ПОЯСНЮВАЛЬНА ЗАПИСКА
до першої редакції проєкту стандарту криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам

СТД-02-ххх-2026-В «Захист інформації. Технічний захист інформації. Порядок виконання вимог з безпеки в інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних системах»
(далі – стандарт)

1. Підстава для розроблення проєкту стандарту

1.1Підстави для розроблення проєкту стандарту Держспецзв’язку «Захист інформації. Технічний захист інформації. Порядок виконання вимог з безпеки в інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних системах» (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».

- Статут Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, затверджений наказом Адміністрації Держспецзв'язку від 19.09.2017 № 517 (зі змінами згідно наказу Адміністрації Держспецзв'язку від 10.06.2025 № 362).

- 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).

- № 3 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: жовтень 2026 року.

3. Призначення і завдання стандарту

3.1 Розроблення Стандарту здійснюється з метою встановлення єдиного підходу до організації виконання вимог з безпеки інформації в інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних системах. Під час розроблення Стандарту передбачається проаналізувати чинні нормативно-правові акти у сфері захисту інформації, міжнародний досвід та сучасні практики організації інформаційної безпеки з метою формування структурованого порядку впровадження системи безпеки інформації.

3.2 Розробка Стандарту сприятиме подальшому розвитку науково-технічного та виробничого потенціалу в сфері технічного захисту інформації.

3.3 Необхідність розроблення такого Стандарту зумовлена наявністю вимог щодо захисту інформації у значній кількості нормативно-правових актів, які регулюють окремі аспекти організації захисту інформації, проте не визначають єдиного узгодженого порядку виконання вимог з безпеки інформації. Відсутність систематизованого підходу призводить до різного трактування вимог законодавства, застосування різнорідних практик під час створення систем безпеки інформації та ускладнює планування і реалізацію заходів із захисту інформації.

3.4 Сучасний розвиток інформаційно-комунікаційних технологій, цифровізація державного управління та широке використання інформаційних ресурсів потребують застосування узгоджених і системних підходів до впровадження заходів безпеки інформації. Визначення на рівні Стандарту єдиного порядку планування, організації, впровадження та супроводження заходів захисту інформації дозволить забезпечити належний рівень захисту інформації, вимога щодо захисту якої встановлена законом, з урахуванням

сучасних технологій, міжнародного досвіду та для забезпечення потреб міністерств, відомств, військових формувань та правоохоронних органів.

3.5Розроблення Стандарту сприятиме впорядкуванню організаційних і технічних процесів виконання вимог з безпеки інформації, підвищенню ефективності реалізації заходів захисту інформації та формуванню єдиної практики їх застосування. Запровадження Стандарту також створить передумови для подальшого розвитку нормативної та методичної бази у сфері захисту інформації та підвищення рівня захищеності державних інформаційних ресурсів.

4. Характеристика об’єкта стандартизації

4.1 Стандарт визначає основи організації та порядок виконання вимог з безпеки інформації в інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних системах.

4.2 Положення Стандарту узгоджуються з вимогами чинного законодавства і сфері технічного захисту інформації.

4.3 Вимоги Стандарту поширюються на інформаційні, електронні комунікаційні, інформаційно-комунікаційні, технологічні системи.

4.4 Стандарт застосовується для захисту відкритої інформації, яка міститься в інформаційних системах, а також для вибору та реалізації заходів захисту спрямованих на забезпечення конфіденційності, цілісності та доступності інформації.

5. Взаємозв’язок з іншими нормативними документами

5.1 Стандарт має бути взаємопов’язаний з наступними 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».

- Постанова Кабінету Міністрів України № 712 від 18.06.2025 р. «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем».

- ДСТУ 7731:2015 «Інформаційні технологій. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, MOD)».

- НД ТЗІ 3.6-006-24 «Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

- НД ТЗІ 3.6-007-21 «Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем».

5.2 Чинні стандарти технічного захисту інформації, які повинні бути переглянуті, замінені або скасовані з дня набрання чинності наказом про прийняття Стандарту, відсутні.

5.3 Після набрання чинності Стандартом внутрішні відомчі інструкції мають бути приведені у відповідність до його положень.

6. Джерела інформації

Під 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».

- Постанова Кабінету Міністрів України № 712 від 18.06.2025 р. «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем».

- ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
- ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
- ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
- ДСТУ 7731:2015 Інформаційні технологій. Методи захисту. Основні положення щодо забезпечення невтручання в особисте життя (ISO/IEC 29100:2011, MOD).
- НД ТЗІ 3.6-006-24 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем.
- НД ТЗІ 3.6-007-21 Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем.
- НД ТЗІ 2.3-025-24 Методика оцінювання заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем.
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), Version 1.1, April 2018.
- NIST Special Publication 800-30. Rev.1. Guide for Conducting Risk Assessments, 2012.
- NIST Special Publication 800-37. Rev.2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 2018.
- NIST Special Publication 800-39. Managing Information Security Risk: Organization, Mission, and Information System View, 2011.
- NIST Special Publication 800-53. Rev.5 Security and Privacy Controls for Information Systems and Organizations, 2020.

- NIST Special Publication 800-128. Guide for Security-Focused Configuration Management of Information Systems, 2011.

- NIST Special Publication 800-160 Vol. 1. Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, 2018.

- NIST Special Publication 800-160 Vol. 2. Developing Cyber Resilient Systems: A Systems Security Engineering Approach, 2019.

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).

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.

Керівники розробки:

Керівник робочої групи із стандартизації
РГ02 «ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»
Начальник 2 науково-дослідного центру
ДержНДІ технологій кібербезпеки
полковник Сергій ЛИСЕНКО

Керівник підгрупи робочої групи із стандартизації
РГ02 «ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ»
Заступник начальника 4 центру технічного захисту інформації
ДержНДІ технологій кібербезпеки
підполковник Ігор НАВРОЦЬКИЙ