

ЗАТВЕРДЖЕНО
Наказ Міністерства
охорони здоров'я України
08 січня 2026 року № 29

Зареєстровано в
Міністерстві юстиції
України
11 лютого 2026 року
за № 194/45588

**Положення
про галузеву команду реагування на кіберінциденти,
кібератаки, кіберзагрози у сфері охорони здоров'я**

I. Загальні положення

1. Це Положення визначає основні завдання, функції та повноваження галузевої команди реагування на кіберінциденти, кібератаки, кіберзагрози у сфері охорони здоров'я (далі – ГКР).
2. Виконання завдань та здійснення діяльності ГКР забезпечується, відповідно до законодавства України, зокрема цього Положення, самостійним структурним підрозділом МОЗ, що відповідає за виконання функцій із забезпечення кібербезпеки, кіберзахисту, захисту інформації (далі – підрозділ кібербезпеки) та державним підприємством «Електронне здоров'я», що належить до сфери управління МОЗ, або його правонаступником у разі ліквідації або реорганізації.
3. МОЗ відповідно до встановлених вимог законодавства України, на договірній основі може залучати для надання окремих завдань ГКР приватні команди реагування, відібрані у відповідності до конкурентних процедур закупівель у відповідності до Закону України “Про публічні закупівлі”, при гарантуванні дотримання ними встановлених законодавством України вимог до таких галузових команд реагування.
4. Матеріально-технічне та програмно-апаратне забезпечення роботи ГКР здійснюється МОЗ за рахунок коштів державного бюджету та/або інших джерел, не заборонених законодавством України.
5. Персональний склад ГКР затверджується наказом МОЗ. До складу ГКР входить представник підрозділу кібербезпеки МОЗ.

6. ГКР очолює керівник, який визначається наказом МОЗ.

7. ГКР комплектується фахівцями на рейтинговій основі, які за своїми професійними якостями та освітнім рівнем здатні виконувати завдання та функції, визначені керівником ГКР в межах завдань та функцій ГКР. Фахівці ГКР повинні відповідати професійним стандартам у сфері кібербезпеки, та обіймати посади, визначені Національним класифікатором України «Класифікатор професій» ДК 003:2010, затвердженим наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 липня 2010 року № 327.

8. ГКР у своїй діяльності керується Конституцією України, законами України, указами Президента України, постановами Кабінету Міністрів України, іншими нормативно-правовими актами у сфері захисту інформації, кібербезпеки, зокрема цим Положенням.

9. Суб'єктами забезпечення кібербезпеки у сфері охорони здоров'я є МОЗ, Національна служба здоров'я України, Державна служба України з лікарських засобів та контролю за наркотиками, підприємства, установи та організації, що належать до сфери управління Міністерства охорони здоров'я України, оператори критичної інфраструктури, власники або розпорядники об'єктів критичної інформаційної інфраструктури сектору «охорона здоров'я» (далі – Суб'єкти забезпечення кібербезпеки).

10. ГКР для вирішення поставлених завдань у межах своєї компетенції взаємодіє із Суб'єктами забезпечення кібербезпеки у сфері охорони здоров'я та закладами охорони здоров'я та фізичними особами – підприємцями, які зареєстровані в установленому законом порядку та одержали ліцензію на провадження господарської діяльності з медичної практики (далі – Суб'єкти взаємодії), органами державної влади та місцевого самоврядування, підприємствами, установами та організаціями, силами безпеки та оборони, суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози тощо.

II. Мета, функції та завдання

1. ГКР створюється з метою забезпечення спроможності національної системи реагування на кібератаки, кіберінциденти, кіберзагрози у сфері охорони здоров'я та виконання завдань, делегованих від національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA (національного CSIRT).

2. Завдання ГКР:

1) моніторинг та проведення аналізу даних про інциденти кібербезпеки, кібератаки, кіберзагрози у сфері охорони здоров'я, динамічний аналіз ризиків та ситуаційної обізнаності;

2) отримання та опрацювання у встановленому Адміністрацією Держспецзв'язку порядку обов'язкових та інших повідомлень про кіберінциденти у сфері охорони здоров'я, отриманих від суб'єктів національної системи кібербезпеки, інших державних органів, у межах функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, надання рекомендацій щодо можливих заходів реагування та технічної підтримки;

3) здійснення заходів щодо надання Суб'єктам взаємодії, сповіщень, оголошень про кіберзагрози, інформування суб'єктів національної системи кібербезпеки щодо кіберінцидентів, кібератак, кіберзагроз і вразливостей у сфері охорони здоров'я у режимі, за можливості, наближеному до реального часу;

4) надання Суб'єктам взаємодії сервісу у зв'язку з реагуванням та рекомендацій щодо реагування на кіберінциденти, кібератаки, кіберзагрози у сфері охорони здоров'я.

3. Функції ГКР:

1) організація та координація у сфері охорони здоров'я заходів із забезпечення кібербезпеки:

інтеграція наявних у Суб'єктів взаємодії заходів та засобів кіберзахисту, організація та здійснення інформаційної взаємодії;

здійснення заходів із розроблення та впровадження систем виявлення, запобігання та нейтралізації кіберзагроз у сфері охорони здоров'я;

забезпечення впровадження організаційно-технічної моделі системи кібербезпеки, оперативного реагування на кібератаки та кіберінциденти у сфері охорони здоров'я;

розробка рекомендацій щодо організації кіберзахисту та кібербезпеки у Суб'єктів взаємодії;

2) виявлення та координація реагування на інциденти інформаційної безпеки / кіберінциденти в інформаційній інфраструктурі у сфері охорони здоров'я:

виявлення потенційно небезпечних подій та інцидентів інформаційної безпеки / кіберінцидентів шляхом моніторингу та аналізу подій в інформаційній інфраструктурі у сфері охорони здоров'я;

розробка оперативних заходів та рекомендацій щодо локалізації, нейтралізації та усунення інцидентів інформаційної безпеки / кіберінцидентів, координація зусиль та засобів щодо їх виконання;

аналіз інцидентів інформаційної безпеки / кіберінцидентів, з'ясування обставин, хронології подій, залучених в інцидент суб'єктів, виявлення кореневих причин та передумов;

розробка коригувальних заходів та рекомендацій щодо запобігання повторенню інцидентів, координація їх реалізації;

облік подій та інцидентів інформаційної безпеки / кіберінцидентів, підготовка статистичних та аналітичних матеріалів для інформування керівництва та здійснення операційної діяльності;

3) запобігання виникненню інцидентів інформаційної безпеки / кіберінцидентів шляхом управління вразливостями:

ідентифікація вразливостей елементів інформаційної інфраструктури, аналіз їхньої релевантності, оцінка пов'язаних ризиків, їх ранжування;

розробка рекомендацій щодо усунення вразливостей або реалізації тимчасових заходів щодо зниження пов'язаних ризиків;

координація, експертний супровід та контроль усунення вразливостей;

облік виявлених та усунених вразливостей, підготовка статистичних та аналітичних матеріалів для інформування керівництва та здійснення операційної діяльності;

моніторинг заходів щодо впровадження стандартів кібербезпеки в інформаційно-комунікаційних системах та реєстрах Суб'єктів взаємодії;

4) запобігання виникненню інцидентів інформаційної безпеки шляхом проактивного виявлення загроз інформаційній безпеці:

збір, обробка, аналіз та розповсюдження інформації про ландшафт загроз, тактики, техніки та процедури, що використовуються зловмисниками проти сфери охорони здоров'я, технічні деталі найбільш релевантних кіберзагроз;

розробка та координація реалізації превентивних заходів з метою запобігання актуальним та перспективним загрозам;

стратегічне планування розвитку системи кібербезпеки у сфері охорони здоров'я, розробка та контроль виконання стратегії кібербезпеки, визначення цілей та завдань з кібербезпеки, визначення пріоритетних програм з підвищення кіберстійкості;

проведення оцінки стану захищеності інформаційних ресурсів (тестування на проникнення) в інформаційно-комунікаційних системах та реєстрах Суб'єктів взаємодії.

5) організація підвищення рівня знань і навичок, проведення навчань:

організація та проведення тренінгів з питань кібербезпеки для працівників структурних підрозділів МОЗ та Суб'єктів взаємодії, надання МОЗ рекомендацій за результатами оцінювання;

за дорученням МОЗ організація та проведення семінарів, конференцій, симпозіумів, виставок, у тому числі міжнародних, сприяння залучення іноземних інвестицій у сфері кібербезпеки;

за погодженням з МОЗ участь у виставках, семінарах, конференціях, конкурсах з метою підготовки персоналу з кіберзахисту, запозичення та впровадження новітніх технологій у сфері кіберзахисту тощо.

III. Права та обов'язки

1. ГКР має право:

1) взаємодіяти (у межах повноважень) з питань кіберзахисту та протидії кіберзагрозам із Суб'єктами взаємодії, органами державної влади та місцевого самоврядування, підприємствами, установами та організаціями, силами безпеки та оборони, суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози тощо.

2) в межах законодавства України залучати до співробітництва з питань посилення кібербезпеки фахівців наукових закладів, органів виконавчої влади, підприємств, установ, організацій (за погодженням з їх керівництвом), представників інститутів громадянського суспільства, а також приватні команди реагування на кіберінциденти, кібератаки, кіберзагрози;

3) обмінюватись у встановленому законодавством України порядку з суб'єктами національної системи кібербезпеки, іншими органами державної влади, та опрацьовувати інформацію, необхідну для виконання покладених на ГКР завдань;

4) вносити на розгляд заступника Міністра охорони здоров'я України (згідно з розподілом повноважень) пропозиції щодо удосконалення роботи з питань, що належать до компетенції ГКР;

5) організовувати за дорученням МОЗ та брати участь у нарадах, семінарах, науково-практичних конференціях з питань діяльності ГКР.

2. ГКР зобов'язана:

1) дотримуватися вимог законодавства України, зокрема цього Положення;

2) виконувати покладені в межах повноважень функції та завдання;

3) надавати МОЗ звітну інформацію з питань кіберзахисту, кібербезпеки

4) здійснювати у встановленому законодавством України порядку обмін інформацією з іншими суб'єктами національної системи обміну

інформацією про кіберінциденти, кібератаки, кіберзагрози, координувати свою діяльність та інформувати CERT-UA і Ситуаційний центр забезпечення кібербезпеки Служби безпеки України про відповідні заходи реагування.

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

Дмитро ЛУК'ЯНОВ