ЗАТВЕРДЖЕНО
Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України
Зареєстровано у Міністерстві юстиції України 21 серпня 2026 року за № 1168/46562 07 серпня 2026 року № 604

Методика здійснення заходу державного контролю за додержанням вимог законодавства у сфері кіберзахисту

І. Загальні положення

1. Ця Методика визначає сукупність питань, що є предметом здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту, та підходи до їх розгляду залежно від форми заходу державного контролю відповідно до Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту, затвердженого постановою Кабінету Міністрів України від 17 грудня 2025 року № 1668 (далі – Порядок).

Ця Методика встановлює:

сукупність питань, що є предметом здійснення контролю;

підходи до розгляду питань перевірки, які визначаються залежно від форми заходу державного контролю;

підходи до визначення рекомендацій щодо усунення виявлених недоліків та заходів, що мають бути виконані для підвищення рівня кіберзахисту на об’єкті державного контролю за результатами моніторингу;

підходи до визначення вимог про усунення виявлених порушень за результатами перевірки.

2. У цій Методиці терміни вживаються в такому значенні:

методи дослідження – сукупність способів, прийомів і процедур, за допомогою яких проводяться збір, перевірка, аналіз та інтерпретація даних під час здійснення державного контролю у сфері кіберзахисту;

об’єкт державного контролю за додержанням вимог законодавства у сфері кіберзахисту (далі – об’єкт державного контролю) – інформаційні, електронні комунікаційні, інформаційно-комунікаційні та технологічні системи (далі – системи), в яких обробляються державні інформаційні ресурси або інформація, вимога щодо захисту якої встановлена законом, об'єкти критичної інфраструктури, об'єкти критичної інформаційної інфраструктури, процеси та процедури, що забезпечують реалізацію дотримання законодавчих вимог щодо кіберзахисту в системах суб’єктів державного контролю;

показники – кількісні та якісні характеристики стану кіберзахисту, що використовуються для об’єктивного вимірювання результатів діяльності суб’єкта державного контролю з виконання вимог законодавства у сфері кіберзахисту;

суб'єкт державного контролю за додержанням вимог законодавства у сфері кіберзахисту (далі – суб'єкт державного контролю) – органи державної влади, державні органи, органи місцевого самоврядування, утворені відповідно до закону військові формування, підприємства, установи, організації, які є власниками або розпорядниками систем, в яких обробляються державні інформаційні ресурси або інформація, вимога щодо захисту якої встановлена законом, оператори критичної інфраструктури, власники або розпорядники об'єктів критичної інформаційної інфраструктури.

Інші терміни вживаються у значенні, наведеному в Законах України «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», «Про захист інформації в інформаційно-комунікаційних системах», «Про Державну службу спеціального зв’язку та захисту інформації України», «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту, затвердженому постановою Кабінету Міністрів України від 17 грудня 2025 року № 1668, Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури, затвердженому постановою Кабінету Міністрів України від 31 грудня 2025 року № 1799.

3. Дія цієї Методики поширюється на суб’єктів державного контролю та об’єкти державного контролю, визначених пунктами 3 та 4 Порядку.

4. Державний контроль за додержанням вимог законодавства у сфері кіберзахисту здійснюється шляхом проведення заходів державного контролю у формі моніторингу стану кіберзахисту та перевірок відповідно до пункту 5 Порядку.

5. Ця Методика не встановлює обов’язків для суб’єктів державного контролю та об’єктів державного контролю, не визначає порядок проведення оцінювання стану кіберзахисту, не встановлює вимог до суб’єктів оцінювання стану кіберзахисту та застосовується виключно в межах здійснення державного контролю відповідно до Порядку.

Висновок про порушення вимог законодавства у сфері кіберзахисту може ґрунтуватися виключно на невиконанні або неналежному виконанні вимоги, встановленої законом або прийнятим відповідно до закону нормативно-правовим актом.

6. Положення цієї Методики, пов’язані з урахуванням звітів або інформації про результати оцінювання стану кіберзахисту, застосовуються у випадках, коли проведення відповідного оцінювання та / або подання інформації про його

результати передбачено законодавством або коли таке оцінювання проведено добровільно власником чи розпорядником об’єкта оцінювання.

Щодо об’єктів критичної інфраструктури та об’єктів критичної інформаційної інфраструктури III і IV категорій критичності такі положення застосовуються з урахуванням вимог частини другої статті 6 Закону України «Про основні засади забезпечення кібербезпеки України».

II. Сукупність питань, що є предметом здійснення контролю

1. Предметом здійснення заходу державного контролю є встановлення стану додержання суб’єктом державного контролю вимог законодавства у сфері кіберзахисту, що визначаються залежно від форми заходу:

під час моніторингу – на предмет повноти, своєчасності подання та достовірності відомостей у звітах про результати оцінювання стану кіберзахисту суб'єкта державного контролю, а також аналізу динаміки впровадження заходів із кіберзахисту, виконання рекомендацій щодо усунення виявлених недоліків та заходів, що мають бути виконані для підвищення рівня кіберзахисту на об’єкті державного контролю;

під час перевірки – на предмет встановлення відповідності об’єктів державного контролю вимогам законодавства у сфері кіберзахисту.

2. Сукупність питань, що підлягають розгляду під час заходу державного контролю, визначається залежно від форми його проведення:

під час моніторингу – перелік питань для аналізу формується за розділами звіту про результати оцінювання, який складається суб'єктом державного контролю за формою та методичними рекомендаціями, визначеними Адміністрацією Держспецзв’язку відповідно до пункту 7 Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури, затвердженого постановою Кабінету Міністрів України від 31 грудня 2025 року № 1799;

під час перевірки – перелік питань формується виключно на підставі вимог законодавства у сфері кіберзахисту та встановлюється уніфікованою формою акта про результати перевірки стану додержання вимог законодавства у сфері кіберзахисту.

III. Підходи до розгляду питань, що є предметом здійснення контролю

1. Моніторинг стану кіберзахисту проводиться на підставі звітів про оцінювання, що подаються суб’єктами державного контролю через інформаційну систему моніторингу стану кіберзахисту відповідно до пункту 7 Порядку.

Під час моніторингу стану кіберзахисту оцінюються:
своєчасність та повнота подання звітності;
наявність та актуальність визначених законодавством документів;
відповідність поданих даних встановленим формам;
наявність ознак ризику, недостовірності або погіршення стану кіберзахисту;
динаміка показників стану кіберзахисту.

2. Перевірка (планова / позапланова) проводиться комісією в межах предмета перевірки шляхом дослідження документів, пояснень, відомостей державного контролю, огляду та візуального обстеження систем, що передбачають ознайомлення з їхнім фактичним станом і параметрами налаштувань без втручання в робочі процеси та без ризику порушення стабільності їхнього функціонування.

Під час дослідження документів, пояснень, відомостей державного контролю, огляду та візуального обстеження систем комісія діє в межах предмета конкретної перевірки. Запит документів, інформації, технічних матеріалів або доступу до систем здійснюється лише в обсязі, необхідному для перевірки конкретних питань, що безпосередньо пов’язані з вимогами законодавства у сфері кіберзахисту, додержання яких перевіряється.

3. Організація роботи з документами та іншими матеріальними носіями інформації з обмеженим доступом здійснюється з дотриманням вимог законодавства у сфері охорони державної таємниці, захисту інформації, а також нормативно-правових актів, що регламентують порядок поводження зі службовою інформацією.

4. Посадові особи, які входять до складу комісії, та залучені фахівці зобов’язані не розголошувати інформацію з обмеженим доступом, що стала їм відома під час здійснення заходу державного контролю, та використовувати таку інформацію виключно для цілей здійснення державного контролю.

5. Якщо доступ до окремих систем, приміщень, документів або відомостей обмежується режимними вимогами, суб’єкт державного контролю забезпечує можливість отримання комісією відомостей державного контролю у спосіб, що не порушує встановленого режиму доступу та не створює ризику розголошення інформації з обмеженим доступом.

6. Під час перевірки встановлюються:
фактичний стан виконання вимог законодавства;
виконання вимог, визначених за результатами попередніх перевірок;
наявність порушень законодавства у сфері кіберзахисту.

7. Планові перевірки проводяться на підставі річного плану здійснення заходів державного контролю за додержанням вимог законодавства у сфері кіберзахисту відповідно до пункту 12 Порядку.

Під час формування пропозицій до річного плану можуть враховуватися у сукупності такі показники за наявності відповідних відомостей:

1) якісні:

вид інформації, що обробляється в системах (відкрита, інформація з обмеженим доступом);

результати оцінювання стану кіберзахисту (загальні стани кіберзахисту: «критичний / частковий», «низький / поінформований про ризик», «знижений / повторюваний», «задовільний / адаптивний»);

результати попередніх перевірок (висновок за результатами проведення перевірки: «відповідність вимогам законодавства» або «невідповідність вимогам законодавства»);

вид суб’єкта державного контролю у сфері кіберзахисту;

2) кількісні:

наявність невиконаних вимог припису (кількість конкретних порушень, які не були усунуті вчасно відповідно до вимог припису);

відомості щодо виявленого у суб’єкта контролю кіберінциденту, який за рівнем критичності визначено як високий, критичний або надзвичайний (відповідно до рівнів, встановлених пунктом 12 Національного плану реагування на кіберінциденти, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533);

відомості про несвоєчасне проведення щорічного оцінювання.

Відомості, зазначені в цьому пункті, використовуються як аналітичні ризик-орієнтовані дані та самі по собі не мають наслідком автоматичного включення суб’єкта державного контролю до річного плану. Пропозиція щодо включення суб’єкта державного контролю до річного плану повинна містити обґрунтування із зазначенням конкретних показників, джерел їх отримання та причин пріоритетності проведення перевірки.

8. Методи дослідження під час перевірок визначають механізм практичного виконання завдань і передбачають поєднання документальних, аналітичних, технічних, інструментальних, організаційних і експертних підходів. Метою є отримання відомостей державного контролю та встановлення їх відповідності вимогам законодавства.

Під час перевірки застосовуються такі методи дослідження:

документальне вивчення (накази, політики, журнали, звіти, плани, договори);

опитування та отримання пояснень (пояснення керівника суб’єкта державного контролю, керівника з кіберзахисту, адміністраторів, користувачів);

огляд і спостереження (огляд робочих місць, програмно-апаратних засобів захисту системи, інтерфейсів адміністрування, журналів подій);

аналітичне зіставлення отриманих даних (порівняння документально задекларованого стану з фактичним).

IV. Підходи до визначення рекомендацій за результатами моніторингу стану кіберзахисту

1. Основним методом моніторингу стану кіберзахисту є дистанційне вивчення звітів, анкет і статистичних даних без безпосереднього доступу до об’єктів державного контролю чи суб’єкта державного контролю.

Під час аналізу звітів про результати оцінювання стану кіберзахисту суб’єкта державного контролю першочергово враховується загальний стан кіберзахисту суб’єкта державного контролю: «критичний / частковий», «низький / поінформований про ризик», «знижений / повторюваний» або «задовільний / адаптивний».

2. Якщо результат оцінювання стану кіберзахисту суб'єкта державного контролю визначено як «задовільний / адаптивний», рекомендації щодо усунення виявлених недоліків та заходів, що мають бути виконані для підвищення рівня кіберзахисту на об’єкті державного контролю, не надаються Адміністрацією Держспецзв’язку та її територіальними органами.

3. Якщо результат оцінювання стану кіберзахисту суб'єкта державного контролю визначено як «низький / поінформований про ризик» або «знижений / повторюваний» та виявлено недоліки щодо стану виконання вимог законодавства у сфері кіберзахисту, повноти запроваджених заходів кіберзахисту, Адміністрація Держспецзв’язку та її територіальні органи надають суб’єкту державного контролю рекомендації щодо усунення виявлених недоліків та заходів, що мають бути виконані для підвищення рівня кіберзахисту на об’єкті державного контролю.

Рекомендації базуються виключно на необхідності додержання вимог законодавства у сфері кіберзахисту та спрямовуються на усунення виявлених недоліків в організації кіберзахисту для запобігання порушенням таких вимог.

Рекомендації за результатами моніторингу оформлюються із зазначенням виявленого недоліку, узагальненого напряму його усунення та у разі потреби – орієнтовного строку або етапності врахування рекомендації з урахуванням характеру недоліку, технічної складності заходів та ризику для стану кіберзахисту.

4. Якщо результат оцінювання стану кіберзахисту суб’єкта державного контролю визначено як «критичний / частковий» та під час моніторингу виявлено ознаки недоліків щодо стану виконання вимог законодавства у сфері кіберзахисту або повноти запроваджених заходів кіберзахисту, Адміністрація

Держспецзв’язку або її територіальні органи можуть надавати рекомендації щодо усунення виявлених недоліків та заходів, що мають бути виконані для підвищення рівня кіберзахисту на об’єкті державного контролю.

Інформація про такий результат оцінювання може враховуватися під час підготовки пропозицій до річного плану відповідно до пункту 12 Порядку.

5. Неподання суб’єктом державного контролю до Адміністрації Держспецзв'язку або її територіального органу в установлені законодавством строки інформації про здійснення щорічного оцінювання стану кіберзахисту є підставою для проведення позапланової перевірки відповідно до пункту 13 Порядку.

6. Для підтвердження фактичного стану виконання вимог законодавства у сфері кіберзахисту Адміністрація Держспецзв'язку використовує механізм письмового запиту до суб’єктів державного контролю щодо надання відповідної інформації та документів (у паперовій або електронній формі) відповідно до абзацу першого пункту 9 Порядку.

У документах, що супроводжують запит, зазначається застереження про те, що невиконання вимоги щодо подання запитуваної інформації та документів (у паперовій або електронній формі) є підставою для накладення адміністративного стягнення на посадових осіб суб’єкта державного контролю відповідно до абзацу п'ятого пункту 9 Порядку.

7. Відповідно до абзацу третього пункту 9 Порядку суб’єкти державного контролю зобов’язані опрацювати запит та надати Адміністрації Держспецзв'язку інформацію та підтвердні документи в паперовій або електронній формі у строк не пізніше 30 календарних днів з дня отримання відповідного запиту.

8. Результати, отримані в ході моніторингу стану кіберзахисту, враховуються під час основного (виконавчого) та заключного (підсумкового) етапів огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

V. Підходи до визначення вимог про усунення виявлених порушень за результатами перевірки

1. Процедурні аспекти перевірки, включаючи строки її проведення, етапи підготовки комісії, порядок взаємодії з керівництвом суб’єкта державного контролю та безпосередній алгоритм здійснення (від аналізу документів до оформлення акта про результати перевірки) визначаються та регулюються Порядком.

2. Реалізація кожного заходу підтверджується шляхом заповнення відповідної графи акта про результати перевірки, де зазначається пряме посилання на документ, що засвідчує виконання конкретної вимоги законодавства.

За кожним контрольним питанням комісія встановлює:

нормативну вимогу;

фактичні обставини;

докази;

висновок щодо дотримання або недотримання вимоги.

3. Методологія визначення результатів перевірки полягає в установленні відповідності діяльності суб’єкта державного контролю вимогам законодавства у сфері кіберзахисту за кожним окремим питанням на підставі даних, отриманих під час перевірки.

При визначенні рівня відповідності вимогам законодавства використовується якісний показник відповідності:

відповідає вимогам законодавства – заходи з кіберзахисту реалізовано у повному обсязі, що підтверджується наявністю актуальної внутрішньої документації та фактичним впровадженням відповідних заходів, зафіксованих під час перевірки;

невідповідність вимогам законодавства – встановлено невиконання або неналежне виконання конкретної обов’язкової вимоги законодавства у сфері кіберзахисту, що підтверджується фактичними даними та матеріалами, отриманими під час проведення перевірки.

4. До завершення перевірки комісія проводить підсумкову нараду, під час якої забезпечує можливість керівнику суб’єкта державного контролю, керівнику з кіберзахисту або іншій уповноваженій особі суб’єкта державного контролю уточнити фактичні обставини, надати письмові пояснення, зауваження, заперечення або додаткові підтвердні документи щодо питань, які розглядалися під час перевірки.

Письмові пояснення, зауваження або заперечення суб’єкта державного контролю, подані до завершення перевірки або під час ознайомлення з актом, долучаються до акта про результати перевірки як його невід’ємна частина.

5. Підсумковий результат перевірки формується на основі сукупності відповідей «так» чи «ні», внесених до акта про результати перевірки.

6. Усі виявлені під час перевірки факти невідповідності, а також копії документів, письмові пояснення або інші матеріали, що підтверджують стан реалізації заходів кіберзахисту, у разі потреби долучаються як додатки до акта про результати перевірки.

7. У разі виявлення порушень вживаються заходи реагування, передбачені Порядком, зокрема: видання припису про усунення порушень, складання протоколу про адміністративне правопорушення або надання рекомендацій щодо усунення порушень.

8. Припис про усунення порушень є обов'язковим до виконання та має містити:

зміст виявленого порушення з посиланням на конкретну норму законодавства;

чіткі вимоги щодо дій, необхідних для усунення порушення;

граничний строк виконання;

спосіб та форму підтвердження усунення порушення.

У разі неможливості своєчасного виконання вимог суб'єкт державного контролю може звернутися до Адміністрації Держспецзв'язку або її територіального органу щодо продовження строку виконання таких вимог з відповідним обґрунтуванням. Під час розгляду такого звернення враховуються характер порушення, ризик для безпечного функціонування об'єкта державного контролю, технічна складність необхідних заходів та надані суб'єктом державного контролю підтвердні матеріали.

Строк усунення порушень встановлюється індивідуально з урахуванням:

категорії та характеру виявленої невідповідності;

технічної складності реалізації необхідних заходів;

виду суб'єкта державного контролю у сфері кіберзахисту.

9. Підтвердження факту усунення порушень здійснюється шляхом повідомлення Адміністрації Держспецзв'язку або її територіального органу про виконання вимог, викладених в акті про результати перевірки, відповідно до абзацу другого пункту 21 Порядку.

10. У разі непідтвердження усунення порушень Адміністрація Держспецзв'язку вживає заходів, передбачених абзацом п'ятим підпункту 3 пункту 13 Порядку.

11. Узагальнені результати заходів державного контролю у сфері кіберзахисту враховуються під час:

планування подальших перевірок;

узагальнення типових порушень з метою удосконалення вимог законодавства;

підготовки щорічного звіту відповідно до абзацу четвертого пункту 12 Порядку.

Т.в.о. заступника директора департаменту –
начальника відділу Департаменту кіберзахисту
Адміністрації Держспецзв'язку Кирило ЗАПОРОЖЕЦЬ