

ПОЯСНЮВАЛЬНА ЗАПИСКА

до першої редакції проєкту стандарту криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам
СТД-04-002-2026-В «Заходи з кіберзахисту. Загальні положення та настанови»
(далі – стандарт)

1. Підстава для розроблення проєкту стандарту

1.1 Підстави для розроблення проєкту стандарту Держспецзв'язку «Заходи з кіберзахисту. Загальні положення та настанови» (далі – Стандарт):

- Закон України від 05 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України»;
- Указ Президента України від 26 серпня 2021 року № 447 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»»;
- Постанова Кабінету Міністрів України від 05 листопада 2025 р. № 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 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 02.09.2026 № 111 «Про створення нових робочих груп з розроблення проєктів стандартів»;
- № 6 Програми робіт із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам на 2026 рік (частина І), затвердженої наказом ДержНДІ технологій кібербезпеки № 290/ДСК від 28.08.2026 року.

2. Строк розроблення стандарту

Дата початку робіт: 14 травня 2026 року.

Дата завершення робіт: 30 листопада 2026 року.

3. Призначення і завдання стандарту

В умовах зростання кількості кібератак, спрямованих проти об'єктів критичної інформаційної інфраструктури (далі – ОКІІ) та інформаційно-комунікаційних систем (далі – ІКС) органів державної влади та місцевого самоврядування, суб'єкти кіберзахисту позбавлені єдиного, систематизованого та методологічно узгодженого нормативного документа, який би визначав загальні засади планування, впровадження, контролю та вдосконалення заходів з кіберзахисту.

Відсутність уніфікованих загальних положень та настанов спричиняє неузгодженість у застосуванні заходів кіберзахисту різними організаціями, ускладнює аудит та оцінювання стану захищеності ІКС, а також знижує ефективність взаємодії між суб'єктами у сфері кібербезпеки. Зазначена проблема призводить до підвищення ризиків реалізації кібератак, витоку інформації та порушення функціонування ОКІІ.

Стандарт призначений для встановлення загальних положень та уніфікованих настанов щодо формування, планування, реалізації та контролю заходів з кіберзахисту ІКС, у яких обробляється інформація, що підлягає захисту відповідно до законодавства України, а також ОКІІ.

Кінцевими результатами розроблення та введення в дію галузевого стандарту є:

- встановлення єдиної термінологічної та концептуальної бази у сфері кіберзахисту;
- визначення принципів, цілей та загальної структури системи заходів кіберзахисту;
- формування вимог до процесів планування, впровадження, моніторингу, реагування та вдосконалення заходів кіберзахисту;
- забезпечення методологічної узгодженості галузевого стандарту з міжнародними стандартами серії ISO/IEC 27000, NIST Cybersecurity Framework 2.0 та директивами ЄС у сфері мережевої та інформаційної безпеки (NIS2).

Стандарт поширюється на сферу стандартизації – кіберзахист.

4. Характеристика об'єкта стандартизації

Об'єктом стандартизації є заходи з кіберзахисту – сукупність організаційних, технічних, правових та кадрових дій, що застосовуються

суб'єктами кіберзахисту з метою забезпечення кіберзахисту інформаційних технологій, ІКС та інформації, що в них обробляється, від кіберзагроз.

Об'єкт стандартизації відповідає принципам стандартизації у сфері кібербезпеки, зокрема:

- принципу науковості – вимоги до заходів ґрунтуються на сучасних наукових підходах та кращих практиках у сфері кібербезпеки;
- принципу системності – заходи розглядаються як єдина взаємопов'язана система засобів і методів захисту;
- принципу гармонізації – положення стандарту розроблені з урахуванням вимог міжнародних стандартів серії ISO/IEC 27000 та NIST Cybersecurity Framework 2.0;
- принципу практичної придатності – вимоги сформульовані з урахуванням реальних умов застосування інформаційних технологій суб'єктами кіберзахисту.

5. Взаємозв'язок з іншими нормативними документами

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

- Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.
- Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР.
- ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT);
- ДСТУ EN ISO/IEC 27002:2024 Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки (EN ISO/IEC 27002:2022, IDT; ISO/IEC 27002:2022, IDT);
- ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT)
- Директива (ЄС) 2022/2555 (NIS2) щодо заходів для забезпечення високого спільного рівня кібербезпеки в усьому Союзі.

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:

- 1) ДСТУ ISO/IEC 27001:2023, ДСТУ EN ISO/IEC 27002:2024, ДСТУ ISO/IEC 27005:2023 – управління інформаційною безпекою та ризиками.
- 2) NIST Cybersecurity Framework (CSF) 2.0 – рамкова структура кібербезпеки NIST.
- 3) NIST SP 800-53 Rev. 5 «Security and Privacy Controls for Information Systems and Organizations».
- 4) Директива NIS2 (ЄС) 2022/2555 та відповідні імплементаційні акти.
- 5) CIS Controls v8 – практичні заходи захисту від кіберзагроз Центру інтернет-безпеки.
- 6) ENISA Guidelines on Cybersecurity Measures (Агентство Європейського Союзу з кібербезпеки).
- 7) Матриця MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).
- 8) Чинні нормативно-технічні документи у сфері технічного та криптографічного захисту інформації (НД ТЗІ серії 1, 2, 3).
- 9) Матеріали CERT-UA щодо актуальних кіберзагроз та рекомендованих захисних заходів (2022–2026).
- 10) Каталог загроз IT-Grundschutz, розроблений Федеральним управлінням з інформаційної безпеки Німеччини (BSI).
- 11) Стратегія кібербезпеки України (2021).
- 12) Наукові та аналітичні праці вітчизняних і зарубіжних дослідників у сфері кіберзахисту.

7. Додаткові дані

Джерело фінансування: реалізація виконання робіт буде здійснюватися в межах бюджетних призначень, передбачених Держспецзв'язку на 2026 рік.

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

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:

Керівник робочої групи із стандартизації

РГЗ «КІБЕРЗАХИСТ»

Начальник 5 центру ДержНДІ технологій кібербезпеки

полковник

Максим КОМАРОВ