ЗАТВЕРДЖЕНО

Наказ Державної служби статистики

24 липня 2024 року № 195

Процес управління вразливостями в інформаційній системі органів державної статистики

І. Загальні положення

Процес управління вразливостями (далі – Процес) визначає механізм здійснення пошуку та виявлення потенційної вразливості в інформаційній системі органів державної статистики (далі – ІС ОДС), а також управління життєвим циклом вразливостей кібербезпеки (далі – КБ) з метою проведення їх оцінки, усунення та пом’якшення.

Цей Процес розроблено відповідно до вимог законодавства України.

Цей Процес не поширюється на інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі, в яких обробляється службова інформація та/або інформація, що становить державну таємницю.

У цьому Процесі терміни вживаються у значенні, наведеному в законах України "Про основні засади забезпечення кібербезпеки України", "Про електронні комунікації", "Про захист інформації в інформаційно-комунікаційних системах", Загальних вимогах до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 р. № 518, ДСТУ ISO/IEC 29147:2016 "Інформаційні технології. Методи захисту. Розкриття вразливостей", ДСТУ ISO/IEC 27000:2019 "Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник" та Політиці управління ризиками кібербезпеки.

Цей Процес поширюється на працівників самостійних структурних підрозділів апарату Держстату, його територіальних органів, установ та організацій, що належать до сфери його управління, які відповідальні за функціонування ІТ-активу та мають використовувати своєчасну інформацію про загрози, доступну їм у вигляді оновлень програмного забезпечення, патчів, рекомендацій із КБ, бюлетенів про загрози тощо, а також регулярно перевіряти свої ІТ-активи для превентивного виявлення вразливостей.

Цей Процес не застосовується безпосередньо до користувачів офіційної державної статистичної інформації, яка виробляється та поширюється органами державної статистики, чи інших третіх сторін (наприклад, постачальників робіт і послуг, партнерів), якщо це не зазначено в договірних умовах.

ІІ. Ролі та відповідальність

Діяльність з управління вразливостями в апараті Держстату проводиться відповідно до встановленого плану управління вразливостями (див. пункт 1 розділу ІІІ). Співвідношення ролей та відповідальних працівників апарату Держстату за процес управління вразливостями КБ визначається за формою, наведеною в додатку 1.

Відповідальність за етапи управління вразливостями, описаними в цьому Процесі, покладається на департамент інформаційних технологій та департамент координації процесу збирання даних апарату Держстату (далі – відповідальні самостійні структурні підрозділи).

Керівники відповідальних самостійних структурних підрозділів, як підрозділів, які безпосередньо залучені до технічного обслуговування та підтримки ІТ-активів ІС ОДС, забезпечують:

обізнаність відповідальних працівників про всі відомі загрози або вразливості, які можуть суттєво вплинути на складові ІС ОДС і на будь-які інші її інфраструктурні компоненти шляхом постійного моніторингу відповідних онлайн-ресурсів;

технічне розуміння відповідальних працівників функціонування та побудови відповідних ІТ-активів ІС ОДС;

інформування користувачів апарату Держстату про умови та правила використання наданих їм у користування ІТ-активів;

сканування ІТ-активів ІС ОДС на виявлення вразливостей КБ за допомогою спеціальних інструментів (далі – засоби кіберзахисту), які визначені та дозволені для використання в апараті Держстату, а також за потреби повторного сканування, доки всі "високо пріоритетні" вразливості КБ не будуть усунені (сканування здійснюється щоквартально та після будь-яких значних змін, наприклад, установлення нових ІТ-активів ІС ОДС, зміни топології мережі, зміни правил брандмауера або їх модифікації тощо);

перевірку звітів сканувань задля моніторингу вразливостей КБ і створення пріоритетів результатів сканувань вразливостей;

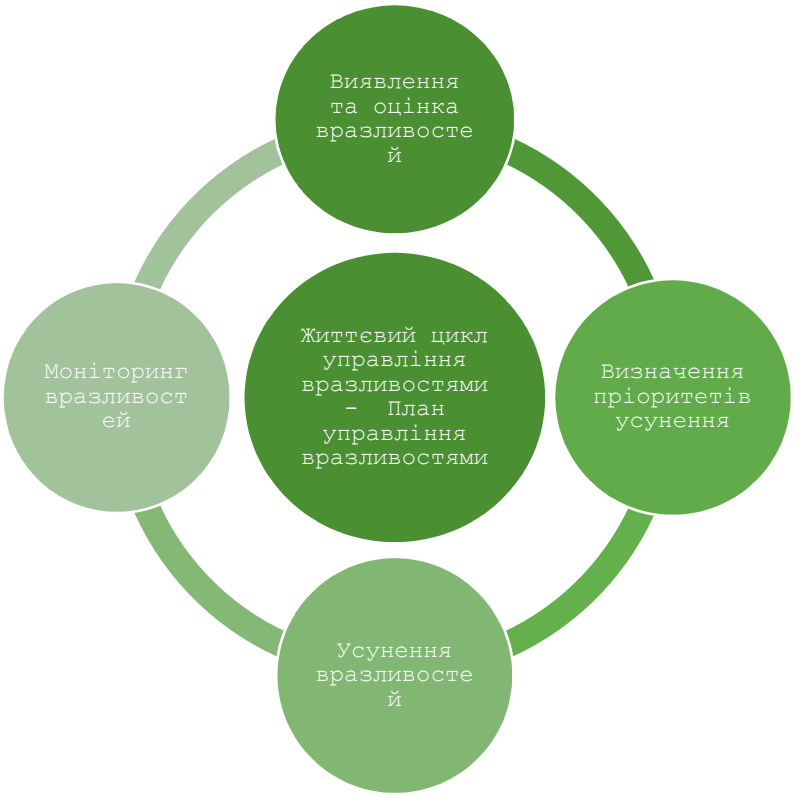
застосування в ІС ОДС оновлень безпеки (відповідно до рівня критичності вразливостей) КБ і виконання інших коригувальних дій;

негайне повідомлення про випадки та масштаби експлуатації вразливостей КБ зловмисниками (про складові ІС ОДС, які постраждали), визначення впливу вразливостей КБ на ІС ОДС у цілому;

ініціацію дій з усунення та/або пом’якшення вразливостей КБ.

ІІІ. Життєвий цикл управління вразливостями

Життєвий цикл управління вразливостями включає діяльність із виявлення та оцінки, пріоритизації, усунення та моніторингу вразливостей:



Діяльність з управління життєвим циклом вразливостей здійснюється згідно з планом управління вразливостями, який складається відповідно до пункту 1 розділу ІІІ цього Процесу.

1. План управління вразливостями:

1) виявлення та оцінка вразливостей.

Держстат може проводити оцінку вразливостей самостійно, а також може залучати третіх сторін (за згодою) згідно із нормами законодавства України, зокрема для оцінки вразливостей відповідно до постанови Кабінету Міністрів України від 16 травня 2023 р. № 497 "Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж".

Відповідальні самостійні структурні підрозділи визначають обсяг і перелік складових ІС ОДС для виявлення вразливостей. Усі складові ІС ОДС, підключені до корпоративної мережі, перевіряються на наявність вразливостей на щомісячній основі та при значних змінах.

Доступ для проведення виявлення вразливостей визначеним працівникам відповідальних самостійних структурних підрозділів має надаватися після погодження з керівником відповідального самостійного структурного підрозділу, а третім сторонам − після погодження з Головою Держстату.

Оцінка вразливостей передбачає поєднання автоматизованого сканування, ручного аналізу та використання даних про загрози для визначення наявності вразливостей КБ у складових ІС ОДС, уключаючи програмне забезпечення.

Відповідальні самостійні структурні підрозділи на постійній основі організовують відстеження повідомлень про вразливості КБ і нові загрози, що стосуються складових ІС ОДС.

Виявлення вразливостей КБ передбачає створення, перегляд та/або доповнення реєстру вразливостей КБ, який складається за формою, наведеною в додатку 2 до цього Процесу, та складання відповідного звіту;

2) визначення пріоритетів усунення вразливостей.

Визначення пріоритетів усунення вразливостей КБ передбачає створення переліку вразливостей КБ, які слід усунути в певному порядку. При визначенні пріоритетності вразливостей керівники відповідальних самостійних структурних підрозділів мають координувати свої дії з робочою групою з управління ризиками (далі − РГУР) КБ, яка визначена в Політиці управління ризиками кібербезпеки та склад якої затверджується наказом Держстату.

З метою визначення пріоритетності усунення виявлених вразливостей КБ звіт про виявлені вразливості КБ опрацьовується РГУР КБ і подається на погодження керівництву Держстату, яке відповідно до розподілу функціональних повноважень уповноважене вирішувати відповідні питання.

Визначення пріоритетів з усунення вразливостей КБ проводиться:

Відповідно до стандарту CVSS (відкритий стандарт, який використовується для передачі інформації про критичність вразливостей. Забезпечує оцінку в діапазоні від 0,0 до 10,0) і на основі інформації про попередні сканування;

Таблиця залежності рейтингу критичності від оцінки CVSS

Оцінка CVSS	Рейтинг критичності
0	Відсутній рейтинг
1–3	Низький рейтинг
4 – 5	Середній рейтинг
6 – 10	Високий рейтинг

Таблиця визначення рейтингу вразливості

Рейтинг вразливості	Опис
A	Критичний. Використання вразливості може завдати шкоди ІС ОДС, а засоби кіберзахисту, спрямовані на запобігання загрозі, відсутні.
B	Високий. Використання вразливості може завдати шкоди ІС ОДС, а засобів кіберзахисту, спрямованих на запобігання загрозі, недостатньо.
C	Середній. Використання вразливості може завдати шкоди ІС ОДС, але засоби кіберзахисту існують, щоб запобігти використанню вразливості.
D	Низький. Використання вразливості не завдасть шкоди ІС ОДС, і впроваджено достатні засоби контролю безпеки.

У цій таблиці засобами кіберзахисту, які використовуються для впровадження організаційно-технічної моделі кіберзахисту, є системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, інформаційні технології, технічні та програмні засоби (пристрої, обладнання, комплекси), які використовуються в інтересах забезпечення кіберзахисту національних електронних інформаційних ресурсів, комунікаційних і технологічних систем, а також об'єктів критичної інформаційної інфраструктури (постанова Кабінету Міністрів України від 29 грудня 2021 р. № 1426 "Про затвердження Положення про організаційно-технічну модель кіберзахисту").

3) усунення вразливостей.

Після оцінки та встановлення пріоритетів усім виявленим вразливостям КБ відповідальні структурні підрозділи сторона уживають заходів щодо усунення вразливостей КБ. Діяльність з усунення вразливостей КБ передбачає їх видалення або пом'якшення.

Для пом'якшення вразливостей можуть проводитися такі дії:

повторне сканування вразливостей КБ, у разі виявлення хибно-позитивних мають бути надані відповідні обґрунтування на основі проведеного сканування для виключення їх зі звіту;

переоцінка вразливостей (за потреби), що включає:

аналіз відповідних ресурсів, які детально описують вразливості КБ;

оцінку можливих ризиків КБ/загроз/впливів;

оцінку слабких місць, заходів безпеки, установленого програмного й апаратного забезпечення.

Для пом'якшення вразливостей відповідальні самостійні структурні підрозділи вживають таких заходів:

якщо вразливості мають високу критичність (високий рейтинг):

установлення відповідного оновлення (високо пріоритетне завдання);

здійснення інших дій для пом'якшення загрози/впливу (високо пріоритетне завдання);

якщо вразливості не можуть бути закриті або їх усунення призведе до додаткового впливу – необхідно повідомити керівництво Держстату, яке згідно з розподілом функціональних повноважень уповноважене вирішувати відповідні питання для затвердження остаточного плану дій;

пом'якшувальні заходи повинні бути застосовані не пізніше, ніж через п'ять днів;

якщо вразливості мають середню або низьку критичність:

для вразливостей середньої критичності необхідно виконати відповідне оновлення складової ІС ОДС не пізніше, ніж через 10 днів;

при низькій критичності повинно встановлюватися оновлення складової ІС ОДС не пізніше, ніж через 15 днів;

якщо вразливості КБ не можуть бути закриті або будь-яке інше рішення призведе до додаткового впливу – необхідно повідомити керівництво Держстату, яке відповідно до розподілу функціональних повноважень уповноважене вирішувати відповідні питання для затвердження остаточного плану дій.

Після застосованих дій/оновлень/будь-яких інших рішень відповідальні самостійні структурні підрозділи мають виконати такі дії:

провести повторне сканування складової ІС ОДС, щоб перевірити, чи існують вразливості КБ;

якщо вразливості КБ все ще існують, виконати дії, що зазначені в цьому етапі з їх усунення;

розробити звіт про пом'якшення виявлених вразливостей.

Після усунення всіх виявлених вразливостей відповідальні самостійні структурні підрозділи мають провести повторне сканування вразливостей відповідно до підпункту 1) пункту 1 розділу ІІІ цього Процесу. Етап усунення вразливостей повинен тривати доти, доки всі вразливості не будуть виправлені або залишковий ризик КБ не буде прийнято керівництвом Держстату, яке згідно з розподілом функціональних повноважень уповноважене вирішувати відповідні питання згідно з Політики управління ризиками кібербезпеки;

4) моніторинг вразливостей.

Процес забезпечення якості існує для перевірки того, що виправлення й оновлення впроваджуються правильно й на всіх відповідних складових ІС ОДС. Моніторинг гарантує, що виправлення правильно усунули виявлені проблеми.

Відповідальні працівники самостійних структурних підрозділів, визначені відповідно до форми додатка 2 до Процесу, мають переконатися, що усунені вразливості більше не впливають на ІТ-активи ІС ОДС або не створюють нових проблем.

Під час цього процесу відповідальні самостійні структурні підрозділи можуть збирати, зберігати й аналізувати дані, які можуть допомогти в подальшому виявити вразливості КБ за допомогою систем управління інформацією та подіями безпеки (SIEM) або інших технологій.

IV. Підтримка, оновлення та розповсюдження

1. Процес є легкодоступним для працівників апарату Держстату для подальшого використання та розміщена на офіційному вебсайті Держстату.

2. РГУР КБ забезпечує організацію оновлення Процесу та подає його до керівництва Держстату відповідно до розподілу функціональних повноважень на затвердження. Процес переглядається щорічно для забезпечення його актуальності та відповідності потребам і цілям захисту ІС ОДС або частіше, якщо це необхідно (під час унесення суттєвих змін).

Заступник директора департаменту
інформаційних технологій Олександра ДОРОХОВА

Додаток 1
до Процесу
(розділ II,
пункт 1 розділу III)

Форма співвідношення ролей і визначених відповідальних працівників за процес управління вразливостями КБ

Роль	Посада	Прізвище, ім’я та по батькові
Відповідальний за ІТ-активи від департаменту інформаційних технологій		
Відповідальний за ІТ-активи від департаменту координації процесу збирання даних		
Відповідальний за ІТ-активи від самостійного структурного підрозділу апарату Держстату		
Керівництво Держстату, яке згідно з розподілом функціональних повноважень уповноважене вирішувати відповідні питання		

_____

Додаток 2
до Процесу
(пункт 1 розділу III)

Форма реєстру вразливостей КБ

№ з/п	Область дії	Уразливість КБ	Посилання на загрози (за наявності)
1	2	3	4
1.	Ідентифікація та аутентифікація	Система неоднозначно ідентифікує й автентифікує користувачів чи процеси	
2.		Система не застосовує парольну політику (складність пароля, мінімальний термін експлуатації та закінчення терміну дії, історію, поріг блокування облікових записів, тривалість блокування облікових записів)	
3.		Система не забезпечує засоби реалізації вимоги до користувача змінити пароль	
4.	Управління доступом	Матриці доступу/список контролю доступу не визначений	
5.		Порушення правил блокування/розблокування ноутбука/ПК/серверу	
6.		Порушення парольної політики (паролі за замовчуванням не змінені, вимоги щодо довжини, складності, періоду використання, правил зберігання не дотримані, неадекватне керування паролями (паролі не зашифровані та легко доступні іншим), використання одного пароля для різних облікових записів)	
7.		Порушення Політики управління доступом для співробітників (перегляд, припинення, надання, керування рівнем доступу, обов’язки не розподілені належним чином)	

1	2	3	4
8.	Обробка інформації та її захист	Перевірки коду безпеки не проводяться для програми, щоб переконатися, що належні елементи керування безпекою присутні, що вони працюють належним чином і що їх було викликано в усіх потрібних місцях	
9.		Мережа, система не захищають передані дані (включаючи зв'язок клієнт-сервер)	
10.		Процес управління змінами є недостатнім	
11.		Недостатній криптографічний захист (криптографічний контроль, керування ключами)	
12.		Порушення Політики управління інцидентами КБ	
13.		Порушення правил використання Інтернету/електронної пошти	
14.		Відсутність фільтрації спаму/фішингу	
15.		Неконтрольоване копіювання/обмін даними	
16.		Порушення політики програмного забезпечення (білий список, дозволи на встановлення)	
17.		Порушення політики захисту від зловмисного коду	
18.		Порушення плану безперервної діяльності	
19.		Порушення правил безпечної утилізації інформації/носіїв (неналежна утилізація конфіденційної інформації (паперової або електронної) видалення в корзину, неповне видалення з хмари, неналежна утилізація носіїв, відсутність контролю за періодом зберігання даних)	
20.	Логування та моніторинг	Система не реєструє всі події доступу	

1	2	3	4
21.		Відсутність контролю над діями адміністратора (реєстрація, огляд, обов'язки контролера не призначаються)	
22.		Відсутність контролю над діями користувача (реєстрація, огляд, обов'язки контролера не призначаються)	
23.		Журнали не зберігаються заздалегідь визначений період часу	
24.		Журнали не захищені	
25.			
26.	Управління патчами	Порушення процесу управління виправленнями (виправлення, пов'язані з безпекою для системи, не оцінюються та не встановлюються протягом визначеного терміну після випуску, виправлення не тестуються перед тим, як їх випустити для повсякденних операцій)	
27.	Управління вразливостями	Сканування вразливостей не виконуються для мережі, систем через регулярні проміжки часу	
28.		Порушення процесу управління вразливостями (відсутність обробки, відсутність перегляду знайдених уразливостей після обробки)	
29.		Тест на проникнення не проводиться для мережі, систем принаймні раз на рік	
30.		Людські помилки, недбалість, порушення внутрішніх правил	
31.	Управління персоналом	Недостатня поінформованість про безпеку та/або тестування	
32.	Аварійне відновлення	Порушення порядку резервного копіювання (частота, безпечне зберігання)	
33.		Відсутність ресурсів для відновлення після катастрофи	
34.	Фізична безпека	Система контролю доступу не записує всі спроби (успішні та невдалі) фізичного доступу до	

1	2	3	4
		приміщень з інформацією про номер картки, дату та час доступу	
35.		Невідповідне управління безпекою кабелів	
36.		Відсутність резервного джерела живлення системи контролю доступу для забезпечення безперебійного електроживлення в разі аварійної ситуації не менше встановленого проміжку часу	
37.		Недостатній рівень послуг з фізичної безпеки	
38.		Відсутність резервного каналу зв’язку	
39.	Юридична	Відсутність або недостатня кількість умов з кібербезпеки у контрактах із третіми сторонами (включаючи NDA, SLA)	
40.		Відсутність регулярних аудитів	
41.	Управління	Відсутність або недостатність регуляторної документації	
42.		Неадекватне управління потужностями/неадекватний контроль над ефективністю роботи (IT-активи, ресурси персоналу)	
43.		Неадекватне призначення керівництвом обов’язків щодо контролю безпеки та управління	
44.		Неадекватна класифікація активів	
45.	Мережева безпека	Порушення правил управління безпекою мережі (незахищені з’єднання публічної мережі, межі не визначаються/не забезпечені належним чином, сегрегація)	