Державна служба
спеціального зв'язку та захисту
інформації України

Державна політика з кіберзахисту: досягнення та виклики на регіональному рівні

т.в.о. директора Департаменту кіберзахисту
Адміністрації Держспецзв’язку
Дмитро ПАХОЛЬЧЕНКО

Закон України № 4336-IX
від 27 березня 2025 року

НАЦІОНАЛЬНІ СИСТЕМИ РЕАГУВАННЯ ТА ОБМІНУ ІНФОРМАЦІЄЮ

функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози

реагування в кризовій ситуації в кібербезпеці

функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози

КАДРОВИЙ ПОТЕНЦІАЛ

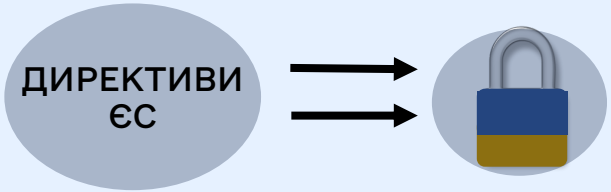
введення штатних посад керівників та фахівців з кібербезпеки в державних органах, а також на об’єктах критичної інфраструктури

Ключові зміни

РИЗИК МЕНЕДЖМЕНТ

відмова від КСЗІ та визначення процесу впровадження заходів з управління ризиками і забезпечення того, щоб такі заходи підтримувалися протягом життєвого циклу систем на основі профілів безпеки

функціонування системи оцінювання стану кіберзахисту включно з методом аудиту без надмірного контролю з боку держави



ЦІЛЬ: імплементація норм європейських директив з кібербезпеки до національного законодавства

Постанови КМУ

Закон України № № 4336-IX від 27 березня 2025 року

1. № 1281 від 08.10.2025: «Деякі питання проведення інструктажів та систематичних тренінгів щодо кібергігієни»
2. № 1470 від 13.11.2025: «Про внесення змін до постанови Кабінету Міністрів України від 19 червня 2019 р. № 518»
3. № 1471 від 13.11.2025: «Про затвердження Порядку взаємодії суб'єктів національної системи реагування із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами, суб'єктами оперативно-розшукової діяльності»
4. № 1516 від 26.11.2025: «Про затвердження Порядку призначення керівника з кіберзахисту на посаду в органі державної влади»
5. № 1531 від 26.11.2025: «Про внесення змін до постанови Кабінету Міністрів України від 29 березня 2006 р. № 373»
6. № 1533 від 26.11.2025: «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози»
7. № 1580 від 03.12.2025: «Деякі питання пошуку та виявлення потенційних вразливостей в інформаційно-комунікаційних системах»

Порядок призначення керівника з кіберзахисту на посаду в органі державної влади

Постанова КМУ № 1516 від 26.11.2025
Наказ АД № 798 від 03.12.2025

Методичні рекомендації щодо типових вимог до підрозділів, загальних вимог до керівників з кіберзахисту в ОДВ, а також до відповідальних осіб, які виконують функції та завдання керівника з кіберзахисту...

Розмежування повноважень

CISO (кіберзахист)

≠

CDTO (цифрова трансформація)

- Посади не можуть поєднуватись
- У підпорядкуванні підрозділ з кіберзахисту

Вимоги до компетентності

Освіта

Вища освіта у сферах IT

Досвід роботи

Стаж у сфері кібербезпеки або IT не менше 3 років

Професійні знання

Процедура погодження

Адміністрація Держспецзв'язку

Оцінює професійну компетентність та відповідність вимогам

СБУ

Проводить перевірку та аналізує можливі ризики національній безпеці

Зміни до постанови Кабінету Міністрів України від 19 червня 2019 р. № 518

Постанова КМУ № 1470 від 13 листопада 2025 року

ОСНОВНА ТЕЗА

кібербезпека ОКІ забезпечується операторами КІ та власниками або керівниками ОКІІ

заходи кіберзахисту здійснюються з урахуванням результатів управління ризиками кібербезпеки

01 Суб'єкт оцінює фактичний стан організації та впровадження заходів кіберзахисту.

Результати фіксуються в Плані кіберзахисту

02 Після проведення оцінки ризиків кібербезпеки суб'єкт визначає для себе всі необхідні заходи кібербезпеки, беручи їх із загального каталогу заходів кіберзахисту. При цьому обов'язковими є базові заходи (близько 60), що входять до складу каталогу

03 Суб'єкт зазначає весь перелік необхідних заходів кіберзахисту в плані кіберзахисту. Це буде його запланований цільовий стан, до якого суб'єкт буде рухатися

04 Суб'єкт досягає цільового стану кіберзахисту поступово і послідовно, впроваджуючи заходи кіберзахисту, зазначені в плані кіберзахисту

Державна служба спеціального зв'язку та захисту інформації України

Зміни до постанови Кабінету Міністрів України від 29 березня 2006 р. № 373

Постанова КМУ № 1531 від 26.11. 2025

Заходи кіберзахисту з урахуванням результатів управління ризиками кібербезпеки	Усі базові заходи з кіберзахисту є обов'язковими до здійснення	**Оцінювання стану кіберзахисту**	План кіберзахисту розробляється з урахуванням управління ризиками кібербезпеки на основі каталогу заходів і включає описи поточного та/або цільового стану кіберзахисту	План кіберзахисту затверджується, щороку переглядається та оновлюється
Базові заходи кіберзахисту	Каталог заходів з кіберзахисту, базові заходи з кіберзахисту, форма плану кіберзахисту, затверджуються Адміністрацією Держспецзв'язку	Оцінювання стану кіберзахисту відбувається відповідно до порядку, з урахуванням каталогу заходів, особливостей функціонування та архітектури	Цільовий стан кіберзахисту досягається поетапно та послідовно	**План кіберзахисту**

Реагування на кіберінциденти, кібератаки та кіберзагрози

Постанова КМУ № 1533 від 26.11.2025

Дія Національного плану поширюється на:

основних суб'єктів національної системи кібербезпеки	ОДВ, ОМС	власників або розпорядників ОКІІ
суб'єктів національної системи реагування	операторів критичної інфраструктури	інших суб'єктів забезпечення кібербезпеки

загальні процедури реагування на кіберінциденти, кібератаки, кіберзагрози

механізм координації та взаємодії між суб'єктами національної системи реагування та суб'єктами забезпечення кібербезпеки

роль суб'єктів національної системи реагування в рамках функціонування національної системи реагування

роль суб'єктів національної системи реагування в рамках функціонування національної системи обміну інформацією

Етапи реагування

Рівень	Назва	Характеристика та вплив
Рівень 0	Некритичний (білий)	Не загрожує сталому функціонуванню систем
Рівень 1	Низький (зелений)	Загрожує функціонуванню, але не загрожує даним (збережено цілісність, конфіденційність і доступність)
Рівень 2	Середній (жовтий)	Створює передумови для порушення захищеності інформації та даних
Рівень 3	Високий (помаранчевий)	Загрожує функціонуванню систем, порушується захищеність інформації та даних, виникають потенційні загрози для національної безпеки і оборони, … , припинення виконання функцій ОКІ
Рівень 4	Критичний (червоний)	Загрожує функціонуванню кількох систем, порушується захищеність, виникають реальні загрози для національної безпеки і оборони, … , припинення виконання функцій ОКІ
Рівень 5	Надзвичайний (чорний)	Загрожує функціонуванню багатьох систем, порушується захищеність, виникають невідворотні загрози для функціонування держави або загроза життю людей

Порядок взаємодії суб'єктів національної системи реагування

Постанова КМУ № 1471 від 13.12. 2025

КЛЮЧОВІ СУБ'ЄКТИ МЕХАНІЗМУ ВЗАЄМОДІЇ

- CERT-UA – силові структури
- Галузеві та регіональні CSIRTs – силові структури та інші суб'єкти національної системи реагування
- Національна поліція та СБУ – інші суб'єкти національної системи реагування

ОБМІН ІНФОРМАЦІЄЮ

про кіберінциденти, кібератаки, кіберзагрози

СПІЛЬНІ ДІЇ

під час реагування на кіберінциденти, кібератаки, кіберзагрози

ДОСТУП ДЛЯ РОЗСЛІДУВАНЬ

надання та отримання в установленому законодавством порядку доступ до технічних та інших деталей кіберінциденту та кібератаки, для проведення слідчих або оперативно-розшукових заходів

МІЖВІДОМЧІ ГРУПИ

із реагування на кіберінциденти, кібератаки, кіберзагрози або кризову ситуацію у сфері кібербезпеки

Національна система обміну інформацією

Національний, галузеві, регіональні, приватні CSIRT інформують

НКЦК

Про всі значні кіберінциденти / кібератаки

СБУ

Про значні кіберінциденти, кібератаки, кіберзагрози, вразливості

Інформує інших суб'єктів про актуальні кіберзагрози у сфері державної безпеки

Нацполіція

Про значні кіберінциденти щодо ОКІІ

Інформує інших суб'єктів про організацію, сили, засоби, методи, тактику дій злочинних угрупувань

Розвідувальні органи

Про зовнішні кіберзагрози

Інформують інших суб'єктів про зовнішні загрози національній безпеці у кіберпросторі

ДБР

Про кіберінциденти / кібератаки, якщо в ході реагування є ознаки кримінального правопорушення

НАБУ

Про кіберінциденти / кібератаки, якщо в ході реагування є ознаки кримінального правопорушення

БЕБ

Про кіберінциденти / кібератаки, якщо в ході реагування є ознаки кримінального правопорушення

Національна система обміну інформацією

Пошук та виявлення потенційних вразливостей

Постанова КМУ № 1580 від 03.12.2025

СФЕРА ЗАСТОСУВАННЯ

- Для ІКС, в яких обробляються ДІР або ІзОД, вимога щодо захисту якої встановлена законом;
- Для ОКІІ

ВІДПОВІДАЛЬНІСТЬ

Пошук вразливостей забезпечується власником або розпорядником системи **на постійній основі** з моменту введення системи в промислову експлуатацію

СКАНУВАННЯ СИСТЕМ

Здійснюється ДЦКЗ згідно з річним планом або позапланово за зверненням

Збір, аналіз, поширення інформації про вразливості, що здійснюються на постійній основі

Оцінка стану захищеності систем з метою пошуку потенційної вразливості

Сканування систем, які забезпечують розміщення державних інформаційних ресурсів в Інтернеті

Впровадження програми пошуку і виявлення потенційних вразливостей за винагороду та узгоджене розкриття вразливостей

Інструктажі та тренінги з кібергігієни

Державна служба спеціального зв'язку та захисту інформації України

Постанова КМУ № 1281 від 8 жовтня 2025 року

СФЕРА ЗАСТОСУВАННЯ ТА МЕТА

ДЛЯ КОГО?

Для членів Кабінету Міністрів України, народних депутатів України, працівників патронатних служб, депутатів місцевих рад, посадових осіб органів місцевого самоврядування, державних службовців, військовослужбовців, працівників органів державної влади, інших державних органів, керівників та працівників державних підприємств, установ та організацій

ЦІЛЬ?

підвищення стійкості державних органів до кібератак

РЕЗУЛЬТАТ?

формування практичних навичок безпечної поведінки в кіберпросторі та захисту персональних даних

ХТО МОЖЕ ПРОВОДИТИ ІНСТРУКТАЖІ ТА ТРЕНІНГИ

ВНУТРІШНІ ПІДРОЗДІЛИ

відповідальні особи підрозділів з кіберзахисту самої установи

ОСНОВНІ СУБ'ЄКТИ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ

Держспецзв'язку, СБУ, Національна поліція та інші

ЗОВНІШНІ ЕКСПЕРТИ

зовнішні експерти, які надають послуги у сфері кіберзахисту, на договірній основі

Ключові завдання в регіонах

Якщо ОДВ – призначити керівника з кіберзахисту; якщо ОМС – призначити відповідальних осіб, які виконують функції та завдання керівника з кіберзахисту

Невідкладно

Авторизувати системи з безпеки / отримати сертифікат відповідності стандарту інформаційної безпеки

Проводити тренінги щодо кібергігієни

Щорічно, після призначення на посаду, після значного кіберінциденту

Створити регіональний CSIRT

За потреби або залучати приватні CSIRT / регіональні центри кіберзахисту Держспецзв'язку

Здійснювати заходи з кіберзахисту, управління ризиками кібербезпеки, реагування на кіберінциденти, обміну інформацією

Постійно

Затвердити план кіберзахисту, план реагування на кіберінциденти, внутрішні політики кібербезпеки

Невідкладно, щороку перегляд

Державна служба
спеціального зв'язку та захисту
інформації України

Питання та пропозиції?

Пахольченко Дмитро
Департамент кіберзахисту Адміністрації Держспецзв’язку
e-mail: d.pakholchenko@ws.cip.gov.ua