**КЛАСИФІКАТОР**
**ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ**
**ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ**

# КЛАСИФІКАТОР СТАНДАРТІВ КРИПТОГРАФІЧНОГО ТА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, КІБЕРЗАХИСТУ, ПРОТИДІЇ ТЕХНІЧНИМ РОЗВІДКАМ

**КСД 001:2026**

**Київ**
**Державний науково-дослідний інститут**
**технологій кібербезпеки та захисту інформації**
**2026**

# Передмова

**ЗАМОВЛЕНО:** Адміністрація Державної служби спеціального зв’язку та захисту інформації України (Адміністрація Держспецзв’язку)

**РОЗРОБЛЕНО:** Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації (ДержНДІ технологій кібербезпеки)

**РОЗРОБНИКИ:** Володимир ПАВЛІКОВ, д-р техн. наук, проф.; Роман ЦИРЕНЬ; Кирило ГУЛЯЄВ, канд. техн. наук, ст. наук. співроб.; Ростислав КРАВЧЕНКО, канд. техн. наук, ст. дослідник; Олексій ПОНОМАРЬОВ

**ЗАТВЕРДЖЕНО:** наказ Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації від 17.06.2026 № 77

**ЧИННИЙ З:** 17.06.2026

**УВЕДЕНО ВПЕРШЕ**

**НАДАЄ РОЗ’ЯСНЕННЯ ЩОДО ПОЛОЖЕНЬ КЛАСИФІКАТОРА:**
ДержНДІ технологій кібербезпеки

**Зміст**

# КЛАСИФІКАТОР СТАНДАРТІВ КРИПТОГРАФІЧНОГО ТА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, КІБЕРЗАХИСТУ, ПРОТИДІЇ ТЕХНІЧНИМ РОЗВІДКАМ

CLASSIFIER OF STANDARDS
FOR CRYPTOGRAPHIC AND TECHNICAL INFORMATION PROTECTION, CYBER PROTECTION, COUNTERACTION TO TECHNICAL INTELLIGENCE

**КСД 001:2026**

## Вступ

Класифікатор стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам (далі – КСД) розроблено для структурування каталогу стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, розроблених ДержНДІ технологій кібербезпеки – органом стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам (далі – Орган стандартизації).

КСД розроблено з урахуванням Українського класифікатора нормативних документів (НК 004:2020).

Ведення КСД виконує Орган стандартизації.

## 1 Сфера застосування

КСД призначений для структурування каталогів стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, а також інших стандартів і нормативних документів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, зокрема міжнародних, європейських та національних. КСД можна також застосовувати для систем замовлення стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам

(далі – СТД) у базах даних, бібліотеках тощо.

## 2 ТЕРМІНИ ТА ЇХ ВИЗНАЧЕННЯ

У КСД терміни та визначення вживаються у значеннях, наведених у:

Законі України від 23 лютого 2006 року № 3475-IV «Про Державну службу спеціального зв'язку та захисту інформації України»;

Законі України від 5 жовтня 2017 року № 2163-VIII «Про основні засади забезпечення кібербезпеки»;

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

Порядку розроблення національних класифікаторів, затвердженому наказом Міністерства економічного розвитку і торгівлі України від 11.01.2018 № 17, зареєстрованим в Міністерстві юстиції України 31 січня 2018 р. за № 124/31576.

## 3 ПОЗНАКИ ТА СКОРОЧЕННЯ

У КСД використано такі познаки та скорочення:

КЗІ – криптографічний захист інформації

КСД – класифікатор стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам

ПДТР – протидія технічним розвідкам

СТД – стандарти криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам

ТЗІ – технічний захист інформації

УКНД – Український класифікатор нормативних документів

## 4 ЗАГАЛЬНІ ПОЛОЖЕННЯ

**4.1** У КСД термін «СТД» застосовується до стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, інших стандартів і нормативних документів криптографічного та технічного

захисту інформації, кіберзахисту, протидії технічним розвідкам, зокрема міжнародних, європейських і національних, а також до їхніх проєктів.

**4.2** КСД є ієрархічним дворівневим класифікатором. Наступний рівень класифікації не змінює значення попереднього рівня.

Код позиції класифікатора має таку структуру:

XX.YY

де XX — клас (рівень класифікації 1);

XX.YY — група (рівень класифікації 2).

Алфавіт коду – цифровий. Довжина коду – чотири значущих цифри. Розділовий знак – «.» (крапка).

**4.3** Рівень класифікації 1 охоплює сфери стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, а також захист інформації в цілому.

**4.4** Класи поділено на групи (рівень класифікації 2). Позначення групи складається з коду класу та двозначного цифрового коду, відокремлених крапкою.

**4.5** До груп з кодом, який закінчується на «.99», належать СТД на об’єкти стандартизації, які не належать ні до об’єктів загальних положень, ні до об’єктів конкретних положень.

## 5 ПРАВИЛА КОРИСТУВАННЯ КСД

**5.1** Для визначення класифікаційних кодів СТД треба застосовувати найостанніше видання КСД з усіма наступними змінами до нього.

**5.2** СТД треба класифікувати відповідно до їхніх об’єктів стандартизації. Спочатку визначають відповідний код класу для даного об’єкта, потім — відповідний код групи, якщо клас поділено на групи.

Якщо визначити сферу застосування СТД за його змістом важко, можна взяти до уваги сферу діяльності відповідної робочої групи, відповідальної за розроблення стандарту.

**5.3** Абетковий покажчик КСД можна використовувати як додатковий

інструмент для ідентифікації відповідних класів і груп СТД.

**5.4** Рекомендовано використовувати всі рівні, придатні для класифікування СТД. Наприклад СТД з назвою:

«Базові вимоги до засобів криптографічного захисту інформації»

необхідно відносити до групи 03.01 (рівень класифікації 2) і не рекомендовано надавати код 03 (рівень класифікації 1), оскільки це може утруднювати обмін даними між базами даних і ускладнити застосування КСД в інформаційних системах.

**5.5** За цим класифікатором СТД можна відносити більше ніж до однієї групи. Наприклад, СТД з назвою:

«Захист інформації. Засоби криптографічного та технічного захисту інформації. Порядок експертних досліджень»

необхідно віднести до одного класу і двох груп:

02.05 Класифікація, вимоги та рекомендації щодо засобів ТЗІ;

03.05 Порядок оцінювання та випробування засобів КЗІ;

06 Оцінювання відповідності, сертифікація, атестація, аудит, експертні та тематичні дослідження, випробування засобів, систем, комплексів, персоналу, організацій.

**5.6** СТД, що має терміни та визначення понять, застосовні тільки в ньому, не допустимо відносити до групи:

01.04 Термінологічні стандарти

**5.7** Зміни або поправки до СТД повинні мати такі самі коди, що й СТД, до якого вносяться зміни або поправки.

**5.8** Якщо клас поділено на групи, то СТД надають тільки код групи.

**5.9** Для розділення кодових позначень у друкованих документах треба використовувати крапку з комою. Для забезпечення послідовності в поданні кодових позначень вони мають бути відсортовані за зростанням числового порядку, наприклад: Код КСД: 02.05; 03.05; 06.

**5.10** Про виявлені помилки в кодових позначеннях через неправильне використання СТД, перенесення цифр, друкарські помилки тощо потрібно повідомити Орган стандартизації.

## 6 ОНОВЛЕННЯ КСД

**6.1** КСД оновлюють відповідно до потреб. Будь-який користувач може подати пропозиції щодо модифікацій та/або доповнень до КСД. Такі пропозиції треба надсилати Органу стандартизації.

**6.2** Усі отримані пропозиції розглядаються у встановленому законодавством порядку.

## 7 ЗВ'ЯЗОК МІЖ КСД ТА УКНД

Зв'язок між КСД та УКНД надано в таблиці відповідності додатка А.

## 8 АБЕТКОВИЙ ПОКАЖЧИК

**8.1** Абетковий покажчик (див. додаток Б) представлено у формі ключового слова в контексті. Назви всіх класів/груп з'являються під усіма словами (ключовими словами), які вони містять, за винятком стоп-слів. Це слова, які не є суттєвими для цілей пошуку. Вони охоплюють приписи та такі слова, як «і», «деякі», «інші», «будь-які» тощо.

**8.2** Ключові слова (виділені жирним шрифтом) розташовано в абетковому порядку в одному стовпчику на сторінці.

**8.3** Ключові слова відокремлено від назв класів/груп символом «•».

**8.4** Позначення класів/груп подано в стовпці ліворуч. Відповідно до їх чисел, відповідні класи/групи легко виявити в систематичній таблиці класів і груп.

## 9 КЛАСИФІКАЦІЙНА ТАБЛИЦЯ

| Код | Назва класифікаційного угруповання |
|---|---|
| **01** | **Загальні положення із стандартизації у сфері захисту інформації** |
| 01.01 | Процедури створення та діяльності робочих груп із стандартизації |
| 01.02 | Порядок проведення робіт із стандартизації |
| 01.03 | Вимоги до розроблення стандартів<br>*Охоплює також правила розроблення змін і поправок до стандартів |
| 01.04 | Термінологічні стандарти<br>* Стандарти цієї групи необхідно також долучати до інших груп відповідно до їхніх об’єктів стандартизації |
| 01.99 | Інші стандарти щодо загальних положень із стандартизації |
| **02** | **Технічний захист інформації (ТЗІ)** |
| 02.01 | Загальні положення та порядок організації робіт з ТЗІ |
| 02.02 | Захист інформації від витоку каналами побічних електромагнітних випромінювань і наведень та акустоелектричними каналами |
| 02.03 | Захист інформації від витоку акустичними, віброакустичними, лазерними акустичними та акустооптичними каналами |
| 02.04 | Захист інформації від витоку каналами високочастотного нав’язування |
| 02.05 | Класифікація, вимоги та рекомендації щодо засобів ТЗІ |
| 02.06 | Методи та засоби виявлення закладних пристроїв |
| 02.99 | Інші стандарти щодо ТЗІ |
| **03** | **Криптографічний захист інформації (КЗІ)** |
| 03.01 | Загальні положення та профілі щодо КЗІ |
| 03.02 | Криптографічні алгоритми та протоколи |
| 03.03 | Управління ключовими даними |
| 03.04 | Засоби КЗІ |
| 03.05 | Порядок оцінювання та випробування засобів КЗІ |
| 03.99 | Інші стандарти щодо КЗІ |
| **04** | **Кіберзахист** |
| 04.01 | Загальні положення та національна система кіберзахисту |

| Код | Назва класифікаційного угруповання |
|---|---|
| 04.02 | Впровадження заходів з кіберзахисту |
| 04.03 | Кіберзахист інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та комунікаційних мереж |
| 04.04 | Кіберзахист інформаційних ресурсів та програмного забезпечення |
| 04.05 | Реагування на кіберінциденти, кібератаки, кіберзагрози |
| 04.06 | Організація, функціонування та керування підрозділами з кіберзахисту |
| 04.07 | Управління ризиками у сфері кібербезпеки |
| 04.08 | Безпека ланцюгів постачання |
| 04.09 | Система управління штучним інтелектом |
| 04.10 | Кіберзахист систем управління технологічними процесами |
| 04.99 | Інші стандарти щодо кіберзахисту |
| **05** | **Протидія технічним розвідкам (ПДТР)** |
| 05.01 | Загальні положення та профілі щодо ПДТР |
| 05.02 | Протидія радіоелектронній розвідці |
| 05.03 | Протидія оптико-електронній та оптичній розвідкам |
| 05.04 | Протидія акустичній, гідроакустичній та сейсмічній розвідкам |
| 05.05 | Протидія хімічній, радіаційній та біологічній розвідкам |
| 05.06 | Методи та засоби виявлення засобів технічної розвідки |
| 05.99 | Інші стандарти щодо ПДТР |
| **06** | **Оцінювання відповідності, сертифікація, атестація, аудит, експертні та тематичні дослідження, випробування засобів, систем, комплексів, персоналу, організацій**<br>* Стандарти цієї групи необхідно також долучати до інших груп відповідно до їхніх об’єктів стандартизації |

Додаток А

(довідковий)

## ТАБЛИЦЯ ВІДПОВІДНОСТІ МІЖ КСД ТА УКНД

| **Коди та назви угруповань** | | | |
|---|---|---|---|
| **КСД** | | **УКНД** | |
| 01 | Загальні положення із стандартизації у сфері захисту інформації | 01 | Загальні положення. Термінологія. Стандартизація. Документація |
| 01.01 | Процедури створення та діяльності робочих груп із стандартизації | 01.120 | Стандартизація. Загальні правила |
| 01.02 | Порядок проведення робіт із стандартизації | 01.120 | Стандартизація. Загальні правила |
| 01.03 | Вимоги до розроблення стандартів | 01.120 | Стандартизація. Загальні правила |
| 01.04 | Термінологічні стандарти | 01.040.35 | Інформаційні технології (Словники термінів) |
| 01.99 | Інші стандарти щодо загальних положень із стандартизації | 01.120 | Стандартизація. Загальні правила |
| 02 | Технічний захист інформації (ТЗІ) | 35.030 | Безпека інформаційних технологій |
| 02.01 | Загальні положення та порядок організації робіт з ТЗІ | 35.030 | Безпека інформаційних технологій |
| 02.02 | Захист інформації від витоку каналами побічних електромагнітних випромінювань і наведень та акустоелектричними каналами | 35.030 | Безпека інформаційних технологій |
| 02.03 | Захист інформації від витоку акустичними, віброакустичними, лазерними акустичними та акустооптичними каналами | 35.030 | Безпека інформаційних технологій |
| 02.04 | Захист інформації від витоку каналами високочастотного нав’язування | 35.030 | Безпека інформаційних технологій |
| 02.05 | Класифікація, вимоги та рекомендації щодо засобів ТЗІ | 35.030 | Безпека інформаційних технологій |
| 02.06 | Методи та засоби виявлення закладних пристроїв | 35.030 | Безпека інформаційних технологій |
| 02.99 | Інші стандарти щодо ТЗІ | 35.030 | Безпека інформаційних технологій |
| | | 35.040.50 | Методи автоматичного ідентифікування та збирання даних |
| 03 | Криптографічний захист інформації (КЗІ) | 35.030 | Безпека інформаційних технологій |
| 03.01 | Загальні положення та профілі щодо КЗІ | 35.030 | Безпека інформаційних технологій |

| Коди та назви угруповань | | | |
|---|---|---|---|
| КСД | | УКНД | |
| | | 35.040.01 | Кодування інформації взагалі |
| 03.02 | Криптографічні алгоритми та протоколи | 35.030 | Безпека інформаційних технологій |
| 03.03 | Управління ключовими даними | 35.030 | Безпека інформаційних технологій |
| 03.04 | Засоби КЗІ | 35.030 | Безпека інформаційних технологій |
| 03.05 | Порядок оцінювання та випробування засобів КЗІ | 35.030 | Безпека інформаційних технологій |
| 03.99 | Інші стандарти щодо КЗІ | 35.030 | Безпека інформаційних технологій |
| | | 35.040.50 | Методи автоматичного ідентифікування та збирання даних |
| 04 | Кіберзахист | 35.030 | Безпека інформаційних технологій |
| 04.01 | Загальні положення та національна система кіберзахисту | 35.030 | Безпека інформаційних технологій |
| 04.02 | Впровадження заходів з кіберзахисту | 35.030 | Безпека інформаційних технологій |
| 04.03 | Кіберзахист інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та комунікаційних мереж | 35.030 | Безпека інформаційних технологій |
| 04.04 | Кіберзахист інформаційних ресурсів та програмного забезпечення | 35.030 | Безпека інформаційних технологій |
| 04.05 | Реагування на кіберінциденти, кібератаки, кіберзагрози | 35.030 | Безпека інформаційних технологій |
| | | 35.040.50 | Методи автоматичного ідентифікування та збирання даних |
| 04.06 | Організація, функціонування та керування підрозділами з кіберзахисту | 35.030 | Безпека інформаційних технологій |
| 04.07 | Управління ризиками у сфері кібербезпеки | 35.030 | Безпека інформаційних технологій |
| | | 03.100.01 | Організування підприємств. Керування взагалі |
| 04.08 | Безпека ланцюгів постачання | 35.030 | Безпека інформаційних технологій |
| | | 03.100.01 | Організування підприємств. Керування взагалі |
| | | 03.100.70 | Системи керування |
| | | 03.120.20 | Сертифікація продукції та підприємств. Оцінювання відповідності |
| 04.09 | Система управління штучним інтелектом | 35.020 | Інформаційні технології (ІТ) взагалі |

| Коди та назви угруповань | | | |
|---|---|---|---|
| КСД | | УКНД | |
| | | 03.100.70 | Системи керування |
| | | 03.120.20 | Сертифікація продукції та підприємств. Оцінювання відповідності |
| 04.10 | Кіберзахист систем управління технологічними процесами | 35.030 | Безпека інформаційних технологій |
| | | 25.040.40 | Вимірювання та керування технологічними процесами |
| | | 35.040.50 | Методи автоматичного ідентифікування та збирання даних |
| 04.99 | Інші стандарти щодо кіберзахисту | 35.030 | Безпека інформаційних технологій |
| 05 | Протидія технічним розвідкам (ПДТР) | 35.030 | Безпека інформаційних технологій |
| 05.01 | Загальні положення та профілі щодо ПДТР | 35.030 | Безпека інформаційних технологій |
| 05.02 | Протидія радіоелектронній розвідці | 35.030 | Безпека інформаційних технологій |
| 05.03 | Протидія оптико-електронній та оптичній розвідкам | 35.030 | Безпека інформаційних технологій |
| 05.04 | Протидія акустичній, гідроакустичній та сейсмічній розвідкам | 35.030 | Безпека інформаційних технологій |
| 05.05 | Протидія хімічній, радіаційній та біологічній розвідкам | 35.030 | Безпека інформаційних технологій |
| 05.06 | Методи та засоби виявлення засобів технічних розвідок | 35.030 | Безпека інформаційних технологій |
| 05.99 | Інші стандарти щодо ПДТР | 35.030 | Безпека інформаційних технологій |
| 06 | Оцінювання відповідності, сертифікація, атестація, аудит, експертні та тематичні дослідження, випробування засобів, систем, комплексів, персоналу, організацій | 03.100.01 | Організування підприємств. Керування взагалі |
| | | 03.100.30 | Керування трудовими ресурсами |
| | | 03.100.70 | Системи керування |
| | | 03.120.20 | Сертифікація продукції та підприємств. Оцінювання відповідності |

Додаток Б

(довідковий)

# АБЕТКОВИЙ ПОКАЖЧИК

## А



## Б



## В

**06** **Відповідності ●** Оцінювання #, сертифікація, атестація, аудит, експертні та тематичні дослідження, випробування засобів, систем, комплексів, персоналу, організацій

**04.02** **Впровадження ●** # заходів з кіберзахисту

**Г**

**05.04** **Гідроакустичній ●** Протидія акустичній, # та сейсмічній розвідкам

**01.01** **Груп ●** Процедури створення та діяльності робочих # із стандартизації

**Д**

**03.03** **Даними ●** Управління ключовими #

**01.01** **Діяльності ●** Процедури створення та # робочих груп із стандартизації

**06** **Дослідження ●** Оцінювання відповідності, сертифікація, атестація, аудит, експертні та тематичні #, випробування засобів, систем, комплексів, персоналу, організацій

**Е**

**06** **Експертні ●** Оцінювання відповідності, сертифікація, атестація, аудит, # та тематичні дослідження, випробування засобів, систем, комплексів, персоналу, організацій

**02.02** **Електромагнітних ●** Захист інформації від витоку каналами побічних # випромінювань і наведень та акустоелектричними каналами

**04.03** **Електронних ●** Кіберзахист інформаційних, # комунікаційних, інформаційно-комунікаційних систем та комунікаційних мереж

**З**

**04.04** **Забезпечення ●** Кіберзахист інформаційних ресурсів та програмного #

**02.06** **Закладних ●** Методи та засоби виявлення # пристроїв

**03.04** **Засоби ●** # КЗІ

**02.06** **Засоби ●** Методи та # виявлення закладних пристроїв

**05.06** **Засоби ●** Методи та # виявлення засобів технічної розвідки

**02.05** **Засобів ●** Класифікація, вимоги та рекомендації щодо # ТЗІ

**06** **Засобів ●** Оцінювання відповідності, сертифікація, атестація, аудит, експертні та тематичні дослідження, випробування #, систем, комплексів, персоналу, організацій

**03.05** **Засобів ●** Порядок оцінювання та випробування # КЗІ

**02.03** **Захист ●** # інформації від витоку акустичними, віброакустичними, лазерними акустичними та акустооптичними каналами

**02.04** **Захист ●** # інформації від витоку каналами високочастотного нав’язування

**02.02** **Захист ●** # інформації від витоку каналами побічних електромагнітних випромінювань і наведень та акустоелектричними каналами

**03** **Захист ●** Криптографічний **#** інформації (КЗІ)

**02** **Захист ●** Технічний # інформації (ТЗІ)

**01** **Захисту ●** Загальні положення із стандартизації у сфері # інформації

**04.02** **Заходів ●** Впровадження # з кіберзахисту

## І

**04.09** **Інтелектом ●** Система управління штучним #
**01** **Інформації ●** Загальні положення із стандартизації у сфері захисту #
**02.03** **Інформації ●** Захист # від витоку акустичними, віброакустичними, лазерними акустичними та акустооптичними каналами
**02.04** **Інформації ●** Захист # від витоку каналами високочастотного нав'язування
**02.02** **Інформації ●** Захист # від витоку каналами побічних електромагнітних випромінювань і наведень та акустоелектричними каналами
**03** **Інформації ●** Криптографічний захист # (КЗІ)
**02** **Інформації ●** Технічний захист # (ТЗІ)
**04.03** **Інформаційних ●** Кіберзахист #, електронних комунікаційних, інформаційно-комунікаційних систем та комунікаційних мереж
**04.04** **Інформаційних ●** Кіберзахист # ресурсів та програмного забезпечення
**04.03** **Інформаційно-комунікаційних ●** Кіберзахист інформаційних, електронних комунікаційних, # систем та комунікаційних мереж

## К

**02.03** **Каналами ●** Захист інформації від витоку акустичними, віброакустичними, лазерними акустичними та акустооптичними #
**02.04** **Каналами ●** Захист інформації від витоку # високочастотного нав'язування
**02.02** **Каналами ●** Захист інформації від витоку # побічних електромагнітних випромінювань і наведень та акустоелектричними #
**04.06** **Керування ●** Організація, функціонування та # підрозділами з кіберзахисту
**03.01** **КЗІ ●** Загальні положення та профілі щодо #
**03.04** **КЗІ ●** Засоби #
**03.99** **КЗІ ●** Інші стандарти щодо #
**03** **КЗІ ●** Криптографічний захист інформації (**#**)
**03.05** **КЗІ ●** Порядок оцінювання та випробування засобів #
**04.05** **Кібератаки ●** Реагування на кіберінциденти, #, кіберзагрози
**04.07** **Кібербезпеки ●** Управління ризиками у сфері #
**04.05** **Кіберзагрози ●** Реагування на кіберінциденти, кібератаки, #
**04** **Кіберзахист ● #**
**04.03** **Кіберзахист ●** # інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та комунікаційних мереж
**04.04** **Кіберзахист ●** # інформаційних ресурсів та програмного забезпечення
**04.10** **Кіберзахист ●** # систем управління технологічними процесами
**04.02** **Кіберзахисту ●** Впровадження заходів з #
**04.01** **Кіберзахисту ●** Загальні положення та національна система #
**04.99** **Кіберзахисту ●** Інші стандарти щодо #
**04.06** **Кіберзахисту ●** Організація, функціонування та керування підрозділами з #
**04.05** **Кіберінциденти ●** Реагування на #, кібератаки, кіберзагрози
**02.05** **Класифікація ●** #, вимоги та рекомендації щодо засобів ТЗІ
**03.03** **Ключовими ●** Управління # даними
**06** **Комплексів ●** Оцінювання відповідності, сертифікація, атестація, аудит, експертні та тематичні дослідження, випробування засобів, систем, #, персоналу, організацій
**04.03** **Комунікаційних ●** Кіберзахист інформаційних, електронних #, інформаційно-комунікаційних систем та # мереж
**03.02** **Криптографічні ●** # алгоритми та протоколи
**03** **Криптографічний ● #** захист інформації (КЗІ)

**Л**

**02.03** **Лазерними ●** Захист інформації від витоку акустичними, віброакустичними, # акустичними та акустооптичними каналами
**04.08** **Ланцюгів ●** Безпека # постачання

**М**

**02.06** **Методи ●** # та засоби виявлення закладних пристроїв
**05.06** **Методи ●** # та засоби виявлення засобів технічної розвідки
**04.03** **Мереж ●** Кіберзахист інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та комунікаційних #

**Н**

**02.02** **Наведень ●** Захист інформації від витоку каналами побічних електромагнітних випромінювань і # та акустоелектричними каналами
**02.04** **Нав'язування ●** Захист інформації від витоку каналами високочастотного #
**04.01** **Національна ●** Загальні положення та # система кіберзахисту

**О**

**05.03** **Оптичній ●** Протидія оптико-електронній та # розвідкам
**05.03** **Оптико-електронній ●** Протидія # та оптичній розвідкам
**02.01** **Організації ●** Загальні положення та порядок # робіт з ТЗІ
**06** **Організацій ●** Оцінювання відповідності, сертифікація, атестація, аудит, експертні та тематичні дослідження, випробування засобів, систем, комплексів, персоналу, #
**04.06** **Організація ● #**, функціонування та керування підрозділами з кіберзахисту
**06** **Оцінювання ●** # відповідності, сертифікація, атестація, аудит, експертні та тематичні дослідження, випробування засобів, систем, комплексів, персоналу, організацій
**03.05** **Оцінювання ●** Порядок # та випробування засобів КЗІ

**П**

**05.99** **ПДТР ●** Інші стандарти щодо #
**05** **ПДТР ●** Протидія технічним розвідкам (#)
**06** **Персоналу ●** Оцінювання відповідності, сертифікація, атестація, аудит, експертні та тематичні дослідження, випробування засобів, систем, комплексів, #, організацій
**04.06** **Підрозділами ●** Організація, функціонування та керування # з кіберзахисту
**02.02** **Побічних ●** Захист інформації від витоку каналами # електромагнітних випромінювань і наведень та акустоелектричними каналами
**01** **Положення ●** Загальні # із стандартизації у сфері захисту інформації
**04.01** **Положення ●** Загальні # та національна система кіберзахисту
**02.01** **Положення ●** Загальні # та порядок організації робіт з ТЗІ
**03.01** **Положення ●** Загальні # та профілі щодо КЗІ
**01.99** **Положень ●** Інші стандарти щодо загальних # із стандартизації
**02.01** **Порядок ●** Загальні положення та # організації робіт з ТЗІ
**03.05** **Порядок ●** # оцінювання та випробування засобів КЗІ

**Р**



**С**

**05.99** **Стандарти ●** Інші # щодо ПДТР
**01.04** **Стандарти ●** Термінологічні #
**01** **Стандартизації ●** Загальні положення із # у сфері захисту інформації
**01.99** **Стандартизації ●** Інші стандарти щодо загальних положень із #
**01.02** **Стандартизації ●** Порядок проведення робіт із **#**
**01.01** **Стандартизації ●** Процедури створення та діяльності робочих груп із #
**01.01** **Створення ●** Процедури # та діяльності робочих груп із стандартизації
**04.07** **Сфері ●** Управління ризиками у # кібербезпеки

**Т**

**06** **Тематичні ●** Оцінювання відповідності, сертифікація, атестація, аудит, експертні та # дослідження, випробування засобів, систем, комплексів, персоналу, організацій
**01.04** **Термінологічні ●** # стандарти
**02** **Технічний ●** # захист інформації (ТЗІ)
**05** **Технічним ●** Протидія # розвідкам (ПДТР)
**05.06** **Технічної ●** Методи та засоби виявлення засобів # розвідки
**04.10** **Технологічними ●** Кіберзахист систем управління # процесами
**02.01** **ТЗІ ●** Загальні положення та порядок організації робіт з #
**02.99** **ТЗІ ●** Інші стандарти щодо #
**02.05** **ТЗІ ●** Класифікація, вимоги та рекомендації щодо засобів #
**02** **ТЗІ ●** Технічний захист інформації (#)

**У**

**04.10** **Управління ●** Кіберзахист систем # технологічними процесами
**03.03** **Управління ●** # ключовими даними
**04.07** **Управління ●** # ризиками у сфері кібербезпеки
**04.09** **Управління ●** Система # штучним інтелектом

**Ф**

**04.06** **Функціонування ●** Організація, # та керування підрозділами з кіберзахисту

**Х**

**05.05** **Хімічній ●** Протидія #, радіаційній та біологічній розвідкам

**Ш**

**04.09** **Штучним ●** Система управління # інтелектом