ПОЯСНЮВАЛЬНА ЗАПИСКА
до першої редакції проєкту стандарту криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам
СТД-200-ххх-2026-Р щодо формування базових вимог до методів аналізу програмного забезпечення на предмет відсутності недокументованих функцій
(далі – Стандарт)

1. Підстава для розроблення проєкту стандарту

1.1 Підстави для розроблення проєкту Стандарту:

– 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».

– № 6 в Програмі робіт зі стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам на 2026 рік (частина ІІ), затвердженої наказом ДержНДІ технологій кібербезпеки від 06.04.2026 № 111/ДСК (зі змінами).

– Пропозиції ДЗІ Адміністрації Держспецзв'язку – лист від 10.03.2026 № 04/01/03–6455/2026/ВН.

2. Термін розроблення

Дата початку робіт: 14 травня 2026 року.

Дата завершення робіт: 30 вересня 2026 року.

3. Призначення і завдання стандарту

3.1 Необхідність створення Стандарту

Необхідність створення стандарту щодо формування базових (загальних, обов'язкових) вимог до методів аналізу програмного забезпечення (ПЗ) на предмет відсутності недокументованих функцій (НДФ) виникла в ході повсякденної діяльності у зв’язку з великою різноманітністю сучасного ПЗ, значними відмінностями в підходах різних розробників до створення ПЗ та підготовки програмної документації.

Сучасний рівень науково-технічного прогресу та розвиток інформаційних технологій потребують єдиного підходу до методів аналізу ПЗ з метою виявлення НДФ. Такий підхід має надавати споживачам необхідний рівень впевненості у відсутності НДФ, в тому числі програмних закладок, при використанні різноманітного ПЗ в ході побудови інформаційно-комунікаційних систем (ІКС).

Базовою умовою для формування такого підходу та, відповідно, надійного захисту державних інформаційних ресурсів, а також інформації з обмеженим доступом, є наявність стандарту, на основі якого можуть бути розроблені найсучасніші методики виявлення НДФ у ПЗ, в тому числі програмних закладок.

Розроблення стандарту забезпечить підвищення впевненості споживачів ПЗ у відсутності НДФ та, як наслідок, зменшення виробничих витрат при впровадженні заходів захисту інформації в ІКС міністерств, державних установ, відомств, військових формувань та правоохоронних органів.

Розроблення стандарту дозволить упорядкувати методи аналізу ПЗ з урахуванням його призначення, інших специфічних особливостей, та необхідної міри впевненості у відсутності НДФ.

3.2 Призначення Стандарту

Стандарт визначає критерії оцінки ПЗ на предмет відсутності НДФ та визначає методи аналізу та групи методів аналізу, рекомендованих для пошуку НДФ у ПЗ, в тому числі із закритим вихідним кодом, та методику оцінки рівня гарантій (рівня упевненості) відсутності НДФ у ПЗ.

Стандарт призначений для встановлення єдиних вимог і підходів до аналізу ПЗ з метою забезпечення його безпечності, прозорості та відповідності задекларованим характеристикам.

3.3 Завдання створення Стандарту

До основних завдань Стандарту належать:

- встановлення чітких і формалізованих критеріїв оцінювання ПЗ щодо відсутності НДФ;
- визначення та класифікація методів аналізу ПЗ (зокрема статичних, динамічних та гібридних методів);
- формування груп методів аналізу, рекомендованих для виявлення НДФ;
- забезпечення єдності підходів до проведення перевірок і тестування ПЗ;
- підвищення об’єктивності, достовірності та відтворюваності результатів оцінювання;
- надання рекомендацій щодо застосування інструментальних засобів аналізу;
- сприяння виявленню потенційних загроз інформаційній безпеці, пов’язаних із наявністю прихованих НДФ;
- підвищення рівня довіри до ПЗ, що використовується в ІКС, зокрема критичного призначення.

3.4 Сфера застосування Стандарту

Стандарт стосується процесів тестування безпеки комп’ютерних програм (їх оновлення), програмних продуктів, програмних засобів та ПЗ, яке використовується для оброблення, передавання, зберігання відкритої інформації та інформації з обмеженим доступом.

4. Характеристика об’єкта стандартизації

Стандарт встановлює вимоги до оцінювання програмного забезпечення з метою виявлення НДФ, які можуть створювати загрози інформаційній безпеці. Документ визначає критерії оцінки, а також регламентує застосування методів аналізу, зокрема статичних, динамічних і гібридних, для забезпечення всебічного дослідження ПЗ. Його положення спрямовані на підвищення прозорості функціонування ПЗ, забезпечення довіри до нього та мінімізацію ризиків прихованих НДФ.

Положення стандарту узгоджуються з вимогами чинного законодавства у сферах криптографічного та технічного захисту інформації, кіберзахисту, а також протидії технічним розвідкам. Зокрема, він сприяє реалізації вимог щодо забезпечення конфіденційності, цілісності та доступності інформації, запобігання несанкціонованому доступу, витоку або модифікації даних, а також виявлення потенційних каналів прихованого впливу чи витоку інформації через ПЗ.

Стандарт є важливим елементом нормативно-правової бази у сфері інформаційної безпеки та забезпечує комплексний підхід до аналізу ПЗ в контексті сучасних кіберзагроз.

5. Взаємозв’язок з іншими нормативними документами

Чинні нормативні документи зі стандартизації, з якими повинен бути пов'язаний стандарт:

– Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем».

– Наказ Адміністрації Держспецзв’язку № 93 від 16.05.2007 «Про затвердження Положення про державну експертизу у сфері технічного захисту інформації», зареєстрований в Міністерстві юстиції України 16 липня 2007 року за № 820/14087.

– Наказ Адміністрації Держспецзв’язку № 278 від 07.05.2021 «Про затвердження Вимог 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», зареєстрований в Міністерстві юстиції України 26 травня 2021 року за № 696/36318.

Чинні стандарти у сфері кіберзахисту, які повинні бути переглянуті, замінені або скасовані з дня набрання чинності наказом про прийняття стандарту, який розробляється:

– відсутні (стандарт є першим нормативним документом у даній предметній сфері).

6. Джерела інформації

Під час розроблення проєкту стандарту необхідно використати такі основні джерела інформації:

– 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 18045:2023 (ISO/IEC 18045:2022, IDT) «Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Методологія оцінювання безпеки ІТ».

– ДСТУ 2851-94. Програмні засоби ЕОМ. Документування результатів випробувань.

– ДСТУ 2853-94. Програмні засоби ЕОМ. Підготовка і проведення випробувань.

– ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

– НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

– НД ТЗІ 1.6-002-03 «Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації».

7. Додаткові дані

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

Ступінь обмеження доступу стандарту: для службового користування (ДСК)

Стандарт є базовим нормативним документом у системі стандартів сфери кіберзахисту та підлягає перегляду не рідше одного разу на п'ять років, а також позачергово – у разі суттєвих змін у нормативно-правовій базі у сфері кібербезпеки, появи нових видів кіберзагроз або прийняття нових міжнародних стандартів, що регулюють заходи з кіберзахисту

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:
РГ 2 «ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»