Міністерство освіти і науки, молоді та спорту України
Державний вищий навчальний заклад
"Національний гірничий університет"
Юридичний факультет

ІНФОРМАЦІЙНЕ ЗАКОНОДАВСТВО

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

ЧАСТИНА 4

Тексти нормативних актів подані
за станом на 1 серпня 2012 р.

Дніпропетровськ
НГУ
2012

MCMXCVIII

УДК 349.004 (075)

Інформаційне законодавство. Правове забезпечення захисту інформації / Уклад.: Р.С. Кірін, С.В. Грищак, Д.О. Шашенко. – Д.: Національний гірничий університет, 2012. Частина 4. – 171 с.

Укладачі:
Р.С. Кірін, доц.
С.В. Грищак, проф.
Д.О. Шашенко, доц.

Наведено основні нормативні акти в сфері захисту інформації, зокрема, щодо захисту інформації в інформаційно-телекомунікаційних системах, Державної служби спеціального зв'язку та захисту інформації України тощо.

Розраховано на студентів, які здобувають вищу освіту в галузях знань "Право", "Інформаційна безпека", "Комп'ютерні науки", "Телекомунікації".

Відповідальний за випуск зав. кафеедри цивільного та господарського права, канд. юрид. наук, доцент Кірін Р.С.

ЗМІСТ

ЗАКОН УКРАЇНИ

Про захист інформації в інформаційно-телекомунікаційних системах

Закон введено в дію з дня опублікування - 2 серпня 1994 року
(згідно з Постановою Верховної Ради України
від 5 липня 1994 року N 81/94-ВР)

Із змінами і доповненнями, внесеними
Законами України
від 11 травня 2004 року N 1703-IV,
від 31 травня 2005 року N 2594-IV
(Законом України від 31 травня 2005 року N 2594-IV
цей Закон викладено у новій редакції),
від 15 січня 2009 року N 879-VI,
від 19 березня 2009 року N 1180-VI

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;

виток інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

власник інформації - фізична або юридична особа, якій належить право власності на інформацію;

власник системи - фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-телекомунікаційна система - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі (далі - користувач) - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

телекомунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Стаття 2. Об'єкти захисту в системі

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Стаття 3. Суб'єкти відносин

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є:

власники інформації;

власники системи;

користувачі;

спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи.

(абзац п'ятий частини першої статті 3 у редакції
Закону України від 15.01.2009 р. N 879-VI)

На підставі укладеного договору або за дорученням власник інформації може надати право розпоряджатися інформацією іншій фізичній або юридичній особі - розпоряднику інформації.

На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі - розпоряднику системи.

Стаття 4. Доступ до інформації в системі

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації.

Порядок доступу до інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством.

У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її власника в порядку, встановленому законом.

Стаття 5. Відносини між власником інформації та власником системи

Власник системи забезпечує захист інформації в системі в порядку та на умовах, визначених у договорі, який укладається ним із власником інформації, якщо інше не передбачено законом.

Власник системи на вимогу власника інформації надає відомості щодо захисту інформації в системі.

Стаття 6. Відносини між власником системи та користувачем

Власник системи надає користувачеві відомості про правила і режим роботи системи та забезпечує йому доступ до інформації в системі відповідно до визначеного порядку доступу.

Стаття 7. Відносини між власниками систем

Власник системи, яка використовується для обробки інформації з іншої системи, забезпечує захист такої інформації в порядку та на умовах, що визначаються договором, який укладається між власниками систем, якщо інше не встановлено законодавством.

Власник системи, яка використовується для обробки інформації з іншої системи, повідомляє власника зазначеної системи про виявлені факти несанкціонованих дій щодо інформації в системі.

Стаття 8. Умови обробки інформації в системі

Умови обробки інформації в системі визначаються власником системи відповідно до договору з власником інформації, якщо інше не передбачено законодавством.

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством.

Для створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Стаття 9. Забезпечення захисту інформації в системі

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Власник системи, в якій обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган.

(частина третя статті 9 із змінами, внесеними
згідно із Законом України від 15.01.2009 р. N 879-VI)

Стаття 10. Повноваження державних органів у сфері захисту інформації в системах

Вимоги до забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Частину другу статті 10 виключено

(згідно із Законом України
від 15.01.2009 р. N 879-VI)

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

(абзац перший частини третьої статті 10 у редакції
Закону України від 15.01.2009 р. N 879-VI)

розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

визначає вимоги та порядок створення комплексної системи захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

здійснює контроль за забезпеченням захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

(частину третю статті 10 доповнено абзацом
згідно із Законом України від 19.03.2009 р. N 1180-VI)

Державні органи в межах своїх повноважень за погодженням відповідно із спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом встановлюють особливості захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

(частина четверта статті 10 із змінами, внесеними
згідно із Законом України від 15.01.2009 р. N 879-VI)

Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Стаття 11. Відповідальність за порушення законодавства про захист інформації в системах

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Стаття 12. Міжнародні договори

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, визначено інші правила, ніж ті, що передбачені цим Законом, застосовуються норми міжнародного договору.

Стаття 13. Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2006 року.

2. Нормативно-правові акти до приведення їх у відповідність із цим Законом діють у частині, що не суперечить цьому Закону.

3. Кабінету Міністрів України та Національному банку України в межах своїх повноважень протягом шести місяців з дня набрання чинності цим Законом:

привести свої нормативно-правові акти у відповідність із цим Законом;

забезпечити приведення міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

Президент України **Л. КУЧМА**

м. Київ
5 липня 1994 року
N 80/94-ВР

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 29 березня 2006 р. N 373

Київ

Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах

Із змінами і доповненнями, внесеними
постановами Кабінету Міністрів України
від 8 грудня 2006 року N 1700,
від 7 вересня 2011 року N 938

Відповідно до статті 10 Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" Кабінет Міністрів України **постановляє**:

Затвердити Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, що додаються.

Прем'єр-міністр України **Ю. ЄХАНУРОВ**

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 29 березня 2006 р. N 373

ПРАВИЛА
забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах

Загальна частина

1. Ці Правила визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

(пункт 1 із змінами, внесеними згідно з постановою
Кабінету Міністрів України від 07.09.2011 р. N 938)

2. Дія цих Правил не поширюється на захист інформації в системах урядового та спеціальних видів зв'язку.

3. У Правилах наведені нижче терміни вживаються у такому значенні:

автентифікація - процедура встановлення належності користувачеві інформації в системі (далі - користувач) пред'явленого ним ідентифікатора;

ідентифікація - процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Інші терміни вживаються у значенні, наведеному в Законах України "Про інформацію", "Про доступ до публічної інформації", "Про державну таємницю", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про телекомунікації", Положенні про технічний захист інформації в Україні, затвердженому Указом Президента України від 27 вересня 1999 р. N 1229.

(абзац четвертий пункту 3 із змінами, внесеними згідно з постановою Кабінету Міністрів України від 07.09.2011 р. N 938)

4. Захисту в системі підлягає:

відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

конфіденційна інформація, яка перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України "Про доступ до публічної інформації" (далі - конфіденційна інформація);

службова інформація;

інформація, яка становить державну або іншу передбачену законом таємницю (далі - таємна інформація);

інформація, вимога щодо захисту якої встановлена законом.

(пункт 4 у редакції постанови Кабінету Міністрів України від 07.09.2011 р. N 938)

Вимоги до забезпечення захисту інформації в системі

5. Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

6. Під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

(пункт 6 із змінами, внесеними згідно з постановою
Кабінету Міністрів України від 07.09.2011 р. N 938)

7. Доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

(абзац перший пункту 7 із змінами, внесеними згідно з
постановою Кабінету Міністрів України від 07.09.2011 р. N 938)

У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки службової інформації або позбавлення його такого права.

(абзац другий пункту 7 із змінами, внесеними згідно з
постановою Кабінету Міністрів України від 07.09.2011 р. N 938)

8. Вимоги до захисту в системі інформації, що становить державну таємницю, визначаються цими Правилами та законодавством у сфері охорони державної таємниці.

9. Забезпечення захисту в системі таємної інформації, яка не становить державну таємницю, та конфіденційної інформації здійснюється згідно з вимогами до захисту службової інформації, якщо інше не передбачено законом.

(пункт 9 у редакції постанови Кабінету
Міністрів України від 07.09.2011 р. N 938)

10. Вимоги до захисту в системі інформації від несанкціонованого блокування визначаються розпорядником інформації, якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством.

(пункт 10 із змінами, внесеними згідно з постановою
Кабінету Міністрів України від 07.09.2011 р. N 938)

11. У системі здійснюється обов'язкова реєстрація:

результатів ідентифікації та автентифікації користувачів;

результатів виконання користувачем операцій з обробки інформації;

спроб несанкціонованих дій з інформацією;

фактів надання та позбавлення користувачів права доступу до інформації та її обробки;

результатів перевірки цілісності засобів захисту інформації.

Забезпечується можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління засобами захисту інформації і контроль за захистом інформації в системі (адміністратор безпеки).

Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки.

Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, а також конфіденційної інформації про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки.

12. Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.

13. Передача службової і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

(пункт 13 із змінами, внесеними згідно з постановою
Кабінету Міністрів України від 07.09.2011 р. N 938)

14. Порядок підключення систем, в яких обробляється службова і таємна інформація, до глобальних мереж передачі даних визначається законодавством.

(пункт 14 із змінами, внесеними згідно з постановою
Кабінету Міністрів України від 07.09.2011 р. N 938)

15. У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації.

Контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

Організаційні засади забезпечення захисту інформації

16. Для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі - система захисту), яка призначається для захисту інформації від:

витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

несанкціонованих дій з інформацією, у тому числі з використанням комп'ютерних вірусів;

спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Захист інформації від витоку технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником інформації.

(абзац п'ятий пункту 16 із змінами, внесеними згідно з
постановою Кабінету Міністрів України від 07.09.2011 р. N 938)

Захист інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, забезпечується в усіх системах.

Захист інформації від спеціального впливу на засоби обробки інформації забезпечується в системі, якщо рішення про необхідність такого захисту прийнято розпорядником інформації.

(абзац сьомий пункту 16 із змінами, внесеними згідно з
постановою Кабінету Міністрів України від 07.09.2011 р. N 938)

17. Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи.

18. Організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

Служба захисту інформації утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи.

У разі коли обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою.

19. Захист інформації на всіх етапах створення та експлуатації системи здійснюється відповідно до розробленого службою захисту інформації плану захисту інформації в системі.

План захисту інформації в системі містить:

завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;

визначення моделі загроз для інформації в системі;

основні вимоги щодо захисту інформації та правила доступу до неї в системі;

перелік документів, згідно з якими здійснюється захист інформації в системі;

перелік і строки виконання робіт службою захисту інформації.

20. Вимоги та порядок створення системи захисту встановлюються Адміністрацією Держспецзв'язку (далі - Адміністрація).

(абзац перший пункту 20 із змінами, внесеними згідно з постановою Кабінету Міністрів України від 08.12.2006 р. N 1700)

Вимоги до захисту інформації кожної окремої системи встановлюються технічним завданням на створення системи або системи захисту.

21. У складі системи захисту повинні використовуватися засоби захисту інформації з підтвердженою відповідністю.

У разі використання засобів захисту інформації, які не мають підтвердження відповідності на момент проектування системи захисту, відповідне оцінювання проводиться під час державної експертизи системи захисту.

22. Порядок проведення державної експертизи системи захисту, державної експертизи та сертифікації засобів технічного і криптографічного захисту інформації встановлюється Адміністрацією.

Органи виконавчої влади, які мають дозвіл на провадження діяльності з технічного захисту інформації для власних потреб, вправі за згодою Адміністрації організовувати проведення державної експертизи системи захисту на підприємствах, в установах та організаціях, які належать до сфери їх управління. Порядок проведення такої експертизи встановлюється органом виконавчої влади за погодженням з Адміністрацією.

(пункт 22 із змінами, внесеними згідно з постановою Кабінету Міністрів України від 08.12.2006 р. N 1700)

23. Виконавцем робіт із створення системи захисту може бути суб'єкт господарської діяльності або орган виконавчої влади, який має ліцензію або дозвіл на право провадження хоча б одного виду робіт у сфері технічного захисту інформації, необхідність проведення якого визначено технічним завданням на створення системи захисту.

Для проведення інших видів робіт з технічного захисту інформації, на провадження яких виконавець не має ліцензії (дозволу), залучаються співвиконавці, що мають відповідні ліцензії.

Якщо для створення системи захисту необхідно провести роботи з криптографічного захисту інформації, виконавець повинен мати ліцензії на провадження виду робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії.

24. Контроль за забезпеченням захисту інформації в системі полягає у перевірці виконання вимог з технічного та криптографічного захисту інформації та здійснюється у порядку, визначеному Адміністрацією.

(пункт 24 із змінами, внесеними згідно з постановою Кабінету Міністрів України від 08.12.2006 р. N 1700)

25. У системі, яка складається з кількох інформаційних та (або) телекомунікаційних систем, ці Правила можуть застосовуватися до кожної складової частини окремо.

ЗАКОН УКРАЇНИ

Про Державну службу спеціального зв'язку та захисту інформації України

Із змінами і доповненнями, внесеними
Законами України
від 3 листопада 2006 року N 328-V,
від 11 травня 2007 року N 1014-V,
від 28 грудня 2007 року N 107-VI
(зміни, внесені Законом України від 28 грудня 2007 року N 107-VI,
діють по 31 грудня 2008 року,
зміни, внесені пунктом 72 розділу II Закону України
від 28 грудня 2007 року N 107-VI,
визнано такими, що не відповідають Конституції України (є неконституційними),
згідно з Рішенням Конституційного Суду України
від 22 травня 2008 року N 10-рп/2008),
від 15 січня 2009 року N 879-VI,
від 19 березня 2009 року N 1180-VI,
від 2 червня 2009 року N 1415-VI,
від 1 червня 2010 року N 2289-VI
(зміни, внесені Законом України від 1 червня 2010 року N 2289-VI,
вводяться в дію з 31 липня 2010 року),
від 7 жовтня 2010 року N 2592-VI,
від 7 липня 2011 року N 3610-VI,
від 17 травня 2012 року N 4711-VI

(У тексті Закону слова "інформаційно-телекомунікаційна система" в усіх відмінках і числах замінено словами "інформаційна, телекомунікаційна та інформаційно-телекомунікаційна система" у відповідному відмінку і числі згідно із Законом України від 19 березня 2009 року N 1180-VI)

Цей Закон відповідно до Конституції України визначає правові основи організації та діяльності Державної служби спеціального зв'язку та захисту інформації України.

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

1. У цьому Законі наведені нижче терміни вживаються в такому значенні:

спеціальний зв'язок - передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень, які містять інформацію з обмеженим доступом, по радіо, проводових, оптичних або інших електромагнітних системах з використанням засобів криптографічного та/або технічного захисту інформації з додержанням вимог законодавства щодо її захисту;

урядовий зв'язок - вид спеціального зв'язку, надання якого забезпечується державною системою урядового зв'язку;

державна система урядового зв'язку - система спеціального зв'язку, яка призначена для забезпечення управління державою в мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайних ситуацій та забезпечує додержання вимог законодавства з питань захисту інформації, яка містить державну таємницю;

об'єкт інформаційної діяльності - інженерно-технічна споруда (приміщення), де здійснюється діяльність, пов'язана з інформацією, що підлягає захисту;

державні інформаційні ресурси - інформація, яка є власністю держави та необхідність захисту якої визначено законодавством.

2. Терміни "Національна система конфіденційного зв'язку", "інформаційна (автоматизована) система", "телекомунікаційна система", "інформаційна, телекомунікаційна та інформаційно-телекомунікаційна система", "криптографічний захист інформації", "технічний захист інформації", "комплексна система захисту інформації", "інформація з обмеженим доступом" вживаються в цьому Законі у значеннях, визначених відповідно в законах України "Про Національну систему конфіденційного зв'язку", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про інформацію".

(частина друга статті 1 із змінами, внесеними
згідно із Законом України від 19.03.2009 р. N 1180-VI)

Стаття 2. Статус Державної служби спеціального зв'язку та захисту інформації України

1. Державна служба спеціального зв'язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації.

2. Частину другу статті 2 виключено

(згідно із Законом України
від 07.10.2010 р. N 2592-VI)

3. Державна служба спеціального зв'язку та захисту інформації України підпорядковується і підконтрольна Президенту України.

(частина третя статті 2 у редакції
Закону України від 07.10.2010 р. N 2592-VI)

4. Кабінет Міністрів України здійснює заходи щодо забезпечення функціонування Державної служби спеціального зв'язку та захисту інформації України.

(статтю 2 доповнено частиною четвертою згідно із Законом України від 07.10.2010 р. N 2592-VI)

Стаття 3. Основні завдання Державної служби спеціального зв'язку та захисту інформації України

1. Основними завданнями Державної служби спеціального зв'язку та захисту інформації України є:

участь у формуванні та реалізація державної політики у сфері захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації;

забезпечення в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб органів державної влади, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації;

забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;

визначення вимог і порядку створення та розвитку систем технічного та криптографічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису;

охорона об'єктів, приміщень, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України.

Стаття 4. Основні принципи діяльності Державної служби спеціального зв'язку та захисту інформації України

1. Основними принципами діяльності Державної служби спеціального зв'язку та захисту інформації України є:

законність;

повага та додержання прав і свобод людини та громадянина;

єдиноначальність та централізація управління;

узгодження дій в особливий період (в умовах надзвичайного та воєнного стану, у разі виникнення надзвичайної ситуації) з Генеральним штабом Збройних Сил України, Службою безпеки України, центральним органом виконавчої влади з питань цивільного захисту;

відкритість для демократичного цивільного контролю з додержанням вимог законодавства про охорону державної таємниці.

Розділ II
ЗАГАЛЬНА СТРУКТУРА, ЧИСЕЛЬНІСТЬ ТА ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Стаття 5. Загальна структура і чисельність Державної служби спеціального зв'язку та захисту інформації України

1. Загальну структуру Державної служби спеціального зв'язку та захисту інформації України складають спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації і підпорядковані йому регіональні органи та територіальні підрозділи.

2. У Державній службі спеціального зв'язку та захисту інформації України утворюються навчальні, медичні, санаторно-курортні та інші заклади, науково-дослідні та науково-виробничі установи. До сфери управління Державної служби захисту інформації входять державні підприємства, діяльність яких пов'язана із забезпеченням виконання покладених на неї завдань.

3. Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації, регіональні органи, територіальні підрозділи, навчальні, медичні, санаторно-курортні та інші заклади, науково-дослідні та науково-виробничі установи, державні підприємства, зазначені у частині другій цієї статті, є юридичними особами, мають печатку із зображенням Державного Герба України та своїм найменуванням, інші печатки і штампи, рахунки відповідно в органах Державного казначейства України та в установах банків, у тому числі в іноземній валюті.

4. Загальна чисельність особового складу Державної служби спеціального зв'язку та захисту інформації України затверджується Кабінетом Міністрів України за поданням спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

(частина четверта статті 5 із змінами, внесеними
згідно із Законом України від 19.03.2009 р. N 1180-VI)

Стаття 6. Голова Державної служби спеціального зв'язку та захисту інформації України

1. Керівництво Державною службою спеціального зв'язку та захисту інформації України здійснює голова Державної служби спеціального зв'язку та захисту інформації України, який очолює спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації та несе особисту відповідальність за виконання покладених на Державну службу спеціального зв'язку та захисту інформації України завдань.

2. Голову Державної служби спеціального зв'язку та захисту інформації України призначає на посаду за поданням Прем'єр-міністра України та звільняє з посади Президент України.

(частина друга статті 6 у редакції
Закону України від 07.10.2010 р. N 2592-VI)

3. Заступників голови Державної служби спеціального зв'язку та захисту інформації України призначає на посади за поданням Прем'єр-міністра України та звільняє з посад Президент України.

(частина третя статті 6 у редакції
Закону України від 07.10.2010 р. N 2592-VI)

4. Частину четверту статті 6 виключено

(згідно із Законом України
від 07.10.2010 р. N 2592-VI)

Стаття 7. Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації

1. Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

організовує, координує та контролює діяльність регіональних органів, територіальних підрозділів, закладів, установ, державних підприємств Державної служби спеціального зв'язку та захисту інформації України;

бере участь у формуванні і відповідає за реалізацію державної політики у сфері захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації, забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку;

здійснює координацію діяльності органів державної влади, органів місцевого самоврядування, утворених відповідно до законів України військових формувань (далі - військові формування), підприємств, установ і організацій незалежно від форм власності з питань, що належать до повноважень Державної служби спеціального зв'язку та захисту інформації України;

здійснює державний контроль за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису;

здійснює відповідно до законодавства функції з управління об'єктами державної власності, у тому числі державними корпоративними правами, утворює і припиняє державні підприємства, установи, діяльність яких пов'язана із забезпеченням виконання покладених на Державну службу спеціального зв'язку та захисту інформації України завдань;

узагальнює практику застосування законодавства з питань, що належать до повноважень Державної служби спеціального зв'язку та захисту інформації України, розробляє пропозиції щодо його вдосконалення і в установленому порядку вносить їх на розгляд Президенту України та Кабінету Міністрів України.

2. Положення про спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації затверджується Президентом України. Організаційна структура спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації, гранична чисельність його особового складу затверджуються Кабінетом Міністрів України.

(частина друга статті 7 у редакції
Закону України від 07.10.2010 р. N 2592-VI)

Стаття 8. Колегія Державної служби спеціального зв'язку та захисту інформації України

1. У Державній службі спеціального зв'язку та захисту інформації України для колективного обговорення найважливіших напрямів її діяльності та погодженого вирішення питань, що належать до її повноважень, утворюється колегія.

2. Положення про колегію Державної служби спеціального зв'язку та захисту інформації України і її персональний склад затверджує голова Державної служби спеціального зв'язку та захисту інформації України.

Стаття 9. Регіональні органи та територіальні підрозділи Державної служби спеціального зв'язку та захисту інформації України

1. З метою виконання покладених на Державну службу спеціального зв'язку та захисту інформації України завдань рішенням спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації утворюються регіональні органи в Автономній Республіці Крим, областях, містах Києві та Севастополі, а також утворюються територіальні підрозділи для забезпечення урядовим зв'язком Президента України, Голови Верховної Ради України та Прем'єр-міністра України.

2. Положення про регіональні органи та територіальні підрозділи Державної служби спеціального зв'язку та захисту інформації України затверджує голова Державної служби спеціального зв'язку та захисту інформації України.

3. Начальники регіональних органів та територіальних підрозділів Державної служби спеціального зв'язку та захисту інформації України призначаються на посади та звільняються з посад головою Державної служби спеціального зв'язку та захисту інформації України.

4. Гранична чисельність особового складу регіональних органів та територіальних підрозділів Державної служби спеціального зв'язку та захисту інформації України затверджується Кабінетом Міністрів України.

Розділ III
ОСОБОВИЙ СКЛАД ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Стаття 10. Особовий склад Державної служби спеціального зв'язку та захисту інформації України

1. До особового складу Державної служби спеціального зв'язку та захисту інформації України належать особи рядового і начальницького складу, які проходять службу за контрактом, державні службовці та інші працівники, з якими укладається трудовий договір.

2. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України встановлюються такі спеціальні звання:

рядовий Державної служби спеціального зв'язку та захисту інформації України;

сержант Державної служби спеціального зв'язку та захисту інформації України;

прапорщик Державної служби спеціального зв'язку та захисту інформації України;

старший прапорщик Державної служби спеціального зв'язку та захисту інформації України;

молодший лейтенант Державної служби спеціального зв'язку та захисту інформації України;

лейтенант Державної служби спеціального зв'язку та захисту інформації України;

старший лейтенант Державної служби спеціального зв'язку та захисту інформації України;

капітан Державної служби спеціального зв'язку та захисту інформації України;

майор Державної служби спеціального зв'язку та захисту інформації України;

підполковник Державної служби спеціального зв'язку та захисту інформації України;

полковник Державної служби спеціального зв'язку та захисту інформації України;

генерал-майор Державної служби спеціального зв'язку та захисту інформації України;

генерал-лейтенант Державної служби спеціального зв'язку та захисту інформації України.

3. До спеціальних звань осіб середнього і старшого начальницького складу Державної служби спеціального зв'язку та захисту інформації України, які мають вищу медичну або юридичну освіту та займають відповідну штатну посаду, після слів "молодший лейтенант", "лейтенант", "старший лейтенант", "капітан", "майор", "підполковник", "полковник" додаються відповідно слова "медичної служби" або "юстиції".

(статтю 10 доповнено новою частиною третьою
згідно із Законом України від 15.01.2009 р. N 879-VI,
у зв'язку з цим частини третю - десяту вважати
відповідно частинами четвертою - одинадцятою)

4. На службу до Державної служби спеціального зв'язку та захисту інформації України приймаються відповідно на конкурсній та контрактній основі громадяни України, які досягли 18-річного віку та спроможні за своїми особистими, діловими і моральними якостями, освітнім і професійним рівнем, станом здоров'я виконувати відповідні службові обов'язки.

Стосовно осіб, які претендують на службу в Державній службі спеціального зв'язку та захисту інформації України, за їх письмовою згодою проводиться спеціальна перевірка в порядку, встановленому Законом України "Про засади запобігання і протидії корупції".

(частину четверту статті 10 доповнено абзацом
другим згідно із Законом України від 17.05.2012 р. N 4711-VI)

Особи, які претендують на службу в Державній службі спеціального зв'язку та захисту інформації України, до призначення на відповідну посаду подають за місцем майбутньої служби декларацію про майно, доходи, витрати і зобов'язання фінансового характеру за формою і в порядку, що встановлені Законом України "Про засади запобігання і протидії корупції", та зобов'язані повідомити керівництву органу, на зайняття посади в якому вони претендують, про працюючих у цьому органі близьких їм осіб.

(частину четверту статті 10 доповнено абзацом
третім згідно із Законом України від 17.05.2012 р. N 4711-VI)

На службу в Державну службу спеціального зв'язку та захисту інформації України не може бути прийнята особа, яка має не погашену або не зняту судимість за вчинення злочину, крім реабілітованої, або на яку протягом останнього року накладалося адміністративне стягнення за вчинення корупційного правопорушення.

(частину четверту статті 10 доповнено абзацом
четвертим згідно із Законом України від 17.05.2012 р. N 4711-VI)

5. Критерії професійної придатності, фахової підготовленості, інші вимоги до осіб рядового і начальницького складу, державних службовців та інших працівників Державної служби спеціального зв'язку та захисту інформації України визначаються спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

6. Порядок проходження служби в Державній службі спеціального зв'язку та захисту інформації України осіб рядового і начальницького складу, присвоєння і позбавлення спеціальних звань, а також пониження і поновлення у спеціальних званнях визначається цим Законом та Положенням про проходження служби в Державній службі спеціального зв'язку та захисту інформації України особами рядового і начальницького складу, яке затверджується Кабінетом Міністрів України.

Особи рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України зобов'язані подавати щороку до 1 квітня за місцем служби декларацію про майно, доходи, витрати і зобов'язання фінансового характеру за минулий рік за формою і в порядку, що встановлені Законом України "Про засади запобігання і протидії корупції".

(частину шосту статті 10 доповнено абзацом другим
згідно із Законом України від 17.05.2012 р. N 4711-VI)

7. У Державній службі спеціального зв'язку та захисту інформації України діє Дисциплінарний статут, який затверджується законом.

8. Громадяни України, які вперше приймаються на службу до Державної служби спеціального зв'язку та захисту інформації України на посади осіб рядового і начальницького складу, складають Присягу такого змісту:

"Я (прізвище, ім'я, по батькові), вступаючи на службу до Державної служби спеціального зв'язку та захисту інформації України, присягаю завжди залишатися відданим Українському народові, неухильно додержуватися Конституції та законів України, бути чесним, сумлінним і дисциплінованим, зберігати державну таємницю. Присягаю з високою відповідальністю виконувати свій службовий обов'язок, постійно вдосконалювати професійну майстерність, не допускати порушень прав і свобод людини та громадянина. Якщо я порушу цю Присягу, то готовий нести відповідальність згідно із законом".

9. Час проходження служби в Державній службі спеціального зв'язку та захисту інформації України зараховується до стажу роботи, стажу роботи за спеціальністю, а також до стажу державної служби і прирівнюється до страхового стажу.

(частина дев'ята статті 10 із змінами, внесеними
згідно із Законом України від 19.03.2009 р. N 1180-VI)

10. Окремі посади осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України можуть заміщатися державними службовцями та іншими працівниками Державної служби спеціального зв'язку та захисту інформації України у порядку, визначеному головою Державної служби спеціального зв'язку та захисту інформації України.

11. Особи начальницького складу Державної служби спеціального зв'язку та захисту інформації України можуть бути відряджені до державних органів, установ і організацій для виконання завдань, визначених цим Законом, із залишенням на службі в Державній службі спеціального зв'язку та захисту інформації України. Перелік посад, які можуть бути заміщені особами начальницького складу в цих державних органах, установах і організаціях, затверджується Кабінетом Міністрів України.

(статтю 10 доповнено новою частиною одинадцятою
згідно із Законом України від 15.01.2009 р. N 879-VI,
у зв'язку з цим частину одинадцяту вважати частиною дванадцятою)

12. Трудові відносини державних службовців та інших працівників Державної служби спеціального зв'язку та захисту інформації України регулюються законодавством про працю і державну службу.

Стаття 10^1. Врегулювання конфлікту інтересів

1. У разі виникнення конфлікту інтересів під час виконання службових повноважень особа рядового або начальницького складу Державної служби спеціального зв'язку та захисту інформації України зобов'язана негайно доповісти про це своєму безпосередньому начальникові.

Безпосередній начальник особи рядового або начальницького складу Державної служби спеціального зв'язку та захисту інформації України зобов'язаний вжити всіх необхідних

заходів, спрямованих на запобігання конфлікту інтересів, шляхом доручення виконання відповідного службового завдання іншій посадовій особі, особистого виконання службового завдання чи в інший спосіб, передбачений законодавством.

Примітка. Термін "конфлікт інтересів" вживається у значенні, наведеному в Законі України "Про засади запобігання і протидії корупції".

(Закон доповнено статтею 101 згідно із
Законом України від 17.05.2012 р. N 4711-VI)

Стаття 10^2. Обмеження щодо роботи близьких осіб

1. Особи рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України не можуть мати в безпосередньому підпорядкуванні або бути безпосередньо підпорядкованими у зв'язку з виконанням повноважень близьким їм особам.

2. У разі виникнення обставин, що порушують вимоги частини першої цієї статті, відповідні особи, близькі їм особи вживають заходів щодо усунення таких обставин у п'ятнадцятиденний строк. Якщо у зазначений строк ці обставини добровільно ними не усунуто, відповідні особи або близькі їм особи в місячний строк з дня виникнення обставин підлягають переведенню в установленому порядку на іншу посаду, що виключає безпосереднє підпорядкування.

3. У разі неможливості такого переведення особа, яка перебуває в підпорядкуванні, підлягає звільненню із служби.

4. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України забороняється брати участь у роботі колегіальних органів під час розгляду питань щодо призначення на посаду близьких їм осіб та в будь-який інший спосіб впливати на прийняття такого рішення.

Примітка. Терміни "безпосереднє підпорядкування" і "близька особа" вживаються у значеннях, наведених у Законі України "Про засади запобігання і протидії корупції".

(Закон доповнено статтею 10^2 згідно із
Законом України від 17.05.2012 р. N 4711-VI)

Стаття 11. Граничний вік перебування на службі у Державній службі спеціального зв'язку та захисту інформації України

1. Граничний вік перебування на службі у Державній службі спеціального зв'язку та захисту інформації України встановлюється:

для осіб рядового і начальницького складу, яким присвоєні спеціальні звання від рядового до капітана Державної служби спеціального зв'язку та захисту інформації України, - до 50 років;

для осіб начальницького складу, яким присвоєні спеціальні звання від майора до полковника Державної служби спеціального зв'язку та захисту інформації України, - до 55 років;

для осіб начальницького складу, яким присвоєні спеціальні звання генерал-майор, генерал-лейтенант Державної служби спеціального зв'язку та захисту інформації України, - до 60 років.

2. У разі необхідності особи рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України, які мають високу професійну підготовку, досвід практичної роботи на займаній посаді, визнані придатними за станом здоров'я для проходження служби, можуть бути залишені на їх прохання на службі понад граничний вік до п'яти років.

Стаття 12. Звільнення із служби в Державній службі спеціального зв'язку та захисту інформації України

1. Звільнення із служби осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України проводиться:

1) у запас Збройних Сил України, якщо звільнені особи не досягли граничного віку перебування у запасі, встановленого законом, і за станом здоров'я придатні до військової служби;

(пункт 1 частини першої статті 12 із змінами, внесеними згідно із Законом України від 19.03.2009 р. N 1180-VI)

2) у відставку, якщо звільнені особи досягли граничного віку перебування у запасі, встановленого законом, або визнані військово-лікарськими комісіями непридатними за станом здоров'я до військової служби з виключенням з військового обліку.

2. Контракт припиняється (розривається), а особи рядового і начальницького складу, які проходять службу за контрактом, звільняються із служби:

1) після закінчення строку контракту;

2) за віком - у разі досягнення граничного віку перебування на службі;

3) за станом здоров'я - на підставі висновку (постанови) військово-лікарської комісії про непридатність або обмежену придатність до служби;

4) у зв'язку із скороченням штатів - у разі неможливості використання на службі у зв'язку із скороченням штатів або проведенням організаційних заходів;

5) через сімейні обставини або з інших поважних причин, перелік яких визначається Кабінетом Міністрів України;

6) у зв'язку із систематичним невиконанням умов контракту особою рядового і начальницького складу;

7) у зв'язку із систематичним невиконанням умов контракту керівництвом Державної служби спеціального зв'язку та захисту інформації України;

8) за службовою невідповідністю;

9) у зв'язку з набранням законної сили обвинувальним вироком суду;

10) набрання законної сили судовим рішенням, відповідно до якого особу рядового чи начальницького складу притягнуто до відповідальності за корупційне правопорушення;

(частину другу статті 12 доповнено пунктом 10
згідно із Законом України від 17.05.2012 р. N 4711-VI)

11) у разі неможливості переведення на іншу посаду у зв'язку з безпосереднім підпорядкуванням близькій особі.

(частину другу статті 12 доповнено пунктом 11
згідно із Законом України від 17.05.2012 р. N 4711-VI)

У випадку, передбаченому пунктом 10 цієї частини, особи рядового і начальницького складу підлягають звільненню із служби у триденний строк з дня отримання відповідним органом або підрозділом Державної служби спеціального зв'язку та захисту інформації України копії відповідного судового рішення, яке набрало законної сили.

(частину другу статті 12 доповнено абзацом згідно із
Законом України від 17.05.2012 р. N 4711-VI)

3. Курсанти, які звільняються зі служби з підстав, визначених пунктами 6, 8 і 9 частини другої цієї статті, а також особи начальницького складу, які звільняються зі служби із зазначених підстав протягом п'яти років після закінчення вищого навчального закладу, у тому числі вищого військового навчального закладу чи військового навчального підрозділу вищого навчального закладу, в якому вони навчалися за державним замовленням і після закінчення якого були прийняті на службу осіб начальницького складу Державної служби спеціального зв'язку та захисту інформації України, відшкодовують Державній службі спеціального зв'язку та захисту інформації України, іншим центральним органам виконавчої влади, яким підпорядковані ці навчальні заклади, витрати, пов'язані з їх утриманням у вищому навчальному закладі, відповідно до порядку та умов, установлених Кабінетом Міністрів України. У разі відмови від добровільного відшкодування витрат таке відшкодування здійснюється у судовому порядку.

(статтю 12 доповнено частиною третьою згідно
із Законом України від 02.06.2009 р. N 1415-VI)

Стаття 13. Обмеження політичної діяльності в Державній службі спеціального зв'язку та захисту інформації України

1. Особи рядового і начальницького складу, державні службовці та інші працівники Державної служби спеціального зв'язку та захисту інформації України на період служби чи роботи в Державній службі спеціального зв'язку та захисту інформації України зупиняють членство в політичних партіях.

2. Особи рядового і начальницького складу, державні службовці та інші працівники Державної служби спеціального зв'язку та захисту інформації України можуть бути членами громадських організацій, статутні положення яких не суперечать засадам діяльності Державної служби спеціального зв'язку та захисту інформації України, і можуть брати участь у їх роботі у вільний від виконання службових обов'язків час.

3. Особам рядового і начальницького складу, державним службовцям та іншим працівникам Державної служби спеціального зв'язку та захисту інформації України заборонено організовувати та брати участь у страйках.

Стаття 14. Підготовка, перепідготовка та підвищення кваліфікації кадрів для Державної служби спеціального зв'язку та захисту інформації України

1. Підготовка, перепідготовка та підвищення кваліфікації особового складу Державної служби спеціального зв'язку та захисту інформації України проводяться в навчальних закладах Державної служби спеціального зв'язку та захисту інформації України та в інших навчальних закладах.

2. Порядок і строки підвищення кваліфікації та перепідготовки кадрів для Державної служби спеціального зв'язку та захисту інформації України визначаються головою Державної служби спеціального зв'язку та захисту інформації України.

3. Особи, які закінчили вищі навчальні заклади Державної служби спеціального зв'язку та захисту інформації України і яким присвоєно спеціальне звання начальницького складу, звільняються від призову на строкову військову службу.

(частина третя статті 14 у редакції
Закону України від 11.05.2007 р. N 1014-V)

Стаття 15. Спеціальний облік осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України, зарахування їх у запас

1. Особи рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України перебувають на спеціальному обліку в Державній службі спеціального зв'язку та захисту інформації України.

Розділ IV
ПОВНОВАЖЕННЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Стаття 16. Обов'язки Державної служби спеціального зв'язку та захисту інформації України

1. На Державну службу спеціального зв'язку та захисту інформації України відповідно до визначених завдань покладаються такі обов'язки:

1) підготовка пропозицій щодо визначення загальної стратегії та пріоритетних напрямів діяльності у сфері захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації;

2) розроблення і здійснення заходів щодо розвитку систем криптографічного та технічного захисту інформації;

3) розроблення порядку та вимог щодо захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

4) забезпечення надійного функціонування, безпеки та розвитку державної системи урядового зв'язку, зокрема її готовності до роботи в особливий період та в разі виникнення надзвичайної ситуації;

5) забезпечення в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України та Прем'єр-міністра України в місцях їх постійного і тимчасового перебування;

6) забезпечення в установленому Президентом України порядку урядовим зв'язком посадових осіб органів державної влади, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій;

7) участь у виконанні завдань територіальної оборони, а також заходів, спрямованих на підтримання правового режиму воєнного та надзвичайного стану відповідно до закону;

8) упровадження комплексних систем захисту інформації на об'єктах інформаційної діяльності та в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах закордонних дипломатичних установ України;

9) здійснення заходів щодо організації та забезпечення безпеки і функціонування урядового зв'язку із закордонними дипломатичними установами України;

10) методичне керівництво та координація діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності у сфері криптографічного та технічного захисту інформації, а також з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;

11) накопичення та аналіз даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, а також про їх наслідки, інформування правоохоронних органів для вжиття заходів із запобігання та припинення злочинів у зазначеній сфері; оцінка стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, надання відповідних рекомендацій;

12) здійснення заходів щодо створення, розвитку та забезпечення функціонування Національної системи конфіденційного зв'язку, забезпечення її безпеки та оперативно-технічного управління;

13) погодження проектів створення інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, в яких оброблятиметься інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, проведення їх експертної оцінки і визначення можливості введення в експлуатацію;

14) погодження та здійснення контролю за виконанням технічних завдань на проектування, будівництво і реконструкцію особливо важливих об'єктів, розробку зразків військової та спеціальної техніки, у процесі експлуатації або застосування яких збирається, обробляється, зберігається, передається чи приймається інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом;

(пункт 14 частини першої статті 16 із змінами, внесеними
згідно із Законом України від 19.03.2009 р. N 1180-VI)

15) погодження проектів нормативно-правових актів з питань захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також з питань щодо умов здійснення міжнародних передач криптографічних систем, засобів криптографічного та технічного захисту інформації, зокрема тих, що наявні у складі озброєння, військової та спеціальної техніки;

16) встановлення порядку і вимог щодо використання інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, у тому числі загального користування, органами державної влади, органами місцевого самоврядування, підприємствами, установами і організаціями незалежно від форм власності, які збирають, обробляють, зберігають та передають інформацію, яка є власністю держави, або інформацію з обмеженим доступом, вимога щодо захисту якої встановлена законом;

17) видача та реєстрація відповідно до вимог законодавства ліцензії на провадження господарської діяльності у сфері криптографічного та технічного захисту інформації, встановлення порядку видачі та видача органам державної влади дозволу на проведення робіт з технічного захисту інформації для власних потреб, а також здійснення контролю за додержанням ліцензійних умов та умов проведення робіт для власних потреб;

(пункт 17 частини першої статті 16 у редакції
Закону України від 19.03.2009 р. N 1180-VI)

18) організація та координація разом з центральним органом виконавчої влади у сфері стандартизації, метрології та сертифікації робіт з проведення сертифікації засобів криптографічного та технічного захисту інформації, організація та проведення державної експертизи у сфері криптографічного та технічного захисту інформації;

19) здійснення технічного регулювання у сферах захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації, організація та проведення оцінки відповідності, розроблення в установленому порядку стандартів, технічних регламентів, технічних умов;

20) розроблення та супроводження моделей технічних розвідок шляхом збору та аналізу інформації про існуючі системи і засоби технічних розвідок, тактику та методи їх застосування, а також перспективи розвитку; надання рекомендацій органам державної влади, органам місцевого самоврядування, військовим формуванням, підприємствам, установам і організаціям щодо забезпечення протидії технічним розвідкам, проведення оцінки загроз та вжиття відповідних заходів для захисту інформації;

(пункт 20 частини першої статті 16 із змінами, внесеними
згідно із Законом України від 19.03.2009 р. N 1180-VI)

21) участь у межах своїх повноважень у погодженні питань щодо розміщення на території України дипломатичних представництв і консульських установ іноземних держав;

22) розроблення та організація виконання наукових і науково-технічних програм за напрямами її діяльності;

23) здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в органах державної влади, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності, у тому числі в закордонних дипломатичних установах України, місцях постійного та тимчасового перебування Президента України, Голови Верховної Ради України та Прем'єр-міністра України, а також під час діяльності на території України іноземних інспекційних груп відповідно до міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України;

(пункт 23 частини першої статті 16 із змінами, внесеними
згідно із Законом України від 19.03.2009 р. N 1180-VI)

24) здійснення державного контролю за додержанням вимог безпеки у процесі розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення і знищення криптографічних систем і засобів криптографічного захисту інформації та обладнання спеціального зв'язку;

25) подання Президенту України за результатами державного контролю аналітичних матеріалів щодо стану криптографічного та технічного захисту інформації в державі, розроблення рекомендацій щодо його поліпшення;

(пункт 25 частини першої статті 16 у редакції
Закону України від 07.10.2010 р. N 2592-VI)

26) здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису;

27) здійснення приймання та контролю якості продукції, інших товарів військового призначення, які виготовляються чи модернізуються на її замовлення;

28) розроблення, виготовлення та постачання ключових документів до засобів криптографічного захисту інформації, що містить державну таємницю, та конфіденційної інформації, що є власністю держави;

29) організація та здійснення разом з центральним органом виконавчої влади у галузі освіти і науки науково-методичного управління підготовкою кадрів у сфері криптографічного та технічного захисту інформації;

30) пункт 30 частини першої статті 16 виключено

(згідно із Законом України
від 01.06.2010 р. N 2289-VI,
який вводиться в дію з 31 липня 2010 року)

31) погодження міжнародних передач криптографічних систем, засобів криптографічного та технічного захисту інформації, зокрема у складі озброєння, військової та спеціальної техніки;

(частину першу статті 16 доповнено пунктом 31
згідно із Законом України від 19.03.2009 р. N 1180-VI)

32) видача атестата відповідності комплексних систем захисту інформації інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, із застосуванням яких обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, вимогам нормативних документів з питань технічного захисту інформації;

(частину першу статті 16 доповнено пунктом 32
згідно із Законом України від 19.03.2009 р. N 1180-VI)

33) здійснення у порядку, визначеному Кабінетом Міністрів України, державного контролю за дотриманням умов експлуатації комплексних систем захисту інформації, які пройшли державну експертизу та на які видано атестат відповідності;

(частину першу статті 16 доповнено пунктом 33
згідно із Законом України від 19.03.2009 р. N 1180-VI)

34) встановлення порядку здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису, а також станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також під час провадження діяльності на території України іноземних інспекційних груп відповідно до міжнародних договорів України.

(частину першу статті 16 доповнено пунктом 34
згідно із Законом України від 19.03.2009 р. N 1180-VI)

2. Посадові особи відповідних підрозділів Державної служби спеціального зв'язку та захисту інформації України несуть відповідальність відповідно до закону за порушення конституційних прав і свобод людини та громадянина у процесі використання засобів спеціального зв'язку.

Стаття 17. Права Державної служби спеціального зв'язку та захисту інформації України

1. Для забезпечення виконання покладених на неї завдань Державна служба спеціального зв'язку та захисту інформації України має право:

1) одержувати в установленому порядку за письмовими запитами керівників відповідних органів та територіальних підрозділів Державної служби спеціального зв'язку та захисту інформації України від органів державної влади, органів місцевого самоврядування,

військових формувань, підприємств, установ і організацій незалежно від форм власності інформацію, документи і матеріали, необхідні для виконання покладених на неї завдань;

2) залучати фахівців органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності за погодженням з їх керівниками до розгляду питань, що належать до її повноважень, а також проведення спільних інспекційних перевірок;

3) доступу в установленому порядку своїх уповноважених представників на об'єкти органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності, на яких знаходяться її засоби спеціального зв'язку, а також об'єкти, щодо яких здійснюється державний контроль за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

4) надавати на договірних засадах допомогу підприємствам, установам і організаціям незалежно від форм власності у розробленні та здійсненні заходів із захисту інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації;

5) здійснювати планові та позапланові інспекційні перевірки стану криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в органах державної влади, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності, у тому числі в закордонних дипломатичних установах України, без одержання доступу до змісту інформації;

6) зупиняти дію або скасовувати в установленому порядку ліцензії на провадження господарської діяльності у сфері криптографічного та технічного захисту інформації, а також дозволів на проведення робіт з технічного захисту інформації для власних потреб органам державної влади;

7) порушувати в установленому порядку питання про припинення інформаційної діяльності з використанням інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем в органах державної влади, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності у разі порушення ними вимог законодавства у сфері захисту державних інформаційних ресурсів, криптографічного та/або технічного захисту інформації;

8) одержувати в установленому порядку смуги радіочастот для використання їх радіозасобами спеціального зв'язку;

9) залучати спеціальних та загальних користувачів радіочастотного ресурсу для виявлення та усунення радіозавад радіоелектронним засобам державної системи урядового зв'язку та Національної системи конфіденційного зв'язку;

10) організовувати, проводити та виконувати науково-дослідні, дослідно-конструкторські роботи;

11) виступати державним замовником з оборонного замовлення та замовником закупівлі товарів, робіт і послуг за державні кошти;

12) виступати замовником будівництва об'єктів Державної служби спеціального зв'язку та захисту інформації України;

13) утворювати координаційні, консультативні та дорадчі органи;

14) провадити в установленому порядку видавничу діяльність;

15) здійснювати в порядку, передбаченому законодавством, господарську діяльність, що безпосередньо пов'язана із забезпеченням виконання покладених на неї завдань, за видами діяльності, перелік яких визначається Кабінетом Міністрів України;

16) відчужувати в порядку, передбаченому законодавством, закріплене за нею державне майно;

17) складати протоколи про адміністративні правопорушення;

18) здійснювати міжнародне співробітництво з питань, що належать до її компетенції, розробляти пропозиції щодо укладення відповідних міжнародних договорів України, взаємодіяти відповідно до міжнародних договорів України з міжнародними організаціями з питань запобігання порушенню безпеки інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;

19) проводити планову та позапланову перевірку додержання ліцензійних умов провадження господарської діяльності у сфері криптографічного та технічного захисту інформації на підприємствах, в установах і організаціях, а також умов проведення робіт з технічного захисту інформації для власних потреб в органах державної влади;

(частину першу статті 17 доповнено пунктом 19
згідно із Законом України від 19.03.2009 р. N 1180-VI)

20) зупиняти дію або скасовувати в установленому порядку атестати відповідності на комплексні системи захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;

(частину першу статті 17 доповнено пунктом 20
згідно із Законом України від 19.03.2009 р. N 1180-VI)

21) проводити планову та позапланову перевірку центрального засвідчувального органу, засвідчувальних центрів і центрів сертифікації ключів щодо додержання ними вимог законодавства у сфері надання послуг електронного цифрового підпису;

(частину першу статті 17 доповнено пунктом 21
згідно із Законом України від 19.03.2009 р. N 1180-VI)

22) звертатися до суду у разі виникнення спорів з питань організації спеціального зв'язку та захисту інформації, криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, спорів у сфері надання послуг електронного цифрового підпису, а також у разі виникнення інших спорів у порядку, встановленому законом.

(частину першу статті 17 доповнено пунктом 22
згідно із Законом України від 19.03.2009 р. N 1180-VI)

2. Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації в межах своїх повноважень на основі та відповідно до законодавства видає накази, організовує та контролює їх виконання.

3. Накази спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації, прийняті в межах його повноважень, обов'язкові для виконання органами державної влади, органами місцевого самоврядування, військовими формуваннями, підприємствами, установами і організаціями незалежно від форм власності та фізичними особами.

Стаття 18. Відносини Державної служби спеціального зв'язку та захисту інформації України з органами державної влади, органами місцевого самоврядування, військовими формуваннями, підприємствами, установами і організаціями

1. Державна служба спеціального зв'язку та захисту інформації України виконує покладені на неї завдання у взаємодії зі Службою безпеки України, Міністерством оборони України, Службою зовнішньої розвідки України, Міністерством закордонних справ України, Міністерством внутрішніх справ України, Управлінням державної охорони України, національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, центральними органами виконавчої влади з питань цивільного захисту та у галузі транспорту і зв'язку, іншими органами державної влади, органами місцевого самоврядування, військовими формуваннями, підприємствами, установами і організаціями.

(частина перша статті 18 із змінами, внесеними
згідно із Законом України від 07.07.2011 р. N 3610-VI)

2. Органи державної влади та органи місцевого самоврядування, їх посадові і службові особи в межах своїх повноважень сприяють діяльності Державної служби спеціального зв'язку та захисту інформації України у виконанні покладених на неї завдань.

3. За перешкоджання законній діяльності Державної служби спеціального зв'язку та захисту інформації України винні особи несуть відповідальність згідно із законом.

4. Громадяни України, об'єднання громадян сприяють діяльності Державної служби спеціального зв'язку та захисту інформації України на добровільних засадах.

Стаття 19. Підстави і порядок застосування зброї

1. Для охорони об'єктів і майна Державної служби спеціального зв'язку та захисту інформації України особи рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України мають право зберігати, носити, використовувати та застосовувати зброю на підставах і в порядку, передбачених статтями 15, 15[1] Закону України "Про міліцію" та іншими нормативно-правовими актами.

Розділ V
ПРАВОВИЙ ТА СОЦІАЛЬНИЙ ЗАХИСТ ОСОБОВОГО СКЛАДУ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Стаття 20. Правове становище та правовий захист особового складу Державної служби спеціального зв'язку та захисту інформації України

1. Особи рядового і начальницького складу, державні службовці та інші працівники Державної служби спеціального зв'язку та захисту інформації України під час виконання покладених на них обов'язків діють на підставі, у межах своїх повноважень та у спосіб, що передбачені Конституцією та законами України. Ніхто інший, за винятком уповноважених посадових осіб органів державної влади у передбачених законами України випадках, не має права втручатися в їх законну діяльність.

2. Особам рядового і начальницького складу, державним службовцям та іншим працівникам Державної служби спеціального зв'язку та захисту інформації України видається службове посвідчення.

3. Особи рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України мають право на носіння форменого одягу із знаками розрізнення, зразки яких затверджуються головою Державної служби спеціального зв'язку та захисту інформації України.

4. Використання спеціальних звань, відзнак, форменого одягу, службового посвідчення особою, яка не належить до особового складу Державної служби спеціального зв'язку та захисту інформації України, тягне за собою відповідальність, передбачену законом.

5. Витрати осіб рядового і начальницького складу, державних службовців та інших працівників Державної служби спеціального зв'язку та захисту інформації України на проїзд усіма видами міського та приміського пасажирського транспорту (крім таксі) при виконанні ними службових обов'язків компенсуються за рахунок коштів Державного бюджету України, призначених на утримання Державної служби спеціального зв'язку та захисту інформації України, в установленому головою Державної служби спеціального зв'язку та захисту інформації України порядку.

Стаття 21. Соціальний захист особового складу Державної служби спеціального зв'язку та захисту інформації України

1. Держава забезпечує соціальний захист особового складу Державної служби спеціального зв'язку та захисту інформації України відповідно до Конституції України, цього Закону та інших актів законодавства.

2. Умови грошового і матеріального забезпечення осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України визначаються законодавством і мають забезпечувати належні матеріальні умови для її комплектування висококваліфікованими фахівцями, враховувати характер і умови служби, стимулювати досягнення високих результатів у службовій та професійній діяльності. Порядок і розміри грошового і матеріального забезпечення осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України та грошової компенсації замість речового майна встановлюються Кабінетом Міністрів України.

3. Для осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України встановлюється 41-годинний робочий тиждень. У разі необхідності особи рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України несуть службу понад встановлену тривалість робочого часу, а також у вихідні та святкові дні з наданням іншого дня відпочинку.

4. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України надаються чергові щорічні відпустки із збереженням грошового забезпечення. Тривалість такої відпустки для осіб рядового і начальницького складу, які мають вислугу років до 10 календарних років, - 30 діб, від 10 до 20 років, - 35 діб, від 20 до 25 років, - 40 діб, 25 і більше календарних років, - 45 діб без урахування часу, необхідного для проїзду до місця проведення відпустки і назад. Учасникам бойових дій та прирівняним до них особам щорічні відпустки надаються незалежно від вислуги років строком 45 діб у зручний для них час.

5. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України та членам їх сімей забезпечується безоплатний проїзд у відпустку, а також безоплатний проїзд і перевезення багажу при переїзді на нове місце служби і виплачується грошова допомога у порядку, встановленому Кабінетом Міністрів України.

6. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України виплачується грошова допомога на оздоровлення у розмірах, що визначаються законодавством України.

7. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України надаються щорічні додаткові відпустки відповідно до законодавства. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України можуть надаватися додаткові відпустки терміном до 10 діб із збереженням грошового забезпечення за сімейними обставинами та з інших поважних причин у порядку, встановленому головою Державної служби спеціального зв'язку та захисту інформації України.

8. Держава забезпечує осіб особового складу Державної служби спеціального зв'язку та захисту інформації України та членів їх сімей жилими приміщеннями на підставах, у порядку і відповідно до вимог, встановлених житловим законодавством. Жилі приміщення для постійного проживання надаються особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України один раз протягом усього часу проходження ними служби в Державній службі спеціального зв'язку та захисту інформації України.

9. До одержання жилого приміщення для постійного проживання особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України, які відповідно до законодавства потребують поліпшення житлових умов, надаються службові жилі приміщення або жила площа в гуртожитку. У разі відсутності такого житла Державна служба спеціального зв'язку та захисту інформації України тимчасово орендує житло для забезпечення ним осіб рядового і начальницького складу або за бажанням цих осіб виплачує їм грошову компенсацію за піднайом (найом, оренду) жилого приміщення в порядку, розмірі та на умовах, які визначаються Кабінетом Міністрів України. За ними зберігається право на жилу площу, яку вони займали до вступу на службу в Державну службу спеціального зв'язку та захисту інформації України. Вони не можуть бути виключені із списків громадян, взятих на квартирний облік.

10. Особи рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України і ті, хто перебував на службі не менше 20 років, звільнені зі служби за станом здоров'я, віком або скороченням штатів, забезпечуються жилими приміщеннями центральними і місцевими органами виконавчої влади у першу чергу, але не пізніше ніж у тримісячний строк з дня прибуття цієї особи до місця проживання, обраного з урахуванням встановленого порядку.

11. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України та членам їх сімей, які перебувають на їх утриманні, батькам та членам сімей осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України, які загинули (померли), пропали безвісти або стали інвалідами при проходженні служби, надається 50-відсоткова знижка плати за користування житлом (квартирної плати) та плати за комунальні послуги (водопостачання, газ, електричну, теплову енергію та інші послуги) в жилих будинках незалежно від форм власності в межах встановлених норм, передбачених законодавством.

Пільги на 50-відсоткову знижку за користування житлом (квартирної плати) та плати за комунальні послуги (водопостачання, газ, електричну, теплову енергію та інші послуги), в жилих будинках незалежно від форм власності в межах норм, встановлених законодавством, надаються:

(частину одинадцяту статті 21 доповнено абзацом згідно із Законом України від 28.12.2007 р. N 107-VI)

(зміни, внесені підпунктом 1 пункту 72 розділу II Закону України від 28.12.2007 р. N 107-VI, визнано такими, що не відповідають Конституції України (є неконституційними), згідно з Рішенням Конституційного Суду України від 22.05.2008 р. N 10-рп/2008)

особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України та членам їх сімей, які перебувають на їх утриманні за умови, якщо розмір наданих пільг у грошовому еквіваленті разом із середньомісячним сукупним доходом цієї особи за попередні шість місяців не перевищує величини доходу, який дає право на податкову соціальну пільгу у порядку, визначеному Кабінетом Міністрів України;

(частину одинадцяту статті 21 доповнено абзацом згідно із Законом України від 28.12.2007 р. N 107-VI)

(зміни, внесені підпунктом 1 пункту 72 розділу II Закону України від 28.12.2007 р. N 107-VI, визнано такими, що не відповідають Конституції України (є неконституційними), згідно з Рішенням Конституційного Суду України від 22.05.2008 р. N 10-рп/2008)

батькам та членам сімей осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України, які загинули (померли), пропали

безвісти або стали інвалідами при проходженні служби за умови, якщо розмір середньомісячного сукупного доходу сім'ї в розрахунку на одну особу за попередні шість місяців не перевищує величини доходу, який дає право на податкову соціальну пільгу у порядку, визначеному Кабінетом Міністрів України.

(частину одинадцяту статті 21 доповнено абзацом згідно із Законом України від 28.12.2007 р. N 107-VI)

(зміни, внесені підпунктом 1 пункту 72 розділу II Закону України від 28.12.2007 р. N 107-VI, визнано такими, що не відповідають Конституції України (є неконституційними), згідно з Рішенням Конституційного Суду України від 22.05.2008 р. N 10-рп/2008)

12. Пенсійне забезпечення осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України здійснюється у порядку, на умовах та у розмірах, установлених Законом України "Про пенсійне забезпечення осіб, звільнених з військової служби, та деяких інших осіб".

(частина дванадцята статті 21 із змінами, внесеними згідно із Законом України від 03.11.2006 р. N 328-V)

13. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України при звільненні зі служби за віком, після закінчення строку контракту, за станом здоров'я, у зв'язку зі скороченням штатів або з організаційними заходами в разі неможливості використання на службі виплачується грошова допомога у розмірі 50 відсотків місячного грошового забезпечення за кожний повний календарний рік служби. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України, звільненим зі служби через сімейні обставини або з інших поважних причин, перелік яких визначається Кабінетом Міністрів України, виплачується грошова допомога у розмірі 25 відсотків місячного грошового забезпечення за кожний повний календарний рік служби. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України, звільненим зі служби за службовою невідповідністю, у зв'язку з обвинувальним вироком суду, що набрав законної сили, грошова допомога не виплачується.

14. На осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України, крім передбачених цим Законом, поширюються права і соціальні гарантії, передбачені Законом України "Про статус ветеранів військової служби, ветеранів органів внутрішніх справ і деяких інших осіб та їх соціальний захист" та іншими актами законодавства.

15. У разі загибелі (смерті) особи рядового чи начальницького складу Державної служби спеціального зв'язку та захисту інформації України під час виконання службових обов'язків сім'ї загиблого (померлого), а в разі її відсутності його батькам та утриманцям виплачується одноразова грошова допомога в розмірі десятирічного грошового забезпечення загиблого (померлого) за останньою посадою, яку він займав, в порядку та на умовах, визначених Кабінетом Міністрів України. За сім'єю загиблого (померлого) зберігається право на одержання жилого приміщення.

16. У разі поранення (контузії, травми або каліцтва), заподіяного особі рядового чи начальницького складу Державної служби спеціального зв'язку та захисту інформації України під час виконання службових обов'язків, а також інвалідності, що настала в період проходження служби або не пізніше ніж через три місяці після звільнення зі служби чи після закінчення цього строку, але внаслідок захворювання або нещасного випадку, що мали місце в період проходження служби, пов'язаних з виконанням службових обов'язків, залежно від ступеня втрати працездатності йому виплачується одноразова грошова допомога в розмірі до п'ятирічного грошового забезпечення за останньою посадою в порядку та на умовах, визначених Кабінетом Міністрів України. Визначення ступеня втрати працездатності особою рядового чи начальницького складу Державної служби спеціального зв'язку та захисту інформації України у період проходження служби в Державній службі спеціального зв'язку та захисту інформації України у кожному випадку ушкодження здоров'я здійснюється в індивідуальному порядку відповідно до законодавства.

17. У всіх випадках розмір одноразової грошової допомоги у разі загибелі (смерті) особи рядового чи начальницького складу Державної служби спеціального зв'язку та захисту інформації України не повинен бути меншим від 100-кратного розміру прожиткового мінімуму, встановленого законом для працездатних осіб на час виплати цих сум.

(частина сімнадцята статті 21 набирає чинності з 1 січня 2008 року згідно із Законом України від 03.11.2006 р. N 328-V)

18. Якщо особа рядового чи начальницького складу Державної служби спеціального зв'язку та захисту інформації України або члени її сім'ї одночасно мають право на отримання одноразової грошової допомоги з підстав, передбачених цією статтею, та одноразової грошової допомоги або компенсаційної виплати, встановлених іншими законами, виплата відповідних грошових сум здійснюється за однією з підстав за вибором особи, яка має право на отримання таких виплат.

(частину п'ятнадцяту - сімнадцяту статті 21 замінено чотирма частинами згідно із Законом України від 03.11.2006 р. N 328-V, у зв'язку з цим частини вісімнадцяту - двадцяту вважати відповідно частинами дев'ятнадцятою - двадцять першою)

19. Діти осіб рядового і начальницького складу, державних службовців та інших працівників Державної служби спеціального зв'язку та захисту інформації України, які загинули під час виконання службових обов'язків, мають право вступу до навчальних закладів Державної служби спеціального зв'язку та захисту інформації України поза конкурсом.

(частина дев'ятнадцята статті 21 із змінами, внесеними згідно із Законом України від 15.01.2009 р. N 879-VI)

20. Шкода, завдана майну особи рядового чи начальницького складу, державного службовця або іншого працівника Державної служби спеціального зв'язку та захисту інформації України чи майну членів його сім'ї у зв'язку з виконанням службових обов'язків, відшкодовується в повному обсязі за рахунок коштів Державного бюджету України з наступним стягненням цієї суми з винних осіб у порядку, встановленому законом.

21. Соціальний захист державних службовців та інших працівників Державної служби спеціального зв'язку та захисту інформації України забезпечується на загальних підставах відповідно до законодавства про працю і державну службу.

Стаття 22. Медичне та санаторно-курортне забезпечення особового складу Державної служби спеціального зв'язку та захисту інформації України

(назва статті 22 у редакції Закону
України від 19.03.2009 р. N 1180-VI)

1. Особам рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України створюються необхідні санітарно-гігієнічні та соціально-психологічні умови. Зазначені особи забезпечуються безоплатною кваліфікованою медичною допомогою в медичних закладах Державної служби спеціального зв'язку та захисту інформації України, а також Служби безпеки України, Міністерства оборони України, Міністерства внутрішніх справ України та Міністерства охорони здоров'я України за рахунок бюджетних коштів, передбачених на утримання Державної служби спеціального зв'язку та захисту інформації України, за угодами, укладеними нею із зазначеними центральними органами виконавчої влади. У разі відсутності за місцем служби чи проживання осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України медичних закладів Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Міністерства оборони України, Міністерства внутрішніх справ України, Міністерства охорони здоров'я України медична допомога надається відповідно до законодавства в інших державних або комунальних закладах охорони здоров'я. При цьому витрати на лікування осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України здійснюються за рахунок бюджетних коштів, передбачених на утримання Державної служби спеціального зв'язку та захисту інформації України.

2. Забезпечення медичною допомогою членів сімей осіб рядового і начальницького складу у разі відсутності за місцем їх проживання державних або комунальних закладів охорони здоров'я, ветеранів Державної служби спеціального зв'язку та захисту інформації України здійснюється на умовах і в порядку, визначених частиною першою цієї статті для осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України.

(статтю 22 доповнено новою частиною другою
згідно із Законом України від 19.03.2009 р. N 1180-VI,
у зв'язку з цим частини другу та третю вважати
відповідно частинами третьою та четвертою)

3. Особи рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України та члени їх сімей мають право на санаторно-курортне лікування та організований відпочинок у відповідних закладах Державної служби спеціального зв'язку та захисту інформації України, а також у санаторно-курортних закладах Служби безпеки України, Міністерства оборони України, Міністерства внутрішніх справ України та Міністерства охорони здоров'я України за рахунок бюджетних коштів, передбачених на утримання Державної служби спеціального зв'язку та захисту інформації України, на основі укладених з ними угод згідно із законодавством.

4. Жінки із числа осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України користуються всіма пільгами, передбаченими законодавством стосовно соціального захисту жінок, охорони материнства і дитинства. Зазначені пільги поширюються також на батьків з числа осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України, які виховують дітей без матері (у разі її смерті, позбавлення батьківських прав, на час перебування в лікувальному закладі та в інших випадках відсутності материнського піклування про дітей).

Розділ VI
ФІНАНСОВЕ ТА МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Стаття 23. Фінансове забезпечення Державної служби спеціального зв'язку та захисту інформації України

1. Фінансове забезпечення Державної служби спеціального зв'язку та захисту інформації України здійснюється за рахунок коштів Державного бюджету України.

2. Пільги, компенсації та гарантії, передбачені цим Законом, надаються за рахунок і в межах бюджетних асигнувань на утримання відповідних бюджетних установ.

(статтю 23 доповнено частиною другою згідно із Законом України від 28.12.2007 р. N 107-VI)

(зміни, внесені підпунктом 2 пункту 72 розділу II Закону України від 28.12.2007 р. N 107-VI, визнано такими, що не відповідають Конституції України (є неконституційними), згідно з Рішенням Конституційного Суду України від 22.05.2008 р. N 10-рп/2008)

Стаття 24. Матеріально-технічне забезпечення діяльності Державної служби спеціального зв'язку та захисту інформації України

1. Держава забезпечує Державну службу спеціального зв'язку та захисту інформації України необхідними матеріальними засобами, технікою, обладнанням, іншим майном для здійснення службової діяльності.

2. Державній службі спеціального зв'язку та захисту інформації України надаються в установленому порядку земельні ділянки з метою розміщення адміністративних і господарських будівель, стаціонарних технічних засобів та інженерних споруд, інших об'єктів, необхідних для функціонування Державної служби спеціального зв'язку та захисту інформації України, розташування її регіональних органів, територіальних підрозділів, навчальних закладів, державних підприємств і установ, зазначених у частині другій статті 5 цього Закону.

3. Майно, що належить Державній службі спеціального зв'язку та захисту інформації України, є державною власністю та закріплюється спеціально уповноваженим центральним

органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації за регіональними органами, територіальними підрозділами, навчальними, медичними, санаторно-курортними та іншими закладами, науково-дослідними та науково-виробничими установами Державної служби спеціального зв'язку та захисту інформації України на праві оперативного управління.

4. Державна служба спеціального зв'язку та захисту інформації України має житловий фонд, може виступати замовником будівництва житла. У разі звільнення особами з числа особового складу Державної служби спеціального зв'язку та захисту інформації України жилих приміщень, замовником будівництва яких виступала Державна служба спеціального зв'язку та захисту інформації України, або які були придбані за рахунок коштів Державного бюджету України, призначених на утримання Державної служби спеціального зв'язку та захисту інформації України, зазначене житло в установленому порядку заселяється особами з числа особового складу Державної служби спеціального зв'язку та захисту інформації України, які потребують поліпшення житлових умов.

Розділ VII
КОНТРОЛЬ ТА НАГЛЯД ЗА ДІЯЛЬНІСТЮ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Стаття 25. Контроль за діяльністю Державної служби спеціального зв'язку та захисту інформації України

1. Контроль за діяльністю Державної служби спеціального зв'язку та захисту інформації України здійснюється в порядку, визначеному Конституцією України та законами України.

2. Голова Державної служби спеціального зв'язку та захисту інформації України в установленому порядку інформує Президента України з основних питань діяльності Державної служби спеціального зв'язку та захисту інформації України, про виконання покладених на Службу завдань, додержання законодавства, прав і свобод людини та громадянина, щороку подає Президенту України звіт про її діяльність.

(частина друга статті 25 у редакції
Закону України від 07.10.2010 р. N 2592-VI)

3. Голова Державної служби спеціального зв'язку та захисту інформації України в установленому порядку інформує Верховну Раду України про виконання покладених на Державну службу спеціального зв'язку та захисту інформації України завдань, додержання законодавства, прав і свобод людини та громадянина, інших питань.

(статтю 25 доповнено частиною третьою згідно із
Законом України від 07.10.2010 р. N 2592-VI)

Стаття 26. Нагляд за додержанням законності в діяльності Державної служби спеціального зв'язку та захисту інформації України

1. Нагляд за додержанням законності в діяльності Державної служби спеціального зв'язку та захисту інформації України здійснюється в порядку, визначеному Конституцією та законами України.

Розділ VIII
ВІДПОВІДАЛЬНІСТЬ ЗА ПРАВОПОРУШЕННЯ У СФЕРІ ДІЯЛЬНОСТІ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Стаття 27. Відповідальність за порушення вимог цього Закону

1. Особи, винні в порушенні вимог цього Закону, несуть відповідальність згідно із законом.

2. За віддання і виконання явно злочинного розпорядження чи наказу винні особи з числа особового складу Державної служби спеціального зв'язку та захисту інформації України несуть відповідальність згідно із законом.

Розділ IX
ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності з 1 січня 2007 року, крім статей 5, 6, 7 та пункту 7 розділу IX "Прикінцеві та перехідні положення", що вводяться в дію з дня його опублікування.

2. Державна служба спеціального зв'язку та захисту інформації України утворюється на базі та за рахунок чисельності Департаменту спеціальних телекомунікаційних систем та захисту інформації і відповідних підрозділів Служби безпеки України. Державна служба спеціального зв'язку та захисту інформації України є правонаступником Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Заходи, пов'язані із створенням Державної служби спеціального зв'язку та захисту інформації України, здійснюються у 2006 році в межах бюджетних коштів, призначених на утримання Служби безпеки України Законом України "Про Державний бюджет України на 2006 рік".

3. Військовослужбовці, які на момент набрання чинності цим Законом проходять військову службу в Службі безпеки України, призначаються за їх згодою на відповідні посади осіб рядового чи начальницького складу Державної служби спеціального зв'язку та захисту інформації України в порядку переатестації або продовжують проходити військову службу на цих посадах відповідно до законодавства з питань проходження військової служби військовослужбовцями Служби безпеки України, але не пізніш як до 31 грудня 2007 року. На зазначених військовослужбовців поширюється дія цього Закону.

4. Установити, що військовослужбовцям Служби безпеки України при зарахуванні їх на службу до Державної служби спеціального зв'язку та захисту інформації України присвоюються спеціальні звання Державної служби спеціального зв'язку та захисту інформації України, рівноцінні тим, які були їм присвоєні при проходженні військової служби. Строк проходження ними військової служби зараховується до строку проходження служби в Державній службі спеціального зв'язку та захисту інформації України.

5. До приведення у відповідність із Законом України "Про Державну службу спеціального зв'язку та захисту інформації України" закони та інші нормативно-правові акти застосовуються в частині, що не суперечить цьому Закону.

6. Внести зміни до таких законів України:

1) у пункті 1 частини першої статті 255 Кодексу України про адміністративні правопорушення (Відомості Верховної Ради УРСР, 1984 р., додаток до N 51, ст. 1122):

в абзаці "органів Служби безпеки України (стаття 164 (у частині, що стосується правопорушень у галузі господарської діяльності, ліцензії на проведення якої видає ця Служба), статті 195^5, 212^2, 212^5 і 212^6)" цифри "212^2" замінити цифрами і словами "212^2 (крім пункту 9 частини першої)" і після цього абзацу доповнити новим абзацом такого змісту:

"органів Державної служби спеціального зв'язку та захисту інформації України (стаття 164 (у частині, що стосується правопорушень у галузі господарської діяльності, ліцензії на проведення якої видає ця Служба), пункт 9 частини першої статті 212^2)";

2) у Законі України "Про Службу безпеки України" (Відомості Верховної Ради України, 1992 р., N 27, ст. 382; 2000 р., N 10, ст. 79; 2003 р., N 27, ст. 209, N 29, ст. 236; 2004 р., N 32, ст. 394; із змінами, внесеними Законом України від 15 грудня 2005 року N 3200-IV):

у другому реченні частини першої статті 10 слова "урядового зв'язку" замінити словом "зв'язку";

у частині першій статті 15 слова "урядового зв'язку" виключити;

пункт 14 частини першої статті 24 виключити;

3) у Законі України "Про пенсійне забезпечення військовослужбовців, осіб начальницького і рядового складу органів внутрішніх справ та деяких інших осіб" (Відомості Верховної Ради України, 1992 р., N 29, ст. 399; 1994 р., N 24, ст. 78; 1996 р., N 17, ст. 73; 1998 р., N 26, ст. 149; 1999 р., N 4, ст. 35, N 48, ст. 409; 2001 р., N 9, ст. 38; 2002 р., N 17, ст. 125, N 35, ст. 262; 2003 р., N 27, ст. 209; 2004 р., N 50, ст. 536; 2005 р., N 4, ст. 107, NN 17 - 19, ст. 267; із змінами, внесеними Законом України від 15 грудня 2005 року N 3200-IV):

преамбулу після слів "органів внутрішніх справ України" доповнити словами "осіб начальницького і рядового складу Державної служби спеціального зв'язку та захисту інформації України";

частину першу статті 1 після слів "в державній пожежній охороні" доповнити словами "службі в Державній службі спеціального зв'язку та захисту інформації України";

частину другу статті 2 після слів "органів внутрішніх справ" доповнити словами "Державної служби спеціального зв'язку та захисту інформації України";

частину другу статті 10 після слів "Міністерством внутрішніх справ України" доповнити словами "Державною службою спеціального зв'язку та захисту інформації України";

частину першу статті 48 і частину другу статті 52 після слів "Служби зовнішньої розвідки України" доповнити словами "Державної служби спеціального зв'язку та захисту інформації України";

частину першу статті 49 після слів "Міністерства внутрішніх справ України" доповнити словами "Державної служби спеціального зв'язку та захисту інформації України";

4) у Законі України "Про статус ветеранів військової служби, ветеранів органів внутрішніх справ і деяких інших осіб та їх соціальний захист" (Відомості Верховної Ради України, 1998 р., N 40 - 41, ст. 249; 2003 р., N 27, ст. 209; 2004 р., N 50, ст. 536; 2005 р., N 4, ст. 107):

пункти 1, 5 і 7 частини першої статті 6 після слів "Служби безпеки України" доповнити словами "Державної служби спеціального зв'язку та захисту інформації України";

у тексті Закону:

слова "і ветеран державної пожежної охорони" у всіх відмінках і числах замінити словами "ветеран державної пожежної охорони, ветеран Державної служби спеціального зв'язку та захисту інформації України" у відповідному відмінку і числі;

слова "служба в органах внутрішніх справ і державної пожежної охорони" у всіх відмінках замінити словами "служба в органах внутрішніх справ, державній пожежній охороні, Державній службі спеціального зв'язку та захисту інформації України" у відповідному відмінку;

5) пункт 2 статті 8 Закону України "Про правовий режим майна у Збройних Силах України" (Відомості Верховної Ради України, 1999 р., N 48, ст. 407) доповнити словами "та Державну службу спеціального зв'язку та захисту інформації України";

6) абзац третій частини першої статті 8 та статтю 9 Закону України "Про державні нагороди України" (Відомості Верховної Ради України, 2000 р., N 21, ст. 162; 2003 р., N 27, ст. 209; із змінами, внесеними Законом України від 15 грудня 2005 року N 3200-IV) після слів "Служби зовнішньої розвідки України" доповнити словами "Державної служби спеціального зв'язку та захисту інформації України";

7) частину другу статті 38 та пункт 9 частини першої статті 39 Закону України "Про телекомунікації" (Відомості Верховної Ради України, 2004 р., N 12, ст. 155; із змінами, внесеними Законом України від 15 грудня 2005 року N 3200-IV) після слів "Служби зовнішньої розвідки України" доповнити словами "Державної служби спеціального зв'язку та захисту інформації України";

8) частину другу статті 5 Закону України "Про радіочастотний ресурс України" (Відомості Верховної Ради України, 2004 р., N 48, ст. 526; із змінами, внесеними Законом України від 15 грудня 2005 року N 3200-IV) після слів "Служби зовнішньої розвідки України" доповнити словами "Державної служби спеціального зв'язку та захисту інформації України";

9) абзац шостий частини першої статті 1 Закону України "Про загальну структуру і чисельність Служби безпеки України" (Відомості Верховної Ради України, 2006 р., N 4, ст. 53) виключити.

7. Кабінету Міністрів України:

1) вирішити питання:

пов'язані з утворенням Державної служби спеціального зв'язку та захисту інформації України на базі Департаменту спеціальних телекомунікаційних систем та захисту інформації та відповідних підрозділів Служби безпеки України;

щодо визначення загальної чисельності Державної служби спеціального зв'язку та захисту інформації України, виходячи з існуючої чисельності Департаменту спеціальних телекомунікаційних систем та захисту інформації та відповідних підрозділів Служби безпеки України, що ліквідовуються у зв'язку з утворенням Державної служби спеціального зв'язку

та захисту інформації України (загальна чисельність якої на день набрання чинності цим Законом має становити 8250 осіб, у тому числі 7400 осіб рядового і начальницького складу);

щодо встановлення умов та розмірів грошового забезпечення особам рядового і начальницького складу, заробітної плати державним службовцям та іншим працівникам створеної Державної служби спеціального зв'язку та захисту інформації України, а також розмірів грошового забезпечення військовослужбовцям, які переходять до Державної служби спеціального зв'язку та захисту інформації України, не допускаючи погіршення умов та розмірів, що були їм встановлені у Службі безпеки України;

щодо підготовки та подання до Верховної Ради України пропозицій стосовно зменшення загальної чисельності Служби безпеки України у зв'язку з утворенням Державної служби спеціального зв'язку та захисту інформації України;

2) розробити та подати до Верховної Ради України пропозиції щодо приведення інших законів України у відповідність із цим Законом;

3) розробити нормативно-правові акти, передбачені цим Законом;

4) привести свої нормативно-правові акти у відповідність із цим Законом;

5) забезпечити перегляд і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів, що суперечать цьому Закону.

Президент України **В. ЮЩЕНКО**

м. Київ
23 лютого 2006 року
N 3475-IV

ЗАКОН УКРАЇНИ

Про Дисциплінарний статут Державної служби спеціального зв'язку та захисту інформації України

Із змінами і доповненнями, внесеними
Законом України
від 17 травня 2012 року N 4711-VI

Верховна Рада України **постановляє**:

1. Затвердити Дисциплінарний статут Державної служби спеціального зв'язку та захисту інформації України (додається).

2. Цей Закон набирає чинності з дня його опублікування.

Президент України **В. ЮЩЕНКО**

м. Київ
4 вересня 2008 року
N 373-VI

ЗАТВЕРДЖЕНО
Законом України
від 4 вересня 2008 року N 373-VI

ДИСЦИПЛІНАРНИЙ СТАТУТ
Державної служби спеціального зв'язку та захисту інформації України

Цей Статут визначає сутність службової дисципліни, обов'язки осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України (далі - особи рядового і начальницького складу) стосовно її дотримання, види заохочень та дисциплінарних стягнень, порядок і права начальників щодо їх застосування, а також порядок оскарження дисциплінарних стягнень.

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Службова дисципліна

1. Службова дисципліна - дотримання особами рядового і начальницького складу Конституції і законів України, актів Президента України і Кабінету Міністрів України, інших нормативно-правових актів, наказів Державної служби спеціального зв'язку та захисту інформації України, а також Присяги, що складається особами рядового і начальницького складу відповідно до закону.

2. Службова дисципліна в Державній службі спеціального зв'язку та захисту інформації України досягається:

створенням належних умов проходження служби особами рядового і начальницького складу;

набуттям високого рівня професіоналізму;

забезпеченням гласності та об'єктивності під час проведення оцінки результатів службової діяльності;

дотриманням законності;

повсякденною вимогливістю начальників до підлеглих, постійною турботою про них, виявленням поваги до їх особистої гідності;

вихованням в осіб рядового і начальницького складу високих моральних і ділових якостей;

забезпеченням соціальної справедливості, високого рівня правового та соціального захисту;

правильним застосуванням заходів дисциплінарного впливу;

належним виконанням умов контракту про проходження служби.

Стаття 2. Начальники та підлеглі, старші й молодші за званням та посадою

1. Начальник - особа начальницького складу, яка має право віддавати накази та розпорядження, застосовувати заохочення і накладати дисциплінарні стягнення або порушувати клопотання про це перед старшим прямим начальником.

2. Начальники, яким особи рядового і начальницького складу підпорядковані по службі хоча б тимчасово, якщо про це оголошено наказом, вважаються прямими.

3. Найближчий до підлеглого прямий начальник є його безпосереднім начальником.

4. Особи рядового і начальницького складу, які займають рівні посади та не підпорядковані одна одній по службі, можуть бути старшими чи молодшими, що визначається згідно із спеціальним званням.

5. У разі спільного виконання службових обов'язків особами рядового і начальницького складу, не підпорядкованими одна одній по службі, старшою вважається особа, яка

визначена начальником або займає вищу посаду. При рівних посадах начальником є старший за спеціальним званням.

6. У разі тимчасового виконання обов'язків, якщо про це оголошено наказом, начальник користується дисциплінарною владою, передбаченою посадою, яку він обіймає тимчасово.

7. Начальники в межах наданих їм повноважень можуть видавати накази, які є обов'язковими для виконання.

Стаття 3. Накази

1. Наказ є формою реалізації службових повноважень особи начальницького складу, згідно з яким визначаються мета і предмет завдання, строк його виконання та відповідальна особа, якій належить його виконати.

2. Накази можуть даватись як в усній, так і в письмовій формі.

3. У разі одержання наказу від старшого прямого начальника підлеглий зобов'язаний виконати його та повідомити про це свого безпосереднього начальника.

4. Скасувати наказ має право тільки начальник, який видав відповідний наказ, або старший прямий начальник.

5. Накази повинні бути законними, зрозумілими і виконуватися беззаперечно, точно та у визначений строк.

6. У разі одержання наказу, який суперечить закону, підлеглий не повинен виконувати його, про що негайно інформує начальника, який віддав наказ, а в разі підтвердження цього наказу - письмово інформує старшого прямого начальника.

7. Віддання і виконання наказу, який суперечить закону, або невиконання правомірного наказу тягне за собою відповідальність, передбачену цим Статутом та іншими законодавчими актами.

Стаття 4. Заохочення осіб рядового і начальницького складу

1. Заохочення - важливий засіб впливу на осіб рядового і начальницького складу та зміцнення службової дисципліни, що реалізується у формі заходів матеріального і морального стимулювання, які застосовуються до осіб рядового і начальницького складу за сумлінне ставлення до своїх службових обов'язків.

2. Особи рядового і начальницького складу заохочуються за сумлінне та бездоганне виконання службових обов'язків.

Стаття 5. Дисциплінарне правопорушення

1. Дисциплінарне правопорушення - недотримання чи неналежне дотримання особою рядового або начальницького складу службової дисципліни.

Стаття 6. Відповідальність осіб рядового і начальницького складу

1. За вчинення дисциплінарних правопорушень особи рядового і начальницького складу несуть дисциплінарну відповідальність згідно з цим Статутом.

2. Особи рядового і начальницького складу, яких в установленому законодавством порядку притягнуто до адміністративної, кримінальної або матеріальної відповідальності, водночас можуть нести і дисциплінарну відповідальність згідно з цим Статутом.

Стаття 7. Облік заохочень і дисциплінарних стягнень

1. Облік заохочень і дисциплінарних стягнень, що застосовуються до осіб рядового і начальницького складу, ведуть підрозділи кадрового забезпечення спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації, підпорядкованих йому регіональних органів і територіальних підрозділів, а також закладів та установ Державної служби спеціального зв'язку та захисту інформації України.

2. Відомості про заохочення та дисциплінарні стягнення, застосовані до осіб рядового і начальницького складу, заносяться в місячний строк до особових справ цих осіб із зазначенням таких даних:

1) хто, коли та на якій підставі застосував заохочення або наклав дисциплінарне стягнення;

2) номер і дата наказу про заохочення або накладення дисциплінарного стягнення, відмітка про ознайомлення з наказом та інформація про те, чи не оскаржувався наказ про накладення дисциплінарного стягнення (а в разі оскарження - яке рішення прийнято, ким і коли);

3) номер і дата наказу про зняття дисциплінарного стягнення або відмітка про закінчення строку його дії.

Розділ II
ОБОВ'ЯЗКИ ОСІБ РЯДОВОГО І НАЧАЛЬНИЦЬКОГО СКЛАДУ ЩОДО ДОТРИМАННЯ СЛУЖБОВОЇ ДИСЦИПЛІНИ

Стаття 8. Обов'язки осіб рядового і начальницького складу

1. Службова дисципліна базується на високій свідомості та зобов'язує кожну особу рядового і начальницького складу:

дотримуватися Конституції і законів України, Присяги, що складається особами рядового і начальницького складу відповідно до закону, і наказів начальників;

дотримуватися норм професійної та службової етики;

зберігати державну таємницю;

стійко переносити всі труднощі та обмеження, пов'язані зі службою;

постійно підвищувати свій професійний рівень;

сприяти начальникам у зміцненні службової дисципліни;

виявляти повагу до колег по службі, дотримуватися правил внутрішнього розпорядку, носіння встановленої форми одягу, вітання та етикету;

з гідністю і честю поводитися в позаслужбовий час;

берегти та підтримувати в належному стані передані їй у користування майно і техніку.

2. У разі виявлення порушень законодавства, корупційного правопорушення чи одержання інформації про вчинення такого правопорушення, зловживань чи інших правопорушень у службовій діяльності особа рядового або начальницького складу повинна вжити заходів щодо припинення цих порушень та доповісти про це безпосередньому або старшому прямому начальнику.

(частина друга статті 8 із змінами, внесеними
згідно із Законом України від 17.05.2012 р. N 4711-VI)

Стаття 9. Обов'язки начальника

1. Начальник несе персональну відповідальність за стан службової дисципліни і повинен постійно її контролювати. Начальник зобов'язаний бути прикладом у дотриманні законності, службової дисципліни, бездоганному виконанні вимог Присяги, що складається особами рядового і начальницького складу відповідно до закону, наказів, у додержанні професійної та службової етики, виховувати і підтримувати у підлеглих сумлінне ставлення до виконання службових обов'язків, виявлення честі і гідності, заохочувати ініціативність, самостійність, старанність у службі, правильно застосовувати заходи дисциплінарного впливу.

2. Особливу увагу начальник повинен приділяти вивченню індивідуальних якостей підлеглих, вихованню поважного ставлення один до одного, створенню здорового морально-психологічного клімату в колективі, його згуртуванню, запобіганню порушенням службової дисципліни та виявленню причин їх учинення, формуванню нетерпимого ставлення до порушників, ураховуючи при цьому думку колективу.

3. Начальник зобов'язаний попередити про неприпустимість порушення службової дисципліни, а в разі вчинення підлеглим таких діянь - за необхідності накласти на нього дисциплінарне стягнення або порушити клопотання про накладення стягнення старшим прямим начальником.

4. Старші за званням та посадою в усіх випадках зобов'язані вимагати від молодших за званням та посадою дотримання службової дисципліни.

5. Голова Державної служби спеціального зв'язку та захисту інформації України, начальники регіональних органів, територіальних підрозділів, закладів та установ Державної служби спеціального зв'язку та захисту інформації України у разі виявлення корупційного правопорушення, вчиненого особою рядового чи начальницького складу, зобов'язані в межах своїх повноважень вжити заходів щодо припинення такого правопорушення та негайно повідомити про його вчинення спеціально уповноваженому суб'єкту у сфері протидії корупції.

(статтю 9 доповнено частиною п'ятою
згідно із Законом України від 17.05.2012 р. N 4711-VI)

Розділ III
ЗАОХОЧЕННЯ

Стаття 10. Види заохочень

1. До осіб рядового і начальницького складу можуть бути застосовані такі види заохочень:

1) дострокове зняття дисциплінарного стягнення;

2) оголошення подяки;

3) грошова винагорода;

4) нагородження цінним подарунком;

5) нагородження Почесною грамотою Державної служби спеціального зв'язку та захисту інформації України;

6) нагородження відзнаками Державної служби спеціального зв'язку та захисту інформації України;

7) дострокове присвоєння чергового спеціального звання;

8) присвоєння спеціального звання, вищого на один ступінь від звання, передбаченого займаною штатною посадою;

9) нагородження відзнакою Державної служби спеціального зв'язку та захисту інформації України "Вогнепальна зброя".

2. Відзнакою Державної служби спеціального зв'язку та захисту інформації України "Вогнепальна зброя" має право нагороджувати Голова Державної служби спеціального зв'язку та захисту інформації України осіб начальницького складу за бездоганну багаторічну службу, зміцнення національної безпеки, зразкове виконання службового обов'язку, виявлені при цьому честь і доблесть.

3. До курсантів навчальних закладів Державної служби спеціального зв'язку та захисту інформації України крім заохочень, передбачених частиною першою цієї статті, можуть також застосовуватися:

1) надання курсанту або слухачу почесного права бути сфотографованим біля розгорнутого прапора навчального закладу з подальшим врученням йому цієї фотокартки;

2) направлення батькам курсанта листа з подякою;

3) надання дозволу на позачергове звільнення з розташування навчального закладу;

4) надання короткострокової відпустки тривалістю до п'яти діб.

4. За мужність, відвагу, героїзм, особливі заслуги перед державою у службовій діяльності особи рядового і начальницького складу можуть бути представлені до присвоєння почесних звань та нагородження державними нагородами і відзнаками Президента України.

Стаття 11. Права начальників щодо застосування заохочень

1. Голова Державної служби спеціального зв'язку та захисту інформації України має право застосовувати заохочення, передбачені цим Статутом, до всіх осіб рядового і начальницького складу.

2. Заступники Голови Державної служби спеціального зв'язку та захисту інформації України, начальники регіональних органів, територіальних підрозділів, а також закладів та установ Державної служби спеціального зв'язку та захисту інформації України мають право застосовувати заохочення, передбачені пунктами 1 - 4, 7 і 8 частини першої статті 10 цього Статуту, а начальники навчальних закладів Державної служби спеціального зв'язку та захисту інформації України мають право застосовувати також заохочення, передбачені частиною третьою статті 10 цього Статуту.

3. Заохочення, передбачені пунктами 7 і 8 частини першої статті 10 цього Статуту, мають право застосовувати начальники, яким надано право присвоєння відповідних спеціальних звань.

4. Начальники структурних підрозділів спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації мають право застосовувати заохочення, передбачені пунктами 1 - 4 частини першої статті 10 цього Статуту.

5. Начальники підрозділів, що входять до складу регіональних органів, територіальних підрозділів, а також закладів та установ Державної служби спеціального зв'язку та захисту інформації України, мають право застосовувати заохочення, передбачені пунктами 1 (щодо накладених ними дисциплінарних стягнень) і 2 частини першої статті 10 цього Статуту.

6. Начальник, не наділений правом застосування заохочення, має право внести подання чи порушити клопотання про заохочення підлеглого перед старшим прямим начальником.

Стаття 12. Порядок застосування заохочень

1. Про застосування заохочення може видаватися наказ. Зміст наказу доводиться до відома особового складу Державної служби спеціального зв'язку та захисту інформації України, а також персонально до відома особи рядового або начальницького складу, яку заохочено.

2. Особа рядового або начальницького складу, яка має дисциплінарне стягнення, може заохочуватися лише шляхом дострокового зняття цього стягнення, але не раніше ніж через три місяці з дня видання наказу про накладення дисциплінарного стягнення.

3. Дострокове зняття дисциплінарного стягнення застосовується в разі, коли особа рядового або начальницького складу ставленням до служби і поведінкою доведе своє виправлення.

4. За мужність, відвагу, героїзм, особливі заслуги перед державою у службовій діяльності, тривалу бездоганну службу особи рядового і начальницького складу можуть бути

представлені до нагородження державними нагородами та відзнаками Президента України незалежно від наявності дисциплінарного стягнення.

5. Подання про присвоєння почесних звань, нагородження державними нагородами і відзнаками Президента України вносить Голова Державної служби спеціального зв'язку та захисту інформації України.

6. Порядок нагородження цінним подарунком, грошовою винагородою, Почесною грамотою, відзнаками Державної служби спеціального зв'язку та захисту інформації України, у тому числі відзнакою "Вогнепальна зброя", встановлює Голова Державної служби спеціального зв'язку та захисту інформації України.

7. Порядок дострокового присвоєння чергового спеціального звання та присвоєння спеціального звання, вищого на один ступінь від звання, передбаченого займаною штатною посадою, встановлюється Положенням про проходження служби в Державній службі спеціального зв'язку та захисту інформації України особами рядового і начальницького складу.

Розділ IV
ДИСЦИПЛІНАРНІ СТЯГНЕННЯ

Стаття 13. Види дисциплінарних стягнень

1. На осіб рядового і начальницького складу Державної служби спеціального зв'язку та захисту інформації України за порушення службової дисципліни можуть накладатися такі види дисциплінарних стягнень:

1) зауваження;

2) догана;

3) сувора догана;

4) попередження про неповну службову відповідність;

5) пониження в посаді;

6) пониження у спеціальному званні на один ступінь;

7) звільнення зі служби.

2. На курсантів навчальних закладів Державної служби спеціального зв'язку та захисту інформації України крім стягнень, передбачених частиною першою цієї статті, може накладатися стягнення у вигляді позбавлення чергового звільнення з розташування закладу.

Стаття 14. Права начальників щодо накладення дисциплінарних стягнень

1. Голова Державної служби спеціального зв'язку та захисту інформації України має право накладати дисциплінарні стягнення, передбачені цим Статутом, на всіх осіб рядового і начальницького складу.

2. Заступники Голови Державної служби спеціального зв'язку та захисту інформації України, начальники регіональних органів, територіальних підрозділів, а також закладів та установ Державної служби спеціального зв'язку та захисту інформації України мають право накладати дисциплінарні стягнення, передбачені частиною першою статті 13 цього Статуту, а начальники навчальних закладів Державної служби спеціального зв'язку та захисту інформації України мають право накладати також дисциплінарне стягнення, передбачене частиною другою статті 13 цього Статуту.

3. Дисциплінарні стягнення у вигляді звільнення зі служби, пониження в посаді, пониження у спеціальному званні на один ступінь накладаються начальниками, яким надано право відповідно прийняття на службу до Державної служби спеціального зв'язку та захисту інформації України, призначення на посаду, присвоєння спеціального звання.

4. Начальники структурних підрозділів спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації мають право накладати дисциплінарні стягнення, передбачені пунктами 1 - 4 частини першої статті 13 цього Статуту.

5. Начальники підрозділів, що входять до складу регіональних органів, територіальних підрозділів, а також закладів та установ Державної служби спеціального зв'язку та захисту інформації України, мають право накладати дисциплінарні стягнення, передбачені пунктами 1 - 3 частини першої статті 13 цього Статуту.

6. Начальник, не наділений правом накладення дисциплінарного стягнення, має право порушити перед старшим прямим начальником клопотання про притягнення особи рядового або начальницького складу до дисциплінарної відповідальності.

7. Правом накладення дисциплінарних стягнень користуються тільки прямі начальники.

8. Начальник, який перевищив надане йому право накладати дисциплінарні стягнення, несе відповідальність згідно з цим Статутом.

9. Дисциплінарне стягнення, накладене з порушенням вимог цього Статуту, скасовується начальником, який його наклав, або старшим прямим начальником.

10. Старший прямий начальник має право протягом одного місяця з дня накладення дисциплінарного стягнення посилити, а протягом року - пом'якшити чи скасувати дисциплінарне стягнення, накладене підлеглим йому начальником, якщо встановлено, що воно не відповідає тяжкості вчиненого правопорушення.

Стаття 15. Порядок накладення дисциплінарних стягнень

1. З метою з'ясування всіх обставин дисциплінарного правопорушення, вчиненого особою рядового або начальницького складу, начальник має право призначити службове розслідування, яке проводиться за участю безпосереднього начальника цієї особи протягом

одного місяця. У разі необхідності цей строк може бути продовжено начальником, який призначив службове розслідування, або старшим прямим начальником, але не більш як на один місяць.

2. Забороняється проводити службове розслідування особам, які є підлеглими порушника, а також особам - співучасникам правопорушення або заінтересованим у наслідках розслідування.

3. Порядок проведення службового розслідування встановлюється Головою Державної служби спеціального зв'язку та захисту інформації України.

4. Перед накладенням дисциплінарного стягнення начальник або особа, яка проводить службове розслідування, повинні витребувати від порушника надання письмового пояснення. У разі відмови порушника давати пояснення складається відповідний акт.

5. Про накладення дисциплінарного стягнення на порушника може видаватися наказ, зміст якого доводиться до відома особового складу Державної служби спеціального зв'язку та захисту інформації України.

6. Оголошувати дисциплінарне стягнення особі начальницького складу в присутності його підлеглих забороняється.

7. Зміст наказу доводиться до відома особи рядового або начальницького складу, яку притягнуто до дисциплінарної відповідальності, під її підпис. У разі пониження в посаді або звільнення зі служби особі рядового або начальницького складу видається витяг з наказу.

8. За кожне порушення службової дисципліни накладається лише одне дисциплінарне стягнення. У разі порушення службової дисципліни кількома особами дисциплінарне стягнення накладається на кожного окремо.

9. При визначенні виду дисциплінарного стягнення повинні враховуватися тяжкість правопорушення, обставини, за яких його вчинено, заподіяна шкода, попередня поведінка особи та визнання нею своєї вини, її ставлення до виконання службових обов'язків, рівень кваліфікації тощо.

10. У разі вчинення незначного порушення службової дисципліни начальник може обмежитись усним попередженням особи рядового або начальницького складу щодо необхідності дотримання службової дисципліни.

11. У разі притягнення до дисциплінарної відповідальності осіб рядового і начальницького складу, які мають дисциплінарне стягнення і знову допустили порушення службової дисципліни, дисциплінарне стягнення, що накладається, має бути більш суворим, ніж попереднє.

12. У разі повторного вчинення особою рядового або начальницького складу незначного правопорушення, з урахуванням його нетяжкості, сумлінного ставлення цієї особи до виконання службових обов'язків, нетривалого перебування на посаді (до шести місяців) та з інших поважних причин начальник може обмежитися раніше накладеним на таку особу дисциплінарним стягненням.

13. Дисциплінарні стягнення у вигляді пониження у спеціальному званні на один ступінь на осіб, які мають перші спеціальні звання, і пониження в посаді на осіб, які обіймають посади найнижчого рівня, не накладаються.

14. Звільнення осіб рядового і начальницького складу зі служби як вид дисциплінарного стягнення є крайнім заходом дисциплінарного впливу.

15. Застосуванню дисциплінарного стягнення у вигляді звільнення зі служби передує обов'язкове службове розслідування.

16. У разі допущення особою рядового або начальницького складу суттєвих недоліків у роботі під час виконання службових обов'язків, а також таких, що виявлені за результатами службового розслідування, може бути проведена позачергова атестація такої особи.

17. З метою виявлення причин та умов, що сприяли вчиненню корупційного правопорушення, недотримання вимог Закону України "Про засади запобігання і протидії корупції" за поданням спеціально уповноваженого суб'єкта у сфері протидії корупції за рішенням начальника особи, яка вчинила таке правопорушення, проводиться службове розслідування.

(статтю 15 доповнено частиною сімнадцятою
згідно із Законом України від 17.05.2012 р. N 4711-VI)

18. Особа рядового або начальницького складу Державної служби спеціального зв'язку та захисту інформації України, яка повідомила про порушення вимог Закону України "Про засади запобігання і протидії корупції" іншою особою рядового або начальницького складу, не може бути звільнена із служби чи змушена до звільнення або притягнута до дисциплінарної відповідальності у зв'язку з таким повідомленням. Рішення про звільнення або притягнення до дисциплінарної відповідальності оскаржується в установленому законом порядку.

(статтю 15 доповнено частиною вісімнадцятою
згідно із Законом України від 17.05.2012 р. N 4711-VI)

Стаття 16. Порядок накладення дисциплінарних стягнень в особливих випадках

1. Накладення дисциплінарних стягнень на осіб рядового і начальницького складу за правопорушення, вчинені під час чергування, несення вартової служби, здійснюється тільки після закінчення чергування, варти або після заміни їх іншими особами та здачі зброї.

2. Накладення дисциплінарного стягнення на особу, яка перебуває у стані сп'яніння, а також одержання від неї пояснень мають бути відкладені до її протверезіння.

Стаття 17. Строки накладення дисциплінарних стягнень

1. Дисциплінарне стягнення накладається у строк до одного місяця з дня, коли про правопорушення стало відомо начальнику.

2. У разі проведення за фактом вчинення правопорушення службового розслідування, провадження в кримінальній справі або справі про адміністративне правопорушення на осіб

рядового і начальницького складу дисциплінарне стягнення може бути накладено не пізніше одного місяця з дня закінчення службового розслідування, провадження в кримінальній справі чи справі про адміністративне правопорушення, не враховуючи періоду тимчасової непрацездатності або перебування у відпустці.

3. Дисциплінарне стягнення не може бути накладено, якщо з дня вчинення правопорушення минуло більше півроку. У цей період не включається строк проведення службового розслідування або провадження в кримінальній справі чи справі про адміністративне правопорушення.

Стаття 18. Відсторонення від виконання службових обов'язків

1. Особа рядового або начальницького складу, щодо якої проводиться службове розслідування, може бути відсторонена від посади із збереженням посадового окладу, окладу за спеціальне звання, надбавок за вислугу років та інших виплат і надбавок.

2. Рішення про відсторонення особи рядового або начальницького складу від посади можуть приймати начальники, яким надано право прийняття на службу або призначення цієї особи на посаду, шляхом видання письмового наказу.

3. Тривалість відсторонення від виконання службових обов'язків за посадою не повинна перевищувати часу, передбаченого для проведення службового розслідування.

4. Особа рядового або начальницького складу, стосовно якої винесено постанову про притягнення її як обвинуваченої у вчиненні злочину у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг, та/або пов'язаного із зловживанням своїм службовим становищем, підлягає відстороненню від виконання повноважень на посаді в порядку, визначеному законом, до розгляду справи судом.

(статтю 18 доповнено частиною четвертою
згідно із Законом України від 17.05.2012 р. N 4711-VI)

5. Особа рядового або начальницького складу, стосовно якої складено протокол про адміністративне корупційне правопорушення, може бути відсторонена керівником відповідного органу, підрозділу, закладу чи установи Державної служби спеціального зв'язку та захисту інформації України від виконання службових повноважень до закінчення розгляду справи судом.

(статтю 18 доповнено частиною п'ятою
згідно із Законом України від 17.05.2012 р. N 4711-VI)

Стаття 19. Виконання та зняття дисциплінарних стягнень

1. Дисциплінарне стягнення виконується негайно, але не пізніше місяця з дня його накладення, не враховуючи періоду перебування особи рядового або начальницького складу у відпустці, відрядженні або її тимчасової непрацездатності. Після закінчення цього строку дисциплінарне стягнення не виконується.

2. У разі тимчасової непрацездатності, перебування у відпустці чи відрядженні осіб рядового і начальницького складу такі дисциплінарні стягнення, як пониження в посаді та звільнення зі служби, виконуються після їх прибуття до місця проходження служби.

3. Особи, з вини яких накладені дисциплінарні стягнення не виконані без поважних причин, несуть відповідальність згідно з цим Статутом.

4. У разі подання скарги виконання накладеного дисциплінарного стягнення не припиняється.

5. Особа рядового або начальницького складу вважається такою, що не має дисциплінарного стягнення, якщо її згодом заохочено шляхом дострокового зняття дисциплінарного стягнення, нагороджено державною нагородою чи відзнакою Президента України або минув рік з дня накладення дисциплінарного стягнення.

Стаття 20. Правові наслідки накладення дисциплінарних стягнень

1. Особа рядового або начальницького складу, яка має дисциплінарне стягнення, не може бути призначена на вищу посаду.

Розділ V
ОСКАРЖЕННЯ ДИСЦИПЛІНАРНИХ СТЯГНЕНЬ

Стаття 21. Порядок оскарження дисциплінарних стягнень

1. Особа рядового або начальницького складу має право оскаржити накладене на неї дисциплінарне стягнення до старшого прямого начальника - аж до Голови Державної служби спеціального зв'язку та захисту інформації України або до суду.

2. Дисциплінарне стягнення може бути оскаржено до старшого прямого начальника протягом трьох місяців з дня ознайомлення з наказом особи, на яку воно накладено.

3. Якщо вирішення питань, порушених у скарзі, не належить до повноважень начальника, який її отримав, скарга не пізніше п'яти днів надсилається за належністю, про що повідомляється заявникові.

4. Забороняється пересилати на розгляд скарги тим начальникам, дії чи рішення яких оскаржуються.

5. Пропущений строк для подання скарги може бути поновлено старшим прямим начальником, який має право накладати дисциплінарні стягнення.

6. Старший прямий начальник у разі надходження заяви про поновлення пропущеного строку подання скарги повинен всебічно та об'єктивно розглянути її та прийняти відповідне рішення не пізніше 10 днів після надходження заяви.

7. Про результати розгляду заяви про поновлення пропущеного строку повідомляються особа рядового або начальницького складу, яка її подала, та начальник, який наклав на неї дисциплінарне стягнення.

УКАЗ
Президента України

Про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України

Із змінами і доповненнями, внесеними
Указом Президента України
від 13 червня 2012 року N 391/2012

1. Затвердити Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України (додається).

2. Установити, що Адміністрація Державної служби спеціального зв'язку та захисту інформації України є правонаступником Державної служби зв'язку України і Державної адміністрації зв'язку - урядового органу, що діяв у складі Міністерства транспорту та зв'язку України (крім прав та обов'язків, пов'язаних із реалізацією функцій у сфері надання послуг поштового зв'язку загального користування).

(стаття 2 із змінами, внесеними згідно з Указом
Президента України від 13.06.2012 р. N 391/2012)

3. Внести до Схеми організації та взаємодії центральних органів виконавчої влади, затвердженої Указом Президента України від 9 грудня 2010 року N 1085 "Про оптимізацію системи центральних органів виконавчої влади" (зі змінами, внесеними Указом від 6 квітня 2011 року N 370), такі зміни:

1) абзац "Адміністрація Державної служби спеціального зв'язку та захисту інформації України" розділу II виключити;

2) розділ III доповнити абзацом такого змісту:

"Адміністрація Державної служби спеціального зв'язку та захисту інформації України".

4. Кабінету Міністрів України у двомісячний строк:

1) забезпечити фінансування виконання покладених на Адміністрацію Державної служби спеціального зв'язку та захисту інформації України функцій;

2) вирішити питання щодо передачі в управління Адміністрації Державної служби спеціального зв'язку та захисту інформації України для виконання покладених на неї функцій об'єктів державної власності.

5. Адміністрації Державної служби спеціального зв'язку та захисту інформації України подати у двомісячний строк у встановленому порядку пропозиції щодо внесення до актів законодавства змін, що випливають із цього Указу.

6. Цей Указ набирає чинності з дня його опублікування.

Президент України **В. ЯНУКОВИЧ**

м. Київ
30 червня 2011 року
N 717/2011

ЗАТВЕРДЖЕНО
Указом Президента України
від 30 червня 2011 року N 717/2011

ПОЛОЖЕННЯ
про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України

1. Адміністрація Державної служби спеціального зв'язку та захисту інформації України (далі - Адміністрація) є центральним органом виконавчої влади у складі Державної служби спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку України).

Адміністрація є центральним органом виконавчої влади зі спеціальним статусом, головним органом у системі центральних органів виконавчої влади з формування і забезпечення реалізації державної політики у сферах організації спеціального зв'язку та захисту інформації, телекомунікацій, користування радіочастотним ресурсом України.

(абзац другий пункту 1 із змінами, внесеними згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

Адміністрація є центральним органом виконавчої влади в галузі зв'язку, спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації.

2. Адміністрація у своїй діяльності керується Конституцією та законами України, актами Президента України, Кабінету Міністрів України, іншими актами законодавства України, а також дорученнями Президента України.

3. Основними завданнями Адміністрації є:

1) забезпечення формування і реалізації державної політики у сферах захисту державних інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем (далі -

інформаційно-телекомунікаційні системи), криптографічного та технічного захисту інформації, використання і захисту державних електронних інформаційних ресурсів, телекомунікацій, користування радіочастотним ресурсом України; участь у формуванні і реалізації державної політики у сфері електронного документообігу органів державної влади та органів місцевого самоврядування, розробленні та впровадженні електронного цифрового підпису в органах державної влади та органах місцевого самоврядування;

(підпункт 1 пункту 3 із змінами, внесеними згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

2) участь у межах своїх повноважень у формуванні і реалізації державної тарифної політики та політики державних закупівель у сферах телекомунікацій, користування радіочастотним ресурсом України;

(підпункт 2 пункту 3 із змінами, внесеними згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

3) забезпечення в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб органів державної влади, місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації;

4) забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;

5) визначення вимог і порядку створення та розвитку систем технічного та криптографічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

6) здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, протидії технічним розвідкам, а також за додержанням технічних вимог керівних документів у сфері надання послуг електронного цифрового підпису;

7) охорона об'єктів та майна Держспецзв'язку України, у тому числі приміщень, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації тощо;

8) розроблення та здійснення заходів щодо розвитку телекомунікаційних мереж, поліпшення їх якості, забезпечення доступності і сталого функціонування;

(підпункт 8 пункту 3 із змінами, внесеними згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

9) сприяння інтеграції сфер телекомунікацій, користування радіочастотним ресурсом України у світовий інформаційно-комунікаційний простір.

(підпункт 9 пункту 3 із змінами, внесеними згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

4. Адміністрація відповідно до покладених на неї завдань:

1) забезпечує надійне функціонування, безпеку та розвиток державної системи урядового зв'язку, зокрема її готовності до роботи в особливий період та в разі виникнення надзвичайної ситуації;

2) здійснює функції щодо забезпечення в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб органів державної влади, місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації;

3) здійснює контроль за виконанням технічних умов у приміщеннях абонентів урядового зв'язку;

4) визначає порядок:

надання операторами телекомунікацій ресурсів своїх мереж у користування державній системі урядового зв'язку, Національній системі конфіденційного зв'язку, органам з надзвичайних ситуацій, безпеки, оборони, внутрішніх справ;

взаємодії операторів телекомунікацій з Національним центром оперативно-технічного управління телекомунікаційними мережами;

5) вирішує в межах компетенції питання щодо забезпечення зв'язку для потреб державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, органів безпеки, оборони, охорони правопорядку;

6) організовує участь Держспецзв'язку України у виконанні завдань територіальної оборони, а також у заходах, спрямованих на підтримання правового режиму воєнного та надзвичайного стану відповідно до закону;

7) бере участь у формуванні і відповідає за реалізацію державної політики у сферах захисту державних інформаційно-телекомунікаційних систем, криптографічного та технічного захисту інформації, створення, використання і захисту державних електронних інформаційних ресурсів, забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, телекомунікацій, користування радіочастотним ресурсом України; бере участь у формуванні і реалізації державної політики у сфері електронного документообігу органів державної влади та органів місцевого самоврядування, розробленні і впровадженні електронного цифрового підпису в органах державної влади та органах місцевого самоврядування;

(підпункт 7 пункту 4 із змінами, внесеними згідно з
Указом Президента України від 13.06.2012 р. N 391/2012)

8) визначає перспективні напрями, розробляє та здійснює інші заходи щодо розвитку систем криптографічного та технічного захисту інформації, а також у сферах телекомунікацій, користування радіочастотним ресурсом України;

(підпункт 8 пункту 4 із змінами, внесеними згідно з
Указом Президента України від 13.06.2012 р. N 391/2012)

9) розробляє в порядку, встановленому законодавством, проекти Концепції розвитку телекомунікацій України, інших концепцій у сферах користування радіочастотним ресурсом України, сприяє їх реалізації;

(підпункт 9 пункту 4 із змінами, внесеними згідно з
Указом Президента України від 13.06.2012 р. N 391/2012)

10) забезпечує нормативно-правове регулювання у сферах організації спеціального зв'язку та захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, розробляє пропозиції щодо вдосконалення законодавчих актів, актів Президента України, Кабінету Міністрів України та в установленому порядку вносить їх на розгляд Президентові України, Кабінету Міністрів України;

(підпункт 10 пункту 4 із змінами, внесеними згідно з
Указом Президента України від 13.06.2012 р. N 391/2012)

11) здійснює технічне регулювання у сферах захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації, організовує та проводить оцінку відповідності, розробляє в установленому порядку стандарти, технічні регламенти і технічні умови;

12) здійснює методичне керівництво та координацію діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності у сферах криптографічного та технічного захисту інформації, протидії технічним розвідкам, а також з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційно-телекомунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

13) розробляє та супроводжує моделі технічних розвідок шляхом збору та аналізу інформації про існуючі системи і засоби технічних розвідок, тактику та методи їх застосування, а також перспективи розвитку; надає рекомендації органам державної влади, органам місцевого самоврядування, військовим формуванням, підприємствам, установам і організаціям щодо забезпечення протидії технічним розвідкам, проведення оцінки загроз та вжиття відповідних заходів для захисту інформації;

14) визначає порядок ведення, веде та здійснює управління реєстром інформаційно-телекомунікаційних систем органів державної влади, а також підприємств, установ і організацій, що належать до сфери їх управління, депозитарієм державних електронних інформаційних ресурсів, визначає порядок ведення Національного реєстру електронних інформаційних ресурсів органів державної влади;

15) розробляє та затверджує порядок і вимоги щодо захисту державних інформаційних ресурсів, у тому числі систем електронного документообігу, в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

16) розробляє критерії та порядок оцінювання стану захищеності державних інформаційних ресурсів, незалежно від виду та змісту інформації, яка утворює такий інформаційний ресурс, в інформаційно-телекомунікаційних системах, організовує та здійснює оцінювання стану їх захищеності, надає відповідні рекомендації;

17) встановлює порядок здійснення державного контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису, а також здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, за станом протидії технічним розвідкам щодо озброєння, військової та спеціальної техніки, об'єктів оборонно-промислового комплексу, військових об'єктів та об'єктів, призначених для застосування в інтересах оборони і безпеки держави, а також під час провадження діяльності на території України іноземних інспекційних груп відповідно до міжнародних договорів України;

18) здійснює державний контроль за додержанням вимог законодавства, а також технічних вимог нормативних документів у сфері надання послуг електронного цифрового підпису;

19) затверджує технічні і технологічні вимоги до акредитованих центрів сертифікації ключів;

20) організовує та координує разом із центральним органом виконавчої влади у сфері стандартизації, метрології та сертифікації роботи з проведення сертифікації засобів криптографічного та технічного захисту інформації, організовує і проводить державну експертизу у сфері криптографічного та технічного захисту інформації;

21) накопичує та аналізує дані про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також про їх наслідки, інформує правоохоронні органи для вжиття заходів із запобігання та припинення злочинів у зазначеній сфері;

22) видає атестат відповідності комплексних систем захисту інформації інформаційно-телекомунікаційних систем, із застосуванням яких обробляється інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, вимогам нормативних документів з питань технічного захисту інформації;

23) розробляє та затверджує єдині технічні вимоги щодо створення та захисту Єдиного веб-порталу державних органів, здійснює контроль за дотриманням цих вимог;

24) погоджує проекти створення та розвитку інформаційно-телекомунікаційних систем, в яких оброблятиметься інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, державних електронних інформаційних ресурсів, систем електронного документообігу та електронного цифрового підпису (в частині захисту інформації), організовує проведення їх експертної оцінки і визначає можливості введення в експлуатацію;

25) здійснює державний контроль за додержанням вимог безпеки у процесі розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, проведення тематичних досліджень, експертизи, ввезення, вивезення та знищення криптографічних систем і засобів криптографічного захисту інформації та обладнання спеціального зв'язку;

26) визначає порядок погодження та погоджує міжнародні передачі криптографічних систем, засобів криптографічного та технічного захисту інформації, зокрема тих, що є складовими частинами озброєння, військової та спеціальної техніки, а також порядок надання відповідних висновків;

27) визначає переліки технічних засобів загального призначення, дозволених для забезпечення технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

28) видає та реєструє відповідно до вимог законодавства ліцензії на провадження господарської діяльності з надання послуг у галузі криптографічного та технічного захисту інформації (крім послуг електронного цифрового підпису), торгівлі криптосистемами і засобами криптографічного захисту інформації (згідно з переліком, що визначається Кабінетом Міністрів України);

29) встановлює порядок видачі та видає дозволи органам державної влади на проведення робіт з технічного захисту інформації для власних потреб, а також здійснює контроль за додержанням ліцензійних умов та умов проведення робіт для власних потреб;

30) організовує розроблення, виготовлення, постачання ключових документів до засобів криптографічного захисту інформації, що містить державну таємницю, та конфіденційної інформації, що є власністю держави;

31) здійснює погодження технічних завдань на проектування, будівництво і реконструкцію особливо важливих об'єктів, розроблення зразків військової та спеціальної техніки, у процесі експлуатації або застосування яких збирається, обробляється, зберігається, передається чи приймається інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, незалежно від виду та змісту такої інформації, здійснює контроль за їх дотриманням;

32) вирішує в межах своєї компетенції питання готовності до функціонування телекомунікаційних мереж загального користування у разі виникнення надзвичайної ситуації, в умовах надзвичайного та воєнного стану, в особливий період, забезпечує переведення мереж зв'язку в особливий період на відповідний режим роботи;

(підпункт 32 пункту 4 у редакції Указу
Президента України від 13.06.2012 р. N 391/2012)

33) здійснює формування та реалізацію державної технічної політики в галузі зв'язку, а саме:

розробляє відповідно до законодавства технічні регламенти, норми, стандарти, методики розрахунків електромагнітної сумісності радіоелектронних засобів та випромінювальних пристроїв, інші нормативні документи у сферах телекомунікацій та користування радіочастотним ресурсом України;

(абзац другий підпункту 33 пункту 4 із змінами, внесеними згідно з
Указом Президента України від 13.06.2012 р. N 391/2012)

здійснює організацію робіт, пов'язаних зі стандартизацією та сертифікацією засобів телекомунікацій;

(абзац третій підпункту 33 пункту 4 із змінами, внесеними згідно з
Указом Президента України від 13.06.2012 р. N 391/2012)

установлює технічні вимоги до телекомунікаційних мереж, засобів та об'єктів телекомунікацій;

визначає перелік технічних засобів, які можуть застосовуватися в телекомунікаційних мережах загального користування, та погоджує в установленому законодавством порядку питання застосування технічних засобів телекомунікацій, не внесених до цього переліку;

організовує відповідно до законодавства роботи з підтвердження відповідності технічних засобів телекомунікацій, призначених для застосування в телекомунікаційних мережах загального користування;

бере участь у створенні державних стандартів щодо користування радіочастотним ресурсом України;

установлює норми, правила і порядки проведення випробувань у сфері користування радіочастотним ресурсом України;

абзац дев'ятий підпункту 33 пункту 4 виключено

(згідно з Указом Президента
України від 13.06.2012 р. N 391/2012)

подає пропозиції щодо призначення органів з оцінки відповідності, що здійснюють діяльність у сферах телекомунікацій, використання радіочастотного ресурсу;

(абзац десятий підпункту 33 пункту 4 із змінами, внесеними
згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

здійснює в межах компетенції заходи із метрологічного забезпечення;

установлює порядок використання лічильників обліку тривалості телекомунікаційних послуг (встановлюються на кінцевому обладнанні);

розробляє та реалізовує технічну політику у формуванні номерного ресурсу, зміни його структури та простору нумерації в інтересах розширення і забезпечення достатньої ємності номерного ресурсу та приведення його у відповідність із міжнародними вимогами;

абзац чотирнадцятий підпункту 33 пункту 4 виключено

(згідно з Указом Президента
України від 13.06.2012 р. N 391/2012)

визначає порядок і забезпечує проведення експертизи телекомунікаційної інфраструктури проектів будівництва, реконструкції та модернізації телекомунікаційних мереж, споруд і засобів телекомунікацій;

(абзац п'ятнадцятий підпункту 33 пункту 4 із змінами, внесеними
згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

34) визначає у порядку, встановленому законодавством, необхідний і достатній для потреб України радіочастотний ресурс, здійснює відповідно до норм міжнародного права заходи щодо його закріплення за Україною і захисту на міжнародному рівні;

35) розробляє у порядку, встановленому законодавством, Національну таблицю розподілу смуг радіочастот України і План використання радіочастотного ресурсу України та подає ці документи на затвердження Кабінету Міністрів України;

36) забезпечує в межах своєї компетенції формування і реалізацію інноваційної та інвестиційної політики;

37) розробляє вимоги щодо надання і отримання телекомунікаційних послуг;

(підпункт 37 пункту 4 із змінами, внесеними згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

38) здійснює відповідно до законодавства повноваження щодо регулювання цін (тарифів) у галузі зв'язку;

39) здійснює державне регулювання у сфері фельд'єгерського і спеціального поштового зв'язку;

40) підпункт 40 пункту 4 виключено

(згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

41) підпункт 41 пункту 4 виключено

(згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

42) підпункт 42 пункту 4 виключено

(згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

43) підпункт 43 пункту 4 виключено

(згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

44) здійснює відповідно до законодавства заходи щодо реалізації науково-технічної політики, організовує наукове забезпечення функціонування і розвитку сфер спеціального зв'язку та захисту інформації, телекомунікацій, користування радіочастотним ресурсом України;

(підпункт 44 пункту 4 із змінами, внесеними згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

45) бере участь у реалізації державного замовлення на виконання робіт і поставок продукції для державних потреб, сприяє залученню інвестицій, новітніх технологій, використанню управлінського досвіду у сферах спеціального зв'язку та захисту інформації, телекомунікацій, користування радіочастотним ресурсом України;

(підпункт 45 пункту 4 із змінами, внесеними згідно з Указом Президента України від 13.06.2012 р. N 391/2012)

46) погоджує технічні характеристики (вимоги), що вносяться до документації конкурсних торгів, при закупівлі товарів і послуг у межах виконання Законів України "Про здійснення державних закупівель", "Про Національну програму інформатизації", "Про електронний цифровий підпис", "Про електронні документи та електронний документообіг", "Про захист інформації в інформаційно-телекомунікаційних системах";

47) бере у межах своїх повноважень участь у погодженні питань щодо розміщення на території України дипломатичних представництв і консульських установ іноземних держав;

48) відповідно до законодавства України виконує функції Адміністрації зв'язку та радіочастот України, здійснює правовий захист інтересів України у міжнародних і регіональних організаціях з питань телекомунікацій, користування радіочастотним ресурсом України;

(підпункт 48 пункту 4 із змінами, внесеними згідно з
Указом Президента України від 13.06.2012 р. N 391/2012)

49) вживає заходів для здійснення галузевого співробітництва з іншими державами;

50) готує пропозиції щодо адаптації законодавства України до законодавства Європейського Союзу з питань функціонування сфер телекомунікацій, користування радіочастотним ресурсом, здійснює відповідні заходи щодо інтеграції України в європейські структури;

(підпункт 50 пункту 4 із змінами, внесеними згідно з
Указом Президента України від 13.06.2012 р. N 391/2012)

51) бере відповідно до законодавства участь у підготовці міжнародних договорів України з питань, що належать до компетенції Адміністрації; готує у межах компетенції пропозиції щодо укладення, денонсації таких договорів та забезпечує їх виконання;

52) здійснює міжнародну координацію і методичне забезпечення реалізації заходів щодо формування та використання різних типів номерного ресурсу для телекомунікаційних мереж, у тому числі для телекомунікаційних мереж наступного покоління;

53) розробляє прогнози розвитку телекомунікаційних мереж і послуг, сфери користування радіочастотним ресурсом України;

(підпункт 53 пункту 4 із змінами, внесеними згідно з
Указом Президента України від 13.06.2012 р. N 391/2012)

54) визначає порядок організації служби з охорони об'єктів, приміщень, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації та вживає заходів для її забезпечення;

55) визначає порядок придбання, перевезення, носіння та використання вогнепальної зброї, боєприпасів до неї, інших предметів і матеріалів, на які поширюється дозвільна система, а також особливості використання і застосування зброї особами рядового і начальницького складу під час охорони об'єктів і майна Держспецзв'язку України на підставах та в порядку, передбачених статтями 15, 15-1 Закону України "Про міліцію" та статтями 195 - 202 Статуту гарнізонної та вартової служб Збройних Сил України;

56) визначає порядок чергування особового складу Держспецзв'язку України, а також несення ним служби (виконання роботи) у підземних спорудах зв'язку та вахтовим методом у зоні відчуження;

57) затверджує порядок оформлення і складання уповноваженими посадовими особами Держспецзв'язку України протоколів про адміністративні правопорушення;

58) розробляє та організовує виконання державних цільових, наукових і науково-технічних програм за напрямами діяльності Держспецзв'язку України;

59) у межах компетенції виступає державним замовником з оборонного замовлення та замовником закупівлі товарів, робіт і послуг за державні кошти;

60) здійснює контроль якості та приймання продукції, інших товарів військового призначення, які виготовляються (модернізуються) на замовлення Держспецзв'язку України;

61) організовує та здійснює разом із центральним органом виконавчої влади у галузі освіти і науки науково-методичне управління підготовкою кадрів у сфері криптографічного та технічного захисту інформації, телекомунікацій, радіотехнологій та радіочастотного ресурсу;

(підпункт 61 пункту 4 із змінами, внесеними згідно з
Указом Президента України від 13.06.2012 р. N 391/2012)

62) організовує підготовку, перепідготовку та підвищення кваліфікації особового складу Держспецзв'язку України, виконує функції державного замовника на підготовку кадрів у вищих навчальних закладах;

63) виконує відповідно до законодавства функції з управління об'єктами державної власності, у тому числі державними корпоративними правами;

64) приймає рішення про подальше використання державного майна, що не ввійшло до статутних капіталів господарських товариств, створених у процесі корпоратизації;

65) веде облік об'єктів державної власності, що перебувають в управлінні Держспецзв'язку України, здійснює контроль за їх ефективним використанням та збереженням;

66) приймає у випадках, передбачених законодавством, рішення про передачу об'єктів державної власності в комунальну власність, до сфери управління інших органів, уповноважених управляти об'єктами державної власності, передачу об'єктів державної власності від одного підприємства до іншого;

67) забезпечує в межах своїх повноважень виконання заходів з охорони праці та пожежної безпеки в Держспецзв'язку України;

68) забезпечує в межах своїх повноважень реалізацію державної політики у сфері охорони державної таємниці, здійснює контроль за її збереженням у структурних підрозділах Адміністрації, підпорядкованих органах та на підприємствах, що належать до сфери її управління;

69) виступає замовником будівництва житла та інших об'єктів Держспецзв'язку України, вживає заходів щодо їх експлуатації, реконструкції та ремонту;

70) підпункт 70 пункту 4 виключено

(згідно з Указом Президента
України від 13.06.2012 р. N 391/2012)

71) організовує в установленому порядку виставки засобів і систем зв'язку в Україні і за її межами, координує участь у таких виставках органів виконавчої влади та органів місцевого самоврядування, підприємств, установ та організацій;

72) провадить в установленому порядку видавничу діяльність, висвітлює діяльність Держспецзв'язку України у засобах масової інформації та на власному веб-сайті;

73) готує пропозиції щодо обсягів і напрямів державних капітальних вкладень у галузь зв'язку;

74) забезпечує відповідно до законодавства правовий і соціальний захист осіб рядового і начальницького складу, державних службовців та інших працівників Держспецзв'язку України і членів їх сімей;

75) погоджує в порядку, встановленому законодавством, призначення керівників органів спеціального зв'язку, підрозділів з питань зв'язку, інформатизації та захисту інформації органів державної влади, Національного банку України та Генеральної прокуратури України;

76) утворює лікарсько-експертну комісію для проведення військово-лікарської експертизи і медичного огляду та визначає порядок її діяльності;

77) здійснює інші повноваження, визначені законами України та покладені на неї Президентом України.

5. Адміністрація з метою організації своєї діяльності:

1) забезпечує в межах повноважень здійснення заходів щодо запобігання корупції і контроль за їх здійсненням в Адміністрації, підпорядкованих органах, установах та на підприємствах, що належать до сфери її управління;

2) здійснює добір кадрів в Адміністрацію, на керівні посади на підприємствах, в установах та організаціях (закладах), що належать до сфери її управління, формує кадровий резерв на відповідні посади, організовує роботу з підготовки, перепідготовки та підвищення кваліфікації особового складу Держспецзв'язку України;

3) організовує планово-фінансову роботу в Адміністрації, підпорядкованих органах, на підприємствах, що належать до сфери її управління, здійснює контроль за використанням фінансових і матеріальних ресурсів, забезпечує організацію та вдосконалення бухгалтерського обліку;

4) забезпечує ефективне, результативне і цільове використання бюджетних коштів;

5) здійснює у межах повноважень разом з відповідними центральними органами виконавчої влади контроль за цільовим використанням державних коштів, передбачених для реалізації проектів, виконання програм, у тому числі міжнародних;

6) забезпечує у межах повноважень реалізацію державної політики стосовно державної таємниці, контроль за її збереженням в Адміністрації, підпорядкованих органах та на підприємствах, що належать до сфери її управління;

7) забезпечує в межах повноважень виконання завдань з мобілізаційної підготовки та мобілізаційної готовності держави;

8) організовує роботу з укомплектування, зберігання, обліку та використання архівних документів;

9) утворює, реорганізовує, ліквідовує відповідно до законодавства у межах загальної структури, чисельності особового складу Держспецзв'язку України і виділених коштів регіональні органи Адміністрації, установи, організації (заклади) та територіальні підрозділи, які входять до структури Держспецзв'язку України (далі - підпорядковані органи), затверджує їх положення (статути), а також здійснює управління ними, організовує матеріальне та інше забезпечення;

10) здійснює внутрішній контроль та аудит у підпорядкованих органах, у тому числі контроль за фінансово-господарською діяльністю підприємств, що належать до сфери управління Адміністрації, та господарських товариств, щодо яких Адміністрація здійснює управління корпоративними правами держави;

11) веде облік об'єктів державної власності, що перебувають у сфері управління Адміністрації, здійснює контроль за їх ефективним використанням та збереженням;

12) приймає рішення про подальше використання державного майна, що не увійшло до статутних капіталів господарських товариств, створених у процесі корпоратизації;

13) приймає у випадках, передбачених законодавством, рішення про передачу об'єктів державної власності в комунальну власність, до сфери управління інших органів, уповноважених управляти об'єктами державної власності, передачу об'єктів державної власності від одного підприємства до іншого.

6. Адміністрація має право:

1) одержувати в установленому порядку від органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності інформацію, документи і матеріали, необхідні для виконання покладених на Держспецзв'язку України завдань;

2) залучати фахівців органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності за погодженням з їх керівниками до розгляду питань, що належать до компетенції Держспецзв'язку України, а також до проведення спільних інспекційних перевірок;

3) доступу в установленому порядку своїх уповноважених представників на об'єкти органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності, на яких знаходяться засоби спеціального зв'язку Держспецзв'язку України, а також на об'єкти, щодо яких здійснюється державний контроль за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

4) надавати на договірних засадах у встановленому порядку допомогу підприємствам, установам і організаціям незалежно від форми власності у розробленні та здійсненні заходів із захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах, із криптографічного та технічного захисту інформації;

5) проводити планові та позапланові перевірки додержання ліцензійних умов провадження господарської діяльності з надання послуг у галузі криптографічного та технічного захисту інформації на підприємствах, в установах і організаціях, а також умов проведення робіт із технічного захисту інформації для власних потреб в органах державної влади;

6) проводити планові та позапланові перевірки центрального засвідчувального органу, засвідчувальних центрів і центрів сертифікації ключів щодо додержання ними вимог законодавства у сфері надання послуг електронного цифрового підпису;

7) проводити планові та позапланові інспекційні перевірки стану криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в органах державної влади, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форми власності, у тому числі в закордонних дипломатичних установах України, без одержання доступу до змісту інформації;

8) зупиняти дію або скасовувати в установленому порядку атестати відповідності комплексних систем захисту інформації в інформаційно-телекомунікаційних системах та актів атестації комплексів технічного захисту інформації на об'єктах інформаційної діяльності, експертні висновки на допуск до експлуатації та свідоцтва про допуск до експлуатації засобів криптографічного захисту інформації, які призначені для захисту інформації з обмеженим доступом та криптографічних алгоритмів, а також дозволи органам державної влади на проведення робіт з технічного захисту інформації для власних потреб;

9) порушувати в установленому порядку питання:

про припинення інформаційної діяльності з використанням інформаційно-телекомунікаційних систем в органах державної влади, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форми власності, у тому числі в закордонних дипломатичних установах України та місцях постійного і тимчасового перебування вищих посадових осіб держави, у разі порушення ними вимог законодавства у сфері захисту державних інформаційних ресурсів, криптографічного та/або технічного захисту інформації;

про зупинення дії або скасування спеціальних дозволів на провадження діяльності, пов'язаної з державною таємницею, у разі виявлення порушень у сфері криптографічного та технічного захисту інформації;

10) залучати спеціальних і загальних користувачів радіочастотного ресурсу до виявлення та усунення радіозавад радіоелектронним засобам державної системи урядового зв'язку та Національної системи конфіденційного зв'язку;

11) організовувати і проводити науково-дослідні, дослідно-конструкторські, технологічні та проектні роботи;

12) виступати державним замовником з оборонного замовлення та замовником закупівлі товарів, робіт і послуг за державні кошти;

13) виступати замовником будівництва об'єктів Держспецзв'язку України;

14) утворювати координаційні, консультативні і дорадчі органи;

15) провадити в установленому порядку видавничу діяльність;

16) скликати наради, проводити наукові та науково-практичні конференції (у тому числі міжнародні), семінари з питань, що належать до компетенції Держспецзв'язку України;

17) здійснювати у порядку, передбаченому законодавством, господарську діяльність, що безпосередньо пов'язана із забезпеченням виконання покладених на Держспецзв'язку України завдань, за видами, перелік яких визначається Кабінетом Міністрів України;

18) відчужувати в установленому порядку закріплене за Держспецзв'язку України державне майно;

19) здійснювати міжнародне співробітництво, розробляти пропозиції щодо укладення відповідних міжнародних договорів України, взаємодіяти відповідно до міжнародних договорів України з міжнародними організаціями з питань, що належать до компетенції Держспецзв'язку України;

20) звертатися до суду в разі виникнення спорів з питань організації спеціального зв'язку та захисту інформації, криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, спорів у сфері надання послуг електронного цифрового підпису, а також у разі виникнення інших спорів у порядку, встановленому законом;

21) одержувати і використовувати в установленому порядку земельні ділянки з метою розміщення адміністративних і господарських будівель, стаціонарних технічних засобів та інженерних споруд, об'єктів житлового будівництва, інших об'єктів, необхідних для функціонування Адміністрації та підпорядкованих їй органів;

22) орендувати в установленому порядку приміщення, майно, а також ресурси телекомунікаційних мереж для забезпечення потреб державної системи урядового зв'язку і Національної системи конфіденційного зв'язку.

Уповноважені посадові особи Держспецзв'язку України мають право в установленому порядку складати протоколи про адміністративні правопорушення.

Уповноважені представники Держспецзв'язку України мають право ознайомлюватися в установленому порядку з усіма документами, необхідними для проведення перевірок стану криптографічного, технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, протидії технічним розвідкам, дотримання умов проведення робіт з технічного захисту інформації для власних потреб, додержання ліцензійних умов провадження господарської діяльності з надання послуг у галузі криптографічного та технічного захисту інформації, а також додержання вимог законодавства у сфері надання послуг електронного цифрового підпису.

7. Адміністрація у процесі виконання покладених на неї завдань взаємодіє в установленому порядку з іншими органами виконавчої влади, допоміжними органами і службами, утвореними Президентом України, органами місцевого самоврядування, військовими

формуваннями, відповідними органами іноземних держав і міжнародних організацій, а також підприємствами, установами, організаціями.

8. Адміністрація в межах своїх повноважень, на основі і на виконання Конституції та законів України, актів і доручень Президента України, актів Кабінету Міністрів України видає накази, які підписує, організовує та контролює виконання Голова Держспецзв'язку України.

Накази Адміністрації, видані у межах її повноважень, є обов'язковими до виконання центральними органами виконавчої влади, їх територіальними органами, місцевими державними адміністраціями, органами влади Автономної Республіки Крим, органами місцевого самоврядування, підприємствами, установами і організаціями всіх форм власності та громадянами.

Накази Адміністрації, які відповідно до закону є регуляторними актами, розробляються, розглядаються, видаються та оприлюднюються з урахуванням вимог Закону України "Про засади державної регуляторної політики у сфері господарської діяльності".

Нормативно-правові акти Адміністрації підлягають державній реєстрації в установленому законодавством порядку.

Адміністрація видає у разі потреби разом з іншими центральними та місцевими органами виконавчої влади спільні нормативно-правові акти.

9. Адміністрація здійснює свої повноваження безпосередньо та через утворені в установленому порядку регіональні органи в Автономній Республіці Крим, областях, містах Києві, Севастополі, Ялті.

10. Адміністрацію очолює Голова Держспецзв'язку України.

Голову Держспецзв'язку України призначає на посаду за поданням Прем'єр-міністра України та звільняє з посади Президент України.

Голова Держспецзв'язку України має першого заступника та заступника Голови, які призначаються на посади за поданням Прем'єр-міністра України, внесеним на підставі пропозицій Голови Держспецзв'язку України, та звільняються з посад Президентом України.

За необхідності для забезпечення здійснення Держспецзв'язку України окремих завдань за рішенням Президента України вводиться посада заступника Голови Держспецзв'язку України.

11. Голова Держспецзв'язку України:

1) здійснює загальне керівництво діяльністю Адміністрації та підпорядкованих органів, представляє Адміністрацію у відносинах з іншими органами, підприємствами, установами, організаціями;

2) несе особисту відповідальність за виконання покладених на Держспецзв'язку України завдань;

3) забезпечує виконання Держспецзв'язку України та Адміністрацією законів України, актів та доручень Президента України, актів Кабінету Міністрів України;

4) інформує Президента України з основних питань діяльності Держспецзв'язку України, Верховну Раду України - з питань виконання покладених на неї завдань, додержання законодавства, прав і свобод людини та громадянина і з інших питань, а також щороку подає Президентові України, Верховній Раді України та Кабінету Міністрів України звіт про свою діяльність;

5) погоджує проекти законів, актів Президента України, Кабінету Міністрів України з питань, що належать до компетенції Держспецзв'язку України;

6) подає на розгляд Кабінету Міністрів України проекти законів, актів Президента України, Кабінету Міністрів України, розробником яких є Адміністрація;

7) вносить пропозиції Прем'єр-міністру України щодо кандидатур на посади своїх заступників;

8) розподіляє обов'язки між своїми заступниками, визначає ступінь їх відповідальності, а також ступінь відповідальності керівників структурних підрозділів Адміністрації та підпорядкованих органів;

9) в установленому порядку призначає на посади та звільняє з посад керівників структурних підрозділів Адміністрації, підпорядкованих органів та підприємств, що належать до сфери її управління;

10) затверджує положення (статути) про структурні підрозділи Адміністрації, підпорядковані органи та підприємства, що належать до сфери її управління;

11) затверджує структуру і штати територіальних підрозділів Держспецзв'язку України;

12) затверджує граничні спеціальні звання за посадами до полковника Держспецзв'язку України включно, а також порядок заміщення окремих посад осіб рядового і начальницького складу державними службовцями та іншими працівниками Держспецзв'язку України;

13) присвоює в установленому законодавством порядку спеціальні звання від рядового до полковника Держспецзв'язку України включно і вносить подання Президентові України про присвоєння особам начальницького складу спеціальних звань (генерал-майор, генерал-лейтенант) Держспецзв'язку України;

14) подає осіб рядового і начальницького складу, державних службовців та інших працівників Держспецзв'язку України до нагородження державними нагородами, відзнаками Президента України;

15) установлює заохочувальні відзнаки і порядок нагородження ними;

16) підписує накази Адміністрації та видає накази про особовий склад Держспецзв'язку України;

17) затверджує програми і плани роботи структурних підрозділів Адміністрації та підпорядкованих органів, розглядає і затверджує звіти про їх виконання;

18) здійснює інші повноваження, передбачені законодавством.

12. Для погодженого вирішення питань, що належать до компетенції Адміністрації, обговорення найважливіших напрямів її діяльності в Адміністрації утворюється колегія у складі Голови Держспецзв'язку України, його заступників, керівників структурних підрозділів Адміністрації, а також представників органів державної влади, установ, громадських організацій, вчених та інших осіб за їх згодою.

Колегія Адміністрації є постійно діючим консультативно-дорадчим органом. Періодичність проведення засідань колегії визначається Головою Держспецзв'язку України.

Для розгляду наукових рекомендацій та проведення фахових консультацій з основних питань діяльності в Адміністрації можуть утворюватись інші постійні або тимчасові консультативні, дорадчі органи.

Рішення про утворення чи ліквідацію колегії, інших постійних або тимчасових консультативних, дорадчих органів, їх кількісний та персональний склад, положення про них затверджуються Головою Держспецзв'язку України.

13. Гранична чисельність особового складу Адміністрації затверджується Кабінетом Міністрів України.

Структура Адміністрації та положення про її структурні підрозділи затверджуються Головою Держспецзв'язку України.

Штатний розпис і кошторис Адміністрації затверджуються Головою Держспецзв'язку України за погодженням із Міністерством фінансів України.

14. Адміністрація є юридичною особою, має печатку із зображенням Державного Герба України та своїм найменуванням, інші печатки і штампи, власні бланки, рахунки в органах Державної казначейської служби України.

Глава Адміністрації Президента України **С. ЛЬОВОЧКІН**

УКАЗ
ПРЕЗИДЕНТА УКРАЇНИ

Про Положення про технічний захист інформації в Україні

Із змінами і доповненнями, внесеними
Указами Президента України
від 6 жовтня 2000 року N 1120/2000,
від 11 квітня 2008 року N 333/2008

1. Затвердити Положення про технічний захист інформації в Україні (додається).

2. Установити, що Служба безпеки України є правонаступником Державного комітету України з питань державних секретів.

(стаття 2 із змінами, внесеними згідно з Указом
Президента України від 11.04.2008 р. N 333/2008)

3. Внести зміни до таких Указів Президента України:

1) пункт 1 статті 3 втратив чинність

(згідно з Указом Президента України
від 11.04.2008 р. N 333/2008)

2) у Положенні про порядок здійснення криптографічного захисту інформації в Україні, затвердженому Указом Президента України від 22 травня 1998 року N 505 (із змінами, внесеними Указом від 15 вересня 1998 року N 1019):

у пункті 3 слова "Головне управління урядового зв'язку Служби безпеки України (далі - Головне управління)" замінити словами "Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (далі - Департамент)";

у пункті 10 слова "Головне управління" замінити словом "Департамент".

4. Кабінету Міністрів України привести свої нормативно-правові акти у відповідність з цим Указом.

Президент України **Л. КУЧМА**

м. Київ
27 вересня 1999 року
N 1229/99

ЗАТВЕРДЖЕНО
Указом Президента України
від 27 вересня 1999 року N 1229/99

Положення
про технічний захист інформації в Україні

1. Це Положення визначає правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства.

Технічний захист інформації здійснюється щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ, організацій (далі - органи, щодо яких здійснюється ТЗІ).

2. Ужиті в цьому Положенні терміни мають таке значення:

конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення;

цілісність - властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

доступність - властивість інформації бути захищеною від несанкціонованого блокування;

технічний захист інформації (ТЗІ) - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;

інформаційна система - автоматизована система, комп'ютерна мережа або система зв'язку;

дозвіл - документ, що надає право на виконання робіт з технічного захисту інформації для власних потреб;

комплекс технічного захисту інформації - сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті.

3. Правову основу технічного захисту інформації в Україні становлять Конституція України, закони України, акти Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України, з питань технічного захисту інформації, а також це Положення.

(пункт 3 із змінами, внесеними згідно з Указом
Президента України від 11.04.2008 р. N 333/2008)

4. Державна політика технічного захисту інформації формується згідно із законодавством і реалізується Державною службою спеціального зв'язку та захисту інформації України (далі –

Держспецзв'язку України) у взаємодії з органами, щодо яких здійснюється ТЗІ.

(пункт 4 із змінами, внесеними згідно з Указом
Президента України від 11.04.2008 р. N 333/2008)

5. Організація технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, покладається на їх керівників.

6. Організаційно-технічні принципи, порядок здійснення заходів з технічного захисту інформації, порядок контролю у цій сфері, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації, порядок атестації та експертизи комплексів технічного захисту інформації визначаються нормативно-правовими актами, прийнятими в установленому порядку відповідними органами.

Нормативно-правові акти з технічного захисту інформації є обов'язковими для виконання всіма суб'єктами системи технічного захисту інформації.

7. Розроблення, видання нормативно-правових актів з питань технічного захисту інформації, а також роботи, пов'язані з розробленням і виконанням загальнодержавних програм розвитку системи технічного захисту інформації, здійснюються за рахунок коштів державного бюджету та інших джерел фінансування, не заборонених законодавством.

8. Суб'єктами системи технічного захисту інформації є:

Держспецзв'язку України;

(абзац другий пункту 8 із змінами, внесеними згідно з
Указом Президента України від 11.04.2008 р. N 333/2008)

органи, щодо яких здійснюється ТЗІ;

науково-дослідні та науково-виробничі установи Держспецзв'язку України, державні підприємства, що перебувають в управлінні Держспецзв'язку України та виконують завдання з питань технічного захисту інформації;

(абзац четвертий пункту 8 у редакції Указу
Президента України від 11.04.2008 р. N 333/2008)

військові частини, підприємства, установи та організації всіх форм власності й громадяни-підприємці, які провадять діяльність з технічного захисту інформації за відповідними дозволами або ліцензіями;

навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців з технічного захисту інформації.

9. Пункт 9 виключено

(пункт 9 в редакції Указу Президента
України від 06.10.2000 р. N 1120/2000,
виключено згідно з Указом Президента
України від 11.04.2008 р. N 333/2008)

10. Пункт 10 втратив чинність

(згідно з Указом Президента
України від 06.10.2000 р. N 1120/2000)

11. Основними завданнями органів, щодо яких здійснюється ТЗІ, є:

забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів з питань технічного захисту інформації;

видання у межах своїх повноважень нормативно-правових актів із зазначених питань;

здійснення контролю за станом технічного захисту інформації.

12. Органи, щодо яких здійснюється ТЗІ, відповідно до покладених на них завдань:

створюють або визначають підрозділи, на які покладається забезпечення технічного захисту інформації та контроль за його станом, узгоджують основні завдання та функції цих підрозділів;

видають за погодженням з Адміністрацією Держспецзв'язку України та впроваджують нормативно-правові акти з питань технічного захисту інформації;

(абзац третій пункту 12 із змінами, внесеними згідно з
Указом Президента України від 11.04.2008 р. N 333/2008)

погоджують з Адміністрацією Держспецзв'язку України проведення підприємствами, установами, організаціями тих науково-дослідних, дослідно-конструкторських і дослідно-технологічних робіт, спрямованих на розвиток нормативно-правової та матеріально-технічної бази системи технічного захисту інформації, які здійснюються за рахунок коштів державного бюджету;

(абзац четвертий пункту 12 із змінами, внесеними згідно з
Указом Президента України від 11.04.2008 р. N 333/2008)

створюють або визначають за погодженням з Адміністрацією Держспецзв'язку України підприємства, установи та організації, що забезпечують технічний захист інформації;

(абзац п'ятий пункту 12 із змінами, внесеними згідно з
Указом Президента України від 11.04.2008 р. N 333/2008)

забезпечують підготовку, перепідготовку та підвищення кваліфікації кадрів з технічного захисту інформації;

надають Адміністрації Держспецзв'язку України за його запитами відомості про стан технічного захисту інформації.

(абзац сьомий пункту 12 із змінами, внесеними згідно з
Указом Президента України від 11.04.2008 р. N 333/2008)

13. Основними завданнями інших суб'єктів системи технічного захисту інформації є:

дослідження загроз для інформації на об'єктах, функціонування яких пов'язано з інформацією, що підлягає охороні;

створення та виробництво засобів забезпечення технічного захисту інформації;

розроблення, впровадження, супроводження комплексів технічного захисту інформації;

підвищення кваліфікації фахівців з технічного захисту інформації.

14. Суб'єкти системи технічного захисту інформації мають право співробітничати з підприємствами, установами, організаціями іноземних держав, які здійснюють аналогічну діяльність, на основі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, та інших актів законодавства України.

15. Матеріально-технічна база системи технічного захисту інформації складається з технічних засобів загального призначення та спеціальних технічних засобів.

Технічні засоби загального призначення повинні мати документ, що засвідчує їх відповідність вимогам нормативно-правових актів з технічного захисту інформації, одержаний у порядку, що встановлюється Адміністрацією Держспецзв'язку України і Державним комітетом України з питань технічного регулювання та споживчої політики.

(абзац другий пункту 15 із змінами, внесеними згідно з
Указом Президента України від 11.04.2008 р. N 333/2008)

16. Техніко-економічне обгрунтування, проектування будівництва та реконструкції об'єктів, проведення наукових досліджень та створення інформаційних систем, зразків озброєнь, військової та спеціальної техніки, критичних і небезпечних технологій виконуються за завданнями, до яких включаються вимоги з технічного захисту інформації, якщо під час виконання передбачених завданням робіт та у процесі функціонування зазначених об'єктів, систем, зразків і технологій циркулюватиме інформація, охорона якої забезпечується державою.

Під час віднесення замовником таких робіт до особливо важливих та створення інформаційних систем державних органів завдання та результати приймання їх етапів погоджуються з Адміністрацією Держспецзв'язку України. Фінансування створення цих систем здійснюється після такого погодження.

(абзац другий пункту 16 із змінами, внесеними згідно з
Указом Президента України від 11.04.2008 р. N 333/2008)

Витрати на заходи з технічного захисту інформації включаються до кошторисної вартості робіт.

17. Під час розроблення і впровадження заходів з технічного захисту інформації використовуються засоби, дозволені Адміністрацією Держспецзв'язку України для застосування та включені до відповідних переліків.

(пункт 17 із змінами, внесеними згідно з Указом
Президента України від 11.04.2008 р. N 333/2008)

18. Контроль у сфері технічного захисту інформації полягає в перевірці виконання вимог цього Положення, інших нормативно-правових актів з питань технічного захисту інформації та в оцінюванні захищеності інформації на об'єкті, де вона циркулюватиме або циркулює.

Оцінювання захищеності інформації здійснюється шляхом атестації або експертизи комплексів технічного захисту інформації та інспекційних перевірок. За результатами атестації або експертизи комплексів технічного захисту інформації визначається можливість введення в експлуатацію об'єкта, де циркулюватиме інформація, охорона якої забезпечується державою.

19. Порядок експертизи та інспекційних перевірок захищеності інформації визначається відповідними нормативно-правовими актами.

20. Розроблення, впровадження, атестація та експлуатація комплексів технічного захисту інформації для власних потреб здійснюються відповідними підрозділами органів, щодо яких здійснюється ТЗІ, або військовими частинами, підприємствами, установами, організаціями, на які в установленому порядку покладено забезпечення технічного захисту інформації, за наявності у них відповідного дозволу.

До виконання цих робіт можуть бути залучені суб'єкти підприємницької діяльності, що мають відповідні ліцензії.

Результати атестації на державних об'єктах, віднесених замовником до особливо важливих, погоджуються з Адміністрацією Держспецзв'язку України.

(абзац третій пункту 20 із змінами, внесеними згідно з
Указом Президента України від 11.04.2008 р. N 333/2008)

21. Роботи з технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, здійснюються за рахунок коштів, що виділяються на їх утримання, прибутку та інших джерел, не заборонених законодавством.

Керівники зазначених органів створюють належні умови для контролю за забезпеченням технічного захисту інформації.

22. У разі порушення вимог щодо забезпечення технічного захисту інформації посадові особи та громадяни несуть відповідальність згідно із законодавством України.

Глава Адміністрації
Президента України **М. БІЛОБЛОЦЬКИЙ**

Позначку "Опублікуванню не підлягає" знято Указом Президента України від 24 листопада 2009 року N 963/2009

УКАЗ
ПРЕЗИДЕНТА УКРАЇНИ

Про Положення про Державний комітет України з питань державних секретів та технічного захисту інформації

Затвердити Положення про Державний комітет України з питань державних секретів та технічного захисту інформації (додається).

Президент України **Л. КУЧМА**

м. Київ
5 листопада 1996 року
N 1047/96

ЗАТВЕРДЖЕНО
Указом Президента України
від 5 листопада 1996 року N 1047/96

ПОЛОЖЕННЯ
про Державний комітет України з питань державних секретів та технічного захисту інформації

1. Державний комітет України з питань державних секретів та технічного захисту інформації (Держкомсекретів України) є центральним органом виконавчої влади у сфері забезпечення охорони державної таємниці та технічного захисту інформації на всій території України, здійснює керівництво дорученою йому сферою, несе відповідальність за її стан та розвиток.

Держкомсекретів України у межах, визначених законами України, реалізує державну політику у сфері забезпечення охорони державної таємниці та технічного захисту інформації, координує режимно-секретну діяльність та функціонування інфраструктури системи технічного захисту інформації центральних та місцевих органів виконавчої влади, підприємств, установ і організацій усіх форм власності, дипломатичних представництв та інших об'єктів України за кордоном.

2. Держкомсекретів України у своїй діяльності керується Конституцією України, законами України, актами Президента України і Кабінету Міністрів України, а також цим Положенням.

Держкомсекретів України в установленому порядку в межах своїх повноважень вирішує питання, що випливають із загальновизнаних норм міжнародного права та укладених Україною міжнародних договорів.

3. Основними завданнями Держкомсекретів України є:

1) розроблення концептуальних основ державної політики охорони державної таємниці та технічного захисту інформації;

2) створення і вдосконалення системи охорони державної таємниці та технічного захисту інформації, розроблення правової та організаційної основи, а також інженерно-технічних заходів забезпечення її функціонування;

3) організаційне та методичне керівництво системою охорони державних секретів і технічного захисту інформації та забезпечення її функціонування;

4) здійснення контролю за режимом секретності та технічним захистом інформації з обмеженим доступом у центральних та місцевих органах виконавчої влади, на підприємствах, в установах і організаціях усіх форм власності, дипломатичних представництвах та на інших об'єктах України за кордоном;

5) реєстрація відомостей, що становлять державну таємницю.

4. Держкомсекретів України відповідно до покладених на нього завдань:

1) розробляє пропозиції щодо основних напрямів державної політики у сфері забезпечення охорони державної таємниці та технічного захисту інформації з обмеженим доступом; реалізує державну стратегію розвитку системи охорони державної таємниці та технічного захисту інформації;

2) бере участь у розробленні проектів загальнодержавних програм у сфері охорони державної таємниці та статей Державного бюджету України (оборона, економіка, наука і техніка, зовнішні відносини, державна безпека і охорона правопорядку) у частині визначення видатків на режимно-секретну діяльність і технічний захист інформації, а також заходів, спрямованих на охорону державної таємниці та технічний захист інформації під час формування та реалізації завдань щодо поставок продукції для державних потреб;

3) вносить до відповідних державних органів пропозиції щодо пріоритетних напрямів розвитку інфраструктури, правового, наукового, матеріально-технічного та фінансового забезпечення системи захисту державної таємниці та технічного захисту інформації;

4) розробляє цільові програми, опрацьовує заходи, спрямовані на забезпечення охорони державної таємниці та технічного захисту інформації, узгоджує проекти державних програм міністерств та інших центральних органів виконавчої влади щодо запровадження вимог режиму секретності та технічного захисту інформації;

5) є державним замовником цільових науково-технічних програм, науково-дослідних і дослідно-конструкторських робіт з проблем охорони державної таємниці та технічного

захисту інформації, координує їх виконання, формує проекти державних замовлень на виробництво, поставку засобів забезпечення охорони державної таємниці та технічного захисту інформації, комплектуючих вузлів та матеріалів;

6) організовує у межах своїх повноважень проведення експертних оцінок рівня науково-технічних рішень з технічного захисту інформації та охорони об'єктів, експертизи проектної, конструкторської та технологічної документації, баз і банків даних, що стосуються її захисту;

7) узгоджує завдання в частині охорони державної таємниці та технічного захисту інформації на проектування будівельних робіт для особливо важливих об'єктів, створення зразків озброєнь, військової та спеціальної техніки, пріоритетних технологій, автоматизованих систем управління, комп'ютерних мереж і систем, систем зв'язку, контролює їх виконання;

8) установлює порядок технічного захисту інформації під час створення обчислювальних мереж на державних підприємствах, в установах і організаціях, підключення їх до обчислювальних мереж загального користування та механізми взаємодії Комітету з недержавним сектором економіки в галузі технічного захисту інформації;

9) забезпечує контроль за відповідністю запроваджуваних на державних підприємствах, в установах, організаціях заходів щодо технічного захисту інформації установленим вимогам;

10) вносить пропозиції щодо визначення особливостей забезпечення охорони державної таємниці та інформації, що підлягає технічному захисту в умовах приватизації підприємств, діяльність яких пов'язана з державною таємницею;

11) визначає єдині вимоги щодо виготовлення, користування, забезпечення схоронності, передачі, транспортування, обліку та зберігання носіїв інформації, що становить державну таємницю, та порядок і умови охорони власником такої інформації або її матеріальних носіїв у разі обмеження в установленому порядку його прав на них;

12) здійснює на підставі рішень державних експертів з питань таємниць реєстрацію відомостей, що становлять державну таємницю, формує, затверджує та організовує публікацію Зводу відомостей, що становлять державну таємницю України, зміни та доповнення до нього; погоджує та реєструє розгорнуті переліки відомостей, що становлять державну таємницю, створені на підставі та в межах цього Зводу;

13) доручає державним експертам з питань таємниць розглядати питання про віднесення інформації до державної таємниці або давати висновки про її розсекречування, проведення відповідної експертизи та надає їм методичну допомогу;

14) подає в установленому законом порядку Президентові України пропозиції щодо покладення на посадових осіб функцій державних експертів з питань таємниць;

15) у порядку, визначеному законодавством, видає дозволи (ліцензії) на здійснення діяльності, пов'язаної з державною таємницею, виробництво, реалізацію, застосування, обслуговування продукції, виконання робіт, надання послуг у сфері технічного захисту інформації, скасовує або тимчасово припиняє дію рішень про надання дозволів (ліцензій);

16) затверджує переліки продукції технічного захисту інформації, що підлягає обов'язковій сертифікації, та визначає методику її сертифікації, видає дозвіл на тимчасове використання

продукції, яка не проходила сертифікацію, створює та забезпечує функціонування державної системи сертифікації засобів технічного захисту інформації;

17) здійснює моніторинг вітчизняних і зарубіжних ринків виробів та послуг у сфері технічного захисту інформації, розробляє рекомендації щодо їх використання;

18) погоджує в межах своїх повноважень розміщення дипломатичних представництв, консульських установ іноземних держав, представництв міжнародних та іноземних організацій на території України;

19) затверджує форму реєстру підприємств, установ і організацій з особливим режимом діяльності та включає до нього ті з них, яким надані категорії режиму секретності;

20) погоджує порядок здійснення наглядових, контрольно-ревізійних та інших функцій щодо підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею та приймає рішення щодо обгрунтованості відмови ними в наданні державним органам інформації, що становить державну таємницю, або виконанні інших рішень цих органів у зв'язку зі здійсненням ними зазначених функцій;

21) контролює у межах, визначених законодавством, діяльність центральних і місцевих органів виконавчої влади, підприємств, установ і організацій усіх форм власності щодо забезпечення охорони державної таємниці та іншої інформації, що підлягає технічному захисту, під час виконання державних замовлень, контрактів і програм, установлення і справджування зовнішньоекономічних та інших міжнародних зв'язків, прийому іноземних делегацій, здійснює методичне керівництво діяльністю режимно-секретних органів і підрозділів технічного захисту інформації зазначених органів, підприємств, установ, організацій;

22) припиняє роботи у разі порушення першої категорії норм і вимог технічного захисту інформації, організовує в установленому порядку розслідування причин, які призвели до цих порушень; вносить до відповідних державних органів пропозиції про вжиття заходів до посадових осіб і громадян за порушення ними вимог законодавства з питань охорони державної таємниці та технічного захисту інформації;

23) призначає із залученням представників міністерств, інших центральних та місцевих органів виконавчої влади, підприємств, установ та організацій (за погодженням з керівниками) службові розслідування фактів розголошення державної таємниці, втрат документів або інших матеріальних носіїв інформації, що містять державну таємницю, витоку або видачі іноземній державі, іноземній організації чи їх представникам державної таємниці та інших порушень режиму секретності та технічного захисту інформації;

24) формує та супроводжує у взаємодії з Міноборони України, Службою безпеки України та іншими органами виконавчої влади моделі технічних розвідок і загроз;

25) затверджує разом з Міністерством охорони здоров'я України перелік психічних захворювань, наявність яких у особи є підставою для відмови у наданні допуску до державної таємниці;

26) бере у межах своїх повноважень участь у підготовці міжнародних договорів України, контролює роботу із забезпечення охорони державної таємниці та технічного захисту інформації у процесі реалізації цих договорів, укладає міжнародні договори міжвідомчого характеру;

27) забезпечує виконання завдань з мобілізаційної підготовки та мобілізаційної готовності Комітету;

28) надає консультаційну допомогу центральним і місцевим органам виконавчої влади, підприємствам, установам і організаціям усіх форм власності з питань віднесення відомостей до державної таємниці та їх розсекречування, організації режиму секретності та технічного захисту інформації, а громадянам, які мають або мали допуск до державної таємниці, - з питань обізнаності їх у державній таємниці;

29) визначає в порядку, передбаченому законодавством, обсяги статистичної звітності центральних і місцевих органів виконавчої влади, підприємств, установ і організацій усіх форм власності у сфері охорони державної таємниці та технічного захисту інформації;

30) бере участь у формуванні державної системи підготовки кадрів із охорони державної таємниці та технічного захисту інформації, створює в установленому порядку навчальні та науково-дослідні інститути, центри, організовує курси з підготовки (перепідготовки) таких спеціалістів, разом з навчальними закладами визначає спеціальності та спеціалізації з підготовки на постійній основі відповідних фахівців;

31) в установленому порядку утворює, реорганізовує і ліквідовує підприємства, установи і організації, засновані на державній власності, що належать до сфери його управління;

32) здійснює у визначеному законодавством порядку видавничу діяльність;

33) виконує у межах повноважень, визначених законодавством, функції управління об'єктами державної власності, що належать до сфери управління Комітету;

34) узагальнює практику застосування законодавства з питань, що належать до сфери його управління, розробляє пропозиції про вдосконалення законодавства та в установленому порядку вносить їх на розгляд Президентові України, Кабінету Міністрів України;

35) організовує виконання актів законодавства, здійснює систематичний контроль за їхньою реалізацією в межах і в порядку, установлених законодавством;

36) здійснює на основі та на виконання Конституції України, законів України, актів Президента України і Кабінету Міністрів України інші функції.

5. Держкомсекретів України очолює Голова, якого за поданням Прем'єр-міністра України призначає Президент України.

Голова несе персональну відповідальність перед Президентом України та Кабінетом Міністрів України за виконання Комітетом покладених на нього завдань і здійснення ним своїх функцій.

Голова має заступників, які призначаються відповідно до законодавства. Голова Комітету розподіляє обов'язки між заступниками, визначає ступінь відповідальності керівників підрозділів центрального апарату Комітету.

Заступники Голови виконують за дорученням Голови окремі його функції та заміщують Голову в разі його відсутності або неможливості здійснення ним своїх повноважень.

6. Голова Держкомсекретів України:

1) здійснює керівництво Комітетом;

2) організовує роботу колегії Комітету і головує на її засіданнях;

3) є розпорядником бюджетних асигнувань на утримання і забезпечення діяльності Комітету;

4) затверджує штатний розпис центрального апарату Комітету;

5) затверджує положення про структурні підрозділи центрального апарату Комітету та місцевих управлінь і відділів;

6) здійснює в установленому порядку призначення на посаду та звільнення з посад керівників місцевих управлінь і відділів;

7) вносить в установленому порядку на розгляд Кабінету Міністрів України проекти законодавчих та інших актів з питань, що належать до компетенції Комітету;

8) здійснює інші повноваження, передбачені законодавством.

7. Для погодженого вирішення питань, що належать до компетенції Держкомсекретів України, обговорення найважливіших напрямів його діяльності у Комітеті утворюється колегія у складі Голови (голова колегії), заступників Голови за посадою, а також інших керівних працівників Комітету.

Членів колегії затверджує та звільняє від виконання обов'язків Кабінет Міністрів України за поданням Голови Комітету.

Рішення колегії проводяться в життя наказами Голови Держкомсекретів України.

8. Для розгляду наукових рекомендацій та інших пропозицій щодо головних напрямів реалізації державної політики у сфері охорони державної таємниці та технічного захисту інформації, обговорення найважливіших програм та інших питань у Держкомсекретів України може бути утворено науково-технічну раду та інші дорадчі і консультаційні органи.

Склад цих рад і положення про них затверджує Голова Комітету.

9. Держкомсекретів України у межах своїх повноважень на основі та на виконання актів законодавства видає накази, контролює їх виконання.

У випадках, передбачених законодавством, нормативно-правові акти Голови Комітету є обов'язковими для виконання центральними та місцевими органами виконавчої влади, Радою міністрів Автономної Республіки Крим, підприємствами, установами, організаціями усіх форм власності та громадянами.

Нормативно-правові акти Голови Комітету підлягають державній реєстрації в порядку, установленому законодавством.

Голова Комітету у разі потреби видає разом з керівниками інших центральних та місцевих органів виконавчої влади спільні акти.

10. Держкомсекретів України у процесі виконання покладених на нього завдань взаємодіє з іншими центральними органами виконавчої влади, органами Автономної Республіки Крим, місцевими державними адміністраціями, а також з відповідними органами інших держав.

11. Держкомсекретів України в установленому порядку утворює управління і відділи в Автономній Республіці Крим, областях, містах Києві та Севастополі. Управління і відділи не входять до складу відповідно Ради міністрів Автономної Республіки Крим, обласних, Київської та Севастопольської міських державних адміністрацій.

12. Держкомсекретів України відповідно до покладених на нього завдань і повноважень має право:

1) залучати спеціалістів центральних органів виконавчої влади, підприємств, установ і організацій (за погодженням з керівниками) для розгляду питань, що належать до його повноважень;

2) одержувати в установленому законодавством порядку від міністерств, інших центральних та місцевих органів виконавчої влади, підприємств, установ і організацій інформацію, документи і матеріали, а від Міністерства статистики України - статистичні дані для виконання покладених на Комітет завдань (безоплатно);

3) скликати в установленому порядку наради з питань, що належать до його повноважень;

4) притягати до дисциплінарної відповідальності керівників місцевих управлінь і відділів Комітету;

5) скасовувати в межах своїх повноважень акти місцевих управлінь і відділів, що суперечать Конституції України, законодавству України та рішенням Комітету;

6) залучати на договірній основі фахівців для підготовки проектів актів законодавства та надання консультацій.

13. Працівники Держкомсекретів України мають право за попереднім повідомленням керівників входити до приміщень центральних та місцевих органів виконавчої влади, підприємств, установ, організацій усіх форм власності, яким було видано дозвіл (ліцензію), дипломатичних представництв та інших об'єктів України за кордоном для виконання своїх повноважень.

14. Граничну чисельність і фонд оплати праці працівників центрального апарату Держкомсекретів України затверджує Кабінет Міністрів України.

Структуру центрального апарату Комітету затверджує Віце-прем'єр-міністр України.

15. Держкомсекретів України є юридичною особою, має самостійний баланс, рахунки в установах банків, печатку із зображенням Державного Герба України і своїм найменуванням.

16. Загальні засади діяльності, статус, умови оплати праці, матеріальне та соціально-побутове забезпечення працівників Комітету визначаються законодавством України.

Глава Адміністрації
Президента України **Д. ТАБАЧНИК**

УКАЗ
ПРЕЗИДЕНТА УКРАЇНИ

Про Положення про порядок здійснення криптографічного захисту інформації в Україні

Із змінами і доповненнями, внесеними
Указами Президента України
від 15 вересня 1998 року N 1019/98,
від 27 вересня 1999 року N 1229/99,
від 11 квітня 2008 року N 333/2008,
від 28 серпня 2009 року N 693/2009

Затвердити Положення про порядок здійснення криптографічного захисту інформації в Україні (додається).

Президент України **Л. КУЧМА**

м. Київ
22 травня 1998 року
N 505/98

ЗАТВЕРДЖЕНО
Указом Президента України
від 22 травня 1998 року N 505/98

ПОЛОЖЕННЯ
про порядок здійснення криптографічного захисту інформації в Україні

1. Це Положення визначає порядок здійснення криптографічного захисту інформації з обмеженим доступом, розголошення якої завдає (може завдати) шкоди державі, суспільству або особі.

2. Вжиті у цьому Положенні терміни мають таке значення:

криптографічний захист - вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

засіб криптографічного захисту інформації - програмний, апаратно-програмний, апаратний або інший засіб, призначений для криптографічного захисту інформації;

криптографічна система (криптосистема) - сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що обробляється, зберігається та (або) передається;

система криптографічного захисту інформації - сукупність органів, підрозділів, груп, діяльність яких спрямована на забезпечення криптографічного захисту інформації, та підприємств, установ і організацій, що розробляють, виробляють, експлуатують та (або) розповсюджують криптосистеми і засоби криптографічного захисту інформації.

3. Державну політику у сфері криптографічного захисту інформації відповідно до закону реалізує Державна служба спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку України).

(пункт 3 із змінами, внесеними згідно з
Указом Президента України від 27.09.99 р. N 1229/99,
у редакції Указу Президента України
від 11.04.2008 р. N 333/2008)

4. Ліцензування діяльності, пов'язаної з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації, здійснюється згідно із законодавством України.

(пункт 4 в редакції Указу
Президента України від 15.09.98 р. N 1019/98)

5. Державні органи, підприємства, установи і організації придбавають, вивозять з України, використовують криптосистеми і засоби криптографічного захисту інформації за погодженням з Адміністрацією Державної служби спеціального зв'язку та захисту інформації України.

(пункт 5 із змінами, внесеними згідно з Указами
Президента України від 11.04.2008 р. N 333/2008,
від 28.08.2009 р. N 693/2009)

6. З метою визначення рівня захищеності від несанкціонованого доступу до інформації з обмеженим доступом проводяться сертифікаційні випробування криптосистем і засобів криптографічного захисту.

7. Для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, використовуються криптосистеми і засоби криптографічного захисту, допущені до експлуатації.

Зазначені криптосистеми і засоби перебувають у державній власності.

Засоби криптографічного захисту службової інформації та криптосистеми з відповідного дозволу можуть перебувати і в недержавній власності.

8. Для криптографічного захисту конфіденційної інформації використовуються криптосистеми і засоби криптографічного захисту, які мають сертифікат відповідності.

9. Порядок розроблення, виготовлення, розповсюдження, експлуатації, збереження, використання, випробування, сертифікації та допуску до експлуатації криптосистем і засобів криптографічного захисту інформації, контролю за додержанням вимог безпеки при проведенні цих робіт визначається відповідними положеннями.

Діяльність, пов'язана зі створенням і експлуатацією систем криптографічного захисту секретної інформації, забезпеченням безпеки інформації, що циркулює в цих системах, регламентується Інструкцією.

10. Роботи, передбачені пунктами 4, 6 і 7 цього Положення, виконує, а положення та Інструкцію, зазначені у пункті 9, затверджує Адміністрація Державної служби спеціального зв'язку та захисту інформації України. Положення та Інструкція є обов'язковими для державних органів, а також підприємств, установ, організацій усіх форм власності та громадян.

(пункт 10 із змінами, внесеними згідно з
Указами Президента України від 27.09.99 р. N 1229/99,
від 11.04.2008 р. N 333/2008)

11. Діяльність, пов'язану з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації, можуть здійснювати суб'єкти підприємницької діяльності, зареєстровані в порядку, встановленому законодавством.

(пункт 11 в редакції Указу
Президента України від 15.09.98 р. N 1019/98)

12. До користування криптосистемами та засобами криптографічного захисту секретної інформації допускаються особи, які у встановленому законодавством України порядку одержали допуск до державної таємниці.

13. Відповідно до Інструкції, зазначеної в пункті 9 цього Положення, міністерства, інші центральні органи виконавчої влади затверджують відомчі інструкції.

14. У разі порушення вимог щодо порядку здійснення криптографічного захисту інформації суб'єкти підприємницької діяльності, установи, організації, посадові особи та громадяни несуть відповідальність згідно із законодавством України.

(пункт 14 із доповненнями, внесеними згідно з
Указом Президента України від 15.09.98 р. N 1019/98)

Глава Адміністрації Президента України **Є. КУШНАРЬОВ**

Про затвердження Положення про державний контроль за станом технічного захисту інформації під час діяльності на території України іноземних інспекційних груп

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
від 16 травня 2007 року N 86

Зареєстровано в Міністерстві юстиції України
4 червня 2007 р. за N 577/13844

Із змінами і доповненнями, внесеними наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 6 жовтня 2011 року N 264

Відповідно до Закону України "Про Державну службу спеціального зв'язку та захисту інформації України", з метою запровадження контролю за виконанням органами державної влади, органами місцевого самоврядування, органами військового управління Збройних Сил України та інших військових формувань, утворених відповідно до законів України, підприємствами, установами та організаціями заходів з технічного захисту інформації під час діяльності на території України іноземних інспекційних груп відповідно до міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, **НАКАЗУЮ**:

1. Затвердити Положення про державний контроль за станом технічного захисту інформації під час діяльності на території України іноземних інспекційних груп, що додається.

2. Організацію та виконання заходів щодо здійснення державного контролю за станом технічного захисту інформації під час діяльності на території України іноземних інспекційних груп покласти на начальника Департаменту державного контролю за станом криптографічного та технічного захисту інформації Адміністрації Державної служби спеціального зв'язку та захисту інформації України.

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

4. Визнати таким, що втратив чинність, наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 30.03.2001 N 9/ДСК, зареєстрований у Міністерстві юстиції України 13.04.2001 за N 347/5538.

5. Контроль за виконанням наказу покласти на першого заступника Голови Державної служби спеціального зв'язку та захисту інформації України.

Голова Служби **Ю. Б. Чеботаренко**

ЗАТВЕРДЖЕНО
наказом Адміністрації Державної
служби спеціального зв'язку та захисту
інформації України
від 16 травня 2007 р. N 86

Зареєстровано
в Міністерстві юстиції України
4 червня 2007 р. за N 577/13844

ПОЛОЖЕННЯ
про державний контроль за станом технічного захисту інформації під час діяльності на території України іноземних інспекційних груп

1. Загальні положення

1.1. Це Положення розроблено відповідно до вимог Законів України "Про Державну службу спеціального зв'язку та захисту інформації України" та "Про захист інформації в інформаційно-телекомунікаційних системах ".

1.2. Положення визначає порядок здійснення Державною службою спеціального зв'язку та захисту інформації України (далі - Держспецзв'язку) державного контролю за ввезеним на територію України інспекційним обладнанням та його використанням на об'єктах інспектування, а також за станом технічного захисту інформації (далі - ТЗІ) в органах державної влади, органах місцевого самоврядування, військових формуваннях, підприємствах, установах та організаціях під час діяльності іноземних інспекційних груп відповідно до міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

1.3. У Положенні терміни вживаються у такому значенні:

іноземна інспекційна місія (далі - ІІМ) - комплекс передбачених міжнародними договорами заходів, що здійснюються Українською Стороною та стороною, яка проводить інспектування (спостереження), протягом усього періоду перебування на території України;

держави-учасниці - держави, що підписали і приєдналися до міжнародних договорів, приймають на своїй території і здійснюють на території інших держав інспекційні місії відповідно до умов діючих договорів;

іноземна інспекційна група (далі - ІІГ) - група персоналу, призначеного відповідною міжнародною організацією або державою-учасницею для проведення інспекційної перевірки відповідно до вимог міжнародних договорів;

пункт в'їзду-виїзду (далі - ПВВ) - пункт, визначений державою, яка інспектується, для прибуття (відбуття) персоналу ІІГ;

передпольотна оглядова процедура - перевірка виконання заходів, які унеможливлюють використання апаратури спостереження під час транзитного перельоту іноземного літака спостереження з пункту дислокації до ПВВ;

об'єкти інспектування - державні органи, військові формування, підприємства, установи та організації, які підлягають інспектуванню ІІГ у рамках міжнародних договорів;

об'єкти спостереження - об'єкти інформаційної діяльності, на яких циркулює службова інформація та/або таємна інформація, що містить державну або іншу передбачену законом таємницю, які потрапляють до зон спостереження іноземних літаків спостереження;

(абзац восьмий пункту 1.3 із змінами, внесеними згідно з наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 06.10.2011 р. N 264)

післяпольотна оглядова процедура - перевірка виконання заходів, які унеможливлюють використання апаратури спостереження під час транзитного перельоту іноземного літака спостереження з ПВВ до пункту дислокації;

передпольотна інспекція - комплекс заходів, передбачених Договором з відкритого неба, ратифікованим Законом України "Про ратифікацію Договору з відкритого неба" (далі - Договір), які проводяться з метою підтвердження того, що літак та апаратура спостереження і пов'язане з нею обладнання відповідають вимогам Договору;

група супроводження - група представників Української Сторони, яка визначена для супроводження ІІГ на об'єктах інспектування.

1.4. Під час діяльності ІІГ на території України Держспецзв'язку перевіряються:

увезена ІІГ інспекційна апаратура та обладнання;

літаки спостереження іноземних держав, апаратура спостереження та пов'язане з нею обладнання;

дотримання договірних умов використання ІІГ інспекційного обладнання під час інспекційних перевірок та використання апаратури спостереження під час спостережних польотів;

своєчасність та повнота оповіщення об'єктів інспектування та об'єктів спостереження;

повнота та достатність виконання заходів з ТЗІ державними органами, військовими формуваннями, підприємствами, установами та організаціями під час діяльності ІІГ.

2. Порядок здійснення державного контролю за ввезеним інспекційним обладнанням та його використанням на об'єктах інспектування

2.1. Контроль увезеної ІІГ інспекційної апаратури та обладнання здійснюється Держспецзв'язку шляхом проведення перевірок апаратури та обладнання у ПВВ. Перевірки проводяться на підставі приписів (додаток 1) і містять у собі:

зовнішній огляд інспекційної апаратури та обладнання з метою визначення їх відповідності паспортним даним та перелікам обладнання, визначеним умовами договорів;

перевірку інспекційної апаратури та обладнання із застосуванням спеціальних технічних засобів, за необхідності, з метою визначення відсутності функцій, не сумісних з договірними, та функцій подвійного призначення;

організацію заходів щодо унеможливлення використання ІІГ під час проведення інспекційних перевірок зразків інспекційної апаратури та обладнання, які не відповідають договірним вимогам.

Результати перевірки оформляються Актом перевірки ввезеного на територію України інспекційного обладнання, у якому надається (або не надається) дозвіл на використання ІІГ інспекційної апаратури та обладнання на об'єктах інспектування (додаток 2).

2.2. Контроль літаків спостереження, апаратури спостереження та пов'язаного з нею обладнання здійснює Адміністрація Держспецзв'язку шляхом проведення, на підставі припису, передпольотних та післяпольотних оглядових процедур, передпольотних інспекцій літаків у ПВВ та, за необхідності, демонстраційних польотів і містить у собі:

перевірки виконання процедур унеможливлення використання апаратури спостереження під час виконання транзитних перельотів;

перевірки літаків спостереження на відсутність на них обладнання, використання якого не передбачено умовами Договору;

перевірки наданих для огляду конфігурацій оптичної, інфрачервоної, радіолокаційної та відеоапаратури спостереження, навігаційних та обчислювальних систем, а також апаратури анотування на відповідність сертифікованим;

підтвердження, за необхідності, максимальної розрізнювальної здатності апаратури спостереження в зазначених конфігураціях шляхом виконання демонстраційних польотів над перевірними мірами.

Результати перевірки оформляються Рішенням за формою, визначеною Положенням про порядок забезпечення інспекційної діяльності в Україні згідно з Договором з відкритого неба, затвердженим постановою Кабінету Міністрів України від 13.03.2002 N 298.

2.3. Контроль за дотриманням узгоджених планів ІІМ та використанням апаратури спостереження членами ІІГ під час виконання інспекційних робіт на об'єктах інспектування проводиться Адміністрацією, регіональними органами Держспецзв'язку у складі груп супроводження безпосередньо на об'єктах інспектування або в ході спостережних польотів і містить у собі:

контроль за дотриманням встановленого порядку використання інспекційного обладнання та апаратури спостереження в ході інспектування;

контроль за відсутністю несанкціонованих дій членів ІІГ під час виконання інспекційних робіт;

ужиття заходів, спрямованих на негайне припинення несанкціонованих дій членами ІІГ, у разі порушень договірних вимог.

3. Порядок здійснення державного контролю за виконанням заходів з ТЗІ на об'єктах інспектування та об'єктах спостереження

3.1. Контроль повноти та достатності виконання заходів з ТЗІ, які виконуються на об'єктах інспектування та об'єктах спостереження під час діяльності ІІГ, здійснюється Адміністрацією, регіональними органами Держспецзв'язку в рамках державного контролю за станом технічного захисту інформації.

3.2. При цьому, крім повноти та достатності виконання заходів з ТЗІ на цих об'єктах, перевіряються:

своєчасність оповіщення об'єктів інспектування та спостереження про діяльність ІІГ, їх цільове призначення та технічне оснащення;

відповідність ужитих заходів з ТЗІ під час діяльності ІІГ вимогам нормативно-правових актів та нормативних документів системи ТЗІ.

Контроль відповідності заходів з ТЗІ під час діяльності ІІГ вимогам керівних та нормативно-методичних документів здійснюється Адміністрацією, регіональними органами Держспецзв'язку в ході проведення комплексних перевірок стану ТЗІ згідно з Планом контрольно-інспекторської роботи. Результати контролю окремим розділом уносяться до Акта комплексної перевірки.

Якщо об'єкти інспектування або об'єкти спостереження згідно з Планом контрольно-інспекторської роботи не підлягають державному контролю стану ТЗІ, контроль відповідності вжитих на цих об'єктах заходів вимогам керівних та нормативно-методичних документів здійснюється шляхом надання відповідних запитів та аналізу надісланих звітів.

3.3. Рекомендації, надані Держспецзв'язку в ході здійснення державного контролю за виконанням заходів з ТЗІ, є обов'язковими для виконання державними органами, військовими формуваннями, підприємствами, установами та організаціями.

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

Додаток 1
до підпункту 2.1 Положення про
державний контроль за станом
технічного захисту інформації під час
діяльності на території України
іноземних інспекційних груп

ПРИПИС

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

_____

(прізвище, ім'я та по батькові)

_____

у період з _____ до _____ ____ року надається право для _____

(перевірки інспекційного обладнання ІІГ, планування роботи місії,

_____

участі в роботі в складі групи супроводження)

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 підпункту 2.1 Положення про
державний контроль за станом
технічного захисту інформації під час
діяльності на території України
іноземних інспекційних груп

АКТ
перевірки інспекційного обладнання, увезеного на територію України

___ _____ 20__ інспекційною групою_____

за договором _____

Пункт в'їзду/виїзду: _____

Час прибуття: _____

Склад інспекційної групи:

_____
_____
_____

Керівник групи супроводження від України: _____

Оголошене місце інспектування: _____

Запланований час відбуття з території України: _____

ПЕРЕЛІК ІНСПЕКЦІЙНОГО ОБЛАДНАННЯ

N з/п	Найменування обладнання	Марка, тип	Заводський (серійний) номер	Кількість	Висновок

Загальний висновок:

_____
_____

_____
(посадова особа Держспецзв'язку, спеціальне звання, прізвище, ініціали)

___ _____ 20__

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

Про затвердження Положення про державний контроль за станом технічного захисту інформації

Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України
від 16 травня 2007 року N 87

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

Із змінами і доповненнями, внесеними
наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України
від 8 грудня 2008 року N 192

Відповідно до Закону України "Про Державну службу спеціального зв'язку та захисту інформації України" **НАКАЗУЮ**:

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 "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 у редакції наказу Адміністрації Державної служби
спеціального зв'язку та захисту інформації України від 08.12.2008 р. N 192)

Голова Служби **Ю. Б. Чеботаренко**

ЗАТВЕРДЖЕНО
наказом Адміністрації Державної
служби спеціального зв'язку та захисту
інформації України
від 16 травня 2007 р. 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", "Про захист інформації в інформаційно-телекомунікаційних системах" та Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації, затвердженого постановою Кабінету Міністрів України від 24.06.2006 N 868.

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 новим абзацом другим згідно з наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 08.12.2008 р. N 192)

відомості, що охороняються, - секретна інформація стосовно ОПД, що становить державну таємницю;

(пункт 1.3 розділу 1 доповнено новим абзацом третім згідно з наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 08.12.2008 р. N 192, у зв'язку з цим абзаци другий - восьмий вважати відповідно абзацами четвертим - десятим)

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 України від 08.12.2008 р. N 192)

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", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про інформацію", "Про Державну службу спеціального зв'язку та захисту інформації України" 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
України від 08.12.2008 р. N 192)

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
України від 08.12.2008 р. N 192)

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
України від 08.12.2008 р. N 192)

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, 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
України від 08.12.2008 р. N 192)

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
України від 08.12.2008 р. N 192)

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 України від 08.12.2008 р. N 192)

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 України від 08.12.2008 р. N 192)

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 новим абзацом шостим згідно з наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 08.12.2008 р. N 192,
у зв'язку з цим абзаци шостий - десятий
вважати відповідно абзацами сьомим - одинадцятим)

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 України від 08.12.2008 р. N 192)

Ознаки порушень другої категорії:

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

(абзац дев'ятий пункту 5.2 розділу 5 із змінами, внесеними згідно з наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 08.12.2008 р. N 192)

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 новим абзацом десятим згідно з наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 08.12.2008 р. N 192, у зв'язку з цим абзаци десятий та одинадцятий вважати відповідно абзацами одинадцятим та дванадцятим)

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 одинадцятий пункту 5.2 розділу 5 із змінами, внесеними згідно з наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 08.12.2008 р. N 192)

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 тринадцятим згідно з наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 08.12.2008 р. N 192)

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 України від 08.12.2008 р. N 192)

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 України від 08.12.2008 р. N 192)

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 у редакції наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 08.12.2008 р. N 192)

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 із змінами, внесеними згідно з наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 08.12.2008 р. N 192)

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:

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. _____

_____
підпис (прізвище, ініціали)

Перевірку здійснили: _____
підпис (прізвище, ініціали)

_____
підпис (прізвище, ініціали)

З актом ознайомлений:
керівник або уповноважений 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**

УПРАВЛІННЯ ДЕРЖАВНОЇ ОХОРОНИ УКРАЇНИ

НАКАЗ

19.08.2011 **м. Київ** **N 388**

Зареєстровано в Міністерстві юстиції України
9 вересня 2011 р. за N 1069/19807

Про затвердження Положення про контроль за станом технічного захисту інформації у місцях постійного і тимчасового перебування посадових осіб, щодо яких здійснюється державна охорона

Відповідно до статті 13 Закону України "Про державну охорону органів державної влади України та посадових осіб" та з метою належного здійснення технічного захисту інформації у місцях постійного і тимчасового перебування посадових осіб, щодо яких здійснюється державна охорона,

НАКАЗУЮ:

1. Затвердити Положення про контроль за станом технічного захисту інформації у місцях постійного і тимчасового перебування посадових осіб, щодо яких здійснюється державна охорона, що додається.

2. Контроль за виконанням цього наказу залишаю за собою.

3. З наказом ознайомити особовий склад Управління державної охорони України.

4. Цей наказ набирає чинності з дня його офіційного опублікування.

Начальник Управління
генерал-майор **І. О. Калінін**

ПОГОДЖЕНО:

Голова Державної служби спеціального
зв'язку та захисту інформації України **Л. І. Нетудихата**

ЗАТВЕРДЖЕНО
Наказ Управління державної охорони України
19.08.2011 N 388

Зареєстровано
в Міністерстві юстиції України
9 вересня 2011 р. за N 1069/19807

ПОЛОЖЕННЯ
про контроль за станом технічного захисту інформації у місцях постійного і тимчасового перебування посадових осіб, щодо яких здійснюється державна охорона

I. Загальні положення

1.1. Це Положення визначає порядок організації та здійснення у місцях постійного і тимчасового перебування посадових осіб, щодо яких здійснюється державна охорона, контролю за станом технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

1.2. Контроль за станом технічного захисту інформації (далі - ТЗІ) у місцях постійного і тимчасового перебування посадових осіб, щодо яких здійснюється державна охорона, здійснюється Управлінням державної охорони України (далі - Управління) відповідно до Закону України "Про державну охорону органів державної влади України та посадових осіб".

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

об'єкт "особливої норми" - місце постійного або тимчасового перебування посадової особи, щодо якої здійснюється державна охорона;

передумови витоку 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 інформації технічними каналами - наявність технічного каналу поширення інформації за умов підтвердження відповідними інструментально-розрахунковими методами невідповідності впроваджених заходів захисту інформації вимогам та нормам з ТЗІ;

стан ТЗІ - сукупність кількісних та якісних характеристик, параметрів та показників, які визначають повноту та достатність вжитих на об'єкті "особливої норми" організаційних та інженерно-технічних заходів захисту від витоку інформації технічними каналами;

інструментальний контроль - комплекс робіт з використанням контрольно-вимірювальної техніки, спрямований на оцінювання стану ТЗІ на об'єкті "особливої норми";

інструментально-розрахунковий метод - процедура оцінювання складових стану ТЗІ з використанням результатів інструментального контролю та алгоритмів розрахунків, визначених нормативними документами в сфері ТЗІ;

порушення стану ТЗІ - невідповідність окремих складових стану ТЗІ вимогам нормативно-правових актів та нормативним документам в сфері ТЗІ;

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

Інші терміни вживаються в цьому Положенні у значеннях, визначених у Законах України "Про державну таємницю", "Про інформацію", "Про Державну службу спеціального зв'язку та захисту інформації України" та ДСТУ 3396.2-97 "Технічний захист інформації. Терміни та визначення".

1.4. Контроль за станом ТЗІ полягає у проведенні інструментального контролю захищеності інформації, яка циркулює на об'єктах "особливої норми" (далі - інструментальний контроль), здійснюється з використанням інструментально-розрахункових методів з метою оцінки повноти та достатності впроваджених на об'єктах організаційних, організаційно-технічних та технічних заходів із захисту від реальної загрози витоку інформації технічними каналами.

1.5. Інструментальний контроль здійснюється шляхом проведення:

спеціальних обстежень об'єктів "особливої норми";

спеціальних перевірок об'єктів "особливої норми";

спеціальних досліджень технічних засобів, призначених для встановлення на об'єктах "особливої норми".

1.6. За результатами спеціальних обстежень, спеціальних перевірок об'єктів "особливої норми" та спеціальних досліджень технічних засобів, призначених для встановлення на об'єктах "особливої норми", здійснюються їх аналіз та надання рекомендацій щодо усунення виявлених порушень у сфері ТЗІ на об'єктах "особливої норми".

Узагальнені аналітичні матеріали щодо стану ТЗІ на об'єктах "особливої норми" подаються Начальнику Управління державної охорони України.

Про результати стану ТЗІ на об'єктах "особливої норми" Начальник Управління державної охорони України інформує Президента України, Голову Верховної Ради України, Прем'єр-міністра України та інших осіб, щодо яких здійснюється державна охорона.

II. Організація проведення інструментального контролю

2.1. Інструментальний контроль може бути плановим та позаплановим.

2.2. Плановий інструментальний контроль проводиться за відповідним планом, який затверджується Начальником Управління державної охорони України.

2.3. Позаплановий інструментальний контроль проводиться за наказом Начальника Управління державної охорони України, першого заступника Начальника Управління державної охорони України або за рапортами начальників особистих охорон посадових осіб, щодо яких здійснюється державна охорона.

2.4. У разі виявлення під час планового або позапланового інструментального контролю порушення у сфері ТЗІ проводиться контрольна перевірка після отримання повідомлення про усунення порушень від керівників об'єктів "особливої норми", під час якої перевіряються повнота та достатність проведених заходів щодо усунення порушень.

2.5. Контроль за станом ТЗІ здійснюється військовослужбовцями підрозділу ТЗІ Управління.

III. Права військовослужбовців підрозділу ТЗІ Управління державної охорони України

Військовослужбовці підрозділу ТЗІ Управління, які здійснюють контроль за станом ТЗІ, за згодою керівників об'єктів "особливої норми" мають право:

доступу на об'єкти "особливої норми" для здійснення контролю за станом ТЗІ;

ознайомлюватися з документами, необхідними для здійснення контролю за станом ТЗІ;

безкоштовно отримувати копії документів, необхідних для здійснення контролю за станом ТЗІ, письмові пояснення посадових осіб (довідки) з питань, що виникають під час здійснення контролю за станом ТЗІ.

IV. Порядок проведення інструментального контролю

4.1. Під час спеціальних обстежень об'єктів "особливої норми" перевіряються повнота та достатність впроваджених організаційних, організаційно-технічних та технічних заходів із захисту інформації від реальної загрози витоку інформації технічними каналами, у тому числі каналами, що створюються за рахунок застосування закладних пристроїв, відповідність впроваджених заходів вимогам нормативно-правових актів та нормативних документів системи ТЗІ, а також наявність атестаційних документів, які визначають необхідність впровадження заходів захисту інформації.

Під час спеціальних перевірок об'єктів "особливої норми" перевіряється наявність технічних каналів витоку інформації, які створюються за рахунок застосування закладних пристроїв.

Під час спеціальних досліджень технічних засобів, призначених для встановлення на об'єктах "особливої норми", перевіряється відповідність захищеності технічних засобів нормам ефективності захисту інформації від витоку технічними каналами.

4.2. За результатами спеціальних обстежень, спеціальних перевірок об'єктів "особливої норми" та спеціальних досліджень технічних засобів, призначених для встановлення на об'єктах "особливої норми", військовослужбовцями підрозділу ТЗІ Управління, які їх здійснювали, складаються акти, висновки, протоколи вимірювань.

4.3. Акти спеціальних обстежень, спеціальних перевірок об'єктів "особливої норми" та висновки спеціальних досліджень технічних засобів оформлюються в одному примірнику, який залишається в Управлінні. За наказом Начальника Управління державної охорони

України або на письмовий запит керівника об'єкта "особливої норми" копія акта або висновку надсилається керівнику об'єкта "особливої норми", на якому здійснювався контроль за станом ТЗІ.

4.4. Протоколи вимірювань технічних засобів, які проводилися під час спеціальних обстежень, спеціальних перевірок об'єктів "особливої норми" та спеціальних досліджень технічних засобів, призначених для встановлення на об'єктах "особливої норми", оформлюються в одному примірнику та залишаються у підрозділі ТЗІ Управління.

4.5. Усі примірники актів та висновків підписуються військовослужбовцями підрозділу ТЗІ Управління, які проводили контроль за станом ТЗІ, та затверджуються Начальником Управління державної охорони України.

V. Кваліфікація порушень з ТЗІ

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 інформації технічними каналами, тобто за умов підтвердження інструментально-розрахунковими методами наявності технічного каналу поширення інформації з обмеженим доступом;

друга категорія - невиконання вимог нормативно-правових актів та нормативних документів з ТЗІ, унаслідок чого створюються передумови до порушення конфіденційності, зокрема за рахунок витоку інформації технічними каналами, тобто за умов відсутності підтвердження інструментально-розрахунковими методами відповідності комплексу ТЗІ нормам та вимогам з ТЗІ;

третя категорія - невиконання вимог нормативно-правових актів щодо впровадження організаційних заходів з ТЗІ, а також інших вимог у сфері захисту інформації, які не призводять до порушень першої або другої категорії.

VI. Звітність за результатами інструментального контролю та рекомендації щодо запобігання порушенням у сфері ТЗІ

6.1. В актах спеціальних обстежень об'єктів "особливої норми" зазначаються виявлені порушення в сфері ТЗІ на об'єкті "особливої норми", наявні канали поширення інформації, визначається відповідність стану ТЗІ вимогам нормативно-правових актів та нормативним документам системи ТЗІ та надаються рекомендації щодо усунення виявлених порушень у сфері ТЗІ.

6.2. В актах спеціальних перевірок об'єктів "особливої норми" зазначаються відомості про наявність технічних каналів поширення інформації, що створюються за рахунок застосування закладних пристроїв, порушення стану ТЗІ, які створюють передумови до впровадження на об'єкті "особливої норми" закладних пристроїв, та надаються рекомендації щодо упередження можливого впровадження на об'єкті "особливої норми" закладних пристроїв.

6.3. У висновках спеціальних досліджень технічних засобів, призначених для встановлення на об'єктах "особливої норми", визначаються можливість, умови та порядок їх використання на об'єкті "особливої норми".

6.4. Рекомендації Управління щодо усунення виявлених порушень у сфері ТЗІ надсилаються керівникам об'єктів "особливої норми".

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

6.5. Критерії складання висновків за результатами інструментального контролю:

6.5.1. Стан технічного захисту інформації відповідає вимогам нормативно-правових актів. Критерієм висновку є відсутність будь-яких порушень норм та вимог з ТЗІ.

6.5.2. Стан технічного захисту інформації відповідає вимогам нормативно-правових актів за винятком виявлених порушень.

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

6.5.3. Стан технічного захисту інформації не повною мірою відповідає вимогам нормативно-правових актів, що створює передумови для порушення її конфіденційності та (або) витоку технічними каналами.

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

6.5.4. Стан технічного захисту інформації не відповідає вимогам нормативно-правових актів, що створює реальну загрозу порушення її конфіденційності та (або) витоку технічними каналами.

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

6.6. У разі виявлення військовослужбовцями Управління на об'єктах "особливої норми" порушень з ТЗІ першої або другої категорії Управління про виявлені порушення інформує Державну службу спеціального зв'язку та захисту інформації України.

Начальник Відділу технічного захисту інформації Управління державної охорони України підполковник **В. А. Юрченко**

ЗАКОН УКРАЇНИ

Про Національну систему конфіденційного зв'язку

Із змінами і доповненнями, внесеними
Законами України
від 18 листопада 2003 року N 1280-IV,
від 31 травня 2005 року N 2599-IV,
від 15 січня 2009 року N 879-VI

Цей Закон регулює суспільні відносини, пов'язані із створенням, функціонуванням, розвитком та використанням Національної системи конфіденційного зв'язку.

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються в такому значенні:

спеціальна телекомунікаційна система (мережа) - телекомунікаційна система (мережа), призначена для обміну інформацією з обмеженим доступом;

(абзац другий частини першої статті 1 із змінами, внесеними
згідно із Законом України від 31.05.2005 р. N 2599-IV)

спеціальна телекомунікаційна система (мережа) подвійного призначення - спеціальна телекомунікаційна система (мережа), призначена для забезпечення телекомунікацій (електрозв'язку) в інтересах органів державної влади та органів місцевого самоврядування, з використанням частини її ресурсу для надання послуг іншим споживачам;

(абзац третій частини першої статті 1 із змінами, внесеними
згідно із Законом України від 31.05.2005 р. N 2599-IV)

Національна система конфіденційного зв'язку - сукупність спеціальних телекомунікаційних систем (мереж) подвійного призначення, які за допомогою криптографічних та/або технічних засобів забезпечують обмін конфіденційною інформацією в інтересах органів державної влади та органів місцевого самоврядування, створюють належні умови для їх взаємодії в мирний час та у разі введення надзвичайного і воєнного стану;

(абзац четвертий частини першої статті 1 із змінами, внесеними
згідно із Законом України від 31.05.2005 р. N 2599-IV)

суб'єкти Національної системи конфіденційного зв'язку - органи державної влади та органи місцевого самоврядування, юридичні та фізичні особи, що беруть участь у створенні, функціонуванні, розвитку та використанні цієї системи.

абзац шостий частини першої статті 1 виключено

(згідно із Законом України
від 31.05.2005 р. N 2599-IV)

Терміни "оператор" та "мережа зв'язку" у цьому Законі вживаються відповідно у значенні термінів "оператор телекомунікацій" та "телекомунікаційна мережа", визначених у Законі України "Про телекомунікації".

(частина друга статті 1 у редакції
Закону України від 31.05.2005 р. N 2599-IV)

Стаття 2. Сфера дії Закону

Дія цього Закону поширюється на відносини між суб'єктами Національної системи конфіденційного зв'язку, що виникають у зв'язку з її створенням, функціонуванням, розвитком та використанням.

Стаття 3. Законодавство у сфері конфіденційного зв'язку

Відносини, пов'язані із створенням, функціонуванням, розвитком та використанням Національної системи конфіденційного зв'язку, регулюються Конституцією України, законами України "Про інформацію", "Про державну таємницю", "Про захист інформації в автоматизованих системах", "Про телекомунікації", "Про підприємництво", "Про ліцензування певних видів господарської діяльності", цим Законом, іншими законами і нормативно-правовими актами.

(частина перша статті 3 із змінами, внесеними
згідно із Законом України від 31.05.2005 р. N 2599-IV)

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлені інші правила, ніж ті, що передбачені цим Законом, застосовуються правила міжнародного договору.

Стаття 4. Державна підтримка Національної системи конфіденційного зв'язку

Державна підтримка Національної системи конфіденційного зв'язку здійснюється Кабінетом Міністрів України шляхом створення сприятливих правових, економічних та інших умов для стимулювання процесу створення, функціонування, розвитку і використання цієї системи.

Стаття 5. Склад Національної системи конфіденційного зв'язку

Частину першу статті 5 виключено

(згідно із Законом України
від 31.05.2005 р. N 2599-IV)

Складовими Національної системи конфіденційного зв'язку є спеціальні телекомунікаційні системи (мережі), їх фіксовані і мобільні компоненти, централізовані системи захисту інформації та оперативно-технічного управління.

(частина друга статті 5 із змінами, внесеними
згідно із Законом України від 31.05.2005 р. N 2599-IV)

Структура побудови Національної системи конфіденційного зв'язку повинна забезпечувати відокремлення конфіденційної інформації органів державної влади та органів місцевого

самоврядування, інших юридичних та фізичних осіб з використанням криптографічних та/або технічних засобів.

Стаття 6. Управління Національною системою конфіденційного зв'язку

Управління Національною системою конфіденційного зв'язку, її функціонування, розвиток, використання та захист інформації забезпечуються спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації відповідно до законодавства.

(частина перша статті 6 із змінами, внесеними
згідно із Законом України від 15.01.2009 р. N 879-VI)

Централізовані системи захисту інформації та оперативно-технічного управління перебувають у державній власності і не підлягають приватизації.

Власниками інших складових Національної системи конфіденційного зв'язку можуть бути суб'єкти господарської діяльності незалежно від форми власності.

Стаття 7. Надання послуг конфіденційного зв'язку

Послуги конфіденційного зв'язку надаються органам державної влади та органам місцевого самоврядування, державним підприємствам, установам, організаціям, іншим юридичним та фізичним особам на платній основі.

Порядок надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям встановлюється Кабінетом Міністрів України.

Надання послуг конфіденційного зв'язку іншим юридичним та фізичним особам здійснюється відповідно до законодавства на підставі договору між споживачем та оператором.

Послуги конфіденційного зв'язку надаються операторами, які є юридичними особами та мають ліцензії на право надання послуг фіксованого та/або рухомого (мобільного) телефонного зв'язку, а також надання послуг у галузі криптографічного та/або технічного захисту інформації відповідно до законодавства.

(частина четверта статті 7 із змінами, внесеними
згідно із Законом України від 31.05.2005 р. N 2599-IV)

Стаття 8. Відповідальність за порушення законодавства у сфері конфіденційного зв'язку

Особи, винні у порушенні законодавства у сфері конфіденційного зв'язку, несуть дисциплінарну, адміністративну, матеріальну, цивільно-правову або кримінальну відповідальність згідно із законом.

Стаття 9. Фінансове забезпечення Національної системи конфіденційного зв'язку

Фінансування витрат, пов'язаних із створенням, функціонуванням та розвитком Національної системи конфіденційного зв'язку, здійснюється за рахунок коштів Державного бюджету України, що передбачається під час його формування на поточний рік у відповідних розділах окремим рядком, а також за рахунок місцевих бюджетів та інших джерел фінансування, не заборонених законом.

Стаття 10. Міжнародне співробітництво

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації в межах своїх повноважень може брати участь у науково-технічному, зовнішньоекономічному та інших формах співробітництва з питань конфіденційного зв'язку відповідно до державних програм та законодавства України.

(частина перша статті 10 із змінами, внесеними згідно із Законом України від 15.01.2009 р. N 879-VI)

Міжнародне співробітництво у сфері конфіденційного зв'язку здійснюється на основі законодавства та відповідних міжнародних договорів України.

Стаття 11. Прикінцеві положення

1. Цей Закон набирає чинності з дня його опублікування.

2. Кабінету Міністрів України протягом шести місяців з дня набрання чинності цим Законом:

привести свої нормативно-правові акти у відповідність з цим Законом;

відповідно до своєї компетенції забезпечити прийняття нормативно-правових актів, передбачених цим Законом;

забезпечити перегляд і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів, що суперечать цьому Закону.

3. Пункт 3 статті 11 втратив чинність

(у зв'язку з втратою чинності Закону України від 16.05.95 р. N 160/95-ВР згідно із Законом України від 18.11.2003 р. N 1280-IV)

Президент України **Л. КУЧМА**

м. Київ
10 січня 2002 року
N 2919-III

ЗАКОН УКРАЇНИ

Про державну таємницю

Закон введено в дію з дня опублікування - 10 березня 1994 року
(згідно з Постановою Верховної Ради України
від 21 січня 1994 року N 3856-XII)

Із змінами і доповненнями, внесеними
Законами України
від 21 вересня 1999 року N 1079-XIV
(Законом України від 21 вересня 1999 року N 1079-XIV
Закон викладено у новій редакції),
від 19 червня 2003 року N 971-IV,
від 19 лютого 2004 року N 1519-IV,
від 21 травня 2008 року N 293-VI,
від 6 липня 2010 року N 2432-VI,
від 7 жовтня 2010 року N 2592-VI,
від 3 лютого 2011 року N 2978-VI,
від 22 грудня 2011 року N 4212-VI,
від 13 квітня 2012 року N 4652-VI

(У тексті Закону слова "орган державної влади" в усіх відмінках і числах замінено словами "державний орган" у відповідному відмінку і числі згідно із Законом України від 6 липня 2010 року N 2432-VI)

Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються у такому значенні:

державна таємниця (далі також - секретна інформація) - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;

віднесення інформації до державної таємниці - процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обгрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей, включенням цієї інформації до Зводу відомостей, що становлять державну таємницю, та з опублікуванням цього Зводу, змін до нього;

гриф секретності - реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації;

державний експерт з питань таємниць - посадова особа, уповноважена здійснювати відповідно до вимог цього Закону віднесення інформації до державної таємниці у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, зміни ступеня секретності цієї інформації та її розсекречування;

допуск до державної таємниці - оформлення права громадянина на доступ до секретної інформації;

доступ до державної таємниці - надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;

засекречування матеріальних носіїв інформації - введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

Звід відомостей, що становлять державну таємницю, - акт, в якому зведено переліки відомостей, що згідно з рішеннями державних експертів з питань таємниць становлять державну таємницю у визначених цим Законом сферах;

категорія режиму секретності - категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях;

криптографічний захист секретної інформації - вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

матеріальні носії секретної інформації - матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо;

охорона державної таємниці - комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;

режим секретності - встановлений згідно з вимогами цього Закону та інших виданих відповідно до нього нормативно-правових актів єдиний порядок забезпечення охорони державної таємниці;

розсекречування матеріальних носіїв секретної інформації - зняття в установленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом скасування раніше наданого грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

спеціальна експертиза щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, - експертиза, що проводиться з метою визначення в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях наявності умов, передбачених цим Законом, для провадження діяльності, пов'язаної з державною таємницею;

ступінь секретності ("особливої важливості", "цілком таємно", "таємно") - категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою;

технічний захист секретної інформації - вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

Стаття 2. Законодавство України про державну таємницю

Відносини у сфері охорони державної таємниці регулюються Конституцією України, Законом України "Про інформацію", цим Законом, міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України та іншими нормативно-правовими актами.

Стаття 3. Сфера дії Закону

Дія цього Закону поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші державні органи, Верховну Раду Автономної Республіки Крим, Раду міністрів Автономної Республіки Крим, органи місцевого самоврядування, підприємства, установи та організації усіх форм власності, об'єднання громадян (далі - державні органи, органи місцевого самоврядування, підприємства, установи та організації), що провадять діяльність, пов'язану з державною таємницею, громадян України, іноземців та осіб без громадянства, яким у встановленому порядку наданий доступ до державної таємниці.

Передані Україні відомості, що становлять таємницю іноземної держави чи міжнародної організації, охороняються в порядку, передбаченому цим Законом. У разі, якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, установлено інші, ніж передбачені цим Законом, правила охорони таємниці іноземної держави чи міжнародної організації, то застосовуються правила міжнародного договору України.

Стаття 4. Державна політика щодо державної таємниці

Державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики визначає Верховна Рада України.

Стаття 5. Компетенція державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці

Президент України, забезпечуючи національну безпеку, видає укази та розпорядження з питань охорони державної таємниці, віднесених цим Законом та іншими законами до його повноважень.

Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері охорони державної таємниці.

Кабінет Міністрів України спрямовує та координує роботу міністерств, інших органів виконавчої влади щодо забезпечення здійснення державної політики у сфері охорони державної таємниці.

Центральні та місцеві органи виконавчої влади, Рада міністрів Автономної Республіки Крим та органи місцевого самоврядування здійснюють державну політику у сфері охорони державної таємниці в межах своїх повноважень, передбачених законом.

Спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці є Служба безпеки України.

Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій.

Стаття 6. Здійснення права власності на секретну інформацію та її матеріальні носії

Власник секретної інформації або її матеріальних носіїв здійснює своє право власності з урахуванням обмежень, установлених в інтересах національної безпеки України відповідно до цього Закону.

Якщо обмеження права власності на секретну інформацію або її матеріальні носії завдають шкоди їх власнику, відшкодування здійснюється за рахунок держави у порядку та розмірах, що визначаються у договорі між власником такої інформації або її матеріальних носіїв і державним органом (органами), якому державним експертом з питань таємниць надається право приймати рішення щодо суб'єктів, які матимуть доступ до цієї інформації та її матеріальних носіїв. Зазначеним договором також визначаються порядок та умови охорони державної таємниці, включаючи режим секретності під час користування і розпорядження секретною інформацією та її матеріальними носіями, обумовлюється згода власника цієї інформації та її матеріальних носіїв на здійснення права власності з урахуванням обмежень, встановлених відповідно до цього Закону, взяття власником на себе зобов'язання щодо збереження державної таємниці та ознайомлення його з мірою відповідальності за порушення законодавства про державну таємницю.

Якщо власник секретної інформації або її матеріальних носіїв відмовляється від укладення договору чи порушує його, за рішенням суду ця інформація або її матеріальні носії можуть бути вилучені у власність держави за умови попереднього і повного відшкодування власникові їх вартості.

Стаття 7. Фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею

Фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею, в бюджетних установах і організаціях здійснюється за рахунок Державного бюджету України, бюджету Автономної Республіки Крим та місцевих бюджетів. Кошти на зазначені витрати передбачаються у відповідних бюджетах окремим рядком. Зазначені витрати інших установ і організацій, а також підприємств відносяться до валових витрат виробника продукції, виготовлення якої пов'язано з державною таємницею.

Витрати на здійснення заходів щодо віднесення інформації до державної таємниці, засекречування, розсекречування та охорони матеріальних носіїв такої інформації, її криптографічного та технічного захисту, інші витрати, пов'язані з державною таємницею, на недержавних підприємствах, в установах, організаціях фінансуються на підставі договору з замовником робіт, пов'язаних з державною таємницею.

Підприємствам, установам і організаціям, які провадять діяльність, пов'язану з державною таємницею, можуть надаватися податкові та інші пільги в порядку, встановленому законом.

Розділ II. ВІДНЕСЕННЯ ІНФОРМАЦІЇ ДО ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 8. Інформація, що може бути віднесена до державної таємниці

До державної таємниці у порядку, встановленому цим Законом, відноситься інформація:

1) у сфері оборони:

про зміст стратегічних і оперативних планів та інших документів бойового управління, підготовку та проведення військових операцій, стратегічне та мобілізаційне розгортання військ, а також про інші найважливіші показники, які характеризують організацію, чисельність, дислокацію, бойову і мобілізаційну готовність, бойову та іншу військову підготовку, озброєння та матеріально-технічне забезпечення Збройних Сил України та інших військових формувань;

про напрями розвитку окремих видів озброєння, військової і спеціальної техніки, їх кількість, тактико-технічні характеристики, організацію і технологію виробництва, наукові, науково-дослідні та дослідно-конструкторські роботи, пов'язані з розробленням нових зразків озброєння, військової і спеціальної техніки або їх модернізацією, а також про інші роботи, що плануються або здійснюються в інтересах оборони країни;

про дислокацію, характеристики пунктів управління, зміст заходів загальнодержавного та регіонального, у разі необхідності міського і районного рівня, щодо приведення у готовність єдиної державної системи цивільного захисту населення і територій до виконання завдань в особливий період та про організацію системи зв'язку (оповіщення) в особливий період, можливості населених пунктів, регіонів і окремих об'єктів щодо евакуації, розосередження

населення і забезпечення його життєдіяльності; забезпечення виробничої діяльності об'єктів національної економіки у воєнний час;

(абзац четвертий пункту 1 частини першої статті 8
у редакції Закону України від 06.07.2010 р. N 2432-VI)

про геодезичні, гравіметричні, картографічні та гідрометеорологічні дані і характеристики, які мають значення для оборони країни;

2) у сфері економіки, науки і техніки:

про зміст мобілізаційних планів державних органів та органів місцевого самоврядування, мобілізаційні потужності, заходи мобілізаційної підготовки і мобілізації та обсяги їх фінансування, запаси та обсяги постачання стратегічних видів сировини і матеріалів, а також зведені відомості про номенклатуру та рівні накопичення, загальні обсяги поставок, відпуску, закладення, освіження, розміщення і фактичні запаси державного матеріального резерву;

(абзац другий пункту 2 частини першої статті 8
у редакції Закону України від 06.07.2010 р. N 2432-VI)

про використання транспорту, зв'язку, потужностей інших галузей та об'єктів інфраструктури держави в інтересах забезпечення її безпеки;

про плани, зміст, обсяг, фінансування та виконання державного оборонного замовлення;

(абзац четвертий пункту 2 частини першої статті 8 із змінами,
внесеними згідно із Законом України від 06.07.2010 р. N 2432-VI)

про плани, обсяги та інші найважливіші характеристики добування, виробництва та реалізації окремих стратегічних видів сировини і продукції;

про державні запаси дорогоцінних металів монетарної групи, коштовного каміння, валюти та інших цінностей, операції, пов'язані з виготовленням грошових знаків і цінних паперів, їх зберіганням, охороною і захистом від підроблення, обігом, обміном або вилученням з обігу, а також про інші особливі заходи фінансової діяльності держави;

про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, на базі яких можуть бути створені прогресивні технології, нові види виробництва, продукції та технологічних процесів, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України;

3) у сфері зовнішніх відносин:

про директиви, плани, вказівки делегаціям і посадовим особам з питань зовнішньополітичної і зовнішньоекономічної діяльності України, спрямовані на забезпечення її національних інтересів і безпеки;

про військове, науково-технічне та інше співробітництво України з іноземними державами, якщо розголошення відомостей про це завдаватиме шкоди національній безпеці України;

про експорт та імпорт озброєння, військової і спеціальної техніки, окремих стратегічних видів сировини і продукції;

4) у сфері державної безпеки та охорони правопорядку:

про особовий склад органів, що здійснюють оперативно-розшукову або розвідувальну чи контррозвідувальну діяльність;

(абзац другий пункту 4 частини першої статті 8 із змінами,
внесеними згідно із Законом України від 06.07.2010 р. N 2432-VI)

про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової, розвідувальної і контррозвідувальної діяльності; про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність; про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють оперативно-розшукову, розвідувальну і контррозвідувальну діяльність;

(абзац третій пункту 4 частини першої статті 8 із змінами,
внесеними згідно із Законом України від 06.07.2010 р. N 2432-VI)

про організацію та порядок здійснення охорони адміністративних будинків та інших державних об'єктів, посадових та інших осіб, охорона яких здійснюється відповідно до Закону України "Про державну охорону органів державної влади України та посадових осіб";

про систему урядового та спеціального зв'язку;

про організацію, зміст, стан і плани розвитку криптографічного захисту секретної інформації, зміст і результати наукових досліджень у сфері криптографії;

про системи та засоби криптографічного захисту секретної інформації, їх розроблення, виробництво, технологію виготовлення та використання;

про державні шифри, їх розроблення, виробництво, технологію виготовлення та використання;

про організацію режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, державні програми, плани та інші заходи у сфері охорони державної таємниці;

про організацію, зміст, стан і плани розвитку технічного захисту секретної інформації;

про результати перевірок, здійснюваних згідно з законом прокурором у порядку відповідного нагляду за додержанням законів, та про зміст матеріалів оперативно-розшукової діяльності, досудового розслідування та судочинства з питань, зазначених у цій статті сфер;

(абзац одинадцятий пункту 4 частини першої статті 8 із змінами,
внесеними згідно із Законом України від 13.04.2012 р. N 4652-VI)

про інші засоби, форми і методи охорони державної таємниці.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності "особливої важливості", "цілком таємно" та "таємно" лише за умови, що вони належать до категорій, зазначених у частині першій цієї статті, і їх розголошення завдаватиме шкоди інтересам національної безпеки України.

Забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

Не відноситься до державної таємниці інформація:

про стан довкілля, про якість харчових продуктів і предметів побуту;

про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;

про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

про факти порушень прав і свобод людини і громадянина;

про незаконні дії державних органів, органів місцевого самоврядування та їх посадових осіб;

інша інформація, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена.

Стаття 9. Державні експерти з питань таємниць

Державний експерт з питань таємниць здійснює відповідно до вимог цього Закону віднесення інформації у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку до державної таємниці, зміни ступеня секретності цієї інформації та її розсекречування.

Виконання функцій державного експерта з питань таємниць на конкретних посадових осіб покладається:

у Верховній Раді України - Головою Верховної Ради України;

в інших державних органах, Національній академії наук України, на підприємствах, в установах і організаціях - Президентом України за поданням Служби безпеки України на підставі пропозицій керівників відповідних державних органів, Національної академії наук України, підприємств, установ і організацій.

(абзац третій частини другої статті 9 у редакції
Закону України від 19.06.2003 р. N 971-IV)

Втручання в діяльність державного експерта з питань таємниць особи, якій за посадою його підпорядковано, не допускається.

Державний експерт з питань таємниць відповідно до покладених на нього завдань:

1) визначає:

підстави, за якими інформацію має бути віднесено до державної таємниці;

підстави та доцільність віднесення до державної таємниці інформації про винаходи (корисні моделі), призначені для використання у сферах, зазначених у частині першій статті 8 цього Закону;

доцільність віднесення до державної таємниці інформації про винаходи (корисні моделі), що мають подвійне застосування, на підставі порівняльного аналізу ефективності цільового використання та за згодою автора (власника патенту);

ступінь секретності інформації, віднесеної до державної таємниці;

державний орган (органи), якому надається право приймати рішення щодо кола суб'єктів, які матимуть доступ до секретної інформації;

2) готує висновок щодо завданої національній безпеці України шкоди у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації;

(пункт 2 частини четвертої статті 9 у редакції
Закону України від 06.07.2010 р. N 2432-VI)

3) установлює та продовжує строк дії рішення про віднесення інформації до державної таємниці із зазначенням дати її розсекречення;

4) дає Службі безпеки України рішення про зміну ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці у разі, якщо підстави, на яких цю інформацію було віднесено до державної таємниці, перестали існувати;

(пункт 4 частини четвертої статті 9 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

5) затверджує за погодженням із Службою безпеки України розгорнуті переліки відомостей, що становлять державну таємницю, зміни до них, контролює відповідність змісту цих переліків Зводу відомостей, що становлять державну таємницю;

6) розглядає пропозиції державних органів, органів місцевого самоврядування, підприємств, установ, організацій, об'єднань громадян та окремих громадян щодо віднесення інформації до державної таємниці та її розсекречування;

7) затверджує висновки щодо обізнаності з державною таємницею громадян, які мають чи мали допуск до державної таємниці;

8) контролює обгрунтованість і правильність надання документам, виробам та іншим матеріальним носіям інформації, які містять відомості, включені до Зводу відомостей чи розгорнутих переліків відомостей, що становлять державну таємницю, відповідного грифа секретності, своєчасність зміни такого грифа та розсекречування цих носіїв із наданням їм реквізиту "розсекречено";

9) бере участь у розробленні критеріїв визначення шкоди, яку може бути завдано національній безпеці України у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації.

(пункт 9 частини четвертої статті 9 у редакції
Закону України від 06.07.2010 р. N 2432-VI)

Державний експерт з питань таємниць під час виконання покладених на нього функцій зобов'язаний:

1) погоджувати за посередництвом Служби безпеки України свої висновки про скасування рішень щодо віднесення інформації до міждержавних таємниць з відповідними посадовими особами держав - учасниць міжнародних договорів України про взаємне забезпечення збереження міждержавних таємниць та повідомляти їх про прийняті рішення щодо віднесення інформації до державної таємниці, на яку поширено чинність цих договорів;

2) подавати Службі безпеки України не пізніш як через десять днів з моменту підписання рішення про віднесення відомостей до державної таємниці або про скасування цих рішень, а розгорнуті переліки відомостей, що становлять державну таємницю, - у той же строк з моменту їх затвердження;

(пункт 2 частини п'ятої статті 9 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

3) розглядати протягом одного місяця пропозиції Служби безпеки України про віднесення інформації до державної таємниці, скасування чи продовження терміну дії раніше прийнятого рішення про віднесення інформації до державної таємниці;

(пункт 3 частини п'ятої статті 9 у редакції
Закону України від 06.07.2010 р. N 2432-VI)

4) надавати відповідний гриф секретності рішенням про віднесення інформації до державної таємниці та про скасування цих рішень залежно від важливості їх змісту;

(пункт 4 частини п'ятої статті 9 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

5) брати участь у засіданнях державних експертів з питань таємниць;

6) ініціювати питання щодо притягнення до відповідальності посадових осіб, які порушують законодавство України про державну таємницю.

(частину п'яту статті 9 доповнено пунктом 6
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Державний експерт з питань таємниць має право:

1) безперешкодно проводити перевірку виконання державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями, що перебувають у сфері його діяльності, рішень про віднесення інформації до державної таємниці, скасування цих рішень, додержання порядку засекречення інформації та у разі виявлення порушень давати обов'язкові для виконання приписи про їх усунення;

(пункт 1 частини шостої статті 9 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

2) створювати експертні комісії з фахівців і науковців, які мають допуск до державної таємниці, для підготовки проектів рішень про віднесення інформації до державної таємниці, зниження ступеня її секретності та скасування зазначених рішень, висновків щодо обізнаності з державною таємницею громадян, які мають чи мали допуск до державної таємниці, а також для підготовки відповідних висновків у разі розголошення секретної інформації чи втрати матеріальних носіїв такої інформації;

(пункт 2 частини шостої статті 9 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

3) скасовувати безпідставні рішення про надання носію інформації грифа секретності, зміну або скасування цього грифа;

4) клопотати про притягнення до відповідальності посадових осіб, які порушують законодавство України про державну таємницю;

5) одержувати в установленому порядку від державних органів, органів місцевого самоврядування, підприємств, установ та організацій відомості, необхідні для виконання своїх функцій.

Державним експертам з питань таємниць, а також фахівцям, які залучаються до підготовки рішень та висновків державних експертів з питань таємниць, встановлюються додаткові виплати у порядку і розмірах, що визначаються Кабінетом Міністрів України.

(частина сьома статті 9 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Державний експерт з питань таємниць несе персональну відповідальність за законність і обгрунтованість свого рішення про віднесення інформації до державної таємниці або про зниження ступеня секретності такої інформації чи скасування рішення про віднесення її до державної таємниці, а також за умисне неприйняття рішення про віднесення до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України.

(частина восьма статті 9 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Стаття 10. Порядок віднесення інформації до державної таємниці

Віднесення інформації до державної таємниці здійснюється мотивованим рішенням державного експерта з питань таємниць за його власною ініціативою, за зверненням керівників відповідних державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян.

Державний експерт з питань таємниць відносить інформацію до державної таємниці з питань, прийняття рішень з яких належить до його компетенції згідно з посадою. У разі, якщо прийняття рішення про віднесення інформації до державної таємниці належить до компетенції кількох державних експертів з питань таємниць, воно за ініціативою державних

експертів або за пропозицією Служби безпеки України приймається колегіально та ухвалюється простою більшістю голосів. При цьому кожен експерт має право викласти свою думку.

Інформація вважається державною таємницею з часу опублікування Зводу відомостей, що становлять державну таємницю, до якого включена ця інформація, чи зміни до нього у порядку, встановленому цим Законом.

Стаття 11. Рішення державного експерта з питань таємниць

У рішенні державного експерта з питань таємниць про віднесення інформації до державної таємниці зазначаються:

(абзац перший частини першої статті 11 із змінами,
внесеними згідно із Законом України від 06.07.2010 р. N 2432-VI)

інформація, яка має становити державну таємницю, та її відповідність категоріям і вимогам, передбаченим статтею 8 цього Закону;

підстави для віднесення інформації до державної таємниці та обгрунтування шкоди національній безпеці України у разі її розголошення;

ступінь секретності зазначеної інформації;

обсяг фінансування заходів, необхідних для охорони такої інформації;

державний орган, орган місцевого самоврядування, підприємство, установа, організація чи громадянин, який вніс пропозицію про віднесення цієї інформації до державної таємниці, та державний орган (органи), якому надається право визначати коло суб'єктів, які матимуть доступ до цієї інформації;

строк, протягом якого діє рішення про віднесення інформації до державної таємниці.

Рішення про віднесення інформації до державної таємниці, продовження строку дії раніше прийнятого рішення про віднесення інформації до державної таємниці, зміну ступеня секретності інформації, скасування раніше прийнятого рішення про віднесення інформації до державної таємниці приймаються державним експертом з питань таємниць протягом одного місяця з часу надходження звернення державного органу, органу місцевого самоврядування, підприємства, установи, організації чи громадянина. Такі рішення підлягають реєстрації Службою безпеки України та є підставою для формування Зводу відомостей, що становлять державну таємницю, і внесення змін до зазначеного Зводу, до галузевих або відомчих розгорнутих переліків відомостей, що становлять державну таємницю. Порядок реєстрації рішень державних експертів з питань таємниць визначається Кабінетом Міністрів України.

(частина друга статті 11 у редакції
Закону України від 06.07.2010 р. N 2432-VI)

Частину третю статті 11 виключено

(згідно із Законом України
від 06.07.2010 р. N 2432-VI)

Частину четверту статті 11 виключено

(згідно із Законом України
від 06.07.2010 р. N 2432-VI)

Частину п'яту статті 11 виключено

(згідно із Законом України
від 06.07.2010 р. N 2432-VI)

Стаття 12. Звід відомостей, що становлять державну таємницю

Звід відомостей, що становлять державну таємницю, формує Служба безпеки України на підставі рішень державних експертів з питань таємниць. Зазначений Звід та зміни до нього набирають чинності з моменту опублікування в офіційних виданнях України.

(частина перша статті 12 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Зміни до Зводу відомостей, що становлять державну таємницю, вносяться не пізніше трьох місяців з дня одержання Службою безпеки України відповідного рішення державного експерта з питань таємниць.

(частина друга статті 12 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Зразки форм рішень державних експертів з питань таємниць, порядок та механізм формування Зводу відомостей, що становлять державну таємницю, і його опублікування визначаються Кабінетом Міністрів України.

(частина третя статті 12 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

На підставі та в межах Зводу відомостей, що становлять державну таємницю, з метою конкретизації та систематизації даних про секретну інформацію державні органи створюють галузеві або відомчі розгорнуті переліки відомостей, що становлять державну таємницю, а також можуть створювати міжгалузеві або міжвідомчі розгорнуті переліки відомостей, що становлять державну таємницю. Підприємства, установи та організації незалежно від форм власності, що провадять діяльність, пов'язану із державною таємницею, за ініціативою та погодженням із замовником робіт, пов'язаних з державною таємницею, можуть створювати власні розгорнуті переліки відомостей, що становлять державну таємницю. Такі переліки погоджуються із Службою безпеки України, затверджуються державними експертами з питань таємниць та реєструються у Службі безпеки України.

Розгорнуті переліки відомостей, що становлять державну таємницю, не можуть суперечити Зводу відомостей, що становлять державну таємницю.

У разі включення до Зводу відомостей, що становлять державну таємницю, або до розгорнутих переліків цих відомостей інформації, яка не відповідає категоріям і вимогам, передбаченим статтею 8 цього Закону, або порушення встановленого порядку віднесення інформації до державної таємниці заінтересовані громадяни та юридичні особи мають право

оскаржити відповідні рішення до суду. З метою недопущення розголошення державної таємниці судовий розгляд скарг може проводитися в закритих засіданнях відповідно до закону.

Стаття 13. Строк дії рішення про віднесення інформації до державної таємниці

Строк, протягом якого діє рішення про віднесення інформації до державної таємниці, встановлюється державним експертом з питань таємниць з урахуванням ступеня секретності інформації, критерії визначення якого встановлюються Службою безпеки України, та інших обставин. Він не може перевищувати для інформації із ступенем секретності "особливої важливості" - 30 років, для інформації "цілком таємно" - 10 років, для інформації "таємно" - 5 років.

Після закінчення передбаченого частиною першою цієї статті строку дії рішення про віднесення інформації до державної таємниці державний експерт з питань таємниць приймає рішення про скасування рішення про віднесення її до державної таємниці або приймає рішення про продовження строку дії зазначеного рішення в межах строків, встановлених частиною першою цієї статті.

(частина друга статті 13 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Президент України з власної ініціативи або на підставі пропозицій державних експертів з питань таємниць чи за зверненням державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян може встановлювати більш тривалі строки дії рішень про віднесення інформації до державної таємниці, ніж строки, передбачені частиною першою цієї статті.

Стаття 14. Зміна ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці

Підвищення або зниження ступеня секретності інформації та скасування рішення про віднесення її до державної таємниці здійснюються на підставі рішення державного експерта з питань таємниць або на підставі рішення суду у випадках, передбачених статтею 12 цього Закону, та оформляються Службою безпеки України шляхом внесення відповідних змін до Зводу відомостей, що становлять державну таємницю.

(частина перша статті 14 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Інформація вважається державною таємницею з більш високим чи нижчим ступенем секретності або такою, що не становить державної таємниці, з часу опублікування відповідних змін до Зводу відомостей, що становлять державну таємницю.

Розділ III. ЗАСЕКРЕЧУВАННЯ ТА РОЗСЕКРЕЧУВАННЯ МАТЕРІАЛЬНИХ НОСІЇВ ІНФОРМАЦІЇ

Стаття 15. Засекречування та розсекречування матеріальних носіїв інформації

Засекречування матеріальних носіїв інформації здійснюється шляхом надання на підставі Зводу відомостей, що становлять державну таємницю (розгорнутих переліків відомостей, що становлять державну таємницю), відповідному документу, виробу або іншому матеріальному носію інформації грифа секретності посадовою особою, яка готує або створює документ, виріб або інший матеріальний носій інформації.

(частина перша статті 15 у редакції
Закону України від 06.07.2010 р. N 2432-VI)

Гриф секретності кожного матеріального носія секретної інформації повинен відповідати ступеню секретності інформації, яка у ньому міститься, згідно із Зводом відомостей, що становлять державну таємницю, - "особливої важливості", "цілком таємно" або "таємно". Реквізити кожного матеріального носія секретної інформації складаються із:

грифа секретності;

номера примірника;

статті Зводу відомостей, що становлять державну таємницю, на підставі якої здійснюється засекречення;

найменування посади та підпису особи, яка надала гриф секретності.

(частина друга статті 15 у редакції
Закону України від 06.07.2010 р. N 2432-VI)

Якщо реквізити, зазначені у частині другій цієї статті, неможливо нанести безпосередньо на матеріальний носій секретної інформації, вони мають бути зазначені у супровідних документах.

Забороняється надавати грифи секретності, передбачені цим Законом, матеріальним носіям іншої таємної інформації, яка не становить державної таємниці, або конфіденційної інформації.

Перелік посад, перебування на яких дає посадовим особам право надавати матеріальним носіям секретної інформації грифи секретності, затверджується керівником державного органу, органу місцевого самоврядування, підприємства, установи, організації, що провадить діяльність, пов'язану з державною таємницею.

(частина п'ята статті 15 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Ступені секретності науково-дослідних, дослідно-конструкторських і проектних робіт, які виконуються в інтересах забезпечення національної безпеки та оборони держави, встановлюються шляхом винесення відповідного висновку державним експертом з питань таємниць, який виконує свої функції у сфері діяльності замовника, разом з підрядником.

(частина шоста статті 15 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Після закінчення встановлених строків засекречування матеріальних носіїв інформації та у разі підвищення чи зниження визначеного державним експертом з питань таємниць ступеня секретності такої інформації або скасування рішення про віднесення її до державної таємниці керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, у яких здійснювалося засекречування матеріальних носіїв інформації, або керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, які є їх правонаступниками, чи керівники вищого рівня зобов'язані протягом шести місяців забезпечити зміну грифа секретності або розсекречування цих матеріальних носіїв секретної інформації та письмово повідомити про це керівників державних органів, органів місцевого самоврядування, підприємств, установ, організацій, яким були передані такі матеріальні носії секретної інформації.

Стаття 16. Строк засекречування матеріальних носіїв інформації

Строк засекречування матеріальних носіїв інформації має відповідати строку дії рішення про віднесення інформації до державної таємниці, встановленого рішенням державного експерта з питань таємниць.

Перебіг строку засекречування матеріальних носіїв інформації починається з часу надання їм грифа секретності.

Стаття 17. Оскарження рішення щодо засекречування матеріальних носіїв інформації

Громадяни та юридичні особи мають право внести посадовим особам, які надали гриф секретності матеріальному носію секретної інформації, обов'язкову для розгляду мотивовану пропозицію про розсекречування цього носія інформації. Зазначені посадові особи повинні протягом одного місяця дати громадянину чи юридичній особі письмову відповідь з цього приводу.

Рішення про засекречування матеріального носія інформації може бути оскаржено громадянином чи юридичною особою в порядку підлеглості вищому органу або посадовій особі чи до суду. У разі незадоволення скарги, поданої в порядку підлеглості, громадянин або юридична особа мають право оскаржити рішення вищого органу або посадової особи до суду.

Розділ IV. ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ

Стаття 18. Основні організаційно-правові заходи щодо охорони державної таємниці

З метою охорони державної таємниці впроваджуються:

єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;

дозвільний порядок провадження державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями діяльності, пов'язаної з державною таємницею;

обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;

обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до державної таємниці, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;

особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, діяльність яких пов'язана з державною таємницею;

режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею;

спеціальний порядок допуску та доступу громадян до державної таємниці;

технічний та криптографічний захисти секретної інформації.

Стаття 19. Єдині вимоги до матеріальних носіїв секретної інформації

Єдині вимоги до виготовлення, обліку, користування, зберігання, схоронності, передачі та транспортування матеріальних носіїв секретної інформації встановлюються Кабінетом Міністрів України.

Стаття 20. Дозвільний порядок провадження діяльності, пов'язаної з державною таємницею, та режим секретності

Державні органи, органи місцевого самоврядування, підприємства, установи, організації мають право провадити діяльність, пов'язану з державною таємницею, після надання їм Службою безпеки України спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею.

Надання дозволу здійснюється на підставі заявок державних органів, органів місцевого самоврядування, підприємств, установ і організацій та результатів спеціальної експертизи щодо наявності умов для провадження діяльності; пов'язаної з державною таємницею. З метою визначення наявності умов для провадження діяльності, пов'язаної з державною таємницею, Служба безпеки України може створювати спеціальні експертні комісії, до складу яких включати фахівців державних органів, органів місцевого самоврядування, підприємств, установ і організацій за погодженням з їх керівниками. Результати спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, оформляються відповідним актом.

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, надається державним органам, органам місцевого самоврядування, підприємствам, установам, організаціям за результатами спеціальної експертизи за умови, що вони:

відповідно до компетенції, державних завдань, програм, замовлень, договорів (контрактів) беруть участь у діяльності, пов'язаній з державною таємницею;

мають приміщення для проведення робіт, пов'язаних з державною таємницею, сховища для зберігання засекречених документів та інших матеріальних носіїв секретної інформації, що відповідають вимогам щодо забезпечення секретності зазначених робіт, виключають можливість доступу до них сторонніх осіб, гарантують збереження носіїв секретної інформації;

додержуються передбачених законодавством вимог режиму секретності робіт та інших заходів, пов'язаних з використанням секретної інформації, порядку допуску осіб до державної таємниці, прийому іноземних громадян, а також порядку здійснення технічного та криптографічного захисту секретної інформації;

(абзац четвертий частини третьої статті 20 із змінами,
внесеними згідно із Законом України від 06.07.2010 р. N 2432-VI)

мають режимно-секретний орган, якщо інше не передбачено цим Законом.

Керівники державних органів, органів місцевого самоврядування, підприємств, установ, організацій, що провадять діяльність, пов'язану з державною таємницею, мають бути обізнані з чинним законодавством про державну таємницю.

Термін дії дозволу на провадження діяльності, пов'язаної з державною таємницею, встановлюється Службою безпеки України і не може перевищувати 5 років. Його тривалість залежить від обсягу робіт (діяльності), що здійснюються державним органом, органом місцевого самоврядування, підприємством, установою, організацією, ступеня секретності та обсягу пов'язаних з цими роботами (діяльністю) відомостей, що становлять державну таємницю, а також категорії режиму секретності.

(частина п'ята статті 20 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, не надається, якщо відсутні умови для провадження такої діяльності, передбачені цією статтею, а також якщо керівник підприємства, установи, організації не є громадянином України або не має допуску до державної таємниці.

(статтю 20 доповнено новою частиною шостою
згідно із Законом України від 06.07.2010 р. N 2432-VI,
у зв'язку з цим частини шосту - дев'яту
вважати відповідно частинами сьомою - десятою)

Дозвіл на провадження діяльності, пов'язаної з державною таємницею, може бути скасований або його дія може бути зупинена Службою безпеки України на підставі акта проведеної нею перевірки, висновки якого містять дані про недодержання державним органом, органом місцевого самоврядування, підприємством, установою, організацією умов, передбачених цією статтею.

(частина сьома статті 20 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Державним органам, органам місцевого самоврядування, підприємствам, установам, організаціям, що провадять діяльність, пов'язану з державною таємницею, за результатами спеціальної експертизи надаються відповідні категорії режиму секретності (перша, друга або третя), що зазначаються Службою безпеки України у дозволах на провадження діяльності, пов'язаної з державною таємницею.

(частина восьма статті 20 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Державні органи, органи місцевого самоврядування, підприємства, установи і організації, яким надано зазначений у цій статті дозвіл, набувають права на доступ до конкретної секретної інформації згідно з рішенням державних органів, уповноважених державним експертом з питань таємниць приймати такі рішення. За погодженням з цими органами здійснюється передача секретної інформації або її матеріальних носіїв державним органам, органам місцевого самоврядування, підприємствам, установам і організаціям, які мають дозвіл на провадження діяльності, пов'язаної з державною таємницею.

Порядок надання, переоформлення, призупинення та поновлення дії або скасування дозволу на провадження діяльності, пов'язаної з державною таємницею, форма акта спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею, форма дозволу на провадження діяльності, пов'язаної з державною таємницею, та категорії режиму секретності встановлюються Кабінетом Міністрів України.

(частина десята статті 20 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Стаття 21. Режимно-секретні органи

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, що провадять діяльність, пов'язану з державною таємницею, з метою розроблення та здійснення заходів щодо забезпечення режиму секретності, постійного контролю за їх додержанням створюються на правах окремих структурних підрозділів режимно-секретні органи (далі - РСО), які підпорядковуються безпосередньо керівнику державного органу, органу місцевого самоврядування, підприємства, установи, організації.

(частина перша статті 21 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Створення, реорганізація чи ліквідація РСО здійснюються за погодженням із Службою безпеки України. У своїй роботі РСО взаємодіють з органами Служби безпеки України.

До складу РСО входять підрозділи режиму, секретного діловодства та інші підрозділи, що безпосередньо забезпечують охорону державних таємниць, залежно від специфіки діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації.

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях із значним обсягом робіт, пов'язаних з державною таємницею, вводиться посада заступника керівника з питань режиму, на якого покладаються обов'язки та права керівника РСО.

В державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях з незначним обсягом робіт, пов'язаних з державною таємницею, де штатним

розписом не передбачено створення РСО, облік і зберігання секретних документів, а також заходи щодо забезпечення режиму секретності здійснюються особисто їх керівниками або спеціально призначеним наказом керівника працівником після створення необхідних умов, що забезпечують режим секретності. На них поширюються обов'язки та права працівників РСО.

Призначення осіб на посади заступників керівників з питань режиму, начальників РСО і їх заступників, а також видання наказу про покладення на окремого працівника обов'язків щодо забезпечення режиму секретності здійснюється за погодженням з органами Служби безпеки України та РСО вищестоящих державних органів, органів місцевого самоврядування, підприємств, установ і організацій.

РСО комплектуються спеціалістами, яким надано допуск до державної таємниці із ступенем секретності "цілком таємно", якщо характер виконуваних робіт не вимагає допуску до державної таємниці із ступенем секретності "особливої важливості". Якщо державний орган, орган місцевого самоврядування, підприємство, установа або організація не провадить діяльність із секретною інформацією, що має ступені секретності "цілком таємно" та "особливої важливості", РСО такого органу, підприємства, установи або організації комплектується спеціалістами, яким надано допуск до державної таємниці зі ступенем секретності "таємно".

(частина сьома статті 21 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Основними завданнями РСО є:

а) недопущення необгрунтованого допуску та доступу осіб до секретної інформації;

б) своєчасне розроблення та реалізація разом з іншими структурними підрозділами державних органів, органів місцевого самоврядування, підприємств, установ і організацій заходів, що забезпечують охорону державної таємниці;

в) запобігання розголошенню секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодінню секретною інформацією іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуску та доступу до неї;

г) виявлення та закриття каналів просочення секретної інформації в процесі діяльності державних органів, органів місцевого самоврядування, підприємства, установи, організації;

д) забезпечення запровадження заходів режиму секретності під час виконання всіх видів робіт, пов'язаних з державною таємницею, та під час здійснення зовнішніх відносин;

е) організація та ведення секретного діловодства;

(пункт "е" частини восьмої статті 21 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

є) здійснення контролю за станом режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях та на підпорядкованих їм об'єктах.

РСО мають право:

а) вимагати від усіх працівників державного органу, органу місцевого самоврядування, підприємства, установи та організації, а також відряджених неухильного виконання вимог законодавства щодо забезпечення охорони державної таємниці;

б) брати участь у розгляді проектів штатних розписів державного органу, органу місцевого самоврядування, підприємства, установи та організації та підвідомчих їм установ, підприємств у частині, що стосується РСО, вносити пропозиції щодо структури та чисельності працівників цих органів;

в) брати участь у проведенні атестації працівників, що виконують роботи, пов'язані з державною таємницею, а також у розгляді пропозицій щодо виплати в установленому нормативними актами порядку компенсації за роботу в умовах режимних обмежень;

г) залучати спеціалістів державного органу, органу місцевого самоврядування, підприємства, установи та організації до здійснення заходів щодо охорони державної таємниці;

д) здійснювати перевірки стану й організації роботи з питань захисту державної таємниці і забезпечення режиму секретності у підрозділах державного органу, органу місцевого самоврядування, підприємства, установи та організації, а також у підвідомчих їм установах та підприємствах, давати відповідні рекомендації;

е) здійснювати перевірки додержання режиму секретності на робочих місцях працівників, що мають допуск до державної таємниці, вмісту спецсховищ (приміщень, сейфів, металевих шаф, спецчемоданів, спецпапок тощо), наявності документів, виробів та інших матеріальних носіїв секретної інформації;

є) порушувати перед керівником державного органу, органу місцевого самоврядування, підприємства, установи та організації питання про призначення службових розслідувань за фактами порушень режиму секретності та секретного діловодства, про притягнення осіб до відповідальності згідно з законом, а також давати рекомендації щодо обов'язкових для виконання вказівок керівникам підрозділів державного органу, органу місцевого самоврядування, підприємства, установи та організації та підвідомчих їм установ, підприємств з питань забезпечення режиму секретності;

ж) брати участь у службових розслідуваннях, у встановленому порядку вимагати від працівників державного органу, органу місцевого самоврядування, підприємства, установи та організації письмових пояснень щодо фактів розголошення ними секретних відомостей, втрати матеріальних носіїв секретної інформації, інших порушень режиму секретності;

з) вносити пропозиції керівникові державного органу, органу місцевого самоврядування, підприємства, установи та організації про припинення робіт, пов'язаних з державною таємницею, в структурних підрозділах, якщо умови для їх виконання не відповідають вимогам режиму секретності; опечатувати приміщення, де ведуться такі роботи або зберігаються матеріальні носії секретної інформації;

и) одержувати від громадян, яким оформляються документи на допуск до державної таємниці, анкетні дані;

і) використовувати засоби зв'язку та вести в установленому порядку поштово-телеграфне листування з іншими державними органами, органами місцевого самоврядування,

підприємствами, установами і організаціями та їх РСО з питань забезпечення режиму секретності;

ї) мати печатку з найменуванням РСО, а також інші печатки та штампи установленої форми.

Передача функцій РСО будь-яким іншим підрозділам державного органу, органу місцевого самоврядування, підприємства, установи та організації не допускається.

Стаття 22. Допуск громадян до державної таємниці

Залежно від ступеня секретності інформації встановлюються такі форми допуску до державної таємниці:

форма 1 - для роботи з секретною інформацією, що має ступені секретності "особливої важливості", "цілком таємно" та "таємно";

форма 2 - для роботи з секретною інформацією, що має ступені секретності "цілком таємно" та "таємно";

форма 3 - для роботи з секретною інформацією, що має ступінь секретності "таємно",

а також такі терміни дії допусків:

для форми 1 - 5 років;

для форми 2 - 7 років;

(абзац сьомий частини першої статті 22 із змінами,
внесеними згідно із Законом України від 06.07.2010 р. N 2432-VI)

для форми 3 - 10 років.

(абзац восьмий частини першої статті 22 із змінами,
внесеними згідно із Законом України від 06.07.2010 р. N 2432-VI)

Допуск до державної таємниці надається дієздатним громадянам України віком від 18 років, які потребують його за умовами своєї службової, виробничої, наукової чи науково-технічної діяльності або навчання, органами Служби безпеки України після проведення їх перевірки. Порядок надання допуску до державної таємниці визначається Кабінетом Міністрів України.

(частина друга статті 22 у редакції
Закону України від 06.07.2010 р. N 2432-VI)

В окремих випадках, які визначаються міністерствами, іншими центральними органами виконавчої влади, за погодженням із Службою безпеки України громадянам України віком від 16 років може надаватися допуск до державної таємниці із ступенями секретності "цілком таємно" та "таємно", а віком від 17 років - також до державної таємниці із ступенем секретності "особливої важливості".

Для розгляду питання про надання громадянам допуску до державної таємниці державними органами, органами місцевого самоврядування, підприємствами, установами, організаціями,

де працюють, проходять службу або навчаються громадяни, оформляються документи, які надсилаються до органів Служби безпеки України. Перелік та форми таких документів, а також порядок їх надання визначаються Кабінетом Міністрів України.

(частина четверта статті 22 із змінами, внесеними
згідно із Законами України від 21.05.2008 р. N 293-VI,
від 07.10.2010 р. N 2592-VI,
у редакції Закону України
від 06.07.2010 р. N 2432-VI)

Допуск до державної таємниці під час застосування до боржника судових процедур банкрутства у встановленому законодавством порядку надається органами Служби безпеки України арбітражному керуючому (розпоряднику майна, керуючому санацією, ліквідатору) після проведення його перевірки за поданням державного органу, органу місцевого самоврядування, підприємства, установи, організації, до сфери управління якого (якої) належить боржник або який (яка) є замовником робіт, пов'язаних з державною таємницею.

(статтю 22 доповнено новою частиною п'ятою
згідно із Законом України від 22.12.2011 р. N 4212-VI,
у зв'язку з цим частини п'яту - сьому
вважати відповідно частинами шостою - восьмою)

Якщо потреба громадянина у відомостях, що становлять державну таємницю, не пов'язана з місцем роботи, служби або навчання, документи про надання допуску до державної таємниці можуть оформлятися за місцем провадження діяльності, пов'язаної з державною таємницею.

(частина шоста статті 22 із змінами, внесеними
згідно із Законом України від 03.02.2011 р. N 2978-VI)

Надання допуску передбачає:

визначення необхідності роботи громадянина із секретною інформацією;

перевірку громадянина у зв'язку з допуском до державної таємниці;

взяття громадянином на себе письмового зобов'язання щодо збереження державної таємниці, яка буде йому довірена;

одержання у письмовій формі згоди громадянина на передбачені законом обмеження прав у зв'язку з його допуском до державної таємниці;

ознайомлення громадянина з мірою відповідальності за порушення законодавства про державну таємницю.

Частину восьму статті 22 виключено

(згідно із Законом України
від 06.07.2010 р. N 2432-VI)

Стаття 23. Відмова у наданні допуску до державної таємниці

Допуск до державної таємниці не надається у разі:

1) відсутності у громадянина обгрунтованої необхідності в роботі із секретною інформацією;

2) сприяння громадянином діяльності іноземної держави, іноземної організації чи їх представників, а також окремих іноземців чи осіб без громадянства, що завдає шкоди інтересам національної безпеки України, або участі громадянина в діяльності політичних партій та громадських організацій, діяльність яких заборонена у порядку, встановленому законом;

3) відмови громадянина взяти на себе письмове зобов'язання щодо збереження державної таємниці, яка буде йому довірена, а також за відсутності його письмової згоди на передбачені законом обмеження прав у зв'язку з допуском до державної таємниці;

4) наявності у громадянина судимості за тяжкі або особливо тяжкі злочини, не погашеної чи не знятої в установленому порядку;

(пункт 4 частини четвертої статті 23 у редакції
Закону України від 06.07.2010 р. N 2432-VI)

5) наявності у громадянина психічних розладів, які можуть завдати шкоди охороні державної таємниці, відповідно до переліку, затвердженого Міністерством охорони здоров'я України і Службою безпеки України.

(пункт 5 частини першої статті 23 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

У наданні допуску до державної таємниці може бути відмовлено також у разі:

1) повідомлення громадянином під час оформлення допуску недостовірних відомостей про себе;

2) постійного проживання громадянина за кордоном або оформлення ним документів на виїзд для постійного проживання за кордоном;

3) невиконання громадянином обов'язків щодо збереження державної таємниці, яка йому довірена або довірялася раніше.

Громадянина, якому відмовлено у допуску до державної таємниці, якщо виконання трудових чи службових обов'язків вимагає доступу до державної таємниці, а переміщення на інше робоче місце чи іншу посаду неможливе, може бути в передбаченому законодавством порядку переведено на іншу роботу або службу, не пов'язану з державною таємницею, чи звільнено.

(статтю 23 доповнено частиною третьою згідно із
Законом України від 03.02.2011 р. N 2978-VI)

Стаття 24. Перевірка громадян у зв'язку з допуском їх до державної таємниці

Перевірка громадян у зв'язку з їх допуском до державної таємниці здійснюється органами Служби безпеки України у двомісячний строк у порядку, встановленому цим Законом і Законом України "Про оперативно-розшукову діяльність".

(частина перша статті 24 із змінами, внесеними
згідно із Законом України від 03.02.2011 р. N 2978-VI)

У ході перевірки органами Служби безпеки України з'ясовуються наявність чи відсутність обставин, передбачених пунктами 2 і 4 частини першої та частиною другою статті 23 цього Закону. За результатами перевірки органи Служби безпеки України надсилають протягом п'яти робочих днів з дня її закінчення до державних органів, органів місцевого самоврядування, підприємств, установ, організацій, що звернулися з приводу надання громадянам допуску до державної таємниці, повідомлення про надання або відмову в наданні такого допуску.

(частина друга статті 24 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Наявність чи відсутність обставин, передбачених пунктами 1, 3 і 5 частини першої статті 23 цього Закону, з'ясовується державним органом, органом місцевого самоврядування, підприємством, установою, організацією, що оформляє документи на допуск.

(частина третя статті 24 із змінами, внесеними
згідно із Законом України від 03.02.2011 р. N 2978-VI)

Повідомлення органів Служби безпеки України про відмову в наданні громадянам допуску до державної таємниці мають містити посилання на відповідні положення статті 23 цього Закону. Відмова не виключає повторного звернення державних органів, органів місцевого самоврядування, підприємств, установ, організацій з цього приводу в разі зміни обставин, за яких у наданні допуску до державної таємниці було відмовлено.

(частина четверта статті 24 у редакції
Закону України від 06.07.2010 р. N 2432-VI)

Стаття 25. Оскарження громадянином відмови у наданні допуску до державної таємниці

Державний орган, орган місцевого самоврядування, підприємство, установа, організація зобов'язані у п'ятиденний строк з дня надходження повідомлення органу Служби безпеки України про відмову у наданні громадянину допуску до державної таємниці письмово повідомити такого громадянина про причини і підстави відмови.

Громадянин має право оскаржити рішення про відмову у наданні допуску до державної таємниці в порядку, встановленому законом.

(стаття 25 у редакції Закону
України від 06.07.2010 р. N 2432-VI)

Стаття 26. Переоформлення допуску до державної таємниці, підвищення або зниження його форми та скасування

(назва статті 26 у редакції Закону України від 06.07.2010 р. N 2432-VI)

Переоформлення громадянам допуску до державної таємниці здійснюється:

у разі закінчення терміну дії допуску до державної таємниці за необхідності подальшої роботи з секретною інформацією;

у разі необхідності підвищення чи зниження громадянину форми допуску для роботи із секретною інформацією вищого чи нижчого ступеня секретності;

(абзац третій частини першої статті 26 у редакції Закону України від 06.07.2010 р. N 2432-VI)

у разі необхідності проведення додаткової перевірки, пов'язаної з можливим виникненням обставин, передбачених пунктами 2 і 4 частини першої та частиною другою статті 23 цього Закону.

Скасування раніше наданого допуску до державної таємниці здійснюється органами Служби безпеки України у разі виникнення або виявлення обставин, передбачених статтею 23 цього Закону, або після припинення громадянином діяльності, у зв'язку з якою йому було надано допуск, втрати ним громадянства або визнання його недієздатним на підставі інформації, здобутої органами Служби безпеки України або отриманої від державних органів, органів місцевого самоврядування, підприємств, установ, організацій.

(частина друга статті 26 у редакції Закону України від 06.07.2010 р. N 2432-VI)

На прохання громадянина його допуск до державної таємниці скасовується протягом трьох днів з часу звернення з приводу скасування допуску.

Повідомлення про скасування громадянину допуску до державної таємниці з посиланням на відповідні положення статті 23 цього Закону орган Служби безпеки України надсилає до державного органу, органу місцевого самоврядування, підприємства, установи, організації, де такий громадянин провадить діяльність, пов'язану з державною таємницею. Громадянин має право оскаржити скасування йому допуску до державної таємниці в порядку, встановленому законом.

(частина четверта статті 26 у редакції Закону України від 06.07.2010 р. N 2432-VI)

Громадянина, якому скасовано допуск до державної таємниці, якщо виконання трудових чи службових обов'язків вимагає доступу до державної таємниці, а переміщення на інше робоче місце чи іншу посаду неможливе, може бути в передбаченому законодавством порядку переведено на іншу роботу або службу, не пов'язану з державною таємницею, чи звільнено.

Порядок надання, переоформлення та скасування громадянам допуску до державної таємниці встановлюється Кабінетом Міністрів України.

Стаття 27. Доступ громадян до державної таємниці

Доступ до державної таємниці надається дієздатним громадянам України, яким надано допуск до державної таємниці та які потребують його за умовами своєї службової, виробничої, наукової чи науково-дослідної діяльності або навчання.

Рішення про надання доступу до конкретної секретної інформації (категорії секретної інформації) та її матеріальних носіїв приймають керівники державних органів, органів місцевого самоврядування, підприємств, установ та організацій, у яких виконуються роботи, пов'язані з державною таємницею, або зберігаються матеріальні носії секретної інформації.

(частина друга статті 27 у редакції
Закону України від 06.07.2010 р. N 2432-VI)

Керівники державних органів, за винятком осіб, передбачених частиною шостою цієї статті, органів місцевого самоврядування, підприємств, установ та організацій доступ до державної таємниці у сфері, що стосується діяльності державного органу, органу місцевого самоврядування, підприємства, установи та організації, отримують за посадою після надання їм допуску до державної таємниці за відповідною формою.

(статтю 27 доповнено новою частиною третьою
згідно із Законом України від 06.07.2010 р. N 2432-VI)

Порядок надання доступу до державної таємниці особам, залученим до конфіденційного співробітництва з оперативними підрозділами правоохоронних та інших спеціально уповноважених органів, які проводять оперативно-розшукову, розвідувальну або контррозвідувальну діяльність, визначається керівниками зазначених органів за погодженням із Службою безпеки України. У Службі безпеки України такий порядок надання доступу до державної таємниці визначається Головою Служби безпеки України.

(статтю 27 доповнено новою частиною четвертою
згідно із Законом України від 06.07.2010 р. N 2432-VI,
у зв'язку з цим частини третю - п'яту
вважати відповідно частинами п'ятою - сьомою)

Відмова надати громадянинові України доступ до конкретної секретної інформації та її матеріальних носіїв можлива лише у разі відсутності підстав, передбачених частиною першою цієї статті, та може бути оскаржена в порядку, встановленому частиною другою статті 25 цього Закону.

Президентові України, Голові Верховної Ради України, Прем'єр-міністрові України та іншим членам Кабінету Міністрів України, Голові Верховного Суду України, Голові Конституційного Суду України, Генеральному прокурору України, Голові Служби безпеки України, народним депутатам України доступ до державної таємниці усіх ступенів секретності надається за посадою після взяття ними письмового зобов'язання щодо збереження державної таємниці.

(частина шоста статті 27 із змінами, внесеними
згідно із Законами України від 19.02.2004 р. N 1519-IV,
від 21.05.2008 р. N 293-VI)

Іноземцям та особам без громадянства доступ до державної таємниці надається у виняткових випадках на підставі міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України, або письмового розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України.

Стаття 28. Обов'язки громадянина щодо збереження державної таємниці

Громадянин, якому надано допуск до державної таємниці, зобов'язаний:

не допускати розголошення будь-яким способом державної таємниці, яка йому довірена або стала відомою у зв'язку з виконанням службових обов'язків;

не брати участі в діяльності політичних партій та громадських організацій, діяльність яких заборонена в порядку, встановленому законом;

не сприяти іноземним державам, іноземним організаціям чи їх представникам, а також окремим іноземцям та особам без громадянства у провадженні діяльності, що завдає шкоди інтересам національної безпеки України;

виконувати вимоги режиму секретності;

повідомляти посадових осіб, які надали йому доступ до державної таємниці, та відповідні режимно-секретні органи про виникнення обставин, передбачених статтею 23 цього Закону, або інших обставин, що перешкоджають збереженню довіреної йому державної таємниці, а також повідомляти у письмовій формі про свій виїзд з України;

(абзац шостий статті 28 із змінами, внесеними
згідно із Законом України від 06.07.2010 р. N 2432-VI)

додержуватися інших вимог законодавства про державну таємницю.

Стаття 29. Обмеження прав у зв'язку з допуском та доступом до державної таємниці

Громадянин, якому було надано допуск та доступ до державної таємниці у порядку, встановленому законодавством, і який реально був обізнаний з нею, може бути обмежений у праві виїзду на постійне місце проживання в іноземну державу до розсекречування відповідної інформації, але не більш як на п'ять років з часу припинення діяльності, пов'язаної з державною таємницею.

Не обмежується виїзд у держави, з якими Україна має міжнародні договори, що передбачають такий виїзд і згода на обов'язковість яких надана Верховною Радою України.

На громадянина також поширюються обмеження свободи інформаційної діяльності, що випливають з цього Закону.

Стаття 30. Компенсація громадянам у зв'язку з виконанням робіт, які передбачають доступ до державної таємниці

У разі коли за умовами своєї професійної діяльності громадянин постійно працює з відомостями, що становлять державну таємницю, йому повинна надаватися відповідна компенсація за роботу в умовах режимних обмежень, види, розміри та порядок надання якої встановлюються Кабінетом Міністрів України.

Стаття 31. Обмеження на оприлюднення секретної інформації

Під час підготовки матеріалів для опублікування, поширення у пресі та інших засобах масової інформації або переміщення їх через державний кордон державні органи, органи місцевого самоврядування, підприємства, установи, організації та громадяни з метою охорони секретної інформації зобов'язані керуватися Законом України "Про інформацію", цим Законом та іншими нормативно-правовими актами про державну таємницю.

Контроль за додержанням законодавства про державну таємницю з метою запобігання її поширенню у пресі та інших засобах масової інформації здійснює центральний орган виконавчої влади з питань інформаційної політики.

Стаття 32. Обмеження щодо передачі державної таємниці іноземній державі чи міжнародній організації

Секретна інформація до скасування рішення про віднесення її до державної таємниці та матеріальні носії такої інформації до їх розсекречування можуть бути передані іноземній державі чи міжнародній організації лише на підставі міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, або письмового мотивованого розпорядження Президента України з урахуванням необхідності забезпечення національної безпеки України на підставі пропозицій Ради національної безпеки і оборони України.

Стаття 33. Обмеження, пов'язані з державною таємницею, щодо перебування і діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, а також розташування та переміщення об'єктів і технічних засобів, що їм належать

Обмеження, пов'язані з державною таємницею, щодо перебування і діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, а також розташування та переміщення об'єктів і технічних засобів, що їм належать, визначаються відповідним законодавством.

Стаття 34. Особливості здійснення державними органами їх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею

Державні органи, в тому числі правоохоронні, контрольно-ревізійні та суди, з метою охорони державної таємниці мають за погодженням із Службою безпеки України встановлювати порядок здійснення своїх функцій щодо державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з державною таємницею.

Державні органи, органи місцевого самоврядування, підприємства, установи і організації, що провадять діяльність, пов'язану з державною таємницею, вправі відмовити у виконанні запиту щодо надання секретної інформації чи інших подібних вимог зазначеним у частині першій цієї статті державним органам, якщо останні не встановили такого порядку або не додержуються його.

Про мотиви такої відмови одночасно повідомляється Служба безпеки України, яка протягом місяця зобов'язана прийняти рішення про її обгрунтованість.

Стаття 35. Технічний та криптографічний захисти секретної інформації

Технічний та криптографічний захисти секретної інформації здійснюються в порядку, встановленому Президентом України.

Стаття 36. Оперативно-розшукові заходи щодо охорони державної таємниці

Оперативно-розшукові заходи щодо охорони державної таємниці здійснюються відповідно до Закону України "Про оперативно-розшукову діяльність".

Розділ V. КОНТРОЛЬ ЗА ЗАБЕЗПЕЧЕННЯМ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА НАГЛЯД ЗА ДОДЕРЖАННЯМ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

Стаття 37. Контроль за забезпеченням охорони державної таємниці

Керівники державних органів, органів місцевого самоврядування, підприємств, установ і організацій зобов'язані здійснювати постійний контроль за забезпеченням охорони державної таємниці.

Державні органи, органи місцевого самоврядування, підприємства, установи і організації, що розміщують замовлення у підрядників, зобов'язані контролювати стан охорони державної таємниці, яка була передана підрядникам у зв'язку з виконанням замовлення.

Державні органи, яким рішенням державного експерта з питань таємниць було надано право вирішувати питання про доступ державних органів, органів місцевого самоврядування, підприємств, установ, організацій до конкретної секретної інформації, зобов'язані контролювати стан охорони державної таємниці в усіх державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, які виконують роботи, пов'язані з відповідною державною таємницею, або зберігають матеріальні носії зазначеної секретної інформації.

Контроль за додержанням законодавства про державну таємницю в системі Служби безпеки України здійснюється відповідно до Закону України "Про Службу безпеки України".

Служба безпеки України має право контролювати стан охорони державної таємниці в усіх державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, а також у зв'язку з виконанням цих повноважень одержувати безоплатно від них інформацію з питань забезпечення охорони державної таємниці. Висновки Служби безпеки України, викладені в актах офіційних перевірок за результатами контролю стану охорони державної таємниці, є обов'язковими для виконання посадовими особами підприємств, установ та організацій незалежно від їх форм власності.

Стаття 38. Нагляд за додержанням законодавства про державну таємницю

Нагляд за додержанням законодавства про державну таємницю здійснюється у порядку, визначеному законом.

Допуск та доступ посадових осіб, які здійснюють нагляд, до відомостей, що становлять державну таємницю, проводяться відповідно до цього Закону.

Розділ VI. ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ДЕРЖАВНУ ТАЄМНИЦЮ

Стаття 39. Відповідальність за порушення законодавства про державну таємницю

Посадові особи та громадяни, винні у:

розголошенні державної таємниці;

втраті документів та інших матеріальних носіїв секретної інформації;

недодержанні встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;

засекречуванні інформації, зазначеної у частинах третій і четвертій статті 8 цього Закону;

навмисному невіднесенні до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України, а також необгрунтованому заниженні ступеня секретності або необгрунтованому розсекречуванні секретної інформації;

безпідставному засекречуванні інформації;

наданні грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненаданні грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставному скасуванні чи зниженні грифа секретності матеріальних носіїв секретної інформації;

порушенні встановленого законодавством порядку надання допуску та доступу до державної таємниці;

порушенні встановленого законодавством режиму секретності та невиконанні обов'язків щодо збереження державної таємниці;

невжитті заходів щодо забезпечення охорони державної таємниці та незабезпеченні контролю за охороною державної таємниці;

провадженні діяльності, пов'язаної з державною таємницею, без одержання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщенні державних замовлень на виконання робіт, доведенні мобілізаційних завдань, пов'язаних з державною таємницею, в державних органах, органах місцевого самоврядування, на підприємствах, в установах, організаціях, яким не надано спеціального дозволу на проводження діяльності, пов'язаної з державною таємницею;

недодержанні вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства і проведення роботи з ними;

невиконанні норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї інформації або просочування її технічними каналами, -

несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно із законом.

Президент України **Л. КРАВЧУК**

м. Київ
21 січня 1994 року
N 3855-XII

ЗАКОН УКРАЇНИ

Про доступ до публічної інформації

Із змінами і доповненнями, внесеними
Законами України
від 13 квітня 2012 року N 4652-VI,
від 17 травня 2012 року N 4711-VI

Цей Закон визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес.

Розділ I. ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Публічна інформація

1. Публічна інформація - це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом.

2. Публічна інформація є відкритою, крім випадків, встановлених законом.

Стаття 2. Мета і сфера дії Закону

1. Метою цього Закону є забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації.

2. Цей Закон не поширюється на відносини щодо отримання інформації суб'єктами владних повноважень при здійсненні ними своїх функцій, а також на відносини у сфері звернень громадян, які регулюються спеціальним законом.

Стаття 3. Гарантії забезпечення права на доступ до публічної інформації

1. Право на доступ до публічної інформації гарантується:

1) обов'язком розпорядників інформації надавати та оприлюднювати інформацію, крім випадків, передбачених законом;

2) визначенням розпорядником інформації спеціальних структурних підрозділів або посадових осіб, які організовують у встановленому порядку доступ до публічної інформації, якою він володіє;

3) максимальним спрощенням процедури подання запиту та отримання інформації;

4) доступом до засідань колегіальних суб'єктів владних повноважень, крім випадків, передбачених законодавством;

5) здійсненням парламентського, громадського та державного контролю за дотриманням прав на доступ до публічної інформації;

6) юридичною відповідальністю за порушення законодавства про доступ до публічної інформації.

Стаття 4. Принципи забезпечення доступу до публічної інформації

1. Доступ до публічної інформації відповідно до цього Закону здійснюється на принципах:

1) прозорості та відкритості діяльності суб'єктів владних повноважень;

2) вільного отримання та поширення інформації, крім обмежень, встановлених законом;

3) рівноправності, незалежно від ознак раси, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак.

Розділ II. ПОРЯДОК ДОСТУПУ ДО ІНФОРМАЦІЇ

Стаття 5. Забезпечення доступу до інформації

1. Доступ до інформації забезпечується шляхом:

1) систематичного та оперативного оприлюднення інформації:

в офіційних друкованих виданнях;

на офіційних веб-сайтах в мережі Інтернет;

на інформаційних стендах;

будь-яким іншим способом;

2) надання інформації за запитами на інформацію.

Стаття 6. Публічна інформація з обмеженим доступом

1. Інформацією з обмеженим доступом є:

1) конфіденційна інформація;

2) таємна інформація;

3) службова інформація.

2. Обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

3. Інформація з обмеженим доступом має надаватися розпорядником інформації, якщо він правомірно оприлюднив її раніше.

4. Інформація з обмеженим доступом має надаватися розпорядником інформації, якщо немає законних підстав для обмеження у доступі до такої інформації, які існували раніше.

5. Не може бути обмежено доступ до інформації про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно. При дотриманні вимог, передбачених частиною другою цієї статті, зазначене положення не поширюється на випадки, коли оприлюднення або надання такої інформації може завдати шкоди інтересам національної безпеки, оборони, розслідуванню чи запобіганню злочину.

6. Не належать до інформації з обмеженим доступом відомості, зазначені у декларації про майно, доходи, витрати і зобов'язання фінансового характеру, оформленої за формою і в порядку, що встановлені Законом України "Про засади запобігання і протидії корупції", крім відомостей, зазначених у пункті 7 примітки додатка до цього Закону.

(частина шоста статті 6 у редакції
Закону України від 17.05.2012 р. N 4711-VI)

7. Обмеженню доступу підлягає інформація, а не документ. Якщо документ містить інформацію з обмеженим доступом, для ознайомлення надається інформація, доступ до якої необмежений.

Стаття 7. Конфіденційна інформація

1. Конфіденційна інформація - інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. Не може бути віднесена до конфіденційної інформація, зазначена в частині першій і другій статті 13 цього Закону.

2. Розпорядники інформації, визначені частиною першою статті 13 цього Закону, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які

обмежили доступ до інформації, а за відсутності такої згоди - лише в інтересах національної безпеки, економічного добробуту та прав людини.

Стаття 8. Таємна інформація

1. Таємна інформація - інформація, доступ до якої обмежується відповідно до частини другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю.

(частина перша статті 8 із змінами, внесеними
згідно із Законом України від 13.04.2012 р. N 4652-VI)

2. Порядок доступу до таємної інформації регулюється цим Законом та спеціальними законами.

Стаття 9. Службова інформація

1. Відповідно до вимог частини другої статті 6 цього Закону до службової може належати така інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

2. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф "для службового користування". Доступ до таких документів надається відповідно до частини другої статті 6 цього Закону.

3. Перелік відомостей, що становлять службову інформацію, який складається органами державної влади, органами місцевого самоврядування, іншими суб'єктами владних повноважень, у тому числі на виконання делегованих повноважень, не може бути обмеженим у доступі.

Стаття 10. Доступ до інформації про особу

1. Кожна особа має право:

1) знати у період збирання інформації, але до початку її використання, які відомості про неї та з якою метою збираються, як, ким і з якою метою вони використовуються, передаються чи поширюються, крім випадків, встановлених законом;

2) доступу до інформації про неї, яка збирається та зберігається;

3) вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання якої здійснюється з порушенням вимог закону;

4) на ознайомлення за рішенням суду з інформацією про інших осіб, якщо це необхідно для реалізації та захисту прав та законних інтересів;

5) на відшкодування шкоди у разі розкриття інформації про цю особу з порушенням вимог, визначених законом.

2. Обсяг інформації про особу, що збирається, зберігається і використовується розпорядниками інформації, має бути максимально обмеженим і використовуватися лише з метою та у спосіб, визначений законом.

3. Розпорядники інформації, які володіють інформацією про особу, зобов'язані:

1) надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, крім випадків, передбачених законом;

2) використовувати її лише з метою та у спосіб, визначений законом;

3) вживати заходів щодо унеможливлення несанкціонованого доступу до неї інших осіб;

4) виправляти неточну та застарілу інформацію про особу самостійно або на вимогу осіб, яких вона стосується.

4. Зберігання інформації про особу не повинно тривати довше, ніж це необхідно для досягнення мети, задля якої ця інформація збиралася.

5. Відмова особі в доступі до інформації про неї, приховування, незаконне збирання, використання, зберігання чи поширення інформації можуть бути оскаржені.

Стаття 11. Захист особи, яка оприлюднює інформацію

1. Посадові та службові особи не підлягають юридичній відповідальності, незважаючи на порушення своїх обов'язків, за розголошення інформації про правопорушення або відомостей, що стосуються серйозної загрози здоров'ю чи безпеці громадян, довкіллю, якщо особа при цьому керувалася добрими намірами та мала обґрунтоване переконання, що інформація є достовірною, а також містить докази правопорушення або стосується істотної загрози здоров'ю чи безпеці громадян, довкіллю.

Розділ III. СУБ'ЄКТИ ВІДНОСИН У СФЕРІ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ

Стаття 12. Визначення та перелік суб'єктів

1. Суб'єктами відносин у сфері доступу до публічної інформації є:

1) запитувачі інформації - фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень;

2) розпорядники інформації - суб'єкти, визначені у статті 13 цього Закону;

3) структурний підрозділ або відповідальна особа з питань запитів на інформацію розпорядників інформації.

Стаття 13. Розпорядники інформації

1. Розпорядниками інформації для цілей цього Закону визнаються:

1) суб'єкти владних повноважень - органи державної влади, інші державні органи, органи місцевого самоврядування, органи влади Автономної Республіки Крим, інші суб'єкти, що здійснюють владні управлінські функції відповідно до законодавства та рішення яких є обов'язковими для виконання;

2) юридичні особи, що фінансуються з державного, місцевих бюджетів, бюджету Автономної Республіки Крим, - стосовно інформації щодо використання бюджетних коштів;

3) особи, якщо вони виконують делеговані повноваження суб'єктів владних повноважень згідно із законом чи договором, включаючи надання освітніх, оздоровчих, соціальних або інших державних послуг, - стосовно інформації, пов'язаної з виконанням їхніх обов'язків;

4) суб'єкти господарювання, які займають домінуюче становище на ринку або наділені спеціальними чи виключними правами, або є природними монополіями, - стосовно інформації щодо умов постачання товарів, послуг та цін на них.

2. До розпорядників інформації, зобов'язаних оприлюднювати та надавати за запитами інформацію, визначену в цій статті, у порядку, передбаченому цим Законом, прирівнюються суб'єкти господарювання, які володіють:

1) інформацією про стан довкілля;

2) інформацією про якість харчових продуктів і предметів побуту;

3) інформацією про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують здоров'ю та безпеці громадян;

4) іншою інформацією, що становить суспільний інтерес (суспільно необхідною інформацією).

3. На розпорядників інформації, визначених у пунктах 2, 3, 4 частини першої та в частині другій цієї статті, вимоги цього Закону поширюються лише в частині оприлюднення та надання відповідної інформації за запитами.

4. Усі розпорядники інформації незалежно від нормативно-правового акта, на підставі якого вони діють, при вирішенні питань щодо доступу до інформації мають керуватися цим Законом.

Стаття 14. Обов'язки розпорядників інформації

1. Розпорядники інформації зобов'язані:

1) оприлюднювати інформацію про свою діяльність та прийняті рішення;

2) систематично вести облік документів, що знаходяться в їхньому володінні;

3) вести облік запитів на інформацію;

4) визначати спеціальні місця для роботи запитувачів з документами чи їх копіями, а також надавати право запитувачам робити виписки з них, фотографувати, копіювати, сканувати їх, записувати на будь-які носії інформації тощо;

5) мати спеціальні структурні підрозділи або призначати відповідальних осіб для забезпечення доступу запитувачів до інформації;

6) надавати достовірну, точну та повну інформацію, а також у разі потреби перевіряти правильність та об'єктивність наданої інформації.

Стаття 15. Оприлюднення інформації розпорядниками

1. Розпорядники інформації зобов'язані оприлюднювати:

1) інформацію про організаційну структуру, місію, функції, повноваження, основні завдання, напрями діяльності та фінансові ресурси (структуру та обсяг бюджетних коштів, порядок та механізм їх витрачання тощо);

2) нормативно-правові акти, акти індивідуальної дії (крім внутрішньоорганізаційних), прийняті розпорядником, проекти рішень, що підлягають обговоренню, інформацію про нормативно-правові засади діяльності;

3) перелік та умови отримання послуг, що надаються цими органами, форми і зразки документів, правила їх заповнення;

4) порядок складання, подання запиту на інформацію, оскарження рішень розпорядників інформації, дій чи бездіяльності;

5) інформацію про систему обліку, види інформації, яку зберігає розпорядник;

6) інформацію про механізми чи процедури, за допомогою яких громадськість може представляти свої інтереси або в інший спосіб впливати на реалізацію повноважень розпорядника інформації;

7) плани проведення та порядок денний своїх відкритих засідань;

8) розташування місць, де надаються необхідні запитувачам форми і бланки установи;

9) загальні правила роботи установи, правила внутрішнього трудового розпорядку;

10) звіти, в тому числі щодо задоволення запитів на інформацію;

11) інформацію про діяльність суб'єктів владних повноважень, а саме про:

їхні місцезнаходження, поштову адресу, номери засобів зв'язку, адреси офіційного веб-сайту та електронної пошти;

прізвище, ім'я та по батькові, службові номери засобів зв'язку, адреси електронної пошти керівника органу та його заступників, а також керівників структурних та регіональних підрозділів, основні функції структурних та регіональних підрозділів, крім випадків, коли ці відомості належать до інформації з обмеженим доступом;

розклад роботи та графік прийому громадян;

вакансії, порядок та умови проходження конкурсу на заміщення вакантних посад;

перелік та умови надання послуг, форми і зразки документів, необхідних для надання послуг, правила їх оформлення;

перелік і службові номери засобів зв'язку підприємств, установ та організацій, що належать до сфери їх управління, та їх керівників, крім підприємств, установ та організацій, створених з метою конспірації, оперативно-розшукової або контррозвідувальної діяльності;

порядок складання, подання запиту на інформацію, оскарження рішень суб'єктів владних повноважень, їх дій чи бездіяльності;

систему обліку, види інформації, якою володіє суб'єкт владних повноважень;

12) іншу інформацію про діяльність суб'єктів владних повноважень, порядок обов'язкового оприлюднення якої встановлений законом.

2. Інформація, передбачена частиною першою цієї статті, підлягає обов'язковому оприлюдненню невідкладно, але не пізніше п'яти робочих днів з дня затвердження документа. У разі наявності у розпорядника інформації офіційного веб-сайту така інформація оприлюднюється на веб-сайті із зазначенням дати оприлюднення документа і дати оновлення інформації.

3. Проекти нормативно-правових актів, рішень органів місцевого самоврядування, розроблені відповідними розпорядниками, оприлюднюються ними не пізніш як за 20 робочих днів до дати їх розгляду з метою прийняття.

4. Невідкладному оприлюдненню підлягає будь-яка інформація про факти, що загрожують життю, здоров'ю та/або майну осіб, і про заходи, які застосовуються у зв'язку з цим.

Стаття 16. Відповідальні особи з питань запитів на інформацію

1. Розпорядник інформації відповідає за визначення завдань та забезпечення діяльності структурного підрозділу або відповідальної особи з питань запитів на інформацію розпорядників інформації, відповідальних за опрацювання, систематизацію, аналіз та контроль щодо задоволення запиту на інформацію та надання консультацій під час оформлення запиту.

2. Запит, що пройшов реєстрацію у встановленому розпорядником інформації порядку, обробляється відповідальними особами з питань запитів на інформацію.

Стаття 17. Контроль за забезпеченням доступу до публічної інформації

1. Парламентський контроль за дотриманням права людини на доступ до інформації здійснюється Уповноваженим Верховної Ради України з прав людини, тимчасовими слідчими комісіями Верховної Ради України, народними депутатами України.

2. Громадський контроль за забезпеченням розпорядниками інформації доступу до публічної інформації здійснюється депутатами місцевих рад, громадськими організаціями,

громадськими радами, громадянами особисто шляхом проведення відповідних громадських слухань, громадської експертизи тощо.

3. Державний контроль за забезпеченням розпорядниками інформації доступу до інформації здійснюється відповідно до закону.

Стаття 18. Реєстрація документів розпорядника інформації

1. Для забезпечення збереження та доступу до публічної інформації документи, що знаходяться у суб'єктів владних повноважень, підлягають обов'язковій реєстрації в системі обліку, що має містити:

1) назву документа;

2) дату створення документа;

3) дату надходження документа;

4) джерело інформації (автор, відповідний підрозділ);

5) передбачену законом підставу віднесення інформації до категорії з обмеженим доступом;

6) строк обмеження доступу до інформації, у разі якщо вона віднесена до інформації з обмеженим доступом;

7) галузь;

8) ключові слова;

9) тип, носій (текстовий документ, плівки, відеозаписи, аудіозаписи тощо);

10) вид (нормативні акти, угоди, рішення, протоколи, звіти, прес-релізи);

11) проекти рішень (доповідні записки, звернення, заяви, подання, пропозиції, листи тощо);

12) форму та місце зберігання документа тощо.

2. Доступ до системи обліку, що містить інформацію про документ, що знаходиться у суб'єкта владних повноважень, забезпечується шляхом:

1) оприлюднення на офіційних веб-сайтах суб'єктів владних повноважень такої інформації, а в разі їх відсутності - в інший прийнятний спосіб;

2) надання доступу до системи за запитами.

3. Система обліку публічної інформації не може бути віднесена до категорії інформації з обмеженим доступом.

4. Розпорядники інформації несуть відповідальність за забезпечення доступу до системи обліку відповідно до закону.

Розділ IV. РЕАЛІЗАЦІЯ ПРАВА НА ДОСТУП ДО ІНФОРМАЦІЇ ЗА ІНФОРМАЦІЙНИМ ЗАПИТОМ

Стаття 19. Оформлення запитів на інформацію

1. Запит на інформацію - це прохання особи до розпорядника інформації надати публічну інформацію, що знаходиться у його володінні.

2. Запитувач має право звернутися до розпорядника інформації із запитом на інформацію незалежно від того, стосується ця інформація його особисто чи ні, без пояснення причини подання запиту.

3. Запит на інформацію може бути індивідуальним або колективним. Запити можуть подаватися в усній, письмовій чи іншій формі (поштою, факсом, телефоном, електронною поштою) на вибір запитувача.

4. Письмовий запит подається в довільній формі.

5. Запит на інформацію має містити:

1) ім'я (найменування) запитувача, поштову адресу або адресу електронної пошти, а також номер засобу зв'язку, якщо такий є;

2) загальний опис інформації або вид, назву, реквізити чи зміст документа, щодо якого зроблено запит, якщо запитувачу це відомо;

3) підпис і дату за умови подання запиту в письмовій формі.

6. З метою спрощення процедури оформлення письмових запитів на інформацію особа може подавати запит шляхом заповнення відповідних форм запитів на інформацію, які можна отримати в розпорядника інформації та на офіційному веб-сайті відповідного розпорядника. Зазначені форми мають містити стислу інструкцію щодо процедури подання запиту на інформацію, її отримання тощо.

7. У разі якщо з поважних причин (інвалідність, обмежені фізичні можливості тощо) особа не може подати письмовий запит, його має оформити відповідальна особа з питань запитів на інформацію, обов'язково зазначивши в запиті своє ім'я, контактний телефон, та надати копію запиту особі, яка його подала.

Стаття 20. Строк розгляду запитів на інформацію

1. Розпорядник інформації має надати відповідь на запит на інформацію не пізніше п'яти робочих днів з дня отримання запиту.

2. У разі якщо запит на інформацію стосується інформації, необхідної для захисту життя чи свободи особи, щодо стану довкілля, якості харчових продуктів і предметів побуту, аварій, катастроф, небезпечних природних явищ та інших надзвичайних подій, що сталися або можуть статись і загрожують безпеці громадян, відповідь має бути надана не пізніше 48 годин з дня отримання запиту.

3. Клопотання про термінове опрацювання запиту має бути обґрунтованим.

4. У разі якщо запит стосується надання великого обсягу інформації або потребує пошуку інформації серед значної кількості даних, розпорядник інформації може продовжити строк розгляду запиту до 20 робочих днів з обґрунтуванням такого продовження. Про продовження строку розпорядник інформації повідомляє запитувача в письмовій формі не пізніше п'яти робочих днів з дня отримання запиту.

Стаття 21. Плата за надання інформації

1. Інформація на запит надається безкоштовно.

2. У разі якщо задоволення запиту на інформацію передбачає виготовлення копій документів обсягом більш як 10 сторінок, запитувач зобов'язаний відшкодувати фактичні витрати на копіювання та друк.

3. Розмір фактичних витрат визначається відповідним розпорядником на копіювання та друк в межах граничних норм, встановлених Кабінетом Міністрів України. У разі якщо розпорядник інформації не встановив розміру плати за копіювання або друк, інформація надається безкоштовно.

4. При наданні особі інформації про себе та інформації, що становить суспільний інтерес, плата за копіювання та друк не стягується.

Стаття 22. Відмова та відстрочка в задоволенні запиту на інформацію

1. Розпорядник інформації має право відмовити в задоволенні запиту в таких випадках:

1) розпорядник інформації не володіє і не зобов'язаний відповідно до його компетенції, передбаченої законодавством, володіти інформацією, щодо якої зроблено запит;

2) інформація, що запитується, належить до категорії інформації з обмеженим доступом відповідно до частини другої статті 6 цього Закону;

3) особа, яка подала запит на інформацію, не оплатила передбачені статтею 21 цього Закону фактичні витрати, пов'язані з копіюванням або друком;

4) не дотримано вимог до запиту на інформацію, передбачених частиною п'ятою статті 19 цього Закону.

2. Відповідь розпорядника інформації про те, що інформація може бути одержана запитувачем із загальнодоступних джерел, або відповідь не по суті запиту вважається неправомірною відмовою в наданні інформації.

3. Розпорядник інформації, який не володіє запитуваною інформацією, але якому за статусом або характером діяльності відомо або має бути відомо, хто нею володіє, зобов'язаний направити цей запит належному розпоряднику з одночасним повідомленням про це запитувача. У такому разі відлік строку розгляду запиту на інформацію починається з дня отримання запиту належним розпорядником.

4. У відмові в задоволенні запиту на інформацію має бути зазначено:

1) прізвище, ім'я, по батькові та посаду особи, відповідальної за розгляд запиту розпорядником інформації;

2) дату відмови;

3) мотивовану підставу відмови;

4) порядок оскарження відмови;

5) підпис.

5. Відмова в задоволенні запиту на інформацію надається в письмовий формі.

6. Відстрочка в задоволенні запиту на інформацію допускається в разі, якщо запитувана інформація не може бути надана для ознайомлення в передбачені цим Законом строки у разі настання обставин непереборної сили. Рішення про відстрочку доводиться до відома запитувача у письмовій формі з роз'ясненням порядку оскарження прийнятого рішення.

7. У рішенні про відстрочку в задоволенні запиту на інформацію має бути зазначено:

1) прізвище, ім'я, по батькові та посаду особи, відповідальної за розгляд запиту розпорядником інформації;

2) дату надсилання або вручення повідомлення про відстрочку;

3) причини, у зв'язку з якими запит на інформацію не може бути задоволений у встановлений цим Законом строк;

4) строк, у який буде задоволено запит;

5) підпис.

Розділ V. ОСКАРЖЕННЯ РІШЕНЬ, ДІЙ ЧИ БЕЗДІЯЛЬНОСТІ РОЗПОРЯДНИКІВ ІНФОРМАЦІЇ

Стаття 23. Право на оскарження рішень, дій чи бездіяльності розпорядників інформації

1. Рішення, дії чи бездіяльність розпорядників інформації можуть бути оскаржені до керівника розпорядника, вищого органу або суду.

2. Запитувач має право оскаржити:

1) відмову в задоволенні запиту на інформацію;

2) відстрочку задоволення запиту на інформацію;

3) ненадання відповіді на запит на інформацію;

4) надання недостовірної або неповної інформації;

5) несвоєчасне надання інформації;

6) невиконання розпорядниками обов'язку оприлюднювати інформацію відповідно до статті 15 цього Закону;

7) інші рішення, дії чи бездіяльність розпорядників інформації, що порушили законні права та інтереси запитувача.

3. Оскарження рішень, дій чи бездіяльності розпорядників інформації до суду здійснюється відповідно до Кодексу адміністративного судочинства України.

Стаття 24. Відповідальність за порушення законодавства про доступ до публічної інформації

1. Відповідальність за порушення законодавства про доступ до публічної інформації несуть особи, винні у вчиненні таких порушень:

1) ненадання відповіді на запит;

2) ненадання інформації на запит;

3) безпідставна відмова у задоволенні запиту на інформацію;

4) неоприлюднення інформації відповідно до статті 15 цього Закону;

5) надання або оприлюднення недостовірної, неточної або неповної інформації;

6) несвоєчасне надання інформації;

7) необґрунтоване віднесення інформації до інформації з обмеженим доступом;

8) нездійснення реєстрації документів;

9) навмисне приховування або знищення інформації чи документів.

2. Особи, на думку яких їхні права та законні інтереси порушені розпорядниками інформації, мають право на відшкодування матеріальної та моральної шкоди в порядку, визначеному законом.

Розділ VI. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності через три місяці з дня його опублікування.

2. До приведення законодавства України у відповідність із цим Законом акти законодавства України застосовуються в частині, що не суперечить цьому Закону.

3. Внести зміни до таких законодавчих актів України:

1) у Кодексі України про адміністративні правопорушення (Відомості Верховної Ради УРСР, 1984 р., додаток до N 51, ст. 1122):

у статті 212^3:

частину першу після слів "Про інформацію" доповнити словами "Про доступ до публічної інформації";

примітку викласти в такій редакції:

"**Примітка.** Особи, визначені в примітці до статті 212^{26} цього Кодексу, притягаються до відповідальності за діяння, передбачені даною статтею, згідно із статтею 212^{26}";

частину першу статті 212^{26} після слів "Про інформацію" доповнити словами "Про доступ до публічної інформації";

2) у назві та абзаці першому частини першої статті 330 Кримінального кодексу України (Відомості Верховної Ради України, 2001 р., N 25 - 26, ст. 131) слова "яка є власністю держави" замінити словами "яка знаходиться у володінні держави";

3) частину десяту статті 9 Закону України "Про оперативно-розшукову діяльність" (Відомості Верховної Ради України, 1992 р., N 22, ст. 303; 2000 р., N 10, ст. 79) доповнити двома реченнями такого змісту: "Забороняється оприлюднювати або надавати зібрані відомості, а також інформацію щодо проведення або непроведення стосовно певної особи оперативно-розшукової діяльності до прийняття рішення за результатами такої діяльності. Питання оприлюднення або надання такої інформації після прийняття рішення регулюється законом";

4) статтю 9 Закону України "Про контррозвідувальну діяльність" (Відомості Верховної Ради України, 2003 р., N 12, ст. 89) доповнити реченням такого змісту: "Забороняється оприлюднювати або надавати (розголошувати) зібрані відомості, а також інформацію щодо проведення або непроведення стосовно певної особи контррозвідувальної діяльності та заходів до прийняття рішення за результатами такої діяльності або заходів";

5) статтю 13 Закону України "Про авторське право і суміжні права" (Відомості Верховної Ради України, 2001 р., N 43, ст. 214) доповнити частиною п'ятою такого змісту:

"5. Зазначені положення не поширюються на випадки оприлюднення чи надання інформації на підставі Закону України "Про доступ до публічної інформації".

4. Кабінету Міністрів України у двомісячний строк з дня набрання чинності цим Законом:

затвердити граничні норми витрат на копіювання або друк, передбачені статтею 21 цього Закону;

внести на розгляд Верховної Ради України законопроекти щодо приведення законів України у відповідність із цим Законом;

привести свої нормативно-правові акти у відповідність із цим Законом;

забезпечити приведення органами виконавчої влади їх нормативно-правових актів у відповідність із цим Законом.

Президент України **В. ЯНУКОВИЧ**

м. Київ
13 січня 2011 року
N 2939-VI

Офіційне видання

Укладачі:

КІРІН Роман Станіславович
ГРИЩАК Сергій Вікторович
ШАШЕНКО Дмитро Олександрович

Інформаційне законодавство
Правове забезпечення захисту інформації

Частина 4

Підписано до друку 01.08.2012. Формат 30х42/4.
Папір офсет. Ризографія. Ум. друк. арк. 9,5.
Обл.-вид. арк. 9,5. Тираж 100 пр. Зам. №

Підготовлено до друку та видрукувано
у Державному ВНЗ "Національний гірничий університет"
Свідоцтво про внесення до Державного реєстру ДК № 1842 від 11.06.2004

49005, м. Дніпропетровськ, просп. К. Маркса, 19.