КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 29 березня 2006 р. № 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 № 1700,
від 7 вересня 2011 року № 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. № 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. № 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. № 1229.

(абзац четвертий пункту 3 із змінами, внесеними згідно з постановою Кабінету Міністрів України від 07.09.2011 р. № 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. № 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. № 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. № 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. № 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. № 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. № 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. № 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. № 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. № 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. № 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. № 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. № 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. № 1700)

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