ПОЯСНЮВАЛЬНА ЗАПИСКА
до першої редакції проєкту стандарту криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам
СТД-300-001-2026-В «Модель зрілості організаційно-технічної спроможності команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT)»
(далі – стандарт)

1. Підстава для розроблення проєкту стандарту

1.1 Підстави для розроблення проєкту стандарту Держспецзв'язку «Модель зрілості організаційно-технічної спроможності команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT)» (далі – Стандарт):

- Закон України від 05 червня 2014 року № 1315-VII «Про стандартизацію»;
- Закон України від 05 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України»;
- Закон України від 23 лютого 2006 року № 3475-IV «Про Державну службу спеціального зв'язку та захисту інформації 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»»;
- 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»;
- № 7 Програми робіт із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам на 2026 рік (частина І), затвердженої наказом ДержНДІ технологій кібербезпеки № 111/ДСК від 06.04.2026 року.

2. Термін розроблення

Дата початку робіт: 14 травня 2026 року.
Дата завершення робіт: 30 вересня 2026 року.

3. Призначення і завдання стандарту

Зростання кількості та рівня складності кіберінцидентів в Україні, у тому числі в умовах дії правового режиму воєнного стану, виявило відсутність єдиного методологічного підходу до визначення та оцінювання рівня спроможності команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT). Відсутність такого підходу унеможливлює об'єктивне порівняння потенціалу різних CSIRT, планування заходів із розвитку їх спроможностей та забезпечення їх відповідності міжнародним стандартам і найкращим практикам.

Кінцевими результатами розроблення та введення в дію стандарту є:

– запровадження єдиної моделі зрілості CSIRT, яка охоплює організаційні параметри, параметри персоналу, інструментів та процесів;

– визначення методу оцінювання зрілості для кожного параметра;

– встановлення порядку проведення оцінювання організаційно-технічної спроможності CSIRT;

– забезпечення методологічної основи для планування розвитку спроможностей CSIRT та моніторингу їх ефективності.

Стандарт поширюється на сферу стандартизації – кіберзахист.

4. Характеристика об’єкта стандартизації

Об'єктом стандартизації є модель зрілості організаційно-технічної спроможності CSIRT – структурована сукупність категорій, параметрів, вимог та критеріїв, що дозволяє систематично оцінювати та розвивати спроможності команди реагування на кіберінциденти, кібератаки, кіберзагрози.

Об'єкт стандартизації відповідає принципам стандартизації у сфері кіберзахисту, зокрема: принципу науковості – модель ґрунтується на міжнародних стандартах (ISO/IEC 27035, ENISA CSIRT Maturity Framework, Security Incident Management Maturity Model (SIM3 v2)) та вітчизняних наукових дослідженнях; принципу відкритості та прозорості – вимоги моделі є явними та перевірними; принципу гармонізації з міжнародними стандартами – модель враховує положення відповідних міжнародних і регіональних стандартів та рекомендацій; принципу практичної придатності – модель розроблена з урахуванням особливостей функціонування CSIRT в умовах реальних кіберзагроз.

5. Взаємозв’язок з іншими нормативними документами

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

– Закон України від 05 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки України»;

– Закон України від 5 липня 1994 року № 80/94-ВР «Про захист інформації в інформаційно-комунікаційних системах»;

– Постанова Кабінету Міністрів України від 26 листопада 2025 р. № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози»;

– НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»;

– НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»;

– ISO/IEC 27001:2022 «Інформаційна безпека, кібербезпека та захист конфіденційності – Системи управління інформаційною безпекою – Вимоги»;

– ISO/IEC 27035-1:2023 «Управління інцидентами інформаційної безпеки – Частина 1: Принципи та процес»;

– ДСТУ ISO/IEC 27001:2015 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»;

–Наказ Адміністрації Держспецзв’язку від 3 лютого 2026 року № 87 «Про затвердження Вимог до організаційно-технічної спроможності національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA), галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT)».

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:

– ENISA CSIRT Maturity Framework (Агентство Європейського Союзу з кібербезпеки, 2020);

– Security Incident Management Maturity Model (SIM3 v2) (2023);

– ISO/IEC 27035-1:2023, ISO/IEC 27035-2:2023 – управління інцидентами інформаційної безпеки;

– RFC 2350 «Expectations for Computer Security Incident Response» (IETF, 1998);

– FIRST (Forum of Incident Response and Security Teams) – матеріали щодо стандартів та найкращих практик діяльності CSIRT/CERT;

– Матеріали НКЦК (Національного координаційного центру кібербезпеки) щодо організації реагування на кіберінциденти в Україні;

– Звіти CERT-UA про стан кіберзагроз та кіберінцидентів (2022–2025);

– Директива NIS2 (ЄС);

– Матеріали Рамки кібербезпеки NIST (CSF 2.0) у частині реагування на інциденти;

– Нормативно-правові акти у сфері кіберзахисту та захисту інформації в Україні.

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.

Керівники розробки:

Керівник робочої групи із стандартизації
РГ3 «КІБЕРЗАХИСТ»
Начальник 5 центру ДержНДІ технологій кібербезпеки
полковник Максим КОМАРОВ