Редакція:
08.02.2021

**КАБІНЕТ МІНІСТРІВ УКРАЇНИ**

**ПОСТАНОВА**

від 8 лютого 2021 р. N 92

Київ

# Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах

Кабінет Міністрів України **постановляє**:

1. Внести до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених постановою Кабінету Міністрів України від 29 березня 2006 р. N 373 (Офіційний вісник України, 2006 р., N 13, ст. 878, N 50, ст. 3324; 2011 р., N 69, ст. 2624), зміни, що додаються.

2. Установити, що атестати відповідності на комплексні системи захисту інформації, які чинні на момент набрання чинності цією постановою, зберігають чинність протягом строку їх дії.

3. Визнати такою, що втратила чинність, постанову Кабінету Міністрів України від 12 квітня 2002 р. N 522 "Про затвердження Порядку підключення до глобальних мереж передачі даних" (Офіційний вісник України, 2002 р., N 16, ст. 864).

4. Адміністрації Державної служби спеціального зв'язку та захисту інформації у тримісячний строк з дати набрання чинності цією постановою затвердити вимоги до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону.

Прем'єр-міністр України Д. ШМИГАЛЬ

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 8 лютого 2021 р. N 92

**ЗМІНИ,**
**що вносяться до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах**

1. Пункт 2 викласти в такій редакції:

"2. Дія цих Правил не поширюється на захист інформації в системах урядового та спеціальних видів зв'язку, в технічних засобах і їх складових, необхідних для здійснення уповноваженими органами оперативно-розшукових, розвідувальних заходів та негласних слідчих (розшукових) дій.".

2. Пункт 9 викласти в такій редакції:

"9. Забезпечення технічного та криптографічного захисту інформації з обмеженим доступом, а також відкритої інформації, вимога щодо захисту якої встановлена законом, здійснюється в системі з дотриманням вимог, що висуваються для забезпечення захисту такої інформації, якщо інше не передбачене законом.

Криптографічний захист в системі таємної інформації, яка не становить державної таємниці, та конфіденційної інформації в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах та організаціях, які належать до сфери їх управління, військових формуваннях, які створені відповідно до закону, здійснюється з використанням засобів криптографічного захисту інформації, які відповідають вимогам до засобів криптографічного захисту інформації, призначених для захисту таємної інформації, яка не становить державної таємниці, та конфіденційної інформації, що підтверджуються експертним висновком у сфері криптографічного захисту інформації або документом про відповідність.".

3. Абзац дев'ятий пункту 11 викласти в такій редакції:

"Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, і службовою інформацією повинна супроводжуватися повідомленням про них адміністратору безпеки (відповідальній особі).".

4. Пункти 13 і 14 викласти в такій редакції:

"13. Передача конфіденційної інформації, службової та таємної інформації через незахищене середовище (середовище, в якому циркулює інформація, стосовно якої відсутнє підтвердження відповідності захисту від усіх можливих загроз, імовірність прояву яких існує у цьому середовищі) здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства у сфері технічного та криптографічного захисту інформації, за винятком інформації, що передається через канали (лінії) зв'язку, які перебувають в межах контрольованої зони (територія (простір), на якій (в якому) унеможливлено несанкціоноване і неконтрольоване перебування сторонніх осіб, розміщення технічних і транспортних засобів).

14. Підключення систем, у яких обробляється службова інформація та інформація, що становить державну таємницю, до глобальних мереж передачі даних здійснюється з використанням засобів криптографічного захисту інформації, які допущені до експлуатації для криптографічного захисту інформації відповідного ступеня обмеження доступу, та/або апаратних, апаратно-програмних засобів технічного захисту інформації, які мають позитивний

експертний висновок за результатами державної експертизи у сфері технічного захисту інформації та реалізують функції безпеки односпрямованої (односторонньої) передачі даних та/або двоспрямованої передачі даних з урахуванням їх змістовного аналізу.

В апаратно-програмних засобах технічного захисту інформації, які реалізують функції односпрямованої (односторонньої) передачі даних та або міжмережевого екранування (фільтрації) даних, що забезпечують захист службової інформації та інформації, що становить державну таємницю, рівень гарантії коректності надання функціональних послуг безпеки повинен бути не нижче третього.

Достатність впроваджених засобів захисту інформації обґрунтовується на етапі технічного проектування системи захисту інформації та оцінюється під час проведення державної експертизи комплексної системи захисту інформації.".

5. Пункт 16 доповнити абзацами такого змісту:

"Державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі без застосування комплексної системи захисту інформації. Умови, за яких можна не застосовувати комплексну систему захисту інформації, визначені Законом України "Про захист інформації в інформаційно-телекомунікаційних системах".

У таких системах повинні бути виконані технічні та організаційні вимоги із захисту інформації, визначені цими Правилами.".

6. Пункт 22 викласти в такій редакції:

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

Органи виконавчої влади, військові формування, створені відповідно до закону, які мають дозвіл на проведення робіт з технічного захисту інформації для власних потреб, мають право організовувати проведення державної експертизи систем захисту на підприємствах, в установах, організаціях, закладах, військових з'єднаннях та частинах, які належать до їх сфери управління або підпорядковані їм. Порядок проведення такої експертизи встановлюється органом виконавчої влади, військовим формуванням, створеним відповідно до закону, за погодженням з Адміністрацією.".

7. Пункт 23 виключити.

_____