



**ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ**

**Стандартизація криптографічного та технічного захисту інформації,
кіберзахисту, протидії технічним розвідкам**

СТД-04-001-2026-В

**МОДЕЛЬ ЗРІЛОСТІ
ОРГАНІЗАЦІЙНО-ТЕХНІЧНОЇ СПРОМОЖНОСТІ
КОМАНДИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ,
КІБЕРАТАКИ, КІБЕРЗАГРОЗИ (CSIRT)**

Київ

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

2026

СТД-04-001-2026-В

ПЕРЕДМОВА

1 РОЗРОБЛЕНО: призначеним органом стандартизації у сфері криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам Державної служби спеціального зв'язку та захисту інформації України – Державним науково-дослідним інститутом технологій кібербезпеки та захисту інформації.

РОЗРОБНИКИ: **М. Комаров** канд. техн. наук, керівник розробки; **В. Павліков**, заслужений діяч науки і техніки України, д-р техн. наук, проф.; **О. Верховець**; **К. Гуляєв**, канд. техн. наук, ст. наук. співроб.; **В. Гольнєв**; **О. Рушак**; **І. Писанко**; **Д. Жарук**; **Т. Грищишина**.

2 ПОГОДЖЕНО: Адміністрацією Державної служби спеціального зв'язку та захисту інформації України (лист від 09.07.2026 № 05/03-18458/2026/ВН).

3 ПРИЙНЯТО ТА НАДАНО ЧИННОСТІ: наказом Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації від «21» вересня 2026 р. № 117, з «30» вересня 2026 р.

4 Цей стандарт застосовується на добровільній основі, крім випадків, якщо обов'язковість його застосування встановлена нормативно-правовими актами.

5 Право власності на стандарти криптографічного та технічного захисту інформації, кібербезпеки, протидії технічним розвідкам належить державі в особі Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації, який розповсюджує такі стандарти.

6 УВЕДЕНО ВПЕРШЕ

СТД-04-001-2026-В
ЗМІСТ

1 СФЕРА ЗАСТОСУВАННЯ.....	4
2 НОРМАТИВНІ ПОСИЛАННЯ.....	4
3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ.....	5
4 ПОЗНАКИ ТА СКОРОЧЕННЯ	6
5 ЗАГАЛЬНІ ПОЛОЖЕННЯ	7
5.1 Мета і принципи моделі зрілості	7
5.2 Суб'єкти та об'єкти застосування	7
6 МОДЕЛЬ ЗРІЛОСТІ ОРГАНІЗАЦІЙНО-ТЕХНІЧНОЇ СПРОМОЖНОСТІ CSIRT	8
7 ВИМОГИ ДО ПАРАМЕТРІВ	10
7.1 Категорія О: Організація	10
7.2 Категорія Н: Персонал.....	19
7.3 Категорія Т: Інструменти	25
7.4 Категорія Р: Процеси	34
8 ПОРЯДОК ПРОВЕДЕННЯ ОЦІНЮВАННЯ ЗРІЛОСТІ CSIRT	47
8.1 Самооцінювання.....	48
8.2 Незалежний аудит	48
8.3 Збір документальних підтверджень	50
9 ВИМОГИ ДО ЗВІТУ ПРО ОЦІНЮВАННЯ	51
Додаток А (обов'язковий). Анкета оцінювання параметрів.....	53
Бібліографія	57

1 СФЕРА ЗАСТОСУВАННЯ

1.1 Цей стандарт встановлює вимоги та критерії оцінювання зрілості команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) у частині їх організаційної спроможності, технічного оснащення, процесів реагування, взаємодії та управління знаннями.

1.2 Цей стандарт застосовують:

- а) державні CSIRT (урядові, відомчі, галузеві, регіональні);
- б) приватні CSIRT (підприємств, установ та організацій незалежно від форми власності);
- в) інші CSIRT.

1.3 Цей стандарт не поширюється на вимоги до технічної реалізації засобів захисту інформації та криптографічних модулів, що є предметом окремих стандартів.

2 НОРМАТИВНІ ПОСИЛАННЯ

У цьому стандарті наведено посилання на такі нормативні документи:

ДСТУ ISO/IEC 27001:2023 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»;

ДСТУ ISO/IEC 27035-1:2024 «Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи та процес»;

ДСТУ ISO/IEC 27035-2:2024 «Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти»;

СТД-01-001-2026-B Вимоги до побудови, викладення, оформлення, позначення та змісту стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам.

Примітка. У разі заміни нормативного документу, на який наведено посилання, слід застосовувати новий нормативний документ. У разі скасування нормативного документу, на

СТД-04-001-2026-В

який наведено посилання, слід застосовувати останню чинну на момент застосування редакцію нормативного документу. Якщо до нормативного документа, на який наведено посилання, внесено зміни (поправки), застосовують цей нормативний документ з урахуванням усіх внесених до нього змін (поправок).

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті вжито терміни відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» [2], постанови Кабінету Міністрів України від 26.11.2025 № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» [5] та ДСТУ ISO/IEC 27001:2023. Нижче подано терміни, додатково вжиті в цьому стандарті, та визначення позначених ними понять.

3.1 команда реагування на кіберінциденти, кібератаки, кіберзагрози (*Computer Security Incident Response Team; CSIRT*)

Організаційний підрозділ або окрема організація, що надає послуги з оброблення та підтримки реагування на кіберінциденти, кібератаки, кіберзагрози, а також здійснює координацію відповідних заходів

Примітка. У цьому стандарті терміни CSIRT, CERT та IRT є синонімами.

3.2 модель зрілості організаційно-технічної спроможності CSIRT

Структурована сукупність категорій, параметрів, вимог та критеріїв, що дає змогу систематично оцінювати та розвивати організаційно-технічну спроможність команди реагування

3.3 клієнти

Суб'єкти, яким надаються сервіси (послуги) з кібербезпеки

3.4 параметр

Характеристика, що стосується організації та функціонування команди реагування

СТД-04-001-2026-B

3.5 сервіси команди реагування (*CSIRT services*)

Функції, що виконує команда реагування для своїх користувачів: реактивні (реагування на інциденти), проактивні (сповіщення, моніторинг), послуги з управління безпекою

3.6 документальне підтвердження

Документ, технічний артефакт або інший доказ, що підтверджує виконання вимоги параметра

4 ПОЗНАКИ ТА СКОРОЧЕННЯ

У цьому стандарті вжито такі позначки та скорочення:

ДСТУ – Державний стандарт України;

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

BCM – управління безперервністю бізнесу (*Business Continuity Management*);

CERT – Команда реагування на надзвичайні комп'ютерні події (*Computer Emergency Response Team*);

CERT-UA – національна команда реагування на кіберінциденти, кібератаки, кіберзагрози України;

CSIRT – Команда реагування на кіберінциденти, кібератаки, кіберзагрози (*Computer Security Incident Response Team*);

ENISA – Агентство ЄС з кібербезпеки (*European Union Agency for Network and Information Security*);

IRT – Команда реагування на інциденти (*Incident Response Team*);

ISAC – Центр з обміну та аналізу інформації (*Information Sharing and Analysis Centre*);

GDPR – Загальний регламент про захист даних (*General Data Protection Regulation*);

СТД-04-001-2026-В

SIM3 – Модель зрілості управління інцидентами безпеки (*Security Incident Management Maturity Model*);

SOAR – автоматизація та оркестрація реагування (*Security Orchestration, Automation and Response*);

SOC – Операційний центр безпеки (*Security Operations Center*);

TF-CSIRT – Спільнота команд реагування (*Task Force for Computer Security Incident Response Teams*).

5 ЗАГАЛЬНІ ПОЛОЖЕННЯ

5.1 Мета і принципи моделі зрілості

Модель зрілості організаційно-технічної спроможності CSIRT призначена для:

- а) систематичного оцінювання поточного рівня організаційно-технічних спроможностей команди реагування;
- б) визначення пріоритетів розвитку та вдосконалення;
- в) порівняння спроможностей різних команд реагування на основі єдиних критеріїв;
- г) забезпечення методологічної основи для планування розвитку спроможностей та моніторингу їх ефективності.

Модель зрілості ґрунтується на таких принципах:

- а) принцип науковості – модель ґрунтується на міжнародних стандартах (ДСТУ ISO/IEC 27035-1, ДСТУ ISO/IEC 27035-2, ENISA CSIRT Maturity Framework [8], SIM3 [9]) та вітчизняних дослідженнях;
- б) принцип відкритості та прозорості – вимоги моделі є явними та перевірними;
- в) принцип гармонізації – модель враховує положення міжнародних стандартів та рекомендацій;

СТД-04-001-2026-B

г) принцип практичної придатності – модель враховує особливості функціонування CSIRT у реальних умовах.

5.2 Суб'єкти та об'єкти застосування

Суб'єктами застосування цього стандарту є:

- а) команди реагування, що проводять самооцінювання;
- б) команди реагування, що проводять інші види оцінювання в рамках спільнот команд реагування або інших вимог законодавства;
- в) аудитори;
- г) органи управління та керівники, що здійснюють нагляд за діяльністю команд реагування.

Об'єктом оцінювання є організаційно-технічна спроможність CSIRT, що охоплює організаційну структуру, персонал, технічні інструменти та процеси.

6 МОДЕЛЬ ЗРІЛОСТІ ОРГАНІЗАЦІЙНО-ТЕХНІЧНОЇ СПРОМОЖНОСТІ CSIRT

Модель зрілості побудована на трьох базових елементах:

- а) параметри – кількісні показники, визначені для вимірювання зрілості (45 параметрів), що детально описані в розділі 7;
- б) категорії параметрів – чотири основні категорії, детально описані в таблиці 2;
- в) рівні зрілості параметрів – єдиний набір рівнів від 0 до 4, що застосовується до всіх параметрів у всіх категоріях параметрів (таблиця 1).

Оцінювання полягає у визначенні рівня (від 0 до 4) для кожного параметра. Простота системи досягається застосуванням єдиного набору рівнів до всіх параметрів у всіх категоріях. Зміст рівнів зрілості наведено в таблиці 1.

СТД-04-001-2026-B

Таблиця 1 – Рівні зрілості параметрів

Значення	Позначення	Зміст
0	Відсутній / невизначений / неусвідомлений	Команда ніколи не обговорювала цього та формально не знає певних аспектів. Процеси або аспекти діяльності не визначені, практика реалізації параметра відсутня, системне розуміння завдань та критеріїв параметра відсутнє. Зустрічається переважно в командах, які лише починають.
1	Неявний	Команда має досить чітке розуміння процесів параметра, проте вимоги, процедури чи правила не зафіксовані в письмовій (документальній) формі («існує лише в голові»). Характерний для команд, що лише починають, але також зустрічається в досвідчених командах, де кілька фахівців знають, як діяти, але так і не спромоглися це задокументувати.
2	Явний, внутрішній	Команда знає і дотримується вимог. Процеси задокументовані та виконуються, проте документація не має офіційного статусу та не затверджена керівництвом команди.
3	Явний, формалізований за рішенням керівника CSIRT або вищого рівня управління	Команда знає і дотримується вимог. Процеси регламентовані та виконуються. Документація офіційно затверджена керівником команди (або уповноваженою посадовою особою вищого рівня управління) та є обов'язковою для виконання.
4	Явний, постійно оцінюється за рішенням органів управління, вищих за керівника CSIRT	Команда знає і дотримується вимог. Процеси регламентовані, виконуються та підлягають регулярному зовнішньому або внутрішньому аудиту (не рідше одного разу на два роки, зазвичай щорічно) за рішенням органу управління вищого рівня. Забезпечено обов'язковий зворотний зв'язок за результатами перевірок. Рівень присвоюється також у разі, якщо параметри діяльності прямо закріплені вимогами національного законодавства в сфері кібербезпеки.

Параметри розподілені між чотирма категоріями таким чином, щоб параметри всередині кожної категорії були якомога більш незалежними один від одного. Категорії параметрів визначені в таблиці 2.

Таблиця 2 – Категорії параметрів

Код	Категорія	Зміст
О	Організація (Organisation)	11 параметрів. Сукупність людей, ресурсів, інструментів та інфраструктури, що скоординовано працюють разом. Параметри охоплюють повноваження, сферу відповідальності та сервіси CSIRT, а також організаційно-правові засади функціонування, що поєднує всі організаційні аспекти.
Н	Персонал (Human)	7 параметрів. Особи, які спільно працюють для надання сервісів та виконання повноважень. Параметри стосуються найважливішого ресурсу будь-якого CSIRT – людського капіталу.
Т	Інструменти (Tools)	10 параметрів. Сукупність програм, застосунків, сервісів та технічних засобів, що уможливають або покращують управління інцидентами безпеки, роблячи його швидшим, якіснішим та більш детальним.
Р	Процеси (Processes)	17 параметрів. Логічно впорядковані сукупності дій, що виконуються персоналом або автоматизованими інструментами з метою досягнення конкретного результату. У зрілих організаціях процеси є задокументованими, вимірюваними та відтворюваними.

7 ВИМОГИ ДО ПАРАМЕТРІВ

Вимоги до кожного параметра подано у вигляді опису, контрольного запитання та характеристики значень за шкалою відповідно до розділу 6. Для деяких параметрів допускається значення «Не застосовується» (N/A); у такому разі параметр виключається з оцінювання.

7.1 Категорія О: Організація

Під організацією мається на увазі сукупність людей, ресурсів, інструментів та інфраструктури, що скоординовано працюють разом. Параметри охоплюють повноваження, сферу відповідальності та сервіси CSIRT, а також організаційно-правові засади функціонування, що поєднує всі організаційні аспекти.

7.1.1 О-1 Призначення

Опис: Призначення команди реагування визначає обґрунтування необхідності її функціонування і доручені їй завдання, що затверджується органом управління вищого рівня. Найбільш ефективною є практика, коли призначення команди затверджуються

СТД-04-001-2026-B

керівництвом найвищого рівня в організації, галузі або системі функціонування (наприклад, директором чи керівником органу державної влади, де її статус додатково закріплюється законодавчо). У деяких випадках, на початкових етапах, призначення може визначатися на рівні керівництва підрозділів.

Чи визначено призначення вашого CSIRT?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього і формально не знаємо нашого призначення чи доручених завдань. Ми просто виконуємо свою роботу.

«1» – У нас є чітке розуміння того, що наша робота відповідає дорученим нам завданням, але це ніколи не було зафіксовано письмово.

«2» – У нас немає формалізованого письмового призначення, тому ми сформулювали його самостійно для власних потреб. Керівництво нашої команди офіційно його не затверджувало.

«3» – У нас є письмове призначення, затверджене керівництвом нашої команди.

«4» – У нас є письмові призначення від органу управління вищого рівня, яке керівництво нашої команди вважає обов'язковими до виконання. Під час періодичного аудиту/перевірки нашої команди за рішенням органу управління вищого рівня (не нами самими) явним чином оцінюється, чи ми виконуємо наше призначення і якою мірою. (Або: наше призначення чітко визначене законодавством у сфері кібербезпеки).

7.1.2 О-2 Сфера відповідальності

Опис: *Сфера відповідальності команди реагування визначає чітко окреслену цільову групу користувачів (клієнтську базу), для якої надаються сервіси (послуги). Залежно від підпорядкування та призначення команди, її сфера відповідальності може бути: внутрішньою – сервіси надаються виключно для забезпечення потреб власної організації чи компанії; зовнішньою – сфера відповідальності команди поширюється на окрему галузь, сектор економіки, конкретний регіон, або охоплює загальнодержавний рівень.*

Чи має ваш CSIRT визначену сферу відповідальності?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – Ми знаємо свою сферу відповідальності, але вона ніколи не була зафіксована письмово.

«2» – У нас немає формалізованого письмового визначення сфери відповідальності, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є письмове визначення сфери відповідальності, затверджене керівництвом нашої команди.

«4» – У нас є письмове визначення сфери відповідальності, затверджене керівництвом нашої команди або органу управління вищого рівня. Під час періодичної перевірки нашої

СТД-04-001-2026-B

команди оцінюється, чи ми обслуговуємо цю сферу відповідальності і якою мірою, а також чи потребує сфера відповідальності змін.

7.1.3 О-3 Повноваження

Опис: Дії, які CSIRT має право виконувати щодо клієнтів сфери відповідальності (параметр О-2), щоб успішно реалізовувати своє призначення (параметр О-1). Команда реагування повинна мати чіткий, однозначний та офіційно затверджений опис своїх повноважень, який слугує правовою опорою для прийняття рішень, особливо під час кризових ситуацій або реагування на масштабні кіберінциденти. Залежно від рівня та призначення команди, її повноваження можуть мати різний характер. Повноваження національної, галузевих або регіональних команд реагування визначається вимогами чинного законодавства, зокрема нормативно-правовими актами компетентних органів. Якщо загальне законодавство не містить вичерпної конкретики, компетенція та межі повноважень команди мають бути детально регламентовані у її внутрішніх положеннях, які розробляються на основі закону та затверджуються органом управління вищого рівня. Без такої підтримки команда не матиме достатнього правового підґрунтя для застосування своїх повноважень у критичних ситуаціях.

Які повноваження має ваша команда?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – Ми знаємо свої повноваження, але вони ніколи не були зафіксовані письмово.

«2» – У нас немає формалізованого письмового визначення повноважень, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є письмове визначення повноважень, затверджене керівництвом нашої команди.

«4» – У нас є письмове визначення повноважень, затверджене керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи відповідаємо ми цим повноваженням і якою мірою, а також чи є вони достатніми для виконання нашого призначення.

7.1.4 О-4 Обов'язки

Опис: Обов'язки команди реагування визначають сукупність високорівневих функцій та завдань, покладених на неї для досягнення визначених цілей та успішної реалізації її призначення (параметр О-1). Вони формують загальну концепцію діяльності команди, яка надалі деталізується через конкретний перелік сервісів (параметр О-5), що надаються клієнтам сфери відповідальності (параметр О-2). Під час формування нормативної бази

СТД-04-001-2026-B

діяльності команди необхідно забезпечити баланс між її обов'язками та реальними повноваженнями. Слід уникати ситуації, коли повноваження команди дуже обмежені, а обов'язки дуже широкі. Якщо розрив між параметрами О-3 і О-4 стає занадто великим, тоді від команди фактично очікують виконання багатьох завдань без реальної можливості забезпечити їх виконання. Це запорука неефективної роботи. Між параметрами О-3 і О-4 існує незначний розрив і він не повинен ставати занадто великим.

Які обов'язки має ваша команда?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – Ми знаємо свої обов'язки, але вони ніколи не були зафіксовані письмово.

«2» – У нас немає формалізованого письмового визначення обов'язків, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є письмове визначення обов'язків, затверджене керівництвом нашої команди.

«4» – У нас є письмове визначення обов'язків, затверджене керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи виконуємо ми ці обов'язки і якою мірою.

7.1.5 О-5 Опис сервісів

Опис: Команда реагування визначає вичерпний перелік сервісів, які вона надає клієнтам сфери відповідальності (параметр О-2), та опис порядку їх отримання. Формування переліку послуг здійснюється на основі затвердженого призначення (параметр О-1) та наявних ресурсів (кадрових, технічних, фінансових). Рекомендованою методичною основою для структурування та визначення видів сервісів є стандарт *FIRST CSIRT Services Framework*. Пріоритет надається сервісам, які є обов'язковими для виконання ключових завдань команди, тоді як додаткові сервіси впроваджуються за умови наявності відповідного ресурсного забезпечення. Затверджений перелік сервісів, а також організаційна інформація публікуються на власному офіційному вебсайті команди реагування або на вебресурсі органу управління, якому вона підпорядкована. Документ із описом діяльності команди є публічно доступним. Для забезпечення міжнародної взаємодії документ із описом діяльності команди викладається англійською мовою.

Мінімальна вимога: Опис містить контактну інформацію CSIRT, графік роботи, стислий опис сервісів, що надаються, а також політику CSIRT щодо обробки та розкриття інформації. Він публічно доступний українською та, за необхідності, англійською мовою.

Пояснення: Чудовою відправною точкою є документ *CSIRT Services Framework* від

СТД-04-001-2026-B

FIRST [11]. Рекомендується використовувати RFC 2350 [10] як уніфікований спосіб публікації опису сервісів.

Чи має ваша команда опис сервісів?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього. Ми просто виконуємо свою роботу.

«1» – Ми знаємо, які сервіси пропонуємо, але вони ніколи не були зафіксовані письмово.

«2» – У нас немає формалізованого письмового опису сервісів, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є письмовий опис сервісів, затверджений керівництвом нашої команди. Він доступний нашим клієнтам.

«4» – У нас є письмовий опис сервісів, затверджений керівництвом нашої команди. Він доступний нашим клієнтам. Під час періодичної перевірки нашої команди оцінюється, чи надаємо ми ці сервіси і якою мірою.

7.1.6 О-6 Політика взаємодії із медіа

Опис: *Описує політику CSIRT щодо взаємодії з медіа. Вашій команді необхідно вміти взаємодіяти з пресою та іншими медіа. Іноді така взаємодія відбувається разом із відділом комунікацій або пресслужбою, а інколи безпосередньо. Це також залежить від типу медіа: взаємодія з пресою відрізняється, наприклад, від взаємодії через соціальні мережі. Політика взаємодії з медіа визначає різні типи медіа, які використовуються, а також способи взаємодії з кожним із них. Крім того, така політика може описувати порядок взаємодії за конкретних обставин, наприклад під час великого кіберінциденту або кризової ситуації, проведення кампаній з підвищення обізнаності або коли медіа самі звертаються до вас, а не навпаки.*

Чи має ваша команда політику взаємодії з медіа?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього. Ми просто вирішуємо такі речі в індивідуальному порядку.

«1» – У нас є розуміння, як взаємодіяти з медіа, але воно не зафіксоване письмово.

«2» – У нас немає формалізованої письмової політики взаємодії з медіа, тому ми сформулювали її самостійно для власних потреб. Наше керівництво офіційно її не затверджувало.

«3» – У нас є письмова політика взаємодії з медіа, затверджена керівництвом нашої команди.

«4» – У нас є письмова політика взаємодії з медіа, затверджена керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи ми взаємодіали з медіа і яким чином.

7.1.7 O-7 Рівні надання сервісів

Опис: *Описує рівень надання сервісів, якого слід очікувати від CSIRT. Під час визначення сервісів (параметр O-5), які надає ваш CSIRT, корисно також встановити для них рівні надання сервісів. Чого можуть очікувати від вас ваші клієнти? Чого можуть очікувати від вас інші CSIRT? Найпростішим описом рівня надання сервісів є показник часу, протягом якого має бути надана перша відповідь на вхідне повідомлення про кіберінцидент. Рівні надання сервісів можуть бути більш деталізованими: у вигляді вимог типу SLA (Service Level Agreement), і тоді вони можуть залежати від типу, рівня критичності та пріоритету кіберінцидентів (наприклад, як визначено в параметрі O-8). Залежно від типу та рівня критичності кіберінциденту, може встановлюватися різний час реагування, а також, наприклад, відсоток кіберінцидентів, які мають бути опрацьовані протягом визначеного часу.*

Мінімальна вимога: Опис визначає швидкість реагування на вхідні повідомлення про кіберінциденти від клієнтів і від інших CSIRT. Для останніх мінімальною вимогою є надання відповіді протягом двох робочих днів.

Чи має ваш CSIRT опис рівнів надання сервісів?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є базове розуміння рівня надання сервісів, який від нас очікується, але це ніколи не було зафіксовано письмово.

«2» – У нас немає формалізованого письмового опису рівня надання сервісів, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є письмовий опис рівня надання сервісів, затверджений керівництвом нашої команди.

«4» – У нас є письмовий опис рівня надання сервісів, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи ми дотримуємося нашого рівня (рівнів) надання сервісів і якою мірою.

7.1.8 O-8 Класифікація кіберінцидентів

Опис: *Наявність схеми класифікації кіберінцидентів і її застосування до зареєстрованих кіберінцидентів. Зазвичай такі схеми містять принаймні типи або категорії кіберінцидентів, однак вони також можуть включати рівень критичності. Зазвичай схема класифікації кіберінцидентів містить як мінімум перелік технічних категорій, до яких можна віднести кіберінцидент або загрозу: наприклад, чи мають вони ознаки "спаму", "компрометації root-прав", "DDoS-атаки" тощо. Популярним прикладом такої системи є*

СТД-04-001-2026-B

Довідкова таксономія класифікації кіберінцидентів (*Reference Incident Classification Taxonomy*) Агентства ЄС з кібербезпеки (ENISA). Водночас рекомендується також включати до такої класифікації оцінку потенційного рівня критичності (впливу) кіберінциденту чи загрози і, за можливості, оцінку їхнього пріоритету (оскільки, наприклад, загроза з високим потенційним впливом може мати низький пріоритет, якщо ймовірність її реалізації найближчим часом дуже мала). Такі більш розвинені підходи до класифікації кіберінцидентів у поєднанні з рівнями надання сервісів (параметр O-7) допомагають структурувати роботу в умовах великої кількості кіберінцидентів. Існує багато способів реалізації такої класифікації, але спершу варто перевірити, чи у вашій організації вже не використовується певна схема оцінки рівня критичності/пріоритету в сфері IT, і за можливості прийняти її. Якщо ж потрібно створити власну, наполегливо рекомендується не ускладнювати її.

Чи має ваша команда схему класифікації кіберінцидентів?

Значення:

«0» – Ми не класифікуємо кіберінциденти, а просто працюємо з ними.

«1» – Ми усвідомлюємо, що існують різні типи кіберінцидентів, але явним чином у нас це не зафіксовано. Якщо кіберінцидент потребує особливої уваги, ми просто працюємо з ним відповідним чином.

«2» – У нас немає формалізованої письмової класифікації кіберінцидентів, тому ми сформулювали її самостійно для власних потреб. Наше керівництво офіційно її не затверджувало.

«3» – У нас є письмова класифікація кіберінцидентів, затверджена керівництвом нашої команди.

«4» – У нас є письмова класифікація кіберінцидентів, затверджена керівництвом нашої команди. Під час періодичної перевірки роботи нашої команди розглядаються різні типи кіберінцидентів і те, як ми з ними працюємо.

7.1.9 O-9 Взаємодія з іншими командами реагування

Опис: Описує рівень участі CSIRT у спільнотах CSIRT напряму або опосередковано через CSIRT вищого рівня. Це необхідно для участі та інтеграції в транснаціональні/глобальні системи CSIRT. Під спільнотами CSIRT маються на увазі сталі об'єднання CSIRT, наприклад у межах вашої країни, галузі, географічного регіону або на глобальному рівні. Ваш CSIRT може брати участь у таких об'єднаннях напряму (наприклад, як член) або опосередковано через CSIRT вищого рівня, який є учасником таких об'єднань. Для ефективної роботи CSIRT участь у таких об'єднаннях є необхідною, оскільки вся спільнота CSIRT значною мірою залежить від співпраці між командами. Важливо розуміти, що участь в об'єднаннях є критично важливою на різних рівнях. Наприклад, на національному рівні необхідно створити мережу CSIRT, яка включає національний CSIRT, команди, що захищають різні сектори

СТД-04-001-2026-В

критичної інфраструктури, а також сектори безпеки та оборони, охорони здоров'я та науки і освіти. Також доцільно об'єднуватися в межах географічних регіонів (наприклад, ініціативи на кшталт TF-CSIRT, APCERT, OAS, LACNIC, AfricaCERT, TBA, OiS-CERT, ASEAN тощо). На глобальному рівні можна брати участь у міжнародних форумах, таких як FIRST, або в ініціативах для CSIRT, започаткованих GFCE, ITU, Африканським Союзом та іншими. Фокус участі вашої команди залежить від її типу та завдань.

Чи взаємодіє ваша команда з іншими командами або бере участь у спільнотах команд напряму або опосередковано через CSIRT вищого рівня?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – Ми знаємо, в яких спільнотах CSIRT беремо участь, але це ніколи не було зафіксовано письмово.

«2» – У нас немає формалізованої письмової угоди участі в спільнотах CSIRT або політики взаємодії з іншими командами, тому ми сформулювали децю для власних потреб. Наше керівництво офіційно її не затверджувало.

«3» – У нас є формалізована письмова угода участі в спільнотах CSIRT або політика взаємодії з іншими командами, які затверджені керівництвом нашої команди і профінансовані з бюджету.

«4» – У нас є формалізована письмова угода участі в спільнотах CSIRT або політика взаємодії з іншими командами, які затверджені керівництвом нашої команди і профінансовані з бюджету. Під час періодичної перевірки нашої команди оцінюється, чи ми беремо участь в цих спільнотах або взаємодіємо з іншими командами, як активно і які переваги це надає.

7.1.10 O-10 Організаційно-правові засади діяльності

Опис: Об'єднує параметри від O-1 до O-9 у цілісний рамковий документ, який є для CSIRT керівним. Те, що ми називаємо статутом команди або організаційним регламентом для CSIRT, – це зведений керівний документ для команди, який описує, з кого складається команда, що вона робить, кому надає сервіси, які до неї висуваються очікування та яким чином це було формально визначено через повноваження. Такий статут має щонайменше охоплювати параметри від O-1 до O-9, а за потреби й деякі інші. В ідеалі цей документ затверджений на тому ж рівні управління, який надав повноваження вашому CSIRT. Основна цінність такого зведеного опису O-10 полягає в тому, що це фактично високорівневий "статут" команди, керівний документ, який визначає всі основоположні питання, що потребують погодження на вищому рівні управління, і надалі може використовуватись як нормативний орієнтир у роботі команди, для аудитів тощо. O-10 не обов'язково має бути єдиним документом, хоча зазвичай доцільно зібрати всі основоположні параметри з категорії O в один документ. Статут команди зазвичай є внутрішнім документом, тому

СТД-04-001-2026-B

RFC 2350, який призначений переважно для публічного опису сервісів команди, не підходить як статут, до того ж його предмет набагато вузьчий. Якщо О-10 складається з кількох документів, RFC 2350 може бути його частиною (але не єдиним документом у його складі). Наприклад, для національних CSIRT значна частина О-10 може бути закріплена в національному законодавстві про кібербезпеку. Водночас навіть у такому випадку корисно перелічити аспекти, що стосуються О-10, у статуті внутрішньої бази знань (вікі-системі) з належними посиланнями. Існує ще один варіант: деякі CSIRT розширюють статут до документа, що охоплює більшість або всі параметри – так званого "посібника CSIRT". Перевага такого підходу полягає в тому, що всі параметри описані в одному консолідованому документі. Недолік – необхідність погодження навіть внутрішніх питань, таких як інструменти та процеси, з органом, що може ускладнювати керування версіями.

Мінімальна вимога: Документ має описувати параметри від О-1 до О-9 через посилання на окремі документи або шляхом об'єднання всієї необхідної інформації в одному документі.

Чи визначено організаційно-правові засади діяльності вашого CSIRT?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – Ми маємо цілісне розуміння наших організаційно-правових засад діяльності, але це ніколи не було зафіксовано письмово.

«2» – У нас немає формалізованого письмового статуту, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є письмовий статут, затверджений керівництвом нашої команди.

«4» – У нас є письмовий статут, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей статут актуальний та чинний.

7.1.11 О-11 Політика безпеки

Опис: *Описує систему безпеки, в межах якої працює CSIRT. Вона може бути частиною більшої системи, або CSIRT може мати власну політику безпеки. CSIRT зазвичай функціонує в межах головної/материнської організації. Така організація, як правило, має власні політики інформаційної безпеки та управління безперервністю бізнесу (Business Continuity Management, або BCM), які також поширюються на вашу команду. Хоча інформаційну безпеку та безперервність бізнесу часто розглядають окремо, у контексті IT/кібербезпеки більш логічно дивитися на безперервність бізнесу як на невід'ємну частину політики безпеки. Тому, коли ми говоримо про "політику безпеки", вона включає такі важливі аспекти, як "доступність" та відновлення нормальної роботи після збоїв, хоча спектр питань, які потрібно врахувати, ще*

СТД-04-001-2026-B

шириший: наприклад безпека та стійкість об'єктів, де провадиться діяльність, а також безпека та стійкість робочого середовища.

Два важливих уточнення:

– деякі інші аспекти, пов'язані з BCM, розглядаються в інших параметрах, зокрема, в H-2 (операційна стійкість персоналу) та від T-5 до T-7 (стійкість базових інструментів CSIRT);

– як CSIRT, ви часто маєте потреби в сфері IT/безпеки/BCM, які відрізняються від стандартних. Наприклад, вам може знадобитися можливість проводити тести без блокування з боку брандмауера, отримувати електронну пошту без фільтрації спаму/шкідливого програмного забезпечення, розгортати ханіпоти, використовувати засоби шифрування (наприклад, GPG) або мати окремі інтернет-з'єднання для резервування чи тестування тощо. Такі специфічні потреби часто означають, що на додачу до політики безпеки головної/материнської організації CSIRT має також власну політику безпеки (знову ж таки, з урахуванням BCM). Звісно, якщо ви є автономним CSIRT без головної/материнської організації (тобто самі виступаєте як така організація), ці уточнення для вас також актуальні.

Чи дотримується ваш CSIRT визначеної політики або політик безпеки (включно з аспектами BCM) – власної та/або від головної/материнської організації?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – Ми знаємо, які обмеження в сфері безпеки до нас застосовуються, але вони ніколи не були зафіксовані письмово.

«2» – У нас немає формалізованої письмової політики безпеки, яка до нас застосовується, тому ми сформулювали її самостійно для власних потреб. Наше керівництво офіційно її не затверджувало.

«3» – У нас є письмова політика безпеки, яка до нас застосовується, затверджена керівництвом нашої команди.

«4» – У нас є письмова політика безпеки, яка до нас застосовується, затверджена керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи ми дотримуємося цієї політики і чи підходить вона нам.

7.2 Категорія Н: Персонал

Під персоналом маються на увазі особи, які спільно працюють для надання сервісів та виконання повноважень. Параметри стосуються найважливішого ресурсу будь-якого CSIRT – людського капіталу.

7.2.1 Н-1 Правила професійної поведінки та етики

Опис: *Набір правил або настанов для членів CSIRT щодо професійної поведінки, дія яких може також поширюватися на поведінку поза роботою. Чи надає ваш CSIRT рекомендації, настанови або правила для своїх членів щодо професійної та етичної поведінки? Часто це називають "кодексом поведінки" або "кодексом професійної етики". Такий документ може визначати еталонні принципи в сфері конфіденційності, надійності та інших ключових якостей, яких очікують від членів команди CSIRT. Зверніть увагу, що у більшості випадків головна/материнська організація, в якій функціонує CSIRT, вже має певний етичний кодекс. Однак такі документи зазвичай є загальними й не враховують специфіку діяльності CSIRT, тому вони не можуть вважатися достатніми для відповідності параметру Н-1. CSIRT регулярно працює з вкрай чутливими даними та комунікує не лише всередині головної/материнської організації, але й із зовнішніми сторонами. Крім того, відповідальна поведінка членів команди CSIRT важлива не лише в робочому контексті, але й у приватному житті, коли справа стосується безпеки. За основу для такого кодексу можна використовувати Кодекс професійної етики CSIRT (CSIRT Code of Practice, або CCoP) від Trusted Introducer, оскільки він розроблений спеціально для CSIRT. Ще одним якісним орієнтиром є ініціатива EthicsFIRST, створена організацією FIRST. Водночас окремі спільноти CSIRT або навіть конкретні команди можуть мати обґрунтовані причини для розробки власного кодексу. Важливо також забезпечити належну узгодженість такого кодексу з політикою безпеки (параметр О-11).*

Пояснення: Наприклад, CCoP від Trusted Introducer (<https://www.trusted-introducer.org/TI-CCoP.pdf>) або EthicsFIRST (<https://ethicsfirst.org>). Поведінка поза роботою є суттєвою, оскільки від членів CSIRT може очікуватися відповідальна поведінка й у приватному житті в усьому, що стосується інформаційної та кібербезпеки.

Чи впроваджено правила професійної поведінки та етики у вашій команді?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – Ми знаємо, якої професійної поведінки та етики від нас очікують, але вони ніколи не були зафіксовані письмово.

«2» – У нас немає формалізованих письмових правил поведінки та етики, тому ми сформулювали їх самостійно для власних потреб. Наше керівництво офіційно їх не затверджувало.

«3» – У нас є письмові правила поведінки та етики, затверджені керівництвом нашої команди.

«4» – У нас є письмові правила поведінки та етики, затверджені керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи ми дотримуємося цих правил, якою мірою і чи вони виконують свою задачу.

7.2.2 Н-2 Операційна стійкість персоналу

Опис: Як у CSIRT забезпечується достатня кількість персоналу, коли співробітники хворіють, ходять у відпустку, звільняються тощо. Чи має ваш CSIRT достатню кількість персоналу, щоб впоратися із запланованою або непередбаченою відсутністю членів команди? До таких випадків належать хвороби, відпустки, звільнення тощо. Залежно від переліку сервісів (параметр О-5) та рівнів надання сервісів (параметр О-7), кількість членів команди може відрізнятися, однак забезпечення доступності в кризових ситуаціях має бути організоване заздалегідь. Виходячи з мінімального переліку сервісів, які мають надаватися за будь-яких умов, загально визнано, що абсолютним мінімумом для будь-якого CSIRT є три члени команди (з частковою зайнятістю). Зверніть увагу, що стійкість персоналу також є складовою управління безперервністю бізнесу (BSM), що також розглядається в параметрах О-11 та від Т-5 до Т-7. Керівництво команди реагування зобов'язане вживати організаційних та адміністративних заходів для підтримки операційної стійкості персоналу на рівні, достатньому для виконання покладених на команду реагування завдань, особливо в кризових ситуаціях. Мінімальна штатна чисельність команди реагування – три співробітники, що можуть бути залучені на умовах повної або часткової зайнятості. Штатна чисельність команди реагування повинна визначатися з урахуванням опису сервісів (параметр О-5), що надаються, та встановлених рівнів їх надання (параметр О-7). Зовнішні ресурси (залучення постачальників послуг кібербезпеки, угоди про взаємодопомогу, залучення персоналу за сумісництвом) можуть доповнювати штатний мінімум, але не заміщувати його. Відповідна залежність підлягає документуванню та узгодженню з параметрами О-11 і Т-5 – Т-7 у частині управління безперервністю діяльності.

Мінімальна вимога: Три члени CSIRT (з частковою або повною зайнятістю).

Чи дотримується ваша команда вимог до операційної стійкості персоналу?

Значення:

«0» – Ми дотримуємося мінімальних вимог.

«1» – У нас достатньо персоналу для забезпечення операційної стійкості, але це ніколи не було зафіксовано письмово.

«2» – У нас немає формалізованого документа щодо операційної стійкості персоналу CSIRT, тому ми сформулювали його самостійно для власних потреб. Керівництво нашої команди офіційно його не затверджувало.

«3» – У нас є формалізований документ щодо операційної стійкості персоналу CSIRT, затверджений керівництвом нашої команди.

СТД-04-001-2026-B

«4» – У нас є формалізований документ щодо операційної стійкості персоналу CSIRT, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, якою була ситуація з кадрами та чи була забезпечена достатня операційна стійкість персоналу.

7.2.3 Н-3 Опис професійних компетенцій

Опис: *Описує професійні компетенції (навички), необхідні для виконання посадових обов'язків персоналу CSIRT. Чи має ваш CSIRT опис необхідних навичок для всіх посад у команді? Усі посади мають бути визначені та супроводжуватися описом очікуваних навичок: сюди входять технічні навички, знання, досвід, а також навички комунікації, роботи в команді, здатності працювати в умовах стресу тощо. Планування професійного розвитку персоналу (параметр Н-4) може допомогти усунути прогалини в навичках членів команди.*

Пояснення: Чудовою відправною точкою є документ CSIRT Roles and Competencies від FIRST (https://www.first.org/standards/frameworks/csirts/csirt_roles_competences).

Чи описала ваша команда необхідні професійні компетенції?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього. У нас досвідчений персонал.

«1» – Ми знаємо, які професійні компетенції повинні мати, але вони ніколи не були зафіксовані письмово.

«2» – У нас немає формалізованого письмового опису професійних компетенцій, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є письмовий опис професійних компетенцій, затверджений керівництвом нашої команди.

«4» – У нас є письмовий опис професійних компетенцій, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цих професійних компетенцій достатньо, щоб справлятися з поточними загрозами та кіберінцидентами.

7.2.4 Н-4 Професійний розвиток персоналу

Опис: *Політика професійного розвитку персоналу, спрямована на забезпечення навчання нових членів команди та підвищення кваліфікації наявних співробітників. Чи має ваш CSIRT політику професійного розвитку персоналу? Цей параметр стосується розвитку персоналу в цілому і включає, з-поміж іншого, план навчання для нових членів команди, планування індивідуального розвитку та каталог навчальних курсів для чинних співробітників, програми тимбілдінгу/освіти тощо. Розвиток персоналу має забезпечувати як новим, так і наявним членам команди можливість покращувати свої навички та досягати цілей, визначених в описі професійних компетенцій (параметр Н-3), що застосовується до їхньої посади. Розвиток персоналу може реалізовуватися у формі наставництва на робочому місці,*

СТД-04-001-2026-B

внутрішніх або зовнішніх навчальних курсів, а також включає програми взаємного менторства (коли колеги допомагають одне одному вдосконалюватися у своїй роботі), оцінювальні співбесіди з керівництвом, командні зустрічі та внутрішні воркшопи. Зверніть увагу, що параметри Н-5 і Н-6 деталізують два важливих аспекти розвитку персоналу, які є настільки значущими, що винесені в окремі параметри, тоді як параметр Н-4 є узагальнюючою політикою.

Чи має ваша команда політику професійного розвитку персоналу?

Значення:

«0» – Ми не надаємо такого виду навчання.

«1» – У нас є ідеї щодо професійного розвитку персоналу та/або ми навчаємо членів команди неформально, але ніколи не документували вимоги до навчання, теми чи матеріали.

«2» – У нас немає формалізованої політики професійного розвитку персоналу, тому ми сформулювали її самостійно для власних потреб. Наше керівництво офіційно її не затверджувало.

«3» – У нас є політика професійного розвитку персоналу, затверджена керівництвом нашої команди.

«4» – У нас є політика професійного розвитку персоналу, затверджена керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи політика професійного розвитку персоналу виконується належним чином для задоволення потреб команди в навчанні.

7.2.5 Н-5 Розвиток технічних навичок

Опис: *Чи пропонує ваш CSIRT членам команди навчання (зовнішнє та/або внутрішнє), яке вони можуть проходити для покращення технічних навичок з метою досягнення рівня, встановленого в описі професійних компетенцій (параметр Н-3) для даної посади? Сюди входять нові теми, майбутні напрями розвитку безпеки, а також поглиблене вивчення технологій. До навчальних курсів, пов'язаних із діяльністю CSIRT, належать TRANSITS, курси, що проводяться Агентством ЄС з кібербезпеки (ENISA) або FIRST чи регіональними спільнотами, а також комерційні навчальні програми, наприклад від CERT/CC, SANS тощо. Зверніть увагу, що параметр Н-5 має бути частиною параметра Н-4, але є настільки важливим, що розглядається як окремий параметр.*

Чи має ваша команда політику розвитку технічних навичок?

Значення:

«0» – У нас немає можливостей, часу чи коштів для такого виду навчання.

«1» – Ми направляємо співробітників на таке навчання за потреби, але не маємо письмової політики розвитку технічних навичок.

СТД-04-001-2026-B

«2» – У нас немає формалізованої політики розвитку технічних навичок, тому ми сформулювали її самостійно для власних потреб, що допомагає організовувати направлення співробітників на таке навчання. Наше керівництво офіційно не затверджувало цю програму.

«3» – У нас є політика розвитку технічних навичок, затверджена керівництвом нашої команди, яка дозволяє направляти співробітників на таке навчання.

«4» – У нас є політика розвитку технічних навичок, затверджена керівництвом нашої команди, яка дозволяє направляти співробітників на таке навчання. Під час періодичної перевірки нашої команди оцінюється, чи політика розвитку технічних навичок виконується належним чином для задоволення потреб команди в навчанні.

7.2.6 Н-6 Розвиток навичок з комунікації та взаємодії

Опис: Програма для надання співробітникам можливості проходити навчання для покращення навичок з комунікації та взаємодії, зокрема навичок міжособистісної комунікації та презентації. Чи пропонує ваш CSIRT членам команди навчання (зовнішнє та внутрішнє), яке вони можуть проходити для розвитку навичок з комунікації та взаємодії з метою досягнення рівня, встановленого в описі професійних компетенцій (параметр Н-3) для даної посади? Усі члени команди повинні проходити навчання з комунікації та взаємодії, як робота в команді, тайм-менеджмент, робота в умовах стресу і особливо міжособистісна комунікація та презентація. Останні необхідні для більш ефективної взаємодії з користувачами, колегами, керівниками, партнерами, місцевими або іноземними органами влади, а інколи й з медіа. Це стосується всіх каналів комунікації, наприклад телефонного зв'язку, чатів, електронної пошти, соціальних мереж, і всіх типів взаємодії: безпосереднього спілкування, зустрічей, презентацій, підготовки попереджень та звітів, написання публікацій в блогах, дописів у соцмережах і текстових повідомлень. Це охоплює як формальну, так і неформальну комунікацію і стосується не лише робочих процесів, але й інколи позаробочої діяльності (з дотриманням правил професійної поведінки та етики, визначених в параметрі Н-1). Також необхідно враховувати, що хоча "звичайна" комунікація охоплює 90% або більше ситуацій, кризова комунікація має інший характер, але є не менш важливою. Також, ті співробітники, які можуть взаємодіяти з медіа, повинні проходити додаткове спеціалізоване навчання. Зверніть увагу, що параметр Н-6 має бути складовою параметра Н-4, але є настільки важливим, що розглядається як окремий параметр.

Чи має ваша команда політику розвитку навичок з комунікації та взаємодії?

Значення:

«0» – У нас немає можливостей, часу чи коштів для такого виду навчання.

«1» – Ми направляємо співробітників на таке навчання за потреби, але не маємо письмової політики з цього питання.

«2» – У нас немає формалізованої політики розвитку навичок з комунікації та взаємодії, тому ми сформулювали її самостійно для власних потреб, що допомагає організовувати направлення співробітників на таке навчання. Наше керівництво офіційно не затверджувало цю політику.

«3» – У нас є політика розвитку навичок з комунікації та взаємодії, затверджена керівництвом нашої команди, яка дозволяє направляти співробітників на таке навчання.

«4» – У нас є політика розвитку навичок з комунікації та взаємодії, затверджена керівництвом нашої команди, яка дозволяє направляти співробітників на таке навчання. Під час періодичної перевірки нашої команди оцінюється, чи політика розвитку навичок з комунікації та взаємодії виконується належним чином для задоволення потреб команди в навчанні.

7.2.7 Н-7 Зовнішня взаємодія та професійні зв'язки

Опис: *Чи має ваш CSIRT політику щодо відрядження членів команди на зустрічі, пов'язані з діяльністю CSIRT або кібербезпекою? Це сприяє роботі спільнот CSIRT на національному, галузевому, регіональному та/або міжнародному рівнях (тема параметра О-9), а такі спільноти є принципово важливими для успіху та ефективності всіх CSIRT. Крім того, особисті зустрічі створюють основу для встановлення довірчих відносин з колегами, а довіра є фундаментом співпраці між CSIRT.*

Чи має ваша команда політику щодо зовнішньої взаємодії та професійних зв'язків?

Значення:

«0» – У нас немає можливостей, часу чи коштів для такої діяльності.

«1» – Ми відвідуємо такі зустрічі, коли є можливість, але це ніяк не задокументовано.

«2» – У нас немає формалізованої письмової політики щодо зовнішньої взаємодії та професійних зв'язків, тому ми сформулювали її самостійно для власних потреб. Наше керівництво офіційно її не затверджувало.

«3» – У нас є формалізована письмова політика щодо зовнішньої взаємодії та професійних зв'язків, затверджена керівництвом нашої команди.

«4» – У нас є формалізована письмова політика щодо зовнішньої взаємодії та професійних зв'язків, затверджена керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи ми налагоджуємо зовнішню взаємодію, наскільки активно, а також які результати це приносить.

7.3 Категорія Т: Інструменти

Під інструментами маються на увазі сукупність програм, застосунків, сервісів та технічних засобів, що уможливають або покращують управління інцидентами безпеки, роблячи його швидшим, якіснішим та більш детальним.

7.3.1 Т-1 ІТ-активи та їх конфігурації

Опис: *Описує активи (апаратне забезпечення, програмне забезпечення, операційні технології тощо), які широко використовуються серед користувачів, зокрема їхні конфігурації, щоб CSIRT міг надавати адресні рекомендації з урахуванням цих особливостей. Наявність актуального та достатньо детального переліку того, які обчислювальні, мережеві та операційно-технологічні (ОТ) ресурси використовують клієнти, є дуже важливою для ефективного управління кіберінцидентами. Такий перелік має включати інформацію про апаратне забезпечення, програмне забезпечення та ОТ, які використовують клієнти. Він також має охоплювати актуальні конфігурації: більш детальна інформація (включно з версіями програмного забезпечення у використанні) необхідна для більш ефективної протидії загрозам. Деякі організації використовують для цього управління ІТ-активами (IT Assets Management, або ITAM) і підтримують базу даних керування конфігураціями (Configuration Management Database, або CMDB). Зазвичай CSIRT не керує такими списками активів/конфігурацій, але потребує доступу до них. Підтримання актуальної та детальної інформації про весь ландшафт ІТ-активів, програмного забезпечення та конфігурацій є складним завданням, а іноді навіть неможливим: наприклад, у випадку координаційних CSIRT, клієнти яких "використовують все, що тільки можна уявити". У такій ситуації можна сфокусуватися лише на найкритичніших активах, і тоді саме CSIRT може збирати та підтримувати цю інформацію у безпосередній взаємодії з клієнтами. Для національних CSIRT це завдання ще складніше, і їм особливо необхідно зосереджуватися на активах критичної інформаційної інфраструктури.*

Чи має ваш CSIRT перелік ІТ-активів або має доступ до переліку ІТ-активів та конфігурацій клієнтів?

Значення:

«0» – Ми насправді не знаємо.

«1» – Ми маємо загальне уявлення про найважливіші ІТ-активи, але формального переліку не існує.

«2» – У нас немає формалізованого переліку ІТ-активів, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

СТД-04-001-2026-B

«3» – Ми маємо доступ до формалізованого переліку ІТ-активів і конфігурацій, який затверджено керівництвом нашої команди.

«4» – Ми маємо доступ до формалізованого переліку ІТ-активів і конфігурацій, який затверджено керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи є цей перелік корисним і достатньо точним для досягнення наших цілей.

7.3.2 Т-2 Перелік джерел інформації

Опис: *Джерела, з яких CSIRT отримує інформацію про вразливості/загрози/результати сканування. Дуже важливою частиною роботи CSIRT є щоденний моніторинг усіх релевантних джерел інформації. Ці джерела повинні включати, наприклад, відповідні акаунти в соціальних мережах, які публікують або поширюють цінну інформацію, а також блоги чи вебсайти з інформацією в сфері кібербезпеки. Важливими є як інформація, що потребує оперативного реагування, так і довгострокові спостереження: це дає змогу постійно коригувати діяльність CSIRT і, що найважливіше, своєчасно та ефективно реагувати на поточні події. Звісно, цей перелік потребує постійного оновлення. До джерел інформації належать, зокрема, але не виключно, платформи кіберрозвідки та канали обміну структурованими даними про загрози у форматах STIX 2.1/TAXII 2.1.*

Чи має ваша команда перелік джерел інформації?

Значення:

«0» – У нас немає такого переліку. Ми не стежимо за джерелами інформації систематично, але натомість реагуємо на повідомлення про кіберінциденти.

«1» – Ми знаємо, які джерела інформації є для нас найважливішими, і стежимо за ними, але не ведемо їхнього переліку.

«2» – У нас немає формалізованого переліку джерел інформації, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований перелік джерел інформації, затверджений керівництвом нашої команди.

«4» – У нас є формалізований перелік джерел інформації, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи є цей перелік корисним і достатнім для наших цілей.

7.3.3 Т-3 Об'єднані системи обміну повідомленнями

Опис: *Якщо вся електронна пошта та інші типи повідомлень CSIRT (з Signal, Threema, WhatsApp тощо) зберігаються в системах, доступних усім членам команди, то такі системи обміну повідомленнями називають об'єднаними. CSIRT має організовувати свою роботу таким чином, щоб забезпечити ефективне опрацювання кіберінцидентів. Це включає постійний обмін інформацією між членами команди – у багатьох випадках навіть тоді, коли вони не перебувають на чергуванні. Крім того, потрібно отримувати повідомлення про*

СТД-04-001-2026-B

кіберінциденти, а також керувати комунікацією з іншими командами. В більшості таких випадків основними механізмами комунікації є електронна пошта та месенджери, наприклад Signal, Threema та WhatsApp. Тому команда повинна мати стійкі, високоякісні системи обміну повідомленнями, які є об'єднаними (в офісі команди з належними можливостями резервування або за допомогою захищених хмарних рішень), і всі члени команди повинні мати до них доступ. Звичайно, можна використовувати системи обміну повідомленнями головної/материнської організації або хмарні сервіси, однак слід враховувати безпеку таких систем та використовувати надійне шифрування для захисту конфіденційних даних.

Чи використовує ваш CSIRT об'єднані системи обміну повідомленнями?

Значення:

«0» – Повідомлення надходять на ноутбуки/комп'ютери членів команди. Немає потреби зберігати їх в одному місці.

«1» – Ми зберігаємо повідомлення у спеціалізованих системах, але ці системи не перебувають під нашим контролем, і ми майже нічого про них не знаємо.

«2» – Ми зберігаємо повідомлення у спеціалізованих системах. Наше керівництво офіційно не затверджувало цього.

«3» – Ми зберігаємо повідомлення у спеціалізованих системах, і це було затверджено керівництвом нашої команди.

«4» – Ми зберігаємо повідомлення у спеціалізованих системах, і це було затверджено керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи відповідають ці системи вимогам.

7.3.4 T-4 Система реєстрації та відстеження кіберінцидентів

Опис: Тікет-система або програмне забезпечення для керування робочими процесами, які використовуються CSIRT для реєстрації кіберінцидентів і відстеження їх опрацювання. Добре спроектована та адаптована під потреби команди тікет-система є важливою для будь-якого CSIRT. На практиці, коли команді доводиться обробляти велику кількість кіберінцидентів, майже неможливо коректно керувати всією інформацією та комунікацією між членами команди й залученими сторонами без такої системи. Лише дуже малі команди з невеликою кількістю кіберінцидентів можуть керувати процесом реагування на кіберінциденти за допомогою дуже простого рішення, наприклад спільної електронної таблиці. У більшості випадків потрібне спеціалізоване рішення. Іноді команда використовує тікет-систему, впроваджену в головної/материнської організації. Безумовно, це можливо, але, подібно до випадку з системою обміну повідомленнями, тут може виникати проблема конфіденційності, оскільки більшість універсальних тікет-систем проєктувалися без урахування вимог безпеки. Багато CSIRT протягом тривалого часу використовують власні спеціалізовані системи реєстрації та відстеження кіберінцидентів, зокрема рішення з

СТД-04-001-2026-B

відкритим вихідним кодом, такі як RT(IR) (Request Tracker for Incident Response), OTRS (Open Source Ticket Request System) або, віднедавна, TheHive. Усі ці рішення є масштабованими та простими у використанні.

Чи використовує ваша команда систему реєстрації та відстеження кіберінцидентів?

Значення:

«0» – Ми обробляємо кіберінциденти, але не маємо інструменту для їх реєстрації та відстеження.

«1» – У нас є спосіб реєстрації та відстеження кіберінцидентів, але він не задокументований.

«2» – У нас є система реєстрації та відстеження кіберінцидентів, офіційно не визначена нашим керівництвом.

«3» – У нас є система реєстрації та відстеження кіберінцидентів, офіційно визначена нашим керівництвом.

«4» – У нас є система реєстрації та відстеження кіберінцидентів, офіційно визначена нашим керівництвом. Під час періодичної перевірки нашої команди оцінюється, чи відповідає ця система вимогам.

7.3.5 T-5 Стійкість послуг голосової електронної комунікації

Опис: Голосова електронна комунікація (як через традиційні телефонні дзвінки, так і через дзвінки в месенджерах) є принципово важливим інструментом комунікації для CSIRT. Це невід'ємна складова в роботі членів команди: як в управлінні кіберінцидентами, так і у виконанні інших обов'язків. Тому час безперебійної роботи доступних засобів голосової електронної комунікації має відповідати рівням надання сервісів команди (параметр O-7). Якщо команда повинна оперативно реагувати на кіберінциденти та швидко їх усувати, то показник часу безперебійної роботи засобів голосової електронної комунікації має бути дуже високим, щоб будь-який збій у цих засобах не заважав роботі команди. Слід брати до уваги всі доступні команді засоби голосової електронної комунікації: класичний стаціонарний телефон, IP-телефонію, мобільні телефони та месенджери, наприклад Signal, Threema, WhatsApp та інші. Мобільні телефони з їхніми численними застосунками часто забезпечують надійне резервування, особливо якщо використовуються сервіси кількох мобільних операторів. Окремий, хоча й рідкісний, випадок – наявність у команди доступу до захищеної системи зв'язку, як правило, національного рівня.

Мінімальна вимога: Резервний механізм на випадок відмови послуги голосової електронної комунікації.

СТД-04-001-2026-B

Які засоби голосової електронної комунікації є у вашої команди й чи достатньо вони стійкі для ваших потреб?

Значення:

«0» – Ми практично нічого не знаємо про рівні надання сервісів наших послуг голосової електронної комунікації і не передбачили жодного резервного механізму.

«1» – Коли наші послуги голосової електронної комунікації виходять з ладу, ми переходимо на резервний механізм, однак це ніде не задокументовано.

«2» – Коли наші послуги голосової електронної комунікації виходять з ладу, ми переходимо на резервний механізм, і це задокументовано. Наше керівництво офіційно цього не затверджувало.

«3» – Коли наші послуги голосової електронної комунікації виходять з ладу, ми переходимо на резервний механізм. Це задокументовано і затверджено керівництвом нашої команди.

«4» – Коли наші послуги голосової електронної комунікації виходять з ладу, ми переходимо на резервний механізм. Це задокументовано і затверджено керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи відповідає резервний механізм нашим вимогам і чи обізнані про це наші співробітники.

7.3.6 T-6 Стійкість систем обміну повідомленнями

Опис: Системи обміну повідомленнями, наявні у CSIRT, вважаються стійкими, якщо їх рівні надання сервісів за часом безперебійної роботи та часом відновлення після збою відповідають вимогам до рівня надання сервісів CSIRT або перевищують їх. Електронна пошта та інші системи обміну повідомленнями є фундаментальним інструментом комунікації для CSIRT. Вони є невід'ємною складовою в роботі членів команди CSIRT: через них надходять повідомлення про кіберінциденти, здійснюється управління кіберінцидентами та виконуються інші обов'язки. Тому час безперебійної роботи наявних засобів обміну повідомленнями має відповідати рівням надання сервісів команди (параметр O-7). Якщо команда повинна мати змогу швидко реагувати на кіберінциденти та оперативно їх усувати, показник часу безперебійної роботи засобів обміну повідомленнями має бути дуже високим, щоб будь-який збій у їхній роботі не перешкоджав ефективності команди. З електронною поштою також пов'язаний репутаційний аспект: коли особа, що повідомила про кіберінцидент, або інший CSIRT отримують у відповідь повідомлення про те, що поштовий сервіс вашої команди не працює, це завдає шкоди репутації. У випадку електронної пошти можливим рішенням на рівні сучасних стандартів є гарячий резерв або повністю відмовостійка конфігурація у поєднанні з надійним резервним копіюванням сховища пошти, яке містить важливі дані про кіберінциденти. Для месенджерів з наскрізним шифруванням,

СТД-04-001-2026-B

таких як *Signal*, важливо передбачити належні схеми резервного копіювання, оскільки за своєю архітектурою ці засоби не передбачають хмарного зберігання даних.

Які системи обміну повідомленнями використовує ваша команда й чи достатньо вони стійкі для ваших потреб?

Значення:

«0» – Ми практично нічого не знаємо про рівні надання сервісів наших систем обміну повідомленнями.

«1» – Рівень надання сервісів наших систем обміну повідомленнями є достатнім для наших потреб, однак ми не маємо жодної документації стосовно цього.

«2» – Рівень надання сервісів наших систем обміну повідомленнями є достатнім для наших потреб, і ми маємо неформальну документацію стосовно цього. Наше керівництво офіційно цього не затверджувало.

«3» – Рівень надання сервісів наших систем обміну повідомленнями є достатнім для наших потреб, і ми маємо документацію стосовно цього, яка була затверджена керівництвом нашої команди.

«4» – Рівень надання сервісів наших систем обміну повідомленнями є достатнім для наших потреб, і ми маємо документацію стосовно цього, яка була затверджена керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи є стійкість систем обміну повідомленнями достатньою.

7.3.7 T-7 Стійкість доступу до мережі Інтернет

Опис: Достатньо швидкий і надійний доступ до мережі Інтернет є критично важливим для CSIRT. Без нього CSIRT не може нормально функціонувати. Тому час безперебійної роботи доступу до мережі Інтернет має щонайменше відповідати рівням надання сервісів команди (параметр O-7), а бажано перевищувати їх. Якщо команда повинна мати змогу швидко реагувати на кіберінциденти та оперативно їх усувати, то показник часу безперебійної роботи доступу до мережі Інтернет має бути дуже високим, щоб будь-який збій у цій сфері не перешкодив ефективності команди. В ідеалі CSIRT або його головна/материнська організація має повністю резервований доступ до мережі Інтернет (навіть на фізичному рівні), однак значно дешевші рішення, як-от наявність альтернативного каналу доступу до мережі Інтернет (із застосуванням технології, відмінної від основної), також можуть забезпечити виконання вимог команди щодо рівня надання сервісів. Оскільки більшість команд у питанні доступу до мережі Інтернет залежать від головної/материнської організації, корисно, щоб всередині організації команда була визнана однією зі структурних одиниць із найвищими вимогами до доступу до мережі Інтернет.

Якими засобами доступу до мережі Інтернет користується ваша команда й чи достатньо вони стійкі для ваших потреб?

Значення:

«0» – Ми фактично нічого не знаємо про рівні надання сервісів нашого доступу до мережі Інтернет.

«1» – Рівень надання сервісів нашого доступу до мережі Інтернет є достатнім для наших потреб, однак ми не маємо жодної документації стосовно цього.

«2» – Рівень надання сервісів нашого доступу до мережі Інтернет є достатнім для наших потреб, і ми маємо неформальну документацію стосовно цього. Наше керівництво офіційно цього не затверджувало.

«3» – Рівень надання сервісів нашого доступу до мережі Інтернет є достатнім для наших потреб, і ми маємо документацію стосовно цього, яка була затверджена керівництвом нашої команди.

«4» – Рівень надання сервісів нашого доступу до мережі Інтернет є достатнім для наших потреб, і ми маємо документацію стосовно цього, яка була затверджена керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи є стійкість доступу до мережі Інтернет достатньою.

7.3.8 T-8 Інструменти для запобігання кіберінцидентам

Опис: Цей параметр полягає в наявності чітко визначеного та належно впровадженого набору інструментів, що сприяють запобіганню кіберінцидентам. Ці інструменти входять в першу лінію захисту для клієнтів. CSIRT має чітко визначити свою роль щодо кожного з таких інструментів. Деякі з них команда може експлуатувати самостійно, в інших випадках вона може виступати архітектором і користувачем – або лише користувачем чи просто мати доступ до результатів. У зв'язку зі зростаючою кількістю можливих інструментів дедалі більшого значення набуває їх "оркестрація". Для будь-якого CSIRT вкрай важливо бути безпосередньо залученим до цієї сфери або навіть ухвалювати рішення щодо таких інструментів. Серед прикладів інструментів для запобігання кіберінцидентам можна навести системи запобігання вторгненням, антивірусне програмне забезпечення, спам-фільтри та сканери вразливостей. До таких інструментів належать, зокрема, але не виключно, платформи автоматизації та оркестрації реагування (SOAR) у частині автоматизованого застосування запобіжних заходів.

Пояснення: Наприклад: система запобігання вторгненням, сканування на наявність вірусів, спам-фільтри, сканування портів. Якщо це до вас не відноситься, оскільки ви суто координаційний CSIRT, виберіть варіант «Не застосовується», і цей параметр буде виключено з оцінювання.

Чи має ваша команда визначений набір інструментів для запобігання кіберінцидентам?

Значення:

Не застосовується – Ми є виключно командою координації/врегулювання кіберінцидентів і не займаємося їх запобіганням.

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є такі інструменти, однак вони не зведені у перелік і не задокументовані.

«2» – У нас є такі інструменти, і ми зафіксували певну інформацію про них для власних потреб. Наше керівництво офіційно цього не затверджувало.

«3» – У нас є такі інструменти, вони задокументовані та затверджені керівництвом нашої команди.

«4» – У нас є такі інструменти, вони задокументовані та затверджені керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи достатньо цих інструментів для виконання наших вимог.

7.3.9 T-9 Інструменти для виявлення кіберінцидентів

Опис: Цей параметр полягає в наявності чітко визначеного та належно впровадженого набору інструментів, що сприяють виявленню кіберінцидентів. Ці інструменти є очима й вухами CSIRT, вони постачають інформацію про загрози та кіберінциденти на всіх етапах – від потенційних до вже реалізованих. CSIRT має чітко визначити свою роль щодо кожного з таких інструментів. Деякі з них команда може експлуатувати самостійно, в інших випадках вона може виступати архітектором і користувачем – або лише користувачем чи просто мати доступ до результатів. У зв'язку зі зростаючою кількістю можливих інструментів дедалі більшого значення набуває їх "оркестрація". Для будь-якого CSIRT вкрай важливо бути безпосередньо залученим до цієї сфери або навіть ухвалювати рішення щодо таких інструментів. Серед прикладів інструментів для виявлення кіберінцидентів можна навести MISP, AbuseHelper, IntelMQ, аналізатори мережесих пакетів. Також пам'ятайте, що телефон та електронна пошта використовуються для отримання повідомлень про кіберінциденти і, відповідно, теж є інструментами їх виявлення. До інструментів виявлення належать, зокрема, але не виключно, платформи кіберрозвідки, засоби приймання структурованих даних про загрози у форматах STIX 2.1/TAXII 2.1 та платформи автоматизації і оркестрації реагування (SOAR) у частині кореляції подій.

Чи має ваша команда визначений набір інструментів для виявлення кіберінцидентів?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є такі інструменти, однак вони не зведені у перелік і не задокументовані.

«2» – У нас є такі інструменти, і ми зафіксували певну інформацію про них для власних потреб. Наше керівництво офіційно цього не затверджувало.

СТД-04-001-2026-B

«3» – У нас є такі інструменти, вони задокументовані та затверджені керівництвом нашої команди.

«4» – У нас є такі інструменти, вони задокументовані та затверджені керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи достатньо цих інструментів для виконання наших вимог.

7.3.10 T-10 Інструменти для реагування на кіберінциденти та усунення їх наслідків

Опис: Цей параметр визначає наявність чітко визначеного та належно впровадженого набору інструментів для оброблення кіберінцидентів. Ці інструменти забезпечують виконання основної діяльності будь-якого CSIRT – оброблення кіберінцидентів. CSIRT має чітко визначити свою роль щодо кожного з цих інструментів. Оскільки вони є критично важливими, команда, найімовірніше, самостійно експлуатує частину з них або виступає головним архітектором і одним із ключових користувачів – однак в окремих випадках команда може бути лише користувачем інструменту, і тоді вона повинна забезпечити собі можливість надавати зворотний зв'язок і домагатися того, щоб її думку брали до уваги. У зв'язку зі зростаючою кількістю можливих інструментів дедалі більшого значення набуває їх "оркестрація". Для будь-якого CSIRT вкрай важливо бути безпосередньо залученим до цієї сфери. Якщо CSIRT опрацьовує певні специфічні типи кіберінцидентів, особливо важливо сформувати спеціалізований набір інструментів, адаптований до конкретних потреб оброблення. Варто пам'ятати, що такий набір охоплює не лише програмне забезпечення, а й може включати спеціалізоване апаратне забезпечення – в окремих випадках навіть може бути створено лабораторію для оброблення кіберінцидентів, наприклад для аналізу шкідливого програмного забезпечення чи комп'ютерної криміналістики. Серед прикладів інструментів для оброблення можна навести MISP та IntelMQ, систему реєстрації й відстеження кіберінцидентів та набори для комп'ютерної криміналістики. До інструментів оброблення належать, зокрема, але не виключно, платформи автоматизації та оркестрації реагування (SOAR) і засоби обміну відомостями про кіберінциденти у форматах STIX 2.1/TAXII 2.1.

Пояснення: Наприклад: базові інструменти CSIRT, зокрема whois, traceroute тощо; набори для комп'ютерної криміналістики.

Чи має ваша команда визначений набір інструментів для реагування на кіберінциденти та усунення їх наслідків?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є такі інструменти, однак вони не зведені у перелік і не задокументовані.

«2» – У нас є такі інструменти, і ми зафіксували певну інформацію про них для власних потреб. Наше керівництво офіційно цього не затверджувало.

«3» – У нас є такі інструменти, вони задокументовані та затверджені керівництвом нашої команди.

«4» – У нас є такі інструменти, вони задокументовані та затверджені керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи достатньо цих інструментів для виконання наших вимог.

7.4 Категорія Р: Процеси

Під процесами маються на увазі логічно впорядковані сукупності дій, що виконуються персоналом або автоматизованими інструментами з метою досягнення конкретного результату. У зрілих організаціях процеси є задокументованими, вимірюваними та відтворюваними

7.4.1 Р-1 Процес ескалації до вищого рівня управління

Опис: *Кожна команда повинна мати можливість ескалювати критичні кіберінциденти до відповідних рівнів керівництва, включаючи найвищий рівень управління (наприклад, директор, керівник органу держаної влади) у разі потенційних криз або кіберінцидентів, що становлять значну загрозу. Якщо команда відповідає за зовнішніх клієнтів, вона також повинна мати змогу ескалювати питання до відповідного рівня керівництва кожного з них. Така ескалація необхідна не лише тоді, коли звичайний контактний представник не реагує (або реагує несвоєчасно), а й може бути виправданою у випадку значного кіберінциденту чи нової загрози. Процедури ескалації, що ініціюються на базі кіберінцидентів або інших подій, мають бути визначені відповідно до класифікації кіберінцидентів, прийнятої в команді (параметр О-8), що дозволяє логічно обґрунтовувати ескалацію на основі таких критеріїв, як вплив і пріоритет. Вкрай важливо, щоб механізми процесу ескалації були доступні в будь-який момент, навіть якщо зворотна реакція не завжди буде негайною, оскільки це визначається вищими рівнями управління у власній організації або в організаціях клієнтів.*

Чи спроможна ваша команда здійснювати ескалацію до вищого рівня управління?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є неформальний спосіб ескалації, але це ніколи не було зафіксовано письмово.

«2» – У нас немає формалізованого письмового процесу ескалації, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес ескалації, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес ескалації, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи використовується цей процес належним чином і які були його результати.

7.4.2 Р-2 Процес комунікації з медіа

Опис: *Необхідно забезпечити належне опрацювання запитів від преси та інших медіа. Навіть якщо більшості або всім членам команди CSIRT заборонено спілкуватися з пресою безпосередньо, запити від преси щодо кіберінцидентів у сфері безпеки все одно мають опрацьовуватися належним чином, незалежно від каналу комунікації, яким вони надходять. Тому команда повинна мати змогу оперативно зв'язуватися з відповідними речниками або підрозділами, відповідальними за комунікацію з медіа. Щоб уникнути помилок у комунікації та затримок, які можуть негативно вплинути на репутацію організації, команда повинна мати змогу звертатися до таких представників пресслужби безпосередньо, зокрема в позаробочий час, з метою забезпечити їх необхідною інформацією про поточну ситуацію. Доцільно також визначити в межах самої команди обмежене коло співробітників, уповноважених спілкуватися з медіа, наприклад спільно з офіційним речником організації: такі представники команди зможуть надати глибше роз'яснення щодо технічних аспектів конкретної ситуації. У такому разі рекомендується забезпечити цим співробітникам відповідну підготовку.*

Чи має ваша команда процес комунікації з медіа?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є неформальний спосіб комунікації з медіа, але це ніколи не було зафіксовано письмово.

«2» – У нас немає формалізованого письмового процесу комунікації з медіа, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес комунікації з медіа, затверджений керівництвом нашої команди.

СТД-04-001-2026-B

«4» – У нас є формалізований письмовий процес комунікації з медіа, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи використовується цей процес належним чином і які були його результати.

7.4.3 Р-3 Процес взаємодії з юридичним підрозділом

Опис: *Необхідно забезпечувати врегулювання юридичних питань, зокрема запитів від правоохоронних органів. Такі запити до команди слід розглядати вкрай оперативно, щоб уникнути знищення або втрати доказів, наприклад внаслідок видалення даних автоматизованими процесами. Окрім того, неналежне врегулювання подібних питань може призвести до репутаційних збитків і фінансових втрат. Тому команда повинна мати можливість безпосередньо звертатися до юридичного підрозділу своєї організації, у тому числі в неробочий час, для інформування про відповідні ситуації, зокрема про надходження запитів або приписів/постанов від правоохоронних органів. Надалі юридичний підрозділ може вирішувати ці питання або самостійно, або спільно з командою.*

Чи має ваша команда процес взаємодії з юридичним підрозділом?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є неформальний спосіб взаємодії з юридичним підрозділом, але це ніколи не було зафіксовано письмово.

«2» – У нас немає формалізованого письмового процесу взаємодії з юридичним підрозділом, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес взаємодії з юридичним підрозділом, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес взаємодії з юридичним підрозділом, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи використовується цей процес належним чином і які були його результати.

7.4.4 Р-4 Процес запобігання кіберінцидентам

Опис: *Описує, яким чином CSIRT запобігає кіберінцидентам, зокрема використовує відповідний набір інструментів. Команда вживає заходів щодо надання попереджень про кіберзагрози, сповіщень, оголошень та інформування щодо кіберінцидентів, кібератак, кіберзагроз та вразливостей. Як правило, для підтримки цих процесів використовуються інструменти (параметр T-8), а порядок їх застосування визначається в рамках самого процесу.*

Пояснення: Якщо це до вас не відноситься, оскільки ви суто координаційний CSIRT, виберіть варіант «Не застосовується», і цей параметр буде виключено з оцінювання.

СТД-04-001-2026-B

Чи має ваша команда процес запобігання кіберінцидентам?

Значення:

Не застосовується – Ми є виключно командою координації/врегулювання кіберінцидентів і не займаємося їх запобіганням.

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є розуміння, як ми це робимо, але воно не задокументоване.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно.

7.4.5 P-5 Процес виявлення кіберінцидентів

Опис: *Без виявлення кіберінцидентів жодний CSIRT не здатний на них реагувати. Залежно від типу CSIRT, одні команди мають власні засоби виявлення (системи виявлення вторгнень, лог-файли брандмауерів, ханіпоти тощо), а інші покладаються на повідомлення від клієнтів або використовують SOC для отримання потенційних кіберінцидентів, що потребують аналізу. Можливий і змішаний підхід. Порядок дій у кожному з випадків описується в процесі (процесах) виявлення кіберінцидентів. Сортування (тріаж) вхідних повідомлень про кіберінциденти та їх направлення на подальше опрацювання, є складовою частиною виявлення кіберінцидентів. Як правило, для підтримки цих процесів використовуються інструменти (параметр T-8), а порядок роботи визначається в самих процесах. Зауважте, що параметри P-5 та P-6 нерідко об'єднуються в єдиний процес, який зазвичай називають процесом управління кіберінцидентами (або процесом врегулювання кіберінцидентів). Таке об'єднання є цілком прийнятним за умови, що належна увага приділяється як виявленню, так і реагуванню на кіберінциденти.*

Чи має ваша команда процес виявлення кіберінцидентів? (Якщо у вас є об'єднаний процес для параметрів P-5 і P-6, оберіть однаковий рівень для обох.)

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є розуміння, як ми це робимо, але воно не задокументоване.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

СТД-04-001-2026-B

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно.

7.4.6 P-6 Процес реагування на кіберінциденти та усунення їх наслідків

Опис: Будь-який CSIRT, що займається управлінням кіберінцидентами, повинен розробити щонайменше узагальнений процес реагування та усунення їх наслідків. Оскільки цей процес є узагальненим, кожен випадок обробляється за однією схемою більш-менш однаковим чином, хоча результати, безперечно, відрізнятимуться. Замість того щоб зосереджуватись на специфіці конкретного кіберінциденту (наприклад, APT-атака з використанням шкідливого програмного забезпечення суттєво відрізняється від DDoS-атаки), цей процес регламентує загальний покроковий підхід після завершення процесу виявлення (параметр P-5). Дотримання узагальненого процесу гарантує, що всі кіберінциденти обробляються відповідно до усталених практик, зокрема з використанням відповідного набору інструментів (параметр T-10). Наприклад, це може включати протоколювання всіх комунікацій з клієнтами або аналіз певних лог-файлів тощо.

Чи має ваша команда процес реагування на кіберінциденти та усунення їх наслідків? (Якщо у вас є об'єднаний процес для параметрів P-5 і P-6, оберіть однаковий рівень для обох.)

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є розуміння, як ми це робимо, але воно не задокументоване.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно.

7.4.7 P-7 Процеси реагування на різні категорії та типи кіберінцидентів і усунення їх наслідків

Опис: Наявність єдиного процесу реагування на всі кіберінциденти та усунення їх наслідків, якими управляє CSIRT, є вкрай важливою – це параметр P-6. Проте такий узагальнений процес забезпечує лише загальну схему роботи і не може бути адаптований до конкретних типів кіберінцидентів, а отже, майже напевно, не охопить деякі важливі

СТД-04-001-2026-B

технічні аспекти. Як уже зазначалося в параметрі Р-6, кіберінцидент, спричинений новим шкідливим програмним забезпеченням у рамках АPT-атаки, суттєво відрізняється від DDoS-атаки, що блокує доступ до мережі Інтернету для важливого користувача. Відмінності стосуються не лише пріоритетів, а й технічного реагування. Тому зрілим CSIRT рекомендується визначити типи кіберінцидентів, що створюють найбільше навантаження, і розробити для них окремі процеси реагування. Це дасть змогу виключити певні кроки чи дії, але натомість детальніше описати інші або додати нові (зокрема у вигляді підкроків узагальненого процесу). Крім того, окремі процеси реагування можна розробляти не лише для найпоширеніших типів кіберінцидентів, а й для критично важливих кіберінцидентів (з високим рівнем впливу та пріоритетом), а також для кіберінцидентів, реагування на які потребує компетенцій, що зазвичай відсутні всередині самого CSIRT. Зауважте, що параметр Р-7 може вже бути складовою параметра Р-6, якщо процес реагування передбачає підпроцеси для окремих типів кіберінцидентів або різні шляхи їх опрацювання – це цілком прийнятний підхід.

Пояснення: Може бути частиною Р-6.

Чи описала ваша команда процеси реагування на різні категорії та типи кіберінцидентів і усунення їх наслідків на додачу до узагальненого процесу реагування?

Значення:

«0» – Ми обробляємо всі кіберінциденти однаково, додаткової інформації для різних категорій та типів кіберінцидентів не передбачено.

«1» – У нас є певні усталені підходи до роботи з різними категоріями та типами кіберінцидентів, однак вони не задокументовані.

«2» – У нас немає формалізованого письмового процесу для реагування на різні категорії та типи кіберінцидентів і усунення їх наслідків, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є не менше одного формалізованого письмового процесу реагування на різні категорії та типи кіберінцидентів і усунення їх наслідків, затвердженого керівництвом нашої команди.

«4» – У нас є не менше одного формалізованого письмового процесу реагування на різні категорії та типи кіберінцидентів і усунення їх наслідків, затвердженого керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес (процеси) працює відповідно.

7.4.8 Р-8 Процес аудиту та отримання відгуку

Опис: *Усі CSIRT мають забезпечувати якість в усіх критичних і чутливих аспектах своєї діяльності. Хоча існують різноманітні засоби підтримання належного рівня якості*

СТД-04-001-2026-B

(наприклад, самооцінювання, покроковий аналіз, взаємні перевірки, внутрішні та зовнішні аудити), перевірка повинна мати чітко визначений рівень і обсяг, які підтримуються в актуальному стані. Крім того, необхідно забезпечити не лише проведення аудиту як такого, але й надання команді відгуку за результатами аудиту задля навчання та вдосконалення. Це є процесом аудиту та отримання відгуку. Цей процес має гарантувати досягнення належного рівня якості та максимально раннє виявлення проблем. Інформація, що формується в результаті, повинна бути корисною не лише для самої команди, а й для вищих рівнів управління. Це особливо важливо для тих параметрів, за якими команда прагне досягти рівня 4, – для них необхідна регулярна й активна форма перевірки з органом управління вищого рівня (вище керівника CSIRT). При цьому має бути задокументовано, що такий аудит проводиться і що команда отримує відгук за його підсумками. Залучення органу управління вищого рівня є ключовим механізмом, оскільки деякі аспекти якості не можуть бути забезпечені самим CSIRT, навіть якщо їх контролює керівник або тімлід команди. Неупереджений, об'єктивний відгук є обов'язковим: його мета не акцентувати увагу на помилках, а зосередити команду на вдосконаленні та прогресі з орієнтацією на призначення чи сферу відповідальності.

Пояснення: Під незалежним аудитом мається на увазі будь-який вид аудиту, що проводиться не самою командою, а здійснюється за рішенням органу управління вищого рівня. Такий аудит може бути внутрішнім (CISO або аудиторський підрозділ) або зовнішнім (підрядник або аудит у рамках спільноти CSIRT).

Чи визначено процес аудиту та отримання відгуку у вашому CSIRT?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є перевірки, однак вони не задокументовані.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Провідну роль у цьому відіграє орган управління вищого рівня.

7.4.9 P-9 Процес екстреної комунікації

Опис: Кожен CSIRT підтримує низку каналів комунікації, якими можна надсилати інформацію або повідомлення про кіберінциденти. Залежно від потреб клієнтів або повноважень CSIRT, такі канали або оприлюднюються для широкого загалу, або є доступними виключно для клієнтів чи партнерських CSIRT (параметр P-17). У більшості випадків години роботи CSIRT збігаються зі стандартним робочим часом. Деякі CSIRT працюють у режимі чергування й поза цим часом відповідно до власних рівнів надання сервісів.

СТД-04-001-2026-B

Проте у разі кризових чи екстрених ситуацій зв'язатися з CSIRT може знадобитися навіть поза звичайними робочими годинами. Щоб надати клієнтам або партнерським командам змогу звертатися до CSIRT у таких особливих випадках, необхідно мати процес екстреної комунікації, в якому визначено номери телефонів, адреси електронної пошти, а також, можливо, спеціальні кодові слова, зарезервовані для екстрених ситуацій. Процес повинен передбачати відповідальність за зловживання, оскільки реагування поза звичайними робочими годинами, як правило, пов'язане зі значними витратами. Водночас, з огляду на потенційну важливість цього механізму, процес необхідно час від часу відпрацьовувати на практиці для підготовки всіх залучених сторін.

Пояснення: Часто доступний лише для інших команд, партнерів або окремих клієнтів.

Чи має ваш CSIRT процес екстреної комунікації?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – Ключові зацікавлені сторони знають, як зв'язатися з нами в екстреній ситуації, однак ці способи не задокументовані.

«2» – У нас немає формалізованого письмового процесу екстреної комунікації, тому ми сформулювали його самостійно для власних потреб і поширили на ключові зацікавлені сторони. Наше керівництво офіційно цього не затверджувало.

«3» – У нас є формалізований письмовий процес екстреної комунікації, доступний зацікавленим сторонам і затверджений керівництвом нашої команди. (Зверніть увагу, що опублікована інформація, лише для клієнтів або у зовнішній базі даних, – також зараховується як рівень 3.)

«4» – У нас є формалізований письмовий процес екстреної комунікації, доступний зацікавленим сторонам і затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно.

7.4.10 P-10 Взаємодія через публічні вебресурси

Опис: Ефективна комунікація є основою роботи та успіху будь-якого CSIRT: вкрай важливо мати можливість звернутися через мережу Інтернет до інших та створити умови, щоб іншим було просто звернутися до вас. Окрім наявності різноманітних засобів комунікації (параметри T-5, T-6 та T-7), кожен CSIRT потребує процесу, який визначає перелік і порядок використання веб-ресурсів для відстеження вхідних запитів, обміну інформацією тощо з метою успішного надання сервісів та виконання повноважень й обов'язків команди. За трьома зазначеними напрямками цей процес має охоплювати таке: (1) Відстеження з боку CSIRT щонайменше стандартних адрес електронної пошти cert@... та security@... із наполегливою рекомендацією враховувати стандарт RFC 2142 та забезпечити відстеження відповідних імен поштових скриньок. Крім того, особи, відповідальні за моніторинг цих поштових скриньок, мають бути обізнані щодо CSIRT і знати, як передавати йому отриману інформацію. (2) Політика інтернет-представництва, що гарантує актуальність і доступність усієї релевантної інформації про CSIRT для клієнтів, а також обов'язкового

СТД-04-001-2026-B

мінімального набору відомостей, зокрема відповідно до RFC 2350 (параметр O-5), для широкого загалу. Додатково рекомендується розглянути можливість створення сторінки /security, яка може містити ширший спектр інформації з питань безпеки щодо вашої головної/материнської організації, але також включати інформацію про ваш CSIRT. (3) Політика щодо того, які соціальні мережі команда відстежує, а також порядок їх використання.

Мінімальна вимога: За трьома зазначеними напрямками цей процес має забезпечувати як мінімум: (1) відстеження командою адрес електронної пошти cert@... та security@...; (2) наявність певної форми інтернет-представництва CSIRT принаймні для внутрішнього використання; (3) наявність політики щодо того, чи використовуються соціальні мережі та яким чином.

Чи має ваш CSIRT процес, який визначає взаємодію через публічні вебресурси?

Значення:

«0» – Ми ніколи не приділяли цьому особливої уваги.

«1» – Ми дотримуємося деяких із цих найкращих практик, але вони не задокументовані.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно.

7.4.11 P-11 Процес безпечного поводження з інформацією

Опис: Описує порядок роботи CSIRT із конфіденційними повідомленнями про кіберінциденти та/або конфіденційною інформацією. Також охоплює відповідні юридичні вимоги, зокрема законодавство про захист персональних даних, наприклад Загальний регламент про захист даних (General Data Protection Regulation, або GDPR). Кожний CSIRT отримує та обробляє інформацію, яку відправники позначили як конфіденційну – наприклад, щоб запобігти її потраплянню до рук зломисників або публічному розповсюдженню в мережі Інтернет до того, як будуть поширені відповідні попередження. Тому CSIRT, а також, наприклад, дослідники вразливостей, неохоче діляться інформацією, якщо це неможливо зробити безпечним чином. Окрім безпеки каналів зв'язку, яку забезпечують протокол TLS та такі криптографічні застосунки, як GPG/PGP, інформація також має бути захищена на боці CSIRT, що її отримує (безпечне зберігання, резервне копіювання тощо), із дотриманням вимог чинного законодавства, зокрема законодавства про захист персональних даних. Для

СТД-04-001-2026-B

позначення обмежень щодо подальшого поширення переданої інформації розроблено протокол TLP (Traffic Light Protocol: див. www.first.org/tlp), і будь-якому CSIRT наполегливо рекомендується використовувати TLP та дотримуватися його вимог. Щонайменше команда повинна вміти належним чином поводитися з інформацією, позначеною мітками TLP. Існують також інші протоколи, які можна застосовувати в контексті роботи CSIRT, однак їх зазвичай потрібно окремо роз'яснювати.

Мінімальна вимога: Процес має підтримувати використання протоколу TLP (Traffic Light Protocol, www.first.org/tlp).

Чи має ваша команда процес безпечного поводження з інформацією?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є розуміння, як ми це робимо, але воно не задокументоване.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно.

7.4.12 P-12 Процес роботи з джерелами інформації

Опис: Описує, як CSIRT опрацьовує різноманітні джерела інформації, доступні команді (параметр T-2). Для кожного CSIRT є обов'язковим відстежувати й оцінювати відповідні джерела інформації. Окрім публічних вебсторінок, це можуть бути соціальні мережі, списки розсилки, постачальники засобів безпеки, бази даних вразливостей або сайти з експлойтами чи нові сповіщення від постачальників сервісів з інформаційної безпеки. Незалежно від кількості та типів джерел інформації, які відстежуються, CSIRT має розробити процес, який забезпечує послідовний підхід до цього з належним рівнем перевірки та контролю якості. Необхідно унеможливити ситуацію, коли CSIRT діє на підставі хибних або фальсифікованих даних, оскільки це ставить під загрозу репутацію команди. Цей процес також має описувати життєвий цикл джерел: від включення в перелік джерел інформації CSIRT (параметр T-2) до виключення звіти через зниження якості (або зникнення актуального контенту).

СТД-04-001-2026-B

Чи має ваша команда процес роботи з джерелами інформації (параметр T-2)?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є розуміння, як ми це робимо, але воно не задокументоване.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно.

7.4.13 P-13 Процес зовнішньої комунікації та інформування

Опис: *Оскільки CSIRT пропонує сервіси клієнтам, він має проводити інформаційно-роз'яснювальну роботу серед наявних та потенційних клієнтів і зацікавлених сторін. Таким чином команда просуває не лише себе, а й рекомендовані нею найкращі практики та процеси. Хоча підвищення обізнаності може розглядатися як елемент інформаційно-роз'яснювальної роботи, його часто вважають окремим сервісом CSIRT, оскільки воно є складовою запобігання кіберінцидентам і, відповідно, основної діяльності команди. Водночас украї важливо забезпечити, щоб користувачі добре знали про існування CSIRT та перелік його сервісів. "Популяризація" команди в такий спосіб є частиною процесу інформаційно-роз'яснювальної роботи. Не менш важливо, щоб цей процес передбачав двосторонній канал комунікації: клієнти також повинні мати можливість надавати команді свої відгуки "знизу вгору" (які не слід плутати з відгуками, описаними у параметрі P-8, що здійснюється "згори вниз"). Процес інформаційно-роз'яснювальної роботи має охоплювати всі форми діяльності, що покращують видимість і репутацію CSIRT: вебсторінки, інформаційні розсилки, вебінари, аналітичні матеріали, конференції тощо. Для будь-якого національного CSIRT це передбачає також налагодження зв'язку (знову ж таки двостороннього) з секторами критичної інфраструктури та відповідними центрами з обміну та аналізу інформації (Information Sharing and Analysis Centre, або ISAC).*

Пояснення: Відгуки від клієнтів (знизу вгору) слід відрізняти від відгуків, згаданих у процесі P-8, які надходять від органу управління вищого рівня (згори вниз).

Чи має ваша команда процес зовнішньої комунікації та інформування?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

СТД-04-001-2026-B

«1» – У нас є розуміння, як ми це робимо, але воно не задокументоване.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно.

7.4.14 P-14 Процес звітування перед органом управління вищого рівня

Опис: *Управляючи кіберінцидентами для своїх клієнтів, CSIRT отримує критично важливу інформацію, яка в інший спосіб залишається недоступною для зацікавлених сторін, осіб, що формують політику, і навіть фахівців з інформаційної безпеки чи захисту даних. У рамках ситуаційної обізнаності (обсяг якої визначається цілями та завданнями конкретного CSIRT) важливо, щоб висновки на базі отриманого досвіду належним чином передавалися та ескалювалися. Процес звітування перед органами управління вищого рівня має забезпечувати актуальні звіти й пояснення контексту з метою підвищення ефективності запобігання та усунення подібних кіберінцидентів, атак і ризиків у майбутньому. Це звітування включає статистику та графіки, що базуються на категоріях та типах кіберінцидентів (параметр O-8) та кількості кіберінцидентів, витрачених ресурсів, рівнів фінансування тощо. Надання статистики для клієнтів або широкого загалу охоплюється параметром P-15.*

Пояснення: Якщо CSIRT функціонує у складі головної/материнської організації, цей процес стосується звітів, що надсилаються керівництву головної/материнської організації та/або CISO, CSO чи CIO. У разі національної команди йдеться про звітування перед відповідним керівником органу державної влади, а також, можливо, перед урядом.

Чи звітує ваш CSIRT перед органами управління вищого рівня відповідно до встановленого процесу?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є розуміння, як ми це робимо, але воно не задокументоване.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно.

7.4.15 P-15 Процес звітування перед клієнтами

Опис: Якщо параметр P-14 стосується звітування перед органами управління вищого рівня, то P-15 – це звітування перед клієнтами або навіть перед широким загалом (як це роблять, наприклад, національні команди у щорічних звітах). Таке звітування може включати статистику та графіки. У такому разі, як і у випадку з параметром P-14, доцільно будувати його на основі категорій та типів кіберінцидентів (параметр O-8) шляхом (напів)автоматичного експортування внутрішньої класифікації та числових даних у потрібні зовнішні формати. Слід зазначити, що можуть існувати й інші схеми звітування, наприклад обов'язкова звітність відповідно до національного законодавства, що ґрунтується на інших засадах.

Пояснення: Такий вид звітування може варіюватися від стислого та узагальненого до детального із включенням статистики та графіків, що базуються на категоріях та типах кіберінцидентів (параметр O-8). Іноді набуває форми щорічних звітів. Якщо команда здійснює лише внутрішнє звітування, варто вибрати варіант «Не застосовується», і цей параметр буде виключено з оцінювання.

Чи здійснює ваша команда звітування перед клієнтами або широким загалом, і чи існує для цього відповідний процес?

Значення:

Не застосовується – Ми обрали лише внутрішнє звітування, без звітування перед клієнтами.

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є розуміння, як ми це робимо, але воно не задокументоване.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно.

7.4.16 P-16 Процес проведення внутрішніх нарад

Опис: Регулярні наради, як правило щотижневі або навіть щоденні, можуть суттєво покращити ефективність роботи і якість внутрішньої комунікації CSIRT. Оскільки потреби команд різняться, а організаційні структури бувають різноманітними (зокрема, коли працівники розосереджені в декількох локаціях), фіксованого розкладу нарад не вимагається.

СТД-04-001-2026-B

Проте кожна команда має визначити оптимальну кількість нарад, їхній предмет і формат проведення: офлайн, онлайн або змішаний. Як мінімум, процес проведення нарад має забезпечувати фіксацію та доведення до відома всіх причетних як визначених завдань, так і висновків на базі аналізу минулого досвіду. Оскільки привід для скасування командних нарад знайти нескладно, процес повинен передбачати обов'язковий мінімум зустрічей, які фактично відбуваються за участі необхідного кола осіб. Запровадження гібридного формату значно спрощує досягнення цієї мети.

Пояснення: Може включати наради, які проводяться у змішаному форматі та онлайн.

Чи має ваша команда визначений процес проведення внутрішніх нарад?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є розуміння, як ми це робимо, але воно не задокументоване.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно

7.4.17 P-17 Процес взаємодії з іншими командами реагування

Опис: Для побудови довірчих відносин з іншими командами, своєчасного отримання якісної інформації та покращення швидкості й якості комунікації важливо брати участь у відповідних спільнотах. Також деякі команди можуть діяти в умовах ієрархічної підпорядкованості: наприклад, CSIRT комерційної організації може звітувати перед координуючим CSIRT на корпоративному рівні, а державні команди нижчого рівня – перед національним CSIRT. У будь-якому випадку такі партнерські відносини і відповідні процеси мають бути визначені з обох боків. За наявності ієрархічної структури її наслідки необхідно чітко задокументувати. Якщо ж партнери є радше командами одного рівня в неієрархічному контексті (наприклад, члени FIRST або регіональних спільнот CSIRT), слід усе одно визначити, як саме ці партнери взаємодіють між собою та які очікування й процеси при цьому діють. Також необхідно враховувати, що партнерами можуть бути не лише інші CSIRT, а й команди безпеки інших типів: SOC, PSIRT, ISAC тощо.

Мінімальна вимога: Процес має визначати перелік партнерів і забезпечувати наявність двосторонньої довірчої комунікації з кожним із них.

СТД-04-001-2026-В

Пояснення: Партнерська команда – це команда безпеки, з якою існують особливі відносини, засновані на спільному членстві в певній спільноті чи об'єднанні або на угодах типу меморандуму про співпрацю.

Чи визначила ваша команда процес взаємодії з іншими командами реагування?

Значення:

«0» – Ми ніколи по-справжньому не обговорювали цього.

«1» – У нас є розуміння, як ми це робимо, але воно не задокументоване.

«2» – У нас немає формалізованого письмового процесу, тому ми сформулювали його самостійно для власних потреб. Наше керівництво офіційно його не затверджувало.

«3» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди.

«4» – У нас є формалізований письмовий процес, затверджений керівництвом нашої команди. Під час періодичної перевірки нашої команди оцінюється, чи цей процес працює відповідно.

8 ПОРЯДОК ПРОВЕДЕННЯ ОЦІНЮВАННЯ ЗРІЛОСТІ CSIRT

Оцінювання зрілості CSIRT полягає у визначенні рівня (від 0 до 4) для кожного параметра відповідно до шкали, наведеної в таблиці 1 розділу 6. Для параметрів Т-8 та Р-4 допускається значення «Не застосовується» (N/A), у такому разі зазначені параметри виключаються з оцінювання. Для параметра Р-15 значення «Не застосовується» (N/A) допускається виключно за умови, що регламентом діяльності команди визначено лише внутрішнє звітування, без інформування зовнішніх клієнтів.

Оцінювання проводиться у формі самооцінювання або незалежного аудиту. Ці форми можуть використовуватися як окремо, так і в поєднанні.

8.1 Самооцінювання

8.1.1 Самооцінювання проводиться командою CSIRT самостійно. Рекомендованим інструментом для проведення самооцінювання є анкета, наведена в додатку А (яка відповідає онлайн-інструменту <http://sim3-check.opencsirt.org>).

СТД-04-001-2026-B

8.1.2 Порядок проведення самооцінювання:

а) для кожного параметра обирається значення від 0 до 4 відповідно до шкали, визначеної в розділі 6;

б) при визначенні рівня параметра члени команди пояснюють, як вони розуміють відповідний аспект діяльності CSIRT, у разі розбіжностей у поясненнях між членами команди це є сигналом для письмового фіксування змісту параметра, що підвищує узгодженість у роботі команди;

в) за результатами самооцінювання формується профіль зрілості CSIRT – зведені значення всіх параметрів;

г) виявлені прогалини між поточними значеннями та цільовими, які команда визначила як бажані для себе, є основою для планування розвитку спроможностей CSIRT;

д) результати самооцінювання фіксуються у звіті відповідно до розділу 9.

8.1.3 Самооцінювання не є достатньою підставою для присвоєння параметру рівня 4. Для рівня 4 необхідна активна участь органу управління вищого рівня відповідно до підрозділу 8.2.

8.2 Незалежний аудит

8.2.1 Незалежний аудит – це будь-який вид аудиту, що проводиться не самою командою, а здійснюється за рішенням органу управління вищого рівня (вищого за керівника CSIRT). Такий аудит є обов'язковою умовою для присвоєння параметру рівня 4.

8.2.2 Особа, яка проводить незалежний аудит, має відповідати таким вимогам:

а) незалежність – не входить до складу команди, що оцінюється, та не брала участі в розробленні документів, які перевіряються;

б) компетентність – володіє знанням цього стандарту та моделі SIM3, має практичний досвід у сфері реагування на кіберінциденти;

СТД-04-001-2026-B

в) призначення – документально призначена рішенням органу управління вищого рівня.

8.2.3 Незалежний аудит може проводитись у таких формах:

а) внутрішній аудит – проводиться CISO, CSO, CIO або аудиторським підрозділом організації за рішенням органу управління вищого рівня;

б) зовнішній аудит – проводиться зовнішнім підрядником за рішенням органу управління вищого рівня;

в) аудит у рамках участі в спільнотах CSIRT – наприклад, у рамках сертифікації спільноти команд TF-CSIRT/Trusted Introducer на основі стандарту SIM3.

8.2.4 Щоб параметр міг бути оцінений на рівні 4, незалежний аудит має відповідати таким вимогам:

а) аудит здійснюється регулярно – за найкращою практикою не рідше одного разу на два роки, зазвичай щорічно;

б) аудит є активним – окрім безпосередньої перевірки та звітування, передбачено механізм зворотного зв'язку з керівником команди (і командою) за підсумками аудиту;

в) результати аудиту документально підтверджують, що відповідний параметр перевірявся органом управління вищого рівня і що команда отримала зворотний зв'язок.

8.2.5 Докази/документи відповідності рівню 4 не завжди є очевидними. Найбільш однозначними є такі два випадки:

а) якщо предмет певного параметра формально та недвозначно закріплений у національному законодавстві у сфері кібербезпеки, такий параметр отримує рівень 4, оскільки система законодавства та механізми стримувань і противаг є достатніми підставами, при цьому команда все одно зобов'язана впровадити відповідні вимоги законодавства всередині через власну документацію та інформаційні системи;

СТД-04-001-2026-B

б) якщо в організаційно-правових засадах діяльності команди (параметр О-10) наявний окремий розділ, присвячений оцінюванням/аудитам команди (параметр Р-8), що охоплює як внутрішні оцінювання, так і аудит з боку вищого рівня управління або аудиторського підрозділу.

8.2.6 За відсутності явних доказів/документів рівня 4 допускається використання ретроспективного аналізу звітів про раніше проведені аудити, якщо вони містять відомості про перевірку відповідних параметрів у спосіб, що відповідає вимогам рівня 4 (включаючи наявність зворотного зв'язку з командою).

8.3 Збір документальних підтверджень

8.3.1 Для кожного параметра, якому присвоюється певне значення, мають бути наявні документальні підтвердження. Вид документальних підтверджень залежить від рівня:

а) рівень 1 – задокументовані результати інтерв'ю, опитувальні листи або протоколи опитування персоналу команди щодо поточної усної практики реалізації процесів;

б) рівень 2 – внутрішні записи, записи у внутрішніх базах знань (вікі-системах) команди, неформальні документи, що підтверджують існування алгоритму дій, не затвердженого розпорядчими документами;

в) рівень 3 – документи: накази, положення, процедури, інструкції, технологічні картки процесів, офіційно затверджені керівником команди або керівництвом вищого рівня управління, а також записи, що підтверджують фактичне застосування процесу (записи в системі обліку кіберінцидентів, журнали, протоколи);

г) рівень 4 – документи, визначені для рівня 3, доповнені офіційними звітами про результати аудитів, актами перевірок, протоколами керівних нарад, що підтверджують взаємодію з органом управління вищого рівня та наявність механізму зворотного зв'язку з командою.

СТД-04-001-2026-B

8.3.2 Рекомендується, щоб CSIRT систематично зберігав документальні підтвердження у зручній для перегляду формі, наприклад у базі знань (вікі-системі) або системі управління документами для забезпечення оперативного доступу під час процедур оцінювання. Це спрощує як самооцінювання, так і проведення незалежного аудиту.

9 ВИМОГИ ДО ЗВІТУ ПРО ОЦІНЮВАННЯ

9.1 Звіт про оцінювання є результатом як самооцінювання, так і незалежного аудиту. Він забезпечує контроль якості в усіх критичних і чутливих аспектах діяльності CSIRT та є основою для вдосконалення.

9.2 Звіт про оцінювання складається в довільній формі та повинен:

а) загальні відомості: найменування CSIRT, дату проведення оцінювання, форму оцінювання (самооцінювання або незалежний аудит), відомості про осіб, що проводили оцінювання;

б) значення кожного параметра (від 0 до 4 або «Не застосовується»), визначені за результатами оцінювання;

в) перелік документальних підтверджень, що були надані або перевірені для кожного параметра;

г) профіль зрілості – зведені значення всіх параметрів у розрізі категорій О, Н, Т, Р;

д) виявлені невідповідності між заявленими значеннями параметрів та наданими документальними підтвердженнями;

е) зворотний зв'язок для команди CSIRT та її керівника – неупереджений та об'єктивний, з фокусом на вдосконаленні та прогресі, а не на помилках і невідповідностях, з орієнтацією на місію організації та її клієнтів;

є) рекомендації щодо пріоритетних напрямів розвитку спроможностей.

9.3 Результати оцінювання мають бути корисними не лише для самої команди, а й для відповідних рівнів управління вище за CSIRT. Це особливо важливо для тих параметрів, за якими команда прагне досягти рівня 4: для них

СТД-04-001-2026-В

необхідна регулярна й активна форма перевірки з боку вищого керівництва з обов'язковим зворотним зв'язком.

9.4 Для параметрів, яким присвоюється рівень 4, у звіті має бути задокументовано:

а) що аудит або перевірка відповідного параметра проводилися за рішенням органу управління вищого рівня (вищого за керівника CSIRT);

б) що за підсумками аудиту/перевірки команда отримала зворотний зв'язок.

9.5 У разі незалежного аудиту звіт додатково має містити:

а) відомості про аудитора та підтвердження відсутності конфлікту інтересів із командою, що оцінюється;

б) підтвердження того, що аудит проводився за рішенням органу управління вищого рівня.

9.6 Звіт є основою для підготовки рекомендацій щодо вдосконалення та планування наступного оцінювання. Рекомендована періодичність оцінювання – не рідше одного разу на два роки, зазвичай – щорічно.

АНКЕТА ОЦІНЮВАННЯ ПАРАМЕТРІВ

АНКЕТА ОЦІНЮВАННЯ ПАРАМЕТРІВ

Таблиця А.1 – Анкета оцінювання параметрів

Код	Назва параметра / Контрольне запитання	N/A	0	1	2	3	4	Документальні підтвердження
1	2	3	4	5	6	7	8	9
О – Організація								
O-1	Призначення <i>Чи визначено призначення вашого CSIRT?</i>	—	☐	☐	☐	☐	☐	
O-2	Сфера відповідальності <i>Чи має ваш CSIRT визначену сферу відповідальності?</i>	—	☐	☐	☐	☐	☐	
O-3	Повноваження <i>Які повноваження має ваша команда?</i>	—	☐	☐	☐	☐	☐	
O-4	Обов'язки <i>Які обов'язки має ваша команда?</i>	—	☐	☐	☐	☐	☐	
O-5	Опис сервісів <i>Чи має ваша команда опис сервісів?</i>	—	☐	☐	☐	☐	☐	
O-6	Політика взаємодії із медіа <i>Чи має ваша команда політику взаємодії з медіа?</i>	—	☐	☐	☐	☐	☐	
O-7	Рівні надання сервісів <i>Чи має ваш CSIRT опис рівнів надання сервісів?</i>	—	☐	☐	☐	☐	☐	
O-8	Класифікація кіберінцидентів <i>Чи має ваша команда схему класифікації кіберінцидентів?</i>	—	☐	☐	☐	☐	☐	
O-9	Взаємодія з іншими командами реагування <i>Чи взаємодіє ваша команда з іншими командами або бере участь у спільнотах команд на пряму або опосередковано через CSIRT вищого рівня?</i>	—	☐	☐	☐	☐	☐	
O-10	Організаційно-правові засади діяльності <i>Чи визначено організаційно-правові засади діяльності вашого CSIRT?</i>	—	☐	☐	☐	☐	☐	
O-11	Політика безпеки <i>Чи дотримується ваш CSIRT визначеної політики або політик безпеки (включно з аспектами BCM) – власної та/або від батьківської організації?</i>	—	☐	☐	☐	☐	☐	

1	2	3	4	5	6	7	8	9
Н – Персонал								
N-1	Правила професійної поведінки та етики <i>Чи впроваджений такий кодекс поведінки/професійної етики у вашій команді?</i>	—	☐	☐	☐	☐	☐	
N-2	Операційна стійкість персоналу <i>Чи дотримується ваша команда вимог до операційної стійкості персоналу?</i>	—	☐	☐	☐	☐	☐	
N-3	Опис професійних компетенцій <i>Чи описала ваша команда необхідні професійні компетенції?</i>	—	☐	☐	☐	☐	☐	
N-4	Професійний розвиток персоналу <i>Чи має ваша команда політику професійного розвитку персоналу?</i>	—	☐	☐	☐	☐	☐	
N-5	Розвиток технічних навичок <i>Чи має ваша команда політику розвитку технічних навичок?</i>	—	☐	☐	☐	☐	☐	
N-6	Розвиток навичок з комунікації та взаємодії <i>Чи має ваша команда політику розвитку навичок з комунікації та взаємодії?</i>	—	☐	☐	☐	☐	☐	
N-7	Зовнішня взаємодія та професійні зв'язки <i>Чи має ваша команда політику щодо зовнішньої взаємодії та професійних зв'язків?</i>	—	☐	☐	☐	☐	☐	
Т – Інструменти								
T-1	ІТ-активи та їх конфігурації <i>Чи має ваш CSIRT перелік ІТ-активів або має доступ до переліку ІТ-активів та конфігурацій клієнтів?</i>	—	☐	☐	☐	☐	☐	
T-2	Перелік джерел інформації <i>Чи має ваша команда перелік джерел інформації?</i>	—	☐	☐	☐	☐	☐	
T-3	Об'єднані системи обміну повідомленнями <i>Чи використовує ваш CSIRT об'єднані системи обміну повідомленнями?</i>	—	☐	☐	☐	☐	☐	
T-4	Система реєстрації та відстеження кіберінцидентів <i>Чи використовує ваша команда систему реєстрації та відстеження кіберінцидентів?</i>	—	☐	☐	☐	☐	☐	
T-5	Стійкість послуг голосової електронної комунікації <i>Які засоби голосової електронної комунікації є у вашої команди й чи достатньо вони стійкі для ваших потреб?</i>	—	☐	☐	☐	☐	☐	

1	2	3	4	5	6	7	8	9
T-6	Стійкість систем обміну повідомленнями <i>Які системи обміну повідомленнями використовує ваша команда й чи достатньо вони стійкі для ваших потреб?</i>	—	☐	☐	☐	☐	☐	
T-7	Стійкість доступу до мережі Інтернет <i>Якими засобами доступу до мережі Інтернет користується ваша команда й чи достатньо вони стійкі для ваших потреб?</i>	—	☐	☐	☐	☐	☐	
T-8	Інструменти для запобігання кіберінцидентам <i>Чи має ваша команда визначений набір інструментів для запобігання кіберінцидентам?</i>	☐	☐	☐	☐	☐	☐	
T-9	Інструменти для виявлення кіберінцидентів <i>Чи має ваша команда визначений набір інструментів для виявлення кіберінцидентів?</i>	—	☐	☐	☐	☐	☐	
T-10	Інструменти для реагування на кіберінциденти та усунення їх наслідків <i>Чи має ваша команда визначений набір інструментів для реагування на кіберінциденти та усунення їх наслідків?</i>	—	☐	☐	☐	☐	☐	
Р – Процеси								
P-1	Процес ескалації до вищого рівня управління <i>Чи спроможна ваша команда здійснювати ескалацію до вищого рівня управління?</i>	—	☐	☐	☐	☐	☐	
P-2	Процес комунікації з медіа <i>Чи має ваша команда процес комунікації з медіа?</i>	—	☐	☐	☐	☐	☐	
P-3	Процес взаємодії з юридичним підрозділом <i>Чи має ваша команда процес взаємодії з юридичним підрозділом?</i>	—	☐	☐	☐	☐	☐	
P-4	Процес запобігання кіберінцидентам <i>Чи має ваша команда процес запобігання кіберінцидентам?</i>	☐	☐	☐	☐	☐	☐	
P-5	Процес виявлення кіберінцидентів <i>Чи має ваша команда процес виявлення кіберінцидентів? (Якщо у вас є об'єднаний процес для параметрів P-5 і P-6, оберіть однаковий рівень для обох.)</i>	—	☐	☐	☐	☐	☐	

1	2	3	4	5	6	7	8	9
P-6	Процес реагування на кіберінциденти та усунення їх наслідків <i>Чи має ваша команда процес реагування на кіберінциденти та усунення їх наслідків? (Якщо у вас є об'єднаний процес для параметрів P-5 і P-6, оберіть однаковий рівень для обох.)</i>	—	☐	☐	☐	☐	☐	
P-7	Процеси реагування на різні категорії та типи кіберінцидентів і усунення їх наслідків <i>Чи описала ваша команда процеси реагування на різні категорії та типи кіберінцидентів і усунення їх наслідків на додачу до узагальненого процесу реагування?</i>	—	☐	☐	☐	☐	☐	
P-8	Процес аудиту та отримання відгуку <i>Чи визначено процес аудиту та отримання відгуку у вашому CSIRT?</i>	—	☐	☐	☐	☐	☐	
P-9	Процес екстреної комунікації <i>Чи має ваш CSIRT процес екстреної комунікації?</i>	—	☐	☐	☐	☐	☐	
P-10	Взаємодія через публічні вебресурси <i>Чи має ваш CSIRT процес, який визначає взаємодію через публічні вебресурси?</i>	—	☐	☐	☐	☐	☐	
P-11	Процес безпечного поводження з інформацією <i>Чи має ваша команда процес безпечного поводження з інформацією?</i>	—	☐	☐	☐	☐	☐	
P-12	Процес роботи з джерелами інформації <i>Чи має ваша команда процес роботи з джерелами інформації (параметр T-2)?</i>	—	☐	☐	☐	☐	☐	
P-13	Процес зовнішньої комунікації та інформування <i>Чи має ваша команда процес зовнішньої комунікації та інформування?</i>	—	☐	☐	☐	☐	☐	
P-14	Процес звітування перед органом управління вищого рівня <i>Чи звітує ваш CSIRT перед органами управління вищого рівня відповідно до встановленого процесу?</i>	—	☐	☐	☐	☐	☐	
P-15	Процес звітування перед клієнтами <i>Чи здійснює ваша команда звітування перед клієнтами або широким загалом, і чи існує для цього відповідний процес?</i>	☐	☐	☐	☐	☐	☐	

1	2	3	4	5	6	7	8	9
P-16	Процес проведення внутрішніх нарад <i>Чи має ваша команда визначений процес проведення внутрішніх нарад?</i>	—	☐	☐	☐	☐	☐	
P-17	Процес взаємодії з іншими командами реагування <i>Чи визначила ваша команда процес взаємодії з іншими командами реагування?</i>	—	☐	☐	☐	☐	☐	

БІБЛІОГРАФІЯ

- 1 Закон України «Про захист інформації в інформаційно-комунікаційних системах»;
- 2 Закон України «Про основні засади забезпечення кібербезпеки України»;
- 3 Постанова Кабінету Міністрів України від 05.11.2025 № 1424 «Про затвердження Порядку розроблення, прийняття, внесення змін, скасування, відновлення дії, оприлюднення та запровадження стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам»;
- 4 Постанова Кабінету Міністрів України від 13.11.2025 № 1471 «Порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози»;
- 5 Постанова Кабінету Міністрів України від 26.11.2025 № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози»;
- 6 ДСТУ ISO/IEC 27001:2023 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»;
- 7 Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS2), 2022;
- 8 ENISA CSIRT Maturity Framework. European Union Agency for Cybersecurity, 2020;
- 9 Security Incident Management Maturity Model (SIM3 v2), 2023;
- 10 RFC 2350 «Expectations for Computer Security Incident Response». IETF, 1998;
- 11 FIRST CSIRT Services Framework Version 2.1. Forum of Incident Response and Security Teams, 2019.

СТД-04-001-2026-B

Коди згідно з КСД 001: 04.01, 04.05;

НК 004: 35.030

Ключові слова: команда реагування на кіберінциденти, кібератаки, кіберзагрози (Computer Security Incident Response Team; CSIRT), модель зрілості, реагування на кіберінциденти, кібератаки, кіберзагрози, організаційно-технічна спроможність, параметр, рівень зрілості, оцінювання спроможностей, кіберзахист.