КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 3 грудня 2025 р. № 1580

Київ

Деякі питання пошуку та виявлення потенційних вразливостей в інформаційно-комунікаційних системах

Відповідно до частини сьомої статті 8 Закону України “Про основні засади забезпечення кібербезпеки України” Кабінет Міністрів України **постановляє**:

1. Затвердити Порядок пошуку та/або виявлення потенційних вразливостей в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також на об’єктах критичної інформаційної інфраструктури, що додається.

2. Внести до Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженого постановою Кабінету Міністрів України від 16 травня 2023 р. № 497 (Офіційний вісник України, 2023 р., № 52, ст. 2911), зміни, що додаються.

Прем’єр-міністр України **Ю. СВИРИДЕНКО**

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 3 грудня 2025 р. № 1580

ПОРЯДОК
пошуку та/або виявлення потенційних вразливостей в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також на об’єктах критичної інформаційної інфраструктури

1. Цей Порядок визначає механізм здійснення пошуку та/або виявлення потенційних вразливостей в інформаційних, електронних комунікаційних, інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, на об’єктах критичної інформаційної інфраструктури (далі — системи).

2. У цьому Порядку термін “сканування системи” означає організаційно-технічний захід з виявлення ризиків кібербезпеки у системі шляхом пасивного або активного пошуку, виявлення та аналізу потенційних вразливостей.

Інші терміни вживаються у значенні, наведеному в Законах України “Про основні засади забезпечення кібербезпеки України”, “Про електронні комунікації”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про Державну службу спеціального зв’язку та захисту інформації України”, Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, затвердженого постановою Кабінету Міністрів України від 16 травня 2023 р. № 497 (Офіційний вісник України, 2023 р., № 52, ст. 2911).

3. Організаційно-технічними заходами з пошуку та/або виявлення потенційних вразливостей в системах є:

збір, аналіз та поширення інформації про вразливості, що здійснюються на постійній основі суб’єктами національної системи реагування на кіберінциденти, кібератаки та кіберзагрози, власниками або розрядниками систем;

сканування систем, які забезпечують розміщення державних інформаційних ресурсів в Інтернеті;

оцінка стану захищеності систем з метою пошуку потенційної вразливості;

впровадження програми пошуку і виявлення потенційних вразливостей за винагороду та узгоджене розкриття вразливостей.

4. Пошук та/або виявлення потенційних вразливостей в системах забезпечується власником або розпорядником системи на постійній основі з моменту введення системи в промислову експлуатацію з урахуванням особливостей, визначених цим Порядком.

Власник або розпорядник системи забезпечує своєчасне виявлення потенційних вразливостей, зокрема шляхом проведення організаційно-технічних заходів, визначених цим Порядком, здійснює в установленому порядку управління вразливостями в рамках виконання базових заходів з кіберзахисту, використовує доступні засоби, механізми і сервіси для виявлення нових вразливостей, своєчасного їх усунення або мінімізації ризиків їх експлуатації.

5. Суб'єкти національної системи реагування на кіберінциденти, кібератаки та кіберзагрози, власники або розрядники систем на постійній основі здійснюють збір, аналіз та поширення інформації про вразливості в системах.

Збір інформації про потенційні вразливості може здійснюватися з будь-яких доступних джерел, зокрема на підставі договорів та інших угод з юридичними або фізичними особами (резидентами або нерезидентами України) або міжнародних договорів, в рамках державно-приватної взаємодії, організаційно-технічних заходів, передбачених цим Порядком, а також інших джерел, не заборонених законодавством.

6. Національна команда реагування на кіберінциденти, кібератаки та кіберзагрози CERT-UA, галузеві та регіональні команди реагування на кіберінциденти, кібератаки та кіберзагрози CSIRT поширюють інформацію про потенційні вразливості та рекомендації щодо їх виявлення, запобігання, усунення і мінімізації потенційних наслідків їх використання в рамках національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та оприлюднюють таку інформацію і рекомендації на власних офіційних веб-сайтах.

7. Власники та розпорядники систем враховують отриману від національної команди реагування на кіберінциденти, кібератаки та кіберзагрози CERT-UA і галузевих та регіональних команд реагування на кіберінциденти, кібератаки та кіберзагрози CSIRT інформацію про потенційні вразливості та з урахуванням наданих рекомендацій здійснюють управління вразливостями в рамках виконання базових заходів з кіберзахисту.

8. Національна команда реагування на кіберінциденти, кібератаки та кіберзагрози CERT-UA інформує Адміністрацію Держспецзв'язку та Ситуаційний центр забезпечення кібербезпеки СБУ про виявлені потенційні вразливості інформаційних, електронних комунікаційних та інформаційно-

комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, а також об’єктів критичної інформаційної інфраструктури із зазначенням обов’язкових та/або рекомендованих заходів реагування для надання вимоги про реагування.

Обов’язкові до виконання вимоги про реагування власникам або розпорядникам систем надаються в межах повноважень СБУ та Адміністрацією Держспецзв’язку — з метою вжиття заходів оперативного реагування на кіберінциденти, кібератаки, кіберзагрози.

9. Сканування систем, які забезпечують розміщення державних інформаційних ресурсів в Інтернеті, здійснюється Державним центром кіберзахисту Держспецзв’язку відповідно до Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених у мережі Інтернет, затвердженого наказом Адміністрації Держспецзв’язку від 15 січня 2016 р. № 20.

10. Сканування систем, які забезпечують розміщення державних інформаційних ресурсів в Інтернеті, проводиться планово згідно з річним планом, який затверджується наказом Адміністрації Держспецзв’язку, або позапланово за письмовим зверненням органу державної влади, іншого державного органу, органу місцевого самоврядування, власника або розпорядника об’єкта критичної інформаційної інфраструктури, оператора критичної інфраструктури.

11. За результатами сканування систем, які забезпечують розміщення державних інформаційних ресурсів в Інтернеті, Державний центр кіберзахисту Держспецзв’язку протягом 15 календарних днів з дня виявлення вразливості повідомляє:

власнику або розпоряднику системи про виявлені вразливості і недоліки у налаштуванні системи з наданням відповідних рекомендацій щодо їх усунення або мінімізації ризику експлуатації вразливості;

національній команді реагування на кіберінциденти, кібератаки та кіберзагрози CERT-UA або галузевим та регіональним командам реагування на кіберінциденти, кібератаки та кіберзагрози CSIRT про виявлені вразливості.

12. Оцінка стану захищеності систем з метою пошуку потенційних вразливостей здійснюється відповідно до порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об’єктів критичної інфраструктури, об’єктів критичної інформаційної інфраструктури, передбаченого частиною третьою статті 5 Закону України “Про основні засади забезпечення кібербезпеки України”.

За результатами оцінки стану захищеності систем суб’єкти оцінювання стану кіберзахисту, які здійснювали оцінку стану захищеності систем відповідно до зазначеного порядку повідомляють власнику або розпоряднику систем, а також національній команді реагування на кіберінциденти, кібератаки та кіберзагрози CERT-UA або відповідним галузевим/регіональним командам реагування на кіберінциденти, кібератаки та кіберзагрози CSIRT про виявлені вразливості.

13. Пошук та/або виявлення потенційних вразливостей в системах, в яких обробляються державні інформаційні ресурси, може здійснюватися відповідно до процедур пошуку і виявлення вразливостей за винагороду та узгодженого розкриття вразливостей, визначених Порядком пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних, затвердженим постановою Кабінету Міністрів України від 16 травня 2023 р. № 497.

14. З метою здійснення інформаційного обміну про вразливості, а також забезпечення сумісності та уніфікації підходів до реєстрації, аналізу та оприлюднення вразливостей національна команда реагування на кіберінциденти, кібератаки та кіберзагрози CERT-UA координує суб’єктів забезпечення кібербезпеки щодо узгодженого розкриття вразливостей та забезпечує взаємодію з Європейською базою вразливостей, адміністрованою Агентством Європейського Союзу з кібербезпеки ENISA.

_____

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 3 грудня 2025 р. № 1580

ЗМІНИ,
що вносяться до Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж

1. Абзац перший пункту 1 після слів “(далі — пошук потенційної вразливості системи)” доповнити словами “шляхом розроблення та проведення програм пошуку і виявлення вразливостей за винагороду та узгодженого розкриття вразливостей”.

2. У пункті 2:

1) абзац другий викласти в такій редакції:

“власник або розпорядник системи (далі — власник системи) — юридична особа будь-якої форми власності та/або фізична особа — підприємець, що на правах власності, оренди або на інших законних підставах здійснює управління системою та відповідає за її поточне функціонування;”;

2) доповнити пункт після абзацу шостого новим абзацом такого змісту:

“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;”.

У зв’язку з цим абзаци сьомий — дванадцятий вважати відповідно абзацами восьмим — тринадцятим;

3) абзац тринадцятий після слів “Про захист інформації в інформаційно-комунікаційних системах” доповнити словами “, “Про Державну службу спеціального зв’язку та захисту інформації України”.

3. У пункті 3:

1) в абзаці другому слова “пошуку потенційної вразливості системи” замінити словами “програм пошуку та виявлення вразливостей системи за винагороду”;

2) в абзаці третьому слова “пошуку потенційної вразливості системи” замінити словами “програми пошуку та виявлення вразливостей системи за винагороду”.

4. Абзац перший пункту 4 після слів “вразливості системи здійснюється” доповнити словом “дослідником”.

5. У пункті 6:

1) абзац п’ятий після слів “внесення змін до системи,” доповнити словами “джерела виплати винагороди”;

2) в абзаці шостому слова “період нерозголошення інформації” замінити словами “умова про нерозголошення або період нерозголошення інформації”;

3) доповнити пункт абзацом такого змісту:

“Залучення послуг організатора та організація програм пошуку потенційних вразливостей системи, а також залучення дослідників може здійснюватися на умовах державно-приватної взаємодії, в тому числі за рахунок джерел, не заборонених законодавством.”.

6. У пункті 7:

1) в абзаці першому слово “може” замінити словами “з дотриманням умов публічної пропозиції має право”;

2) останній абзац після слова “здійснювати” доповнити словами “експлуатацію вразливості,”.

7. Пункт 8 доповнити абзацом такого змісту:

“На підставі даних, викладених у звіті, дослідник одночасно повідомляє про виявлену вразливість національній команді реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA або відповідним галузевим/регіональним командам реагування на кіберінциденти, кібератаки, кіберзагрози CSIRT шляхом подання інформації за формою, розміщеною на їх офіційних веб-сайтах.”.

8. Пункт 10 викласти в такій редакції:

“10. Власник системи та/або організатор перевіряє отриманий звіт на відповідність вимогам, визначеним публічною пропозицією, предмет наявності в ньому інформації про вразливість системи, виявлену раніше іншими дослідниками, вивчає умови та можливі ризики використання виявленої вразливості.

За результатами перевірки звіту власник системи оцінює можливі наслідки використання вразливості системи для її безпеки, порушення сталого, надійного та штатного режиму її функціонування, здійснення несанкціонованого втручання в її роботу, створення загрози для безпеки (захищеності) електронних інформаційних ресурсів, конфіденційності, цілісності, доступності таких ресурсів (далі — наслідки вразливості системи) та приймає рішення щодо внесення або невнесення змін до системи.

Після перевірки звіту власник системи або організатор протягом 30 робочих днів з дати реєстрації такого звіту повідомляє дослідникy, національній команді реагування на кіберінциденти, кібератаки,

кіберзагрози CERT-UA або відповідним галузевим/регіональним командам реагування на кіберінциденти, кібератаки, кіберзагрози CSIRT про прийняте рішення щодо внесення або невнесення змін до системи.

У разі отримання від власника системи або організатора повідомлення щодо невнесення змін до системи дослідник має право після закінчення періоду нерозголошення інформації про вразливість оприлюднити інформацію про виявлену вразливість та її технічні особливості, якщо умовами публічної пропозиції не було передбачено заборону на розголошення інформації про вразливість.”.

9. Абзац четвертий пункту 11 після слів “щодо внесення змін до системи” доповнити словами “, якщо умовами публічної пропозиції не було передбачено заборону на розголошення інформації про вразливість,”.

10. Доповнити Порядок пунктами 12—16 такого змісту:

“12. Узгоджене розкриття вразливостей системи є процесом офіційного поширення інформації про вразливості системи, в яких обробляються державні інформаційні ресурси, з метою подальшого реагування в рамках національної системи реагування на кіберінциденти, кібератаки, кіберзагрози.

13. Дослідник має право без згоди власника системи здійснювати пошук та виявлення вразливостей системи без втручання в її роботу (функціонування) та за умови нездійснення експлуатації вразливості.

За результатами виявлення вразливості дослідник невідкладно, але в будь-якому разі не пізніше 24 годин, надсилає повідомлення про вразливість власнику системи, в якій виявлено вразливість, національній команді реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA або відповідним галузевим/регіональним командам реагування на кіберінциденти, кібератаки, кіберзагрози CSIRT за формою, розміщеною на їх офіційних веб-сайтах. Дослідник має право повідомити про вразливість анонімно або із зазначенням свого псевдоніма.

Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA або галузеві/регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози CSIRT, власники систем, в яких обробляються державні інформаційні ресурси, розміщують на власних офіційних веб-сайтах форму повідомлення про вразливість.

Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA, як координатор узгодженого розкриття вразливостей, визначає форму повідомлення про вразливість.

Форма повідомлення про вразливість повинна містити необхідний мінімум технічної інформації, достатньої для відтворення та перевірки вразливості без здійснення її експлуатації.

14. Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA або галузеві/регіональні команди реагування на

кіберінциденти, кібератаки, кіберзагрози CSIRT, які отримали відповідне повідомлення, передбачене пунктом 13 цього Порядку, від дослідника про виявлену вразливість системи, фіксують дату надходження повідомлення про вразливість, присвоюють йому реєстраційний номер, забезпечують анонімність дослідника у разі, коли дослідник зазначив про таку необхідність під час подання форми, реєструють його із зазначенням дати надходження та присвоєного реєстраційного номера.

Після проведення аналізу вразливості, зокрема оцінки потенційного впливу вразливості на національну систему кібербезпеки, національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA або галузеві/регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози CSIRT здійснюють поширення інформації про вразливість в рамках національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та разом із власником системи вживають заходів реагування в рамках національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, а також у разі потреби ініціюють взаємодію з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, координують подальші дії під час узгодженого розкриття вразливості.

15. Власник системи після отримання повідомлення про вразливість проводить його перевірку та, оцінивши можливі наслідки використання вразливості стосовно системи, приймає рішення щодо внесення або невнесення змін до системи.

16. Публічне поширення інформації про виявлені вразливості за умови отримання згоди власника системи, в якій виявлено вразливість, у разі, коли таке публічне поширення інформації не створює ризиків порушення сталого, надійного та штатного режиму функціонування системи та/або порушення конфіденційності, цілісності, доступності інформації в системі, можуть здійснювати національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA або галузеві/регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози CSIRT, або дослідники, які виявили вразливості.".

11. У тексті Порядку слово "координатор" в усіх відмінках замінити словом "організатор" у відповідному відмінку.
