

ПОЯСНЮВАЛЬНА ЗАПИСКА

до першої редакції проєкту стандарту криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам
СТД-03-xxx-2026-В «Захист інформації. Засоби криптографічного захисту інформації. Загальні вимоги»
(далі – стандарт)

1. Підстава для розроблення проєкту стандарту

1.1 Підстави для розроблення проєкту стандарту Держспецзв'язку «Захист інформації. Засоби криптографічного захисту інформації. Загальні вимоги» (далі – Стандарт):

- Наказ Адміністрації Держспецзв'язку від 16 грудня 2025 року № 832 «Про затвердження Порядку формування програми робіт із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, технічної перевірки проєкту стандарту криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, розсилання, перевірки та перегляду стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, ведення їх каталогу та форм документів».

- Постанова Кабінету Міністрів України від 5 листопада 2025 року № 1424 «Про затвердження Порядку розроблення, прийняття, внесення змін, скасування, відновлення дії, оприлюднення та запровадження стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам».

- Наказ Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації від 23.03.2026 № 32 «Про створення робочих груп з розроблення проєктів стандартів» (зі змінами).

- пункт № 4 Програми робіт зі стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам на 2026 рік (частина І), затвердженої наказом ДержНДІ технологій кібербезпеки від 06.04.2026 № 111/ДСК (зі змінами).

2. Термін розроблення

Дата початку робіт: травень 2026 року.

Дата завершення робіт: жовтень 2026 року.

3. Призначення і завдання стандарту

3.1 Стандарт спрямований на упорядкування умов та вимог до розроблення засобів криптографічного захисту інформації (далі – КЗІ) з урахуванням їх призначення та виду інформації, яка захищається.

3.2 Вимоги до побудови засобів КЗІ, а також їх криптографічних якостей, включених до Стандарту, повинні враховувати чинні нормативно-правові акти, міжнародний досвід, а також світові тенденції розвитку технологій КЗІ, визначені у результаті їх комплексного аналізу.

3.3 Необхідність створення Стандарту зумовлена відсутністю упорядкованості вимог до засобів КЗІ відповідних ступенів обмеження доступу у чинних нормативно-правових актах.

3.4 Стандарт обов'язковий для виконання державними органами, підприємствами, установами, а також організаціями незалежно від форм власності, діяльність яких пов'язана з розробленням, виробництвом, сертифікаційними випробуваннями (експертними роботами) або проведенням тематичних досліджень засобів КЗІ.

4. Характеристика об'єкта стандартизації

4.1 Засіб КЗІ – це програмний, апаратно-програмний чи апаратний засіб, призначений для криптографічного захисту інформації.

4.2 До засобів КЗІ належать:

- засоби шифрування інформації;
- засоби, призначені для виготовлення ключових даних або документів та управління ключовими даними, що використовуються засобами КЗІ;

- засоби захисту від нав'язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізують алгоритми криптографічного перетворення інформації (криптоалгоритми), включаючи засоби імітозахисту та електронного цифрового підпису;

- засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані криптоалгоритми.

4.3 Етапи життєвого циклу засобу КЗІ (управління якими гарантується надійність виконання захисних функцій) включають:

- розроблення;
- виробництво;
- експлуатація;
- технічне обслуговування;
- виведення з експлуатації та утилізація.

4.4 Сучасний рівень науково-технічного прогресу та розвиток технологій оброблення інформації потребують єдиного підходу у процесі розробки засобів КЗІ. При цьому, базовою умовою надійного захисту державних інформаційних ресурсів, у тому числі інформації з обмеженим доступом, є наявність стандартів у сфері КЗІ. Саме ці нормативно-правові акти покликані стати підґрунтям, на якому можуть створюватися найсучасніші засоби КЗІ для забезпечення потреб міністерств, відомств, військових формувань та правоохоронних органів.

5. Взаємозв'язок з іншими нормативними документами

5.1 Стандарт повинен бути пов'язаний з наступними чинними нормативними документами:

- Технічний регламент засобів криптографічного захисту інформації, затверджений постановою Кабінету Міністрів України від 21.10. 2020 № 991.

- 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, затверджені наказом Адміністрації Держспецзв'язку від 07.05.2021 № 278, та зареєстровані в Міністерстві юстиції України 26.05.2021 за № 696/36318.

- Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141, зареєстроване у Міністерстві юстиції України 30.07.2007 за № 862/14129 (зі змінами).

5.2 Чинні стандарти криптографічного захисту інформації, які повинні бути переглянуті, замінені або скасовані з дня набрання чинності наказу про прийняття Стандарту:

- 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, затверджені наказом Адміністрації Держспецзв'язку від 07.05.2021 № 278, та зареєстровані в Міністерстві юстиції України 26.05.2021 за № 696/36318.

- Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141, зареєстроване у Міністерстві юстиції України 30.07.2007 за № 862/14129 (зі змінами).

6. Джерела інформації

При розробленні проекту Стандарту необхідно використовувати наступні основні джерела інформації:

- Технічний регламент засобів криптографічного захисту інформації, затверджений постановою кабінету міністрів України від 21.10.2020 № 991.

- 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, затверджені наказом Адміністрації Держспецзв'язку від 07.05.2021 № 278, та зареєстровані в Міністерстві юстиції України 26.05.2021 за № 696/36318.

- Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 20.07.2007 № 141 та зареєстроване в Міністерстві юстиції України 30.07.2007 за № 862/14129 (зі змінами).

- Положення про порядок розроблення, виробництва та введення в експлуатацію засобів криптографічного захисту службової інформації, яке затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14.07.2021 № 116/ДСК та зареєстроване в Міністерстві юстиції України 13.08.2021 за № 806/28936.

- Зміни до Положення про порядок розроблення, виробництва та введення в експлуатацію засобів криптографічного захисту службової інформації, затверджені наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 20.06.2023 № 161/ДСК та зареєстровані в Міністерстві юстиції України 28.07.2024 за №1273/40329.

- Перелік стандартів та технічних специфікацій, дозволених для реалізації в засобах криптографічного захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 27.10.2020 № 687 та зареєстрований в Міністерстві юстиції України 21 грудня 2020 року за № 1272/35555 та №1272/35556 (зі змінами).

- ДСТУ ISO/IEC 15408-1:2023 Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель (ISO/IEC 15408-1:2022, IDT).

- ДСТУ ISO/IEC 15408-2:2022 Інформаційні технології. Методи захисту. Критерії оцінки. Частина 2. Функціональні вимоги (EN ISO/IEC15408-

2:2020, ITD, ISO/IEC 15408-1:2008, IDT.

- ДСТУ ISO/IEC 19790:2015 Інформаційні технології. Методи захисту. Вимоги до безпеки криптографічних модулів (ISO/IEC 19790:2012, IDT).

7. Додаткові дані

7.1 Фінансування робіт передбачається здійснювати за рахунок коштів державного бюджету, у межах видатків, передбачених на діяльність Держспецзв'язку на 2026 рік.

7.2 Гриф обмеження доступу: для відкритого використання (без грифу обмеження доступу).

7.3 Стандарт є базовим нормативним документом у системі стандартів з криптографічного захисту інформації та підлягає перегляду не рідше одного разу на п'ять років, а також позачергово – у разі суттєвих змін нормативно-правової бази у сфері криптографічного захисту інформації, прийняття нових міжнародних стандартів, що регулюють заходи з криптографічного захисту інформації.

8. Дата набрання чинності

Інформацію буде надано до остаточної редакції проєкту стандарту.

9. Інформація про розгляд та погодження проєкту стандарту (для другої (наступної) та остаточної редакцій)

Інформацію буде надано до остаточної редакції проєкту стандарту.

Керівник розробки:

Керівник робочої групи із стандартизації

РГ 03 «КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»

Начальник 1 центру ДержНДІ технологій кібербезпеки

полковник

Дмитро БОНДАРЕНКО