



АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ

Департамент державного контролю
у сфері захисту інформації
та кіберзахисту

Адміністрації Державної служби
спеціального зв'язку та захисту
інформації України
(ДДК Адміністрації Держспецзв'язку)

вул. Солом'янська, 13, м. Київ, Україна, 03110

тел./факс: (044) 281-88-50

e-mail: ddk@cip.gov.ua

Голові Правління Інтернет Асоціації
України

Олександру САВЧУКУ

вул. О.Гончара, 15/3, офіс 22, м. Київ, 04053

№_____

Шановний пане Олександрє!

У Департаменті опрацьовано Ваші пропозиції та зауваження від 29.07.2025 № 79 до проєкту постанови Кабінету Міністрів України «Про затвердження Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту» (далі – проєкт постанови) в межах громадського обговорення.

За результатами опрацювання, підготовлено інформаційно-довідкові матеріали про врахування вищезазначених пропозицій і зауважень та проведено робочу зустріч з метою їх обговорення.

За результатами обговорення, Департаментом підготовлено оновлену редакцію проєкту постанови.

З огляду на необхідність невідкладного врегулювання визначених у проєкті постанови питань, у разі відсутності зауважень, просимо повідомити про це протягом трьох днів.

Додаток : Проєкт постанови на 11 арк.

З повагою

Директор Департаменту

Ігор СТЕЛЬНИК



UB Ольга Баленко, (044) 281-80-51

Адміністрація Держспецзв'язку

№11/01/01-9005/2025 від 28.08.2025

КЕП: Стельник І. В. 28.08.2025 11:42

3FAA9288358EC003040000008A373B0099AFE100

Сертифікат дійсний з 11.03.2025 00:00 до 10.03.2027 23:59



КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від _____ 2025 р. № _____

Київ

Про затвердження Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту

Відповідно до частини четвертої статті 15 Закону України «Про основні засади забезпечення кібербезпеки України» Кабінет Міністрів України **постановляє:**

Затвердити Порядок здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту, що додається.

Прем'єр-міністр України

Ю. СВИРИДЕНКО



UB
Адміністрація Держспецзв'язку
№11/01/01-9005/2025 від 28.08.2025
КЕП: Стельник І. В. 28.08.2025 11:42
3FAA9288358EC003040000008A373B0099AFE100
Сертифікат дійсний з 11.03.2025 00:00 до 10.03.2027 23:59

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від _____ 2025 р. № _____

ПОРЯДОК
здійснення державного контролю за додержанням вимог законодавства
у сфері кіберзахисту

Загальні положення

1. Цей Порядок визначає заходи державного контролю за додержанням вимог законодавства у сфері кіберзахисту (далі – державний контроль), порядок їх здійснення, права та обов’язки під час здійснення такого державного контролю, а також вимоги до оформлення результатів здійснення заходу державного контролю.

2. У цих Загальних вимогах терміни вживаються у такому значенні:

докази – будь-які фактичні дані, отримані під час проведення перевірки у відповідності до методики здійснення заходу державного контролю, на підставі яких встановлюється наявність чи відсутність фактів та обставин, що мають значення для складення акту за результатами перевірки;

методика здійснення заходу державного контролю – унормована сукупність питань, що є предметом контролю та підходів до їх розгляду, що визначаються в залежності від виду заходу контролю, передбачених цим Порядком, а також підходи до визначення рекомендацій щодо усунення виявлених недоліків та заходів, що мають бути виконанні для підвищення рівня кіберзахисту на об’єкті контролю за результатами моніторингу, або визначення вимог про усунення виявлених порушень за результатами перевірки.

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 авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 р. № 712 та 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, затвердженого Кабінетом Міністрів України.



УВ
Адміністрація Держспецзв’язку
№ 13/01/004003/2025 від 28.08.2025
КЕП: Стельник І. В. 28.08.2025 11:42
3FAA9288358EC003040000008A373B0099AFE100
Сертифікат дійсний з 11.03.2025 00:00 до 10.03.2027 23:59

3. Суб'єктами державного контролю за додержанням вимог законодавства у сфері кіберзахисту є органи державної влади, державні органи, органи місцевого самоврядування, утворені відповідно до закону військові формування, підприємства, установи, організації, які є власниками або розпорядниками інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація, вимога щодо захисту якої встановлена законом, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури (крім банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України) (далі – суб'єкти державного контролю).

4. Об'єктами державного контролю є:

інформаційні, електронні комунікаційні та інформаційно-комунікаційні системи, в яких обробляються державні інформаційні ресурси або інформація, вимога щодо захисту якої встановлена законом, об'єкти критичної інфраструктури, об'єкти критичної інформаційної інфраструктури (крім систем банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України);

процеси та процедури суб'єктів державного контролю, у разі, якщо методики здійснення заходів державного контролю передбачають контроль дотримання законодавства в сфері кіберзахисту у суб'єкта державного контролю в цілому, а не в окремій інформаційній, електронній комунікаційній та інформаційно-комунікаційній системі.

5. Державний контроль здійснюється Адміністрацією Держспецзв'язку та її територіальними органами шляхом проведення заходів контролю, зокрема у формі моніторингу стану кіберзахисту та перевірок, метою яких є аналіз стану додержання вимог законодавства в сфері кіберзахисту, виявлення недоліків або порушень вимог законодавства у сфері кіберзахисту, надання рекомендацій та вимог щодо усунення таких порушень, та запобігання таким порушенням у майбутньому.

6. Методика здійснення заходів державного контролю затверджується Адміністрацією Держспецзв'язку з урахуванням відповідного виду заходу державного контролю, визначеного цим Порядком.

Проведення моніторингу стану кіберзахисту

7. Моніторинг стану кіберзахисту є заходом державного контролю, який полягає в зборі та аналізі інформації про виконання заходів з оцінювання стану кіберзахисту, які здійснюються 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, затвердженого Кабінетом Міністрів України.

8. Суб'єкти державного контролю для цілей здійснення моніторингу стану кіберзахисту здійснюють планове оцінювання стану кіберзахисту (оцінювання дотримання вимог цільових профілів безпеки системи, самооцінювання та/або зовнішнє оцінювання стану кіберзахисту) щорічно та інформують Адміністрацію Держспецзв'язку або її відповідний територіальний орган про здійснення такого оцінювання в строк не пізніше 30 календарних днів з дати його завершення.

Оцінювання стану кіберзахисту та, відповідно, заходи державного контролю щодо об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури III і IV категорій критичності проводяться на добровільних засадах або у випадках, визначених законодавством.

9. Перше оцінювання стану кіберзахисту для цілей здійснення моніторингу здійснюється протягом дванадцяти календарних місяців з дати набрання чинності цього Порядку.

10. Узагальнені результати оцінювання стану кіберзахисту, оформлені відповідно до методики здійснення заходу державного контролю, та актуальний план кіберзахисту з урахуванням рекомендацій, викладених у звіті про результати оцінювання, направляються до Адміністрації Держспецзв'язку або її територіального органу разом з інформуванням про проведення оцінювання стану кіберзахисту.

11. Інформування про узагальнені результати оцінювання стану кіберзахисту та направлення планів кіберзахисту до Адміністрації Держспецзв'язку здійснюється шляхом завантаження уповноваженою особою суб'єкта державного контролю інформації про такі узагальнені результати та планів кіберзахисту з використанням електронної платформи моніторингу стану кіберзахисту, створення та забезпечення функціонування якої забезпечується Адміністрацією Держспецзв'язку.

До створення та початку функціонування електронної платформи моніторингу стану кіберзахисту, або у разі неможливості її використання (призупинення її роботи) більш ніж на одну добу, надсилання звітної документації здійснюється на адресу Адміністрації Держспецзв'язку шляхом:

використання системи електронної взаємодії органів виконавчої влади на адресу;

поштовим відправленням;

нарочним.

У випадку коли узагальнені результати та плани кіберзахисту містять службову інформацію або інформацію, що становить державну таємницю, їх надсилання здійснюється з дотримання нормативно-правових актів, які регламентують порядок поводження з такою інформацією.

12. Результати моніторингу враховуються Адміністрацією Держспецзв'язку при формуванні річного плану здійснення заходів державного контролю шляхом перевірок, а також 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, що здійснюється відповідно до Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, затвердженого постановою Кабінету Міністрів України від 11 листопада 2020 р. № 1176 (Офіційний вісник України 2020 р., № 98, ст. 3187).

13. Адміністрацією Держспецзв'язку здійснюється постійний моніторинг стану виконання суб'єктами державного контролю своїх планів кіберзахисту та, у разі необхідності, може письмово витребувати у суб'єктів державного контролю інформацію, що може підтверджувати фактичний стан їх виконання. Суб'єкти державного контролю зобов'язані надати Адміністрації Держспецзв'язку витребувану інформацію у строк не пізніше тридцяти календарних днів з дня надання такого запиту.

Проведення перевірки

14. Перевірка є заходом державного контролю, що здійснюється комісією, яка складається із посадових осіб Адміністрації Держспецзв'язку та/або її територіальних органів. В рамках підготовки до перевірки, Адміністрація Держспецзв'язку та/або її територіальний орган має право запитувати звіти про проведення суб'єктом державного контролю оцінювання стану кіберзахисту та інші додаткові матеріали, що стосуються предмету перевірки.

До заходів державного контролю за рішенням Адміністрації Держспецзв'язку можуть залучатися фахівці інших підрозділів Держспецзв'язку, а також органів державної влади, органів місцевого самоврядування, суб'єктів забезпечення кібербезпеки, визначених законодавством, за погодженням з їх керівниками.

15. Перевірки проводяться у формі планових або позапланових перевірок. Строк проведення перевірки не може перевищувати десяти робочих днів.

16. Підставою проведення планової перевірки є річний план здійснення заходів державного контролю, який затверджується Головою Держспецзв'язку або його заступником згідно з функціональним розподілом обов'язків у строк до 1 грудня року, що передує плановому та оприлюднюється на офіційному веб-сайті Держспецзв'язку.

Планова перевірка здійснюється у одного суб'єкта державного контролю не частіше ніж раз на три роки.

Про проведення планової перевірки суб'єкт державного контролю повідомляється письмово та (або) електронним листом на його офіційну електронну адресу за десять робочих днів до дати її початку.

Щороку до 01 квітня Адміністрацією Держспецзв'язку готується узагальнений звіт про результати здійснення моніторингу стану кіберзахисту та виконання річного плану здійснення заходів державного контролю, відкрита інформація з якого оприлюднюється на офіційному веб-сайті Держспецзв'язку.

17. Підставами проведення позапланової перевірки є:
звернення суб'єкта державного контролю до Адміністрації Держспецзв'язку про необхідність проведення перевірки;

повідомлення органу державної влади, державного органу, правоохоронного або контррозвідувального органу, який при здійсненні своїх повноважень, визначених законодавством, встановив ознаки порушення вимог законодавства в сфері кіберзахисту, в тому числі, ознаки порушення порядку 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;

неотримання Адміністрацією Держспецзв'язку та/або її територіальним органом у встановлені законодавством строки інформації про:

проведення суб'єктом державного контролю планової або позапланової авторизації з безпеки системи відповідно до Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затвердженого постановою Кабінету Міністрів України від 18 червня 2025 р. № 712;

проведення суб'єктом державного контролю щорічного оцінювання стану кіберзахисту для цілей здійснення моніторингу відповідно до цього Порядку;

проведення суб'єктом державного контролю оцінювання поточного стану кіберзахисту на підставі рекомендацій, наданих у встановленому законодавством порядку відповідною CSIRT в рамках функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози;

виконання у встановлені терміни вимог, визначених в акті за результатами проведення перевірки.

Рішення про проведення позапланової перевірки приймається Головою Держспецзв'язку або його заступником згідно з розподілом функціональних обов'язків.

Під час проведення позапланової перевірки з'ясовуються лише ті питання, необхідність перевірки яких стала підставою для здійснення такої перевірки, з обов'язковим зазначенням цих питань у приписі про здійснення заходу державного контролю.

18. Перевірка здійснюється відповідно до припису про здійснення заходу державного контролю за дотриманням законодавства в сфері кіберзахисту, який є документальною підставою для проведення перевірки, що затверджується Головою Держспецзв'язку або його заступником згідно з функціональним розподілом обов'язків, керівником територіального органу Адміністрації Держспецзв'язку (особою, що виконує його обов'язки), документів що

засвідчують осіб, які прибули для проведення перевірки, а також, за необхідності, довідок про наявність допуску до державної таємниці за встановленою формою.

В приписі про здійснення заходу державного контролю за дотриманням законодавства в сфері кіберзахисту має зазначатись наступна інформація:

- 1) дата затвердження та термін дії припису;
- 2) суб'єкт та об'єкт державного контролю, щодо якого здійснюється перевірка;
- 3) застосована методика здійснення заходу державного контролю;
- 4) форма проведення перевірки (планова чи позапланова);
- 5) підстава проведення перевірки;
- 6) перелік посадових осіб, які беруть участь у здійсненні заходу, із зазначенням їх посади, прізвища, ім'я та по батькові;
- 7) дата початку та дата закінчення перевірки;
- 8) інформація про здійснення попереднього заходу (тип заходу і строк його здійснення, за наявності).

19. Припис про здійснення заходу державного контролю головою комісії надається керівнику суб'єкта державного контролю в перший робочий день початку проведення перевірки.

У разі відсутності голови комісії з поважних причин, припис про здійснення заходу державного контролю надається керівнику суб'єкта державного контролю членом комісії.

Резолюція керівника суб'єкта державного контролю або особи, що виконує його обов'язки, про дозвіл на перевірку на лицьовому боці першого аркушу припису на право перевірки є підставою для початку перевірки.

У випадку ненадання керівником суб'єкта державного контролю або особою, що виконує його обов'язки, дозволу на перевірку встановленим вище порядком, зазначена посадова особа може бути притягнута до адміністративної або іншої відповідальності, згідно з законодавством.

Суб'єкт державного контролю має право не допускати членів комісії, що відповідно до припису про здійснення заходу державного контролю за дотриманням законодавства в сфері кіберзахисту уповноважені на проведення перевірки, якщо вони не пред'явили припису про здійснення заходу державного контролю та службового посвідчення.

20. Перевірка має проводитися в присутності особи, відповідальної за виконання функцій та завдань з кіберзахисту у суб'єкта державного контролю. У разі відсутності такої відповідальної особи перевірка проводиться в присутності керівника суб'єкта державного контролю або іншої уповноваженої особи, визначеної керівником суб'єкта державного контролю.

21. Комісія, що відповідно до припису про здійснення заходу державного контролю за дотриманням законодавства в сфері кіберзахисту уповноважена на проведення перевірки, під час здійснення перевірки має право:

ознайомлюватися з усіма документами та матеріалами, необхідними для здійснення перевірки;

надавати письмові запити та отримувати інформацію, у тому числі з обмеженим доступом з дотриманням вимог нормативно-правових актів щодо порядку поводження з такою інформацією, копії необхідних документів, письмові та усні пояснення посадових осіб з питань, що безпосередньо пов'язані із здійсненням заходів державного контролю;

отримувати доступ з урахуванням вимог нормативно-правових актів щодо охорони державної таємниці до території, будівлі, споруди, приміщення, робочого місця тощо у разі, якщо такий доступ безпосередньо пов'язаний із предметом перевірки з урахуванням методики здійснення заходу державного контролю;

здійснювати фактичну перевірку суб'єкта державного контролю та дослідження питань, що є предметом перевірки відповідно до методики здійснення заходу державного контролю, в тому числі перевіряти документи та дані, що стали підставою для проведення перевірки, отримувати докази та фіксувати процес порушення вимог нормативно-правових актів із кіберзахисту;

здійснювати опитування посадових осіб суб'єкта державного контролю, тестування та/або випробування впроваджених заходів кіберзахисту з урахуванням методики здійснення заходів державного контролю;

перевіряти дотримання нормативно-правових актів України щодо використання засобів технічного та криптографічного захисту інформації (зокрема на відповідність базовому та цільовому профілям безпеки, що затверджені в установленому законодавством порядку), а також програмного забезпечення, що виконує функції захисту інформації і використовується в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах суб'єктів контролю та на об'єктах критичної інформаційної інфраструктури (зокрема щодо відсутності їх у переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання);

складати за результатами проведення перевірки акт;

складати протоколи про адміністративні правопорушення, отримувати персональні дані та інші дані, необхідні для складання такого протоколу;

призначати службові розслідування для з'ясування причин та умов виникнення порушення вимог законодавства.

Суб'єкт державного контролю зобов'язаний надати комісії запитувану інформацію, що необхідна для проведення перевірки, у строк, що не перевищує три робочих дні.

22. В акті, який складається за результатами перевірки та надається суб'єкту державного контролю, зазначається:

1) дата початку та завершення перевірки в рамках державного контролю;

- 2) суб'єкт та об'єкт державного контролю, щодо якого здійснюється перевірка;
 - 3) особа, в присутності якої здійснювалась перевірка;
 - 4) підстава проведення перевірки;
 - 5) застосована методика здійснення заходів державного контролю;
 - 6) документи та інформація що були надані суб'єктом державного контролю;
 - 7) заходи перевірки, що були здійснені;
 - 8) у разі виявлення, опис встановленого порушення суб'єктом державного контролю, норма (норми) законодавства, недотримання якої (-их) визначено за результатами перевірки, або недоліки впровадження заходів з кіберзахисту та захисту інформації, які не є порушенням вимог законодавства;
 - 9) докази, зібрані під час перевірки, в тому числі ті що підтверджують встановлене порушення вимоги законодавства у сфері кіберзахисту, захисту інформації та/або недоліків впровадження заходів з кіберзахисту, які не є порушенням вимог законодавства;
 - 10) висновок перевірки;
 - 11) вимоги до суб'єкта державного контролю за результатами перевірки з метою усунення встановленого порушення вимоги законодавства та/або рекомендації для усунення виявлених недоліків, а також граничні терміни їх виконання;
 - 12) власні імена, прізвища та підписи голови, і членів комісії, що здійснювали перевірку.
- До акту перевірки, за наявності, додаються зауваження керівника суб'єкта державного контролю, або особи, яка виконує його обов'язки.

23. Акт перевірки складається у двох примірниках, які підписують голова та члени комісії.

Перший примірник акту перевірки надається суб'єкту державного контролю, другий зберігається в Адміністрації Держспецзв'язку.

У разі проведенні перевірки територіальним органом Адміністрації Держспецзв'язку додатково складається третій примірник акту, який зберігається у відповідному територіальному органі Адміністрації Держспецзв'язку.

24. Факт ознайомлення з актом перевірки керівник суб'єкта державного контролю або особа, яка виконує його обов'язки, засвідчує власним підписом. Якщо керівник суб'єкта державного контролю або особа, яка виконує його обов'язки, не погоджується з результатами перевірки, викладеними в акті перевірки, він підписує акт перевірки із зауваженнями. Зауваження є невід'ємною частиною акту перевірки.

У разі відмови керівника суб'єкта державного контролю або особи, яка виконує його обов'язки, засвідчити своїм підписом факт ознайомлення з актом перевірки, голова комісії робить в акті перевірки запис «відмовлено в підписанні», який засвідчується підписом голови та членів комісії.

25. Вимоги щодо приведення стану кіберзахисту у відповідність до норм та вимог встановлених нормативно-правовими актами України, викладені в акті складеному за результатами перевірки, є обов'язковими для виконання суб'єктом державного контролю.

Про результати виконання таких вимог суб'єкт державного контролю повідомляє Адміністрацію Держспецзв'язку або її територіальний орган у визначений в акті термін. У разі неможливості своєчасного виконання таких вимог, суб'єкт державного контролю письмово звертається до Адміністрації Держспецзв'язку або її територіального органу стосовно продовження термінів виконання таких вимог з відповідним обґрунтуванням.

26. У разі виявлення за результатами перевірки ознак порушення вимог законодавства в сфері кіберзахисту, які є передумовою для реалізації загрози безпечного функціонування відповідної інформаційної, електронної комунікаційної, інформаційно-комунікаційної системи, об'єкту критичної інфраструктури, об'єкту критичної інформаційної інфраструктури або технологічної системи суб'єкта державного контролю, або може призвести до завдання шкоди інтересам держави, Адміністрація Держспецзв'язку має право порушувати перед відповідними державними та/або правоохоронними органами питання про перевірку наявності ознак кримінальних правопорушень в діяльності суб'єктів державного контролю, або про порушення дисциплінарних проваджень за наявності ознак невиконання або неналежного виконання посадових обов'язків в частині виконання функцій та завдань з кіберзахисту у суб'єкта державного контролю.

Адміністрація Держспецзв'язку має право складати протоколи про адміністративні правопорушення та надсилати до суду матеріали про адміністративні правопорушення.

27. Посадові особи суб'єкта державного контролю зобов'язані забезпечувати: умови для проведення перевірки відповідно до припису про здійснення заходу державного контролю та законодавства;

надання за запитом голови комісії всіх необхідних для проведення перевірки документів та інформації, у тому числі з обмеженим доступом з дотриманням відповідних зобов'язань щодо її охорони, копії необхідних документів, у разі необхідності, письмових та усних пояснень відповідних посадових осіб з питань, що безпосередньо пов'язані із здійсненням заходів державного контролю;

безперешкодний доступ комісії до об'єктів, що підлягають фактичній перевірці;

безперешкодне збирання доказів;

надання за запитом комісії необхідних персональних та інших даних для складання протоколу про адміністративне правопорушення.

28. Посадові особи суб'єкта державного контролю несуть відповідальність згідно із законом за перешкоджання законній діяльності посадовим особам

Держспецзв'язку або невиконання їх вимог, наданих відповідно до цього Порядку при здійсненні ними заходів державного контролю.

29. Посадові особи Держспецзв'язку, які проводять перевірки, зобов'язані дотримуватись норм законодавства та несуть відповідальність згідно із законодавством.

30. Суб'єкт державного контролю має право вимагати нерозголошення інформації з обмеженим доступом. Під час та після здійснення заходів державного контролю посадові особи Держспецзв'язку зобов'язані поводитись такою інформацією відповідно до законодавства.
