# КАБІНЕТ МІНІСТРІВ УКРАЇНИ
# ПОСТАНОВА
**від 29 березня 2006 р. № 373**
**Київ**

## Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем

*{Назва Постанови із змінами, внесеними згідно з Постановою КМ № 645 від 03.06.2022; в редакції Постанови КМ № 1531 від 26.11.2025}*

*{Із змінами, внесеними згідно з Постановами КМ*
№ 1700 від 08.12.2006
№ 938 від 07.09.2011
№ 991 від 21.10.2020
№ 92 від 08.02.2021
№ 645 від 03.06.2022
№ 1171 від 14.10.2022
№ 447 від 28.03.2025
№ 1531 від 26.11.2025*}*

Відповідно до статті 10 Закону України "Про захист інформації в інформаційно-комунікаційних системах" Кабінет Міністрів України **п о с т а н о в л я є :**

*{Вступна частина із змінами, внесеними згідно з Постановою КМ № 645 від 03.06.2022}*

Затвердити Мінімальні вимоги до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, що додаються.

*{Постановляюча частина із змінами, внесеними згідно з Постановою КМ № 645 від 03.06.2022; в редакції Постанови КМ № 1531 від 26.11.2025}*

**Прем'єр-міністр України** **Ю. ЄХАНУРОВ**

**Інд. 49**

**ЗАТВЕРДЖЕНО**
**постановою Кабінету Міністрів України**
**від 29 березня 2006 р. № 373**
**(в редакції постанови Кабінету Міністрів України**
**від 26 листопада 2025 р. № 1531)**

# МІНІМАЛЬНІ ВИМОГИ
# до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем

## Загальні положення

1. Ці Мінімальні вимоги визначають сукупність організаційних та технічних вимог до заходів захисту інформації та кіберзахисту, що підлягають впровадженню органами державної влади, іншими державними органами, органами місцевого самоврядування, державними підприємствами, установами та організаціями, які є власниками або розпорядниками інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем (далі - система), в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Вимоги до захисту інформації, що становить державну таємницю, визначаються цими Мінімальними вимогами та законодавством у сфері охорони державної таємниці.

2. Дія цих Мінімальних вимог не поширюється на захист інформації в технічних засобах і їх складових, необхідних для здійснення уповноваженими органами оперативно-розшукових, розвідувальних заходів та негласних слідчих (розшукових) дій, та на захист інформації, вимоги щодо захисту якої встановлені законом у сфері надання платіжних, банківських та інших фінансових послуг.

3. У системі, яка складається з кількох інформаційних, електронних комунікаційних систем, ці Мінімальні вимоги можуть застосовуватися до кожної складової частини системи окремо.

4. У цих Мінімальних вимогах терміни вживаються у значенні, наведеному в Законах України “Про інформацію”, “Про доступ до публічної інформації”, “Про державну таємницю”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про електронні комунікації”, “Про основні засади забезпечення кібербезпеки України”, “Про Державну службу спеціального зв’язку та захисту інформації України”, “Про електронну ідентифікацію та електронні довірчі послуги”, Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженому постановою Кабінету Міністрів України від 18 червня 2025 р. № 712 (Офіційний вісник України, 2025 р., № 57, ст. 3921), Положенні про організаційно-технічну модель кіберзахисту, затвердженому постановою Кабінету

Міністрів України від 29 грудня 2021 р. № 1426 (Офіційний вісник України, 2022 р., № 4, ст. 219), Загальних вимогах до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 р. № 518 (Офіційний вісник України, 2019 р., № 50, ст. 1697).

5. Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її модифікації чи знищення.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

Створення та/або обробка в системі електронних документів, аналоги яких на паперових носіях повинні містити власноручний підпис відповідно до законодавства, здійснюються із застосуванням електронного підпису чи печатки відповідно до Закону України "Про електронну ідентифікацію та електронні довірчі послуги" або порядку надання та використання послуг електронної ідентифікації та електронних довірчих послуг, які використовуються в інформаційно-комунікаційних системах, в яких обробляються службова інформація та державна таємниця, передбаченого пунктом 37 частини першої статті 14 Закону України "Про Державну службу спеціального зв'язку та захисту інформації України".

Перевірка та підтвердження кваліфікованого електронного підпису чи печатки здійснюються відповідно до вимог статті 18 Закону України "Про електронну ідентифікацію та електронні довірчі послуги".

Перевірка електронного підпису чи печатки у системах, у яких обробляється службова інформація та/або інформація, що становить державну таємницю, проводиться з дотриманням вимог порядку надання та використання послуг електронної ідентифікації та електронних довірчих послуг, які використовуються в інформаційно-комунікаційних системах, в яких обробляються службова інформація та державна таємниця, передбаченого пунктом 37 частини першої статті 14 Закону України "Про Державну службу спеціального зв'язку та захисту інформації України".

6. Під час обробки конфіденційної, службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

7. Доступ до інформації з обмеженим доступом надається тільки ідентифікованим, автентифікованим та авторизованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб або користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора та неавторизованих користувачів повинні блокуватися.

Авторизація в системі повинна забезпечувати можливість надання користувачеві права на обробку в системі інформації з обмеженим доступом або позбавлення його такого права.

8. Вимоги до захисту інформації в системі від несанкціонованого блокування визначаються власником або розпорядником системи, якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством.

9. У системі проводиться обов'язкова реєстрація:

результатів електронної ідентифікації та автентифікації користувачів;

результатів обробки користувачем інформації в системі;

спроб несанкціонованих дій з інформацією;

фактів надання та позбавлення користувачів права доступу до інформації та права на обробку інформації в системі;

результатів перевірки цілісності засобів захисту інформації.

Забезпечується можливість проведення аналізу реєстраційних даних виключно користувачами, яких уповноважено здійснювати управління засобами обробки інформації, захисту інформації, аудиту та контролю за захистом інформації в системі.

Реєстрація проводиться автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають на це повноважень.

Під час реєстрації спроб несанкціонованих дій з інформацією, що становить державну таємницю, і службовою інформацією одночасно повідомляється про них користувачу, уповноваженому здійснювати управління засобами обробки інформації, захисту інформації, аудиту та контролю за захистом інформації в системі.

10. Електронна ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюються автоматизованим способом.

Електронна ідентифікація та автентифікація користувачів у системі здійснюється відповідно до вимог статті 14 Закону України "Про електронну ідентифікацію та електронні довірчі послуги", порядку надання та використання послуг електронної ідентифікації та електронних довірчих послуг, які використовуються в інформаційно-комунікаційних системах, в яких обробляються службова інформація та державна таємниця, передбаченого пунктом 37 частини першої статті 14 Закону України "Про Державну службу спеціального зв'язку та захисту інформації України", та інших нормативно-правових актів у сферах електронної ідентифікації та електронних довірчих послуг.

11. Передача конфіденційної інформації, службової та таємної інформації через незахищене середовище (середовище функціонування технічних або програмних засобів, у якому немає гарантій цілісності, конфіденційності та доступності інформації через відсутність або невідповідність вимогам до захисту інформації) здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства у сфері технічного та криптографічного захисту інформації, за винятком інформації, що передається через канали (лінії) зв'язку, які перебувають в межах контрольованої зони

(територія (простір), на якій (в якому) унеможливлено несанкціоноване і неконтрольоване перебування сторонніх осіб, розміщення технічних і транспортних засобів).

12. Підключення систем, у яких обробляється службова інформація та інформація, що становить державну таємницю, до глобальних мереж передачі даних здійснюється з використанням засобів криптографічного захисту інформації, які допущені до експлуатації для криптографічного захисту інформації відповідного ступеня обмеження доступу, та/або апаратних, апаратно-програмних засобів технічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації та виконують функції безпеки односпрямованої (односторонньої) передачі даних та/або двоспрямованої передачі даних з урахуванням їх змістовного аналізу.

В апаратно-програмних засобах технічного захисту інформації, які виконують функції односпрямованої (односторонньої) передачі даних та/або міжмережевого екранування (фільтрації) даних, що забезпечують захист службової інформації та інформації, що становить державну таємницю, рівень гарантії коректності надання функціональних послуг безпеки повинен бути не нижче третього.

13. У системі здійснюється контроль за цілісністю програмних та технічних засобів захисту інформації та програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації.

## Організаційні та технічні вимоги щодо захисту інформації та кіберзахисту

14. Для забезпечення захисту інформації в системі запроваджуються заходи захисту, які призначаються для захисту інформації від:

витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

несанкціонованих дій з інформацією, зокрема з використанням шкідливого програмного забезпечення;

кіберзагроз;

спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято володільцем інформації.

Захист інформації від витоку технічними каналами забезпечується в системі із застосуванням комплексу технічного захисту інформації з підтвердженою відповідністю у разі обробки у ній інформації, що становить державну таємницю, або прийняття володільцем інформації відповідного рішення щодо необхідності такого захисту.

Захист від кіберзагроз здійснюється у разі поширення вимог Закону України “Про основні засади забезпечення кібербезпеки України” на систему.

Захист інформації від несанкціонованих дій, зокрема від шкідливого програмного забезпечення, забезпечується в усіх системах.

15. Власник або розпорядник системи обирає стандарти, нормативні документи у сферах криптографічного та технічного захисту інформації, кіберзахисту, які використовуються під час здійснення заходів захисту інформації, шляхи і способи здійснення таких заходів.

16. У системі повинні бути виконані технічні та організаційні вимоги до захисту, визначені цими Мінімальними вимогами, відповідно до базового або галузевого профілю безпеки залежно від інформації, що обробляється у ній (відкрита інформація чи інформація з обмеженим доступом), та її функціонального призначення.

Виконання цих Мінімальних вимог підтверджується авторизацією системи з безпеки або шляхом отримання сертифіката відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності (крім систем, у яких обробляється інформація, що становить державну таємницю).

Оцінка відповідності комплексних систем захисту інформації здійснюється з урахуванням вимог пункту 2 постанови Кабінету Міністрів України від 18 червня 2025 р. № 712 “Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем”.

17. Обрання базового або галузевого профілю безпеки системи залежно від інформації, що обробляється (оброблятиметься) у системі, здійснюється власником або розпорядником системи з урахуванням проведеної експертної оцінки інформації, яка обробляється (оброблятиметься) у системі.

Така експертна оцінка проводиться власником або розпорядником системи не рідше ніж кожні два роки з моменту проведення попередньої оцінки.

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

19. Підготовка та здійснення заходів із захисту інформації та кіберзахисту в системі забезпечується підрозділом із кіберзахисту або призначеними особами.

20. Органи державної влади, інші державні органи, державні підприємства, установи та організації, органи місцевого самоврядування як володільці інформації, що оброблятиметься в системі, якщо вони не є власниками або розпорядниками цієї системи, повинні встановлювати умови обробки щодо забезпечення її захисту шляхом виконання вимог базового або галузевого профілю безпеки залежно від інформації, що обробляється у системі (відкрита інформація чи інформація з обмеженим доступом) та функціонального призначення такої системи, що підтверджується авторизацією системи з безпеки або шляхом отримання сертифіката відповідності стандарту інформаційної безпеки, виданого органом з оцінки відповідності.

21. Власники або розпорядники систем повинні встановлювати вимоги щодо запровадження постачальниками товарів, робіт і послуг, що забезпечують функціонування цих систем, заходів безпеки, визначених Адміністрацією Держспецзв'язку.

22. Забезпечення технічного та криптографічного захисту інформації з обмеженим доступом, а також відкритої інформації, вимога щодо захисту якої встановлена законом, здійснюється з дотриманням вимог, передбачених для забезпечення захисту такої інформації, якщо інше не визначено законом.

Криптографічний захист таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в органах державної влади, інших державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, здійснюється з використанням засобів криптографічного захисту інформації, які відповідають вимогам до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації.

23. У складі систем повинні використовуватися засоби технічного та/або криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації або документ про відповідність, виданий органом з оцінки відповідності.

Програмне забезпечення, яке забезпечує функціонування систем, у яких обробляється інформація, що становить державну таємницю, використовується за умови проведення державної експертизи вбудованих функцій захисту такого програмного забезпечення у рамках державної експертизи у сфері технічного та/або криптографічного захисту інформації.

24. Засоби технічного та/або криптографічного захисту інформації, які мають чинний документ про відповідність міжнародному стандарту ISO/IEC 15408 "The Common Criteria for Information Technology Security Evaluation", використовуються у складі систем (крім систем, у яких обробляється службова інформація або інформація, що становить державну таємницю) за умов проведення їх оцінки відповідності з рівнем гарантії оцінювання не нижче другого (EAL2) у рамках міжнародної Домовленості про визнання сертифікатів загальних критеріїв у сфері безпеки інформаційних технологій (The Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security) органом з оцінки відповідності, який акредитовано національним органом України з акредитації або національним органом з акредитації іноземної держави, якщо національний орган України з акредитації та національний орган з акредитації відповідної держави є членами міжнародної або регіональної організації з акредитації та/або уклали угоду про взаємне визнання щодо оцінки відповідності.

Засоби технічного та/або криптографічного захисту інформації, які мають чинний документ про відповідність міжнародному стандарту ISO/IEC 15408 "The Common Criteria for Information Technology Security Evaluation", використовуються у складі систем, у яких обробляється службова інформація, за умов проведення оцінки відповідності з рівнем гарантії оцінювання не нижче четвертого (EAL4) у рамках міжнародної Домовленості про визнання сертифікатів загальних критеріїв у сфері безпеки інформаційних технологій (The Arrangement on the Recognition of Common Criteria Certificates in the field of Information

Technology Security) органом з оцінки відповідності, який акредитовано національним органом України з акредитації або національним органом з акредитації іноземної держави, якщо національний орган України з акредитації та національний орган з акредитації відповідної держави є членами міжнародної або регіональної організації з акредитації та/або уклали угоду про взаємне визнання щодо оцінки відповідності, а також за наявності експертного висновку у сфері технічного та/або криптографічного захисту інформації щодо відповідності результатів такої оцінки вимогам законодавства у сфері захисту інформації.

Засоби технічного та/або криптографічного захисту інформації, які внесені до переліку сертифікованих продуктів в НАТО (NATO Information Assurance Product Catalogue), використовуються у складі систем, в яких обробляється службова інформація, за умов наявності експертного висновку у сфері технічного та/або криптографічного захисту інформації щодо відповідності результатів такої оцінки вимогам законодавства у сфері захисту інформації.

Використання засобів криптографічного захисту інформації, зазначених у цьому пункті, призначених для захисту службової інформації, дозволяється за умови контролю з боку власника або розпорядника системи засобів генерації та розподілу ключових даних до них.

25. Кіберзахист систем забезпечується шляхом здійснення власниками або розпорядниками систем заходів з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки.

Усі базові заходи з кіберзахисту є обов’язковими до здійснення власниками або розпорядниками систем.

26. З метою належного здійснення заходів з кіберзахисту власники або розпорядники систем затверджують, щороку переглядають та за потреби (зокрема у разі зміни рівня ризику кібербезпеки) оновлюють план кіберзахисту.

План кіберзахисту розробляється з урахуванням управління ризиками кібербезпеки на основі каталогу заходів з кіберзахисту та включає описи поточного та/або цільового стану кіберзахисту.

Власники або розпорядники систем поетапно та послідовно досягають цільового стану кіберзахисту шляхом здійснення заходів, передбачених планом кіберзахисту.

Каталог заходів з кіберзахисту, базові заходи з кіберзахисту, форма плану кіберзахисту, а також методичні рекомендації щодо здійснення заходів з кіберзахисту затверджуються Адміністрацією Держспецзв’язку.

27. Власники або розпорядники систем забезпечують оцінювання стану кіберзахисту систем відповідно до порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно- комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури (крім систем та об’єктів банків), передбаченого частиною третьою статті 5 Закону України “Про основні засади забезпечення кібербезпеки України”, з урахуванням каталогу заходів з кіберзахисту, особливостей функціонування та архітектури об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури.

28. Власники або розпорядники систем здійснюють управління ризиками кібербезпеки на постійній та системній основі для запобігання виникненню кіберінциденту та/або кіберзагрози і мінімізації можливих наслідків у разі настання кіберінциденту та/або кіберзагрози.

Управління ризиками кібербезпеки здійснюється із застосуванням національних та міжнародних стандартів управління у сфері кібербезпеки та включає:

організацію управління ризиками кібербезпеки;

оцінювання ризиків кібербезпеки;

запобігання ризикам (мінімізація ризиків) кібербезпеки;

проведення моніторингу і здійснення контролю за ризиками кібербезпеки та перегляд їх актуальності;

здійснення обміну інформацією про ризики кібербезпеки.

Методика оцінювання ризиків кібербезпеки затверджується Адміністрацією Держспецзв'язку.

29. Власники або розпорядники систем забезпечують реагування на кіберінциденти, кібератаки та кіберзагрози з урахуванням національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, передбаченого частиною третьою статті 5 Закону України "Про основні засади забезпечення кібербезпеки України".

30. Керівники з кіберзахисту та підрозділи з кіберзахисту власників або розпорядників систем здійснюють заходи з кіберзахисту, управління ризиками кібербезпеки, реагування на кіберінциденти, кібератаки та кіберзагрози, обмін інформацією про кіберінциденти, кібератаки та кіберзагрози.

31. Власники або розпорядники систем отримують доступ до Інтернету через систему захищеного доступу державних органів до Інтернету Державного центру кіберзахисту або через постачальників електронних комунікаційних мереж та/або послуг, які мають захищені вузли доступу до глобальних мереж передачі даних, або через власні авторизовані з безпеки системи захищеного доступу до Інтернету.

32. Власники або розпорядники систем організовують та забезпечують регулярне навчання своїх співробітників з питань кіберзахисту, яке проводиться диференційовано залежно від функціональних обов'язків та з урахуванням професійної кваліфікації співробітників.

33. Власники або розпорядники систем забезпечують планування витрат та фінансування заходів з кіберзахисту з урахуванням результатів управління ризиками кібербезпеки.

*{Мінімальні вимоги в редакції Постанови КМ № 1531 від 26.11.2025}*

# Публікації документа

- **Офіційний вісник України** від 12.04.2006 — 2006 р., № 13, стор. 164, стаття 878, код акта 35747/2006
- **Урядовий кур'єр** від 18.04.2006 — № 73, / 73-74 /