ПОЯСНЮВАЛЬНА ЗАПИСКА
до першої редакції проєкту стандарту криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам
СТД-100-200-ххх-2026-В «Захист інформації. Засоби криптографічного та технічного захисту інформації. Порядок експертних досліджень»
(далі – стандарт)

1. Підстава для розроблення проєкту стандарту

1.1Підстави для розроблення проєкту стандарту Держспецзв'язку «Захист інформації. Засоби криптографічного та технічного захисту інформації. Порядок експертних досліджень» (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».
- 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).
- 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».
- пункт № 1 в Програмі робіт із 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: вересень 2026 року.

3. Призначення і завдання стандарту

3.1Актуальність розроблення Стандарту зумовлена відсутністю

уніфікованого нормативного документа, який би комплексно регламентував процедури експертних досліджень засобів захисту інформації, визначав вимоги до суб'єктів експертних досліджень, об'єктів оцінювання, технічних вимог, технічного протоколу експертних досліджень, звіту експертних досліджень та експертного висновку з урахуванням сучасних міжнародних підходів.

3.2Призначенням Стандарту є встановлення єдиного нормативного порядку проведення експертних досліджень засобів криптографічного захисту інформації (далі - КЗІ) та технічного захисту інформації (далі - ТЗІ), що забезпечить уніфікацію процедур оцінювання безпеки, визначення чітких вимог до суб'єктів експертних досліджень, об'єктів оцінювання, складу технічної документації та результатів експертних досліджень.

3.3Завданням Стандарту є встановлення:

- вимог до суб'єктів експертних досліджень;
- єдиного порядку проведення експертних досліджень;
- правил формування результатів оцінювання.

3.4Очікується, що впровадження Стандарту дасть можливість забезпечити:

- гармонізацію національної практики з вимогами ДСТУ ISO/IEC 15408 та ДСТУ ISO/IEC 18045;
- підвищення рівня довіри до результатів експертних досліджень;
- прозорість та відтворюваність процедур оцінювання;
- створення передумов для міжнародного визнання результатів.

3.5Стандарт призначений для застосування суб'єктами експертних досліджень у сфері КЗІ і ТЗІ та поширюється на засоби КЗІ (крім тих, що призначені для захисту службової інформації і інформації, що становить державну таємницю) та засоби ТЗІ (крім експертних досліджень їх властивостей захисту інформації від витоку технічними каналами).

4. Характеристика об'єкта стандартизації

4.1Об'єктом стандартизації є процес проведення експертних досліджень засобів КЗІ та ТЗІ, що базується на методології оцінювання безпеки інформаційних технологій, включаючи:

- визначення ролей суб'єктів (замовник, експертна організація, експертний орган);
- чітку послідовність етапів (підготовчий, основний, підсумковий), що визначає взаємодію між замовником, експертною організацією та експертним органом;
- застосування критеріїв оцінювання згідно зі стандартами серії ДСТУ ISO/IEC 15408 (частини 1-5);

- процедури проведення оцінювання згідно з ДСТУ ISO/IEC 18045;
- формування результатів;
- супроводження життєвого циклу засобів КЗІ та ТЗІ.

4.2Стандарт повинен відповідати:

- Закону України «Про захист інформації в інформаційно-комунікаційних системах».
- Постанові Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем».
- 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 15408-2:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки» (ISO/IEC 15408-2:2022, IDT).
- ДСТУ ISO/IEC 15408-3:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення» (ISO/IEC 15408-3:2022, IDT).
- ДСТУ ISO/IEC 15408-4:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності» (ISO/IEC 15408-4:2022, IDT).
- ДСТУ ISO/IEC 15408-5:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки» (ISO/IEC 15408-5:2022, IDT).
- ДСТУ ISO/IEC 18045:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Методологія оцінювання безпеки ІТ» (ISO/IEC 18045:2022, IDT).
- Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).
- Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security від 02.07.2014.
- Assurance Continuity: CCRA Requirements від 29.02.2024.
- ISO/IEC TS 9569:2023 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Patch Management Extension for the ISO/IEC 15408 series and ISO/IEC 18045.

5. Взаємозв’язок з іншими нормативними документами

5.1Цей стандарт повинен бути частиною системи нормативних документів у сфері захисту інформації та кібербезпеки України. Стандарт повинен бути пов’язаний з наступними чинними нормативними документами:

- Закон України «Про захист інформації в інформаційно-комунікаційних системах» (щодо обов’язковості державної експертизи).
- Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем», затверджено постановою Кабінету Міністрів України від 29.03.2006 № 373.
- 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 15408-2:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки» (ISO/IEC 15408-2:2022, IDT).
- ДСТУ ISO/IEC 15408-3:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення» (ISO/IEC 15408-3:2022, IDT).
- ДСТУ ISO/IEC 15408-4:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності» (ISO/IEC 15408-4:2022, IDT).
- ДСТУ ISO/IEC 15408-5:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки» (ISO/IEC 15408-5:2022, IDT).
- ДСТУ ISO/IEC 18045:2023 «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Методологія оцінювання безпеки ІТ» (ISO/IEC 18045:2022, IDT).
- Наказ Адміністрації Держспецзв'язку від 23.06.2008 № 100 «Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації», зареєстрований в Міністерстві юстиції України 16.07.2008 за № 651/15342 (зі змінами).
- Наказ Адміністрації Держспецзв’язку від 16.05.2007 № 93 «Про затвердження Положення про державну експертизу у сфері технічного захисту інформації», зареєстрований в Міністерстві юстиції України 16 липня 2007 року за № 820/14087 (зі змінами).

5.2 Чинні стандарти криптографічного захисту інформації, які повинні бути переглянуті, замінені або скасовані з дня набрання чинності наказом про

прийняття Стандарту, відсутні

5.3 Стандарт вводиться вперше та доповнює нормативну базу Держспецзв'язку щодо практичного впровадження Common Criteria в Україні.

5.4 Після набрання чинності Стандарту нормативно-правові акти щодо проведення експертизи у сфері КЗІ та ТЗІ мають бути приведені у відповідність до його положень.

6. Джерела інформації

6.1Під час розроблення проєкту Стандарту необхідно використовувати наступні основні джерела інформації:

- Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем».
- 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 15408-2:2023 (ISO/IEC 15408-2:2022, IDT) «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 2. Функційні компоненти безпеки».
- ДСТУ ISO/IEC 15408-3:2023 (ISO/IEC 15408-3:2022, IDT) «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 3. Компоненти убезпечення».
- ДСТУ ISO/IEC 15408-4:2023 (ISO/IEC 15408-4:2022, IDT) «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 4. Структура для визначення методів оцінювання та діяльності».
- ДСТУ ISO/IEC 15408-5:2023 (ISO/IEC 15408-5:2022, IDT) «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 5. Попередньо визначені пакети вимог до безпеки».
- ДСТУ ISO/IEC 18045:2023 (ISO/IEC 18045:2022, IDT) «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Методологія оцінювання безпеки ІТ».
- Commission Implementing Regulation (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).
- Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security від 02.07.2014.

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 та технічного 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 та технічного захисту інформації, прийняття нових міжнародних стандартів, що регулюють заходи з криптографічного та технічного 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:

Начальник
ДержНДІ технологій кібербезпеки Володимир ПАВЛІКОВ