Державна служба
спеціального зв'язку
та захисту інформації
України

НАСТАНОВА З ОБРОБКИ КІБЕРІНЦИДЕНТІВ: ПРІОРИТЕТНІСТЬ З УРАХУВАННЯМ ВИЗНАЧЕНИХ РІВНІВ ЇХ КРИТИЧНОСТІ

Київ 2026

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІКС — інформаційно-комунікаційна система

КА — кібератака

КІ — кіберінцидент

CERT — (англ. Computer Emergency Response Team) група (команда) реагування на надзвичайні події в кіберпросторі

CERT-UA — (англ. Computer Emergency Response Team Ukraine) національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (національний CSIRT)

CISA — (англ. Cybersecurity And Infrastructure Security Agency) агентство з кібербезпеки та захисту інфраструктури США

CSIRT — (англ. Computer Security Incident Response Team) комп'ютерна група реагування на надзвичайні ситуації

CVE — (англ. Common Vulnerabilities and Exposures) база даних загальновідомих вразливостей інформаційної безпеки

CVSS — (англ. Common Vulnerability Scoring System) загальна система оцінки вразливостей

IEC — (англ. International Electrotechnical Commission) Міжнародна електротехнічна комісія

IS — (англ. International Organization for Standardization) Міжнародна організація зі стандартизації

NIST — (англ. National Institute of Standards and Tech№logy) Національний інститут стандартів та технологій США

NVD — (англ. National Vulnerability Database) Національна база даних про вразливість

TLP — (англ. Traffic Light Protocol) кольоровий протокол класифікації повідомлень

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.

Настанова з обробки кіберінцидентів: пріоритетність з урахуванням визначених рівнів їх критичності (далі — Настанова) розроблено на виконання пункту 72 рішення Ради національної безпеки і оборони України від 30 грудня 2021 року, введеного в дію Указом Президента України від 01 лютого 2022 року № 37/2022 «Про План реалізації Стратегії кібербезпеки України», Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» та призначено для використання під час визначення пріоритетності обробки кіберінцидентів/кібератак з метою зменшення потенційних наслідків кібератаки для організації і країни в цілому.

2.

Настанову розроблено відповідно до Законів України «Про основні засади забезпечення кібербезпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про критичну інфраструктуру», Стратегії кібербезпеки України, затвердженої Указом Президента України від 01 лютого 2022 року № 37, Загальних вимог з кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, постанови Кабінету Міністрів України від 23 грудня 2020 р. № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки», Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози», постанови Кабінету Міністрів України від 16 травня 2023 року № 497 «Про затвердження Порядку

пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж».

3.

Настанову розроблено з урахуванням положень:

- посібника (сценаріїв) з реагування на інциденти та вразливості у сфері кібербезпеки: Оперативні процедури планування та проведення заходів із реагування на інциденти і вразливості у сфері кібербезпеки в інформаційних системах федеральних органів виконавчої влади (Cybersecurity Incident & Vulnerability Response Playbooks: Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems), виданого Агентством з кібербезпеки та захисту інфраструктури (CISA);

- посібника федеральних вказівок щодо розкриття вразливостей (NIST SP 800-216: Recommendations for Federal Vulnerability Disclosure Guidelines), виданого Національним інститутом стандартів та технології Сполучених Штатів Америки (NIST);

- керівництва із планування керування виправленнями на підприємстві: профілактичне технічне обслуговування (NIST SP 800-40 Rev.4: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology), виданого Національним інститутом стандартів та технології Сполучених Штатів Америки (NIST);

- посібника із заходів безпеки та приватності для інформаційних систем і організацій (NIST SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations), виданого Національним інститутом стандартів та технології Сполучених Штатів Америки (NIST);

- посібника з опрацювання інцидентів комп'ютерної безпеки (NIST SP 800-61 Rev. 2 Computer Security Incident

Handling Guide), виданого Національним інститутом стандартів та технології Сполучених Штатів Америки (NIST);

- посібника із практики управління кіберризиками ланцюга поставок для систем і організацій (NIST SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations), виданого Національним інститутом стандартів та технології Сполучених Штатів Америки (NIST);
- рекомендації із управління безпекою інформаційних обмінів (NIST SP 800-47 Rev. 1 Managing the Security of Information Exchanges), виданого Національним інститутом стандартів та технології Сполучених Штатів Америки (NIST);
- національної бази даних вразливостей США (NIST national vulnerability database);
- ДСТУ EN ISO/IEC 29147:2022 Інформаційні технології. Методи захисту. Розкриття вразливостей (EN ISO/IEC 29147:2020, IDT; ISO/IEC 29147:2018, IDT);
- ДСТУ EN ISO/IEC 30111:2022 Інформаційні технології. Методи захисту. Процеси оброблення вразливостей (EN ISO/IEC 30111:2020, IDT; ISO/IEC 30111:2019, IDT);
- ДСТУ EN ISO/IEC 27002:2022 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (EN ISO/IEC 27002:2017, IDT; ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015, IDT);
- ДСТУ ISO/IEC 27035-1:2023 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами (ISO/IEC 27035-1:2023-2, IDT);
- ДСТУ ISO/IEC 27035-2:2022 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2022, IDT);
- НД ТЗІ 3.6-006-21 Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем;

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

4.

Настанова не є нормативно-правовим актом, має інформаційний та рекомендаційний характер, не встановлює правових норм і є добровільною для використання. Настанова може бути використана усіма суб'єктами забезпечення кібербезпеки.

5.

У цій Настанові терміни вживаються в такому значенні:

- **вразливість** — властивість системи, через використання якої створюється загроза для її безпеки, порушується сталий, надійний та штатний режим функціонування системи, здійснюється несанкціоноване втручання в її роботу, створюється загроза для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів;

- **загальний список кіберінцидентів** — таблиця кіберінцидентів, які надійшли на обробку;

- **звіт про вразливість системи за результатами пошуку її потенційної вразливості (далі — звіт)** — інформація про вразливість системи, підготовлена дослідником за результатами проведення ним пошуку її потенційної вразливості;

- **зміни до системи** — зміни, внесені до інформаційної (автоматизованої), електронної комунікаційної, інформаційно-комунікаційної системи, електронної комунікаційної мережі (далі — система) для розв'язання проблеми вразливості системи, запобігання

використанню вразливості, мінімізації можливих наслідків її використання;

- **перевірка звіту про вразливість** — перевірка достовірності інформації, зазначеної у звіті про вразливість системи, та оцінка ризику від експлуатації вразливості;

- **пріоритизація кіберінцидентів** — обробка кіберінцидентів та додавання їх у чергу обробки кіберінцидентів залежно від рівня критичності;

- **черга обробки кіберінцидентів** — таблиця кіберінцидентів, які потребують обробки і відсортовані в порядку зменшення рівня критичності.

Інші терміни вживаються у значеннях, наведених в Цивільному процесуальному кодексі України, Законах України «Про основні засади забезпечення кібербезпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про критичну інфраструктуру», «Про електронні комунікації», «Про захист інформації в інформаційно-комунікаційних системах», Загальних вимогах з кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози», Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженому постановою Кабінету Міністрів України від 16 травня 2023 року № 497.

6.

Інформаційний обмін, координація та спільні дії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки проводяться відповідно до Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою

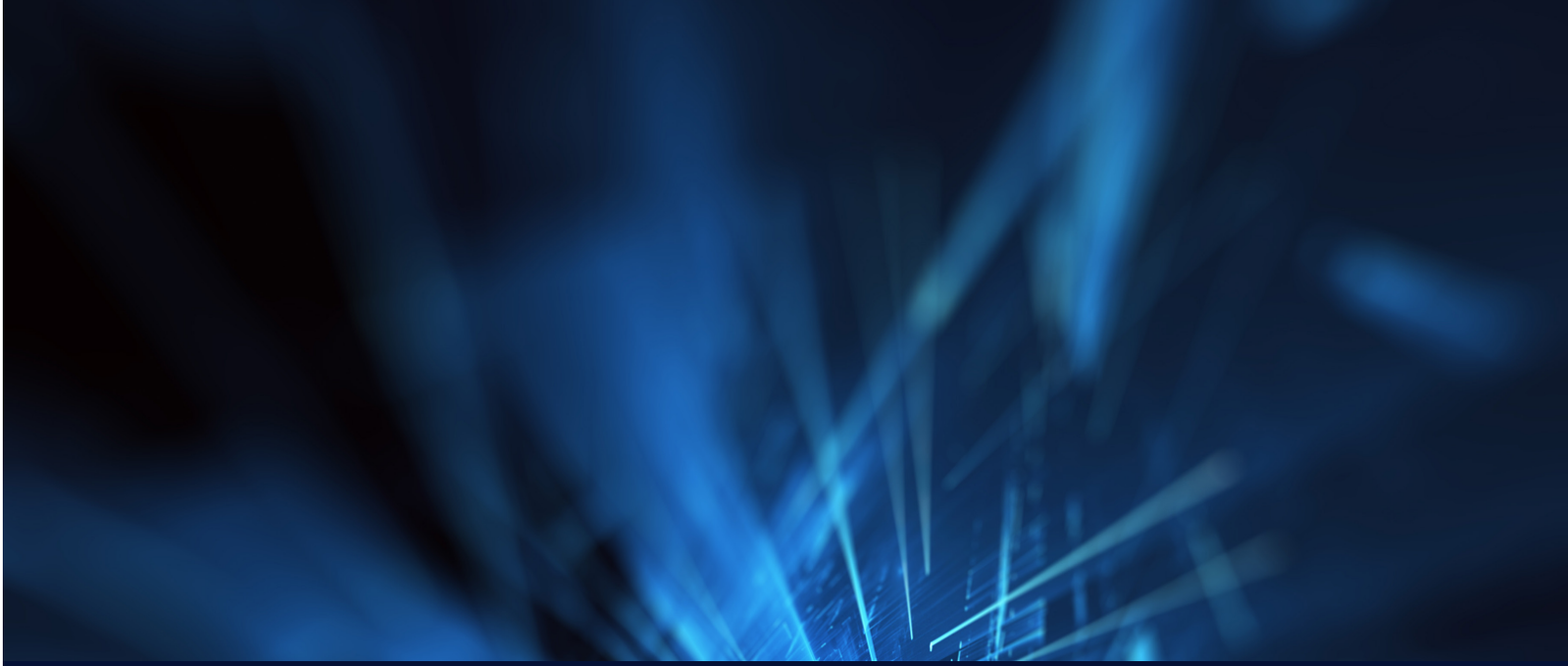
Кабінету Міністрів України від 26 листопада 2025 року № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» (далі — Національний план). Під час обміну інформацією про кіберінциденти/кібератаки суб'єкти забезпечення кібербезпеки керуються загальними правилами обміну інформацією про кіберінциденти (Протокол TLP) та переліком категорій і типів кіберінцидентів.

7.

Настанова містить послідовність заходів щодо пріоритетності обробки кіберінцидентів/кібератак з урахуванням визначених рівнів критичності, які проводяться на етапі виявлення та аналізу.

Процес пріоритизації кіберінциденту/кібератаки (за умови, якщо мають місце два та більше кіберінцидентів/кібератак) передбачає:

- визначення функціональних наслідків кіберінциденту/кібератаки;
- визначення інформаційних наслідків кіберінциденту/кібератаки;
- визначення впливу на відновлення після кіберінциденту/кібератаки;
- оцінка впливу кожного кіберінциденту/кібератаки та надання пріоритету реагування для кожного кіберінциденту/кібератаки.



II. ПРІОРИТИЗАЦІЯ КІБЕРІНЦИДЕНТУ / КІБЕРАТАКИ

II. ПРІОРИТИЗАЦІЯ КІБЕРІНЦИДЕНТУ / КІБЕРАТАКИ

1.

Для ефективної пріоритизації кіберінцидентів вхідна інформація повинна містити дані про запропонований рівень критичності, рівень значущості організації в економічному і соціальному середовищі України, деталізовану інформацію про спосіб здійснення кібератаки та потенційні наслідки кібератаки для організації і країни в цілому.

2.

Такий набір даних отримуємо завдяки поєднанню інформації з повідомлення про кіберінцидент, кібератаку, кіберзагрозу та метрик Загальної системи оцінки вразливостей версії 3.1 (CVSS, Common Vulnerability Scoring System) американського Національного інституту стандартів та технологій (NIST, National Institute of Standards and Technology).

3.

Алгоритм визначення пріоритетності обробки кіберінцидентів/кібератак з урахуванням визначених рівнів критичності наводиться в додатку 1. Перелік значень за показниками Рекомендацій та за метриками CVSS наводиться у додатках 2 та 3 відповідно.

4.

Для реєстрації і обробки кіберінцидентів створюється два списки:

- загальний список кіберінцидентів — таблиця кіберінцидентів, які надійшли на обробку, незалежно від того, чи потрібна обробка, чи відмовлено в обробці. Використовується для зберігання всього масиву інформації про кіберінциденти, який надійшов на обробку та створення звітності із діяльності з обробки кіберінцидентів;
- список черги обробки кіберінцидентів — таблиця кіберінцидентів, які потребують обробки і відсортовані в порядку зменшення рівня критичності. Використовується командами реагування на кіберінциденти, кібератаки, кіберзагрози для визначення порядку обробки кіберінцидентів.

5.

Список черги обробки кіберінцидентів є підмножиною кіберінцидентів, доданих до загального списку кіберінцидентів. Розділення необхідне, оскільки додавання всіх кіберінцидентів в єдину чергу для обробки створюватиме "сміттєві записи (шум)", які не впливатимуть на черговість обробки інцидентів, що цього потребують, проте можуть відволікати команди реагування і призводити до помилок. Наприклад, якщо в обробку буде прийнято кіберінцидент, який уже обробляється командою реагування на боці організації, то буде витрачено час на комунікацію із представниками організації, хоча корисніше буде при цьому займатися кіберінцидентами, які дійсно потребують обробки.

6.

Список полів таблиці списку черги обробки кіберінцидентів:

ID — ідентифікатор/порядковий номер;

CRY — рівень критичності (Criticality level);

CVSS — значення метрики CVSS (Common Vulnerability Scoring System);

SL — загроза на державному рівні (State Layer);

SEC — сектор (галузь) атакованого об'єкта (Sector);

LOSS — збитки, грн;

DOWN — час застою;

CA — кількість постраждалих осіб (Clients Affected);

RE — результат впливу (Result of Exposure);

DTD — дата та час виявлення кіберінциденту/кібератаки (Date and time of discovery);

STD — дата та час початку кіберінциденту/кібератаки (Start date and time);

IS — вплив на функціонування систем/мереж, сервіси (послуги) (Impact on Services);

NET — кількість скомпрометованих систем/мереж;

AST — тип скомпрометованої системи/мережі за функціоналом (Affected System Type);

RDT — час надходження (Registration Date and Time).

7.

При надходженні кіберінциденту він додається до Загального списку кіберінцидентів та приймається рішення про додавання його до Черги обробки кіберінцидентів. При цьому враховуються такі відомості:

- не потребують додавання в чергу обробки та визначення пріоритизації інциденти, які вже оброблені;
- не потребують обробки кіберінциденти, про які заявлено, що вони можуть бути і будуть оброблені спеціалістами організації, де стався кіберінцидент, або сторонніми організаціями, яким буде делеговано обробку;

- якщо звіт про кіберінцидент видається недостовірним, потрібно зв'язатися з представниками організації щодо уточнень. Якщо це неможливо або надана інформація викликає сумніви, такий кіберінцидент не додається в чергу обробки кіберінцидентів.

8.

При додаванні кіберінциденту в чергу обробки кіберінцидентів потрібно обчислити метрику CVSS за базовими, часовими показниками та показниками середовища. При обчисленні значення CVSS наявність якомога більшої кількості інформації дозволяє отримати точнішу оцінку. У випадку відсутності базових чи часових метрик оцінка буде менш точною, значення CVSS буде меншим, що відобразиться на позиції кіберінциденту в черзі обробки кіберінцидентів і на його пріоритеті, який буде нижчим. У разі відсутності базових метрик CVSS оцінка не проводиться і встановлюється мінімальне значення CVSS, тобто 0 (нуль). За наявності базових і часових метрик значення CVSS розраховується згідно з методикою CVSS.

9.

При надходженні додаткової інформації про кіберінцидент її потрібно оновити в загальному списку кіберінцидентів.

Якщо додаткова інформація стосується кіберінциденту, який обробляється командою реагування і його вирішено іншою командою, потрібно припинити роботу над кіберінцидентом.

Якщо вирішення кіберінциденту, який обробляється командою реагування, делегували іншій команді, слід зв'язатися з представниками організації та визначити потребу участі команди реагування.

Якщо кіберінцидент перебуває в черзі обробки кіберінцидентів та за оновленими даними він уже

обробляється командою реагування організації, делегований сторонній організації або вказано, що допомога команді реагування не потрібна, кіберінцидент потрібно вилучити з черги обробки кіберінцидентів.

Якщо оновлений звіт видається неповним чи недостовірним, потрібно зв'язатися з представниками організації щодо уточнень та видалити кіберінцидент із черги на обробку у випадку, якщо інформація викликає сумніви.

10.

Якщо черга обробки кіберінцидентів містить один кіберінцидент, він не потребує пріоритизації і повинен одразу братися в обробку незалежно від рівня критичності.

Обробкою також є прийняття рішення про відмову в реагуванні через незначний рівень критичності. При цьому кіберінцидент вилучається із черги обробки кіберінцидентів.

11.

Якщо в черзі на обробку наявні кіберінциденти, які мають різні рівні критичності, їх потрібно відсортувати у порядку зниження рівня критичності (Надзвичайний (5) — Не критичний (0)). Після цього потрібно брати в обробку кіберінциденти починаючи з початку черги. Кіберінциденти, які взяли в обробку, повинні вилучатися із черги очікування.

12.

Якщо кілька кіберінцидентів пов'язані між собою, особливо, якщо вони відбуваються в межах однієї організації, їх потрібно об'єднати в один кіберінцидент-контейнер (група кіберінцидентів).

Перед об'єднанням інциденти мають бути відсортовані по рівню критичності і значенню CVSS.

При цьому рівень критичності та значення метрики CVSS отриманої групи присвоюється відповідно до значення найбільш критичного кіберінциденту. Якщо в групі є кіберінциденти з однаковим рівнем критичності, їх варто об'єднати в одну підгрупу, при цьому потрібно змінити рівень критичності на вищий відповідно до наведеної таблиці 1:

Таблиця 1. Категорія (рівень) критичності.

Рівень критичності	Числове значення
Не критичний	0
Низький	1
Середній	2
Високий	3
Критичний	4
Надзвичайний	5

Для визначення значення CVSS групи кіберінцидентів потрібно взяти максимальне значення CVSS у цій групі, отримати якісну оцінку рівня, визначити наступний за ним рівень і присвоїти групі мінімальне значення з діапазону, що відповідає вищому рівню. Якщо в групі є кілька кіберінцидентів з «Критичним» рівнем, групі необхідно встановити максимальне значення CVSS для цього рівня.

Для визначення якісної оцінки рівня CVSS відповідно до числового значення використовується наступна таблиця 2.

Таблиця 2. Рейтинг рівнів за CVSS 3.1

Якісна оцінка	Кількісна оцінка
Відсутній	0
Низький	0,1 — 3,9
Середній	4,0 — 6,9
Високий	7 — 8,9
Критичний	9,0 — 10,0

13.

Якщо все ще існують кіберінциденти з однаковими значеннями рівня критичності та метрики CVSS, потрібно вдатися до аналізу додаткових показників.

На початковому етапі ці показники можуть мати значення 0 і заповнюватися тільки за потреби.

Якщо існує кілька кіберінцидентів, для яких значення показників мають однакові значення, для них проводиться оцінка значень наступного показника. Для інших кіберінцидентів оцінка може не проводитися. При надходженні нового кіберінциденту цикл оцінки повторюється. Залежно від кількості кіберінцидентів, які надходять на обробку в одиницю часу, з метою прискорення обробки і зменшення кількості циклів переоцінки можна проводити уточнення додаткових показників одразу після обчислення метрики CVSS.

14.

При уточненні пріоритету кіберінциденту значення додаткових показників встановлюються в порядку, описаному нижче:

A. Що є під загрозою на державному рівні (SL, State Layer):

- національна безпека — 6;
- сталість економіки — 5;
- функціонування уряду — 4;
- безпека персональних даних громадян — 3;
- національний імідж — 2;
- інше — 1;
- немає даних — 0.

B. Сектор (галузь) атакованого об'єкта (SEC, Sector):

- сектор безпеки і оборони — 12;

- органи державної влади — 11;
- фінансовий сектор — 10;
- енергетичний сектор — 9;
- інші критичні організації — 8;
- сфера електронних комунікаційних послуг — 7;
- органи місцевого самоврядування — 6;
- IT сектор — 5;
- транспортна галузь — 4;
- підприємства та організації відповідної форми власності — 3;
- засоби масової інформації — 2;
- інше — 1;
- немає даних — 0.

C. Збитки (LOSS):

- тис. грн — одна або дві значущі цифри;
- не оцінювалося або менше 1 тис. грн — 0.

D. Час застою (DOWN):

- час простою обладнання у робочих годинах — одна значуща цифра;
- невідомо або не оцінювалося — 0.

E. Кількість постраждалих осіб (CA, Clients Affected):

- більше 1000000 — 4;
- 100001-1000000 — 3;
- 20001-100000 — 2;
- 1-20000 — 1;
- немає даних або постраждалих — 0.

F. Результат впливу (RE, Result of Exposure):

- витік даних — 4;

- злам (компрометація) системи — 3;
- втрата функціональності систем/сервісів — 2;
- інше — 1;
- немає даних — 0.

G. Вплив на функціонування систем/мереж, сервіси (послуги) (IS, Impact on Services):

- втрата доступності критичних сервісів (послуг) — 8;
- втрата доступності некритичних сервісів (послуг) — 7;
- значний вплив на критичні сервіси (послуги) — 6;
- значний вплив на некритичні сервіси (послуги) — 5;
- мінімальний вплив на критичні сервіси (послуги) — 4;
- мінімальний вплив на некритичні сервіси (послуги) — 3;
- немає впливу на сервіси (послуги) — 2;
- немає впливу взагалі — 1;
- немає даних — 0.

H. Кількість скомпрометованих систем/мереж (NET):

- більше ніж 100 — 4;
- 50 – 100 — 3;
- 0 – 50 — 2;
- 1 – 10 — 1;
- немає даних — 0.

I. Тип скомпрометованої системи/мережі за функціоналом (AST, Affected System Type):

- сервер(и) баз даних — 9;
- поштовий сервер — 8;
- сервер(и) застосунків — 7;
- вебсервер(и) — 6;

- сервери доменних імен — 5;
- робочі станції — 4;
- брандмауер(и) — 3;
- мережеве обладнання — 2;
- інше — 1;
- немає даних — 0.

Значення показників відображають важливість вибраного значення і потрібні для визначення порядку при сортуванні.

15.

Після встановлення значень додаткових показників потрібно відсортувати таблицю в порядку значущості показників:

CRY — рівень критичності — від більшого до меншого;

CVSS — значення метрики CVSS — від більшого до меншого;

SL — що є під загрозою на державному рівні — від більшого до меншого;

SEC — сектор (галузь) атакованого об'єкта — від більшого до меншого;

LOSS — збитки, грн — від більшого до меншого;

DOWN — час застою — від більшого до меншого;

CA — кількість постраждалих осіб — від більшого до меншого;

RE — результат впливу — від більшого до меншого;

IS — вплив на функціонування систем/мереж, сервіси (послуги) — від більшого до меншого;

NET — кількість скомпрометованих систем/мереж — від більшого до меншого;

AST — тип скомпрометованої системи/мережі за функціоналом — від більшого до меншого;

RDT — час надходження — від меншого до більшого.

16.

Після сортування за списком черги на обробку порядковий номер інциденту встановлює його пріоритет. Найбільш пріоритетним є кіберінцидент з порядковим номером нуль, а всі наступні значення пріоритетів збільшуються на одиницю, що відповідає зниженню пріоритетності кіберінциденту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України "Про захист інформації в інформаційно-комунікаційних системах" № 80/94-ВР зі змінами на підставі № 2801-IX від 31.12.2023/ Відомості Верховної Ради, 1994. [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр.

2. Закон України «Про основні засади забезпечення кібербезпеки України» / Відомості Верховної Ради України, — № 2163-VIII. — Київ, 2017. [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.

3. Закон України «Про електронні комунікації» / Відомості Верховної Ради України, — № 1089-IX. — Київ, 2020. [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/1089-20.

4. Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж / Постанова Кабінету Міністрів України 16.05.2023 № 497. [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/497-2023-п.

5. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози / Постанова Кабінету Міністрів України від 126.11.2025 No 1533. [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text.

6. Загальні вимоги з кіберзахисту об'єктів критичної інфраструктури / Постанова Кабінету Міністрів України від 19.06.2019 № 518. [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/518-2019-п.

7. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки / Постанова Кабінету Міністрів України від 23.2020 № 1295. [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/1295-2020-п.

8. Про План реалізації Стратегії кібербезпеки України / Рішення Ради національної безпеки і оборони України від 30.12.2021. Введено в дію Указом Президента України від 1 лютого 2022 року № 37/2022. — Київ: РНБО, 2022. — 15 с.

9. Про План реалізації Стратегії кібербезпеки України / Рішення Ради національної безпеки і оборони України від 30.12.2021. Введено в дію Указом Президента України

від 1 лютого 2022 року № 37/2022. — Київ: РНБО, 2022. [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/n0087525-21.

10. ДСТУ EN ISO/IEC 29147:2022 Інформаційні технології. Методи захисту. Розкриття вразливостей (EN ISO/IEC 29147:2020, IDT; ISO/IEC 29147:2018, IDT).

11. ДСТУ EN ISO/IEC 30111:2022 Інформаційні технології. Методи захисту. Процеси оброблення вразливостей (EN ISO/IEC 30111:2020, IDT; ISO/IEC 30111:2019, IDT).

12. ДСТУ EN ISO/IEC 27002:2022 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (EN ISO/IEC 27002:2017, IDT; ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015, IDT).

13. ДСТУ ISO/IEC 27035-1:2023 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами (ISO/IEC 27035-1:2023-2, IDT).

14. ДСТУ ISO/IEC 27035-2:2022 Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти (ISO/IEC 27035-2:2022, IDT).

15. NIST Special Publication 800-216. Recommendations for Federal Vulnerability Disclosure Guidelines. May 2023 [Електронний ресурс]. — Режим доступу: https://csrc.nist.gov/pubs/sp/800/216/final.

16. NIST Special Publication 800-40 Rev.4 Guide to Enterprise Patch Management Planning: Preventive Maintenance for TechNºlogy. April 2022 [Електронний ресурс]. — Режим доступу: https://csrc.nist.gov/pubs/sp/800/40/r4/final.

17. NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations). September 2020. [Електронний ресурс]. — Режим доступу: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

18. NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide. Режим доступу: https://csrc.nist.gov/pubs/sp/800/61/r2/final.

19. NIST SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. — Режим доступу: https://csrc.nist.gov/pubs/sp/800/161/r1/final.

20. NIST SP 800-47 Rev. 1 Managing the Security of Information Exchanges. — Режим доступу: https://csrc.nist.gov/pubs/sp/800/47/r1/final.

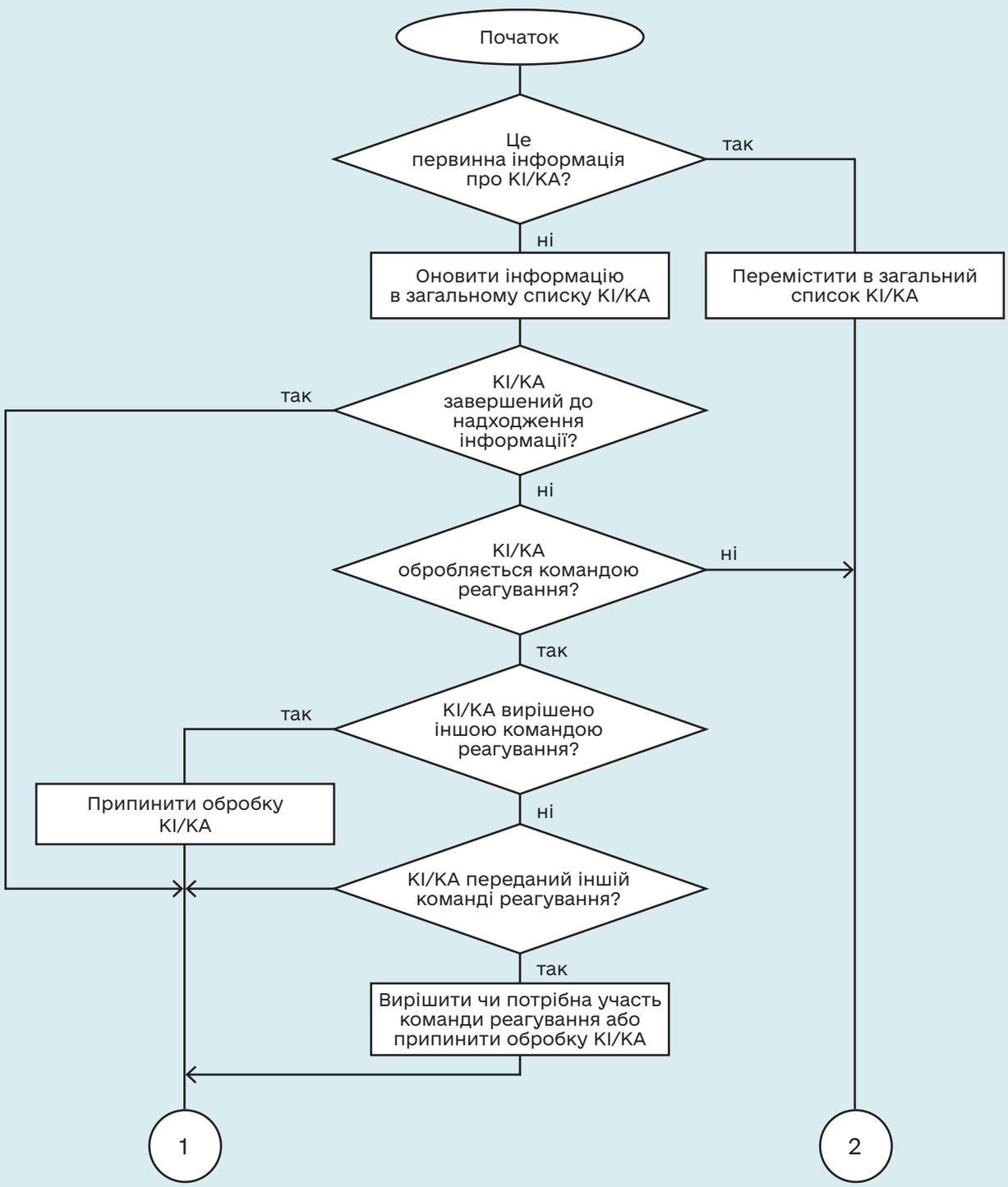
21. Національна база даних вразливостей США (NIST national vulnerability database). [Електронний ресурс]. — Режим доступу: https://nvd.nist.gov.

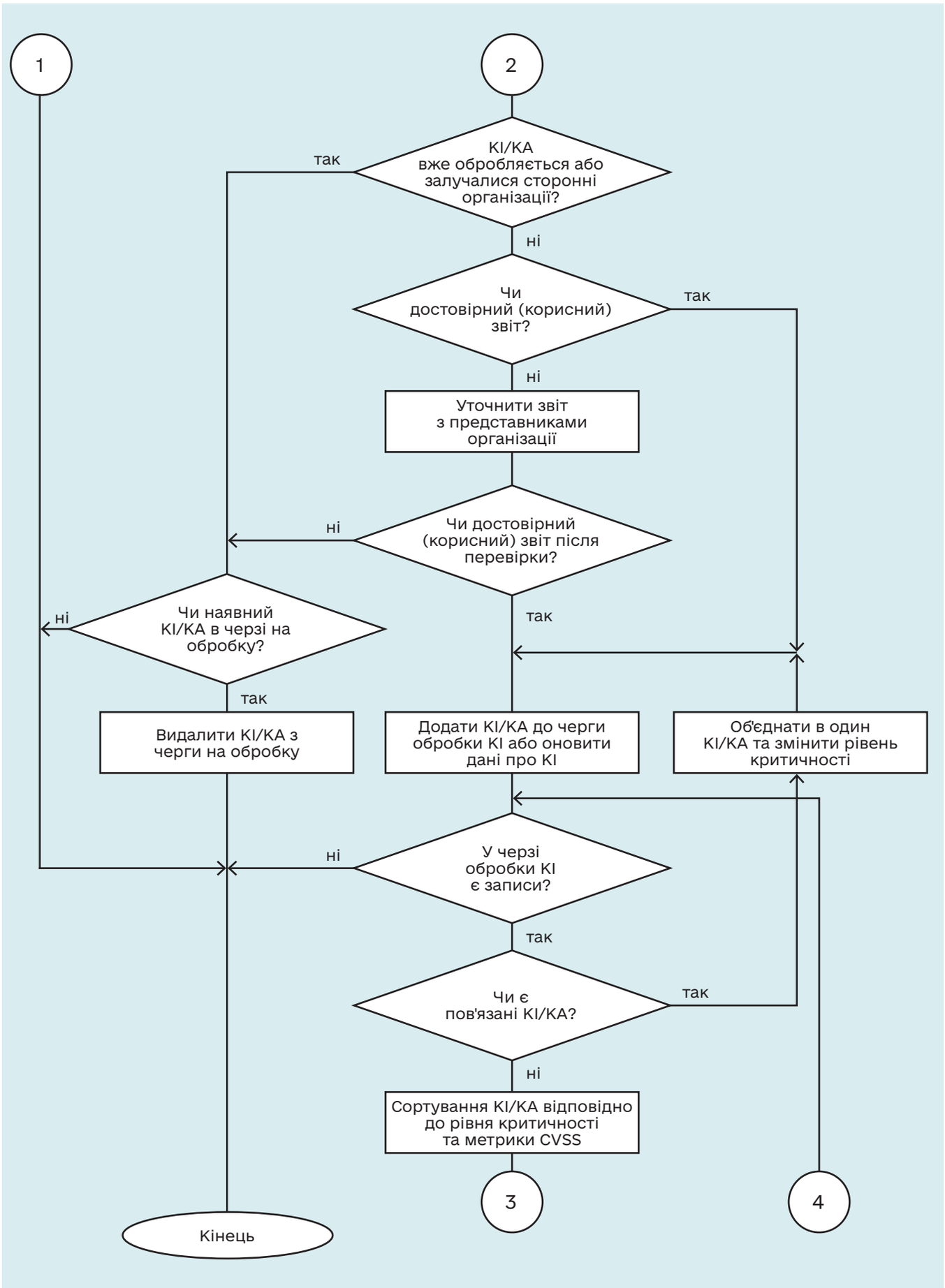
22. Протокол маркування конфіденційної інформації повідомлень про кіберінциденти TLP 2.0 Посібник користувача (Traffic Light Protocol 2.0 User Guide). — Режим доступу: https://www.cisa.gov/sites/default/files/2023-02/tlp-2-0-user-guide_508c.pdf.

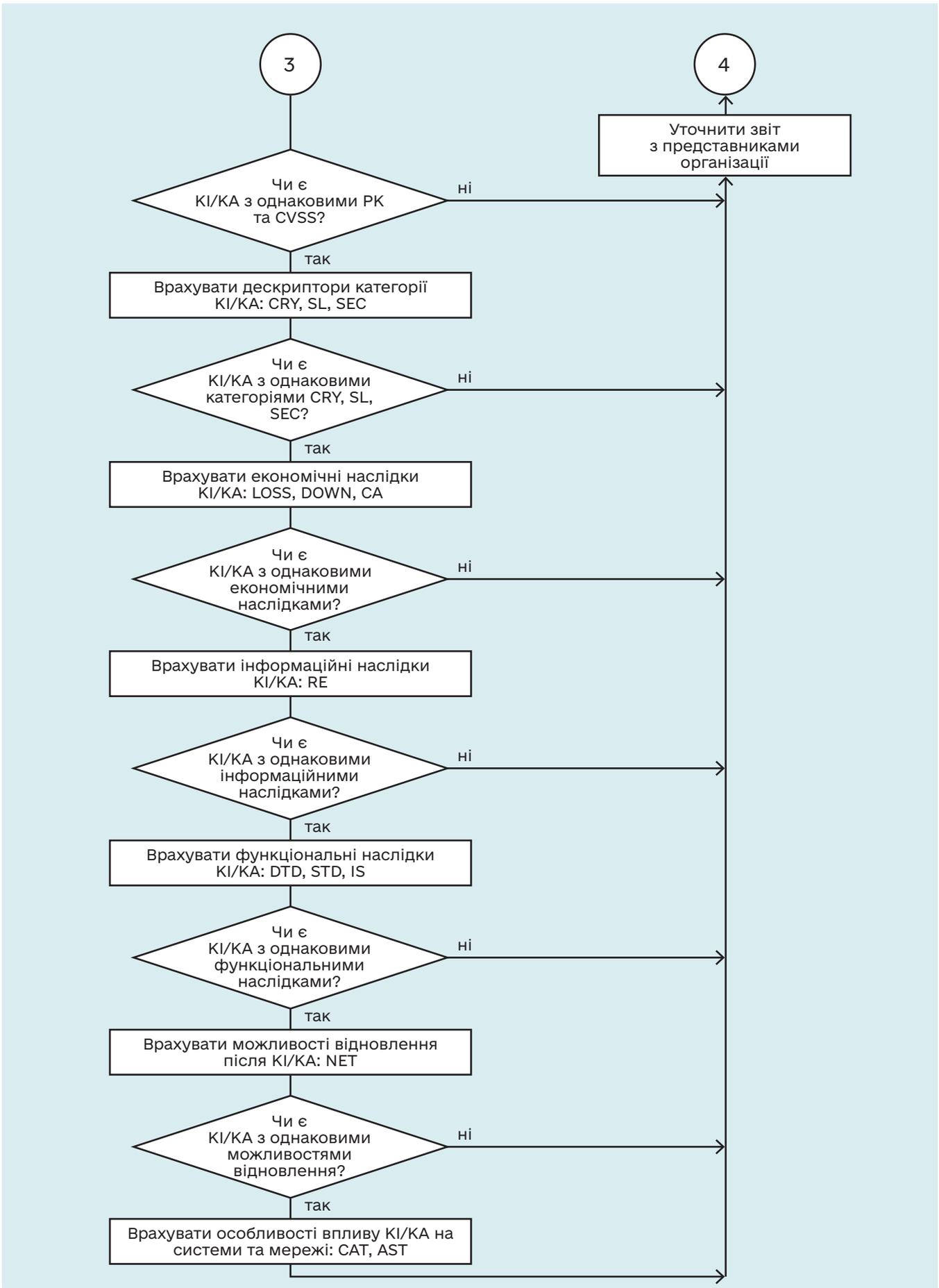
ДОДАТКИ

Додаток 1
до Настанови з обробки
кіберінцидентів:
пріоритетність з урахуванням
визначених рівнів їх
критичності
(пункт 3 розділу II)

АЛГОРИТМ ВИЗНАЧЕННЯ ПРІОРИТЕТНОСТІ ОБРОБКИ КІБЕРІНЦИДЕНТІВ/КІБЕРАТАК




1
2
КІ/КА вже обробляється або залучалися сторонні організації?
так
ні
Чи достовірний (корисний) звіт?
так
ні
Уточнити звіт з представниками організації
Чи достовірний (корисний) звіт після перевірки?
ні
так
Чи наявний КІ/КА в черзі на обробку?
ні
так
Видалити КІ/КА з черги на обробку
Додати КІ/КА до черги обробки КІ або оновити дані про КІ
Об'єднати в один КІ/КА та змінити рівень критичності
У черзі обробки КІ є записи?
ні
так
Чи є пов'язані КІ/КА?
так
ні
Сортування КІ/КА відповідно до рівня критичності та метрики CVSS
3
4
Кінець


3
4
Уточнити звіт з представниками організації
Чи є KI/KA з однаковими PK та CVSS?
ні
так
Врахувати дескриптори категорії KI/KA: CRY, SL, SEC
Чи є KI/KA з однаковими категоріями CRY, SL, SEC?
ні
так
Врахувати економічні наслідки KI/KA: LOSS, DOWN, CA
Чи є KI/KA з однаковими економічними наслідками?
ні
так
Врахувати інформаційні наслідки KI/KA: RE
Чи є KI/KA з однаковими інформаційними наслідками?
ні
так
Врахувати функціональні наслідки KI/KA: DTD, STD, IS
Чи є KI/KA з однаковими функціональними наслідками?
ні
так
Врахувати можливості відновлення після KI/KA: NET
Чи є KI/KA з однаковими можливостями відновлення?
ні
так
Врахувати особливості впливу KI/KA на системи та мережі: CAT, AST

Додаток 2
до Настанови з обробки
кіберінцидентів:
пріоритетність з урахуванням
визначених рівнів їх
критичності
(пункт 3 розділу II)

Група показників / показник	Код	Знач.	Опис
Загальні			
Чи вирішено кіберінцидент/кібератаку?		1	Так
		0	Ні
Чи потрібна допомога CERT-UA?		1	Так
		0	Ні
Чи повідомлялося про кіберінцидент/кібератаку іншим основним суб'єктам забезпечення кібербезпеки? Яким саме?		1	Так
		0	Ні
			Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, Розвідувальні органи, Національний банк України, Національна поліція України, Національний координаційний центр кібербезпеки при РНБО України, Департамент кіберполіції Національної поліції України, інше
Чи залучалися сторонні організації до вирішення кіберінциденту/кібератаки?		1	Так
		0	Ні
			Інший CERT, CSIRT, SOC], Антивірусні компанії, Обслуговуюча компанія, інтегратор, представник вендора, інше (вказати)
Чи пов'язаний цей (ця) кіберінцидент/кібератака з попередніми?		1	Так
		0	Ні
			ID пов'язаного кіберінциденту / кібератаки
Категорія кіберінциденту/кібератаки			
Запропонована категорія (рівень) критичності кіберінцидент/кібератаки	CRY	5	Надзвичайний
		4	Критичний
		3	Високий
		2	Середній
		1	Низький
		0	Не критичний
Загроза на державному рівні	SL (State Layer)	6	Національна безпека
		5	Сталість економіки
		4	Функціонування уряду
		3	Безпека персональних даних громадян
		2	Національний імідж
		1	Інше
		0	Немає даних

Група показників / показник	Код	Знач.	Опис
Сектор (галузь) атакованого об'єкта	SEC (Sector)	12	Сектор безпеки і оборони
		11	Органи державної влади
		10	Фінансовий сектор
		9	Енергетичний сектор
		8	Інші критичні організації
		7	Сфера електронних комунікаційних послуг
		6	Органи місцевого самоврядування
		5	IT сектор
		4	Транспортна галузь
		3	Підприємства та організації відповідної форми власності
		2	Засоби масової інформації
		1	Інше
		0	Немає даних
Постраждалий суб'єкт забезпечення кібербезпеки (юридична назва)			Для перевірки правильності даних
Економічні наслідки кіберінциденту			
Збитки	LOSS	N	Одна або дві значущі цифри
		0	Не оцінювалося або менше 1 тис. грн.
Час застою	DOWN	N	Час простою обладнання у робочих годинах
		0	невідомо або не оцінювалося
Кількість постраждалих осіб	CA (Clients Affected)	4	Більше ніж 1000000
		3	100001 – 1000000
		2	20001 – 100000
		1	1 – 20000
		0	Немає даних або постраждалих
Інформаційні наслідки кіберінциденту/кібератаки			
Результат впливу	RE (Result of Expo-sure)	4	Витік даних
		3	Злам (компрометація) системи
		2	Втрата функціональності систем/сервісів
		1	Інше
		0	Немає даних
Функціональні наслідки кіберінциденту/кібератаки			
Дата та час виявлення кіберінциденту/кібератаки	DTD (Date and time of discovery)		Для перевірки правильності даних
Дата та час початку кіберінциденту/кібератаки	STD (Start date and time)		Для перевірки правильності даних
Вплив на функціонування систем/мереж, сервіси (послуги)	IS (Impact on Services)	8	Втрата доступності критичних сервісів (послуг)

Група показників / показник	Код	Знач.	Опис
		7	Втрата доступності некритичних сервісів (послуг)
		6	Значний вплив на критичні сервіси (послуги)
		5	Значний вплив на некритичні сервіси (послуги)
		4	Мінімальний вплив на критичні сервіси (послуги)
		3	Мінімальний вплив на некритичні сервіси (послуги)
		2	Немає впливу на сервіси (послуги)
		1	Немає впливу взагалі
		0	Немає даних
Можливості відновлення після кіберінциденту/кібератаки			
Кількість скомпрометованих систем/мереж	NET	4	Більше ніж 100
		3	51 – 100
		2	11 – 50
		1	1 – 10
		0	Немає даних
Особливості впливу кіберінциденту/кібератаки системи/мережі суб'єкта забезпечення кібербезпеки			
Категорія та тип кіберінциденту (відповідно до Переліку категорій та типів кіберінцидентів)	CAT		Для перевірки правильності
Тип скомпрометованої системи/мережі за функціоналом	AST (Affected System Type)	9	Сервер(и) баз даних
		8	Поштовий сервер
		7	Сервер(и) застосунків
		6	Вебсервер(и)
		5	Сервери доменних імен
		4	Робочі станції
		3	Брандмауер(и)
		2	Мережеве обладнання
		1	Інше
		0	Немає даних
Опис кіберінциденту/кібератаки			Для перевірки правильності даних

Додаток 3
до Настанови з обробки
кіберінцидентів:
пріоритетність з урахуванням
визначених рівнів їх
критичності

МЕТРИКИ СИСТЕМИ ОЦІНКИ ВРАЗЛИВОСТЕЙ CVSS ВЕРСІЇ 3.1

Метрична група	Множина метрик	Набори символьних значень метрик		Числові значення метрик
Базова	AV (Вектор атаки)	Network (N)	Мережа	0.85
		Adjacent (A)	Сполучена мережа	0.62
		Local (L)	Локальний доступ	0.55
		Physical (P)	Фізичний доступ	0.2
	AC (Складність атаки)	Low (L)	Низькі	0.77
		High (H)	Високі	0.44
	PR (Необхідні повноваження)	Nºne (N)	Немає	0.85
		Low (L)	Середні	0.62 або 0,68*
		High (H)	Високі	0,27 або 0,50*
	UI (Взаємодія з користувачем)	Nºne (N)	Немає	0,85
		Required (R)	Потрібна	0,65
	S Область дії	Unchanged (U)	Без змін	—
		Changed (C)	Змінена	—
	C (Вплив на конфіденційність); I (Вплив на цілісність); A (Вплив на доступність)	High (H)	Високий	0,56
		Low (L)	Середній	0,22
		Nºne (N)	Немає	0
Часова	E (Можливість використання)	Nºt Defined (X)	Не визначена	1
		High (H)	Висока	1
		Functional (F)	Функціональна	0,97
		Proof-of-Concept (P)	Експериментальна	0,94
		Unproven (U)	Теоретична (немає доказів)	0,91
	RL (Рівень виправлення)	Nºt Defined (X)	Не визначені	1
		Unavailable (U)	Немає	1
		Workaround (W)	Рішення на основі порад та рекомен-дацій	0.97
		Temporary Fix (T)	Тимчасове рішення	0.96
		Official Fix (O)	Офіційний патч	0.95
	RC (Достовірність звіту)	Nºt Defined (X)	Не визначена	1
		Confirmed (C)	Підтверджена	1
		Reasonable (R)	Обґрунтована	0.96
		UnkNºwn (U)	Немає	0.92

Метрична група	Множина метрик	Набори символьних значень метрик		Числові значення метрик
	CR (Вимога конфіденційності); IR (Вимога цілісності); AR (Вимога доступності)	№t Defined (X)	Не визначені	1
		High (H)	Високі	1.5
		Medium (M)	Середні	1
		Low (L)	Низькі	0.5
	Мають ті ж символьні та числові значення показників, що і відповідні немодифіковані показники в базовій метричній групі, а також «№t Defined» (не визначені)			
Середовища	MAV	модифікований вектор атаки		
	MAC	модифікована складність атаки		
	MPR	модифіковані необхідні повноваження		
	MUI	модифікована взаємодія з користувачем		
	MS	модифікована область дії		
	MC	модифікована конфіденційність		
	MI	модифікована цілісність		
	MA	модифікована доступність		

Державна служба
спеціального зв'язку
та захисту інформації
України

НАСТАНОВА З ОБРОБКИ КІБЕРІНЦИДЕНТІВ: ПРІОРИТЕТНІСТЬ З УРАХУВАННЯМ ВИЗНАЧЕНИХ РІВНІВ ЇХ КРИТИЧНОСТІ

Київ 2026