



**НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

**Створення комплексів технічного захисту інформації
Атестація комплексів
Основні положення**

Департамент спеціальних телекомунікаційних систем та
захисту інформації Служби безпеки України

Київ 2001

**НОРМАТИВНИЙ ДОКУМЕНТ
СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

Затверджено
наказом Департаменту спеціальних
телекомунікаційних систем та
захисту інформації
Служби безпеки України
від “9” лютого 2001 р. № 2

**Створення комплексів технічного захисту інформації
Атестація комплексів
Основні положення**

НД ТЗІ 2.1-001-2001

ДСТСЗІ СБ України

Київ

ПЕРЕДМОВА

РОЗРОБЛЕНО І ВНЕСЕНО Головним управлінням технічного захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

ВВЕДЕНО ВПЕРШЕ

Цей нормативний документ не може бути повністю чи частково відтворений, тиражований та розповсюджений без дозволу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України

ЗМІСТ

1	Галузь використання	1
2	Нормативні посилання	1
3	Визначення.....	1
4	Загальні положення.....	1
5	Порядок організації та проведення атестації.....	2
	Додаток 1 Перелік відомостей про об'єкт інформаційної діяльності та комплекси технічного захисту інформації	4
	Додаток 2 Зміст акта атестації.....	5
	Додаток 3 Зміст акта атестації комплексу технічного захисту інформації на особливо важливому об'єкті інформаційної діяльності	6

**Створення комплексів технічного захисту інформації.
Атестація комплексів.
Основні положення**

Чинний від 2001-02-20

1 Галузь використання

Дія цього нормативного документа (НД) поширюється на комплекси технічного захисту інформації (ТЗІ) від витоку технічними каналами на об'єктах інформаційної діяльності (ОІД).

НД встановлює загальні вимоги до організації атестації комплексів щодо повноти та якості робіт з ТЗІ відповідно до ДСТУ 3396.1-96 та визначає порядок проведення цієї атестації.

НД призначений для державних органів, органів місцевого самоврядування, органів управління Збройних Сил України, інших військових формувань, підприємств, організацій, установ, діяльність яких пов'язана з інформацією, необхідність охорони якої визначено законодавством України, а також виконавців робіт з ТЗІ.

2 Нормативні посилання

У цьому НД наведено посилання на такі документи:

ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;

ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

3 Визначення

У цьому НД використовують терміни відповідно до ДСТУ 3396.2-97.

Визначення інших термінів:

Об'єкт інформаційної діяльності - інженерно-технічна споруда, приміщення, де здійснюється адміністративна, виробнича та інша діяльність, пов'язана з інформацією, що підлягає захисту від витоку технічними каналами.

Комплекс ТЗІ - сукупність заходів та засобів, призначених для реалізації ТЗІ на ОІД.

Атестація комплексу ТЗІ - оцінювання ефективності комплексу технічного захисту інформації, що циркулюватиме на ОІД, на відповідність вимогам нормативних документів з ТЗІ.

Особливо важливий ОІД - ОІД, на якому циркулює інформація, захист якої забезпечується згідно з вимогами 1 категорії.

4 Загальні положення

4.1 Атестація комплексу ТЗІ (далі - атестація) здійснюється за відповідними програмою і методиками випробувань.

На підставі результатів випробувань складається висновок щодо відповідності стану ТЗІ, який забезпечується комплексом, вимогам нормативних документів з ТЗІ.

4.2 Атестація може бути первинною, черговою та позачерговою.

Первинна атестація здійснюється після (або під час) приймання робіт із створення комплексу ТЗІ.

Термін проведення чергової атестації визначається технічним паспортом на комплекс ТЗІ або актом попередньої атестації.

Позачергову атестацію проводять у разі змін умов функціонування ОІД, що приводять до змін загроз для інформації, та за висновками органів, які контролюють стан ТЗІ.

4.3 Етапи атестації:

- визначення організації-виконавця атестації та оформлення відповідних організаційних документів;

- аналіз умов функціонування ОІД, технічної документації на комплекс ТЗІ та розроблення і оформлення Програми і методик атестації (ПМА);

- проведення випробувань відповідно до ПМА та оформлення протоколів випробувань і підсумкового документа - акта атестації.

4.4 Суб'єкти атестації:

- Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України (далі - Департамент);

- організації-замовники атестації;

- організації-виконавці атестації.

4.5 Департамент

- організує розроблення та удосконалення нормативних документів з атестації;

- контролює виконання вимог щодо атестації та розглядає апеляції;

- узгоджує вибір організації-виконавця атестації, ПМА та результати атестації на особливо важливих ОІД.

4.6 Витрати на проведення атестації включаються до кошторису на проектування, будівництво та експлуатацію (утримання) ОІД.

5 Порядок організації та проведення атестації

5.1 Організація-замовник на засадах, передбачених законодавством щодо закупівель послуг за рахунок державних коштів, визначає організацію-виконавця атестації.

Організацією-виконавцем атестації може бути підприємство, установа чи організація, які мають відповідну ліцензію або дозвіл на провадження діяльності в галузі ТЗІ, одержані у встановленому законодавством порядку.

Відносини між організацією-замовником та організацією-виконавцем, яка є ліцензіатом, регламентуються укладеним між ними договором.

У разі проведення атестації на особливо важливих ОІД визначення організації-виконавця атестації узгоджується з Департаментом.

5.2 Організація-виконавець за результатами аналізу відомостей (додаток 1), наданих організацією-замовником, та, за необхідності, за результатами аналізу умов функціонування ОІД і загроз для інформації безпосередньо на ОІД, розробляє проект ПМА та подає його на узгодження організації-замовнику.

Узгоджений організацією-замовником проект ПМА затверджує організація-виконавець.

У разі атестації комплексу ТЗІ на особливо важливих ОІД проект ПМА узгоджується також з Департаментом.

5.3 Організація-замовник створює умови проведення атестації, передбачені договором та ПМА.

Організація-виконавець проводить випробування відповідно до ПМА та оформляє акт атестації за формою додатку 2 у 2-х примірниках (1-й надається організації-замовнику, 2-й – зберігається у організації-виконавця).

До акту атестації додаються протоколи випробувань, передбачених ПМА.

За результатами атестації заповнюється технічний паспорт на комплекс ТЗІ.

5.4 У разі проведення атестації на особливо важливих ОІД матеріали з атестації у 5-денний термін організація-виконавець надає Департаменту. Департамент у 2-тижневий термін розглядає результати атестації, приймає рішення щодо можливості їх узгодження, реєструє акт атестації (додаток 3) та надсилає його організації-замовнику, одночасно інформуючи про це організацію-виконавця.

5.5 У разі незгоди з результатами атестації організація-замовник має право направити до Департаменту апеляцію. Департамент у місячний термін за апеляцією приймає відповідні рішення.

Повторна атестація проводиться за рахунок винного.

Додаток 1
(рекомендований)

Перелік відомостей
про об'єкти інформаційної діяльності та комплекси технічного захисту
інформації

Гриф обмеження доступу
(за необхідності)

1 Відомості про ОІД (по кожному ОІД окремо): найменування, позначення, розташування, приналежність відповідному підрозділу тощо.

2 Технологічні процеси під час функціонування ОІД із визначенням інформації, що підлягає захисту від витоку технічними каналами. Ступінь обмеження доступу до інформації.

3 Схеми затверджених контрольованих зон, їх опис.

4 Перелік технічних засобів (основних і допоміжних), розташованих в межах контрольованих зон, та відомості про їх елементи, що перетинають цю межу.

5 Зовнішні фактори, які можуть спричинити виникнення загроз для інформації.

6 Організаційна структура забезпечення захисту інформації на об'єкті.

7 Короткі відомості про комплекс ТЗІ на ОІД:

- про категорію вимог із захищеності інформації;
- можливі технічні канали витоку інформації;
- склад комплексу ТЗІ та схема розміщення його елементів;
- перелік експлуатаційних документів на комплекс ТЗІ.

8 Розробник комплексу ТЗІ.

9 Проектувальник та виконавець будівельно-монтажних робіт, які проводилися на забезпечення впровадження комплексу ТЗІ.

10 Виконавець робіт з ТЗІ.

11. Відомості про приймання робіт із створення комплексу ТЗІ.

12 Строк проведення та висновки попередньої атестації.

13 Підстави для проведення атестації.

Керівник організації-замовника

підпис, ініціали, прізвище

Додаток 2

Зміст
акта атестації

Гриф обмеження доступу
(за необхідності)

повна назва організації-виконавця

АКТ АТЕСТАЦІЇ
комплексу технічного захисту інформації
(позначення об'єкта інформаційної діяльності, на якому розташований комплекс,
повна назва організації-замовника)

№ _____ « ____ » _____ 200_ р.

Дійсний до « ____ » _____ 200_ р.

Період проведення атестації.

Підстави для проведення атестації (документ щодо залучення організації-виконавця, повна назва Програми і методик атестації з реквізитами, ким погоджено, затверджено).

Короткі відомості про об'єкт інформаційної діяльності та комплекс технічного захисту інформації.

Виклад результатів випробувань (за окремими пунктами Програми і методик атестації).

Зауваження і рекомендації.

Додаткові умови, яких необхідно дотримуватись під час експлуатації (відмінні відносно передбачених експлуатаційною документацією, за необхідності).

Висновки щодо відповідності комплексу технічного захисту інформації вимогам нормативних документів.

Строк проведення чергової атестації.

Перелік додатків (протоколи випробувань та інші матеріали, що були оформлені під час проведення атестації).

Керівник організації-виконавця

підпис, ініціали, прізвище

« ____ » _____ 200__ р.

Додаток 3

Зміст
акта атестації комплексу технічного захисту інформації
на особливо важливому об'єкті інформаційної діяльності

Гриф обмеження доступу
(за необхідності)

повна назва організації-виконавця

АКТ АТЕСТАЦІЇ
комплексу технічного захисту інформації
(позначення об'єкта інформаційної діяльності, на якому розташований комплекс,
повна назва організації-замовника)

№ _____

« ____ » _____ 200__ р.

Зареєстровано в Департаменті спеціальних
телекомунікаційних систем та захисту
інформації Служби безпеки України

« ____ » _____ 200__ р. за № _____

Дійсний до « ____ » _____ 200__ р.

Керівник Департаменту

(підпис) (ініціали, прізвище)
« ____ » _____ 200__ р.
м.п.

Період проведення атестації.

Підстави для проведення атестації (документ щодо залучення організації-виконавця,
повна назва Програми і методик атестації з реквізитами, ким погоджено, затверджено).

Короткі відомості про об'єкт інформаційної діяльності та комплекс технічного
захисту інформації.

Виклад результатів випробувань (за окремими пунктами Програми і методик
атестації).

Зауваження і рекомендації.

Додаткові умови, яких необхідно дотримуватись під час експлуатації (відмінні відносно передбачених експлуатаційною документацією, за необхідності).

Висновки щодо відповідності комплексу технічного захисту інформації вимогам нормативних документів.

Строк проведення чергової атестації.

Перелік додатків (протоколи випробувань та інші матеріали, що були оформлені під час проведення атестації).

Керівник організації-виконавця

«___»_____200__ р.

підпис, ініціали, прізвище