Адміністративно-правові заходи захисту інформації в органах публічної влади.

Зміст

[1.Класифікація інформації. 2](#_gjdgxs)

[2. Адміністративно-правові заходи захисту інформації в органах публічної](#_30j0zll)

[влади.](#_30j0zll) 4

[2.1 Органи публічної влади.](#_1fob9te)  4

[2.2 Об'єкти та суб'єкти інформаційної безпеки. 5](#_3znysh7)

[2.3 Заходи захисту інформації в органах публічної влади. 6](#_1t3h5sf)

3.Пере[лік використаних джерел. 9](#_3whwml4)

# 1.Класифікація інформації.

За режимом доступу інформація в автоматизованій системі поділяється на:

* відкриту;
* з обмеженим доступом.

Відкрита інформація поділяється на відкриту, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкриту, яка такого захисту потребує. До другої слід відносити інформацію, важливу для особи, суспільства і держави (відповідно до Концепції технічного захисту інформації в Україні), важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків.

За правовим режимом інформація з обмеженим доступом поділяється на таємну та конфіденційну.

Інформація, що становить державну таємницю, в свою чергу, поділяється на категорії відповідно до Закону України “Про державну таємницю”.

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

* у сфері оборони;
* у сфері економіки, науки і техніки;
* у сфері зовнішніх відносин;
* у сфері державної безпеки та охорони правопорядку.

Правила доступу до конфіденційної інформації встановлює її власник. Конфіденційна інформація може мати велику цінність для її власника, втрата або передача якої іншим особам може завдати організації (власнику) значних збитків.

Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ - надано статус конфіденційної (для службового користування). Порядок обліку, зберігання і використання документів та інших носіїв інформації, що містять зазначену інформацію, визначається Кабінетом Міністрів України.

# 2. Адміністративно-правові заходи захисту інформації в органах публічної влади.

## 2.1 Органи публічної влади.

Органи публічної влади виступають владними інститутами політично організованого [суспільства](https://uk.wikipedia.org/wiki/%D0%A1%D1%83%D1%81%D0%BF%D1%96%D0%BB%D1%8C%D1%81%D1%82%D0%B2%D0%BE) сучасного типу.

Однією з ознак держави є наявність [населення](https://uk.wikipedia.org/wiki/%D0%9D%D0%B0%D1%81%D0%B5%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F), що певним чином організоване та самоорганізоване за допомогою публічних правил поведінки. Цей процес самоорганізації здійснюється через мережу органів публічної влади. Незважаючи на очевидну однорідність функцій, у різних країнах ці органи пройшли свій шлях становлення і становлять собою продукт даного суспільства.

Традиційно, органи публічної влади розподіляються на органи державної влади та [органи місцевого самоврядування](https://uk.wikipedia.org/wiki/%D0%9E%D1%80%D0%B3%D0%B0%D0%BD%D0%B8_%D0%BC%D1%96%D1%81%D1%86%D0%B5%D0%B2%D0%BE%D0%B3%D0%BE_%D1%81%D0%B0%D0%BC%D0%BE%D0%B2%D1%80%D1%8F%D0%B4%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F).

В України можна говорити про такі типи органів публічної влади:

1. Система органів державної влади

2. Система органів влади Автономної Республіки Крим

- Єдиний представницький орган автономії - [Верховна Рада Автономної Республіки Крим](https://uk.wikipedia.org/wiki/%D0%92%D0%B5%D1%80%D1%85%D0%BE%D0%B2%D0%BD%D0%B0_%D0%A0%D0%B0%D0%B4%D0%B0_%D0%90%D0%B2%D1%82%D0%BE%D0%BD%D0%BE%D0%BC%D0%BD%D0%BE%D1%97_%D0%A0%D0%B5%D1%81%D0%BF%D1%83%D0%B1%D0%BB%D1%96%D0%BA%D0%B8_%D0%9A%D1%80%D0%B8%D0%BC)

- Система органів виконавчої влади автономії:

* Рада міністрів Автономної Республіки Крим - вищий виконавчий орган автономії
* міністерства і республіканські комітети - центральні виконавчі органи автономії

3. Система органів місцевого самоврядування

* Представницькі органи місцевого самоврядування.
* Виконавчі органи місцевого самоврядування.
* Органи самоорганізації населення.

Якщо виходити з поняття публічної служби, даного в [Кодексі адміністративного судочинства України](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%B4%D0%B5%D0%BA%D1%81_%D0%B0%D0%B4%D0%BC%D1%96%D0%BD%D1%96%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D0%B3%D0%BE_%D1%81%D1%83%D0%B4%D0%BE%D1%87%D0%B8%D0%BD%D1%81%D1%82%D0%B2%D0%B0_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8), до органів публічної влади також можна віднести:

* політичні партії;
* Збройні Сили України;
* дипломатичні установи України.

## 2.2 Об'єкти та суб'єкти інформаційної безпеки.

Суб'єкти – держава, що здійснює свої функції через відповідні органи; громадяни, суспільні або інші організації і об’єднання, що володіють повноваженнями щодо забезпечення інформаційної безпеки відповідно до законодавства.

Об'єкти – свідомість, психіка людини; інформаційні системи різного масштабу й різного призначення. До соціальних об’єктів інформаційної безпеки відносять особистість, колектив, державу, суспільство, світове товариство.

У залежності від об’єктного складу (особи, суспільства або держави, що є об’єктом загрози) визначають: міжнародну безпеку (безпеку багатьох держав), безпеку окремої держави, особисту безпеку (безпеку конкретної особи) та суспільну безпеку (безпека невизначеного кола осіб). У залежності від сфери суспільних відносин, що є об’єктом загрози, ми можемо виділити: інформаційну, військову, економічну, політичну, екологічну та інші види безпеки. Хоча буває дуже важко відділити один вид безпеки від іншого, або безпеку одного суб’єкта від безпеки інших суб’єктів.

Суб'єктами є:

* юридичні та фізичні особи - власники (розпорядники) інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, технічних і програмних засобів, які реалізують функції ТЗІ;
* Адміністрація Держспецзв’язку;
* територіальні органи Адміністрації Держспецзв'язку;
* навчальні заклади, науково-дослідні, науково-виробничі установи Державної служби спеціального зв'язку та захисту інформації України, підприємства, установи та організації;
* фізичні особи, які на постійній або професійній основі здійснюють діяльність, пов’язану з наданням експертних послуг, - виконавці експертних робіт з ТЗІ.

Об'єктами є:

* комплексна система захисту інформації;
* технічні та програмні засоби, які реалізують функції ТЗІ та оцінки стану захисту інформації (далі - засоби ТЗІ);
* організаційно-технічне рішення на розгортання типової складової компоненти КСЗІ в ІТС.

## 2.3 Заходи захисту інформації в органах публічної влади.

Оцінка стану захищеності в державному органі, органі місцевого самоврядування, військовому формуванні, здійснюється Держспецзв'язку.

За результатами оцінки стану захищеності складається акт оцінки стану захищеності державних інформаційних ресурсів в ІТС (далі – Акт) згідно з додатком, де викладаються результати роботи комісії та рекомендації стосовно підвищення рівня захищеності державних інформаційних ресурсів, який затверджується Головою Держспецзв'язку або його заступником за напрямом діяльності згідно з розподілом функціональних обов'язків.

З метою здійснення оцінки стану захищеності:

1.Держспецзв'язок:

* створює комісію з оцінки стану захищеності (далі – комісія);

* здійснює планування проведення оцінки стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності;

* розробляє загальну програму та методику оцінки стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності, а також окремі програми та методики оцінки захищеності залежно від виду ІТС та режиму доступу до інформації, що в ній обробляється;

* визначає перелік документів, що стосуються функціонування ІТС та підлягають аналізу під час проведення оцінки стану захищеності;

* визначає та оприлюднює на офіційному веб-сайті Держспецзв'язку у мережі Інтернет перелік спеціалізованого програмного забезпечення та програмно-апаратних засобів, які використовуються для проведення оцінки захищеності.

2. Державні органи, органи місцевого самоврядування, військові формування, підприємства, установи і організації незалежно від форм власності, в яких здійснюється оцінка стану захищеності:

* + надають комісії всі необхідні документи, що стосуються функціонування ІТС;

* + надають комісії доступ до ІТС;

* + повідомляють Держспецзв'язку про стан виконання рекомендацій, зазначених в Акті.
  + Оцінка стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності проводиться згідно з річним планом, який затверджується наказом Адміністрації Держспецзв'язку, або позапланово.

* + Планова оцінка стану захищеності проводиться в державних органах, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності не частіше ніж один раз на п'ять років.

* + Витяги з річного плану надсилаються до вказаних у ньому державних органів, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності щороку до 01 лютого.

* + Позапланова оцінка стану захищеності проводиться в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності за їх безпосередніми зверненнями та рішенням Голови Держспецзв'язку або його заступника за напрямом діяльності згідно з розподілом функціональних обов'язків.

* + Держспецзв'язку письмово повідомляє державні органи, органи місцевого самоврядування, військові формування, підприємства, установи, організації незалежно від форм власності, в яких планується здійснити оцінку стану захищеності, не менше ніж за десять діб до її початку.

# 3.Перелік використаних джерел.

1.НД ТЗІ 1.4-001-2000

2.Закону України “Про державну таємницю”.

3.Наказ від 02.12.2014 № 660 Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.