

АНАЛІЗ РЕГУЛЯТОРНОГО ВПЛИВУ
проекту наказу Міністерства охорони здоров'я України
«Про затвердження галузевих вимог з кіберзахисту об'єктів критичної
інфраструктури сектору «охорона здоров'я»

I. Визначення проблеми

В умовах зростання кількості кіберзагроз та активізації кібератак на інформаційно-комунікаційні системи державного сектору особливого значення набуває забезпечення належного рівня кіберзахисту об'єктів критичної інфраструктури сектору «охорона здоров'я» (далі – ОІ).

Специфіка функціонування сфери охорони здоров'я обумовлена необхідністю забезпечення безперервності надання медичної допомоги населенню, обробкою значних обсягів персональних даних та даних про стан здоров'я пацієнтів, використанням електронної системи охорони здоров'я, медичних інформаційних систем, а також інших інформаційно-комунікаційних систем, що забезпечують діяльність закладів охорони здоров'я.

Водночас на сьогодні тільки розроблюється єдиний галузевий підхід до організації та реалізації заходів кіберзахисту ОІ, який би враховував особливості функціонування зазначеної сфери та забезпечував уніфіковане застосування вимог законодавства у сфері кібербезпеки.

Відсутність такого підходу може призвести до неоднакового застосування вимог законодавства операторами ОІ, виникнення ризиків порушення безперервності надання медичної допомоги, зниження рівня захисту інформаційних ресурсів, а також створення передумов для компрометації персональних даних і державних інформаційних ресурсів, що обробляються в інформаційно-комунікаційних системах сфери охорони здоров'я.

Проблема не може бути розв'язана шляхом застосування виключно рекомендаційних механізмів, оскільки забезпечення єдиного підходу до впровадження заходів кіберзахисту потребує нормативного врегулювання та встановлення обов'язкових для виконання вимог у межах компетенції Міністерства охорони здоров'я України.

У свою чергу, можливість розробляти галузеві вимоги з кіберзахисту з урахуванням секторальної (галузевої) специфіки функціонування ОІ визначена вимогами законодавства, зокрема, пункту 11 Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (в редакції постанови Кабінету Міністрів України від 13 листопада 2025 року № 1470) та Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту, затверджених наказом Адміністрації Держспецзв'язку від 30 січня 2026 року № 75.

Таким чином, прийняття проєкту акта створить правові передумови для уніфікації підходів щодо забезпечення кіберзахисту ОКІ, підвищення рівня захищеності персональних даних і державних інформаційних ресурсів, забезпечення безперервності надання медичної допомоги та формування єдиного підходу до виконання вимог законодавства у сфері кібербезпеки.

Основні групи (підгрупи), на які проблема справляє вплив:

Групи (підгрупи)	Так	Ні
Держава	+	-
Громадяни	+	-
Суб'єкти господарювання	+	-
у тому числі суб'єкти малого підприємництва	+	-

Врегулювання зазначених проблемних питань не може бути здійснено за допомогою:

ринкових механізмів, оскільки такі питання регулюються лише нормативно-правовими актами;

діючих регуляторних актів, оскільки порушені законодавством питання висвітлюються у вигляді загальних вимог з кіберзахисту об'єктів критичної інфраструктури, без врахування секторальної специфіки їх функціонування.

II. Цілі державного регулювання

Цілями державного регулювання є:

- забезпечення єдиного підходу до організації та реалізації заходів кіберзахисту ОКІ;
- створення правових передумов для належного виконання операторами ОКІ вимог законодавства у сфері кібербезпеки з урахуванням галузевої специфіки сфери охорони здоров'я;
- підвищення рівня захищеності інформаційно-комунікаційних систем, що використовуються у сфері охорони здоров'я, зокрема електронної системи охорони здоров'я, медичних інформаційних систем та інших цифрових сервісів;
- забезпечення безперервності функціонування інформаційно-комунікаційних систем і процесів надання медичної допомоги в умовах зростання кіберзагроз;
- мінімізація ризиків несанкціонованого доступу, втрати, модифікації або компрометації інформації, що обробляється в інформаційно-комунікаційних системах сфери охорони здоров'я;
- створення умов для ефективної координації діяльності операторів ОКІ в питаннях забезпечення кіберзахисту.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів:

Вид альтернативи	Опис альтернативи
Альтернатива 1 Залишення існуючої ситуації без змін	Кіберзахист ОКІ забезпечуватиметься відповідно до законодавчо визначених загальних вимог з кіберзахисту ОКІ без врахування специфіки сфери охорони здоров'я та потребуватиме від відповідальних осіб з питань кіберзахисту ОКІ самостійного визначення заходів з кіберзахисту, необхідних для вжиття на об'єкті. Такий підхід не гарантує формування єдиного по всьому сектору охорони здоров'я підходу до організації заходів з кіберзахисту ОКІ внаслідок різного професійного рівня підготовки відповідальних осіб з питань кіберзахисту ОКІ, що може призвести до неоднакового застосування вимог законодавства та створюватиме ризики для безперервності надання медичної допомоги та захисту інформаційних ресурсів.
Альтернатива 2 Прийняття запропонованого проєкту акта	Прийняття проєкту акта забезпечить можливість для формування єдиного підходу до організації та реалізації заходів з кіберзахисту ОКІ, визначення достатності вжитих заходів з урахуванням специфіки сектору охорони здоров'я, зокрема особливостей функціонування закладів охорони здоров'я, використання електронної системи охорони здоров'я, медичних інформаційних систем, а також забезпечення захисту персональних даних та іншої інформації, що обробляється під час надання медичної допомоги.

Оптимальним способом досягнення визначених цілей є прийняття проєкту акта, оскільки саме цей спосіб забезпечить нормативне врегулювання питання та створить правові передумови для формування єдиного підходу до забезпечення кіберзахисту ОКІ.

2. Оцінка вибраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави:

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Залишення існуючої ситуації без змін	Відсутня.	Кіберзахист ОКІ забезпечуватиметься відповідно до законодавчо визначених загальних вимог з кіберзахисту ОКІ без врахування специфіки сектору охорони здоров'я, що потребуватиме від відповідальних осіб з питань кіберзахисту ОКІ самостійного визначення заходів з кіберзахисту, необхідних для вжиття на об'єкті. Зважаючи на різний професійний рівень їх підготовки з питань кіберзахисту, не гарантується формування єдиного підходу до організації заходів з кіберзахисту, що зберігатиме ризики неоднакового застосування вимог з

		кіберзахисту, порушення безперервності надання медичної допомоги та недостатнього рівня захисту інформаційних ресурсів.
Альтернатива 2 запропонованого проєкту акта	Буде створено умови для формування єдиного підходу до організації та реалізації заходів кіберзахисту ОКІ, для належного виконання вимог законодавства у сфері кібербезпеки з урахуванням галузевої специфіки, підвищення рівня захищеності інформаційно-комунікаційних систем та мінімізації ризиків порушення безперервності надання медичної допомоги.	Реалізація проєкту акта не потребуватиме окремих видатків з державного чи місцевих бюджетів, бо здійснюватиметься в межах наявних повноважень та організаційних можливостей операторів ОКІ.

Оцінка впливу на сферу інтересів громадян

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Залишення існуючої ситуації без змін	Відсутні	Унаслідок різного професійного рівня підготовки відповідальних осіб з питань кіберзахисту ОКІ зберігатимуться ризики неоднакового застосування вимог з кіберзахисту, порушення безперервності надання медичної допомоги.
Альтернатива 2 Прийняття запропонованого проєкту акта	Створюються умови для підвищення рівня захисту персональних даних пацієнтів, забезпечення безперервності надання медичної допомоги та підвищення стійкості інформаційних систем галузі охорони здоров'я до кіберзагроз.	Відсутні. Реалізація проєкту акта не створюватиме окремого адміністративного чи фінансового навантаження для громадян.

Оцінка впливу на сферу інтересів суб'єктів господарювання

Відповідно до пункту третього статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» функціонування національної системи кібербезпеки забезпечується шляхом **встановлення обов'язкових вимог до інформаційної безпеки ОКІ**, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням

міжнародних стандартів та специфіки галузі, до якої належать відповідні ОКІ.

Наказом Адміністрації Держспецзв'язку від 30 січня 2026 року № 75 визначено перелік **базових заходів з кіберзахисту, обов'язкових для здійснення органами державної влади, іншими державними органами, органами місцевого самоврядування, державними підприємствами, установами та організаціями, які є власниками або розпорядниками інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, в яких обробляються державні інформаційні ресурси, операторами критичної інфраструктури та власниками або розпорядниками об'єктів критичної інформаційної інфраструктури.**

Відповідно до пункту 11 Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 (в редакції постанови Кабінету Міністрів України від 13 листопада 2025 року № 1470), **секторальні органи у сфері захисту критичної інфраструктури можуть розробляти галузеві вимоги з кіберзахисту, які враховуватимуть секторальну (галузеву) специфіку функціонування об'єктів критичної та критичної інформаційної інфраструктури, які відносяться до сфери їх управління.**

Зважаючи на зазначене, проєкт акта дозволить відповідальним особам з питань кіберзахисту ОКІ чітко визначати перелік заходів, які необхідно запровадити для виконання вимог з кіберзахисту.

Під дію проєкту акта підпадають всі ОКІ, проєкт акта не створюватиме окремого адміністративного чи фінансового навантаження на суб'єктів господарювання ніж це передбачено чинним законодавством у сфері захисту інформації.

Вид альтернативи	Вигоди	Витрати
Альтернатива 1 Залишення існуючої ситуації без змін	Відсутні.	Кіберзахист ОКІ забезпечуватиметься відповідно до законодавчо визначених загальних вимог з кіберзахисту ОКІ без врахування специфіки сфери охорони здоров'я та потребуватиме самостійного визначення відповідальними особами з питань кіберзахисту ОКІ заходів, необхідних для вжиття на об'єкті. Такий підхід не гарантує формування єдиного по всьому сектору охорони здоров'я підходу до організації заходів з кіберзахисту ОКІ внаслідок різного професійного рівня підготовки відповідальних осіб з питань кіберзахисту ОКІ, що може призвести до

		неоднакового застосування вимог законодавства та створюватиме ризики для безперервності надання медичної допомоги та захисту даних про пацієнтів, які користуються інформаційно-комунікаційними сервісами в охороні здоров'я.
Альтернатива 2 Прийняття запропонованого проєкту акта	Буде забезпечено можливість для формування єдиного підходу до організації та реалізації заходів з кіберзахисту ОКІ та визначення достатності вжитих заходів з урахуванням специфіки сектору охорони здоров'я	Відсутні. Реалізація проєкту акта не створюватиме окремого адміністративного чи фінансового навантаження на суб'єктів господарювання.

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей:

За результатами опрацювання альтернативних способів досягнення цілей державного регулювання здійснено вибір оптимального альтернативного способу з урахуванням системи бальної оцінки ступеня досягнення визначених цілей.

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного балу
Альтернатива 1 Залишення існуючої ситуації без змін	1	Не дозволить вирішити проблему, зазначену в Розділі I Аналізу, та досягти цілей державного регулювання, передбачених у Розділі II Аналізу.
Альтернатива 2 Прийняття запропонованого проєкту акта	4	Дозволить вирішити проблему, зазначену в Розділі I Аналізу, та досягти цілей державного регулювання, передбачених у Розділі II Аналізу.

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1 Залишення існуючої ситуації без змін	Для держави: відсутні	Для держави: Відсутність єдиного підходу до організації	Зазначена альтернатива не забезпечує

	Для громадян: відсутні Для суб'єктів господарювання: відсутні	заходів з кіберзахисту ОКІ. Для громадян: Відсутність єдиного підходу до організації заходів з кіберзахисту ОКІ може спричинити порушення безперервності надання медичної допомоги та необхідного рівня захисту персональних даних пацієнтів Для суб'єктів господарювання: різний професійний рівень підготовки відповідальних осіб з питань кіберзахисту ОКІ може спричинити різне розуміння та застосування вимог законодавства з кіберзахисту ОКІ.	досягнення цілей державного регулювання, передбачених у Розділі II Аналізу.
Альтернатива 2 Прийняття запропонованого проєкту акта	Для держави: буде створено умови для формування єдиного підходу до організації та реалізації заходів кіберзахисту ОКІ з урахуванням галузевої специфіки, підвищення рівня захищеності інформаційних систем галузі охорони здоров'я та мінімізації ризиків порушення безперервності надання медичної допомоги. Для громадян: створює умови для збільшення рівня захисту персональних даних пацієнтів, забезпечення безперервності надання медичної	Для держави: відсутні, реалізація проєкту акта не потребуватиме окремих видатків з державного чи місцевих бюджетів, бо здійснюватиметься в межах наявних повноважень та організаційних можливостей операторів ОКІ. Для громадян: Відсутні, реалізація проєкту акта не створюватиме окремого адміністративного чи фінансового навантаження для	Зазначена альтернатива забезпечує досягнення цілей державного регулювання, передбачених у Розділі II Аналізу.

	допомоги та підвищення стійкості інформаційних систем галузі охорони здоров'я до кіберзагроз. Для суб'єктів господарювання: прийняття запропонованого проєкту забезпечить єдиний підхід до організації та реалізації заходів кіберзахисту ОКІ, створення чітких та зрозумілих механізмів виконання вимог законодавства у сфері кібербезпеки з урахуванням галузевої специфіки.	громадян. Для суб'єктів господарювання: відсутні, реалізація проєкту акта не створюватиме окремого адміністративного чи фінансового навантаження на суб'єктів господарювання.	
--	--	---	--

Рейтинг	Аргументи щодо переваги обраної альтернативи / причини відмови від альтернативи	Оцінка ризику зовнішніх чинників на дію запропонованого регуляторного акта
Альтернатива 1 Залишення існуючої ситуації без змін	Альтернатива не забезпечує досягнення цілей державного регулювання, оскільки не передбачає врахування галузевої специфіки галузі охорони здоров'я при організації та реалізації заходів кіберзахисту. Зберігатимуться ризики неоднакового застосування вимог законодавства та порушення безперервності функціонування інформаційно-комунікаційних систем.	Високий. Існує ризик подальшого зростання кіберзагроз, неоднакового застосування вимог законодавства відповідальними особами з питань кіберзахисту ОКІ та недостатнього рівня захисту інформаційних ресурсів сфери охорони здоров'я.
Альтернатива 2 Прийняття запропонованого проєкту акта	Обрана альтернатива. Забезпечить досягнення цілей державного регулювання шляхом формування єдиного підходу до організації та реалізації заходів кіберзахисту об'єктів критичної інфраструктури сектору «охорона здоров'я», створення правових передумов для належного виконання вимог законодавства у сфері кібербезпеки та врахування галузевої специфіки сфери охорони здоров'я.	Низький. Ризики можуть бути пов'язані виключно зі змінами законодавства у сфері кібербезпеки або трансформацією організаційних процесів у галузі охорони здоров'я, однак не матимуть суттєвого впливу на досягнення цілей державного регулювання.

V. Механізми та заходи, які забезпечать розв'язання визначеної проблеми

Механізмом розв'язання визначеної проблеми є нормативне врегулювання особливостей організації та реалізації заходів кіберзахисту ОКІ шляхом прийняття відповідного регуляторного акта.

Для досягнення визначених цілей державного регулювання передбачається реалізація таких заходів:

З боку держави:

прийняття та офіційне оприлюднення регуляторного акта;

забезпечення методологічного супроводу його реалізації;

забезпечення координації діяльності суб'єктів, на яких поширюватиметься дія акта;

забезпечення моніторингу практики застосування положень акта та, за необхідності, подальшого удосконалення нормативного регулювання;

забезпечення єдиного підходу до організації та реалізації заходів кіберзахисту ОКІ з урахуванням галузевої специфіки.

З боку суб'єктів, на яких поширюватиметься дія акта:

організація діяльності у сфері кіберзахисту відповідно до вимог законодавства у сфері кібербезпеки та положень регуляторного акта;

впровадження визначених організаційних заходів з урахуванням специфіки функціонування ОКІ;

забезпечення належного рівня захисту інформаційно-комунікаційних систем та інформації, що обробляється під час надання медичної допомоги.

Реалізація зазначених заходів забезпечить формування єдиного підходу до організації кіберзахисту ОКІ, підвищення рівня захищеності інформаційних ресурсів, мінімізацію ризиків порушення безперервності надання медичної допомоги та створення правових передумов для належного виконання вимог законодавства у сфері кібербезпеки.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

Реалізація регуляторного акта не потребуватиме додаткових бюджетних витрат і ресурсів на адміністрування регулювання органами виконавчої влади чи органами місцевого самоврядування.

Державне регулювання не передбачає утворення нового державного органу або нового структурного підрозділу діючого органу. Передбачається виконання галузевих вимог з кіберзахисту наявними на ОКІ підрозділами з кіберзахисту / відповідальними особами з кіберзахисту.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Пропонується встановити необмежений строк дії регуляторного акта, оскільки він регулює відносини, які мають пролонгований характер.

Зміна строку дії регуляторного акта можлива в разі зміни міжнародно-правових актів чи законодавчих актів України вищої юридичної сили, на виконання яких розроблений цей проєкт регуляторного акта.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозними значеннями показників результативності дії регуляторного акта є:

1. кількість суб'єктів господарювання, на яких поширюватиметься дія регуляторного акта, – об'єкти критичної інфраструктури сектору «охорона здоров'я», визначені відповідно до законодавства;

2. розмір коштів та час, що витратимуться суб'єктами господарювання у зв'язку з виконанням вимог регуляторного акта, – додаткових витрат коштів та часу не передбачається, оскільки регуляторний акт не встановлює нових обов'язків, а деталізує механізми виконання вимог, уже передбачених законодавством у сфері кібербезпеки;

3. рівень поінформованості суб'єктів господарювання щодо основних положень регуляторного акта – високий, оскільки проєкт регуляторного акта та аналіз регуляторного впливу будуть оприлюднені на офіційному вебсайті Міністерства охорони здоров'я України та проходитимуть процедуру громадського обговорення відповідно до законодавства.

Після набрання чинності регуляторним актом його результативність визначатиметься за такими показниками:

1. частка об'єктів критичної інфраструктури сектору «охорона здоров'я», які впровадили заходи кіберзахисту відповідно до вимог законодавства;

2. частка об'єктів критичної інфраструктури сектору «охорона здоров'я», які впровадили управління ризиками кібербезпеки;

3. частка об'єктів критичної інфраструктури сектору «охорона здоров'я», які досягли визначеного цільового стану кібербезпеки;

4. рівень застосування єдиного підходу до організації та реалізації заходів кіберзахисту з урахуванням галузевої специфіки галузі охорони здоров'я;

5. рівень забезпечення безперервності функціонування інформаційно-комунікаційних систем та цифрових сервісів у сфері охорони здоров'я;

6. розмір надходжень до державного та місцевих бюджетів, пов'язаних із дією регуляторного акта, – не передбачається.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Відстеження результативності регуляторного акта здійснюватиметься шляхом проведення базового та повторного (періодичного) відстеження

статистичних показників результативності акта, визначених під час проведення аналізу впливу регуляторного акта.

Базове відстеження результативності цього регуляторного акта здійснюватиметься у II кварталі 2027 року, для цього використовуватимуться виключно статистичні показники (у відсотках) щодо оцінки стану виконання заходів кібербезпеки.

Повторне (періодичне) відстеження результативності регуляторного акта здійснюватиметься у II кварталі 2028 року, шляхом аналізу статистичних показників у звітних матеріалах щодо оцінки прогресу (у відсотках) у досягненні цільового стану кібербезпеки.

За результатами даного відстеження відбудеться порівняння показників базового та повторного відстеження.

Періодичне відстеження результативності буде здійснюватися один раз на кожні три роки починаючи з дня закінчення заходів з повторного відстеження результативності цього акта.

Метод проведення відстеження результативності – статистичний.

Вид даних, за допомогою яких здійснюватиметься відстеження результативності, – статистичні.

Цільові групи осіб, що обиратимуться для участі у відповідному опитуванні для проведення відстеження, – суб'єкти національної системи реагування на кіберінциденти, кібератаки, кіберзагрози.

У разі надходження пропозицій та зауважень щодо вирішення не врегульованих або проблемних питань буде розглядатися необхідність внесення відповідних змін.

Відстеження результативності регуляторного акта буде здійснюватися Міністерством охорони здоров'я України протягом усього строку його дії.

Міністр охорони здоров'я України

Віктор ЛЯШКО

«___» _____ 2026 р.