АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Н А К А З

16.05.2007 N 87

Зареєстровано в Міністерстві юстиції України 10 липня 2007 р. за N 785/14052

Про затвердження Положення про державний контроль за станом технічного захисту інформації

{ Із змінами, внесеними згідно з Наказами Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 N 275 (z0876-13) від 20.05.2013 }

Відповідно до Закону України "Про Державну службу спеціального зв'язку та захисту інформації України" (3475-15) **Н А К А З У Ю**:

1. Затвердити Положення про державний контроль за станом технічного захисту інформації, що додається.

2. Департаменту державного контролю за станом криптографічного та технічного захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України.

3. Визнати таким, що втратив чинність, наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 22.12.99 N 61 (z0010-00) "Про затвердження Положення про контроль за функціонуванням системи технічного захисту інформації", зареєстрований у Міністерстві юстиції України 11.01.2000 за N 10/4231.

4. Контроль за виконанням наказу покласти на заступника Голови Держспецзв'язку відповідно до розподілу функціональних обов'язків.

{ Пункт 4 в редакції Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

Голова Служби Ю.Б.Чеботаренко

ЗАТВЕРДЖЕНО Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.2007 N 87

Зареєстровано в Міністерстві юстиції України 10 липня 2007 р. за N 785/14052

ПОЛОЖЕННЯ про державний контроль за станом технічного захисту інформації

1. Загальні положення

1.1. Це Положення визначає порядок організації та здійснення державного контролю за станом технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Державний контроль за станом технічного захисту інформації (далі - ТЗІ) здійснюється Державною службою спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку) відповідно до Законів України "Про Державну службу спеціального зв'язку та захисту інформації України" (3475-15), "Про захист інформації в інформаційно-телекомунікаційних системах" (80/94-ВР) та Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України (717/2011), затвердженого Указом Президента України від 30 червня 2011 року N 717. { Абзац другий пункту 1.1 розділу 1 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 275 (z0876-13) від 20.05.2013 }

1.2. Дія Положення поширюється на всі суб'єкти системи технічного захисту інформації.

Державний контроль за станом технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, здійснюється в органах державної влади, органах місцевого самоврядування, утворених відповідно до законодавства військових формуваннях, на підприємствах, в установах і організаціях незалежно від форми власності, у тому числі в закордонних дипломатичних установах України, а також місцях постійного і тимчасового перебування вищих посадових осіб держави (далі - органи, щодо яких здійснюється ТЗІ).

1.3. У Положенні наведені нижче терміни вживаються у таких значеннях:

об'єкти протидії (ОПД) - озброєння, військова та спеціальна техніка, об'єкти оборонно-промислового комплексу, військові об'єкти та об'єкти, використання яких передбачено в ході проведення заходів з мобілізації, інші об'єкти, призначені для застосування в інтересах оборони і безпеки держави; { Пункт 1.3 розділу 1 доповнено абзацом згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

відомості, що охороняються, - секретна інформація стосовно ОПД, що становить державну таємницю; { Пункт 1.3 розділу 1 доповнено абзацом згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

контрольно-інспекторська робота з питань ТЗІ - діяльність, спрямована на визначення та вдосконалення стану ТЗІ в органах, щодо яких здійснюється ТЗІ;

об'єкт "особливої норми" - місце постійного або тимчасового перебування посадової особи, щодо якої здійснюється державна охорона, призначене для здійснення нею діяльності, пов'язаної з інформацією, необхідність захисту якої визначено законодавством; { Абзац п'ятий пункту 1.3 розділу 1 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

передумови витоку (просочення) інформації технічними каналами - наявність технічного каналу поширення інформації за відсутності підтвердженої відповідності впроваджених заходів вимогам та нормам з ТЗІ;

порушення в сфері ТЗІ - невиконання вимог нормативно-правових актів та нормативних документів системи ТЗІ за категоріями, які визначають можливість реалізації загроз безпеці інформації;

реальна загроза витоку (просочення) інформації технічними каналами - наявність технічного каналу поширення інформації за умов підтвердження відповідними інструментально-розрахунковими методами невідповідності впроваджених заходів вимогам та нормам з ТЗІ;

технічний канал поширення інформації - сукупність джерела інформації та середовища її поширення.

Інші терміни вживаються в Положенні у значеннях, визначених у Законах України "Про державну таємницю" (3855-12), "Про захист інформації в інформаційно-телекомунікаційних системах" (80/94-ВР), "Про інформацію" (2657-12), "Про Державну службу спеціального зв'язку та захисту інформації України" (3475-15) та ДСТУ 3396.2-97 "Технічний захист інформації. Терміни та визначення", НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу".

1.4. Державний контроль за станом ТЗІ полягає в перевірці виконання вимог нормативно-правових актів і нормативних документів з ТЗІ та здійснюється з метою визначення стану ТЗІ в органах, щодо яких здійснюється ТЗІ, виявлення порушень з ТЗІ та запобігання їм.

1.5. Державний контроль за станом ТЗІ здійснюється Держспецзв'язку шляхом організації та проведення контрольно-інспекторської роботи з питань ТЗІ стосовно органів, щодо яких здійснюється ТЗІ.

1.6. Контрольно-інспекторська робота з питань ТЗІ включає планування, проведення інспекційних перевірок стану ТЗІ в органах, щодо яких здійснюється ТЗІ (далі - перевірка), аналіз їх результатів та надання рекомендацій щодо вдосконалення стану ТЗІ в зазначених органах.

1.7. За результатами контрольно-інспекторської роботи здійснюються аналіз та узагальнення стану ТЗІ в державі.

Аналітичні матеріали щодо стану ТЗІ в державі подаються Президентові України, Голові Верховної Ради України і Прем'єр-міністру України.

2. Організація проведення перевірок стану ТЗІ

2.1. Перевірки стану ТЗІ поділяються на комплексні, цільові (тематичні) та контрольні. Зазначені перевірки можуть бути плановими та позаплановими.

2.2. При комплексній перевірці визначається відповідність комплексу ТЗІ (комплексної системи захисту інформації) та заходів протидії технічним розвідкам вимогам нормативно-правових актів та нормативних документів системи ТЗІ.

{ Пункт 2.2 розділу 2 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

2.3. При цільовій (тематичній) перевірці перевіряються окремі складові комплексу ТЗІ (комплексної системи захисту інформації) та заходів протидії технічним розвідкам на відповідність упроваджених заходів вимогам нормативно-правових актів та нормативних документів системи ТЗІ.

{ Пункт 2.3 розділу 2 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

2.4. При контрольній перевірці перевіряється повнота та достатність проведених заходів щодо усунення недоліків, які були виявлені в ході проведення попередньої комплексної або цільової перевірки. Контрольні перевірки проводяться за потреби, як правило, після отримання повідомлення про усунення недоліків.

2.5. Планові перевірки здійснюються згідно з річним планом контрольно-інспекторської роботи з питань ТЗІ, затвердженим Головою Держспецзв'язку. Витяги з плану контрольно-інспекторської роботи надсилаються до центральних органів виконавчої влади та в разі потреби до підприємств, установ і організацій.

2.6. Позапланові перевірки здійснюються у разі наявності відомостей щодо порушень виконання вимог нормативно-правових актів з питань ТЗІ або з метою визначення повноти та достатності заходів з ТЗІ, вжитих органами, щодо яких здійснюється ТЗІ. Зазначені перевірки можуть проводитися з попередженням або без попередження.

2.7. Керівництву органів, щодо яких здійснюється ТЗІ, повідомляється про проведення перевірки не менше ніж за десять діб до її початку (за винятком проведення позапланової перевірки).

2.8. Перевірки стану ТЗІ здійснюються посадовими особами структурного підрозділу Адміністрації Держспецзв'язку з питань державного контролю за станом криптографічного та технічного захисту інформації і регіональних органів Держспецзв'язку. До перевірок можуть залучатися фахівці інших підрозділів Держспецзв'язку, а також органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій за погодженням з їх керівниками.

{ Пункт 2.8 розділу 2 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

2.9. Підставою для допуску посадових осіб Держспецзв'язку до перевірки стану ТЗІ є наявність припису (додаток 1) на право проведення перевірки за підписом керівництва Адміністрації Держспецзв'язку або начальника регіонального органу Держспецзв'язку.

2.10. Посадові особи Держспецзв'язку, включені до припису на право проведення перевірки, є уповноваженими особами для складання протоколів про адміністративні правопорушення.

3. Права посадових осіб Держспецзв'язку

3.1. Посадові особи Держспецзв'язку, які здійснюють перевірки стану ТЗІ, мають право:

доступу на об'єкти інформаційної діяльності органів, щодо яких здійснюється ТЗІ, для здійснення державного контролю за станом ТЗІ, а також до інших приміщень (на територію, у споруди тощо) для вивчення питань, безпосередньо пов'язаних з перевіркою;

ознайомлюватися з будь-якими документами, необхідними для перевірки;

безкоштовно отримувати копії необхідних документів, письмові пояснення посадових осіб (довідки тощо) з питань, що виникають під час перевірки;

надавати за результатами перевірок рекомендації щодо приведення стану ТЗІ у відповідність до вимог нормативно-правових актів та здійснювати контроль за ходом їх виконання;

порушувати в установленому порядку питання щодо зупинення дії або скасування спеціальних дозволів на провадження діяльності, пов'язаної з державною таємницею, у разі виявлення порушень з технічного захисту секретної інформації;

складати протоколи про адміністративні правопорушення та надавати до суду на розгляд справи про адміністративні правопорушення.

3.2. При встановленні фактів вчинення порушень, передбачених Кодексом України про адміністративні правопорушення (80731-10, 80732-10), посадовими особами Держспецзв'язку, у межах повноважень, визначених статтею 255 Кодексу України про адміністративні правопорушення, складається протокол про адміністративне правопорушення.

4. Порядок проведення перевірок стану ТЗІ

4.1. Для проведення перевірки стану ТЗІ посадові особи Держспецзв'язку повинні пред'явити керівнику або вповноваженому представнику органу, щодо якого здійснюється ТЗІ, припис на право проведення перевірки та службові посвідчення.

4.2. При проведенні перевірки стану ТЗІ контролю підлягають повнота та достатність упроваджених на об'єктах інформаційної діяльності та об'єктах протидії заходів з ТЗІ, їх відповідність вимогам нормативно-правових актів, виконання рекомендацій щодо усунення порушень з ТЗІ.

{ Пункт 4.2 розділу 4 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

4.3. За результатами перевірок посадовими особами Держспецзв'язку, які їх здійснювали, складаються акти перевірок стану ТЗІ.

4.4. Акт комплексної перевірки стану ТЗІ складається за встановленою формою (додаток 2). Акти контрольних та цільових (тематичних) перевірок складаються у довільній формі.

4.5. Акт перевірки стану ТЗІ готується в двох примірниках. Перший примірник акта перевірки надсилається до суб'єкта системи ТЗІ, що перевірявся, другий - до структурного підрозділу Адміністрації Держспецзв'язку з питань державного контролю за станом криптографічного та технічного захисту інформації.

У разі проведення перевірки регіональним органом Держспецзв'язку готується третій примірник, який надсилається до органу Держспецзв'язку, посадові особи якого здійснювали перевірку.

4.6. Усі примірники акта підписуються посадовими особами Держспецзв'язку, якими проводилася перевірка, та затверджуються керівником Адміністрації Держспецзв'язку або начальником регіонального органу Держспецзв'язку, який підписав припис на проведення перевірки.

Ознайомлення керівника органу, щодо якого здійснюється ТЗІ, з актом здійснюється за його підписом.

4.7. У разі відмови керівника органу, щодо якого здійснюється ТЗІ, засвідчити факт ознайомлення з актом перевірки своїм підписом, посадовими особами Держспецзв'язку, що здійснювали перевірку, робиться в акті відповідний запис.

5. Кваліфікація порушень з ТЗІ

5.1. Порушення вимог з ТЗІ поділяються на три категорії, які визначають можливість реалізації загроз безпеці інформації:

перша категорія - невиконання вимог нормативно-правових актів та нормативних документів з ТЗІ, унаслідок чого створюється реальна загроза порушення конфіденційності, зокрема за рахунок витоку (просочення) технічними каналами та (або) цілісності й доступності інформації; { Абзац другий пункту 5.1 розділу 5 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

друга категорія - невиконання вимог нормативно-правових актів та нормативних документів з ТЗІ, унаслідок чого створюються передумови до порушення конфіденційності, зокрема за рахунок витоку (просочення) технічними каналами та (або) цілісності й доступності інформації; { Абзац третій пункту 5.1 розділу 5 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

третя категорія - невиконання інших вимог з ТЗІ.

5.2. Кваліфікаційні ознаки порушень з ТЗІ

Ознаки порушень першої категорії:

установлення факту циркуляції інформації з обмеженим доступом на об'єктах інформаційної діяльності, в інформаційних або інформаційно-телекомунікаційних системах за умов підтвердження інструментально-розрахунковими методами наявності технічного каналу поширення інформації з обмеженим доступом;

установлення факту обробки інформації з обмеженим доступом в інформаційних, телекомунікаційних або інформаційно-телекомунікаційних

системах, які мають вихід незахищеними каналами зв'язку за межі контрольованої зони, за умов відсутності атестата відповідності на комплексну систему захисту інформації; { Абзац четвертий пункту 5.2 розділу 5 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

установлення факту обробки інформації з обмеженим доступом в інформаційних або інформаційно-телекомунікаційних системах, які не мають виходу за межі контрольованої зони, за умов доступу до її інформаційних ресурсів користувачів, які мають різні повноваження (права доступу до інформації), та відсутності атестата відповідності на комплексну систему захисту інформації;

установлення факту обробки відкритої інформації, що є власністю держави, вимога щодо захисту якої встановлена законом, в інформаційно-телекомунікаційних системах, які мають підключення до телекомунікаційних мереж (у тому числі телекомунікаційних мереж загального користування), за умов відсутності атестата відповідності на комплексну систему захисту інформації; { Пункт 5.2 розділу 5 доповнено абзацом згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

установлення факту несанкціонованого доступу користувачів інформаційних, телекомунікаційних або інформаційно-телекомунікаційних систем до інформації, що є власністю держави, або інформації з обмеженим доступом шляхом порушення встановлених правил розмежування доступу або подолання заходів захисту. { Абзац сьомий пункту 5.2 розділу 5 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

Ознаки порушень другої категорії:

установлення факту циркуляції інформації з обмеженим доступом на об'єктах інформаційної діяльності, в інформаційних або інформаційно-телекомунікаційних системах за умов відсутності підтвердження інструментально-розрахунковими методами відповідності комплексу ТЗІ нормам та вимогам з ТЗІ;

установлення факту обробки інформації з обмеженим доступом в інформаційно-телекомунікаційних системах, які мають вихід за межі контрольованої зони захищеними каналами, за умов відсутності атестата відповідності на комплексну систему захисту інформації; { Пункт 5.2 розділу 5 доповнено абзацом згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

установлення факту обробки інформації, що є власністю держави, або інформації з обмеженим доступом в інформаційних, телекомунікаційних або інформаційно-телекомунікаційних системах, які не мають виходу за межі контрольованої зони, за умов відсутності атестата відповідності на комплексну систему захисту інформації. { Абзац пункту 5.2 розділу 5 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

Невиконання вимог нормативно-правових актів щодо впровадження організаційних заходів з ТЗІ, а також інших норм та вимог у сфері захисту інформації, які не призводять до порушень першої або другої категорії, кваліфікується як порушення третьої категорії.

Визначення ознак порушень з протидії технічним розвідкам за відповідними категоріями та їх кваліфікація здійснюються згідно з вимогами нормативних документів системи ТЗІ. { Пункт 5.2 розділу 5 доповнено абзацом згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

6. Висновки перевірок стану ТЗІ та рекомендації

6.1. Висновок перевірки є результатом адміністративно-правової оцінки стану ТЗІ, повноти та достатності заходів щодо впровадження комплексу технічного захисту інформації (комплексної системи захисту інформації) та заходів протидії технічним розвідкам, їх відповідності вимогам нормативно-правових актів з ТЗІ. { Абзац перший пункту 6.1 розділу 6 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

Основним критерієм відповідності стану ТЗІ вимогам нормативних документів та нормативно-правових актів є відсутність порушень з ТЗІ.

6.2. Висновки перевірок стану ТЗІ та критерії їх складання:

6.2.1. Стан технічного захисту інформації відповідає вимогам нормативно-правових актів.

Критерієм висновку є відсутність будь-яких порушень норм та вимог з ТЗІ.

6.2.2. Стан технічного захисту інформації відповідає вимогам нормативно-правових актів за винятком виявлених недоліків.

Критерієм висновку є наявність хоча б одного порушення з ТЗІ третьої категорії.

6.2.3. Стан технічного захисту інформації не повною мірою відповідає вимогам нормативно-правових актів, що створює передумови для порушення її конфіденційності, цілісності, доступності та (або) витоку технічними каналами, а також витоку відомостей про ОПД, що охороняються. { Абзац перший підпункту 6.2.3 пункту 6.2 розділу 6 із змінами, внесеними згідно з Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

Критерієм висновку є наявність хоча б одного порушення з ТЗІ другої категорії.

6.2.4. Стан технічного захисту інформації не відповідає вимогам нормативно-правових актів, що створює реальну загрозу порушення її конфіденційності, цілісності, доступності та (або) витоку технічними каналами, а також витоку відомостей про ОПД, що охороняється. { Абзац перший підпункту 6.2.4 пункту 6.2 розділу 6 в редакції Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

Критерієм висновку є наявність хоча б одного порушення з ТЗІ першої категорії.

6.3. Висновок за результатами контрольної перевірки, крім оцінки стану ТЗІ, повинен відображати повноту виконання рекомендацій (виконано, не виконано, виконано не в повному обсязі) щодо приведення стану ТЗІ у відповідність до вимог нормативно-правових актів та нормативних документів з ТЗІ, наданих в акті попередньої перевірки.

6.4. Висновок за результатами цільової (тематичної) перевірки повинен визначати оцінку стану ТЗІ в окремих складових комплексу технічного захисту інформації (комплексної системи захисту інформації) та/або заходів протидії, що перевірялися.

{ Пункт 6.4 розділу 6 в редакції Наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації N 192 (z0029-09) від 08.12.2008 }

6.5. З метою приведення стану ТЗІ у відповідність до вимог нормативно-правових актів та нормативних документів з ТЗІ посадовими особами Держспецзв'язку, які здійснювали перевірку, в акті перевірки надаються конкретні рекомендації щодо усунення виявлених порушень, виконання яких є обов'язковим для посадових осіб органів, щодо яких здійснюється ТЗІ.

6.6. Для з'ясування причин, які призвели до порушень першої категорії, а також притягнення осіб, які їх вчинили, до відповідальності посадовими особами Держспецзв'язку ініціюється проведення відповідних розслідувань.

6.7. У разі виявлення порушень з ТЗІ першої або другої категорії посадовими особами Держспецзв'язку, що здійснювали перевірку, у встановленому порядку можуть порушуватися питання про припинення інформаційної діяльності на відповідних об'єктах.

Дозвіл на відновлення робіт, під час виконання яких були виявлені порушення норм і вимог з ТЗІ першої або другої категорії, дає керівник органу, щодо якого здійснюється ТЗІ, за погодженням з Держспецзв'язку після усунення порушень.

6.8. З метою приведення стану ТЗІ у відповідність до вимог нормативно-правових актів та нормативних документів з ТЗІ, а також виконання рекомендацій, наданих за результатами перевірки, керівниками органів, щодо яких здійснюється ТЗІ, у місячний термін після отримання акта перевірки затверджується план усунення недоліків, один примірник якого надсилається до органу Держспецзв'язку, посадовими особами якого було здійснено перевірку.

6.9. Повідомлення про виконання рекомендацій щодо приведення стану ТЗІ у відповідність до вимог нормативно-правових актів та нормативних документів з ТЗІ надсилається керівнику підрозділу Держспецзв'язку, посадовими особами якого було здійснено перевірку, у терміни, зазначені в акті перевірки та плані усунення недоліків.

6.10. Керівники органів, щодо яких здійснюється ТЗІ, мають право оскаржувати результати перевірок у порядку, визначеному законодавством України.

7. Обов'язки та відповідальність

7.1. Посадові особи органів, щодо яких здійснюється ТЗІ, під час перевірки зобов'язані надавати всі необхідні для проведення перевірки документи та забезпечувати умови для її проведення.

7.2. За перешкоджання законній діяльності Держспецзв'язку при здійсненні державного контролю за станом ТЗІ винні особи несуть відповідальність згідно із законодавством України.

7.3. Посадові особи та громадяни, винні в невиконанні норм і вимог технічного захисту секретної інформації, унаслідок чого виникає реальна загроза порушенню конфіденційності, зокрема за рахунок витоку (просочення) технічними каналами, цілісності й доступності цієї інформації, несуть відповідальність згідно із законодавством України.

7.4. Керівники органів, щодо яких здійснюється ТЗІ, зобов'язані вжити невідкладних заходів щодо виконання рекомендацій, викладених в актах перевірок, та несуть персональну відповідальність за приведення стану ТЗІ у відповідність до вимог нормативно-правових актів системи ТЗІ.

7.5. Посадові особи Держспецзв'язку за порушення конституційних прав і свобод людини та громадянина у ході здійснення державного контролю за станом ТЗІ несуть відповідальність згідно із законодавством України.

8. Проведення державного інструментального контролю захищеності інформації, яка циркулює на об'єктах "особливої норми"

8.1. Державний інструментальний контроль захищеності інформації, яка циркулює на об'єктах "особливої норми", здійснюється з використанням інструментально-розрахункових методів з метою оцінки повноти та достатності впроваджених на об'єктах організаційних, організаційно-технічних та технічних заходів із захисту інформації від поширення (просочення) технічними каналами.

8.2. Державний інструментальний контроль захищеності інформації, яка циркулює на об'єктах "особливої норми", здійснюється шляхом проведення:

спеціальних обстежень об'єктів "особливої норми", у ході яких перевіряються повнота та достатність упроваджених організаційних, організаційно-технічних та технічних заходів із захисту інформації від поширення (просочення) технічними каналами, у тому числі каналами, що створюються за рахунок застосування закладних пристроїв, відповідність упроваджених заходів вимогам нормативно-правових актів, а також наявність атестаційних документів, які визначають необхідність упровадження заходів захисту інформації;

спеціальних перевірок об'єктів "особливої норми", у ході яких перевіряється наявність технічних каналів поширення інформації, які створюються за рахунок застосування закладних пристроїв;

спеціальних досліджень технічних засобів, призначених для встановлення на об'єктах "особливої норми", у ході яких перевіряється відповідність захищеності технічних засобів нормам ефективності захисту інформації від поширення (просочення) технічними каналами.

8.3. Спеціальні обстеження, спеціальні перевірки об'єктів "особливої норми" та спеціальні дослідження технічних засобів, призначених для

встановлення на об'єктах "особливої норми", можуть бути плановими та позаплановими.

8.4. Планові спеціальні обстеження, спеціальні перевірки об'єктів "особливої норми", спеціальні дослідження технічних засобів, призначених для встановлення на об'єктах "особливої норми", проводяться згідно з відповідним планом, який погоджується з Управлінням державної охорони України та затверджується Головою Держспецзв'язку.

8.5. Позапланові спеціальні обстеження, спеціальні перевірки об'єктів "особливої норми", спеціальні дослідження технічних засобів, призначених для встановлення на об'єктах "особливої норми", проводяться за запитами Управління державної охорони України або органів державної влади, у підпорядкуванні яких ці об'єкти перебувають.

8.6. За результатами спеціальних обстежень та спеціальних перевірок об'єктів "особливої норми" посадовими особами Держспецзв'язку, які їх здійснювали, складаються відповідні акти в довільній формі.

В актах спеціальних обстежень об'єктів зазначаються виявлені недоліки в організації технічного захисту інформації на об'єкті, наявні канали поширення (просочення) інформації, визначається відповідність стану технічного захисту інформації вимогам нормативно-правових актів з ТЗІ та надаються рекомендації щодо усунення виявлених недоліків.

В актах спеціальних перевірок зазначаються відомості про наявність технічних каналів поширення інформації, які створюються за рахунок застосування закладних пристроїв, недоліки організації ТЗІ, які створюють передумови до впровадження на об'єкті закладних пристроїв, та надаються рекомендації щодо упередження можливого впровадження на об'єкті закладних пристроїв.

8.7. За результатами спеціальних досліджень технічних засобів, призначених для встановлення на об'єктах "особливої норми", посадовими особами Держспецзв'язку, які їх здійснювали, оформлюються висновки.

У висновках спеціальних досліджень визначаються можливість, умови та порядок використання технічних засобів на об'єкті.

8.8. Акти спеціальних обстежень, акти спеціальних перевірок та висновки спеціальних досліджень оформлюються у двох примірниках. Один примірник залишається у Держспецзв'язку, а другий - згідно із запитом надсилається на адресу Управління державної охорони або державного органу, у підпорядкуванні якого перебуває об'єкт "особливої норми".

У разі отримання запиту на проведення спеціальних обстежень, спеціальних перевірок об'єктів "особливої норми", спеціальних досліджень технічних засобів, призначених для встановлення на об'єктах "особливої норми", від Управління державної охорони України надсилати акти спеціальних обстежень, акти спеціальних перевірок та висновки спеціальних досліджень на адресу третьої сторони, у тому числі на адресу державного органу, у підпорядкуванні якого перебуває об'єкт "особливої норми", забороняється.

При отриманні запиту на проведення спеціальних обстежень, спеціальних перевірок об'єктів "особливої норми", спеціальних досліджень технічних засобів,

призначених для встановлення на об'єктах "особливої норми", від державного органу, у підпорядкуванні якого перебуває об'єкт "особливої норми", акти спеціальних обстежень, акти спеціальних перевірок та висновки спеціальних досліджень за окремим запитом можуть бути надіслані на адресу Управління державної охорони України.

8.9. Протоколи вимірювань, які проводилися у ході спеціальних обстежень, спеціальних перевірок об'єктів "особливої норми", спеціальних досліджень технічних засобів, призначених для встановлення на об'єктах "особливої норми", оформлюються в єдиному примірнику та залишаються у підрозділі Держспецзв'язку, який їх здійснював. Ознайомлення з протоколами вимірювань інших сторін забороняється.

Начальник Департаменту державного контролю за станом криптографічного та технічного захисту інформації Адміністрації Держспецзв'язку В.Є. Прасолов

Додаток 1 до пункту 2.9 Положення про державний контроль за станом технічного захисту інформації

ПРИПИС на право проведення перевірки

Посадовим особам Державної служби спеціального зв'язку та захисту інформації України _____

(прізвища, ім'я та по батькові)

_____

приписується провести _____ перевірку стану

(комплексну, контрольну, цільову)

технічного захисту інформації, яка є власністю держави, та інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, у

_____

(найменування державного органу, військового формування,

_____

установи, підприємства, організації, що перевіряється)

Посадові особи _____

(прізвища, ім'я та по батькові)

_____

мають допуск до державної таємниці за формою _____

Припис дійсний до "___" _____ 20__ року.

М.П.

_____

(посадова особа Держспецзв'язку, прізвище, ініціали, підпис)

Начальник Департаменту державного контролю за станом криптографічного та технічного захисту інформації Адміністрації Держспецзв'язку В.Є. Прасолов

Додаток 2 до пункту 4.4 Положення про державний контроль за станом технічного захисту інформації

ЗАТВЕРДЖУЮ

_____

_____

"___"_____ 20__ р.

АКТ комплексної перевірки стану технічного захисту інформації у _____

(найменування державного органу, військового формування, установи, підприємства, організації, що перевіряється)

"____" _____ 20__ р. м._____

Посадовими особами Державної служби спеціального зв'язку та захисту інформації України у складі _____

(прізвища, ім'я та по батькові)

_____

на підставі припису від "___" _____20__ р. N_____ проведено комплексну перевірку стану технічного захисту інформації

у _____

(найменування державного органу, військового формування,

_____

установи, підприємства або організації, що перевіряється, їх підпорядкованість)

Перевіркою встановлено:

1. Загальні питання

_____

_____

2. Заходи з технічного захисту мовної інформації

_____

_____

3. Заходи з технічного захисту інформації, яка обробляється в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, засобах розмноження документів та інших технічних засобах, які використовуються для обробки інформації

_____

_____

4. Заходи з технічного захисту інформації з обмеженим доступом при створенні продукції та технологій для державних потреб і виконанні НДДКР

_____

_____

5. Заходи з технічного захисту інформації з обмеженим доступом під час організації проектування будівництва, реконструкції та капітального ремонту ОІД

_____

_____

6. Заходи з технічного захисту інформації з обмеженим доступом під час прийому іноземних делегацій, іноземців, осіб без громадянства та здійснення діяльності іноземних інспекційних місій на території України

_____

_____

Висновок _____

_____

_____

Рекомендації

1. _____

2. _____

3. _____

Перевірку здійснили:

_____

(підпис, прізвище, ініціали)

_____

(підпис, прізвище, ініціали)

З актом ознайомлений: керівник або вповноважений представник державного органу, військового формування, установи, підприємства, організації, що перевірялася, _____

(підпис, прізвище, ініціали)

Начальник Департаменту державного контролю за станом криптографічного та технічного захисту інформації Адміністрації Держспецзв'язку В.Є. Прасолов