КАБІНЕТ МІНІСТРІВ УКРАЇНИ
ПОСТАНОВА

від 18 червня 2025 р. № 712
Київ

Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем

{Із змінами, внесеними згідно з Постановою КМ № 1166 від 17.09.2025}

Відповідно до частини третьої статті 8, абзацу десятого частини третьої та частини шостої 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**:

1. Затвердити такі, що додаються:

Порядок авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем;

Порядок розроблення та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем.

2. Установити, що:

декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням базових та цільових профілів безпеки інформації, розпочате до набрання чинності цією постановою, завершується відповідно до Порядку реалізації експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації, затвердженого постановою Кабінету Міністрів України від 30 травня 2024 р. № 627 (Офіційний вісник України, 2024 р., № 54, ст. 3202);

у разі, коли власником чи розпорядником системи визнано за необхідне завершення робіт із створення комплексних систем захисту інформації, розпочатих до набрання чинності цією постановою, такі роботи завершуються в рамках проведення державної

експертизи у сфері технічного захисту інформації з подальшою авторизацією з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем протягом 12 місяців з дня набрання чинності цією постановою.

{Абзац третій пункту 2 в редакції Постанови КМ № 1166 від 17.09.2025}

3. Визнати такою, що втратила чинність, постанову Кабінету Міністрів України від 30 травня 2024 р. № 627 "Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації" (Офіційний вісник України, 2024 р., № 54, ст. 3202).

4. Адміністрації Державної служби спеціального зв'язку та захисту інформації забезпечити подання до 1 лютого 2026 р. звіт за результатами реалізації експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації, який здійснювався відповідно до постанови Кабінету Міністрів України від 30 травня 2024 р. № 627 "Про реалізацію експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації".

5. Ця постанова набирає чинності з дня її опублікування, крім пункту 3, який набирає чинності з 1 січня 2026 року.

Прем'єр-міністр України **Д. ШМИГАЛЬ**

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 18 червня 2025 р. № 712

ПОРЯДОК
авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем

1. Цей Порядок визначає процедури проведення авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, інші державні органи, державні підприємства, установи та організації, органи місцевого самоврядування (далі - системи), а також підтвердження дотримання вимог з безпеки щодо таких систем протягом їх життєвого циклу.

2. У цьому Порядку терміни вживаються в такому значенні:

базовий профіль безпеки системи (далі - базовий профіль) - мінімальні вимоги з безпеки інформації та взаємопов'язана сукупність заходів щодо її захисту, які встановлюються залежно від інформації, що обробляється у системі (відкрита інформація чи інформація з обмеженим доступом), або функціонального призначення такої системи;

галузевий профіль безпеки системи (далі - галузевий профіль) - взаємопов'язана сукупність заходів щодо захисту інформації, визначених для системи органом державної влади, іншим державним органом у межах своїх повноважень у відповідній сфері або галузі з урахуванням мінімальних вимог щодо таких заходів із захисту (базового профілю), відповідних стандартів, політик безпеки та особливостей функціонування системи у відповідній сфері або галузі, а також надання відповідних рекомендацій;

галузеві уповноважені органи - органи державної влади, інші державні органи, які в межах своїх повноважень у відповідній сфері або галузі затверджують галузевий профіль;

оцінювання дотримання вимог цільових профілів безпеки системи - процес перевірки обраних та/або запроваджених методів, заходів, засобів захисту інформації та кіберзахисту системи з метою встановлення стану захищеності систем або їх відповідності вимогам законодавства, національним стандартам, нормативним документам у сферах криптографічного та технічного захисту інформації, кіберзахисту;

цільовий профіль безпеки системи (далі - цільовий профіль) - взаємопов'язана сукупність заходів із захисту інформації, визначених органами державної влади, іншими державними органами, державними підприємствами, установами та організаціями, органами місцевого самоврядування (далі - власник або розпорядник системи) для

відповідних систем з урахуванням мінімальних вимог щодо таких заходів із захисту (базового профілю), вимог законодавства та національних стандартів у сферах криптографічного та технічного захисту інформації, кіберзахисту, нормативних документів системи технічного та криптографічного захисту інформації, кіберзахисту, а також галузевого профілю (за наявності), політик безпеки, призначення системи, її структурно-функціональних характеристик та особливостей функціонування системи, результатів проведеної оцінки (аналізу) ризиків безпеки.

Інші терміни вживаються у значенні, наведеному в Законах України "Про Державну службу спеціального зв'язку та захисту інформації України", "Про захист інформації в інформаційно-комунікаційних системах", "Про основні засади забезпечення кібербезпеки України", "Про інформацію".

3. Авторизація з безпеки систем проводиться з метою прийняття рішення щодо можливості функціонування (експлуатації) системи з урахуванням її відповідності вимогам законодавства, національним стандартам та нормативним документам у сферах технічного та криптографічного захисту інформації, кіберзахисту.

Авторизація з безпеки систем здійснюється з дотриманням вимог, передбачених частиною сьомою статті 8 Закону України "Про захист інформації в інформаційно-комунікаційних системах".

4. Авторизація з безпеки системи здійснюється для систем, щодо яких затверджено цільовий профіль.

Під час розроблення та затвердження цільового профілю власник або розпорядник системи самостійно обирає національні стандарти у сферах технічного та криптографічного захисту інформації, кіберзахисту, засоби і методи здійснення таких заходів.

Оцінювання дотримання вимог цільового профілю та оформлення його результатів здійснюється з урахуванням рекомендацій, затверджених Адміністрацією Держспецзв'язку.

Оцінювання дотримання вимог цільового профілю здійснюється юридичними особами, фізичними особами - підприємцями або фізичними особами (далі - суб'єкти оцінювання), вимоги до яких затверджуються Адміністрацією Держспецзв'язку відповідно до законодавства та з урахуванням особливостей, встановлених цим Порядком.

За результатами оцінювання дотримання вимог цільового профілю складається звіт з оцінювання дотримання вимог цільового профілю для авторизації з безпеки системи. Такий звіт повинен зберігатися у власника або розпорядника системи протягом дії авторизації з безпеки системи та протягом року після скасування авторизації з безпеки системи.

5. Суб'єктами авторизації з безпеки системи є:

власники або розпорядники системи;

галузеві уповноважені органи;

Адміністрація Держспецзв'язку.

6. Авторизація з безпеки системи здійснюється такими етапами:

розроблення та затвердження для системи цільового профілю;

виконання вимог цільового профілю;

оцінювання дотримання вимог цільового профілю;

оформлення та подання Адміністрації Держспецзв'язку авторизаційного листа згідно з додатком 1;

внесення даних щодо авторизації до переліку авторизованих систем з безпеки.

7. Авторизація з безпеки системи може бути первинною, плановою, позаплановою.

Первинна авторизація з безпеки системи є основним видом авторизації та здійснюється з метою початку функціонування (експлуатації) системи.

Планова авторизація з безпеки системи проводиться з метою підтвердження авторизації за результатами перегляду цільового профілю на підставі щорічної оцінки (перегляду) ризиків.

Планова авторизація з безпеки системи здійснюється протягом життєвого циклу системи, не пізніше одного календарного року після первинної, планової або позапланової авторизації з безпеки системи.

Позапланова авторизація з безпеки системи проводиться у разі:

внесення змін до базового профілю або галузевого профілю, з урахуванням якого був сформований цільовий профіль, якщо інше не передбачено актами, якими затверджуються базовий профіль або галузевий профіль;

внесення змін до цільового профілю, зокрема в результаті зміни умов функціонування (експлуатації), модернізації системи, або у разі виконання вимог за результатами державного контролю за додержанням вимог законодавства у сферах технічного та криптографічного захисту інформації, кіберзахисту, за станом технічного або криптографічного захисту.

Позапланова авторизація з безпеки системи проводиться протягом шести місяців з дати внесення змін до базового профілю, галузевого профілю або цільового профілю, якщо інше не передбачено нормативно-правовими актами.

8. Підставою для подання системи на первинну авторизацію з безпеки системи є позитивні результати оцінювання дотримання вимог цільового профілю, для планової та позапланової авторизації з безпеки системи - позитивні результати оцінювання дотримання вимог цільового профілю у частині, що стосується заходів, які зазнали змін.

9. Авторизація з безпеки системи, крім систем, в яких обробляється інформація, що становить державну таємницю, здійснюється на підставі авторизаційного листа, поданого власником або розпорядником такої системи до Адміністрації Держспецзв'язку згідно з додатком 1.

Включення такої системи до переліку авторизованих систем з безпеки здійснюється Адміністрацією Держспецзв'язку протягом десяти робочих днів на підставі поданого в

установленому порядку авторизаційного листа у разі зазначеної в ньому повної інформації згідно з додатком 1.

Посадові особи власника або розпорядника системи, що подав до Адміністрації Держспецзв'язку авторизаційний лист, на підставі якого здійснена авторизація з безпеки системи, відповідно до закону несуть відповідальність за достовірність зазначеної в ньому інформації, а також за повноту та правильність обрання засобів і методів здійснення заходів відповідно до профілів безпеки з урахуванням вимог законодавства.

Адміністрація Держспецзв'язку протягом десяти робочих днів з дня надходження авторизаційного листа повертає авторизаційний лист власнику або розпоряднику системи, що його подав, на доопрацювання із зазначенням рекомендацій щодо усунення недоліків та невідповідності, якщо:

в авторизаційному листі зазначено неповну інформацію;

в авторизаційному листі виявлено невідповідність інформації фактичним даним щодо системи, власника, суб'єкта оцінювання;

в авторизаційному листі виявлено неправильно обраний базовий профіль або галузевий профіль для затвердження цільового профілю щодо системи залежно від інформації, що обробляється у ній (відкрита інформація чи інформація з обмеженим доступом), або її функціонального призначення.

10. Авторизація з безпеки системи, в якій обробляється інформація, що становить державну таємницю, здійснюється на підставі авторизаційного листа за формою згідно з додатком 1, поданого власником або розпорядником системи до Адміністрації Держспецзв'язку, до якого додаються:

копія затвердженого цільового профілю, на підставі якого (змін до якого) здійснюється авторизація з безпеки системи;

копія звіту з оцінювання дотримання вимог цільового профілю для цілей авторизації з безпеки системи або в частині впровадження змін, внесених до цільового профілю, або за відсутності таких змін до цільового профілю під час планової авторизації з безпеки системи - звіту з оцінювання дотримання вимог цільового профілю для цілей авторизації з безпеки системи з підтвердженням про відсутність змін до цільового профілю на підставі щорічної оцінки ризиків;

копія документа про оцінку відповідності комплексу технічного захисту інформації.

Рішення про авторизацію з безпеки системи та внесення даних до переліку авторизованих систем з безпеки приймається Адміністрацією Держспецзв'язку протягом 30 календарних днів з дня подання авторизаційного листа та додатків до нього, передбачених цим пунктом (далі - авторизаційна документація), аналізу цільового профілю та реалізації звіту з оцінювання дотримання вимог цільового профілю для цілей авторизації з безпеки системи щодо відповідності вимогам базового профілю або галузевого профілю (за наявності), вимогам законодавства, національним стандартам та нормативним документам у сферах технічного та криптографічного захисту інформації, кіберзахисту.

11. Перевірка авторизаційної документації щодо правильності або повноти обраних засобів і методів дотримання вимог цільового профілю, відповідності впроваджених заходів вимогам законодавства, національним стандартам, нормативним документам у сферах технічного та криптографічного захисту інформації, кіберзахисту щодо систем, які є локалізованими одномашинними однокористувачевими комплексами, за рішенням Адміністрації Держспецзв'язку може проводитися відповідним галузевим уповноваженим органом, Генеральним штабом Збройних Сил, які мають дозвіл Адміністрації Держспецзв'язку на проведення робіт з технічного захисту інформації для власних потреб, в порядку, затвердженому Адміністрацією Держспецзв'язку.

У разі виявлення недоліків щодо правильності або повноти обраних засобів і методів виконання вимог цільового профілю щодо систем, в яких обробляється інформація, що становить державну таємницю, або ознак невідповідності впроваджених заходів вимогам законодавства, національним стандартам, нормативним документам у сферах технічного та криптографічного захисту інформації, кіберзахисту Адміністрація Держспецзв'язку або галузевий уповноважений орган під час розгляду авторизаційної документації визначає необхідність подання власником або розпорядником такої системи додаткових документів або інформації щодо заходів її захисту. Власник або розпорядник системи протягом п'яти робочих днів з дня отримання такого запиту подає до Адміністрації Держспецзв'язку або відповідного уповноваженого органу додаткові документи та інформацію, що запитується.

Адміністрація Держспецзв'язку за результатами розгляду авторизаційної документації протягом десяти робочих днів з дня надходження повертає її власнику або розпоряднику системи, що її подав, на доопрацювання із зазначенням рекомендацій щодо усунення недоліків та невідповідності, якщо:

в авторизаційному листі зазначено неповну інформацію;

в авторизаційному листі виявлено невідповідність інформації фактичним даним щодо системи, власника або розпорядника системи, суб'єкта оцінювання;

в авторизаційному листі виявлено неправильно обраний базовий профіль або галузевий профіль для затвердження цільового профілю щодо системи залежно від інформації, що обробляється у ній (відкрита інформація чи інформація з обмеженим доступом), або її функціонального призначення;

в авторизаційній документації встановлено суттєві недоліки щодо правильності та повноти обраних засобів і методів, визначених у цільовому профілі, або невідповідності впроваджених заходів вимогам законодавства, національним стандартам, нормативним документам у сферах технічного та криптографічного захисту інформації, кіберзахисту щодо систем, в яких обробляється інформація, що становить державну таємницю.

Усунення недоліків щодо правильності та повноти обраних засобів і методів, визначених в цільовому профілі, або невідповідності впроваджених заходів вимогам законодавства, національним стандартам, нормативним документам у сферах технічного та криптографічного захисту інформації, кіберзахисту є підставою для перегляду власником або розпорядником системи цільового профілю та проведення нового оцінювання впровадження цільового профілю.

12. За результатами включення системи до переліку авторизованих систем з безпеки Адміністрація Держспецзв’язку протягом п’яти робочих днів з дня включення надсилає власнику або розпоряднику системи повідомлення за формою згідно з додатком 2.

13. Авторизація з безпеки системи скасовується на підставі:

подання до Адміністрації Держспецзв’язку письмового звернення власника або розпорядника системи про скасування авторизації з безпеки системи;

непроведення у встановлені строки планової авторизації з безпеки системи;

непроведення у встановлені строки позапланової авторизації з безпеки системи у випадках змін базового профілю або галузевого профілю, на основі якого був сформований цільовий профіль;

невиконання у встановлені строки вимог щодо усунення порушень, виявлених за результатами проведення державного контролю за додержанням вимог законодавства у сферах технічного та криптографічного захисту інформації, кіберзахисту.

Рішення про скасування авторизації з безпеки системи приймається Адміністрацією Держспецзв’язку протягом 30 робочих днів після отримання відповідних відомостей, зазначених у цьому пункті.

У разі скасування авторизації з безпеки системи наступне включення системи до переліку авторизованих систем з безпеки здійснюється як первинна авторизація з безпеки системи.

14. З метою оцінки ефективності реалізації державної політики у сфері захисту інформації під час авторизації з безпеки систем Адміністрацією Держспецзв’язку здійснюється моніторинг у визначеному нею порядку.

Додаток 1
до Порядку авторизації з безпеки
інформаційних, електронних комунікаційних,
інформаційно-комунікаційних,
технологічних систем

АВТОРИЗАЦІЙНИЙ ЛИСТ

Додаток 2
до Порядку авторизації з безпеки
інформаційних, електронних комунікаційних,
інформаційно-комунікаційних,
технологічних систем

ПОВІДОМЛЕННЯ

про включення інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування до переліку авторизованих систем з безпеки

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 18 червня 2025 р. № 712

ПОРЯДОК
розроблення та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем

1. Цей Порядок визначає механізм розроблення та затвердження базових, галузевих та цільових профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем (далі - системи).

2. У цьому Порядку терміни вживаються у значенні, наведеному в Законах України "Про захист інформації в інформаційно-комунікаційних системах", "Про основні засади забезпечення кібербезпеки України", "Про інформацію", Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженому постановою Кабінету Міністрів України від 18 червня 2025 р. № 712 "Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем".

3. Базові профілі безпеки системи розробляються залежно від інформації, що обробляється у системі (відкрита інформація чи інформація з обмеженим доступом), а також функціонального призначення системи та затверджуються Адміністрацією Держспецзв'язку.

Адміністрація Держспецзв'язку публікує на офіційному веб-сайті Держспецзв'язку базові профілі безпеки системи, які містять відкриту інформацію.

Базові профілі безпеки системи, які містять інформацію з обмеженим доступом, надаються уповноваженим органом з авторизації власникам або розпорядникам систем за окремим запитом в установленому порядку з дотриманням встановлених правил роботи з документами, які містять інформацію з обмеженим доступом.

Адміністрація Держспецзв'язку кожні два роки здійснює перегляд вимог базового профілю безпеки системи та у разі необхідності вносить відповідні зміни.

4. Галузевий профіль безпеки системи розробляється з урахуванням визначеного базового профілю безпеки системи для відповідної категорії систем залежно від інформації, що обробляється у них (відкрита інформація чи інформація з обмеженим доступом), відповідних стандартів, політик безпеки та особливостей функціонування системи у відповідній сфері або галузі, а також надання відповідних рекомендацій, погоджується з Адміністрацією Держспецзв'язку та затверджується галузевим уповноваженим органом. Затверджений галузевий профіль безпеки системи протягом десяти днів з дати

затвердження надсилається галузевим уповноваженим органом до Адміністрації Держспецзв'язку.

Галузевий уповноважений орган може здійснювати перегляд та вносити зміни до галузевого профілю безпеки системи за необхідності.

Галузевий уповноважений орган вносить зміни до галузевого профілю безпеки системи в разі зміни базового профілю безпеки системи, на базі якого він був розроблений, протягом трьох місяців з дати внесення змін до базового профілю безпеки системи.

Зміни до галузевого профілю безпеки системи вносяться в порядку, визначеному абзацом першим цього пункту.

5. Цільовий профіль безпеки системи розробляється для відповідної системи, що підлягає авторизації з безпеки системи з урахуванням мінімальних вимог щодо таких заходів із захисту (базового профілю), вимог законодавства та національних стандартів у сферах криптографічного та технічного захисту інформації, кіберзахисту, нормативних документів системи технічного та криптографічного захисту інформації, кіберзахисту, а також галузевого профілю (за наявності), політик безпеки, призначення системи, її структурно-функціональних характеристик та особливостей функціонування системи, результатів проведеної оцінки (аналізу) ризиків безпеки.

У випадках, передбачених галузевим профілем безпеки системи, цільовий профіль безпеки системи погоджується з галузевим уповноваженим органом.

Розроблення цільового профілю безпеки системи здійснюється з урахуванням рекомендацій, затверджених Адміністрацією Держспецзв'язку.

Власник або розпорядник системи з метою планової авторизації з безпеки системи або за необхідності здійснює перегляд та вносить зміни до цільового профілю безпеки системи на основі щорічного аналізу ризиків щодо функціонування (експлуатації) відповідної системи.

Власник або розпорядник системи вносить зміни до цільового профілю безпеки системи в разі зміни базового профілю безпеки системи або галузевого профілю безпеки системи, з урахуванням якого він був розроблений, протягом трьох місяців з дати внесення змін до базового профілю безпеки системи або галузевого профілю безпеки системи, якщо інше не передбачено актами, на підставі яких затверджено зміни до базового або галузевого профілю безпеки системи.

Документи та файли

- Сигнальний документ — **f545905n112.docx** від 23.06.25 16:45, 21 кб
- Сигнальний документ — **f545905n113.docx** від 23.06.25 16:45, 19 кб

Публікації документа

- **Урядовий кур'єр** від 19.06.2025 — № 123
- **Офіційний вісник України** від 25.07.2025 — 2025 р., № 57, стаття 3921, код акта 132962/2025