МІНІСТЕРСТВО РОЗВИТКУ ГРОМАД ТА ТЕРИТОРІЙ УКРАЇНИ
пр-т Берестейський, 14, м. Київ, 01135,
тел.: (044) 351-40-96, (044) 351-40-35, (044) 351-40-01,
E-mail: miu@mtu.gov.ua, сайт: www.mtu.gov.ua, код згідно з ЄДРПОУ 37472062

від _____ 20__ р. № _____ На № _____ від _____ 2025 р.

Обласні, Київська міська військові адміністрації, оператори критичної інфраструктури
(за списком розсилки)

Міністерство розвитку громад та територій України відповідно до пункту 5 протокольного рішення наради з питань забезпечення фізичного та радіоелектронного захисту об'єктів розподіленої генерації, що відбулася 20.01.2025 під головуванням Секретаря Ради національної безпеки і оборони України Литвиненка О.В. стосовно надання операторам критичної інфраструктури рекомендацій щодо поводження та використання чутливої інформації стосовно об'єктів критичної інфраструктури повідомляє таке.

Наразі в Україні йде війна не тільки фізично, але й інформаційно. В цей час пильність та обачність потребує особливої уваги, для недопущення ситуацій витоку чутливої інформації. Хакерські атаки та інші форми цифрових загроз усе частіше спрямовані на викрадення важливих даних.

Інформація вже давно стала стратегічним активом, тож захист даних є життєво необхідним. Витік інформації може коштувати занадто дорого, а нехтування політиками конфіденційності можуть призвести до серйозних наслідків.

У Законі України «Про критичну інфраструктуру» (далі – Закон) наявні норми, які визначають зміст відомостей у сфері захисту критичної інфраструктури, що повинні належати до інформації з обмеженим доступом.

Зокрема, у Законі вказано, що: відомості, що містяться у паспорті безпеки, є інформацією з обмеженим доступом, вимога щодо захисту якої встановлена законом (ч. 7 ст. 12 Закону); уповноважений орган у сфері захисту критичної інфраструктури України розробляє та затверджує Проектні загрози критичній інфраструктурі національного рівня, що становлять інформацію з обмеженим доступом (п. 10 ч. 2 ст. 16 Закону); пропозиції щодо удосконалення системи

захисту об'єктів критичної інфраструктури, підготовлені за результатами моніторингу оцінки стану захищеності, є інформацією з обмеженим доступом (ч. 3 ст. 23 Закону).

Також у частині шостій статті 11 Закону передбачено, що інформація про об'єкти критичної інфраструктури, що міститься в Реєстрі об'єктів критичної інфраструктури, є відкритою, загальнодоступною та безоплатною, крім інформації з обмеженим доступом.

Відповідно до пункту 8 Порядку віднесення об'єктів до критичної інфраструктури, затвердженого постановою Кабінету Міністрів України від 09.10.2020 № 1109, відомості про об'єкти критичної інфраструктури, що містяться у секторальних переліках об'єктів критичної інфраструктури, є інформацією з обмеженим доступом, захист якої забезпечується відповідно до вимог законодавства.

Пунктами 12 та 13 Порядку ведення Реєстру об'єктів критичної інфраструктури, включення таких об'єктів до Реєстру, доступу та надання інформації з нього, затвердженого постановою Кабінету Міністрів України від 28.04.2023 № 415, визначено яка інформація про об'єкт критичної інфраструктури у Реєстрі віднесена до відкритої інформації та до інформації з обмеженим доступом.

Крім того, обмеження доступу до інформації здійснюється при дотриманні сукупності вимог, визначених частиною другою статті 6 Закону України «Про доступ до публічної інформації».

Важливо наголосити, що згідно із Законом правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури є складовою законодавства у сфері національної безпеки.

Основні загрози для витоку інформації:

1. Недобросовісність співробітників: один із найпоширеніших ризиків – навмисне розголошення інформації працівниками.

2. Випадкове розголошення: іноді працівниками можуть розкрити конфіденційну інформацію ненавмисно, через недостатнє усвідомлення правил безпеки.

3. Інсайдерські ризики: ситуації, коли працівники навмисно зловживають своїм доступом до інформації, передають важливі дані третім особам.

4. Відсутність контролю за доступом до інформації: неналежна організація системи доступу до даних.

5. Кіберзлочини: використання шкідливого програмного забезпечення (віруси, трояни), фішингові атаки для отримання паролів чи іншої чутливої інформації, злом корпоративних систем з метою заволодіння даними.

6. Корпоративне шпигунство: наймання інформаторів серед співробітників ОКІ, використання спеціальних технічних засобів для перехоплення даних,

проникнення на територію ОКІ для збору документів чи обладнання – пряма крадіжка.

З огляду на зазначене, неналежне поводження та використання інформації про об'єкти критичної інфраструктури може завдати істотної шкоди національним інтересам, спричинити переривання чи порушення надання життєво важливих функцій та/або послуг об'єктами критичної інфраструктури та призвести до загроз національній безпеці. Тому запровадження ефективних заходів для захисту чутливої інформації стає пріоритетним завданням, а її захист є вкрай важливим.

Ураховуючи викладене, пропонуємо зазначену інформацію розповсюдити серед операторів критичної інфраструктури секторів транспорту і пошти та системи життєзабезпечення.

Заступник Міністра з питань
цифрового розвитку, цифрових
трансформацій і цифровізації

Андрій БРАТУСЬ

Юрій Михайлов 351 41 19