Іванченко, В.О. Хорошко, Ю.Є. Хохлачова – К: Вид. НАУ, 2016. – 256 с.