Державна служба
спеціального зв'язку
та захисту інформації
України

НАСТАНОВА З УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ЗА РІВНЯМИ КРИТИЧНОСТІ КІБЕРІНЦИДЕНТІВ

Київ 2026

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ІКС — інформаційно-комунікаційна система

КА — кібератака

КІ — кіберінцидент

ШПЗ — шкідливе програмне забезпечення

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

CWE — (англ. Common Weakness Enumeration) загальний перелік

DDoS — (англ. Distributed Denial Of Service) розподілена атака на відмову в обслуговуванні вразливостей

DoS — (англ. Denial Of Service) атака на відмову в обслуговуванні

ENISA — (англ. European Union Agency for Cybersecurity) Агентство Європейського Союзу з кібербезпеки

FIRST — (англ. Forum for Incident Response and Security Teams) форум команд реагування на інциденти безпеки

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

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

ISS — (англ. Impact Sub-Score) показник впливу

MISS — (англ. Modified Impact Sub-Score) модифікований показник впливу

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.

Настанову з управління вразливостями інформаційно-комунікаційних систем за рівнями критичності кіберінцидентів (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». Настанова призначена для використання під час організації та проведення пошуку та виявлення потенційних вразливостей інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

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» постанови Кабінету Міністрів України від 3 грудня 2025 року № 1580 «Деякі питання пошуку та виявлення потенційних вразливостей в інформаційно-комунікаційних системах».

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 Tech№logy), 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);

- 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);
- 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 Настанові терміни вживаються в такому значенні:

- **"білий" хакер** — людина, яка спрямовує свої навички з метою виявлення прогалин та слабких місць у компаніях та пристроях, підключених до Інтернету, а також підписує різні міжнародні зобов'язання (кодекс честі), що свідчить про те, що його роль позитивна і корисна;
- **виправлення** — зміни, внесені до системи, щоб видалити вразливість, унеможливити її використання або зменшити наслідки її використання;

- **власник системи** — фізична або юридична особа, якій належить право власності на систему;

- **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;

- **дослідник потенційної вразливості (далі — дослідник)** — фізична або юридична особа, яка здійснює пошук потенційної вразливості системи відповідно до вимог Настанови;

- **експлойт** — комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують вразливості в програмному забезпеченні та призначені для проведення атаки на інформаційну та інформаційно-комунікаційну систему;

- **експлуатація вразливості** — будь-які дії з використання вразливості системи, що можуть призвести до порушення сталого, надійного та штатного режиму функціонування системи та/або порушення конфіденційності, цілісності, доступності інформації в системі;

- **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;

- **організатор пошуку потенційної вразливості системи (далі — організатор)** — фізична або юридична особа, яка надає послуги з організації пошуку потенційної вразливості системи;

- **перевірка звіту про вразливість** — перевірка достовірності інформації, зазначеної у звіті про

вразливість системи, та оцінка ризику від експлуатації вразливості;

- **публічна пропозиція** — оферта, політика, відповідний розділ політики інформаційної безпеки, публічно оприлюднені умови договору приєднання, інший документ, які врегульовують умови пошуку та виявлення потенційних вразливостей систем та оприлюднені загальнодоступно у мережі Інтернет;

- **шкідливе програмне забезпечення (ШПЗ)** — програмне забезпечення, функціональні можливості якого передбачають реалізацію несанкціонованих або неавторизованих процесів, які мають прямий або опосередкований вплив на сталий, надійний та штатний режим функціонування систем суб'єкта забезпечення кібербезпеки, за якого порушуються властивості інформації, що обробляється в цих системах.

Інші терміни вживаються у значеннях, наведених у 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.

Рекомендації містять стандартизовані заходи управління вразливостями, що можуть проводитися суб'єктами

забезпечення кібербезпеки послідовно за такими етапами, як підготовка, ідентифікація (виявлення), оцінювання, усунення (відновлення), звітування.

Процес управління вразливостями передбачає визначення ознак використання експлойтів та можливості встановлення оновлень або внесення виправлень (патчів), як графічно наведено у додатку 1.

7.

Організація пошуку потенційної вразливості системи здійснюється її власником. У разі потреби власник системи може прийняти рішення про залучення організатора для організації пошуку потенційної вразливості системи. Необхідність залучення організатора визначає власник системи з урахуванням наявності достатніх у нього ресурсів для забезпечення визначених заходів. Взаємовідносини між власником системи та організатором, права та їх обов'язки визначаються окремим договором.

Власник системи, який прийняв рішення про проведення пошуку та виявлення потенційних вразливостей системи, розробляє та оприлюднює на офіційному вебсайті публічну пропозицію. Розробка та оприлюднення публічної пропозиції можуть бути доручені власником системи організатору на підставі окремого договору.

Перед пошуком потенційних вразливостей дослідник повинен пересвідчитися, що системи, щодо яких він має намір здійснити пошук вразливостей, визначені чітко в межах публічної пропозиції. Проведення такого пошуку та виявлення потенційних вразливостей дослідник повинен здійснювати в межах, визначених публічною пропозицією.

Дослідник, знайшовши потенційну вразливість, повідомляє про неї власника системи/організатора згідно з умовами публічної пропозиції.

8.

Стандартизований процес управління вразливостями гарантує, що організації можуть зрозуміти вплив критичних і небезпечних вразливостей на ІКС.

Окремі заходи управління вразливостями є повторюваними і можуть виконуватися та змінюватися безперервно, доки вразливість в ІКС не буде усунена, а електронні докази, необхідні для проведення розслідування та аналізу вразливостей, не будуть зібрані.

9.

Вразливості, котрі розглядаються у цій Настанові, можуть бути виявлені відповідним державним органом, Національним координаційним центром кібербезпеки, галузевими партнерами або іншими сторонами, залученими до виконання відповідних завдань. Більшість вразливостей матимуть дескриптори загальновідомих вразливостей інформаційної безпеки (Common Vulnerabilities and Exposures, CVE).

CVE — база даних загальновідомих вразливостей інформаційної безпеки.

Кожній вразливості присвоюється ідентифікаційний номер виду CVE-рік-номер.

10.

В інших випадках організації можуть стикнутися з новими вразливостями, які ще не мають CVE (наприклад, тими, що належать до нульового дня), або з вразливостями, котрі є результатом неправильної конфігурації чи налаштувань.

У додатку 2 наведено контрольний список для одночасного відстеження заходів до їх завершення.

II. ЕТАП ПІДГОТОВКИ

II. ЕТАП ПІДГОТОВКИ

1.

Ефективне усунення вразливостей базується на надійному управлінні вразливостями й розпочинається з етапу підготовки.

2.

Слід переконатися, що в організації дотримуються ефективних практик управління вразливостями. Такі практики включають створення та підтримку надійного управління активами, що включає інвентаризацію:

- систем та мереж, котрими управляє Організація;
- систем та мереж, які передбачають партнерство з іншими організаціями;
- систем та мереж, котрими управляють інші, включаючи хмарні системи, системи підрядників (виконавців) і постачальників послуг.

3.

Сформулювати процес для розуміння значущості вразливостей для середовища шляхом відстеження операційних систем та інших застосунків для всіх систем.

Врахувати, що всі системи можуть мати вразливості, та розглянути наслідки потенційної вразливості для діяльності.

4.

Організація постійно оцінює та регулярно оновлює свої процеси захисту, щоб на систематичній основі виявляти можливі існуючі вразливості задля визначення їх як цілі у плані усунення.

5.

В Організації розробляється та впроваджується план управління вразливостями для інформаційно-комунікаційної системи, ризики, пов'язані з вразливостями враховуються.

6.

Організація надає необхідні ресурси для проведення експертизи під час процесу обробки кіберінциденту. Така експертиза допомагає виявити вразливості, а потім розробити способи їх пом'якшення.

III. ЕТАП ІДЕНТИФІКАЦІЇ (ВИЯВЛЕННЯ)

III. ЕТАП ІДЕНТИФІКАЦІЇ (ВИЯВЛЕННЯ)

1.

Цей етап визначає потреби активного проведення пошуку потенційних вразливостей, які часто експлуатовуються, їх виявлення та звітування, відстежуючи канали інформації про загрози та джерела інформації.

2.

Заходи з ідентифікації (виявлення) містять:

- розроблення процедури управління вразливістю та план для всієї організації;
- визначення та призначення ролей та обов'язків для підтримки управління вразливістю;
- вразливості системи, які проаналізовані, ідентифіковані та задокументовані;
- отримання з форумів та офіційних джерел інформації про загрози безпеки та вразливості;
- проведення організацією аналізу та перевірки інформаційних джерел, офіційних сайтів уповноважених органів з метою отримання актуальної інформації щодо безпеки на національному рівні, забезпечення постійного контакту з групами та асоціаціями тощо з безпеки, які мають великий досвід роботи з мінливими технологіями та загрозами;
- регулярне сканування вразливостей як автоматично, так і за запитом;
- запровадження автоматизованих механізмів з метою отримання, аналізу та реагування на вразливості;

- запровадження програми аналізу загроз (дослідження та обізнаність) із належним обсягом для включення всіх компонентів і активів Організації.

3.

Збір додаткової інформації про вразливості відповідно до рівнів критичності (додаток 3), щоб допомогти процесу реагування на кіберінциденти, включаючи тяжкість наслідків експлуатації вразливості, вразливі версії програмного забезпечення та індикатори або інші етапи дослідження, які можна використати, щоб визначити, чи скористалися цією вразливістю.

4.

Виявлення вразливостей інформаційно-комунікаційної системи споживачами послуг здійснюється так званими «білими хакерами/дослідниками». «Білі хакери/дослідники» не становлять небезпеки для системи, а націлені на її захист.

Пошук та ліквідація цих вразливостей необхідні для того, щоб забезпечити безпеку тих підприємств, які беруть участь у ланцюгу постачання і використовують визначену систему. Якщо хоча б одне таке підприємство знаходить якусь вразливість у системі, воно повинно повідомити про це розробника самої системи, який в свою чергу має повідомити негайно про це інших користувачів такої системи, особливо, якщо вони належать до сектору критичної інфраструктури. Після цього, розробник системи розпочинає вжиття заходів із усунення визначеної вразливості. Після її усунення він повинен повідомити усіх споживачів про те, що вразливість усунена.

IV. ЕТАП ОЦІНЮВАННЯ

IV. ЕТАП ОЦІНЮВАННЯ

1.

Мета етапу оцінювання полягає у визначенні дослідником, чи існує у середовищі вразливість і наскільки критичним є відповідне програмне або апаратне забезпечення за допомогою таких методологій, наприклад, як використання метрик CVSS (Common Vulnerability Scoring System).

2.

Заходи з оцінювання містять:

- визначення вразливостей ІКС (визначення, чи ІКС є чутливою до вразливості та існування патчу або подібного рішення для вразливості);
- визначення ризику кібербезпеки із застосуванням даних щодо загроз, вразливостей, їх ймовірностей та рівня шкоди;
- виконання технічного аналізу (оцінки). Він включає перегляд відповідних індикаторів, щоб визначити ступінь (потенційного чи фактичного) проникнення вразливості в ІКС; оцінку вразливості з урахуванням рівнів критичності, які наведені в додатку 4; повідомлення національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA, а в разі наявності — галузевої або регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози про будь-яку вразливість та початок процедури її усунення (відновлення).

3.

Потрібно переконатися щодо наявності й застосування критично важливих інструментів встановлення оновлень

чи внесення виправлень (патчів) та можливостей їх використання для автоматизації процесу виявлення більшості вразливостей.

4.

Для вразливостей, якими активно користуються, потрібно використовувати процеси «швидкого реагування» у цих інструментах.

У рідкісних випадках, таких як разові неправильні конфігурації чи налаштування та випадки «нульового дня», може знадобитися виконання додаткових сканувань вручну.

Перелік конкретних технічних етапів для оцінювання наявної вразливості також може бути викладений в обов'язкових для виконання рекомендаціях Національного координаційного центру кібербезпеки, або в наказах Адміністрації Держспецзв'язку.

5.

Якщо в середовищі інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж існує вразливість, усувається сама вразливість, як це описано на етапі «Усунення (відновлення)», визначається ступінь її використання в середовищі Організації. Для цього потрібно застосовувати найкращі практики, щоб знайти ознаки використання експлойтів, зокрема:

- перевірку відомих індикаторів, пов'язаних з використанням вразливості;
- розслідування будь-якої ненормальної активності, пов'язаної з вразливими системами чи службами, включаючи аномальні спроби доступу та поведінку;
- проведення будь-яких процесів виявлення, зазначених у наказах Адміністрації Держспецзв'язку;

- співпрацю зі сторонньою командою, службою та спеціалістом, що забезпечують реагування на кіберінциденти.

6.

Якщо в середовищі інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж скористалися вразливістю, негайно починаються заходи із реагування на кіберінциденти, як це описано в Методичних рекомендаціях щодо реагування на кіберінциденти.

7.

Кінцевим результатом етапу оцінювання є розуміння статусу кожної системи у середовищі інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж у форматі визначених рівнів критичності для базових, часових метрик та показників середовища.

V. ЕТАП УСУНЕННЯ (ВІДНОВЛЕННЯ)

V. ЕТАП УСУНЕННЯ (ВІДНОВЛЕННЯ)

1.

Метою етапу є своєчасне усунення всіх вразливостей, які існують довкола або всередині середовища інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якими активно користуються.

2.

Заходи з усунення (відновлення) містять:

- визначення чи доступний патч;
- якщо патч недоступний або його неможливо застосувати, визначити, застосування патчу або пом'якшення до відповідних систем;
- після виконання патчу або пом'якшення проведення оцінювання системи, щоб переконатися, що вразливість дійсно усунуто;
- збір і збереження інформації для звітності.

3.

Здебільшого усунення (відновлення) повинно полягати в установленні оновлень чи внесенні виправлень (патчів).

В інших випадках доцільними можуть бути такі варіанти пом'якшення наслідків:

- обмеження доступу;
- ізолювання вразливих систем, програм, служб, профілів або інших активів;
- постійне внесення змін до конфігурації (налаштувань).

4.

Наявні інструменти і процеси патч-менеджменту можна використовувати для регулярного виправлення всіх вразливостей.

Також застосовуються процеси «швидкого реагування», як це описано в розділі етапу «Оцінювання», в рамках тих інструментів для вразливостей, які активно експлуатуються.

5.

У випадках, коли не існує патчів (оновлень, виправлень, так званих «латок»), коли вони не перевірені або не можуть бути негайно застосовані, потрібно вжити іншіих заходів, щоб запобігти використанню експлойтів, наприклад:

- відключення служб;
- переналаштування мережевих екранів (фаєрволів) для блокування доступу;
- посилення моніторингу для виявлення використання експлойтів.

6.

Коли виправлення стануть доступними та їх можна буде безпечно застосувати, засіб пом’якшення наслідків можна буде видалити і застосувати відповідні патчі.

7.

Коли вразливості в інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних системах, електронних комунікаційних мережах буде усунуто, потрібно відстежувати їх статуси для звітування.

Результатом етапу є опис кожної системи як однієї з таких категорій:

- вразливості усунуто. Застосовано патчі або змінено конфігурацію чи налаштування, і система більше не вразлива;
- пом'якшено наслідки вразливості. Діють інші компенсаційні засоби контролю, такі як виявлення або обмеження доступу, і ризик використання вразливості зменшується;
- вразлива/скомпрометована. Жодних дій не було вжито, і система все ще є вразливою або скомпрометованою.

VI. ЕТАП ЗВІТУВАННЯ

VI. ЕТАП ЗВІТУВАННЯ

1.

Метою цього етапу є здійснення обміну інформацією про те, як зловмисники експлуатують вразливості, він може допомогти експертам із захисту інформації, які саме вразливості є найбільш критично важливими для виправлення.

2.

Заходи зі звітування містять:

- зберігання артефактів (журналів тощо), що описують вразливі системи відповідно до порядку пошуку та виявлення потенційних вразливостей;
- складання графіка (час виявлення вразливості, вжиті дії, залишкове положення) для звітування;
- вперше виявлені вразливості, які усунено або задокументовано як прийняті ризики;
- повідомлення національній команді реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA, а в разі наявності — галузевої або регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози про деталі, масштаб і хронологію вразливості.

3.

У випадку тих вразливостей, які активно експлуатуються, Національний координаційний центр кібербезпеки має бути поінформовано про статус реагування на вразливість.

Така обізнаність дає змогу Національному координаційному центру кібербезпеки допомагати іншим організаціям зрозуміти вплив вразливостей і скорочувати час між розкриттям інформації та використанням вразливості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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. 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.

6. 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.

7. 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.

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. 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.

13. 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.

14. 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.

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

16. Наказ Адміністрації Держспецзв'язку від 15.01.2016 № 20 «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті». [Електронний ресурс]. — Режим доступу: https://zakon.rada.gov.ua/laws/show/z0196-16.

ДОДАТКИ

Додаток 1
до Настанови з управління
вразливостями інформаційно-
комунікаційних систем
за рівнями критичності
кіберінцидентів
(пункт 6 розділу I)

ПОСЛІДОВНІСТЬ ЕТАПІВ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

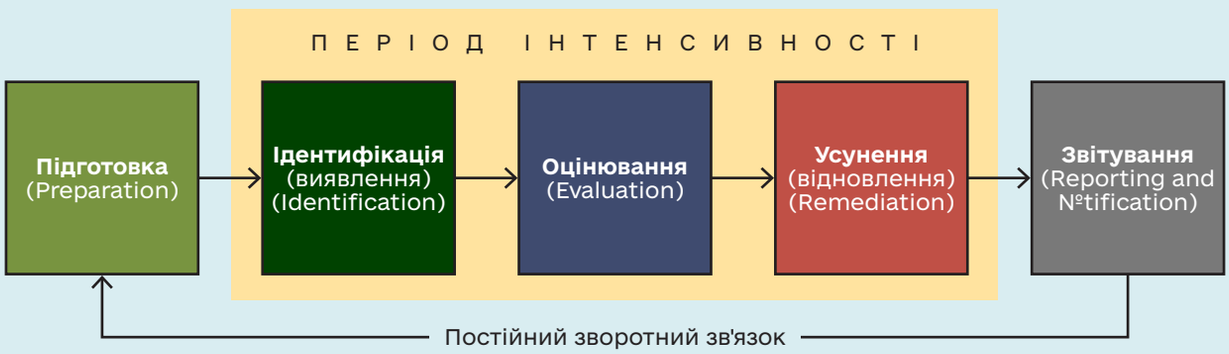

Рисунок 1. Етапи управління вразливостями інформаційно-комунікаційних систем

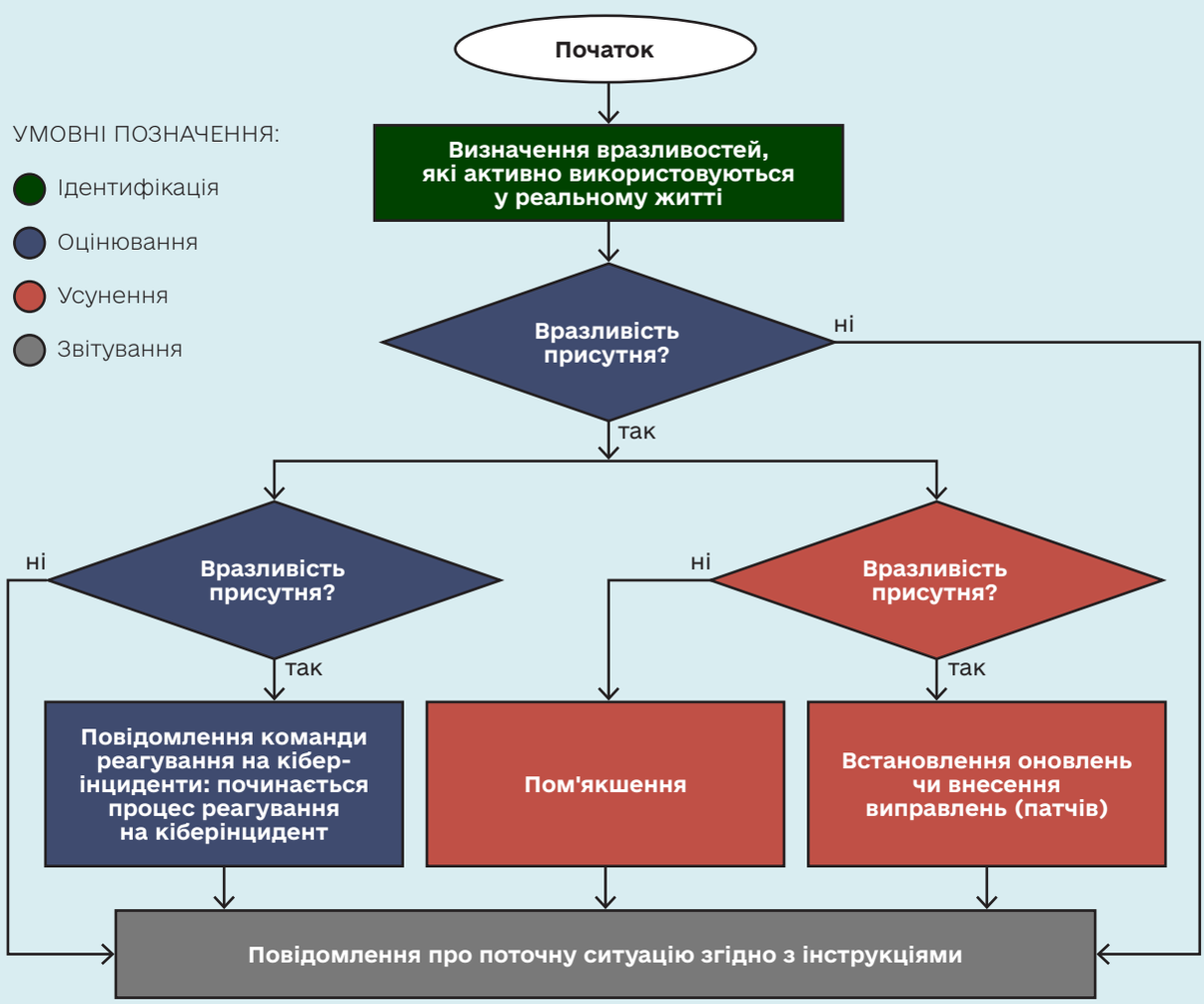

Рисунок 2. Процес управління вразливостями у сфері кібербезпеки

Додаток 2
до Настанови з управління
вразливостями інформаційно-
комунікаційних систем
за рівнями критичності
кіберінцидентів
(пункт 10 розділу I)

КОНТРОЛЬНИЙ СПИСОК ІЗ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ

Етап	Управління вразливостями	Заходи, яких було вжито	Дата, коли було вжито заходів
1	2	3	4
Етап ідентифікації (виявлення)			
1.	**Виявлення та ідентифікація вразливості, яка активно використовується в життєвих ситуаціях**		
1.1.	Розроблення процедури управління вразливістю та план для всієї Організації.		
1.2.	Визначення та призначення ролей та обов'язків для підтримки управління вразливістю.		
1.3.	Вразливості системи, які проаналізовані, ідентифіковані та задокументовані.		
1.4.	Отримання з форумів та офіційних джерел інформації про загрози безпеки та вразливості.		
1.5.	Проведення Організацією аналізу та перевірки інформаційних джерел, офіційних сайтів уповноважених органів з метою отримання актуальної інформації щодо безпеки на національному рівні, забезпечення постійного контакту з групами та асоціаціями тощо з безпеки, які мають великий досвід роботи з мінливими технологіями та загрозами.		
1.6.	Регулярне сканування вразливостей як автоматично, так і за запитом.		
1.7.	Запровадження автоматизованих механізмів з метою отримання, аналізу та реагування на вразливості.		
1.8.	Запровадження програми аналізу загроз (дослідження та обізнаність) із належним обсягом для включення всіх компонентів і активів Організації.		
Етап оцінювання			
2.	**Визначення вразливостей Організації**		
2.1.	Визначення чи є Організація чутливою до вразливості.		
2.2.	Визначення чи існує патч або подібне рішення для вразливості.		
2.3.	Визначення ризику кібербезпеки із застосуванням даних щодо загроз, вразливостей, їх ймовірностей та рівня шкоди.		
3.	**Виконання технічного аналізу**		
3.1.	Перегляд відповідних індикаторів, щоб визначити ступінь (потенційного чи фактичного) проникнення вразливості в Організації.		
3.2.	Оцінка серйозності на основі впливу, величини, уражених систем тощо.		
3.3.	Повідомити національну команду реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA, а в разі наявності — галузевої або регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози про будь-яку вразливість та почати процедуру реагування на кіберінциденти.		

1	2	3	4
Етап усунення (відновлення)			
4.	**Реакція на вразливість**		
4.1.	Визначити чи доступний патч.		
4.2.	Якщо патч недоступний або його неможливо застосувати, визначити чи можливе додаткове пом'якшення для відповідної вразливої системи.		
4.3.	Застосування патчу або пом'якшення до відповідних систем.		
4.4.	Після виконання патчу або пом'якшення проведення оцінювання системи, щоб переконатися, що вразливість дійсно усунуто.		
4.5.	Збір і збереження інформації для звітності.		
Етап звітування			
5.	**Звітування до Національного координаційного центру кібербезпеки**		
5.1.	Зберігання артефактів (журналів тощо), що описують вразливі системи відповідно до порядку пошуку та виявлення потенційних вразливостей.		
5.2.	Складання графіка (час виявлення вразливості, вжиті дії, залишкове положення) для звітування.		
5.3.	Вперше виявлені вразливості, які усунено або задокументовано як прийняті ризики		
6.	**Звітування до національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA, а в разі наявності – галузевої або регіональної команди реагування на кіберінциденти, кібератаки, кіберзагрози**		
6.1.	Повідомлення групі реагування на кіберінциденти про деталі, масштаб і хронологію вразливості.		

Додаток 3
до Настанови з управління
вразливостями інформаційно-
комунікаційних систем
за рівнями критичності
кіберінцидентів
(пункт 3 розділу III)

РІВНІ КРИТИЧНОСТІ КІБЕРІНЦИДЕНТУ/КІБЕРАТАКИ

Суб'єкти забезпечення кібербезпеки визначають критичність кіберінциденту/кібератаки 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», за такими категоріями (рівнями):

Таблиця 1. Рівні критичності

Категорії (рівні) критичності	0	1	2	3	4	5
	некритичний (білий)	**низький (зелний)**	**середній (жовтий)**	**високий (помаранч.)**	**критичний (червоний)**	**надзвичайн. (чорний)**
Кіберінцидент/кібератака сталому, надійному та штатному режиму функціонування інформаційних, електронних комунікаційних, інформаційно- комунікаційних систем, технологічних систем	не загрожує	безпосередньо загрожує	безпосередньо загрожує	безпосередньо загрожує	безпосередньо загрожує	безпосередньо загрожує
Кількість систем	–	одна	одна	одна	кілька	значна кількість
Захищеність (конфіденційності, цілісності і доступності) інформації та даних, що обробляються в системах	–	не загрожує	створюються передумови для порушення	порушується	порушується	порушується
Припинення виконання функцій та/або надання послуг критичною інфраструктурою	–	–	виникають передумови	виникають потенційні загрози	виникають реальні загрози	виникають невідворотні загрози
Об'єкти загроз	–	–	–	національна безпека і оборона, стан навколишнього природнього середовища, соціальна сфера, національна економіка та її окремі галузі	національна безпека і оборона, стан навколишнього природнього середовища, соціальна сфера, національна економіка та її окремі галузі	повноцінне функціонування держави або загроза життю громадян України
Тип впливу кіберінциденту / кібератаки	–	–	–	–	транскордонний вплив	транскордонний вплив
Залученість сил та засобів основних суб'єктів національної системи кібербезпеки для реагування	–	–	–	–	потребує	потребує максимально

Додаток 4
до Настанови з управління
вразливостями інформаційно-
комунікаційних систем
за рівнями критичності
кіберінцидентів
(пункт 2 розділу IV)

ОЦІНКА ВРАЗЛИВОСТЕЙ З УРАХУВАННЯМ РІВНІВ КРИТИЧНОСТІ КІБЕРІНЦИДЕНТУ/КІБЕРАТАКИ

Загальноприйнятим способом розрахунку небезпеки вразливості у кількісному вираженні є використання метрики CVSS (Common Vulnerability Scoring System) американського Національного інституту стандартів та технологій (NIST).

На цей час вона належить і керується Міжнародним форумом групи реагування на інциденти і безпеку (The Forum of Incident Response and Security Teams, FIRST) (https://www.first.org/). Загальна система оцінки вразливостей — група, що складається з багатьох організацій і приватних осіб, які допомагають розвивати і вдосконалювати систему, спонсорується і підтримується FIRST.

Рейтинги CVSS призначені для використання командами інформаційної безпеки як частина програми управління вразливістю для порівняння та визначення пріоритетів засобів усунення вразливостей.

Серйозності вразливості інформаційної безпеки присвоюється числове значення (за шкалою від 0 до 10) з допомогою Загальної системи оцінки вразливостей (CVSS Scores) (таблиця 1).

Таблиця 1. Рівні критичності за CVSS

Рейтинг рівнів за CVSS 3.0, 3.1 та 4.0	
Якісна оцінка	Кількісна оцінка
Відсутній	0
Низький	0.1 – 3.9
Середній	4.0 – 6.9
Високий	7.0 – 8.9
Критичний	9.0 – 10.0

Ця метрика (показник) дозволяє описати основні особливості вразливості та кількісно оцінити її небезпеку (за шкалою від 0 до 10) залежно від складності експлуатації, впливу на властивості безпеки активу, наявності готового експлойту та його доступності для зловмисника, можливості усунути вразливість, рівня достовірності повідомлення про наявність вразливості, а також у прив'язці до конкретного середовища експлуатації вразливої системи. Оцінки розраховуються на основі формули, яка залежить від кількох метрик, які приблизно описують легкість і вплив експлойту.

CVSS складається з трьох типів показників (рис. 1):

- базові метрики відображають якість вразливості відповідно до її внутрішніх характеристик, які є постійними в часі, під час оцінювання передбачається найгірший вплив у різних розгорнутих середовищах;
- часові метрики регулюють базовий показник вразливості на основі факторів, які змінюються з часом, наприклад, наявності експлойтів, які використовують цю вразливість;
- метрики середовища змінюють базові та часові показники для конкретного обчислювального середовища. Вони розглядають такі фактори, як наявність пом'якшення наслідків у цьому середовищі.

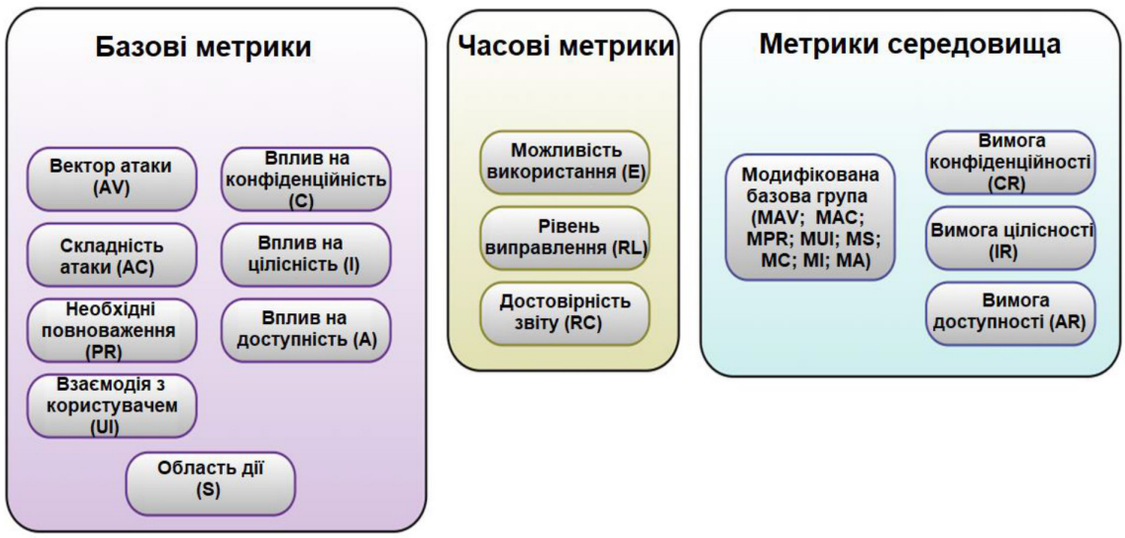

Рисунок 1. Групи метрик (показників) CVSS версії 3.1

У межах стандарту CVSS вводяться два таких базових поняття:

- **вразливий компонент (vulnerable component)** — компонент ІС, що містить уразливість і бере участь у процесі експлуатації;
- **атакуючий компонент (impacted component)** — компонент ІС, базові характеристики безпеки якого (конфіденційність, цілісність, доступність) можуть бути порушені при успішній реалізації атаки.

Як правило, вразливий та атакуючий компоненти збігаються, але існують класи вразливостей, для яких це правило не працює.

Кожна з метрик (показників) характеризується своїм набором значень, які описуються в мнемонічному та числовому вигляді (за рахунок експертного оцінювання) (таблиця 2).

Таблиця 2. Значення показників оцінок CVSS v3.1

Метрична група	Множина метрик	Набори символьних значень метрик		Числові значення метрик
1	2	3		4
Базова	AV	Network (N)	Мережа	0,85
		Adjacent (A)	Сполучена мережа	0,62
		Local (L)	Локальний доступ	0,55
		Physical (P)	Фізичний доступ	0,2
	AC	Low (L)	Низькі	0,77
		High (H)	Високі	0,44
	PR	№ne (N)	Відсутні	0,85
		Low (L)	Середні	0,62 (або 0,68*)
		High (H)	Високі	0,27 (або 0,50*)
	UI	№ne (N)	Відсутня	0,85
		Required (R)	Потрібна	0,62
	S	Unchanged (U)	Без змін	—
		Changed (C)	Змінена	—
	C; I; A	High (H)	Високий	0,56
		Low (L)	Середній	0,22
		№ne (N)	Відсутній	0

Закінчення таблиці 2. Значення показників оцінок CVSS v3.1

1	2	3		4
Часова	E	Nøt 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	Nøt Defined (X)	Не визначені	1
		Unavailable (U)	Відсутня	1
		Workaround (W)	Рішення на основі порад та рекоменд.	0,97
		Temporary Fix (T)	Тимчасове рішення	0,96
		Official Fix (O)	Офіційний патч	0,95
	RC	Nøt Defined (X)	Не визначена	1
		Confirmed (C)	Підтверджена	1
		Reasonable (R)	Обґрунтована	0,96
		UnkNøwn (U)	Відсутня	0,92
Середовище	CR; IR; AR	Nøt Defined (X)	Не визначені	1
		High (H)	Високі	1,5
		Medium (M)	Середні	1
		Low (L)	Низькі	0,5
Модифікована базова	Мають ті ж символьні та числові значення показників, що і відповідні немодифіковані показники в базовій метричній групі, а також «Nøt Defined» (не визначені)			
	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		

Коли аналітик присвоює значення базовим показникам, базове рівняння обчислює оцінку вразливості в діапазоні від 0,0 до 10,0, як наведено на рис. 2.

Зокрема, базове рівняння виводиться з двох підрівнянь: рівняння підрахунку експлуатаційної здатності та рівняння підрахунку впливу. Рівняння підпоказника експлуатаційної здатності отримано з показників базової здатності до використання, а рівняння підпоказника впливу — на основі показників базового впливу.

Потім базову оцінку можна уточнити шляхом підрахунку часових метрик та показників середовища, щоб точніше відобразити відносну серйозність вразливості середовища користувача у конкретний момент часу. Оцінювання часових метрики та показників середовища не є обов'язковим, але рекомендується для більш точних оцінок.

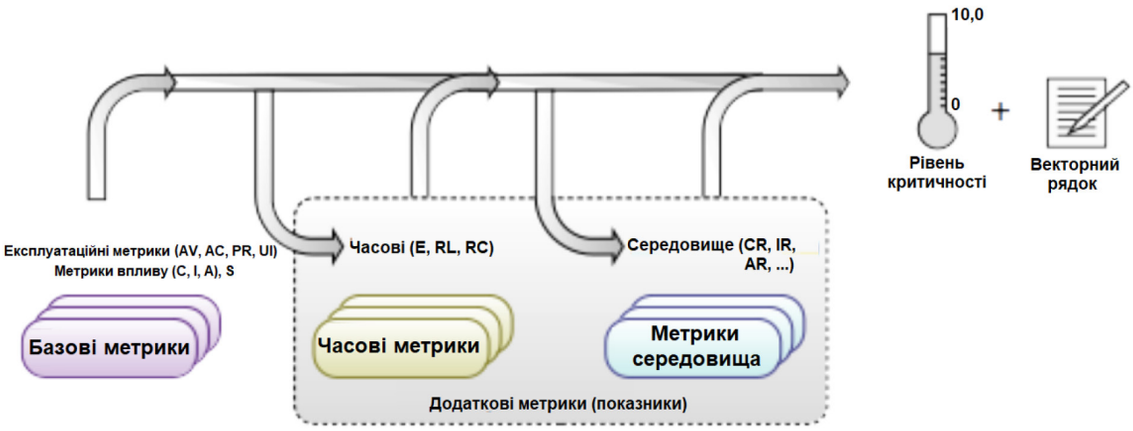

Рисунок 2. Показники та рівняння CVSS версії 3.1

Як правило, базові та часові показники визначаються аналітиками бюлетенів вразливостей, постачальниками продуктів безпеки або постачальниками програм, оскільки вони зазвичай володіють найточнішою інформацією про характеристики вразливості. Показники середовища визначаються організаціями кінцевих користувачів, оскільки вони найкраще можуть оцінити потенційний вплив вразливості у своєму власному комп'ютерному середовищі.

Показники підлягають конкатенації, щоб створити вектор CVSS для вразливості.

Оцінка метрик CVSS також створює векторний рядок, текстове представлення значень метрики, які використовуються для оцінки вразливості. Цей векторний рядок є спеціально відформатованим текстовим рядком, який містить кожне значення, призначене кожній метриці, і завжди має відображатися з оцінкою вразливості.

Рівняння обчислення оцінки вразливості за CVSS визначені таким чином:

– мінімум (Minimum) повертає менший з двох аргументів;

– функція округлення вверх (Roundup) повертає найменше число з точністю до 1 знаку після коми, яке дорівнює або перевищує введене значення. Наприклад, Roundup(4.02) повертає 4.1, а Roundup(4.00) повертає 4.0.

Розрахунок за базовими метриками (BaseScore) залежить від значення показника впливу (Impact Sub-Score, ISS), експлуатаційних метрик та метрик впливу.

$$BaseScore = \begin{cases} \text{якщо } Impact <= 0, & 0 \\ \text{якщо } S = U, & Roundup(Minimum[(Impact + Exploitability), 10]) \\ \text{якщо } S = C, & Roundup(Minimum[1.08 \times (Impact + Exploitability), 10]) \end{cases} \quad (1)$$

де S – значення області дії.

$$Impact = \begin{cases} \text{якщо } S = U, 6.42 \times ISS; \\ \text{якщо } S = C, 7.52 \times (ISS - 0.029) - 3.25 \times (ISS - 0.02)^{15}. \end{cases} \quad (2)$$

$$Exploitability = 8.22 \times AV \times AC \times PR \times UI; \quad (3)$$

$$ISS = 1 - [(1 - C) \times (1 - I) \times (1 - A)], \quad (4)$$

де AV, AC, PR, UI, C, I, A – числові значення метрик базової групи (табл. 2).

Розрахунок за часовими метриками (TemporalScore) здійснюється за формулою

$$TemporalScore = Roundup(BaseScore \times E \times RL \times RC). \quad (5)$$

Формула оцінки впливу на середовище (EnvironmentalScore) залежить від підформул для показника модифікованого впливу (Modified Impact Sub- Score, MISS), модифікованих експлуатаційних метрик та метрик впливу (таблиця 2). Обчислюється за формулою

$$MISS = Minimum(1 - [(1 - CR \times MC) \times (1 - IR \times MI) \times (1 - AR \times MA)], 0.915), \quad (6)$$

де CR, IR, AR — числові значення метрик середовища (таблиця 2);
MC, MI, MA — числові значення модифікованих базових метрик C, I, A.

Модифікація показника впливу (ModifiedImpact) за метриками впливу (2) обчислюється за формулою

$$ModifiedImpact = \begin{cases} \text{якщо } MS = U, & 6.42 \times MISS; \\ \text{якщо } MS = C, & 7.52 \times (MISS - 0.029) - 3.25 \times (MISS \times 0{,}9731 - 0.02)^{13} \end{cases} \quad (7)$$

де MS — значення модифікованої області дії.

Модифікація показника за експлуатаційними метриками (ModifiedExploitability) здійснюється за рахунок зміни формули (3):

$$\text{ModifiedExploitability} = 8.22 \times MAV \times MAC \times MPR \times MUI, \quad (8)$$

де MAV, MAC, MPR, MUI — числові значення модифікованих метрик базової групи (таблиця 2).

Тоді, загальне значення EnvironmentalScore визначатиметься:

$$\text{Якщо } ModifiedImpact <= 0, \text{ то EnvironmentalScore} = 0; \quad (9)$$

$$\text{Якщо MS} = \text{U, то EnvironmentalScore} = Roundup(Roundup[Minimum([ModifiedImpact} + \text{ModifiedExploitability}], 10)] \times E \times RL \times RC)$$

$$\text{Якщо MS} = \text{C, то EnvironmentalScore} = Roundup(Roundup[Minimum(1.08 \times [ModifiedImpact} + \text{ModifiedExploitability}], 10)] \times E \times RL \times RC)$$

Враховуючи обмежену кількість числових результатів (діапазон від 0,0 до 10,0), кілька комбінацій оцінок можуть дати однакову числову оцінку. Крім того, деякі числові показники можуть бути пропущені, оскільки ваги та обчислення отримано з рейтингу серйозності комбінацій показників. Крім того, у деяких випадках комбінації показників можуть відхилятися від бажаного порогу серйозності. Це неминуче, і проста корекція не є легкодоступною, оскільки коригування, внесені до одного метричного значення або параметра рівняння для фіксації відхилення, викликають інші, потенційно більш серйозні відхилення.

Визначення прийнятних числових діапазонів для кожного рівня критичності проводиться за 6-рівневою шкалою із застосуванням для критичного рівня правила "золотого перетину" та розподілу на два підрівня, які відповідають критичному та надзвичайному рівню критичності (табл. 3).

Таблиця 3. Розподіл показників оцінки вразливості за рівнями критичності

Якісна оцінка	BaseScore, TemporalScore, EnvironmentalScore
Не критичний	0
Низький	0.1 – 3.9
Середній	4.0 – 6.9
Високий	7.0 – 8.9
Критичний	9.0 – 9,6
Надзвичайний	9,7 – 10,0

Таким чином, CVSS цілком підходить як стандартна система вимірювань для галузей, організацій та урядів, які потребують точних та послідовних показників щодо вираженої вразливості.

Державна служба
спеціального зв'язку
та захисту інформації
України

НАСТАНОВА З УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ЗА РІВНЯМИ КРИТИЧНОСТІ КІБЕРІНЦИДЕНТІВ

Київ 2026