Прим. № __

АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

від _____ 20__ р. Київ № _____

Зареєстровано в Міністерстві юстиції України 31 грудня 2025 року за №1975/45381

Про встановлення вимог щодо запровадження постачальниками заходів безпеки відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт і послуг власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури

Відповідно до пункту 96 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», підпункту 95^{25} пункту 4, пункту 10 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 03 вересня 2014 року № 411,

НАКАЗУЮ:

1. Затвердити такі, що додаються:

Вимоги щодо запровадження постачальниками заходів безпеки відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт і послуг власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури;

Критерії критичності товарів, робіт, послуг, що постачаються власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури;

Порядок визначення власниками або розпорядниками інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури рівня ризику, пов'язаного з критичністю таких товарів, робіт, послуг, для забезпечення функціонування, та заходів безпеки, що відповідають такому ризику;

Порядок підтвердження постачальниками товарів, робіт, послуг відповідності впроваджених заходів безпеки інформації встановленим вимогам відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт, послуг власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури.

2. Департаменту захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України забезпечити подання цього наказу в установленому порядку на державну реєстрацію до Міністерства юстиції України.

3. Цей наказ набирає чинності з дня його офіційного опублікування.

4. Контроль за виконанням цього наказу залишаю за собою.

Голова Служби Олександр ПОТІЙ

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
___ _____20__ року №____

Зареєстровано в Міністерстві юстиції України
31 грудня 2025 року за № 1975/45381

Вимоги
щодо запровадження постачальниками заходів безпеки відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт і послуг власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури

1. Ці Вимоги встановлюють вимоги щодо запровадження постачальниками заходів безпеки відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт і послуг власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури (далі – системи).

2. Ці Вимоги застосовуються до постачальників товарів, робіт, послуг і власників або розпорядників систем у разі, якщо товари, роботи, послуги, які постачають постачальники, забезпечують функціонування систем.

3. У цих Вимогах терміни вживаються у такому значенні:

постачальник – будь-яка фізична або юридична особа, яка постачає товари, роботи і послуги власникам або розпорядникам систем;

уповноважений користувач – представник постачальника, який має доступ до інформаційно-комунікаційної системи (далі – ІКС) постачальника, де обробляється інформація щодо договору про постачання товарів, робіт, послуг власникам або розпорядникам систем.

Інші терміни вживаються у значенні, наведеному в Законі України «Про захист інформації в інформаційно-комунікаційних системах», Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженому постановою Кабінету Міністрів України від 18 червня 2025 року № 712.

4. Для постачання товарів, робіт і послуг, що належать до першого рівня ризику, постачальник повинен виконати вимоги базових заходів безпеки в ІКС

постачальника, де обробляється інформація щодо договору про постачання товарів, робіт, послуг власникам або розпорядникам систем (у разі наявності), а саме:

обмежувати доступ до ІКС постачальника для уповноважених користувачів, процесів, що діють від імені уповноважених користувачів в ІКС постачальника, або пристроїв (у тому числі інших ІКС);

обмежувати доступ до ІКС постачальника уповноважених користувачів тими функціями, які дозволено їм виконувати;

обмежувати зовнішні підключення до ІКС постачальника та контролювати їх використання;

забезпечувати захист інформації щодо договору про постачання товарів, робіт, послуг від несанкціонованого витоку до публічно доступних інформаційних ресурсів ІКС постачальника;

визначати уповноважених користувачів ІКС постачальника, процеси, що діють від імені уповноважених користувачів в ІКС постачальника, або пристрої;

автентифікувати уповноважених користувачів, процеси, що діють від імені уповноважених користувачів в ІКС постачальника, пристрої перед наданням доступу до ІКС постачальника;

забезпечувати гарантоване знищення інформації щодо договору про постачання товарів, робіт, послуг на фізичному носії інформації перед його утилізацією або передачею для іншого використання;

надавати фізичний доступ до ІКС постачальника, обладнання та фізичного середовища розташування ІКС постачальника лише уповноваженим особам;

здійснювати контроль дій і супровід відвідувачів у приміщення, де розташовано обладнання ІКС постачальника;

вести журнали аудиту фізичного доступу до приміщення, де розташовано обладнання ІКС постачальника;

здійснювати контроль та управління фізичним доступом до обладнання ІКС постачальника;

проводити моніторинг, контроль і захист інформації, що передається або отримується ІКС постачальника з інших мереж;

упроваджувати підмережі для публічно доступних компонентів ІКС постачальника;

своєчасно виявляти та виправляти збої та помилки у роботі ІКС постачальника;

забезпечувати захист від шкідливого програмного забезпечення в ІКС постачальника;

оновлювати механізми захисту ІКС постачальника від шкідливого програмного забезпечення за наявності оновлень;

виконувати періодичне сканування ІКС постачальника та сканування файлів із зовнішніх джерел у режимі реального часу під час завантаження,

відкриття або виконання файлів на наявність шкідливого програмного забезпечення.

5. Для постачання товарів, робіт і послуг, що належать до другого – четвертого рівнів ризику постачальник повинен виконати вимоги базового або галузевого профілю безпеки системи в ІКС постачальника відповідно до інформації, що обробляється в ІКС постачальника (відкрита інформація чи інформація з обмеженим доступом), або функціонального призначення ІКС постачальника.

6. ІКС постачальника, що має комплексну систему захисту інформації з підтвердженою відповідністю, може застосовуватися для постачання товарів, робіт і послуг власникам або розпорядникам систем, в межах функцій, визначених цією комплексною системою захисту інформації.

Директор Департаменту захисту інформації
Адміністрації Держспецзв'язку Андрій ГОЛОВЕНКО

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
___ _____20__ року №____

Зареєстровано в Міністерстві юстиції України
31 грудня 2025 року за №1976/45382

Критерії
критичності товарів, робіт, послуг, що постачаються власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури

1. Ці Критерії встановлюють критерії критичності товарів, робіт, послуг, що постачаються власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури (далі – системи).

2. Ці Критерії застосовуються до постачальників товарів, робіт, послуг і власників або розпорядників систем у разі, якщо товари, роботи, послуги, які постачають постачальники, забезпечують функціонування систем.

3. У цих Критеріях під терміном «постачальник» слід розуміти будь-яку фізичну або юридичну особу, яка постачає товари, роботи і послуги власникам або розпорядникам систем.

Інші терміни вживаються у значенні, наведеному в Законах України «Про захист інформації в інформаційно-комунікаційних системах» і «Про Державну службу спеціального зв'язку та захисту інформації України».

4. Критерії критичності товарів, робіт та послуг, що постачаються власникам або розпорядникам систем:

перший критерій критичності – товари, роботи і послуги, що постачаються власникам або розпорядникам систем, не стосуються участі інформаційно-комунікаційної системи постачальника в обробці державних інформаційних ресурсів або службової інформації та інформації, що становить державну таємницю;

другий критерій критичності – товари, роботи і послуги, що постачаються власникам або розпорядникам систем, безпосередньо стосуються участі

інформаційно-комунікаційної системи постачальника в обробці державних інформаційних ресурсів або службової інформації та інформації, що становить державну таємницю.

Директор Департаменту захисту інформації
Адміністрації Держспецзв'язку Андрій ГОЛОВЕНКО

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
____ _____20__ року №____

Зареєстровано в Міністерстві юстиції України
31 грудня 2025 року за № 1977/45383

Порядок
визначення власниками або розпорядниками інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури рівня ризику, пов'язаного з критичністю таких товарів, робіт, послуг, для забезпечення функціонування та заходів безпеки, що відповідають такому ризику

1. Цей Порядок встановлює процедуру визначення власниками або розпорядниками інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури (далі – системи) рівня ризику, пов'язаного з критичністю таких товарів, робіт, послуг, для забезпечення функціонування та заходів безпеки, що відповідають такому ризику.

2. Цей Порядок застосовується до постачальників товарів, робіт, послуг і власників або розпорядників систем у разі, якщо товари, роботи, послуги, які постачають постачальники, забезпечують функціонування систем.

3. У цьому Порядку під терміном «постачальник» слід розуміти будь-яку фізичну або юридичну особу, яка постачає товари, роботи і послуги власникам або розпорядникам систем.

Інші терміни вживаються у значенні, наведеному в Законах України «Про захист інформації в інформаційно-комунікаційних системах» і «Про Державну службу спеціального зв'язку та захисту інформації України».

4. Власники або розпорядники систем зобов'язані визначити рівні ризику, пов'язані з критичністю товарів, робіт, послуг, що постачаються для забезпечення функціонування та заходів безпеки і відповідають такому ризику.

5. Ризики, пов'язані з критеріями критичності постачання товарів, робіт, послуг власникам або розпорядникам систем для забезпечення їх функціонування та заходів безпеки, поділяються на такі рівні:

перший рівень ризику – товари, роботи і послуги за першим критерієм критичності, призначені для інформаційно-комунікаційних систем, де обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури;

другий рівень ризику – товари, роботи і послуги за другим критерієм критичності, призначені для інформаційно-комунікаційних систем, де обробляються державні інформаційні ресурси, об'єктів критичної інформаційної інфраструктури, інформація про яких віднесена до відкритої або конфіденційної інформації;

третій рівень ризику – товари, роботи і послуги за другим критерієм критичності, призначені для інформаційно-комунікаційних систем, де обробляються державні інформаційні ресурси, об'єктів критичної інформаційної інфраструктури, інформація про яких віднесена до службової інформації;

четвертий рівень ризику – товари, роботи і послуги за другим критерієм критичності, призначені для інформаційно-комунікаційних систем, де обробляються державні інформаційні ресурси, об'єктів критичної інформаційної інфраструктури, інформація про яких віднесена до інформації, що становить державну таємницю.

Директор Департаменту захисту інформації
Адміністрації Держспецзв'язку Андрій ГОЛОВЕНКО

ЗАТВЕРДЖЕНО

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
___ _____20__ року №____

Зареєстровано в Міністерстві юстиції України
31 грудня 2025 року за № 1978/45384

Порядок
підтвердження постачальниками товарів, робіт, послуг відповідності впроваджених заходів безпеки інформації встановленим вимогам відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт, послуг власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури

1. Цей Порядок встановлює процедуру підтвердження постачальниками товарів, робіт, послуг відповідності впроваджених заходів безпеки інформації встановленим вимогам відповідно до рівня ризику, пов'язаного з постачанням товарів, робіт, послуг власникам або розпорядникам інформаційно-комунікаційних систем, у яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інформаційної інфраструктури (далі – системи).

2. Цей Порядок застосовується до постачальників товарів, робіт, послуг і власників або розпорядників систем у разі, якщо товари, роботи, послуги, які постачають постачальники, забезпечують функціонування систем.

3. У цьому Порядку під терміном «постачальник» слід розуміти будь-яку фізичну або юридичну особу, яка постачає товари, роботи і послуги власникам або розпорядникам систем.

Інші терміни вживаються у значенні, наведеному в Законі України «Про захист інформації в інформаційно-комунікаційних системах», Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженому постановою Кабінету Міністрів України від 18 червня 2025 року № 712.

4. Виконання вимог базових заходів безпеки відповідно до першого рівня ризику в інформаційно-комунікаційній системі постачальника (в разі наявності) підтверджується постачальником декларативним принципом у рамках укладення договору про постачання товарів, робіт і послуг з власником або розпорядником системи.

5. Виконання вимог відповідно до другого – четвертого рівнів ризику підтверджується постачальником шляхом підтвердження наявності однієї з таких умов:

авторизації з безпеки інформаційно-комунікаційної системи та наявності у переліку авторизованих систем з безпеки;

сертифіката відповідності стандарту інформаційної безпеки, виданого 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 з такою організацією угоду про взаємне визнання щодо оцінки відповідності;

чинного атестата відповідності на комплексну систему захисту інформації.

Директор Департаменту захисту інформації
Адміністрації Держспецзв'язку Андрій ГОЛОВЕНКО