КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 24 березня 2023 р. № 257

Київ

Деякі питання проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури

Відповідно до частини третьої статті 6 Закону України “Про основні засади забезпечення кібербезпеки України” Кабінет Міністрів України **постановляє:**

1. Затвердити Порядок проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури, що додається.

2. Адміністрації Державної служби спеціального зв’язку та захисту інформації забезпечити:

затвердження вимог до аудиторів інформаційної безпеки на об’єктах критичної інфраструктури та порядку їх атестації (переатестації);

проведення аналізу звітів за результатами незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури, надання узагальненої інформації про стан інформаційної безпеки на об’єктах критичної інфраструктури Апарату Ради національної безпеки і оборони України та Кабінетові Міністрів України.

Прем’єр-міністр України **Д. ШМИГАЛЬ**

Інд. 49

ЗАТВЕРДЖЕНО
постановою Кабінету Міністрів України
від 24 березня 2023 р. № 257

ПОРЯДОК
проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури

1. Цей Порядок визначає механізм організації та проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури та вимоги до його проведення.

Метою проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури є оцінка аудитором інформаційної безпеки стану інформаційної безпеки на об’єктах критичної інфраструктури, що повинна відповідати вимогам законодавства у сферах кібербезпеки та захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

Дія цього Порядку не поширюється на:

банки, інші об’єкти, що провадять діяльність на ринку фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, платіжні організації, учасників платіжних систем, операторів послуг платіжної інфраструктури, віднесення яких до критичної інфраструктури здійснюється в порядку, встановленому Національним банком;

діяльність, пов’язану із захистом інформації, що становить державну та розвідувальну таємницю, комунікаційні та технологічні системи, призначені для її оброблення.

2. Терміни, що вживаються в цьому Порядку, мають таке значення:

1) аудитор інформаційної безпеки (далі — аудитор) — фізична або юридична особа, яка пройшла атестацію відповідно до порядку, встановленого Адміністрацією Держспецзв’язку;

2) вразливість — недолік в інформаційній, електронній комунікаційній, інформаційно-комунікаційній системі та/або технологічних системах, що створює імовірність порушення безпеки, сталого, надійного та штатного режиму функціонування таких систем, несанкціонованого втручання в їх роботу, загрозу безпеці (захищеності) електронних інформаційних ресурсів, порушення їх конфіденційності, цілісності, доступності інформаційних ресурсів;

3) звіт за результатами незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури (далі — звіт) — документ, підготовлений аудитором за результатами проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури;

4) інформаційна безпека — це стан захищеності, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та/або технологічних систем, конфіденційність, цілісність та доступність електронних інформаційних ресурсів, а також забезпечується своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз штатного режиму функціонування таких систем і ресурсів, несанкціонованого втручання в їх роботу;

5) незалежний аудит інформаційної безпеки на об’єктах критичної інфраструктури (далі — незалежний аудит) — систематизований, незалежний і документований процес отримання оцінки стану інформаційної безпеки на об’єктах критичної інфраструктури на відповідність вимогам законодавства у сферах кібербезпеки та захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах;

6) ризик — можливість виникнення негативної події та вірогідні масштаби її наслідків протягом певного періоду часу;

7) тестування на проникнення — метод оцінювання захищеності інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та/або технологічних систем шляхом імітування дій щодо несанкціонованого втручання в їх роботу.

Інші терміни вживаються у значенні, наведеному в Кодексі цивільного захисту України, в Законах України “Про інформацію”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про основні засади забезпечення кібербезпеки України”, “Про критичну інфраструктуру”, в Загальних вимогах до кіберзахисту об’єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 р. № 518 (Офіційний вісник України, 2019 р., № 50, ст. 1697).

3. Проведення незалежного аудиту є обов’язковим для об’єктів критичної інфраструктури та забезпечується операторами критичної інфраструктури.

4. Незалежний аудит проводиться відповідно до умов договору, укладеного між оператором критичної інфраструктури і аудитором.

5. Між оператором критичної інфраструктури і аудитором укладається договір про нерозголошення конфіденційної інформації, отриманої для проведення незалежного аудиту.

6. Незалежний аудит проводиться:

не рідше ніж один раз на два роки для об’єктів I та II категорії критичності;

не рідше ніж один раз на три роки для об’єктів III категорії критичності;

невідкладно, у разі настання кризової ситуації на об’єкті критичної інфраструктури.

7. Оператор критичної інфраструктури має право самостійно обирати аудитора для проведення незалежного аудиту.

Оператор критичної інфраструктури не може залучати до проведення незалежного аудиту одного і того самого аудитора двічі підряд.

8. Проводити незалежний аудит мають право аудитори, які пройшли атестацію в порядку, встановленому Адміністрацією Держспецзв’язку.

Аудитор проводить незалежний аудит відповідно до вимог цього Порядку.

Аудитор може залучати до проведення незалежного аудиту інших аудиторів за згодою з оператором критичної інфраструктури, на яких поширюються всі вимоги, передбачені цим Порядком.

9. Проведення незалежного аудиту здійснюється такими етапами:

1) організація проведення незалежного аудиту, що передбачає визначення об’єкта аудиту (інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та/або технологічних систем);

2) вибір аудитора, визначення процедур і методик проведення незалежного аудиту;

3) підготовка аудитором програми проведення незалежного аудиту та її погодження з оператором критичної інфраструктури;

4) збір необхідної інформації незалежного аудиту та її аналіз;

5) підготовка звіту за результатами незалежного аудиту.

10. Аудитор використовує узгоджені з оператором критичної інфраструктури:

критерії оцінки захищеності інформації, що враховують вимоги законодавства у сферах кібербезпеки та захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, а також особливості об’єкта критичної інфраструктури;

програму, процедури, методики проведення незалежного аудиту та спеціалізовані програмно-апаратні засоби для тестування на проникнення з урахуванням необхідності забезпечення функціональності, безперервності роботи, відновлюваності, цілісності і стійкості об’єкта критичної інфраструктури.

11. Під час проведення незалежного аудиту аудитор:

1) використовує попередні звіти незалежного аудиту (за наявності) та аналізує системні журнали та журнали реєстрації подій програмного і програмно-апаратного забезпечення (за наявності);

2) проводить анкетування (інтерв'ю) працівників оператора критичної інфраструктури в рамках аудиту;

3) використовує загальне та/або спеціалізоване ліцензійне програмне забезпечення для пошуку вразливостей, перевірки властивостей, характеристик та функцій в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах та/або технологічних системах;

4) аналізує технічну документацію та документацію користувача, рекомендації постачальника компонентів інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем та/або технологічних систем (за наявності);

5) аналізує налаштування інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем;

6) узагальнює отриману інформацію про стан інформаційної безпеки на об'єкті критичної інфраструктури і перевіряє її на відповідність вимогам законодавства у сферах кібербезпеки та захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

12. Аудитор під час проведення незалежного аудиту має право:

отримувати від оператора критичної інфраструктури, а також його працівників необхідну інформацію, що стосується незалежного аудиту, в усній чи письмовій формі;

ознайомлюватися з необхідними документами, що стосуються питань аудиту, які перебувають у оператора критичної інфраструктури;

звертатися за необхідною інформацією до третіх осіб, які мають у своєму розпорядженні документи стосовно питань перевірки, за згодою з оператором критичної інфраструктури.

13. Аудитор під час проведення незалежного аудиту зобов'язаний:

1) дотримуватися вимог цього Порядку та інших актів законодавства у сферах кібербезпеки та захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах;

2) повідомляти операторам критичної інфраструктури, уповноваженим ними особам про виявлені під час проведення незалежного аудиту вразливості інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем та/або технологічних систем/або критичних технологічних процесів, а також забезпечення пропорційності та/або співрозмірності заходів реальним та потенційним ризикам;

3) не розголошувати та не використовувати у своїх інтересах або інтересах третіх осіб інформацію, отриману під час проведення незалежного аудиту;

4) повідомляти оператору критичної інфраструктури про виникнення реального, потенційного конфлікту інтересів.

14. Доступ аудиторам до інформації з обмеженим доступом надається оператором критичної інфраструктури відповідно до законодавства.

15. За розголошення інформації з обмеженим доступом, отриманої під час проведення незалежного аудиту, аудитор несе відповідальність відповідно до закону.

16. За результатами незалежного аудиту аудитором не пізніше ніж протягом 14 робочих днів після його завершення складається звіт за формою згідно з додатком.

Звіт підписується аудитором та оператором критичної інфраструктури.

Якщо оператор критичної інфраструктури не погоджується із звітом, він підписує його із зауваженнями, які є невід'ємною частиною такого звіту.

У разі залучення до проведення незалежного аудиту інших аудиторів, звіт підписується усіма аудиторами, що його проводили.

Звіт може містити інформацію з обмеженим доступом.

17. Оператор критичної інфраструктури надає Адміністрації Держспецзв'язку та СБУ копію звіту протягом 30 робочих днів з дати отримання його від аудитора.

_____

Додаток
до Порядку

ЗВІТ
незалежного аудиту інформаційної безпеки на об’єкті критичної інфраструктури

_____

(найменування об’єкта критичної інфраструктури, на якому проводився незалежний аудит,

_____

найменування оператора критичної інфраструктури, місцезнаходження, код згідно з ЄДРПОУ**)**

_____

Аудитори _____

(найменування юридичних осіб та/або

_____

прізвище, власне ім’я та по батькові (за наявності) фізичних осіб,

_____

які проводили незалежний аудит, код згідно з ЄДРПОУ)

на підставі укладеного договору між оператором критичної інфраструктури і аудитором _____

(назва укладеного договору,

_____

згідно з яким проводився незалежний аудит,

_____

дата, реєстраційний номер та місце укладення договору)

у присутності _____

(найменування посади, прізвище, власне ім'я та по батькові (за наявності)

_____

посадової особи оператора критичної інфраструктури та працівників об’єкта критичної інфраструктури)

у період з _____ _____ 20___ р. по ____ _____ 20___ р. проведено незалежний аудит інформаційної безпеки на об’єкті критичної інфраструктури

1. Мета проведення незалежного аудиту інформаційної безпеки _____

(встановлена оператором об’єкта критичної інфраструктури мета проведення

_____

незалежного аудиту)

2. Додаткові умови проведення аудиту _____

_____

(зазначаються компоненти і підсистеми, що стосуються проведення аудиту,

_____
розміщення комплексу програмно-технічних засобів систем за майданчиками (приміщеннями),

_____
основні класи загроз інформаційній безпеці, що розглядаються в ході проведення аудиту)

3. Опис інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем _____
(призначення і основні функції систем,

_____
групи завдань, які вирішуються

_____
в системі, класифікація користувачів систем, організаційна структура обслуговуючого персоналу

_____
систем, структура і склад комплексу програмно-технічних засобів систем,

_____
види інформаційних ресурсів, що обробляються в системах, структура інформаційних потоків,

_____
характеристика каналів взаємодії з іншими системами тощо)

4. Програма та методики проведення аудиту _____
(зазначається програма

_____
та методика проведення аудиту)

5. Забезпечення відповідності об’єкта критичної інфраструктури вимогам законодавства _____
(виконання оператором об’єкта

_____
критичної інфраструктури вимог законодавства у сфері захисту інформації в інформаційних,

_____
електронних комунікаційних та інформаційно-комунікаційних системах, у сфері кібербезпеки,

_____
Загальних вимог до кіберзахисту об’єктів критичної інфраструктури)

6. Результати тестування на проникнення в інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних системах _____
(середовище тестування, опис та класифікація виявлених вразливостей,

_____
оцінка рівня захищеності,

_____
рекомендації щодо усунення виявлених вразливостей)

7. Аналіз ризиків, пов’язаних із загрозами інформаційній безпеці

_____
(політика безпеки організації,

_____

модель загроз інформаційній безпеці і вразливостей інформаційних ресурсів,

_____

оцінка загроз і вразливостей, оцінка ризиків для кожного класу загроз та групи ресурсів)

Висновок _____

(зазначаються вжиті оператором критичної інфраструктури заходи

_____

до забезпечення захищеності об'єкта аудиту)

Рекомендації _____

(опис заходів, які рекомендується застосувати для мінімізації загроз

_____

інформаційній безпеці, рекомендації щодо обробки (уникнення, зменшення, перекладання

_____

чи прийняття) ризиків інформаційної безпеки) та усунення існуючих недоліків)

_____	_____	_____
(найменування посади фізичної особи, яка проводила незалежний аудит)	(підпис)	(власне ім'я та прізвище)

Із звітом ознайомлений

_____	_____	_____
(найменування посади керівника оператора критичної інфраструктури)	(підпис)	(власне ім'я та прізвище)

У разі незгоди керівника оператора критичної інфраструктури з викладеними у звіті фактами чи висновками оператор критичної інфраструктури власноручно після фрази "Із звітом ознайомлений" робить допис "із зауваженнями" та ставить підпис про ознайомлення. Зауваження викладаються на окремих аркушах у довільній формі та є невідємною частиною звіту.

_____