ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 5 листопада 2025 р. № 1424

ПОРЯДОК
розроблення, прийняття, внесення змін, скасування, відновлення дії, оприлюднення та запровадження стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам

1. Цей Порядок встановлює механізм розроблення, прийняття, внесення змін, скасування, відновлення дії, оприлюднення та запровадження стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам (далі — стандарти захисту інформації).

Стандарти захисту інформації застосовуються на добровільній основі, крім випадків, якщо обов'язковість їх застосування встановлена нормативно-правовими актами.

Обробка інформації, що міститься в стандартах захисту інформації, їх складових та інших документах, які містять інформацію з обмеженим доступом, що створюється під час їх розроблення, прийняття, внесення змін, скасування, відновлення дії, оприлюднення та запровадження, проводиться відповідно до Законів України "Про доступ до публічної інформації" і "Про державну таємницю", Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, затвердженого постановою Кабінету Міністрів України від 18 грудня 2013 р. № 939, Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затвердженої постановою Кабінету Міністрів України від 19 жовтня 2016 р. № 736 (Офіційний вісник України, 2016 р., № 85, ст. 2783), та цього Порядку.

2. У цьому Порядку терміни вживаються в такому значенні:

життєвий цикл стандартів захисту інформації — сукупність етапів, які проходить стандарт захисту інформації від моменту визначення потреби розроблення до його скасування;

заінтересовані суб'єкти — державні органи, підприємства, установи та організації, військові формування, утворені відповідно до законів України, які у межах компетенції застосовують стандарти захисту інформації;

замовник — заінтересований суб'єкт, в інтересах якого розробляються стандарти захисту інформації за дорученням або на договірних засадах.

Інші терміни вживаються у значенні, наведеному в Законах України “Про основні засади забезпечення кібербезпеки України”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про Державну службу спеціального зв’язку та захисту інформації України”.

3. Суб’єктами стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам є:

Адміністрація Держспецзв’язку;

визначений Адміністрацією Держспецзв’язку орган стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам (далі — орган стандартизації);

заінтересовані суб’єкти.

4. Право власності на стандарти захисту інформації та каталоги таких стандартів належить державі в особі органу стандартизації.

5. Адміністрація Держспецзв’язку:

1) визначає пріоритетні напрями розвитку у сфері стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам;

2) погоджує пропозиції заінтересованих суб’єктів до програми робіт із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам (далі — програма);

3) є замовником робіт із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам;

4) проводить контроль за здійсненням заходів із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам;

5) визначає порядок формування програми;

6) визначає форму технічного завдання на розроблення проекту стандарту захисту інформації;

7) визначає форму пояснювальної записки до проекту стандарту захисту інформації;

8) визначає форму відгуку заінтересованого суб’єкта до проекту стандарту захисту інформації;

9) визначає порядок технічної перевірки проекту стандарту захисту інформації;

10) визначає порядок перевірки та перегляду стандартів захисту інформації;

11) визначає порядок розсилання стандартів захисту інформації з обмеженим доступом;

12) визначає порядок ведення каталогу стандартів захисту інформації;

13) здійснює інші повноваження, визначені законодавством.

6. Орган стандартизації:

1) здійснює розроблення, прийняття, внесення змін, скасування, відновлення дії, оприлюднення стандартів захисту інформації;

2) формує та затверджує програму;

3) приймає за погодженням із Адміністрацією Держспецзв'язку та без включення до програми і узгодження із заінтересованими суб'єктами стандарти захисту інформації, які встановлюють загальні вимоги до розроблення проектів стандартів захисту інформації, їх форму, структуру та техніко-юридичні особливості їх розроблення;

4) проводить технічну перевірку справ стандартів захисту інформації;

5) розробляє, складає та веде каталог стандартів захисту інформації;

6) розповсюджує стандарти захисту інформації;

7) веде фонд стандартів захисту інформації;

8) здійснює інші повноваження, визначені законодавством.

7. Фінансування робіт із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам здійснюється відповідно до вимог законодавства.

8. Життєвий цикл стандартів захисту інформації складається з таких етапів:

1) визначення потреби у розробленні;

2) планування розроблення;

3) розроблення;

4) прийняття;

5) внесення змін за результатами перевірки та перегляду;

6) скасування.

9. Роботи із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам виконуються органом стандартизації відповідно до програми.

10. Програма включає роботи з розроблення, перегляду, скасування стандартів захисту інформації і змін до них.

11. Розроблення проекту стандарту захисту інформації здійснюється органом стандартизації в такому порядку:

1) складення технічного завдання на розроблення проекту стандарту захисту інформації (далі — технічне завдання);

2) розроблення проекту стандарту захисту інформації;

3) формування справи проекту стандарту захисту інформації;

4) технічна перевірка справи проекту стандарту захисту інформації;

5) прийняття проекту стандарту захисту інформації;

6) оприлюднення або розсилання проекту стандарту захисту інформації.

12. Технічне завдання встановлює вимоги до розроблення стандартів захисту інформації, визначає призначення, показники якості, технічні, спеціальні та інші характеристики проекту стандарту захисту інформації та містить опис проекту стандарту і умови застосування стандарту захисту інформації.

Технічне завдання готується органом стандартизації та надсилається на погодження Адміністрації Держспецзв'язку. Адміністрація Держспецзв'язку погоджує технічне завдання або надає вмотивовану відмову органу стандартизації протягом 30 робочих днів з дня його надходження. Керівник органу стандартизації затверджує погоджене технічне завдання.

Зміни до технічного завдання готуються в порядку, встановленому для його підготовки.

13. Орган стандартизації розробляє проект стандарту захисту інформації згідно з технічним завданням та готує пояснювальну записку до нього.

14. Для отримання відгуків до проекту стандарту захисту інформації від заінтересованих суб'єктів орган стандартизації оприлюднює на своєму веб-сайті проект стандарту захисту інформації разом із пояснювальною запискою до нього.

У разі коли проект стандарту захисту інформації містить інформацію з обмеженим доступом, орган стандартизації надсилає такий проект стандарту заінтересованому суб'єкту для підготовки відгуку.

15. Заінтересований суб'єкт надає органу стандартизації у строк, що не перевищує 45 календарних днів з дня надходження на розгляд (оприлюднення) проекту стандарту захисту інформації, відгук до такого проекту стандарту.

16. Керівник заінтересованого суб'єкта надсилає органу стандартизації лист за своїм підписом разом із відгуком до проекту стандарту захисту інформації, в якому зазначає однозначну позицію щодо такого проекту стандарту: погоджено без зауважень, із зауваженнями і пропозиціями.

17. Під час розроблення проекту стандарту захисту інформації вживаються вичерпні заходи для врегулювання розбіжностей (проводяться узгоджувальні процедури, консультації, наради, робочі зустрічі тощо).

18. Орган стандартизації після погодження остаточної редакції проекту стандарту захисту інформації із заінтересованими суб'єктами формує справу стандарту, проводить його технічну перевірку і надає висновок за результатами перевірки.

У разі отримання за результатами технічної перевірки справи стандарту негативного висновку орган стандартизації здійснює заходи з проведення узгоджувальних процедур.

19. Прийняттю підлягають проекти стандартів захисту інформації, які отримали позитивний висновок технічної перевірки справи стандарту.

20. Стандарти захисту інформації приймаються шляхом видання органом стандартизації наказу.

21. Стандарти захисту інформації, що не містять службової інформації або інформації, що становить державну таємницю, розміщуються на веб-сайті органу стандартизації протягом 15 робочих днів з дня їх прийняття.

22. Розсилання стандартів захисту інформації з обмеженим доступом здійснюється у порядку, встановленому Адміністрацією Держспецзв'язку, з дотриманням вимог законодавства у сфері захисту державної таємниці та службової інформації.

23. Внесення змін до стандарту захисту інформації здійснюється органом стандартизації за результатами перевірки та перегляду стандартів захисту інформації.

Необхідність розроблення проекту змін до стандарту захисту інформації визначає замовник за власною ініціативою або за пропозиціями органу стандартизації та/або заінтересованих суб'єктів.

24. Проект змін до стандарту захисту інформації розробляється відповідно до вимог щодо розроблення проекту стандарту захисту інформації.

Технічне завдання на розроблення проекту змін до стандарту захисту інформації не складається.

25. Скасування стандарту захисту інформації здійснюється органом стандартизації за результатами перевірки та перегляду стандартів захисту інформації.

26. Стандарт захисту інформації скасовують, якщо:

1) стандарт захисту інформації суперечить законодавству;

2) стандарт захисту інформації втратив актуальність;

3) розроблено інший стандарт захисту інформації на той самий об’єкт стандартизації;

4) вимоги стандарту захисту інформації суперечать вимогам іншого стандарту захисту інформації на той самий об’єкт стандартизації.

27. Відновлення дії скасованого стандарту захисту інформації здійснюється за пропозицією замовника стандарту захисту інформації, яка надсилається разом з обґрунтуванням до органу стандартизації.

Орган стандартизації опрацьовує пропозицію щодо відновлення дії скасованого стандарту захисту інформації протягом 30 робочих днів з дня її надходження.

Орган стандартизації може відмовити у відновленні дії скасованого стандарту захисту інформації у разі, коли пропозиція замовника суперечить вимогам законодавства або не узгоджується із стандартами захисту інформації. У такому разі орган стандартизації інформує замовника про відхилення його пропозиції із зазначенням причин.

28. У разі врахування пропозиції замовника щодо відновлення дії скасованого стандарту захисту інформації орган стандартизації у строк, визначений у пункті 27 цього Порядку, видає наказ про відновлення дії стандарту захисту інформації із зазначенням дати відновлення його дії.

29. Інформація про прийняті або скасовані протягом одного календарного місяця стандарти захисту інформації, зміни до них та стандарти технічного захисту інформації, дію яких відновлено, оприлюднюється на веб-сайті органу стандартизації або розсилається заінтересованим суб’єктам до 5 числа місяця, що настає за звітним періодом.

30. Для подання заінтересованим суб’єктам інформації про розроблені органом стандартизації стандарти захисту інформації на веб-сайті органу стандартизації оприлюднюються каталоги стандартів захисту інформації та тексти стандартів захисту інформації, що не містять службової інформації або інформації, що становить державну таємницю.

_____