ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 30 травня 2024 р. № 627

ПОРЯДОК
реалізації експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації

1. Цей Порядок визначає механізм реалізації експериментального проекту з декларування відповідності комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі — системи), створених з використанням базових та цільових профілів безпеки інформації (далі — експериментальний проект).

Метою експериментального проекту є підвищення рівня захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, оптимізація процесу державної експертизи та підтвердження відповідності комплексних систем захисту інформації в системах.

Дія цього Порядку не поширюється на заходи із захисту інформації від витоку технічними каналами.

2. У цьому Порядку терміни вживаються у значенні, наведеному в Законах України “Про інформацію”, “Про доступ до публічної інформації”, “Про державну таємницю”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про електронні комунікації”, “Про Державну службу спеціального зв’язку та захисту інформації України”.

3. Під час реалізації експериментального проекту підтвердження відповідності комплексних систем захисту інформації в системах, створених з використанням базових та цільових профілів безпеки інформації, здійснюється шляхом декларування згідно з цим Порядком.

Базовим профілем безпеки інформації (далі — базовий профіль) є вимоги з безпеки інформації та взаємопов’язана сукупність заходів з її захисту, визначені Адміністрацією Держспецзв’язку для відкритої інформації та інформації з обмеженим доступом, яка обробляється у системах.

Цільовим профілем безпеки інформації (далі — цільовий профіль) є взаємопов’язана сукупність заходів із захисту інформації та їх налаштування, визначених для системи її власником (розпорядником) відповідно до базового профілю з урахуванням вимог законодавства та

стандартів у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, нормативних документів системи технічного захисту інформації, галузевих вимог, політик безпеки в системах, а також призначення системи, її характеристик та особливостей функціонування, результатів проведеної оцінки ризиків.

Під час визначення цільового профілю власник (розпорядник) системи самостійно обирає стандарти у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, які використовуються під час здійснення заходів із захисту інформації, шляхи і способи здійснення таких заходів відповідно до цільового профілю, а також визначає наявність у ньому інформації з обмеженим доступом та забезпечує дотримання встановлених правил роботи з документами, які містять інформацію з обмеженим доступом.

Передбачені у цільовому профілі заходи із захисту інформації, обрані стандарти, шляхи і способи здійснення таких заходів повинні включати відповідні вимоги та заходи, визначені базовим профілем.

4. Створення комплексних систем захисту інформації в системах з використанням базових та цільових профілів та декларування відповідності таких комплексних систем здійснюється за такими етапами:

визначення для систем цільового профілю відповідно до базового профілю;

створення комплексних систем захисту інформації в системах відповідно до базових та цільових профілів;

оцінка достатності заходів захисту інформації комплексних систем захисту інформації в системах, створених з використанням профілів безпеки;

декларування відповідності комплексних систем захисту інформації в системах, створених з використанням профілів безпеки.

5. Оцінка достатності заходів захисту інформації комплексних систем захисту інформації в системах, створених з використанням профілів безпеки, здійснюється з урахуванням рекомендацій, затверджених Адміністрацією Держспецзв’язку.

Процедура оцінки комплексних систем захисту інформації в системах, створених з використанням базових та цільових профілів, для впровадження таких комплексних систем визначається власником (розпорядником) системи та здійснюється суб’єктами господарювання, які мають ліцензії на право надання послуг у галузі криптографічного захисту інформації (крім електронних довірчих послуг та електронної ідентифікації) та технічного захисту інформації в частині оцінювання захищеності інформації, або учасниками експериментального проекту, які

мають дозвіл на проведення робіт з технічного захисту інформації для власних потреб в частині оцінювання захищеності інформації.

Результати оцінки комплексних систем захисту інформації в системах, створених з використанням базових та цільових профілів, підготовлені в рамках цього експериментального проекту, приймаються як результати державної експертизи.

6. Після виконання всіх етапів та вимог, передбачених цим Порядком, власник (розпорядник) системи декларує відповідність комплексної системи захисту інформації в системі, створеної з використанням базових та цільових профілів, за формою згідно з додатком.

Декларація про відповідність комплексної системи захисту інформації в системі, створеної з використанням базових та цільових профілів безпеки інформації (далі — декларація), подається до Адміністрації Держспецзв'язку власником (розпорядником) системи в електронній формі з використанням системи електронної взаємодії органів виконавчої влади з накладенням електронного підпису, що базується на кваліфікованому сертифікаті електронного підпису відповідно до вимог законодавства у сферах електронної ідентифікації та електронних довірчих послуг, а у разі наявності в них інформації з обмеженим доступом подання таких документів здійснюється з дотриманням встановлених правил роботи з документами, які містять інформацію з обмеженим доступом.

Строк дії декларації становить три роки з дня підтвердження її відповідності.

7. Дата подання декларації до Адміністрації Держспецзв'язку вважається датою підтвердження відповідності комплексної системи захисту інформації та не потребує відповіді Адміністрації Держспецзв'язку.

Адміністрація Держспецзв'язку протягом двох робочих днів з дня надходження декларації публікує на власному офіційному веб-сайті інформацію про декларанта (ідентифікатор/назва системи, найменування власника системи, дата подання декларації, дата закінчення дії декларації, стан декларації), крім матеріалів, що містять інформацію з обмеженим доступом.

8. Власник (розпорядник) системи несе відповідальність за відповідність комплексних систем захисту інформації в системах, створених з використанням базових та цільових профілів, повноту та достатність визначених у цільовому профілі безпеки заходів із захисту інформації, обрані стандарти, шляхи і способи здійснення таких заходів відповідно до вимог законодавства у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, нормативних документів системи технічного захисту інформації, галузевих вимог, політик безпеки в системах, а також

призначення системи, її характеристик та особливостей функціонування, результатів проведеної оцінки ризиків.

9. Перевірка відповідності комплексної системи захисту інформації в системі, створеної з використанням базових та цільових профілів, проводиться у рамках державного контролю за станом технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

10. З метою оцінки ефективності реалізації експериментального проекту та надання методично-консультативної підтримки його учасникам Адміністрацією Держспецзв'язку у визначеному нею порядку, здійснюється моніторинг систем захисту інформації в системі, створених з використанням базових та цільових профілів.

11. У разі зміни цільового профілю декларація вважається недійсною.

12. Повторне декларування відповідності комплексної системи захисту інформації в системі, створеної з використанням базових та цільових профілів, здійснюється у разі зміни цільового профілю або усунення недоліків, виявлених за результатами проведення державного контролю за станом технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом.

13. Облік систем, що мають комплексні системи захисту інформації, створені з використанням базових та цільових профілів, ведеться Адміністрацією Держспецзв'язку.

14. Видатки на реалізацію експериментального проекту здійснюються за рахунок і в межах видатків, передбачених Адміністрації Держспецзв'язку у Державному бюджеті України на відповідний рік, а також інших джерел, не заборонених законодавством.

_____

Додаток
до Порядку

ДЕКЛАРАЦІЯ
про відповідність комплексної системи захисту інформації в системі, створеної з використанням базових та цільових профілів безпеки інформації

_____
(найменування державного органу, підприємства, установи, організації, органу військового

_____
управління та військового формування — власника (розпорядника)

_____
системи, код згідно з ЄДРПОУ, місцезнаходження)

в особі _____
(посада, власне ім'я, прізвище керівника державного органу, підприємства, установи,

_____
організації, органу військового управління та військового

_____
формування — власника (розпорядника) системи)

підтверджує, що:

комплексна система захисту інформації _____

_____
(повне найменування інформаційної, електронної комунікаційної, інформаційно-комунікаційної системи)

забезпечує захист _____ інформації
(відкрита інформація або зазначається вид інформації з обмеженим доступом)

відповідно до вимог базового профілю безпеки інформації, що затверджено _____

_____,
(реквізити документа, яким затверджено базовий профіль безпеки інформації)

на основі якого створено цільовий профіль безпеки інформації, що затверджено _____

_____ ;
(реквізити документа, яким затверджено цільовий профіль безпеки інформації)

передбачені у цільовому профілі безпеки інформації заходи із захисту інформації, обрані стандарти, шляхи і способи здійснення таких заходів включають вимоги з безпеки інформації та заходи з її захисту, визначені базовим профілем безпеки інформації;

визначені у цільовому профілі безпеки інформації заходи із захисту інформації та їх налаштування враховують вимоги законодавства та стандартів у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, нормативних

документів системи технічного захисту інформації, галузевих вимог, політик безпеки в системах, а також призначення таких систем, їх характеристик та особливостей функціонування, результати аналізу щодо пропорційності та/або співрозмірності заходів реальним та потенційним ризикам;

створена комплексна система захисту інформації в такій системі відповідає вимогам з безпеки інформації цільового профілю безпеки інформації;

дотримано вимоги з безпеки інформації та здійснено заходи з її захисту, визначені базовим профілем безпеки інформації, а саме:

Порядковий номер	Найменування вимоги з безпеки інформації/ зміст заходу із захисту інформації, визначені базовим профілем безпеки інформації	Інформація про здійснення заходів/дотримання вимог
1	2	3

_____

Примітка. Зміст графи 2 визначається базовим профілем безпеки інформації.

З положеннями Закону України “Про захист інформації в інформаційно-комунікаційних системах”, зокрема статтями 9, 11, ознайомлений.

_____ _____ _____

(найменування посади керівника державного органу, підприємства, установи, організації, органу військового управління та військового формування — власника (розпорядника) системи)

(підпис)

(власне ім’я, прізвище)

___ _____ 20__ р.

МП (у разі наявності)

_____