

ЗАТВЕРДЖЕНО

Наказ Міністерства охорони
здоров'я України

від _____ № _____

Галузеві вимоги з кіберзахисту об'єктів критичної інфраструктури сектору «охорона здоров'я»

I. Загальні положення

1.1. Галузеві вимоги з кіберзахисту об'єктів критичної інфраструктури сектору «охорона здоров'я» (далі – Вимоги) визначають організаційно-методологічні умови з кіберзахисту об'єктів критичної інфраструктури сектору «охорона здоров'я» (далі – ОКІ), що є обов'язковими до виконання операторами критичної інфраструктури сектору «охорона здоров'я» та власниками або розпорядниками об'єктів критичної інформаційної інфраструктури сектору «охорона здоров'я» (далі – суб'єкти).

1.2. У цих Вимогах терміни вживаються у такому значенні:

1) активи – дані, інформація (в тому числі медична), персонал, програмне забезпечення, пристрої та носії інформації, що дозволяють оператору критичної інфраструктури забезпечити надання життєво важливих послуг та функцій у сфері охорони здоров'я;

2) рівень впровадження заходів з кіберзахисту – це поточний або цільовий рівень кіберзахисту об'єкту критичної інфраструктури, який визначається ступенем розвитку системи управління інформаційною безпекою та кількісно-якісними показниками впровадження системи заходів з кіберзахисту.

Інші терміни у цих Вимогах вживаються у значеннях, наведених у Законах України «Про інформацію», «Про критичну інфраструктуру», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронні комунікації», «Загальних вимогах 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), «Деяких питаннях об'єктів критичної інформаційної інфраструктури», затверджених постановою Кабінету Міністрів України від 09 жовтня 2020 року № 943, «Деяких питаннях об'єктів критичної інфраструктури», затверджених постановою Кабінету Міністрів України від 09 жовтня 2020 року № 1109, «Мінімальних вимогах до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем», затверджених постановою Кабінету Міністрів України від 29 березня 2006 року № 373 (в редакції постанови Кабінету Міністрів України

від 26 листопада 2025 року № 1531), «Положенні про організаційно-технічну модель кіберзахисту», затверджені постановою Кабінету Міністрів України від 29 грудня 2021 року № 1426, «Деяких питаннях створення, адміністрування та забезпечення функціонування засобу інформатизації», затверджених постановою Кабінету Міністрів України від 21 лютого 2025 року № 205, «Порядку авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем», затверджені постановою Кабінету Міністрів України від 18 червня 2025 року № 712, «Деяких питаннях реагування на кіберінциденти, кібератаки та кіберзагрози», затверджених постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533, «Каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, формі плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту», затверджених наказом Адміністрації Держспецзв'язку від 30 січня 2026 року № 75.

1.3. Ці Вимоги формують для об'єкта критичної інфраструктури сектору «охорона здоров'я» (далі – ОКІ) та об'єкта критичної інформаційної інфраструктури, що експлуатується на об'єкті критичної інфраструктури сектору «охорона здоров'я» (далі – ОКІІ) необхідний перелік заходів з кіберзахисту, визначених постановою Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» (в редакції постанови Кабінету Міністрів України від 13 листопада 2025 р. № 1470), наказом Адміністрації Держспецзв'язку від 30 січня 2026 року № 75 «Про затвердження каталогу заходів з кіберзахисту, базових заходів з кіберзахисту, форми плану кіберзахисту та методичних рекомендацій щодо здійснення заходів з кіберзахисту», нормативними документами у сфері технічного захисту інформації, міжнародними стандартами з питань інформаційної безпеки, кібербезпеки та кіберзахисту.

1.4. Кіберзахист ОКІ / ОКІІ забезпечується шляхом здійснення суб'єктами наведених у розділі II цих Вимог та обов'язкових для виконання заходів з кіберзахисту з урахуванням поточного стану кіберзахисту ОКІ / ОКІІ та результатів управління ризиками кібербезпеки.

1.5. Здійснення заходів з кіберзахисту дозволяє підвищити рівень забезпечення кібербезпеки суб'єкта шляхом зниження ризиків кібербезпеки. Заходи з кіберзахисту мають інтеграційний характер та формують цикл управління кібербезпекою.

II. Поточний та цільовий стан кіберзахисту

2.1. Визначення поточного та цільового стану кіберзахисту для ОКІ / ОКІІ здійснює відповідальна особа, яка виконує функції та завдання керівника з кіберзахисту, або відповідальний за інформаційну безпеку суб'єкта.

2.2 Поточний стан кіберзахисту є фактичним станом кіберзахисту ОКІ / ОКІІ. Визначення поточного стану кіберзахисту містить заходи з оцінювання рівня захисту інформації, раніше впровадженого на ОКІ / ОКІІ.

2.3 Цільовий стан кіберзахисту є планованим станом кіберзахисту ОКІ / ОКІІ, який обумовлює досягнення стратегічних цілей суб'єкта з поступовим просуванням до належного рівня кібербезпеки ОКІ / ОКІІ. Визначення цільового стану кіберзахисту містить заходи та цільові показники забезпечення кібербезпеки, які необхідні для досягнення бажаних цілей управління ризиками кібербезпеки та більш високого рівня кіберзахисту ОКІ / ОКІІ.

2.4 Порівняння поточного та цільового станів кіберзахисту сприяє виявленню недоліків, які треба усунути для досягнення цілей управління ризиками кібербезпеки ОКІ / ОКІІ.

III. Заходи з кіберзахисту

3.1 Детальний опис заходів з кіберзахисту, які є обов'язковими до виконання для операторів критичної інфраструктури та власників або розпорядників об'єктів критичної інформаційної інфраструктури I та II категорії критичності, наведений у Додатку 1 до цих Вимог.

3.2 Детальний опис заходів з кіберзахисту, які є обов'язковими до виконання для операторів критичної інфраструктури та власників або розпорядників об'єктів критичної інформаційної інфраструктури III та IV категорії критичності, наведений у Додатку 2 до цих Вимог.

3.3 Розробка та впровадження заходів з кіберзахисту проводиться за такими етапами:

1) **Визначення пріоритетів та сфери застосування цих Вимог.** Визначаються цілі та організаційні пріоритети щодо надання критично важливих послуг та виконання функцій. Визначається обсяг інформаційних систем та активів, що підтримують надання критично важливих послуг та виконання функцій.

2) **Аналіз середовища надання критично важливих послуг та виконання функцій.** Визначаються відповідні системи та активи, що безпосередньо забезпечують надання критично важливих послуг та виконання функцій, аналізуються нормативні вимоги та загальний підхід до управління ризиками для таких систем.

3) **Визначення поточного стану кіберзахисту.** Визначаються і фіксуються заходи з кіберзахисту, що містяться в цих Вимогах, реалізовані на поточний момент часу. Цей етап є етапом самоаналізу, що дозволяє з'ясувати, які заходи захисту інформації впроваджено на ОКІ / ОКІІ та на якому рівні вони реалізовані.

4) **Оцінка ризиків.** Проведення оцінки ризиків кібербезпеки базується на процесі, раніше впровадженому на ОКИ / ОКІІ, або на результатах попередньої оцінки ризиків. Аналіз середовища експлуатації інформаційних систем та активів проводиться з метою визначення ймовірності настання кіберінцидентів, реалізації кібератак та оцінки наслідків, які можуть настати у результаті такої події.

5) **Формування цільового стану кіберзахисту.** Цільовий стан кіберзахисту це планований стан, який описує бажані результати із забезпечення кібербезпеки ОКИ / ОКІІ. Суб'єкт впроваджує заходи кіберзахисту з урахуванням ризиків, притаманних системам і процесам надання життєво важливих послуг та функцій. При формуванні цільового стану кіберзахисту треба розглянути та врахувати вплив і вимоги з кібербезпеки для партнерів ОКИ / ОКІІ.

6) **Визначення, аналіз та пріоритизація недоліків.** Проводиться порівняння поточного і цільового стану кіберзахисту з метою визначення недоліків, з'ясовуються заходи та ресурси (матеріальні, людські), необхідні для їх усунення і досягнення цільового стану кіберзахисту.

7) **Реалізація плану кіберзахисту.** Визначаються і виконуються конкретні дії щодо усунення виявлених недоліків. Під час виконання плану кіберзахисту постійно відстежується відповідність поточного і цільового стану кіберзахисту, визначаються стандарти, нормативні документи, що стосуються ОКИ / ОКІІ, та впроваджуються необхідні заходи для забезпечення кібербезпеки.

8) **Зазначені етапи повторюються щорічно.** Відстеження прогресу проводиться шляхом ітеративного оновлення поточного стану кіберзахисту та порівняння його з цільовим станом кіберзахисту.

IV. Рівні впровадження заходів з кіберзахисту

4.1 Для формування поточного та цільового стану кіберзахисту ОКИ / ОКІІ суб'єкт використовує зазначені нижче рівні впровадження заходів з кіберзахисту.

4.2 Ці рівні описують перехід від ситуативних заходів реагування на кіберінциденти, кібератаки, кіберзагрози до підходів, заснованих на оцінці ризиків кібербезпеки, які постійно вдосконалюються.

4.3 Рівні впровадження заходів з кіберзахисту ОКИ / ОКІІ базуються на оцінці і управлінні ризиками кібербезпеки та включають частковий (рівень 1), ризик-орієнтований (рівень 2), повторюваний (рівень 3) та адаптивний (рівень 4).

4.3.1 Частковий рівень.

а. Застосування організаційної стратегії ризиків кібербезпеки управляється в індивідуальному порядку, пріоритизація є випадковою і формально не базується на цілях чи середовищі загроз.

b. Обізнаність про ризики кібербезпеки на організаційному рівні обмежена.

c. Суб'єкт впроваджує управління ризиками кібербезпеки на нерегулярній основі, від випадку до випадку.

d. Суб'єкт може не мати процесів, які дозволяють обмінюватися інформацією про кібербезпеку всередині.

e. Суб'єкт, як правило, не знає про ризики кібербезпеки, пов'язані з його постачальниками товарів, робіт, послуг, які він придбав та використовує.

4.3.2 Ризик-орієнтований рівень.

a. Методи управління ризиками затверджуються керівництвом та можуть бути (або не бути) встановлені як загальна організаційна політика.

b. Пріоритизація діяльності з кібербезпеки та потреб у захисті безпосередньо залежить від цілей організаційних ризиків, середовища загроз або вимог суб'єкта, його місії.

c. Існує усвідомлення ризиків кібербезпеки на організаційному рівні, але загально-організаційного підходу до управління ризиками кібербезпеки не встановлено. Врахування кібербезпеки в організаційних цілях і програмах може мати місце на деяких, але не на всіх рівнях.

d. Оцінка ризиків кібербезпеки організаційних та зовнішніх активів здійснюється, але зазвичай не є повторюваною або періодичною.

e. Суб'єкт усвідомлює ризики кібербезпеки, пов'язані з його постачальниками товарів, робіт, послуг, які він придбав та використовує, але не діє послідовно чи формально у відповідь на ці ризики.

4.3.3 Повторюваний рівень.

a. Практика управління ризиками офіційно затверджена та виражена як політика. Політики, процеси та процедури з урахуванням ризиків визначаються, впроваджуються за призначенням і переглядаються.

b. Існує загально-організаційний підхід до управління ризиками кібербезпеки.

c. Існують узгоджені методи для ефективного реагування на зміни ризику.

d. Персонал суб'єкта володіє знаннями та навичками для виконання своїх призначених ролей і обов'язків.

e. Суб'єкт постійно та точно відстежує ризики кібербезпеки активів. Керівники вищої ланки з кібербезпеки та керівники суб'єкта регулярно спілкуються щодо ризиків кібербезпеки, забезпечують врахування кібербезпеки на всіх напрямках діяльності суб'єкта.

f. Стратегія ризиків ґрунтується на ризиках кібербезпеки, пов'язаних з постачальниками товарів, робіт, послуг суб'єкта, які він придбав і використовує.

g. Працівники суб'єкта офіційно реагують на ці ризики за допомогою таких механізмів, як письмові договори, що визначають базові вимоги, структури управління, а також впровадження та моніторинг політики.

h. Ці дії впроваджуються послідовно та за призначенням, а також постійно контролюються та переглядаються.

4.3.4 Адаптивний рівень.

a. Існує загально-організаційний підхід до управління ризиками кібербезпеки, який використовує політику, процеси та процедури з урахуванням ризиків для вирішення потенційних подій кібербезпеки.

b. Взаємозв'язок між ризиками кібербезпеки та цілями чітко розуміється та враховується під час прийняття рішень.

c. Керівники суб'єкта контролюють ризики кібербезпеки на одному рівні з фінансовими та іншими організаційними ризиками.

d. Бюджет суб'єкта формується з урахуванням аналізу поточного та прогнозованого середовища ризику, а також рівня прийнятної толерантності до ризику.

e. Процес управління ризиками кібербезпеки є частиною організаційної культури суб'єкта та ґрунтується на аналізі попереднього досвіду діяльності та забезпеченні постійного моніторингу операцій у системах та мережах.

f. Суб'єкт оперативно й ефективно адаптується до змін у цілях діяльності або завданнях, пов'язаних з основною місією. Це дозволяє своєчасно коригувати підходи до управління ризиками та інформувати про них відповідно до актуальних потреб інших суб'єктів.

g. Суб'єкт адаптує свої практики кібербезпеки на основі попередньої та поточної діяльності з кіберзахисту, включаючи отримані навички та прогнозні показники. Завдяки процесу безперервного вдосконалення, який включає передові технології та практики кібербезпеки, суб'єкт активно адаптується до мінливого технологічного ландшафту та своєчасно й ефективно реагує на складні кіберзагрози, що розвиваються.

h. Суб'єкт застосовує інформацію в реальному часі або максимально наближену до нього для оцінки ризиків кібербезпеки, пов'язаних з постачальниками товарів, робіт, послуг, які закуповуються та використовуються.

V. Оцінювання стану кіберзахисту

5.1 З метою визначення поточного або цільового стану ОКІ / ОКП суб'єкт забезпечує проведення оцінювання стану кіберзахисту відповідно до вимог Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури, затвердженого постановою Кабінету Міністрів України від 31 грудня 2025 року № 1799 (далі – Постанова № 1799).

5.2 Оцінювання поточного стану кіберзахисту проводиться в формі самооцінювання або зовнішнього оцінювання, з метою підготовки та перегляду планів кіберзахисту або отримання об'єктивної інформації про фактичний стан

виконання вимог законодавства у сфері кіберзахисту, повноти запроваджених заходів кіберзахисту тощо.

5.3 Оцінювання поточного стану кіберзахисту в формі самооцінювання проводиться в такі терміни:

- планове самооцінювання поточного стану кіберзахисту – щороку;
- позапланове самооцінювання поточного стану кіберзахисту – за рішенням власника або розпорядника об'єкта оцінювання.

5.4 Оцінювання поточного стану кіберзахисту в формі зовнішнього оцінювання проводиться на плановій основі, не рідше ніж один раз на два роки.

VI. План кіберзахисту

6.1 З метою належного виконання заходів з кіберзахисту суб'єкти розробляють, затверджують, щороку переглядають та за потреби, зокрема у разі зміни рівня ризику кібербезпеки, оновлюють план кіберзахисту.

6.2 План кіберзахисту дозволяє суб'єкту визначитися з обсягом заходів з кіберзахисту ОКІ / ОКП, які необхідно вжити або адаптувати раніше вжиті заходи відповідно до цих Вимог.

6.3 При розробці та оновленні плану кіберзахисту враховуються результати проведення аналізу ефективності реагування на кіберінциденти, кібератаки, кіберзагрози та результати управління ризиками кібербезпеки.

6.4 Форма плану кіберзахисту з визначеними базовими заходами з кіберзахисту, обов'язковими до виконання для операторів критичної інфраструктури та власників або розпорядників об'єктів критичної інформаційної інфраструктури I та II категорії критичності, наведена у Додатку 3 до цих Вимог.

6.5 Форма плану кіберзахисту з визначеними базовими заходами з кіберзахисту, обов'язковими до виконання для операторів критичної інфраструктури та власників або розпорядників об'єктів критичної інформаційної інфраструктури III та IV категорії критичності, наведена у Додатку 4 до цих Вимог.

6.6 План кіберзахисту описує поточний та цільовий стани кіберзахисту і складається для кожного ОКІ / ОКП окремо. Заходи, передбачені планом кіберзахисту, мають узгоджуватися з планом захисту об'єкта критичної інфраструктури за проєктною загрозою національного рівня «кібератака/кіберінцидент».

6.7 Для оцінки поточного стану кіберзахисту визначаються заходи та результати ефективності впроваджених заходів з кіберзахисту, які реалізовані та досягнуті на ОКІ / ОКП на момент складання або модернізації плану. Суб'єкти досягають цільового стану кіберзахисту ОКІ / ОКП поетапно, шляхом послідовного здійснення заходів з кіберзахисту, передбачених планом кіберзахисту.

6.8 План містить опис сфери застосування заходів з кіберзахисту (зокрема, перелік та межі підрозділів і основних операційних процесів суб'єкта, перелік систем, електронно-комунікаційних мереж та програмного забезпечення, на які поширюються заходи з кіберзахисту, а також географічне розташування систем, приміщення, опис серверних кімнат тощо), що сприяє об'єктивному оцінюванню поточного стану та визначенню оптимального цільового стану кіберзахисту.

VII. Звітування про результати оцінювання стану кіберзахисту

7.1 Звітування про результати оцінювання стану кіберзахисту ОКІ / ОКП здійснюється відповідно до вимог Постанови № 1799.

7.2 Сторона, яка проводила оцінювання стану кіберзахисту ОКІ / ОКП, складає звіт про результати оцінювання стану кіберзахисту ОКІ / ОКП, копія якого надсилається до Адміністрації Держспецзв'язку у визначений Постановою № 1799 термін.

**Директор Департаменту цифрових
трансформацій в охороні здоров'я**

Дмитро ЛУК'ЯНОВ