МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ МЕДИЧНИЙ УНІВЕРСИТЕТ
імені О.О.БОГОМОЛЬЦЯ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ГРОМАДСЬКОГО ЗДОРОВ'Я ТА ПРОФІЛАКТИЧНОЇ МЕДИЦИНИ
КАФЕДРА МЕНЕДЖМЕНТУ ОХОРОНИ ЗДОРОВ'Я

Кваліфікаційна робота магістра

на тему

«Інформаційне забезпечення в рамках реагування на надзвичайні ситуації у сфері громадського здоров'я»

Студента групи 14401БМН,
спеціальності 073 «Менеджмент»
ОПП «Менеджмент у сфері
охорони здоров'я »

Богдан КРАСЬКО

Науковий керівник
науковий ступінь,
вчене звання

Іван ВИШНЕВЕЦЬКИЙ,
к.мед.н.

Гарант освітньо-
професійної програми
науковий ступінь
вчене звання

Ганна МАТУКОВА,
д.пед.н., професор

Завідувач кафедри,
науковий ступінь
вчене звання

Валентин ПАРІЙ,
д.мед.н, провесор

Київ, 2025

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ МЕДИЧНИЙ УНІВЕРСИТЕТ
імені О.О.БОГОМОЛЬЦЯ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ГРОМАДСЬКОГО ЗДОРОВ'Я ТА ПРОФІЛАКТИЧНОЇ МЕДИЦИНИ
КАФЕДРА МЕНЕДЖМЕНТУ ОХОРОНИ ЗДОРОВ'Я

Освітній рівень __магістр_____
Спеціальність _073 «Менеджмент»_____

ЗАТВЕРДЖУЮ:
Завідувач кафедри менеджменту
охорони здоров'я
_____
_____20__ року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Красько Богдан Олександрович
(прізвище, ім'я, по батькові)

1. **Тема роботи** Інформаційне забезпечення в рамках реагування на надзвичайні ситуації у сфері громадського здоров'я

керівник роботи __Іван ВИШНЕВЕЦЬКИЙ, к.мед.н._____
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "13"травня 2025 р. № 381_____

2. **Строк подання студентом роботи** 15.12.2025_____

3. **Вихідні дані до роботи**
_____
_____

4. **Цільова установка кваліфікаційної роботи**

Мета кваліфікаційної роботи

Розробити концептуальні та управлінські засади створення національного цифрового інструменту для оперативного, стандартизованого та узгодженого обміну інформацією між суб'єктами реагування на надзвичайні ситуації у сфері громадського здоров'я України.

Об'єкт дослідження

Система реагування на надзвичайні ситуації у сфері громадського здоров'я України, її організаційна структура, механізми управління та інформаційні процеси.

Предмет дослідження

Інформаційно-комунікаційні та управлінські механізми забезпечення реагування

на надзвичайні ситуації у сфері громадського здоров’я, включно з принципами, процедурами, цифровими інструментами та технологіями, що можуть бути інтегровані в єдину систему реєстрації та оповіщення.

5. **Перелік графічного (ілюстративного) матеріалу**

табл. 1, рис. 4

6. Дата видачі завдання"01"вересня 2025 р._____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Затвердження та надання теми роботи	травень 2025 р.	
2	Обґрунтування актуальності теми роботи	вересень 2025 р.	
3	Робота з бібліографічними джерелами, підготовка матеріалів для написання першого розділу роботи	вересень 2025 р.	
4	Надання матеріалів по першому розділу роботи	жовтень 2025 р.	
5	Збір інформації для написання другого розділу роботи	жовтень 2025 р.	
6	Надання матеріалів по другому розділу роботи	листопад 2025 р.	
7	Підготовка матеріалів та написання третього розділу роботи	листопад 2025 р.	
8	Надання матеріалів по третьому розділу роботи	листопад 2025 р.	
9	Написання висновків, заключне оформлення роботи та демонстраційних матеріалів	листопад 2025 р.	
10	Антиплагіатна перевірка роботи	грудень 2025 р.	
11	Підготовка доповіді до захисту роботи	грудень 2025 р.	

Студент _____ Богдан КРАСЬКО
(підпис) (прізвище та ініціали)

Керівник кваліфікаційної роботи _____ Іван ВИШНЕВЕЦЬКИЙ
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

У магістерській роботі досліджено інформаційно-комунікаційні та управлінські механізми реагування на надзвичайні ситуації у сфері громадського здоров'я. Проаналізовано організаційну структуру системи реагування, особливості міжвідомчої взаємодії та нормативно-правові вимоги щодо обміну інформацією між суб'єктами реагування. Розглянуто міжнародні підходи, зокрема положення Міжнародних медико-санітарних правил (2005) та сучасні цифрові інструменти оповіщення.

Метою роботи є розроблення концептуальних та управлінських засад створення національного цифрового інструменту для оперативного та стандартизованого обміну інформацією в умовах надзвичайних ситуацій. У дослідженні визначено ключові принципи менеджменту в охороні здоров'я – стратегічне планування, управління ресурсами, ризик-менеджмент і комунікація – як основу ефективності реагування.

Наукова новизна полягає у формуванні моделі інтегрованої цифрової системи оповіщення та реєстрації подій, що поєднує управлінські принципи, вимоги національного законодавства, міжнародні стандарти та сучасні технології. Практичне значення полягає у можливості використання запропонованих підходів для модернізації інформаційних систем, удосконалення нормативних документів, оптимізації управлінських процесів та підготовки фахівців у сфері громадського здоров'я та цивільного захисту.

ANNOTATION

The master's thesis examines the information-communication and managerial mechanisms for responding to emergencies in the field of public health. The organizational structure of the response system, the specifics of interagency coordination, and the regulatory requirements governing information exchange between response actors are analyzed. International approaches are reviewed, including the provisions of the International Health Regulations (IHR 2005) and modern digital alert and notification tools.

The aim of the thesis is to develop conceptual and managerial foundations for creating a national digital instrument that ensures rapid and standardized information exchange during emergencies. The study identifies key principles of health-care management - strategic planning, resource management, risk management, and communication - as essential components of effective emergency response.

The scientific novelty lies in the development of a model for an integrated digital system for event notification and registration, which combines managerial principles, national regulatory requirements, international standards, and modern technologies. The practical significance of the research is reflected in the applicability of the proposed approaches for modernizing information systems, improving regulatory documents, optimizing management processes, and enhancing the training of professionals in the fields of public health and civil protection.

ЗМІСТ

Визначення, скорочення та абревіатури

ЦКПХ	центри контролю та профілактики хвороб Міністерства охорони здоров'я України
ММСП	Міжнародні медико-санітарні правила – 2005 (III редакція)
ЦЕМД та МК	центри екстреної медичної допомоги та медицини катастроф
НПЦЕМД та МК	Державний заклад «Український науково-практичний центр екстреної медичної допомоги та медицини катастроф Міністерства охорони здоров'я України»
ДСНС	Державна служба України з надзвичайних ситуацій
МОЗ	Міністерство охорони здоров'я України
ЗМІ	Засоби масової інформації
НС	Надзвичайні ситуації
ЄДСЦЗ	Єдина державна система цивільного захисту
CDC	Центр контролю та профілактики захворювань США
ЦГЗ	Державна установа «Центр громадського здоров'я Міністерства охорони здоров'я України»

ВСТУП

Актуальність теми

Система громадського здоров'я України функціонує в умовах невпинного зростання ризиків, зумовлених поєднанням воєнних дій, руйнуванням критичної інфраструктури, збільшенням частоти техногенних, природних та екологічних інцидентів, а також підвищеною ймовірністю виникнення та поширення інфекційних захворювань. Така конфігурація загроз формує новий контекст державного управління, у якому традиційні механізми реагування виявляються недостатніми без сучасних інструментів інформаційного забезпечення.

У багатофакторному та кризовому середовищі саме якість, швидкість і стандартизованість управління інформаційними процесами визначають ефективність реагування. Від моменту реєстрації сигналу про небезпечну подію до ухвалення управлінського рішення критично важливими є оперативне отримання даних, їх верифікація, аналіз та передавання між усіма суб'єктами реагування - від закладів охорони здоров'я до центральних органів виконавчої влади. Проте, нині в Україні спостерігається фрагментарність інформаційних потоків**,** наявність великої кількості каналів комунікації та асинхронність процедур оповіщення, що створює ризики затримок, дублювання або втрати важливої інформації.

Воєнний час значно підсилює вразливість системи громадського здоров'я. Пошкодження телекомунікацій, перебої з електропостачанням, кібератаки, зміна логістики, масове переміщення населення та руйнування медичних закладів створюють ситуації, коли традиційні канали передачі інформації стають ненадійними або недоступними**.** За таких умов лише цифрова система, побудована на принципах захищеності та безперервності, здатна забезпечити належний рівень інформаційної стійкості.

Міжнародний досвід переконливо демонструє, що ефективні системи громадського здоров'я інтегрують дані через спеціалізовані цифрові платформи - такі як WHO EIOS, EWRS Європейського Союзу, CDC Epi-X**,** які забезпечують

не лише швидкість та точність обміну інформацією, а й відповідність вимогам глобального епідеміологічного нагляду. Відповідно до Міжнародних медико-санітарних правил (ММСП-2005), держави-учасниці зобов'язані забезпечувати здатність до оперативного виявлення, оцінки, реєстрації та повідомлення про небезпечні події. В Україні такі вимоги не можуть бути виконані повною мірою без створення єдиного національного цифрового інструменту**,** здатного інтегрувати всі джерела інформації та забезпечити міжвідомчий обмін у реальному часі.

Необхідність цифрової трансформації системи реагування посилюється також внутрішніми потребами системи громадського здоров'я. Наявність двох функціональних підсистем цивільного захисту в Міністерстві охорони здоров'я України, зокрема медичного захисту населення та санітарного та епідеміологічного благополуччя населення, створює складну мережу інформаційних зв'язків, що вимагає чіткої взаємної координації та стандартизованих механізмів до інформаційного обміну. Відсутність такого інструменту призводить до затримок у комунікації, збільшення навантаження на персонал, а також обмежує можливість аналітичної оцінки ризиків у режимі реального часу.

Таким чином, створення єдиного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я в Україні є не лише технологічним завданням, а й стратегічною потребою держави. Він має стати основою для інтеграції даних, міжвідомчої координації, підвищення оперативності та ефективності реагування, а також забезпечення відповідності міжнародним стандартам, насамперед вимогам ММСП (2005).

Запровадження такого інструменту дозволить сформувати цілісний інформаційний простір, скоротити час між виявленням події та реагуванням на неї, знизити ризики для здоров'я населення, а також зміцнити стійкість національної системи громадського здоров'я у період воєнних та післявоєнних викликів. Саме тому дослідження проблематики інформаційного забезпечення

реагування є актуальним, стратегічно важливим і має значний практичний потенціал для модернізації державної системи реагування на надзвичайні ситуації.

Мета і завдання дослідження

Мета дослідження полягає у науковому обґрунтуванні та розробці управлінських підходів до створення єдиного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я України, здатного забезпечити оперативний, стандартизований і узгоджений обмін даними між центрами контролю та профілактики хвороб, Центром громадського здоров'я МОЗ України, службами екстреної медичної допомоги та медицини катастроф, Науково-практичним центром екстреної медичної допомоги тат медицини катастроф, закладами охорони здоров'я та Міністерством охорони здоров'я України.
В основу мети покладено концепцію сучасного менеджменту, що акцентує увагу на важливості ефективної координації, прискоренні інформаційних процесів та дотримання міжнародних стандартів, зокрема вимог ММСП.

Досягнення поставленої мети передбачає виконання комплексу взаємопов'язаних дослідницьких завдань**,** що охоплюють теоретичні, нормативні, аналітичні та прикладні аспекти інформаційного менеджменту у сфері громадського здоров'я:

1. Обґрунтувати теоретико-методологічні засади інформаційного менеджменту, визначити роль інформаційних процесів у системі реагування на надзвичайні ситуації та окреслити особливості взаємодії між системою громадського здоров'я та системою цивільного захисту в умовах кризових подій.
2. Проаналізувати нормативно-правові та організаційні засади реагування на надзвичайні ситуації у сфері громадського здоров'я та ідентифікувати проблеми та обмеження чинної моделі інформаційного забезпечення.

3. Вивчити міжнародний досвід використання цифрових систем раннього попередження та реагування (WHO EIOS, ECDC EWRS, CDC Epi-X та ін.) та визначити структурні та функціональні елементи, релевантні для адаптації в українських умовах.

4. Розробити концептуальну модель національного цифрового інструменту реагування на надзвичайні ситуації**,** визначивши його архітектуру, ключові функціональні модулі, алгоритми міжвідомчої взаємодії та вимоги до управлінського супроводу.

5. Сформулювати практичні рекомендації щодо впровадження національного цифрового інструменту**,** з урахуванням управлінських, нормативних, організаційних і технічних аспектів, а також специфіки воєнного часу й вимог Міжнародних медико-санітарних правил.

Реалізація цих завдань забезпечує комплексний управлінський підхід до удосконалення інформаційного забезпечення реагування на надзвичайні ситуації та сприятиме підвищенню оперативності прийняття рішень, посиленню міжвідомчої координації та зміцненню стійкості системи громадського здоров’я України до сучасних загроз.

Об’єкт і предмет дослідження

Об’єкт дослідження

Система реагування на надзвичайні ситуації у сфері громадського здоров’я України, її організаційні структури, механізми управління, інформаційні потоки та суб’єкти, залучені до моніторингу, оповіщення і координації дій у разі виникнення небезпечних подій.

Предмет дослідження – інформаційно-комунікаційні та управлінські механізми забезпечення реагування на надзвичайні ситуації у сфері громадського здоров’я, а також принципи, процедури, цифрові інструменти та технології, що можуть бути інтегровані в єдину систему реєстрації й оповіщення відповідно до потреб центрів контролю та профілактики хвороб, Центру

громадського здоров’я, служб екстреної медичної допомоги, Науково-практичного центру ЕМД та МК, а також Міністерства охорони здоров’я України.

Методи дослідження

Для досягнення мети та виконання завдань магістерської роботи застосовано комплекс взаємодоповнюючих наукових методів, що забезпечують всебічне дослідження управлінських, інформаційних, організаційних та нормативних аспектів реагування на надзвичайні ситуації у сфері громадського здоров’я. Вибір методів ґрунтується на принципах сучасного менеджменту, системного підходу та доказового аналізу.

1. Метод системного аналізу

Використаний для дослідження системи реагування на надзвичайні ситуації як цілісної, багатокомпонентної структури. Метод дав змогу визначити взаємозв’язки між органами цивільного захисту, Центром громадського здоров’я МОЗ України, центрами контролю та профілактики хвороб, службами екстреної медичної допомоги, Науково-практичним центром ЕМД та МК та закладами охорони здоров’я.

2. Структурно-функціональний метод

Застосований для визначення функцій і ролей суб’єктів реагування, аналізу їхніх інформаційних обов’язків і механізмів координації. Метод дав можливість систематизувати інформаційні потоки, окреслити зони відповідальності та оцінити їхню узгодженість у процесі реагування.

3. Метод порівняльного аналізу

Використаний для зіставлення української системи інформаційного забезпечення реагування з міжнародними практиками. У межах методу проаналізовано цифрові платформи та системи раннього попередження, зокрема WHO EIOS, ECDC EWRS, CDC Epi-X та інші моделі, що дозволило ідентифікувати елементи, придатні для адаптації в Україні.

4. Метод контент-аналізу нормативно-правових актів

Застосований для аналізу законодавчої та регуляторної бази України: законів, постанов Кабінету Міністрів України, наказів МОЗ, стандартів, регламентів і процедур, які визначають порядок організації реагування на надзвичайні ситуації та інформаційного обміну між суб'єктами. Метод надав можливість оцінити відповідність національної системи реагування міжнародним стандартам, зокрема вимогам ММСП.

5. SWOT-аналіз

Використаний для оцінки сильних і слабких сторін, можливостей та загроз, характерних для інформаційного менеджменту реагування на надзвичайні ситуації. Метод дозволив визначити стратегічні напрями удосконалення національної інформаційної системи.

6. Метод моделювання

Застосований для розробки концептуальної моделі єдиного цифрового інструменту реєстрації та оповіщення. У рамках моделювання визначено архітектурні елементи, функціональні модулі, алгоритми взаємодії суб'єктів та ключові управлінські параметри майбутньої системи.

Узагальнене застосування зазначених методів забезпечило комплексне наукове дослідження проблеми інформаційного забезпечення реагування на надзвичайні ситуації та дозволило сформувати обґрунтовані управлінські рішення щодо удосконалення національної системи громадського здоров'я.

Наукова новизна дослідження

Наукова новизна магістерської роботи полягає у комплексному обґрунтуванні управлінських підходів до створення та впровадження єдиного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я України**,** інтегрованого у національну систему реагування на надзвичайні ситуації та узгодженого з вимогами Міжнародних медико-санітарних правил.

Уперше:

– обґрунтовано концептуальну модель єдиного цифрового інструменту оповіщення**,** що забезпечує стандартизований, безперервний і міжвідомчий обмін інформацією між суб'єктами реагування: центрами контролю та профілактики хвороб, Центром громадського здоров'я МОЗ України, службами екстреної медичної допомоги та медицини катастроф, Науково-практичним центром ЕМД та МК, а також МОЗ України;

– запропоновано управлінську модель координації суб'єктів реагування**,** що ґрунтується на принципах інформаційного менеджменту, кризового управління та міжвідомчої інтеграції.

Удосконалено:

- підходи до організації інформаційних потоків між установами системи громадського здоров'я та службами екстреної медичної допомоги та медицини катастроф шляхом формування єдиного стандарту повідомлень, алгоритмів передачі даних та процедур міжвідомчої взаємодії;

- підхід до оцінювання ефективності інформаційного забезпечення реагування на надзвичайні ситуації**,** що включає часові параметри, швидкість і точність верифікації, структурованість інформаційних потоків та рівень координації між суб'єктами реагування.

Набули подальшого розвитку:

– теоретико-методологічні положення менеджменту у сфері громадського здоров'я**,** особливо в частині застосування цифрових технологій у реагуванні на надзвичайні ситуації;

– практичні рекомендації щодо інтеграції міжнародних систем раннього попередження та реагування (WHO EIOS, ECDC EWRS, CDC Epi-X) у національне інформаційне середовище з урахуванням організаційної структури та нормативного забезпечення функціональних підсистем МОЗ України.

– управлінські підходи до удосконалення нормативно-правового регулювання інформаційного забезпечення реагування на надзвичайні ситуації,

включно з обґрунтуванням потреби у стандартах оповіщення, процедури передачі даних і формалізації міжвідомчої комунікації.

Загалом результати дослідження формують наукове підґрунтя для створення сучасної, інтегрованої, технологічно адаптованої цифрової системи інформаційного забезпечення реагування на надзвичайні ситуації**,** здатної забезпечити швидкість, узгодженість та доказовість управлінських рішень.

Практичне значення результатів дослідження

Практичне значення дослідження полягає у розробленні прикладних управлінських рішень та інструментів, спрямованих на підвищення ефективності інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я**.** Отримані результати можуть бути використані суб'єктами реагування: центрами контролю та профілактики хвороб, Центром громадського здоров'я МОЗ України, службами екстреної медичної допомоги та медицини катастроф, Науково-практичним центром ЕМД та МК, закладами охорони здоров'я та МОЗ України.

У ході дослідження сформовано такі практичні результати:

- запропоновано модель єдиного цифрового інструменту реєстрації та оповіщення**,** що забезпечує інтегрованість інформаційних потоків, скорочує час реагування та мінімізує втрату даних;
- сформовано управлінський підхід до міжвідомчої координації**,** який може бути застосований під час розроблення стандартів інформаційної взаємодії між суб'єктами реагування;
- розроблено пропозиції щодо удосконалення нормативно-правової бази**,** включно з інтеграцією цифрової системи у функціональні підсистеми МОЗ України та уточненням алгоритмів оповіщення;
- обґрунтовано необхідність гармонізації національної інформаційної інфраструктури з міжнародними системами раннього виявлення та

попередження**,** що сприятиме виконанню вимог Міжнародних медико-санітарних правил.

– запропоновано інструменти підвищення ефективності управлінських рішень**,** які стосуються збору, верифікації, передачі інформації про небезпечні події та надзвичайні ситуації.

Отримані результати можуть бути використані для:

– формування державної політики у сфері цифровізації процесів громадського здоров’я та реагування на НС;

– розроблення проєктів нормативних актів, регламентів, стандартних операційних процедур та алгоритмів оповіщення;

– удосконалення підготовки кадрів у системі громадського здоров’я та екстреної медичної допомоги;

– модернізації існуючих інформаційних систем;

– створення навчальних модулів, тренінгів і симуляційних сценаріїв для фахівців, задіяних у реагуванні на надзвичайні ситуації.

Загалом практичне значення результатів полягає у можливості їх прямого застосування в системі громадського здоров’я України для підвищення швидкості реагування, якості міжвідомчої взаємодії та рівня захисту населення.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ У СФЕРІ ГРОМАДСЬКОГО ЗДОРОВ'Я

1.1. Менеджмент у сфері громадського здоров'я: сутність, функції та роль в умовах надзвичайних ситуацій

Менеджмент у сфері громадського здоров'я є комплексною цілеспрямованою діяльністю, спрямованою на організацію, координацію та оптимізацію процесів, що забезпечують охорону і зміцнення здоров'я населення в умовах як повсякденного функціонування, так і надзвичайних ситуацій. Згідно з сучасними підходами до управління, його зміст розкривається через функції планування, організації, мотивації, координації, комунікації та контролю, реалізація яких має забезпечувати досягнення визначених цілей системи громадського здоров'я, зокрема попередження, виявлення та мінімізацію ризиків для здоров'я населення.

В умовах надзвичайних ситуацій роль менеджменту істотно посилюється, оскільки саме якість управлінських рішень визначає швидкість вжиття заходів реагування, ефективність використання ресурсів, узгодженість дій суб'єктів реагування та здатність системи запобігати розповсюдженню негативних факторів загроз. Надзвичайні ситуації у сфері громадського здоров'я характеризуються високою динамічністю, певною невизначеністю, дефіцитом часу та необхідністю ухвалення рішень в умовах неповної інформації. За таких обставин менеджмент виконує функцію стабілізації та підтримки функціональної спроможності системи, забезпечуючи адаптацію управлінських процесів до кризового контексту.

Ключовим ресурсом менеджменту виступає інформація, яка слугує основою для ідентифікації ситуації, визначення масштабу загрози, вибору стратегії реагування та оцінювання результатів. Управління інформаційними

процесами включає своєчасне збирання даних, їхню верифікацію, аналітичну обробку, їх передачу та використання для прийняття рішень. У сфері громадського здоров'я це охоплює процеси виявлення небезпечних подій, моніторингу епідемічної, санітарної та екологічної ситуації, а також організацію комунікації між установами, що залучені до реагування.

Менеджмент у сфері громадського здоров'я виконує низку стратегічних та операційних функцій, серед яких особливого значення в умовах надзвичайних ситуацій набувають:

- планування заходів готовності та реагування на загрози для здоров'я населення;
- організація діяльності установ і служб, залучених до ліквідації наслідків надзвичайних ситуацій;
- координація взаємодії між суб'єктами реагування (ЦКПХ, ЦГЗ, ЦЕМД та МК, органами цивільного захисту, закладами охорони здоров'я тощо);
- забезпечення належного комунікаційного супроводу та обміну інформацією для формування єдиного бачення ситуації;
- контроль і моніторинг виконання заходів, оцінювання їхньої результативності та коригування управлінських рішень.

В умовах надзвичайних ситуацій особлива увага приділяється оперативності та точності інформаційних процесів, оскільки від якості даних залежить своєчасність оповіщення, коректність оцінювання ризиків і адекватність мобілізації сил та ресурсів. У цьому контексті інформаційний менеджмент розглядається як структурний елемент менеджменту у сфері громадського здоров'я та один із чинників, що визначають спроможність системи реагувати на сучасні загрози.

Отже, менеджмент у сфері громадського здоров'я є фундаментом функціонування системи реагування на надзвичайні ситуації, забезпечуючи стратегічне та оперативне управління, координацію дій суб'єктів реагування.

Ефективність цієї системи залежить від здатності організувати безперервні, стандартизовані та узгоджені між різними відомствами інформаційні процеси.

1.2. Інформаційний менеджмент у кризових ситуаціях у сфері громадського здоров'я: сутність, принципи та функції

За результатами аналізу Health Emergency and Disaster Risk Management Framework (World Health Organization) інформаційний менеджмент у сфері громадського здоров'я являє собою систему управлінських рішень і дій, спрямованих на організацію, забезпечення та оптимізацію процесів збирання, аналізу, передавання, використання та зберігання інформації, необхідної для ефективного функціонування системи реагування на надзвичайні ситуації [1]. Інформація в цьому контексті розглядається як стратегічний ресурс, який формує основу для проведення оцінки ризиків, планування заходів, координації дій і контролю результатів.

У сфері громадського здоров'я інформаційний менеджмент охоплює, зокрема, організацію комунікації між центрами контролю та профілактики хвороб, ЦГЗ, ЦЕМД та МК, НПЦЕМД та МК, закладами охорони здоров'я та органами цивільного захисту. Взаємодія цих суб'єктів реагування на основі узгоджених інформаційних процедур є необхідною умовою формування цілісної картини ситуації, що виникла, або може виникнути, а також забезпечити своєчасні та ефективні заходи реагування.

У кризових ситуаціях інформаційний менеджмент набуває особливого значення через такі чинники, як висока динамічність подій, значний обсяг інформаційних потоків, підвищений рівень невизначеності та потреба в оперативному прийнятті рішень. За цих умов інформаційний менеджмент виконує функцію забезпечення ситуаційної обізнаності, підтримки процесів оцінювання ризиків і міжвідомчої координації, створюючи інформаційну основу для організації заходів реагування.

Ефективність інформаційного менеджменту визначається дотриманням низки принципів, серед яких ключовими є:

- своєчасність - мінімізація часових затримок між моментом виявлення події та передаванням інформації відповідному суб'єкту реагування;
- достовірність - забезпечення точності, достовірності та надійності даних;
- безперервність - підтримання стійкого функціонування інформаційних каналів, включно з резервними механізмами комунікації;
- доступність - надання суб'єктам реагування доступу до необхідних даних у межах їхніх повноважень;
- стандартизованість - уніфікація форматів повідомлень, критеріїв реєстрації подій та процедур здійснення оповіщення;
- інтегрованість - узгодженість роботи інформаційних систем різних відомств, наявність єдиного інформаційного простору;
- захищеність - дотримання вимог кібербезпеки, конфіденційності та міжнародних стандартів захисту інформації.

На основі цих принципів інформаційний менеджмент у кризових ситуаціях виконує такі основні функції:

- аналітичну - опрацювання даних, формування висновків, підтримка оцінки ризиків і прогнозування розвитку подій;
- координаційну - забезпечення узгодженої взаємодії між суб'єктами реагування на основі єдиних інформаційних процедур;
- комунікаційну - організація безперервного й стандартизованого обміну інформацією;
- контрольну - моніторинг подій, контроль якості інформації та виконання визначених алгоритмів реагування;
- прогностичну - підтримка прогнозування можливих сценаріїв розвитку ситуації та визначення оптимальних управлінських рішень;
- організаційну - формування структури інформаційних процесів, регламентів взаємодії та алгоритмів обробки даних.

В умовах воєнного стану інформаційний менеджмент стикається з додатковими викликами, пов’язаними з руйнуванням інфраструктури, порушенням логістики, ризиками кібератак та масовими переміщеннями населення. Це підвищує вимоги до стійкості інформаційних систем, наявності резервних каналів зв’язку, гнучкості регламентів та здатності функціонувати в умовах обмежених ресурсів.

Розвиток цифрових технологій та міжнародних систем раннього попередження (зокрема EIOS, EWRS, Epi-X) формує нові стандарти до організації інформаційних процесів у сфері охорони здоров’я. Виконання вимог ММСП (2005) передбачає розбудову інтегрованих, стандартизованих і технологічно адаптованих систем інформаційного менеджменту [2].

Отже, інформаційний менеджмент у кризових ситуаціях є одним із ключових елементів функціонування системи реагування на надзвичайні ситуації у сфері громадського здоров’я, забезпечуючи швидкість, точність і узгодженість управлінських рішень та сприяючи підвищенню стійкості системи до сучасних загроз.

1.3. Система цивільного захисту та її інформаційно-комунікаційна складова в контексті реагування на надзвичайні ситуації у сфері громадського здоров’я

Система цивільного захисту України є сукупністю організаційних, управлінських, нормативних та інформаційно-технологічних механізмів, спрямованих на запобігання виникненню надзвичайних ситуацій, забезпечення готовності до них, організацію реагування та ліквідацію їхніх наслідків. Її правові засади визначено Кодексом цивільного захисту України, законами України, постановами Кабінету Міністрів України та міжвідомчими регламентами, що формують багаторівневу систему управління на державному, регіональному та місцевому рівнях.

Функціонування системи цивільного захисту ґрунтується на принципах централізації, координації, субординації, оперативності, інформаційної узгодженості та міжвідомчої взаємодії. Реалізація цих принципів значною мірою забезпечується через інформаційно-комунікаційну складову, яка визначає якість та швидкість обміну даними між суб'єктами реагування й, відповідно, ефективність управлінських рішень.

Інформаційно-комунікаційна складова системи цивільного захисту охоплює сукупність технологій, регламентів, платформ та каналів комунікації, що забезпечують координацію дій між органами влади, службами, установами та об'єктами критичної інфраструктури. До її ключових елементів належать:

- системи раннього оповіщення населення та служб реагування;
- державні та відомчі інформаційні мережі;
- цифрові платформи збору, накопичення та передавання даних;
- аналітичні та комунікаційні центри органів влади;
- канали інформаційної взаємодії між закладами охорони здоров'я, центрами контролю та профілактики хвороб, Центром громадського здоров'я МОЗ України, службами екстреної медичної допомоги та органами цивільного захисту.

У сфері громадського здоров'я інформаційно-комунікаційні процеси системи цивільного захисту мають визначальне значення, оскільки саме інформація ініціює вжиття заходів реагування: реєстрацію випадків захворювання, виявлення хімічних або радіаційних інцидентів, фіксацію техногенних подій чи масових уражень населення. Для ЦКПХ, ЦГЗ, ЦЕМД та МК, НПЦЕМД та МК доступ до своєчасної та верифікованої інформації є передумовою проведення оцінки ризиків, планування заходів та мобілізації сил та ресурсів.

У системі цивільного захисту та громадського здоров'я функціонує низка інституцій (суб'єктів забезпечення цивільного захисту), які формують єдиний інформаційний простір, зокрема:

– Державна служба України з надзвичайних ситуацій (ДСНС України) - координує заходи реагування, здійснює оповіщення населення, організовує ліквідацію наслідків надзвичайних ситуацій;

– органи місцевого самоврядування та комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій - забезпечують міжвідомчу координацію на регіональному та місцевому рівнях;

– ЦГЗ - виконує аналітичні, координаційні та методичні функції, у тому числі в контексті виконання вимог ММСП ;

– ЦКПХ - здійснюють епідеміологічний нагляд, первинну верифікацію та оцінку інформації, а також передавання даних по вертикалі охорони здоров'я;

– ЦЕМД та МК - фіксують події, пов'язані з масовими ураженнями, травмами, аваріями, організовують медичну допомогу;

– заклади охорони здоров'я - є первинною ланкою збору інформації про випадки захворювань, отруєнь та інших подій, що можуть становити загрозу для населення.

За результатами аналізу нормативно-правової основи системи цивільного, зокрема Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту, що затверджено постановою Кабінету Міністрів України від 27 вересня 2017 р. № 733 [3] інформаційно-комунікаційна складова заходів реагування на надзвичайні ситуації включає такі основні процеси:

1) виявлення сигналу про подію (моніторинг середовища, отримання первинної інформації від установ охорони здоров'я, екстрених служб, населення, автоматизованих систем);

2) верифікація інформації та первинна оцінка рівня загрози;

3) передавання даних суб'єктам реагування відповідно до встановлених регламентів;

4) оцінка ризиків для здоров'я населення, довкілля та інфраструктури;

5) оповіщення та інформування органів влади, служб реагування та, за потреби, населення;

6) координація дій між медичними, рятувальними та іншими службами;

7) документування та зберігання інформації для подальшого аналізу та формування політик.

Попри наявність нормативної та інституційної основи, система інформаційної взаємодії в Україні залишається фрагментованою. Серед основних проблем можна виокремити:

- відсутність єдиної цифрової системи реєстрації небезпечних подій і надзвичайних ситуацій у сфері громадського здоров'я;
- різнорідність каналів комунікації та форматів даних;
- затримки у передаванні інформації та дублювання повідомлень;
- недостатню інтеграцію між медичними та немедичними службами;
- уразливість інформаційних мереж у воєнних умовах;
- неповну відповідність окремих процедур вимогам ММСП .

В умовах воєнного стану значення стійких, стандартизованих, а також резервних каналів комунікації суттєво зростає. Від ефективності інформаційно-комунікаційної складової залежить здатність держави своєчасно ідентифікувати подію, здійснити оцінку ризику, ухвалити рішення щодо заходів реагування, запобігти поширенню загрози та мінімізувати її негативні наслідки для здоров'я населення.

Таким чином, система цивільного захисту України функціонує не лише як організаційна та управлінська структура, але й як складна інформаційно-комунікаційна мережа. Підвищення її ефективності потребує створення інтегрованого цифрового інструменту реєстрації небезпечних подій і надзвичайних ситуацій, який забезпечить єдність інформаційного простору, підвищить стійкість системи та відповідність міжнародним стандартам у сфері громадського здоров'я.

1.4. Міжнародні підходи до організації інформаційних систем реагування на надзвичайні ситуації у сфері громадського здоров'я та можливості їх адаптації в Україні

Міжнародний досвід організації реагування на надзвичайні ситуації у сфері громадського здоров'я свідчить, що ефективність управління ризиками значною мірою визначається наявністю інтегрованих, стандартизованих та технологічно розвинених цифрових систем інформаційного забезпечення. Такі системи забезпечують оперативний збір, обробку, верифікацію та обмін даними між установами охорони здоров'я, органами влади, службами екстреної допомоги, науковими інституціями та міжнародними організаціями.

Центральне місце у глобальній системі реагування на загрози здоров'ю населення посідають ММСП, які визначають вимоги до спроможності держав:

- виявляти події, що можуть становити міжнародну загрозу;
- здійснювати своєчасну оцінку ризиків;
- забезпечувати міжвідомчу координацію й обмін інформацією всередині країни;
- повідомляти ВООЗ про події, що мають потенційний міжнародний вплив, у визначені терміни.

Виконання вимог ММСП потребує наявності в країні розвиненої інформаційної інфраструктури, у тому числі цифрових платформ, які забезпечують роботу Національного координатора з питань ММСП, а також підтримують сталі інформаційні потоки та інтегрують дані з різних секторів.

У цьому контексті особливий науковий та практичний інтерес становлять такі міжнародні інформаційні системи, як:

- EIOS (Epidemic Intelligence from Open Sources, ВООЗ) - глобальна система епідеміологічної розвідки на основі відкритих джерел, що забезпечує цілодобовий моніторинг інформаційного простору, автоматизований аналіз великих масивів даних, виявлення сигналів про потенційні загрози та

передавання релевантної інформації національним органам охорони здоров'я; [4].

– EWRS (Early Warning and Response System, ЄС) - система раннього попередження і реагування на транскордонні загрози здоров'ю в Європейському Союзі, яка забезпечує оперативний обмін інформацією між країнами-членами та Європейським центром профілактики та контролю захворювань (ECDC), а також координацію заходів реагування, за результатами аналізу 5. Early Warning and Response System (EWRS) (European Centre for Disease Prevention and Control) [5];

– Epi-X (CDC, США) - національна система стандартизованого обміну інформацією між службами охорони здоров'я США, що функціонує як захищена платформа для повідомлення про події, аналітичної підтримки та прийняття управлінських рішень у режимі реального часу, як представлено інформацію на офіційному ресурсі Epi-X: The Epidemic Information Exchange (Centers for Disease Control and Prevention) [6].

Аналіз зазначених інформаційних систем дозволяє виокремити низку спільних принципів, релевантних для розбудови національної інформаційної системи в Україні:

– централізованість і наявність єдиного цифрового середовища для реєстрації та аналізу подій;

– стандартизовані протоколи повідомлень, уніфіковані критерії реєстрації подій;

– інтеграція між секторами (медицина, цивільний захист, екологія тощо);

– захищеність і стійкість каналів комунікації, здатність систем функціонувати в умовах надзвичайних ситуацій;

– використання аналітичних модулів і інструментів, орієнтованих на роботу з великими масивами даних;

– цілодобовий моніторинг подій та оперативність оповіщення;

– відповідність вимогам ММСП.

З урахуванням воєнного стану, транскордонних загроз та реформування системи громадського здоров'я, Україна має потенціал адаптувати зазначені підходи до власного контексту. Перспективним напрямом розвитку системи громадського здоров'я є впровадження національної цифрової платформи реєстрації та оповіщення про небезпечні події, призначеної для централізованого збору, обробки та поширення інформації. Така платформа має забезпечувати формування єдиної інтегрованої бази даних із можливістю взаємодії з іншими державними інформаційними ресурсами, підтримувати автоматизовані механізми верифікації інформації та оцінювання ризиків, а також реалізовувати уніфіковані алгоритми обміну повідомленнями між усіма суб'єктами реагування. Важливою вимогою є наявність захищених каналів передачі даних і резервних механізмів безперервного функціонування, а також сумісність із інформаційними системами ВООЗ та ECDC. В загальному це сприятиме підвищенню оперативності прийняття управлінських рішень, зміцненню міжвідомчої координації та ефективності реагування на загрози у сфері громадського здоров'я.

Таким чином, міжнародні підходи до організації інформаційних систем реагування на надзвичайні ситуації у сфері громадського здоров'я формують концептуальну основу для розроблення національного цифрового інструменту оповіщення в Україні. Їх адаптація сприятиме підвищенню стійкості системи громадського здоров'я, зміцненню спроможності держави щодо виконання міжнародних зобов'язань та інтеграції в європейський простір охорони здоров'я.

ВИСНОВКИ ДО РОЗДІЛУ 1

У першому розділі обґрунтовано теоретичні та методологічні засади інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я. Проведений аналіз дозволяє сформулювати такі узагальнені висновки:

1. Менеджмент у сфері громадського здоров’я визначено як системну діяльність, що забезпечує організацію, координацію та контроль функціонування установ у повсякденних і кризових умовах. Підкреслено його ключову роль у формуванні готовності та оперативності реагування на надзвичайні ситуації.

2. Інформаційний менеджмент розглянуто як центральний елемент кризового управління, що забезпечує своєчасний збір, верифікацію, аналіз та передачу даних, необхідних для ухвалення управлінських рішень. Визначено базові принципи його організації (своєчасність, достовірність, стандартизованість, інтегрованість, захищеність), які формують основу якісного інформаційного простору реагування.

3. Система цивільного захисту України охарактеризована як багаторівнева модель, ефективність якої значною мірою залежить від стану інформаційно-комунікаційної інфраструктури. Установлено, що фрагментованість інформаційних каналів, різнорідність форматів даних та недостатня інтеграція між суб’єктами реагування є ключовими проблемами сучасної системи.

4. Виявлено основні виклики інформаційної взаємодії, зокрема: відсутність єдиного цифрового інструменту реєстрації небезпечних подій, затримки у передачі інформації, дублювання повідомлень, низьку стійкість до кіберзагроз та неповну відповідність вимогам ММСП (2005). Це підтверджує необхідність модернізації інформаційної інфраструктури в секторі громадського здоров’я.

5. Обґрунтовано, що створення єдиного національного цифрового інструменту реєстрації та оповіщення про небезпечні події є логічним і необхідним кроком розвитку системи громадського здоров’я України, який забезпечить підвищення оперативності вжиття заходів реагування, узгодженість дій між суб’єктами реагування та відповідність міжнародним стандартам.

РОЗДІЛ 2
НОРМАТИВНО-ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ У СФЕРІ ГРОМАДСЬКОГО ЗДОРОВ'Я УКРАЇНИ

Нормативно-правові та організаційні засади функціонування системи реагування на надзвичайні ситуації у сфері громадського здоров'я України визначають рамкові умови для формування, руху та використання інформації, необхідної для своєчасного виявлення подій, оцінювання ризиків та координації дій суб'єктів реагування. Структура державної системи цивільного захисту, розподіл повноважень між органами влади та установами охорони здоров'я, а також встановлені правила інформування й оповіщення створюють основу для організації інформаційного менеджменту в умовах надзвичайних ситуацій.

Разом із тим, чинна модель інформаційного забезпечення характеризується фрагментованістю, неоднорідністю каналів комунікації та відсутністю єдиного цифрового інструменту реєстрації та оповіщення, що зумовлює організаційні та управлінські обмеження.

2.1. Нормативно-правові засади реагування на надзвичайні ситуації у сфері громадського здоров'я

Нормативно-правова база у сфері цивільного захисту та охорони здоров'я визначає основні принципи організації реагування на надзвичайні ситуації, структуру Єдиної державної системи цивільного захисту (ЄДСЦЗ), статус функціональних підсистем, а також загальні вимоги до інформаційного забезпечення. Ці документи формують правову основу для координації дій суб'єктів реагування, але лише частково враховують сучасні потреби цифрової інтеграції й стандартизації інформаційних процесів.

2.1.1. Кодекс цивільного захисту України [7]: правові засади державної системи реагування

Базовим нормативно-правовим актом, що визначає правові, організаційні та управлінські засади функціонування державної системи цивільного захисту, є Кодекс цивільного захисту України.

У контексті інформаційного забезпечення особливе значення мають такі положення Кодексу:

- закріплення принципів пріоритету збереження життя і здоров'я людей, превентивності, безперервності управління, централізації координації та інтегрованості заходів;
- визначення повноважень центральних і місцевих органів виконавчої влади, органів місцевого самоврядування, керівників підприємств, установ і організацій;
- встановлення структури Єдиної державної системи цивільного захисту, включно з функціональними й територіальними підсистемами;
- загальні вимоги до інформування, оповіщення населення та взаємодії між суб'єктами реагування.

Кодекс передбачає створення функціональних підсистем цивільного захисту у відповідних секторах, у тому числі у сфері охорони здоров'я, що фактично формує інституційний каркас для організації медичного реагування та санітарно-епідеміологічних заходів.

Разом із тим, положення Кодексу мають рамковий характер і не містять деталізованих вимог щодо:

- використання єдиних цифрових платформ або інформаційних систем для обміну даними;
- стандартизованих електронних форматів повідомлень;
- автоматизованих механізмів оцінки ризику та ситуаційної обізнаності.

Це створює правову основу для реагування, але не забезпечує нормативного регулювання цифрового виміру інформаційного забезпечення в системі громадського здоров’я.

2.1.2. Єдина державна система цивільного захисту: структура, рівні управління та інформаційні механізми

Організаційні засади функціонування Єдиної державної системи цивільного захисту визначено Постановою Кабінету Міністрів України від 9 січня 2014 р. № 11 «Про затвердження Положення про єдину державну систему цивільного захисту». [8].

ЄДСЦЗ включає наступе:

- органи управління;
- координаційні органи (державні, регіональні та місцеві комісії з питань техногенно-екологічної безпеки та надзвичайних ситуацій);
- сили цивільного захисту;
- функціональні та територіальні підсистеми;
- об’єкти, на яких можуть виникати небезпечні події.

Система функціонує у чотирьох режимах:

- повсякденного функціонування;
- підвищеної готовності;
- надзвичайної ситуації;
- надзвичайного стану.

Зі зміною режимів змінюється обсяг і інтенсивність інформаційних потоків, частота звітності, рівень деталізації даних і швидкість ухвалення рішень.

Постанова КМУ від 9 січня 2014 р. № 11 встановлює ключові вимоги до інформаційного забезпечення ЄДСЦЗ, зокрема:

- невідкладність надання інформації про надзвичайні ситуації;
- необхідність дотримання визначених форм оповіщення;
- вимоги до своєчасності, достовірності, повноти та цілісності даних;

– забезпечення безперервної роботи інформаційних і комунікаційних систем.

Як визначено наказом МОЗ України від 23 травня 2002 р. № 190 «Про надання позачергових повідомлень Міністерству охорони здоров'я України» [9] для сфери охорони здоров'я це стосується повідомлень про спалахи інфекційних хвороб, групові неінфекційні ураження, масові отруєння, хімічні, біологічні й радіаційні загрози, а також події з великою кількістю постраждалих.

Разом з тим, Положення про ЄДСЦЗ не визначає:

– єдиного національного цифрового інструменту, обов'язкового для всіх суб'єктів реагування;

– уніфікованих електронних форматів повідомлень;

– механізмів цифрової інтеграції систем охорони здоров'я з інформаційними системами інших відомств.

Це сприяє фрагментації практик інформування, різнорідності каналів зв'язку та ускладнює централізований аналіз ситуації.

2.1.3. Функціональні підсистеми цивільного захисту у сфері охорони здоров'я: структура, завдання та інформаційна діяльність

У межах ЄДСЦЗ у сфері охорони здоров'я функціонують функціональні підсистеми, що забезпечують організацію медичного реагування та санітарно-епідеміологічних заходів у разі надзвичайних ситуацій. Їх діяльність безпосередньо пов'язана з формуванням, рухом та аналізом інформації.

Рис.2.1. Приклад функціональних підсистем ЄДСЦЗ в ЦОВВ

Функціональна підсистема медичного захисту населення

Її діяльність регламентується наказом Міністерства охорони здоров'я України від 23 березня 2023 р. № 542 «Про затвердження Положення про функціональну підсистему медичного захисту населення єдиної державної системи цивільного захисту» [10]. До структури підсистеми належать:

- Міністерство охорони здоров'я України;
- державна установа «Український науково-практичний центр екстреної медичної допомоги та медицини катастроф МОЗ України»;
- центри екстреної медичної допомоги та медицини катастроф;
- залучені сили цивільного захисту у сфері охорони здоров'я.

Серед основних завдань підсистеми:

- організація екстреної медичної допомоги постраждалим;
- медичне сортування, евакуація та лікування постраждалих;
- моніторинг медичних наслідків надзвичайних ситуацій;

- збирання, узагальнення та передавання даних про кількість постраждалих, завантаженість закладів, потребу в ресурсах;
- інформаційна взаємодія з іншими суб'єктами ЄДСЦЗ.

Функціональна підсистема забезпечення санітарного та епідеміологічного благополуччя населення

Діяльність цієї підсистеми визначена наказом МОЗ України від 6 грудня 2022 р. № 2213 «Про затвердження Положення про функціональну підсистему забезпечення санітарного та епідеміологічного благополуччя населення єдиної державної системи цивільного захисту» [11].

До її ключових суб'єктів належать:

- Центр громадського здоров'я МОЗ України;
- центри контролю та профілактики хвороб (ЦКПХ);
- групи оперативного реагування (групи радіаційного спостереження і дозиметричного контролю, групи хімічного спостереження і контролю, групи епідеміологічного спостереження і контролю, дезінфекційні бригади, мобільні лабораторії).

Основні завдання функціональної підсистеми забезпечення санітарного та епідеміологічного благополуччя населення охоплюють:

- здійснення епідеміологічного нагляду;
- лабораторний контроль;
- реагування на інфекційні, хімічні та радіаційні загрози;
- оцінку ризиків для здоров'я населення;
- підготовку пропозицій для органів влади щодо запровадження протиепідемічних та інших захисних заходів;
- інформування населення.

Наведені положення формують цілісну правову основу функціонування підсистем, але не встановлюють єдиного цифрового механізму реєстрації та опрацювання інформації, що створює передумови для розпорошення даних і різноспрямованих практик їх передавання.

2.2. Інформаційні процеси та взаємодія між суб'єктами реагування у сфері охорони здоров'я: структура, проблеми та управлінські виклики

Інформаційні процеси у сфері громадського здоров'я в умовах надзвичайних ситуацій включають багатоступеневе збирання, верифікацію, передавання, аналіз і використання даних для прийняття управлінських рішень. Взаємодія між суб'єктами реагування - закладами охорони здоров'я, ЦКПХ, ЦГЗ, ЦЕМД та МК, ДСНС та іншими органами - має визначальне значення для своєчасного реагування та координації дій.

2.2.1. Структура інформаційних потоків між суб'єктами реагування

Типовий інформаційний цикл у системі охорони здоров'я можливо умовно поділити на такі етапи:

1. Виявлення та реєстрація сигналу про подію. Первинне інформування здійснюється на рівні закладів охорони здоров'я, бригад ЦЕМД та МК, ЦКПХ, груп оперативного реагування, а також інформація може надходити від ДСНС, Національної поліції, інших суб'єктів забезпечення цивільного захисту та населення. Форми та алгоритми надання інформації визначено наказом МОЗ від 31 жовтня 2006 р. № 686 «Про затвердження Форм первинної облікової документації з інфекційної, дерматовенерологічної, онкологічної захворюваності та інструкцій щодо їх заповнення» [12].

2. Первинна верифікація та уточнення інформації. Оцінюються достовірність повідомлення, характер загрози, орієнтовний масштаб події та необхідність подальшого реагування. Цей етап зазвичай реалізується силами ЦКПХ, центрів екстреної медичної допомоги та медицини катастроф, а також профільних підрозділів закладів охорони здоров'я.

3. Передавання інформації по вертикалі управління охорони здоров'я. Відповідно до наказу МОЗ від 21 грудня 2023 р. № 2172 «Про затвердження Плану реагування на надзвичайні ситуації Міністерства охорони здоров'я України у сфері медичного захисту населення та санітарного і епідеміологічного

благополуччя населення» [13] верифіковані дані передаються до ЦГЗ МОЗ України, відповідних ЦКПХ та структурних підрозділів МОЗ України.

4. Міжвідомче інформування. За встановленими процедурами МОЗ та ЦГЗ МОЗ інформують ДСНС України, інші центральні органи виконавчої влади, регіональні та місцеві комісії з питань ТЕБ і НС, що визначено Інструкцією щодо організації взаємодії між Державною службою України з надзвичайних ситуацій і Міністерством охорони здоров'я України в разі виникнення надзвичайних ситуацій, яка затверджена спільним наказом Міністерства охорони здоров'я України та Міністерства внутрішніх справ України 03 квітня 2018р. № 275/600 [14].

5. Оцінка ризиків та формування управлінських рішень. На основі отриманих даних визначається рівень надзвичайної ситуації, оцінюються потенційні наслідки для здоров'я населення та довкілля, формуються пропозиції щодо комплексу заходів реагування для локалізації або ліквідації наслідків події. Проведення оцінки ризиків в Україні, зокрема в системі громадського здоров'я здійснюється відповідно до Порядку проведення оцінки ризиків для здоров'я та санітарно-епідемічного благополуччя населення та здійснення за її результатами профілактичних, обстежувальних, консультаційних та інших заходів, яка затверджена наказом МОЗ від 01 вересня 2025 р. № 1373 [15]. Класифікація надзвичайних ситуацій проводиться відповідно до Постанови Кабінету Міністрів України від 17 березня 2004 р. № 368 «Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями» [16].

6. Зворотній зв'язок, координація дій та моніторинг Здійснюється організація заходів реагування, мобілізація ресурсів, маршрутизація пацієнтів, інформування населення та подальший моніторинг розвитку ситуації.

Така багаторівнева структура потребує чітких регламентів, стандартизованих форматів даних та інтегрованих цифрових каналів, оскільки

навіть незначні затримки або розриви в інформаційному ланцюзі можуть негативно позначитися на своєчасності вжиття заходів реагування.

2.2.2. Взаємодія підсистем медичного захисту населення та забезпечення санітарно-епідеміологічного благополуччя населення

Функціональні підсистеми медичного захисту населення й забезпечення санітарного та епідеміологічного благополуччя населення виконують взаємодоповнюючі ролі, а їх інформаційна взаємодія є ключовою для комплексної оцінки події та планування заходів реагування.

До основних напрямів обміну інформацією належать:

- передавання даних про постраждалих, завантаженість медичної інфраструктури та потребу в ресурсах від підсистеми медичного захисту до ЦГЗ МОЗ України та ЦКПХ;
- надання результатів лабораторних досліджень, даних епідеміологічного моніторингу та оцінки ризиків від підсистеми санітарного та епідеміологічного благополуччя населення;
- спільне формування рекомендацій для органів влади та комісій з питань ТЕБ і НС щодо встановлення рівня надзвичайної ситуації, запровадження обмежувальних та протиепідемічних заходів, необхідності інформування ВООЗ відповідно до ММСП (2005);
- узгодження дій під час подій, що включають кілька видів небезпеки (хімічні інциденти, техногенні аварії з ризиком ураження населення, комбіновані інфекційно-техногенні загрози тощо).

Попри наявність формальних регламентів, на практиці значна частина взаємодії реалізується через різні несумісні або частково формалізовані канали (телефонні дзвінки, електронні листи, відомчі інформаційні системи, окремі електронні журнали), що ускладнює стандартизацію даних і створює передумови для інформаційних розривів.

2.2.3. Основні проблеми та управлінські виклики інформаційної взаємодії

Аналіз практики функціонування інформаційних процесів у межах ЄДСЦЗ у сфері охорони здоров'я дозволяє виокремити низку системних проблем:

- відсутність єдиного національного цифрового інструменту реєстрації та оповіщення про небезпечні події й надзвичайні ситуації у сфері громадського здоров'я;
- фрагментованість інформаційних потоків між ЦКПХ, службами екстреної медичної допомоги та медицини катастроф, закладами охорони здоров'я та ЦГЗ МОЗ України;
- обмежена цифрова інтеграція з інформаційними системами ДСНС та інших центральних органів виконавчої влади;
- різний рівень цифрової готовності суб'єктів реагування, використання різних програмних рішень і форматів обліку;
- часткова відповідність вимогам Міжнародних медико-санітарних правил (2005), зокрема відсутність автоматизованих механізмів оцінки подій за Додатком 2 ММСП (2005);
- додаткові виклики воєнного часу, пов'язані з кібератаками, пошкодженням інфраструктури, необхідністю дублювання каналів зв'язку та ухвалення рішень за умов неповної інформації.

Ці проблеми суттєво обмежують потенціал існуючої моделі інформаційного забезпечення та зумовлюють потребу в її системному оновленні.

2.3. Проблеми, обмеження та системні виклики нормативно-правового регулювання інформаційного забезпечення реагування

Нормативно-правові акти у сфері цивільного захисту та охорони здоров'я визначають загальні принципи інформування, обов'язки суб'єктів реагування та регламентують взаємодію органів влади під час надзвичайних ситуацій. Водночас у низці сфер відсутня належна деталізація цифрових аспектів інформаційних процесів, що формує нормативні прогалини й обмеження. Серед них:

– відсутність нормативно закріпленого єдиного цифрового інструменту обміну інформацією між усіма суб’єктами реагування;

– невизначеність стандартизованих електронних форм повідомлень і даних у форматах, зручних для автоматичного оброблення комп’ютерними системами;

– відсутність чітких часових регламентів для передачі інформації між ланками системи;

– відсутність детальних вимог до резервування каналів зв’язку, стійкості та захищеності інформаційних систем від кіберзагроз;

– різний рівень технічної й цифрової готовності установ, що не врегульований єдиними стандартами;

– відсутність нормативно закріплених механізмів автоматизованої оцінки ризику, сумісних із Додатком 2 до ММСП;

– відсутність вимог щодо створення централізованого цифрового середовища міжвідомчої взаємодії та єдиного формату електронного документообігу між секторами.

Наведені чинники не суперечать безпосередньо чинному законодавству, однак створюють істотні організаційні обмеження, знижують оперативність і узгодженість управлінських рішень, ускладнюють адаптацію національної системи до міжнародних стандартів та вимог Міжнародних медико-санітарних правил.

ВИСНОВКИ ДО РОЗДІЛУ 2

Нормативно-правові та організаційні засади інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров’я України формують цілісну правову та інституційну рамку, яка визначає структуру ЄДСЦЗ, статус функціональних підсистем, повноваження суб’єктів реагування та загальні вимоги до інформування й оповіщення.

Разом із тим, проведений аналіз дозволяє зробити такі узагальнені висновки:

1. Наявна нормативно-правова база забезпечує структурованість і розподіл повноважень між суб’єктами реагування, але має переважно рамковий характер щодо цифрових аспектів інформаційного забезпечення.

2. Кодекс цивільного захисту України та Постанова КМУ № 11 визначають принципи, структуру та режими функціонування ЄДСЦЗ, проте не встановлюють єдиного цифрового механізму реєстрації, обробки та обміну інформацією у сфері громадського здоров’я.

3. Функціональні підсистеми медичного захисту населення та забезпечення санітарного та епідеміологічного благополуччя населення мають чітко регламентовані завдання й повноваження, однак не інтегровані в єдине цифрове середовище, що обмежує ефективність їх інформаційної взаємодії.

4. Фактична модель інформаційних процесів характеризується фрагментованістю каналів комунікації, різнорідністю форматів повідомлень, дублюванням даних, затримками в передаванні інформації та обмеженою міжвідомчою цифровою інтеграцією.

5. Нормативні прогалини у сфері стандартизованих електронних форм, часових регламентів, резервування каналів зв’язку, автоматизованої оцінки ризиків та міжвідомчої цифрової взаємодії створюють системні обмеження для оперативності та узгодженості управлінських рішень, а також ускладнюють повноцінне виконання вимог ММСП.

6. Виявлені проблеми, обмеження та системні виклики обґрунтовують об’єктивну необхідність розроблення та впровадження національного єдиного цифрового інструменту реєстрації та оповіщення про небезпечні події у сфері громадського здоров’я, який би забезпечив уніфікацію інформаційних потоків, підвищив стійкість комунікаційних систем, скоротив час реагування та створив доказову основу для прийняття управлінських рішень.

Отримані висновки реалізують друге завдання дослідження та формують підґрунтя для подальшого аналізу міжнародного досвіду цифрових систем раннього попередження й реагування, а також для розроблення концептуальної моделі національного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров’я України.

РОЗДІЛ 3
АНАЛІЗ МІЖНАРОДНОГО ДОСВІДУ СТВОРЕННЯ ЦИФРОВИХ СИСТЕМ СПОВІЩЕННЯ ПРО НАДЗВИЧАЙНІ ПОДІЇ У СФЕРІ ГРОМАДСЬКОГО ЗДОРОВ'Я

3.1. Концептуальні підходи та глобальні моделі цифрових систем раннього попередження у сфері громадського здоров'я

Ефективність реагування на надзвичайні ситуації у сфері громадського здоров'я значною мірою визначається рівнем розвитку цифрових систем раннього виявлення, обробки та передачі інформації про потенційні загрози. У міжнародній практиці такі системи стали фундаментальним елементом архітектури глобальної безпеки здоров'я, оскільки забезпечують своєчасне отримання сигналів, формування ситуаційної обізнаності, підтримку управлінських рішень та міжвідомчу координацію.

Сучасні цифрові платформи раннього попередження та реагування поєднують класичні підходи епідеміологічного нагляду з інструментами штучного інтелекту, автоматизованими аналітичними модулями, системами машинного збору даних та глобальними мережами професійного обміну. У цьому контексті вони розглядаються не лише як інструменти інформування, але і як складні багаторівневі системи управління ризиками, що забезпечують оперативність, точність та відтворюваність процедур реагування.

3.1.1. Еволюція міжнародних цифрових систем сповіщення

Поштовхом до створення сучасних цифрових систем стала потреба в оперативній міждержавній комунікації та швидкому обміні інформацією про події, які можуть становити загрозу не лише для окремої країни, а й для регіону або глобальної спільноти. Подальший розвиток технологій забезпечив можливості для:

- моніторингу відкритих джерел у режимі реального часу;
- автоматизації виявлення аномалій;

- побудови аналітичних моделей прогнозування подій;
- швидкого міжвідомчого інформування;
- інтеграції лабораторних, клінічних та ситуаційних даних.

Сучасні системи (EIOS, EWRS, Epi-X) поєднують дані різної природи - від офіційних повідомлень, електронних медичних записів та лабораторних даних до новинних стрічок, соціальних мереж і супутникових джерел.

3.1.2. Основні принципи функціонування міжнародних цифрових систем

Міжнародні системи раннього попередження ґрунтуються на низці базових принципів, що визначають їх ефективність:

1. Своєчасність - мінімізація часу між виявленням сигналу та його опрацюванням;
2. Чутливість і специфічність - здатність виявляти події, що становлять загрозу, та мінімізувати хибні сигнали;
3. стандартизація інформаційних процесів - єдині формати повідомлень, параметри ризику, критерії верифікації подій;.
4. міжвідомча та міждержавна інтеграція - залучення служб охорони здоров'я, лабораторій, служб надзвичайних ситуацій, безпеки, екологічного контролю;
5. інтероперабельність - здатність систем обмінюватися даними та технологічна сумісність між різними платформами;
6. аналітична підтримка управлінських рішень - використання алгоритмів ризик-аналізу, аналітичних панелей, автоматизованої класифікації подій;
7. кібербезпека та захист даних - дотримання вимог до конфіденційності, резервування каналів та стійкості систем.

Ці принципи є універсальними та застосовуються у всіх глобальних системах, що забезпечує їхню стабільність і масштабованість, як зазначено в роботі Ayebare R., Moriyón O.J., Grant L., et al. Event-based surveillance for outbreak

detection in low-resource settings: opportunities and challenges (BMC Public Health) [17].

3.1.3. Архітектурні моделі цифрових систем раннього попередження

У міжнародній практиці виділяють три узагальнені моделі архітектури цифрових систем:

1) Централізована модель.

Характеризується наявністю єдиного центру збору та обробки інформації.
Приклад: EWRS (ЄС).
Переваги: стандартизація процесів, швидкість реагування.
Недоліки: залежність від централізованого сервера, потреба в уніфікації процедур.

2) Федеративна модель.

Передбачає збереження автономії учасників із можливістю обміну структурованими даними.
Приклад: Epi-X (CDC).
Переваги: гнучкість, доступ до інформації різного рівня, можливість використання локальних систем.
Недоліки: потреба у високій організаційній координації.

3) Гібридна модель.

Поєднує централізоване управління з децентралізованими аналітичними інструментами.
Приклад: EIOS (ВООЗ).
Переваги: масштабованість, використання відкритих джерел, машинне навчання.
Недоліки: необхідність обробки великого масиву даних.

Розуміння цих моделей дозволяє оцінити, які підходи можуть бути адаптовані під потреби України.

3.1.4. Типові функціональні модулі міжнародних систем

Аналіз провідних цифрових платформ показує, що всі вони містять подібні ключові модулі:

- модуль збору даних (офіційні джерела, відкриті дані, лабораторні результати, медичні реєстри);
- модуль автоматизованої фільтрації сигналів (машинне навчання, алгоритмічні правила);
- модуль епідемічної розвідки - виявлення аномалій, класифікація повідомлень;
- модуль верифікації - участь національних контактних пунктів або фахівців;
- модуль ситуаційної обізнаності - аналітичні панелі, карти, дашборди;
- модуль оперативного сповіщення - автоматизовані повідомлення, рекомендації, міжвідомче інформування;
- модуль безпеки та управління доступом - шифрування, багаторівнева автентифікація, розмежування ролей.

Наявність таких модулів є передумовою функціонування будь-якої сучасної системи епіднагляду.

3.1.5. Значення міжнародних систем у реалізації Міжнародних медико-санітарних правил (2005)

Цифрові системи раннього попередження є ключовими інструментами виконання вимог ММСП (2005), зокрема положень щодо:

- моніторингу подій, що можуть становити загрозу міжнародній безпеці здоров’я;
- оперативного інформування Національного координатора з питань ММСП;
- оцінки подій за алгоритмом Додатку 2 ММСП (2005);
- забезпечення міжнародної комунікації;
- попередження транскордонного поширення інфекцій.

Таким чином, міжнародні цифрові системи не лише забезпечують інформаційну підтримку реагування, а й формують нормативний контекст, у якому повинна розвиватися національна система України.

3.2. Глобальна система епідеміологічної розвідки ВООЗ EIOS (Epidemic Intelligence from Open Sources): можливості, структура та значення для України

Глобальна система епідеміологічної розвідки ВООЗ EIOS (Epidemic Intelligence from Open Sources) є одним із ключових інструментів раннього виявлення ризиків для громадського здоров'я на міжнародному рівні. Її роль стрімко зросла у зв'язку з глобалізацією інформаційних потоків, збільшенням кількості небезпечних подій, воєнними конфліктами, міграцією населення та швидким поширенням інфекційних захворювань. EIOS забезпечує цілодобовий моніторинг відкритих джерел інформації та автоматизовану аналітичну підтримку державам - учасникам Міжнародних медико-санітарних правил (2005) у процесі виявлення і реагування на потенційні загрози.

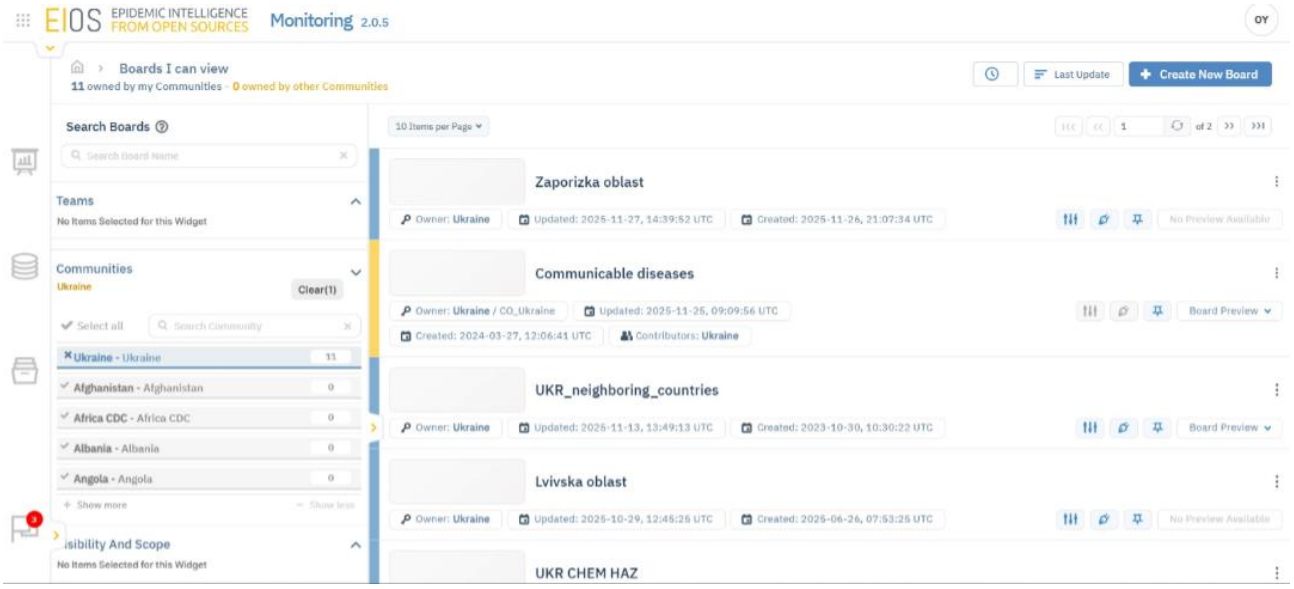

Рисунок.3.1. Дошка новин в системі EIOS

3.2.1. Організаційно-правові засади та місце EIOS у глобальній системі реагування ВООЗ.

EIOS є складовою глобальної архітектури безпеки здоров'я, яку адмініструє ВООЗ відповідно до Міжнародних медико-санітарних правил (IHR 2005). Система створена для підтримки держав у виконанні ключових обов'язків за ММСП, зокрема:

- виявлення подій, що можуть мати міжнародне значення;
- оцінка ризиків відповідно до Додатку 2 ММСП (2005);
- вчасне інформування Національного координатора з питань ММСП;
- забезпечення міждержавного обміну інформацією у режимі реального часу.

EIOS не замінює національні системи раннього попередження, а доповнює їх, дозволяючи країнам отримувати сигнали про події, що не були виявлені внутрішніми джерелами.

3.2.2. Архітектура системи EIOS та її ключові компоненти.

EIOS поєднує методи аналітики великих даних (Big Data), машинного навчання та автоматичного семантичного аналізу текстів. Архітектура платформи включає такі ключові елементи:

1. Модуль збору інформації з відкритих джерел.

Система збирає дані з більш ніж 10 000 інформаційних каналів, включно з:

- онлайн-ЗМІ;
- офіційними публікаціями;
- соціальними мережами;
- спеціалізованими моніторинговими платформами;
- регіональними інформаційними ресурсами;
- науковими оглядами та бюлетенями.

Алгоритми EIOS працюють у режимі 24/7.

2. Модуль автоматизованої обробки та класифікації даних.

За допомогою обробки природної мови (NLP):

– текст аналізується на предмет релевантності,

– інформація класифікується за типом загрози (інфекційна, хімічна, радіаційна, екологічна),

– визначаються ключові ознаки події (місце, час, кількість постраждалих, тип збудника тощо).

3. Модуль аналітики та ризик-індикаторів.

Система пропонує аналітичні функції:

– автоматичне групування схожих повідомлень;

– визначення трендів;

– виявлення аномалій;

– формування сигналів високого ризику.

Цей модуль використовується багатьма національними центрами для формування ситуаційної обізнаності.

4. Панелі моніторингу для користувачів (дашборди).

Панелі дозволяють:

– налаштовувати категорії моніторингу;

– відстежувати події у реальному часі;

– будувати карти загроз;

– експортувати дані для внутрішніх систем аналізу.

5. Модуль спільної роботи.

Призначений для:

– обговорення сигналів між аналітиками різних країн;

– спільної верифікації подій;

– підготовки матеріалів для оцінки ризику.

Це ключова частина міжнародної взаємодії у рамках ММСП (2005).

3.2.3. Значення EIOS для систем раннього попередження та виконання ММСП.

EIOS є ефективним інструментом для:

- виявлення подій, які не потрапляють у національні системи моніторингу;
- раннього виявлення інформаційних аномалій, що свідчать про потенційний спалах;
- виявлення транскордонних загроз;
- підтримки Національного координатора з питань ММСП у підготовці повідомлень до ВООЗ;
- забезпечення обміну інформацією в режимі реального часу.

За результатами аналізу Artificial intelligence in epidemic intelligence systems: improving early detection of public health threats (BMC Public Health, 2025) [18] у період пандемії COVID-19 EIOS стала одним із основних джерел глобальної ситуаційної обізнаності для держав-учасників ММСП.

3.2.4. Практична цінність EIOS для України та її можливі напрями інтеграції.

В умовах збройної агресії проти України та значного зростання кількості небезпечних подій (хімічних, екологічних, інфекційних), EIOS є важливим інструментом підсилення національної системи реагування.

Для України ключове значення можуть мати такі елементи:

1. Розширення можливостей епідеміологічної розвідки.

Система дозволяє отримувати дані про:

- спалахи в країнах-сусідах,
- хімічні та промислові інциденти,
- інформацію про міграційні потоки,
- зміни у захворюваності на прикордонних територіях.

2. Підтримка Національного координатора з питань ММСП.

EIOS надає інформацію для оцінювання ризиків відповідно до Додатку 2 ММСП.

3. Резервний канал ситуаційної обізнаності.

В умовах руйнування інфраструктури або кібератак EIOS може виконувати роль зовнішнього незалежного джерела первинних сигналів.

4. Інтеграція з майбутньою українською цифровою платформою.

Україна може:

- налаштувати автоматичний імпорт релевантних сигналів EIOS,
- інтегрувати модулі EIOS у національний інструмент реагування,
- адаптувати підходи NLP та класифікації подій.

5. Методична та технічна підтримка ВООЗ.

ВООЗ надає державам:

- аналітичні моделі,
- інструменти прогнозування,
- тренінги для аналітиків,
- методичні рекомендації.

Це сприятиме професійному розвитку української системи епідеміологічного нагляду.

3.2.5. Аспекти міжнародної взаємодії та значення для України.

Досвід EIOS демонструє, що ефективна міжнародна система епідеміологічної розвідки повинна:

- мати доступ до великих масивів відкритих даних;
- використовувати сучасні технології машинного навчання;
- забезпечувати оперативну класифікацію та аналіз сигналів;
- підтримувати механізми спільної роботи між різними країнами;
- бути інтегрованою в глобальну архітектуру ММСП.

Для України важливим аспектом є необхідність створення централізованої платформи для прийому та аналізу сигналів включно із впровадженням автоматизованих алгоритмів оцінки ризику, що дозволить забезпечити міжвідомчу інтеграцію та розбудувати систему ситуаційної обізнаності, що працює у реальному часі.

3.3. Національна система епідеміологічного сповіщення CDC Epi-X (США): структура, функції та управлінська модель

Система Epi-X (Emergency Preparedness and Information Exchange) - це захищена цифрова платформа Центрів з контролю та профілактики захворювань США (CDC), призначена для оперативного обміну інформацією про події, що становлять ризик для громадського здоров'я. Система функціонує як ключовий інструмент кризової комунікації, який забезпечує швидке виявлення небезпечних подій, підтримку аналітичних процесів і міжвідомчу координацію на національному рівні.

Epi-X вважається одним із найефективніших прикладів національної системи епідемічного сповіщення, що забезпечує високу оперативність, стандартизованість, кіберстійкість та управлінську інтеграцію.

3.3.1. Загальна характеристика та правові засади функціонування Epi-X.

Epi-X була створена CDC як централізована платформа для служб охорони здоров'я різних рівнів: місцевих, штатних, федеральних та спеціалізованих підрозділів CDC. Її робота ґрунтується на таких основних принципах:

- чинне федеральне законодавство США у сфері громадського здоров'я та реагування на загрози;
- національні стандарти безпеки даних (HIPAA, FISMA, NIST);
- управлінські рішення CDC, що регламентують порядок повідомлень, алгоритми перевірки інформації та механізми міжвідомчої взаємодії.

Інформаційна система охоплює повний спектр подій, що мають значення для громадського здоров'я, включаючи випадки інфекційних захворювань, хімічні та радіаційні інциденти, спалахи невстановленої етіології, події з великою кількістю постраждалих, а також загрози для біобезпеки та потенційні прояви біотероризму. Такий широкий спектр охоплення дозволяє забезпечити своєчасне виявлення різнопрофільних загроз, інтегровану оцінку ризиків і комплексне реагування відповідно до природи інциденту.

3.3.2. Архітектура та ключові компоненти системи Epi-X.

Архітектура Epi-X розроблена з урахуванням високих вимог до інформаційної безпеки, швидкості передачі даних та персональної відповідальності посадових осіб за достовірність і верифікацію поданої інформації. Система функціонує як багаторівнева цифрова платформа, що об'єднує процеси реєстрації подій, їх фахової оцінки, аналітичного опрацювання та оперативного обміну повідомленнями між усіма структурами, залученими до реагування на загрози громадському здоров'ю.

Її робота розпочинається з модуля реєстрації подій, у межах якого уповноважені фахівці CDC або епідеміологи штатів вносять стандартизовані дані про інцидент: місце виникнення, дату та час, характеристику загрози, попередню оцінку ризику, а також інформацію про постраждалих і служби, що брали участь у реагуванні. Стандартизація форми дозволяє мінімізувати ризики помилок, втрати критично важливих даних і забезпечує високу інтероперабельність інформаційних потоків. Внесена інформація автоматично передається до модуля фахової верифікації, де аналітики CDC здійснюють багаторівневу перевірку: уточнюють деталі, підтверджують достовірність джерел, коректують класифікацію події, оцінюють рівень загрози та визначають її пріоритетність у контексті необхідності подальшого реагування. Така процедура забезпечує високу якість даних, що надходять до системи, та унеможливлює поширення недостовірної або неповної інформації.

Після завершення верифікації Epi-X автоматизовано активує механізм розсилки сповіщень відповідним органам і партнерам: місцевим департаментам охорони здоров'я, спеціалізованим лабораторіям, центрам із реагування на надзвичайні ситуації CDC та федеральним інституціям, які можуть бути залучені до подальших дій. Завдяки цьому забезпечується швидка циркуляція підтвердженої інформації та можливість оперативного реагування відповідно до рівня загрози. Паралельно система використовує вбудований аналітичний інструментарій для виявлення тенденцій і аномалій, групування подій за типами або регіонами, побудови ситуаційних карт і формування коротких аналітичних

оглядів, що слугують підтримкою для управлінських рішень і стратегічного планування.

Окремим важливим компонентом є захищене середовище співпраці, яке забезпечує можливість обговорення подій у режимі реального часу, проведення спільної аналітики фахівцями різних штатів та координації між різними агентствами. Це середовище підсилює прозорість взаємодії, сприяє швидкому узгодженню управлінських рішень і забезпечує цілісність процесу реагування на загрози.

У своїй сукупності всі елементи архітектури Epi-X формують стійку, безпечну та ефективну систему швидкого обміну інформацією та аналітичної підтримки, що є ключовою для своєчасного виявлення подій, оцінювання ризиків і прийняття рішень у сфері громадського здоров’я.

3.3.3. Механізми управління, координації та відповідальності.

Ефективність Epi-X забезпечується цілісною та чітко вибудованою управлінською моделлю, яка поєднує структуроване розмежування повноважень, регламентовані часові рамки, багаторівневий контроль якості даних та розвинену міжвідомчу координацію. Система функціонує на принципі послідовного руху інформації: локальні установи здійснюють первинний збір даних і формування початкових повідомлень; органи штатів відповідають за їх змістову верифікацію, уточнення та підтвердження; CDC виконує глибинний аналіз, інтеграцію з іншими інформаційними потоками та координацію національного реагування. Така модель гарантує структурованість процесу та уникнення дублювання функцій.

Чітко встановлені часові регламенти визначають максимально допустимий час для кожного етапу роботи — від моменту первинного повідомлення до його верифікації та подальшої розсилки критично важливих сповіщень. Дотримання цих строків контролюється через систему показників якості, які безпосередньо впливають на оцінку ефективності роботи установ та формують культуру оперативності й дисципліни у сфері епідеміологічного нагляду.

Паралельно Epi-X забезпечує багаторівневий контроль якості інформації: технічну перевірку повноти й коректності заповнення полів, експертну оцінку достовірності та відповідність даних стандартам CDC. Це гарантує високий рівень валідності інформації, що надходить до системи, та її придатність для прийняття управлінських рішень.

Важливою складовою моделі є міжвідомча інтеграція. Платформа здатна взаємодіяти з національною мережею лабораторій (LIMS), службами екстреного реагування, центрами управління кризовими ситуаціями та низкою федеральних програм безпеки, що забезпечує комплексність реагування та інформаційну сумісність у масштабах країни. У сукупності ці елементи формують стійку, надійну та високоефективну систему управління подіями, що мають значення для громадського здоров'я.

3.3.4. Ключові переваги Epi-X як моделі національної системи сповіщення.

Серед значних переваг системи Epi-X є:

1) централізованість - одна база даних для всієї країни;
2) стандартизованість повідомлень - уніфіковані протоколи і форми;
3) кіберзахищеність - відповідність федеральним стандартам безпеки;
4) автоматизація аналітики - аналіз трендів, сигналів, ризиків;
5) інтеграція між секторами - медицина, лабораторії, рятувальники, безпека;
6) оперативність відповідей - сповіщення в межах хвилин;
7) підтримка кризового управління CDC - пряма інтеграція з Національним центром реагування (EOC CDC).

Ці особливості роблять Epi-X еталоном для країн, що прагнуть розвивати власні цифрові платформи безпеки здоров'я.

3.3.5. Елементи Epi-X, релевантні для адаптації в Україні.

Українська система реагування на надзвичайні ситуації може ефективно адаптувати ключові підходи, закладені в архітектуру Epi-X, інтегрувавши їх у національну цифрову інфраструктуру громадського здоров'я. Насамперед

йдеться про створення єдиного цифрового інструменту для реєстрації подій різного походження — хімічних, біологічних, радіаційних, техногенних та екологічних. Стандартизовані форми збору даних дозволять уніфікувати інформаційні потоки, зменшити кількість помилок, усунути непорівнянність повідомлень та забезпечити сумісність між установами.

Важливим кроком може стати впровадження нормативно закріплених часових стандартів передавання інформації, що визначатимуть максимальний час на первинне повідомлення, його верифікацію та подальшу передачу до відповідних органів. Це створить передумови для підвищення оперативності реагування, а також дозволить використовувати показники дотримання строків як індикатори ефективності роботи установ.

Запровадження модуля експертної верифікації сприятиме усуненню дублювання інформації, фільтрації недостовірних даних та підвищенню точності оцінки ризиків шляхом аналітичного доопрацювання первинних повідомлень перед їх передачею в систему національного реагування. Водночас створення захищеного середовища міжвідомчої взаємодії забезпечить єдине комунікаційне поле та прозору координацію між МОЗ, ДСНС, ЦКПХ, Центром громадського здоров’я та іншими суб’єктами, залученими до реагування на події.

Аналітичні модулі, включно з інструментами автоматизованого аналізу ризику, можуть бути інтегровані в модель національного цифрового інструменту, що наразі розробляється в Україні, забезпечивши виявлення тенденцій, аналіз сценаріїв, формування ситуаційних карт та підтримку управлінських рішень. Окрему цінність ці елементи можуть мати для роботи Національного координатора з питань ММСП, оскільки дозволять прискорити підготовку повідомлень до ВООЗ, забезпечити відповідність вимогам Додатку 2 ММСП (2005) та підтримувати високий рівень ситуаційної обізнаності. У сукупності ці підходи створюють основу для побудови відкаліброваної, технологічно стійкої та стратегічно орієнтованої системи реагування на небезпечні події та надзвичайні ситуації в Україні.

3.3.6. Значення досвіду Epi-X для розвитку української системи інформаційного забезпечення реагування.

Досвід Epi-X демонструє важливість:

- централізації інформаційних потоків,
- цифрової інтеграції між секторами,
- наявності єдиних стандартів і форм,
- захисту інформації,
- національної відповідальності за якість даних,
- аналітичної підтримки прийняття рішень.

Ці елементи можуть стати основою для проектування українського цифрового інструменту реєстрації та оповіщення, що відповідатиме міжнародним стандартам і вимогам ММСП.

3.4. Система раннього попередження та реагування Європейського Союзу (EWRS) та платформа епідеміологічного нагляду TESSy: структура, функції та релевантність для України

Система раннього попередження та реагування Європейського Союзу (EWRS) та європейська платформа епідеміологічного нагляду TESSy є центральними цифровими інструментами, що забезпечують координацію дій держав-членів ЄС у межах реагування на транскордонні загрози здоров'ю. Їх функціонування регулюється законодавством ЄС і організаційно підтримується Європейським центром профілактики та контролю захворювань (ECDC). EWRS та TESSy вважаються найефективнішими та найбільш стандартизованими системами епідеміологічного нагляду в Європейському регіоні, що робить їхнім аналіз надзвичайно важливим для адаптації відповідних елементів в Україні.

3.4.1. Правові засади функціонування EWRS та роль ECDC.

Система EWRS створена відповідно до Регламенту (EU) 2022/2371 «Про серйозні транскордонні загрози здоров'ю», який визначає порядок оповіщення, обміну інформацією, проведення оцінки ризиків і координації заходів

реагування між країнами ЄС. EWRS є обов'язковою для всіх держав-членів та координується ECDC у тісній співпраці з Європейською Комісією.

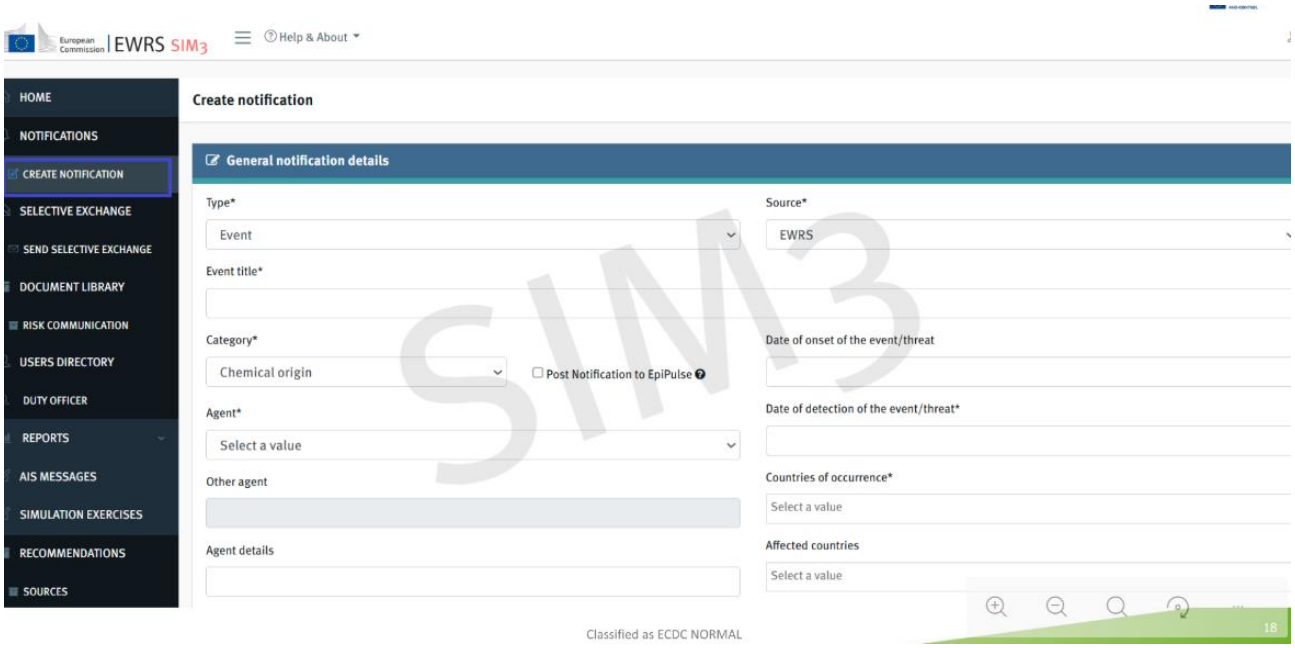

Рис.3.2. Версія EWRS у щорічній вправі JADE 2025

Ключові юридичні положення визначають функціонування EWRS :

- обов'язок держав-членів повідомляти про серйозні загрози здоров'ю впродовж визначеного часу;
- проведення стандартизованої оцінки ризиків ECDC;
- обмін інформацією у захищеному цифровому середовищі;
- ініціювання спільних заходів реагування;
- інтеграцію з лабораторними та епідеміологічними мережами.

EWRS функціонує як центральний цифровий канал інформування між державами ЄС та дозволяє здійснювати оперативне реагування у масштабі всього регіону.

3.4.2. Архітектура та ключові функціональні модулі EWRS.

EWRS має чітко структуровану архітектуру, орієнтовану на безперервний обмін інформацією між країнами-членами та наднаціональними органами. Основні модулі системи включають:

1. Модуль раннього сповіщення.

Забезпечує оперативну передачу інформації про події, що можуть становити транскордонну загрозу:

- спалах інфекційної хвороби;
- хімічні або біологічні інциденти;
- радіаційні події;
- незвичні кластери захворювань;
- загрози з невстановленим етіологічним фактором.

Повідомлення містить стандартизовані поля: опис події, часові рамки, епідемічні характеристики, популяційні ризики, запропоновані заходи реагування.

2. Модуль оцінки ризиків.

ECDC проводить:

- оцінку ризику для населення ЄС;
- аналіз можливого поширення;
- рекомендації для держав-членів;
- пропозиції щодо координаційних дій.

3. Комунікаційний модуль.

Дає змогу державам-членам:

- уточнювати інформацію;
- обмінюватися технічними деталями;
- узгоджувати заходи реагування.

Цей модуль забезпечує міждержавну комунікацію в режимі реального часу.

4. Модуль координації спільних заходів.

Дає змогу ініціювати і координувати:

- спільні розслідування;
- міжнародні епідеміологічні групи;
- лабораторні дослідження;
- транскордонні заходи з управління ризиками.

5. Модуль захищеної передачі даних.

Забезпечує:

- шифрування інформації;
- контроль доступу;
- аудит інформаційних сесій.

3.4.3. Система TESSy: структура та значення для європейського епідеміологічного нагляду.

TESSy (The European Surveillance System) - централізована цифрова платформа ECDC, призначена для збору, гармонізації та аналізу даних епідеміологічного нагляду з усіх країн ЄС та ЄЕЗ.

Її ключові функції:

- стандартизований збір епідеміологічних та лабораторних даних;
- інтеграція даних понад 90 систем спостереження;
- підтримка моделювання поширення хвороб;
- формування європейських аналітичних звітів;
- підтримка EWRS та інших мереж ECDC.

Рис.3.3. Новина в системі TESSY щодо захворюваності вірусом чикунгунья, для материкової частини ЄС/ЄЕЗ

Основними елементами TESSy є:

1. Модуль завантаження даних (Upload Module) - приймає уніфіковані електронні формати даних.

2. Модуль валідації - перевірка на відповідність стандартам ECDC.

3. Аналітичний модуль - автоматичне створення індикаторів, епідемічних кривих, карт, моделей поширення.

4. Модуль інтеграції з лабораторними системами - поєднання геномних, мікробіологічних та епідемічних даних.

5. Модуль доступу для фахівців - багаторівнева система доступу відповідно до ролей.

3.4.4. Значення EWRS та TESSy для реагування на транскордонні загрози.

Системи EWRS та TESSy довели свою ефективність у період пандемії COVID-19, під час спалахів mpox, холери, кору, поліомієліту та хімічних інцидентів у ЄС. Їх ключове значення полягає у:

- прискоренні міждержавного обміну інформацією;
- стандартизації повідомлень, критеріїв реєстрації та оцінки подій;
- забезпеченні єдиного аналітичного середовища;
- інтеграції лабораторних, клінічних та епідемічних даних;
- моделюванні розвитку подій і підтримці рішень;
- виконанні міжнародних зобов’язань відповідно до IHR 2005.

EWRS фактично є цифровим елементом безпеки здоров’я Європейського Союзу.

3.4.5. Релевантні для України елементи EWRS і TESSy.

Аналіз структурних і функціональних характеристик EWRS та TESSy дозволяє визначити низку компонентів, які можуть бути адаптовані в Україні:

1. Стандартизовані електронні форми повідомлень з чіткими параметрами події, вірусологічної інформації, лабораторних результатів.

2. Єдиний захищений канал комунікації між суб’єктами реагування, подібний до EWRS.

3. Автоматизована оцінка ризику, що може бути адаптована на основі підходів ECDC.

4. Інтеграція епідеміологічних та лабораторних даних, аналогічно TESSy.

5. Можливість обміну інформацією в реальному часі з міжнародними партнерами, у т. ч. ЄС та ВООЗ.

6. Багаторівнева система доступу, що передбачає розмежування повноважень і відповідальності різних суб’єктів.

7. Аналітичні панелі ситуаційної обізнаності, що дозволяють створювати єдину картину подій.

3.4.6. Значення досвіду ЄС для побудови національного цифрового інструменту України.

Досвід Європейського Союзу, зокрема функціонування систем EWRS та TESSy, має важливе стратегічне значення для формування українського національного цифрового інструменту раннього виявлення та реагування на загрози громадському здоров’ю. Європейська модель демонструє, що ефективна система попередження повинна працювати як централізоване цифрове середовище, у межах якого всі повідомлення реєструються, обробляються та передаються за уніфікованими правилами та процедурами. Стандартизація форматів даних є критичною умовою для забезпечення точності, повноти та сумісності інформації, що циркулює між установами охорони здоров’я, лабораторіями, системами цивільного захисту та іншими суб’єктами реагування.

Інтегрований підхід, характерний для системи ЄС, об’єднує в одному інформаційному контурі різні операційні сектори — клінічний, лабораторний, епідеміологічний, логістичний і кризовий — що дозволяє забезпечити комплексне бачення та своєчасне прийняття рішень. Аналітична орієнтованість, включно з автоматизованим аналізом, прогнозуванням і моделюванням ризиків,

посилює здатність системи до раннього виявлення загроз, зменшує час реагування та підвищує точність оцінки ситуації.

Невід'ємним компонентом є високий рівень кіберстійкості та наявність резервних каналів і механізмів безперервності роботи, що гарантують незмінність функціонування системи в умовах надзвичайних ситуацій або кібератак. Інтероперабельність, тобто здатність до обміну інформацією з міжнародними платформами (зокрема з ВООЗ, ECDC та суміжними європейськими системами), є ключовим чинником забезпечення транскордонної готовності та виконання міжнародних зобов'язань.

Усі ці принципи — централізація, стандартизація, інтеграція, аналітична спрямованість, захищеність та інтероперабельність — повинні бути враховані під час розроблення української національної цифрової системи сповіщення та інформаційного забезпечення реагування на надзвичайні ситуації. Їх імплементація дозволить створити сучасний, стійкий та міжнародно сумісний інструмент, який забезпечить підвищення рівня епідеміологічної готовності, ситуаційної обізнаності та оперативності управлінських рішень у сфері громадського здоров'я України.

3.5. Порівняльний аналіз міжнародних цифрових систем сповіщення про надзвичайні події у сфері громадського здоров'я та можливості їх адаптації в Україні

Аналіз міжнародних цифрових систем раннього попередження та реагування - EWRS (ЄС), TESSy (ECDC), EIOS (ВООЗ) та Epi-X (CDC, США) - дозволяє виокремити ключові характеристики, які зумовлюють їхню ефективність у забезпеченні інформаційної готовності держав до реагування на надзвичайні події у сфері громадського здоров'я. Порівняння цих систем дає можливість визначити найбільш релевантні інструменти та управлінські підходи, які можуть бути адаптовані до українського контексту з урахуванням

чинних нормативних обмежень, воєнного стану та реформування системи громадського здоров’я.

3.5.1. Ключові характеристики і функціональні можливості міжнародних систем.

Порівняльний аналіз чотирьох систем демонструє, що їхня ефективність базується на спільних групах характеристик.

1. Централізованість та єдиний цифровий простір.

EWRS: централізована платформа для країн ЄС.

TESSy: єдина база епідемічних даних для усієї Європи, що представлено на офіційному ресурсі European Centre for Disease Prevention and Control (European Surveillance System (TESSy)) [19].

EIOS: глобальна централізована система агрегування відкритих джерел.

Epi-X: федеральна платформа для всіх штатів США.

Досвід для України:

створення єдиного центру збору і верифікації даних, який інтегрує інформацію від ЦКПХ, ЕМД, ДСНС, закладів охорони здоров’я.

2. Стандартизовані форми повідомлень і протоколи комунікації.

У всіх системах існують уніфіковані шаблони:

- тип події;
- місце;
- опис загрози;
- первинна оцінка ризику;
- рекомендації для реагування.

Стандартизованість дозволяє:

- уникати дублювання між інституціями;
- забезпечувати можливість автоматичного аналізу;
- формувати одноманітні та якісні дані.

Досвід для України:

нормативно закріпити електронну форму повідомлення про подію разом із стандартизованим переліком полів.

3. Високий рівень інформаційної безпеки:

- EWRS та TESSy працюють у захищеному середовищі ECDC.
- Epi-X відповідає вимогам HIPAA, FISMA та NIST.
- EIOS забезпечує багаторівневий захист даних із глобальним резервуванням.

Досвід для України**:**

забезпечення кіберстійкості та дублювання каналів зв'язку - ключова вимога в умовах війни.

4. Механізми експертної верифікації інформації:

- EWRS: верифікація через ECDC та національні Focal Points.
- TESSy: контроль якості даних при завантаженні.
- EIOS: модерація та аналітична фільтрація сигналів.
- Epi-X: обов'язкова експертна перевірка CDC.

Досвід для України:

впровадження в цифровій системі ролі верифікатора (оператора ризику), який підтверджує або відхиляє інформацію до її поширення.

5. Автоматизована аналітика та підтримка управлінських рішень:

- EWRS: прогнозування поширення інфекцій.
- TESSy: інструменти аналізу тенденцій і порівняння між країнами.
- EIOS: машинне навчання для виявлення аномалій.
- Epi-X: аналітичні огляди та трендовий аналіз.

Досвід для України:

автоматизований аналіз ризику має бути частиною національної системи, зокрема модуль оцінки відповідно до Додатку 2 ММСП (2005).

6. Цілодобова робота та оперативність:

- EWRS - 24/7 оперативність у транскордонних загрозах.

- Epi-X - негайне інформування служб CDC.
- EIOS - безперервний глобальний моніторинг.

Урок для України:

впровадження моделі чергування та оперативних чергових у рамках цифрової платформи.

Таблиця 3.1. Порівняльна таблиця ключових елементів систем

Характеристика	EWRS	TESSy	EIOS	Epi-X	Релевантність для України
Єдиний центр управління	+	+	+	+	Критично важливо
Стандартизовані повідомлення	+	+	частково	+	Потребує нормативного врегулювання
Автоматизований аналіз	+	+	+++	++	Висока пріоритетність
Захищені канали зв'язку	+	+	+	+++	Особливо важливо у воєнний час
Підтримка міжвідомчої взаємодії	+	+	+++	++	Відсутня в Україні
Оцінка ризику у реальному часі	+	+	+++	+	Потребує впровадження
Підтримка виконання IHR	+++	++	+++	++	Критична вимога
Інтеграція лабораторних даних	++	+++	+	++	Потрібно розвивати

3.5.3. Виявлені ключові елементи, що є релевантними для адаптації в Україні.

Узагальнення міжнародного досвіду дає змогу виокремити низку структурних та функціональних елементів, які є пріоритетними для адаптації під час розроблення національного цифрового інструменту України. Насамперед ідеться про формування єдиного національного цифрового реєстру небезпечних подій, який має замінити наявні фрагментовані канали комунікації (телефонні дзвінки, електронну пошту, месенджери) та забезпечити централізований, стандартизований облік усіх інцидентів, релевантних для громадського здоров'я та цивільного захисту. Важливою складовою такого реєстру є запровадження

уніфікованих електронних форм повідомлень за аналогією до форм EWRS або Epi-X, із чітко визначеною структурою, переліком обов'язкових полів і вбудованою автоматизованою перевіркою повноти та коректності заповнення.

Ключовим елементом архітектури має стати модуль експертної верифікації, що дозволятиме оперативно оцінювати події відповідно до критеріїв Додатку 2 ММСП, усувати нерелевантні або непідтверджені дані, узгоджувати класифікацію подій та визначати рівень ризику для подальшого реагування. Не менш принциповою є глибока інтеграція цифрового інструменту з інформаційними системами ДСНС, лабораторних мереж, служб екстреної медичної допомоги та медицини катастроф, а також інших суб'єктів забезпечення цивільного захисту. Такий підхід створює єдиний інформаційний простір замість множини ізольованих систем, що не обмінюються даними в режимі реального часу.

Суттєву додану вартість формує модуль автоматизованої аналітики та прогнозування, який має включати алгоритми виявлення аномалій, геопросторовий аналіз, трендові моделі та інструменти ситуаційного моделювання. У поєднанні із системою пріоритезації подій, що класифікує інциденти за рівнем ризику (підходи, які успішно застосовуються в EWRS та CDC), це забезпечує обґрунтоване визначення черговості реагування, концентрацію ресурсів на найбільш критичних загрозах та підвищення ефективності управлінських рішень.

В умовах триваючої війни та постійних загроз для критичної інфраструктури особливого значення набуває створення захищеного інформаційного середовища з режимом роботи 24/7, із резервними каналами зв'язку, механізмами стійкості та належним рівнем кібербезпеки. Важливо, щоб розроблюваний інструмент безпосередньо підтримував діяльність Національного координатора з питань ММСП, зокрема забезпечував можливість автоматизованого формування повідомлень до ВООЗ, ведення ситуаційної обізнаності та документування рішень відповідно до міжнародних вимог.

Окремо слід підкреслити необхідність нормативного закріплення чітких часових регламентів передачі даних, які є усталеною практикою у США та ЄС, але наразі відсутні в українській системі. Визначення граничного часу для первинного повідомлення, верифікації, передачі інформації до центрального рівня та міжнародних структур має стати важливим елементом регуляторної бази, що підвищить прогнозованість, керованість і відповідальність усіх ланок системи реагування. Сукупність цих елементів формує концептуальний каркас, на який може спиратися створення сучасного, інтегрованого та міжнародно сумісного національного цифрового інструменту України.

3.5.4. Перешкоди для інтеграції міжнародних практик у національний контекст.

1. Нормативна неврегульованість цифрової взаємодії.

Немає закріпленого обов'язку використання єдиної системи (на відміну від EWRS/Epi-X).

2. Низький рівень цифрової сумісності між секторами.

Відсутність єдиних стандартів обміну даними.

3. Кіберризики та фізичні загрози в умовах війни.

Потребують резервування каналів зв'язку та дублювання серверної інфраструктури.

4. Кадрові обмеження.

Потрібні спеціалісти з аналітики, IT та кризового менеджменту.

5. Обмежена інтеграція з міжнародними цифровими платформами.

Зокрема, EWRS доступна лише країнам ЄС, TESSy має обмежений формат участі партнерів.

3.5.5. Узагальнення: можливості адаптації та стратегічні напрямки розвитку в Україні.

Порівняльний аналіз демонструє, що міжнародні системи мають низку спільних характеристик, які визначають їх успіх: централізована цифрова

інфраструктура, стандартизація, автоматизована аналітика, кіберзахист, міжсекторальна інтеграція та відповідність вимогам ММСП.

Для України найбільш релевантними напрямами адаптації є:

1. Створення національної цифрової платформи реєстрації та сповіщення за прикладом Epi-X/EWRS.
2. Інтеграція функцій оцінки ризику, орієнтованих на Додаток 2 ММСП (2005).
3. Запровадження нормативних вимог до форм та часових регламентів повідомлень.
4. Впровадження аналітичного модуля, аналогічного можливостям EIOS.
5. Побудова захищеного операційного середовища 24/7 для кризового управління.
6. Структурована міжвідомча взаємодія МОЗ - ДСНС - ЦКПХ-лабораторій - системи охорони здоров'я.
7. Підтримка міжнародної сумісності, необхідної для виконання ММСП (2005) та інтеграції з ЄС.

Таким чином, міжнародний досвід підтверджує: Україна має всі передумови для створення сучасної цифрової системи сповіщення про небезпечні події, яка стане ключовим елементом національної моделі інформаційного менеджменту у сфері громадського здоров'я.

ВИСНОВКИ ДО РОЗДІЛУ 3

Проведений аналіз міжнародних цифрових систем раннього попередження та реагування у сфері громадського здоров'я - EWRS та TESSy Європейського центру профілактики та контролю захворювань, глобальної платформи ВООЗ EIOS та системи Epi-X Центрів з контролю та профілактики захворювань США - дозволив сформувати цілісне уявлення про ключові принципи, архітектуру та

управлінські механізми сучасних систем епідемічного моніторингу та кризової комунікації.

У результаті виконання завдання 3 встановлено такі положення:

1. Міжнародні цифрові системи сповіщення характеризуються високим рівнем централізації, інтегрованістю та уніфікацією інформаційних процесів. Всі системи - EWRS, TESSy, EIOS, Epi-X - функціонують як єдині інформаційні середовища, що забезпечують стандартизований збір, верифікацію, аналіз та поширення даних. Централізованість дозволяє уникати фрагментації потоків інформації та забезпечує оперативність управлінських рішень.

2. Стандартизовані електронні форми повідомлень, єдині комунікаційні протоколи та чіткі процедури інформаційної взаємодії є ключовою умовою ефективності міжнародних систем. Такі інструменти забезпечують сумісність даних між секторами, дозволяють здійснювати автоматизовану обробку інформації, підвищують точність оцінки ризиків і мінімізують можливість помилок та затримок в передачі інформації.

3. Значну роль відіграють механізми експертної верифікації та автоматизованої аналітики. EWRS та Epi-X використовують обов'язкову експертну перевірку повідомлень, тоді як EIOS впроваджує алгоритми машинного навчання для аналізу великих масивів даних з відкритих джерел. Наявність таких інструментів забезпечує оперативне виявлення подій, що можуть становити загрозу громадському здоров'ю на міжнародному рівні.

4. Міжвідомча та міжсекторальна інтеграція є наскрізним принципом функціонування всіх розглянутих систем. Вони об'єднують дані від центрів контролю та профілактики хвороб, лабораторних мереж, органів цивільного захисту, екстреної медичної допомоги та інших секторів. Це забезпечує комплексну ситуаційну обізнаність і є критичним фактором успішного реагування.

5. Системи EWRS та Epi-X демонструють високий рівень кіберстійкості та захищеності інформації.

Функціонування цих платформ здійснюється в безпечних цифрових середовищах із багаторівневими механізмами контролю доступу, що є особливо важливим для України в умовах війни та постійних кіберзагроз.

6. Визначено системні перешкоди для впровадження міжнародних підходів в Україні.
Серед них - відсутність нормативно визначеного єдиного цифрового інструменту, фрагментованість інформаційних потоків, недостатня цифрова сумісність між відомствами, обмеженість ресурсів та кіберризики воєнного часу.

Таким чином, аналіз міжнародних підходів дозволив визначити низку архітектурних, технологічних та управлінських рішень, які можуть слугувати основою для розроблення національного цифрового інструменту реагування на надзвичайні ситуації у сфері громадського здоров’я. Отримані результати формують концептуальну базу для наступного розділу, присвяченого моделюванню та обґрунтуванню такої системи в умовах України.

РОЗДІЛ 4
ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ СТВОРЕННЯ НАЦІОНАЛЬНОЇ ЦИФРОВОЇ СИСТЕМИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ У СФЕРІ ГРОМАДСЬКОГО ЗДОРОВ'Я

4.1. Аналіз прогалин існуючої моделі інформаційного забезпечення в Україні

Ефективне реагування на надзвичайні ситуації у сфері громадського здоров'я базується на своєчасному отриманні, верифікації, аналітичній обробці та передачі інформації між суб'єктами єдиної державної системи цивільного захисту. Водночас, результати проведеного аналізу нормативно-правових документів, організаційної структури функціональних підсистем Міністерства охорони здоров'я та практики застосування чинних процедур свідчать про наявність низки системних обмежень і прогалин, які перешкоджають формуванню ефективного, інтегрованого та технологічно адаптованого інформаційного середовища. Чинна модель інформаційного забезпечення є фрагментованою, недостатньо стандартизованою та не забезпечує необхідного рівня оперативності прийняття управлінських рішень, що особливо критично в умовах воєнного стану, високої інтенсивності надзвичайних подій та зростання кількості хімічних, біологічних і техногенних загроз.

Однією з ключових проблем - це відсутність нормативно визначеного єдиного цифрового інструменту реєстрації та оповіщення про небезпечні події у сфері громадського здоров'я. Наявні законодавчі акти регламентують загальні вимоги щодо інформування, проте не містять положень щодо застосування конкретної цифрової платформи, обов'язкової для всіх суб'єктів реагування. На практиці це призводить до використання різнорідних каналів комунікації - електронної пошти, телефонного зв'язку, відомчих систем, паперових форм та неформальних інструментів, що суттєво ускладнює стандартизацію процедур,

збільшує ймовірність втрати інформації та створює ризики затримок у ланцюгу повідомлень.

Важливою проблемою є відсутність узгодженості та стандартизації інформаційних потоків між установами охорони здоров'я, службами екстреної медичної допомоги та медицини катастроф, центрами контролю та профілактики хвороб, Центром громадського здоров'я МОЗ України, ДСНС та іншими суб'єктами цивільного захисту. Кожна з установ використовує різні інформаційні ресурси, програмне забезпечення та підходи до фіксації даних. Відсутність інтегрованої цифрової інфраструктури унеможливлює автоматизований обмін інформацією, перешкоджає формуванню узгодженого інформаційного простору та негативно впливає на якість ситуаційної обізнаності на національному рівні.

Нормативно-правова база не забезпечує належного рівня стандартизації інформаційних повідомлень. Хоча, чинне законодавство визначає обов'язок інформувати про події, що становлять загрозу здоров'ю населення, воно не регламентує уніфікованих електронних форм повідомлень, обов'язкових полів, структур даних та вимог до їх м та вимог до того, щоб ці дані могли автоматично зчитуватися й оброблятися комп'ютерними системами. Унаслідок цього повідомлення подаються в різних форматах, що ускладнює їх інтеграцію та аналітичну обробку, а також унеможливлює автоматизацію процесів оцінювання ризиків.

Важливим обмеженням є відсутність чітко встановлених нормативних строків передачі інформації у кризових умовах. Використання у законодавстві оціночних формулювань («негайно», «у найкоротші строки», «у встановленому порядку») призводить до різного тлумачення термінів і різнорівневої практики в регіонах. Нерівномірність оперативності передачі даних створює ризики некоректного визначення рівня надзвичайної ситуації, затримує мобілізацію ресурсів та обмежує спроможність центральних органів влади забезпечувати координацію заходів реагування.

Виявлено також відсутність нормативної регламентації алгоритмів та цифрових інструментів оцінки ризику відповідно до вимог ММСП. Національні процедури покладаються переважно на експертне судження фахівців, що ускладнює стандартизацію підходів у різних регіонах, знижує швидкість ухвалення рішень та підвищує ризик несвоєчасного повідомлення ВООЗ про події, що можуть становити загрозу транскордонного значення.

Існуюча модель також характеризується обмеженим рівнем міжсекторальної інтеграції. Дані про постраждалих, результати лабораторних досліджень, показники хімічного, біологічного та радіаційного моніторингу, інформація про навантаження на систему екстреної медичної допомоги та стан інфраструктури системи охорони здоров'я передаються різними шляхами без можливості їх автоматичного об'єднання в єдине інформаційне поле. В умовах воєнних загроз така фрагментація істотно впливає на точність прогнозування сценаріїв розвитку подій та ефективність управління ресурсами.

Додатковим системним обмеженням є відсутність регламентованих вимог щодо резервування каналів зв'язку, кіберстійкості та захищеності інформаційних систем суб'єктів реагування. За умов високої інтенсивності кібератак та пошкоджень телекомунікаційної інфраструктури це створює загрозу порушення безперервності інформаційного обміну.

Нерівномірність цифрової готовності суб'єктів реагування, включаючи різний рівень технічного оснащення, різноманіття програмних рішень і обмежені цифрові компетентності персоналу, додатково ускладнюють впровадження стандартизованих процедур і цифрових інструментів у масштабах держави.

Узагальнюючи, існуюча модель інформаційного забезпечення реагування на надзвичайні ситуації в Україні характеризується відсутністю єдиної цифрової інфраструктури, нестачею інтегрованості між секторами, неоднорідністю інформаційних потоків та недостатньою відповідністю вимогам Міжнародних медико-санітарних правил. Сукупність цих факторів створює суттєві управлінські, організаційні та технічні обмеження, які знижують ефективність

реагування. Виявлені прогалини визначають об’єктивну необхідність створення національної цифрової системи інформаційного забезпечення, здатної забезпечити стандартизований, оперативний та захищений обмін даними між усіма суб’єктами реагування.

4.2. Обґрунтування потреби у створенні інтегрованої національної цифрової системи інформаційного забезпечення реагування на надзвичайні події у сфері громадського здоров’я

Аналіз нормативно-правових засад реагування на надзвичайні ситуації та оцінка реального функціонування інформаційних процесів у системі громадського здоров’я України засвідчили, що чинна модель інформаційного забезпечення не відповідає сучасним вимогам оперативності, достовірності та міжвідомчої інтеграції. Виявлені прогалини та обмеження, зокрема фрагментація каналів комунікації, різнорідність форматів повідомлень, відсутність єдиних стандартів електронних процедур і недостатня інтеграція між суб’єктами реагування, створюють системні ризики для ефективного управління подіями, що становлять загрозу громадському здоров’ю.

Потреба у створенні національної інтегрованої цифрової системи формується насамперед у зв’язку з тим, що наявні інформаційні механізми цивільного захисту та охорони здоров’я базуються на різнорідних технологічних рішеннях і не забезпечують повноцінної синхронізації між функціональними підсистемами Міністерства охорони здоров’я, службами екстреної медичної допомоги та медицини катастроф, ЦГЗ, ЦКПХ та ДСНС. Значна частина обміну інформацією досі залежить від ручних процедур, включно з телефонним оповіщенням, електронною поштою або неформальними цифровими каналами. Це об’єктивно обмежує швидкість та точність передавання даних, ускладнює верифікацію інформації та створює можливість її дублювання або втрати. У надзвичайних ситуаціях навіть незначні затримки можуть впливати на своєчасність реагування та координації між установами.

Узагальнений аналіз функціонування інформаційних процесів також свідчить, що відсутність єдиного цифрового середовища унеможливлює формування безперервної ситуаційної обізнаності, яка є необхідною умовою оцінювання ризиків та прийняття управлінських рішень. Наразі кожен суб'єкт реагування оперує власними джерелами інформації, що ускладнює створення загальної картини події та потребує додаткових етапів узгодження і підтвердження даних. Це не лише збільшує часові витрати, але й підвищує ймовірність помилок, що є неприйнятним в умовах швидкоплинних кризових подій.

Потреба у створенні інтегрованої цифрової системи обумовлюється також вимогами Міжнародних медико-санітарних правил (2005), які передбачають наявність у країни механізмів оперативного виявлення, оцінювання та повідомлення про події, що можуть становити міжнародну загрозу. Відсутність автоматизованих механізмів оцінювання ризику, сумісних із Додатком 2 до ММСП, а також відсутність електронного маршруту передачі інформації до Національного координатора з питань ММСП ускладнюють виконання цих міжнародних зобов'язань. З огляду на зростання кількості транскордонних загроз (інфекційних, хімічних, радіаційних, екологічних), створення уніфікованого цифрового середовища стає необхідною умовою відповідності міжнародним стандартам.

Важливою передумовою для створення національної цифрової системи є також те, що чинна модель інформаційного забезпечення характеризується нерівномірністю технічної готовності суб'єктів реагування. Заклади охорони здоров'я, центри екстреної медичної допомоги, територіальні підрозділи ЦКПХ та служби ДСНС використовують різні програмні продукти, які не мають сумісності між собою. Це унеможливлює автоматизований обмін даними та ускладнює інтеграцію інформаційних потоків. Впровадження національної цифрової системи дозволить уніфікувати технічні вимоги, забезпечивши єдиний

стандарт функціонування інформаційної інфраструктури в секторі громадського здоров’я.

Додатковим чинником, що обґрунтовує необхідність створення такої системи, є потреба у підвищенні кіберстійкості та резервування інформаційних процесів в умовах воєнного стану. Постійні кібератаки, пошкодження інфраструктури та загальна висока турбулентність операційного середовища потребують наявності стійкої, захищеної та резервованої цифрової платформи, яка забезпечуватиме безперервність управлінських процесів та стабільну роботу каналів комунікації навіть за умов часткової втрати інфраструктури.

З огляду на зазначені фактори, створення інтегрованої національної цифрової системи інформаційного забезпечення реагування на надзвичайні події у сфері громадського здоров’я є об’єктивною та науково обґрунтованою потребою. Така система не лише усуне фрагментацію інформаційних потоків та забезпечить уніфікацію управлінських процедур, але й створить умови для формування єдиного інформаційного простору, підвищення оперативності та точності оповіщення, забезпечення ситуаційної обізнаності на всіх рівнях управління та відповідності України міжнародним нормам у сфері охорони здоров’я та цивільного захисту. У довгостроковій перспективі її впровадження стане ключовим елементом зміцнення національної системи громадського здоров’я, підвищення стійкості держави до надзвичайних подій та розбудови ефективної інфраструктури системи реагування у сфері охорони здоров’я.

4.3. Формування цілей і принципів створення національного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров’я

Побудова сучасної моделі управління надзвичайними ситуаціями у сфері громадського здоров’я є неможливою без запровадження інтегрованого цифрового інструменту, який забезпечував би уніфіковані механізми збору, обробки, передачі та аналізу інформації між усіма суб’єктами реагування.

Проведений аналіз вітчизняної нормативно-правової бази, міжнародних практик і виявлених структурних прогалин свідчить про нагальну потребу у створенні єдиного цифрового середовища, що здатний об’єднати функціональні підсистеми цивільного захисту Міністерства охорони здоров’я, забезпечити синхронізацію процесів та підвищити ефективність управлінських рішень.

Стратегічною метою формування національного цифрового інструменту є створення єдиного національного інформаційного простору для фіксації, передачі, аналізу та прогнозування подій, що становлять загрозу громадському здоров’ю. Такий простір має забезпечувати оперативність і повноту інформації про небезпечні події, інтегрувати діяльність функціональних підсистем медичного захисту населення та забезпечення санітарно-епідеміологічного благополуччя населення, сприяти виконанню міжнародних зобов’язань України відповідно до Міжнародних медико-санітарних правил (2005) та формувати високий рівень стійкості системи охорони здоров’я в умовах воєнних викликів і зростаючої кількості техногенних і біологічних інцидентів.

Ця мета узгоджується із сучасною концепцією менеджменту охорони здоров’я, відповідно до якої інформація є ключовим стратегічним ресурсом, а цифрові інструменти - основним засобом підвищення швидкості, точності та доказовості управлінських рішень.

У межах стратегічної мети визначено низку взаємопов’язаних операційних цілей, спрямованих на усунення системних прогалин та забезпечення повноцінного функціонування інформаційного простору реагування.

Першою ціллю є забезпечення своєчасного виявлення небезпечних подій і їх стандартизованої реєстрації. Система має надавати можливість швидкого внесення первинної інформації з урахуванням логічних перевірок, уніфікованих полів та процедур, що мінімізує ризики помилок та неповноти даних.

Другою ціллю є забезпечення уніфікованого обміну інформацією між усіма суб’єктами реагування. Цифровий інструмент має інтегрувати центри контролю та профілактики хвороб, служби екстреної медичної допомоги та

медицини катастроф, ЦГЗ, структурні підрозділи охорони здоров'я обласних військових адміністрацій, ДСНС та інші установи, забезпечуючи їм роботу в єдиній інформаційній мережі.

Третьою ціллю є автоматизована оцінка ризику. Система повинна підтримувати алгоритми попереднього автоматичного визначення рівня небезпеки, пріоритетності подій та необхідності проведення подальшої верифікації, що відповідає вимогам Додатку 2 до ММСП.

Четвертою ціллю є формування єдиної оперативної ситуаційної картини надзвичайної ситуації. Інструмент повинен забезпечувати можливість інтегрованого відображення географії подій, типів загроз, динаміки їх розвитку, доступних ресурсів реагування та потенційних факторів ризику. Наявність інтерактивного ситуаційного поля створює передумови для підвищення ситуаційної обізнаності керівних органів та підрозділів, що залучені до ліквідації наслідків надзвичайних ситуацій.

П'ятою ціллю є забезпечення аналітичної підтримки управлінських рішень. Система повинна автоматично генерувати статистичні звіти, візуалізовані дашборди та прогностичні моделі, необхідні для оцінки епідемічної та техногенної ситуації, а також для аналізу ефективності вже здійснених заходів реагування.

Шостою ціллю є інтеграція з лабораторними, клінічними та епідеміологічними інформаційними системами, що дозволить забезпечити оперативне підтвердження діагнозів, динамічне оновлення статусу подій та раннє виявлення інфекційних загроз.

Сьомою ціллю є забезпечення двосторонньої комунікації між функціональними підсистемами медичного захисту населення та забезпечення санітарно-епідеміологічного благополуччя населення, що є важливою умовою для повноцінного та узгодженого реагування на інциденти з багатофакторними загрозами.

Восьмою ціллю є те, що цифровий інструмент має забезпечувати автоматизоване оповіщення відповідальних суб'єктів, фіксацію часу передачі інформації та підтвердження доставки, а також створення національного довгострокового реєстру небезпечних подій, який забезпечуватиме накопичення, аналіз і використання даних для стратегічного планування.

Ключові принципи створення цифрової системи

Розроблення національного цифрового інструменту повинно ґрунтуватися на низці фундаментальних принципів, які визначають його архітектуру, функціональну логіку та механізми міжвідомчої взаємодії.

Першим з них є принцип єдиного інформаційного простору, що передбачає роботу всіх суб'єктів реагування в інтегрованій системі з узгодженими правилами та механізмами збору і передачі даних. Важливим є принцип стандартизації, відповідно до якого вся інформація подається уніфікованими електронними формами, що забезпечує сумісність і коректність обміну.

Принцип оперативності вимагає забезпечення передачі інформації в режимі, максимально наближеному до реального часу, що є необхідним для ухвалення рішень у критичних ситуаціях. Принцип інтероперабельності передбачає можливість інтеграції системи з іншими цифровими платформами охорони здоров'я, лабораторними інформаційними системами, картографічними сервісами та інструментами цивільного захисту.

Система повинна відповідати принципу кіберстійкості та надійності, що передбачає захист даних, резервування каналів зв'язку та забезпечення безперервності функціонування навіть в умовах пошкодження інфраструктури. Високий рівень автоматизації процесів, включно з оцінкою ризику, формуванням аналітичних звітів та маршрутизацією інформаційних потоків, відповідає принципу автоматизації.

Принцип прозорості та відстежуваності передбачає фіксацію всіх дій користувачів, що підвищує підзвітність і довіру до системи. Не менш важливими є принципи доступності, адаптивності та безперервного вдосконалення, які

забезпечують сталість функціонування інструменту, можливість його модернізації та масштабування відповідно до появи нових загроз чи зміни законодавств

4.4. Пропозиції до архітектури національної цифрової системи інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я

Аналіз нормативно-правових засад, існуючих інформаційних процесів та міжнародних практик свідчить, що ефективна цифрова система інформаційного забезпечення реагування має ґрунтуватися на багаторівневій архітектурі, яка поєднує функціональні можливості збору, обробки, аналізу, обміну та довготривалого зберігання даних. Запропонована архітектурна модель покликана забезпечити усунення ідентифікованих прогалин, підвищити якість міжвідомчої взаємодії, забезпечити відповідність вимогам ММСП та створити єдиний інформаційний простір для всіх суб'єктів реагування.

У запропонованій архітектурі система складається з декількох взаємопов'язаних рівнів, які забезпечують повний цикл управління подіями: від моменту їхнього виявлення до підготовки управлінських рішень.

Перший рівень - рівень збору даних - охоплює заклади охорони здоров'я, центри контролю та профілактики хвороб, центри екстреної медичної допомоги та медицини катастроф, лабораторні мережі, органи влади та оперативні служби. На цьому етапі забезпечується швидке внесення інформації за уніфікованими формами, прикріплення матеріалів, автоматична прив'язка до місцевості та первинне структурування даних. Такий підхід унеможливлює фрагментованість повідомлень і забезпечує єдині стандарти фіксації подій по всій країні.

Другий рівень - рівень верифікації та первинної обробки - передбачає автоматичні логічні перевірки, підтвердження інформації відповідальними особами, стандартизовану класифікацію подій і видалення дубльованих записів. Це дозволяє підвищити точність і достовірність інформації, мінімізувати

помилки та усунути проблему надлишкового навантаження на аналітичні підрозділи.

Третій рівень формують аналітичні модулі, які забезпечують автоматизовану оцінку ризиків, прогнозування розвитку подій, визначення рівнів пріоритетності та формування рекомендацій для управлінців. Алгоритми оцінки ризику повинні бути адаптовані до підходів WHO та ECDC (Rapid Risk Assessment), включати аналіз джерела загрози, масштабів події, можливих наслідків та рівня невизначеності. Завдяки цьому система забезпечуватиме оперативну та науково обґрунтовану підтримку прийняття управлінських рішень.

Четвертий рівень - рівень ситуаційної обізнаності - відповідає за створення інтегрованої динамічної картини подій. Про це свідчить міжнародний досвід роботи EWRS, Epi-X та CNPHI: візуалізація даних у реальному часі є ключовим інструментом для міжвідомчої координації. Національна система має забезпечувати інтерактивні карти, аналітичні панелі, графіки, «heat maps», часові ряди та інші інструменти ситуаційного моніторингу.

На п’ятому рівні відбувається управлінська координація та ухвалення рішень. Цей рівень забезпечує роботу Міністерства охорони здоров’я України, Центру громадського здоров’я, регіональних ЦКПХ, центрів екстреної медичної допомоги та медицини катастроф та ДСНС у частині спільних ризиків. Модель передбачає доступ до узагальнених даних, спільне формування рішень, автоматизований обмін повідомленнями, а також можливість виконання міжнародних обов’язків щодо інформування ВООЗ у режимі, наближеному до реального часу.

Важливим елементом архітектури є впровадження функціональних модулів, які забезпечують гнучкість і масштабованість системи. До таких модулів належать: модуль реєстрації небезпечних подій, модуль оцінки ризику, модуль аналітики та візуалізації, модуль оперативного оповіщення, модуль міжвідомчої взаємодії та модуль звітності й архівування. Їх інтеграція забезпечує

прозорість, оперативність та повноту інформаційного обміну між усіма суб'єктами реагування.

Одним з ключових принципів побудови архітектури є забезпечення інтероперабельності. Система має бути сумісною з Електронною системою охорони здоров'я України, лабораторними інформаційними системами, GIS-платформами, інформаційними ресурсами цивільного захисту та іншими державними цифровими інструментами. Це дасть змогу створити єдине інформаційне середовище та усунути фрагментованість даних, що є одним із ключових викликів поточної моделі.

Не менш важливим є принцип безпеки та стійкості: система повинна мати механізми резервування, захисту від кібератак, аудиту доступу та безперервності роботи у кризових умовах, включно з воєнними ризиками. Враховуючи сучасний контекст, саме інформаційна стійкість стає критичним фактором для забезпечення функціонування системи охорони здоров'я під час надзвичайних ситуацій.

Запропонована архітектура дозволяє створити цілісну, стійку та стандартизовану систему інформаційного забезпечення реагування на небезпечні події. Вона узгоджується з найкращими міжнародними практиками, враховує специфіку українського контексту та відповідає стратегічним цілям реформування системи громадського здоров'я. Реалізація такої архітектури стане ключовим елементом модернізації національної системи охорони здоров'я, забезпечивши підвищення оперативності реагування, покращення міжвідомчої координації та зміцнення національної готовності до сучасних і майбутніх загроз.

ВИСНОВКИ ДО РОЗДІЛУ 4

Аналіз чинної моделі інформаційного забезпечення засвідчив її фрагментованість, відсутність уніфікованих цифрових інструментів та недостатню інтеграцію між суб'єктами реагування, що створює затримки в обміні даними та знижує оперативність реагування.

Нормативна база визначає загальні принципи інформування, але не містить вимог до стандартизованих електронних форм, автоматизованої оцінки ризику, цифрової інтеграції підсистем та міжвідомчих каналів обміну, що обмежує можливості формування єдиного інформаційного простору.

Виявлені прогалини у процесах обміну інформацією, зокрема різнорідність каналів комунікації, дублювання повідомлень та відсутність підтверджуваних цифрових маршрутів, унеможливлюють ефективну координацію в умовах збільшення кількості загроз та викликів воєнного часу.

Обґрунтовано необхідність створення національної цифрової системи, яка забезпечить швидке виявлення подій, автоматизовану оцінку ризику, аналітичну підтримку прийняття рішень та відповідність вимогам Міжнародних медико-санітарних правил (2005).

Сформульовано цілі та принципи майбутнього цифрового інструменту, орієнтовані на створення єдиного інформаційного простору, стандартизацію даних, інтероперабельність, безпеку, автоматизацію та оперативність.

Запропоновані концептуальні підходи до архітектури системи доводять її потенціал для об’єднання всіх суб’єктів реагування та підвищення ефективності інформаційного менеджменту у сфері громадського здоров’я.

РОЗДІЛ 5
ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ НАЦІОНАЛЬНОГО ЦИФРОВОГО ІНСТРУМЕНТУ, З УРАХУВАННЯМ УПРАВЛІНСЬКИХ, НОРМАТИВНИХ, ОРГАНІЗАЦІЙНИХ І ТЕХНІЧНИХ АСПЕКТІВ, А ТАКОЖ СПЕЦИФІКИ ВОЄННОГО ЧАСУ Й ВИМОГ МІЖНАРОДНИХ МЕДИКО-САНІТАРНИХ ПРАВИЛ

5.1. Управлінські рекомендації щодо організації впровадження національного цифрового інструменту

Ефективне впровадження національного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров’я потребує формування цілісної системи управління, здатної забезпечити узгодженість дій усіх суб’єктів реагування, раціональне планування, контроль виконання та адаптацію процесів до умов воєнного часу. Успішність проєкту значною мірою залежить від того, наскільки чітко вибудувана управлінська модель, що поєднує стратегічні, тактичні та операційні рівні взаємодії.

На першому етапі Міністерству охорони здоров’я України доцільно створити спеціалізований координаційний орган - проектний офіс, який виконуватиме функції центрального управлінського ядра. Такий орган має включати представників Міністерства охорони здоров’я, Центру громадського здоров’я, центрів контролю та профілактики хвороб, центрів екстреної медичної допомоги та медицини катастроф, фахівців Державної служби України з надзвичайних ситуацій (у частині міжвідомчих ризиків), а також експертів з інформаційних технологій і кібербезпеки. Проектний офіс відповідатиме за формування технічних вимог, методологічний супровід розробки, проведення тестування, координацію міжвідомчої взаємодії та забезпечення оперативного вирішення управлінських питань.

Наступним важливим управлінським кроком є розроблення узгодженої дорожньої карти впровадження цифрового інструменту. Вона повинна містити чітко визначені етапи реалізації: формування функціональних вимог, створення архітектури та модулів системи, проведення пілотування в окремих областях, масштабування, введення в промислову експлуатацію та подальший супровід. Для кожного етапу необхідно встановити відповідальних виконавців, конкретні строки, необхідні ресурси й критерії оцінки ефективності. Дорожня карта створює підґрунтя для прозорості, прогнозованості та відповідальності під час реалізації проєкту, а також мінімізує ризики затримок та управлінської неузгодженості.

Ключовою передумовою успішного впровадження цифрового інструменту є налагоджена міжвідомча координація між системою громадського здоров'я та системою цивільного захисту. Сучасні надзвичайні ситуації, особливо в умовах воєнного часу, характеризуються багатофакторністю ризиків і потребують оперативного обміну даними між МОЗ, ДСНС, обласними військовими адміністраціями, комісіями з питань техногенно-екологічної безпеки та надзвичайних ситуацій, закладами охорони здоров'я та лабораторними мережами. Для цього необхідно створити сталу систему міжвідомчих робочих груп, розробити регламенти інформаційної взаємодії та визначити відповідальних осіб у кожній установі. Такий підхід забезпечить синхронність управлінських дій, уніфікованість процедур та швидкість прийняття рішень.

Важливим управлінським завданням є запровадження системи управління змінами, оскільки цифровий інструмент передбачає трансформацію традиційних підходів до збору та передачі інформації. В рамках управління змінами необхідно проводити роз'яснювальну роботу серед персоналу, розробляти методичні матеріали та алгоритми роботи, запроваджувати заходи щодо підвищення залученості та відповідальності користувачів. Особливу увагу слід приділити формуванню позитивної мотивації персоналу до використання

цифрової платформи та подоланню бар'єрів, пов'язаних із впровадженням нових інструментів у стресових та ресурсно обмежених умовах воєнного часу.

Успішне функціонування цифрового інструменту залежить також від рівня підготовки користувачів. Тому управлінські рекомендації повинні включати створення системи навчання, що охоплює онлайн-курси для базових користувачів, спеціальні тренінги для фахівців, відповідальних за оцінку ризику та аналітику, навчальні програми для керівників закладів охорони здоров'я та ситуаційні симуляційні тренування, які дозволяють інтегрувати нову систему у практику реагування. Навчання персоналу гарантує належну якість ведення даних, своєчасність повідомлень та правильність використання функціональних модулів системи.

Окрім цього, необхідно забезпечити систематичний управлінський контроль та моніторинг функціонування цифрового інструменту. Доцільним є впровадження механізмів оцінки якості даних, періодичних аудитів інформаційних потоків, аналізу показників швидкості реагування, точності переданих даних та відповідності процесів вимогам Міжнародних медико-санітарних правил (2005). Регулярні звіти проєктного офісу забезпечать прозорість упровадження системи та дозволять своєчасно виявляти та усувати проблеми.

Окремої уваги потребує питання ресурсного забезпечення. Управлінські рішення повинні містити довгострокове планування фінансових, кадрових і технічних ресурсів, необхідних для створення, підтримки та модернізації цифрового інструменту. Важливо передбачити фінансування заходів кіберзахисту, резервування каналів зв'язку, технічну підтримку користувачів, а також можливість масштабування системи на нові типи загроз. Такий підхід гарантує стійкість функціонування платформи та її адаптацію до змін у законодавстві, технологічних вимогах та міжнародних стандартах.

Отже, управлінські рекомендації формують основу для системного, контрольованого та ефективного впровадження цифрового інструменту,

забезпечуючи узгодженість дій між усіма суб'єктами реагування, підвищення якості інформаційних процесів, стійкість системи охорони здоров'я та відповідність міжнародним вимогам у сфері епідемічної безпеки.

5.2. Нормативно-правові рекомендації щодо впровадження національного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я

Ефективне впровадження національного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації в Україні потребує належного нормативного супроводу, який забезпечує узгодженість функціональних процедур, юридичну визначеність відповідальності суб'єктів, стандартизацію інформаційних потоків та відповідність міжнародним зобов'язанням України. При цьому чинна нормативно-правова база дає можливість упроваджувати зазначений цифровий інструмент без необхідності зміни законів України**,** оскільки повноваження для організації інформаційної взаємодії, затвердження форм повідомлень, визначення порядку реагування та ведення державних інформаційних систем уже закріплені в чинних актах МОЗ, Кабінету Міністрів України та міжнародних нормативних документах, ратифікованих Україною.

Нормативно-правові рекомендації зосереджені на деталізації існуючих процедур, стандартизації цифрових процесів та узгодженні міжвідомчої взаємодії в межах ЄДСЦЗ, що дозволяє забезпечити практичну реалізацію цифрової трансформації системи реагування без зміни базових положень законодавства.

1. Актуалізація та деталізація підзаконних актів МОЗ України.

Відповідно до Кодексу цивільного захисту України, Закону України «Про захист населення від інфекційних хвороб» [20]. та Закону України «Основи законодавства України про охорону здоров'я» Міністерство охорони здоров'я наділене повноваженнями з організації інформаційного забезпечення

реагування, затвердження форм повідомлень, визначення порядку дій суб'єктів охорони здоров'я та встановлення вимог до повідомлення про події, що становлять загрозу громадському здоров'ю.

На основі цих повноважень доцільним є ухвалення наказу МОЗ України "Про організацію інформаційної взаємодії у сфері громадського здоров'я за допомогою національного цифрового інструменту реагування на надзвичайні ситуації", який має:

– порядок використання цифрового інструменту суб'єктами підсистем медичного захисту населення та забезпечення санітарного та епідеміологічного благополуччя населення;

– затвердити уніфіковані електронні форми повідомлень про небезпечні події;

– процедури первинної та повторної верифікації;

– часові регламенти передачі даних (в рамках повноважень МОЗ);

– порядок внесення, уточнення та закриття подій;

– унормувати статус цифрового запису як офіційного повідомлення відповідно до Закону України «Про електронні документи та електронний документообіг».

Таке розширення нормативної деталізації не суперечить діючим актам і забезпечує юридичні підстави для повноцінного впровадження цифрової системи.

2. Узгодження цифрової системи з положеннями Постанови про ЄДСЦЗ.

Постанова Кабінету Міністрів України від 09.01.2014 № 11 визначає загальні обов'язки суб'єктів ЄДСЦЗ щодо:

– своєчасного надання інформації,

– використання затверджених форм,

– забезпечення безперервності інформування,

– взаємодії між суб’єктами цивільного захисту.

Це створює нормативне підґрунтя для впровадження цифрової системи, оскільки цифровий інструмент є не альтернативою, а формою реалізації вимог Постанови Кабінету Міністрів України від 09.01.2014 № 11.

Доцільно врегулювати взаємодію у спосіб:

– закріпити в наказі МОЗ, що робота в цифровій системі вважається виконанням вимог Постанови Кабінету Міністрів України від 09.01.2014 № 11 щодо надання інформації про події;

– визначити цифрові форми повідомлень як еквівалент паперовим та/або традиційним формам;

– забезпечити можливість спільного використання цифрової функціональними підсистемами МОЗ.

Таким чином, цифровий інструмент набуває статусу офіційного каналу комунікації, узгодженого з чинним адміністративним порядком реагування.

3. Відповідність міжнародним зобов’язанням України за ММСП.

Міжнародні медико-санітарні правила (2005), ратифіковані Україною, визначають вимоги до:

– оперативної оцінки подій відповідно до Додатку 2,

– інформування Національного координатора з питань ММСП,

– забезпечення надання інформації про оперативну ситуацію на місці події,

– формування звітності.

Цифровий інструмент дозволить виконувати ці вимоги автоматизовано.

Для цього необхідно нормативно встановити:

– використання автоматизованого алгоритму оцінки подій відповідно до Додатку 2;

– обов’язкове включення системи до процесу оповіщення Національного координатора ММСП;

– уніфіковану форму електронних повідомлень, сумісну з формою WHO Event Information Site (EIS).

Такий підхід посилює відповідність України міжнародним стандартам.

4. Вимоги кібербезпеки та захисту державних інформаційних ресурсів.

Цифровий інструмент повинен відповідати існуючим нормам, зокрема:

– Постанова КМУ від 18 червня 2025 р. № 712 щодо захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем [22];

– вимоги Держспецзв'язку;

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [23];

– Закон України «Про електронну ідентифікацію та електронні довірчі послуги» [24].

З огляду на це необхідно забезпечити:

– багаторівневу автентифікацію користувачів;

– шифрування переданих і збережених даних;

– журнали аудиту та фіксації операцій;

– резервні центри обробки даних;

– безперервність роботи в умовах воєнних загроз.

Ці вимоги є критичними, оскільки система міститиме дані оперативного реагування.

5. Інтероперабельність із державними інформаційними системами у сфері охорони здоров'я.

Законодавство України, зокрема Закон України «Про державні фінансові гарантії медичного обслуговування населення», створює правові підстави для інтеграції галузевих цифрових рішень з Електронною системою охорони здоров'я (ЕСОЗ), лабораторними інформаційними системами та іншими суміжними сервісами. У межах розбудови національного цифрового інструменту реагування на небезпечні події необхідно нормативно закріпити використання

стандартизованих протоколів обміну даними, визначити порядок автоматичного імпорту лабораторних результатів у відповідний цифровий модуль, встановити механізми передачі інформації між системою реагування та ЕСОЗ через API, а також забезпечити узгодженість довідників і класифікаторів — включно з МКХ, класифікатором подій та геоданними. Такий підхід повністю відповідає чинним наказам МОЗ і відображає принципи інтероперабельності, що лежать в основі стратегії цифрової трансформації у сфері охорони здоров'я, гарантує сумісність інформаційних систем та підвищує ефективність міжвідомчого обміну даними.

6. Міжвідомча інтеграція у межах чинного законодавства.

Постанова КМУ від 09.01.2014 № 11 передбачає міжвідомчу взаємодію суб'єктів цивільного захисту, що дає змогу використати цифровий інструмент як спільну платформу для:

- МОЗ України;
- Центру громадського здоров'я;
- центрів контролю та профілактики хвороб;
- центрів екстреної медичної допомоги та медицини катастроф;
- ДСНС України.

Для цього необхідно:

- розробити спільний наказ МОЗ і ДСНС щодо інформаційної взаємодії через цифрову систему;
- закріпити порядок міжвідомчого доступу та розмежування ролей;
- визначити, що дані цифрової системи є офіційною основою для рішень комісій ТЕБ і НС.

Це підвищує узгодженість дій і зменшує дублювання інформації.

5.3. Організаційні рекомендації щодо впровадження національного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я

Організаційне забезпечення впровадження національного цифрового інструменту реагування на надзвичайні ситуації у сфері громадського здоров'я передбачає формування узгодженої системи дій між органами державної влади, установами охорони здоров'я та службами цивільного захисту. Враховуючи нормативні вимоги Кодексу цивільного захисту України та положення, що регламентують діяльність функціональних підсистем Міністерства охорони здоров'я України, впровадження цифрового інструменту має спиратися на чіткі організаційні механізми, які забезпечують його ефективну інтеграцію в існуючі процеси.

Передусім необхідно визначити уповноважені структури та посадових осіб, відповідальних за координацію впровадження. Національний рівень має забезпечити загальне управління процесом, методичний супровід та контроль виконання, тоді як регіональні центри контролю та профілактики хвороб і центри екстреної медичної допомоги повинні відповідати за організацію роботи на місцях, у тому числі за навчання персоналу, взаємодію із закладами охорони здоров'я та забезпечення своєчасного внесення інформації. Такий підхід відповідає структурі повноважень функціональних підсистем, визначених наказами МОЗ України.

Для кожної установи, яка бере участь у реагуванні на небезпечні події, рекомендовано затвердити внутрішні регламенти роботи з цифровим інструментом. Такі документи мають визначати порядок введення та верифікації даних, відповідальність за своєчасність і повноту внесеної інформації, алгоритми взаємодії між структурними підрозділами та порядок дій у разі технічних чи організаційних збоїв. Наявність уніфікованих регламентів сприятиме зменшенню помилок, усуненню дублювання та забезпечить сталість інформаційних процесів навіть в умовах підвищених операційних навантажень.

Важливим організаційним аспектом є підготовка та підвищення компетентностей персоналу. З огляду на те, що цифровий інструмент охоплює широкий спектр суб'єктів - від закладів охорони здоров'я до регіональних

центрів та центрального рівня, - навчання має бути системним, поетапним і спрямованим на зміцнення навичок роботи з даними, розуміння алгоритмів реагування та вимог Міжнародних медико-санітарних правил (IHR 2005). Доцільним є впровадження регулярних тренінгів і симуляційних вправ, що допоможуть відпрацювати дії персоналу в умовах стресу та обмеженого часу.

У межах організаційного впровадження необхідно забезпечити сталі механізми взаємодії між суб'єктами єдиної державної системи цивільного захисту. Рекомендовано закріпити канали і форми комунікації між МОЗ України, Державною службою України з надзвичайних ситуацій, Центром громадського здоров'я, регіональними ЦКПХ та центрами екстреної медичної допомоги. Особливу увагу слід приділити синхронізації процедур передавання інформації між медичними та немедичними службами, що відповідає вимогам Постанови Кабінету Міністрів України від 09.01.2014 № 11 щодо організації взаємодії суб'єктів реагування.

Окремим організаційним блоком має стати забезпечення безперервності роботи цифрового інструменту в умовах воєнних загроз, пошкодження критичної інфраструктури або перебоїв зі зв'язком. Рекомендується передбачити дублювання ключових функцій, резервні канали передачі даних, інструкції для персоналу щодо дій у випадку обмеження доступу до системи, а також механізми відновлення інформації після аварійних ситуацій. Це відповідає загальним принципам безперервності управління, визначеним у системі цивільного захисту.

Важливим елементом організаційних рекомендацій є створення механізму постійного моніторингу та оцінювання ефективності впровадження цифрового інструменту. Доцільним є застосування регулярного аналізу якості даних, оцінки часу реагування, дотримання регламентів, а також проведення аналізів огляду післядії («after-action review») для виявлення вузьких місць та вдосконалення процесів. Такий підхід забезпечує адаптивність системи та її поступове удосконалення.

Узагальнюючи викладене, організаційні рекомендації спрямовані на створення умов, за яких цифровий інструмент стане невід'ємним елементом інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я. Реалізація запропонованих заходів дозволить забезпечити узгодженість дій суб'єктів реагування, підвищити якість і своєчасність інформації, зміцнити готовність системи охорони здоров'я та сприятиме виконанню міжнародних зобов'язань України у сфері епідемічної безпеки.

5.4. Технічні рекомендації щодо проєктування та підтримки функціонування національного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації

Технічне забезпечення впровадження національного цифрового інструменту реагування на надзвичайні ситуації у сфері громадського здоров'я є ключовою умовою його надійності, безперебійної роботи та сумісності з існуючими інформаційними системами державного сектору. Технічні рекомендації мають сприяти створенню стабільної, захищеної та масштабованої інфраструктури, що відповідає сучасним вимогам кібербезпеки, управління даними та інтероперабельності, визначеним законодавством України та міжнародними стандартами.

Першим елементом технічного забезпечення є створення стійкої сервісної інфраструктури. Рекомендовано використовувати рішення, що забезпечують географічно розподілене резервування даних та можливість автоматичного перемикання у разі аварійних ситуацій. Такий підхід узгоджується з вимогами Постанови Кабінету Міністрів України щодо кіберзахисту державних інформаційних ресурсів та принципами безперервності управління, закладеними у Кодексі цивільного захисту України. Наявність резервних дата-центрів та дублювання ключових модулів системи дозволить мінімізувати ризики втрати

даних під час технічних збоїв або у разі впливу зовнішніх загроз, зокрема пов’язаних із воєнним станом.

Другим елементом є забезпечення інформаційної безпеки та захисту даних. З огляду на особливу чутливість інформації про надзвичайні ситуації, персональні дані постраждалих, лабораторні результати та інші захищені категорії інформації, система має відповідати вимогам Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», а також нормам Закону України «Про основи національної безпеки України» щодо критичної інфраструктури. Доцільним є застосування засобів багаторівневої автентифікації, шифрування каналів зв’язку, протоколів захищеної авторизації, а також фіксацію всіх дій користувачів, що забезпечує прозорість роботи системи та можливість відстеження виконаних операцій.

Третім елементом є інтероперабельність системи з існуючими цифровими ресурсами сектору охорони здоров’я та цивільного захисту. З технічної точки зору система має забезпечувати обмін даними з електронною системою охорони здоров’я (eHealth), лабораторними інформаційними системами, геоінформаційними платформами та цифровими ресурсами Державної служби України з надзвичайних ситуацій. Така взаємодія має ґрунтуватися на відкритих стандартах передачі даних, уніфікованих структурах повідомлень та сумісних API-інтерфейсах, що дозволить забезпечити синхронність інформації та уникнути дублювання.

Четвертим елементом є стандартизація даних та уніфікація форматів. Для забезпечення автоматизованої логічної перевірки, можливості машинного аналізу та коректної інтеграції з іншими інформаційними системами необхідно запровадити єдині класифікатори небезпечних подій, типів загроз, джерел інформації та рівнів ризику. Використання стандартизованих структур відповідатиме підходам, рекомендованим Всесвітньою організацією охорони здоров’я та Європейським центром профілактики та контролю захворювань.

П’ятим елементом технічного забезпечення є створення аналітичного модуля, здатного працювати з великими масивами даних та здійснювати прогнозування розвитку подій. Для цього система повинна підтримувати сучасні інструменти візуалізації, моделювання та автоматизованої оцінки ризиків, що дозволить підвищити доказовість управлінських рішень та оперативність реагування. Аналітичний компонент має включати інтеграцію з геоінформаційними системами, інструментами побудови ситуаційних дашбордів та можливістю створення автоматизованих звітів.

Шостим елементом є необхідність у забезпеченні технічних можливостей для масштабування системи. З огляду на змінний рівень навантаження у періоди епідемічних спалахів, техногенних аварій або масових подій, інфраструктура має підтримувати динамічне збільшення ресурсів та розширення функціоналу без зупинки роботи системи. Це сприятиме оперативному реагуванню на збільшення кількості подій та забезпечить стабільність сервісу.

Сьомим елементом технічних рекомендацій є організація технічної підтримки та оновлення системи. Доцільно створити спеціалізований сервісний центр або групу технічного супроводу, відповідальну за усунення збоїв, проведення профілактичних заходів, виконання оновлень програмного забезпечення та забезпечення цілодобової підтримки користувачів. Регулярне оновлення системи дозволить враховувати нові нормативні вимоги, міжнародні стандарти, технологічний розвиток та результати аналізу ефективності її застосування.

Таким чином, технічне забезпечення цифрового інструменту має базуватися на принципах надійності, безпеки, інтероперабельності та адаптивності. Реалізація цих рекомендацій створить передумови для стабільної, стійкої та ефективної роботи національної цифрової системи, здатної забезпечити належну ситуаційну обізнаність, підтримку управлінських рішень та відповідність міжнародним зобов’язанням України у сфері реагування на надзвичайні ситуації.

5.5. Очікувані результати впровадження національного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я

Впровадження національного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я має забезпечити якісні зміни в управлінні подіями, що становлять загрозу для здоров'я населення, підвищити стійкість системи охорони здоров'я та сприяти інтеграції України у міжнародний простір епідемічної безпеки. На основі проведеного аналізу та сформульованих рекомендацій визначаються такі очікувані результати.

1. Підвищення оперативності реагування на події.

Створення уніфікованого цифрового інструменту забезпечить значне скорочення часу між виявленням події та початком реагування. Автоматизовані алгоритми оцінки ризику, стандартизовані форми реєстрації та системи оповіщення дозволять прискорити ухвалення управлінських рішень та запустити необхідні заходи реагування у визначені терміни.

2. Формування єдиного інформаційного простору у сфері громадського здоров'я.

Інструмент забезпечить інтеграцію інформаційних потоків між функціональними підсистемами цивільного захисту, центрами контролю та профілактики хвороб, закладами охорони здоров'я, службами екстреної медичної допомоги та органами державної влади. Така інтеграція мінімізує дублювання даних, розбіжності у повідомленнях і сформує єдину оперативну картину подій.

3. Підвищення якості та достовірності даних.

Завдяки стандартизованим формам повідомлень, логічним перевіркам і єдиному алгоритму оцінки ризику система забезпечить точність, повноту і

верифікованість інформації. Це підвищить рівень доказовості управлінських рішень та дозволить уникнути помилок, пов’язаних із людським фактором.

4. Зміцнення міжвідомчої координації.

Цифрова система забезпечить прозорість комунікацій, структуровану взаємодію між суб’єктами реагування та можливість одночасного доступу до актуальної інформації для всіх відповідальних установ. Це сприятиме скоординованому реагуванню на надзвичайні події та раціональному використанню ресурсів.

5. Підвищення стійкості системи охорони здоров’я в умовах воєнного часу.

Завдяки резервним каналам зв’язку, підвищеним вимогам до інформаційної безпеки та можливості працювати за умов часткового зниження інфраструктурної доступності система дозволить підтримувати неперервність інформаційних процесів навіть у кризових ситуаціях.

6. Відповідність вимогам Міжнародних медико-санітарних правил. Інструмент забезпечить можливість автоматизованого застосування алгоритмів оцінки ризику згідно з Додатком 2 до ММСП, забезпечить своєчасне інформування Національного координатора з питань ММСП і полегшить передачу інформації до ВООЗ у встановлені терміни.

7. Підвищення ефективності управлінських рішень.

Інтегровані аналітичні модулі, дашборди, карти ризиків та автоматизовані звіти сприятимуть формуванню стратегічної та оперативної інформації, необхідної для планування заходів, визначення пріоритетів та оцінки результативності реагування.

8. Оптимізація використання ресурсів.

Система дозволить раціонально розподіляти наявні ресурси (медичні, лабораторні, кадрові), запобігати їх дублюванню та забезпечити своєчасне залучення необхідних підрозділів на основі об’єктивної оцінки ризиків і масштабів події.

9. Підвищення прозорості та підзвітності інформаційних процесів.

Журнали дій, фіксація часу внесення даних, відстеження змін та автоматизована історія подій забезпечать контроль якості, підзвітність суб'єктів та можливість проведення аудитів після завершення реагування.

10. Формування національного реєстру небезпечних подій.

Тривале централізоване зберігання даних дозволить аналізувати багаторічні тренди, здійснювати прогнозування, удосконалювати політики безпеки та підсилювати наукове обґрунтування управлінських рішень.

Узагальнюючи, впровадження національного цифрового інструменту сприятиме переходу до сучасної моделі управління надзвичайними ситуаціями у сфері громадського здоров'я, заснованої на доказах, інтегрованій взаємодії, технологічній стійкості та відповідності міжнародним стандартам.

ВИСНОВКИ ДО РОЗДІЛУ 5

У межах розділу здійснено комплексне опрацювання управлінських, нормативно-правових, організаційних та технічних аспектів впровадження національного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров'я. Проведений аналіз дозволив сформувати практичні рекомендації, релевантні чинним умовам функціонування системи охорони здоров'я України, з урахуванням воєнного стану та вимог Міжнародних медико-санітарних правил (IHR 2005). На основі виконаної роботи можна сформулювати такі узагальнені висновки:

1. Управлінська складова впровадження потребує створення єдиного координаційного центру, визначення відповідальних суб'єктів та чіткої системи підзвітності між усіма рівнями управління охороною здоров'я. Запропоновані рекомендації забезпечують можливість впровадження цифрового інструменту в умовах міжвідомчої взаємодії та підвищеного навантаження, характерного для воєнного часу.

2. Організаційні механізми впровадження повинні включати стандартизацію інформаційних потоків, розмежування ролей суб’єктів, наскрізну підготовку персоналу та створення інфраструктурних умов для роботи системи на регіональному й локальному рівнях. Запропоновані підходи сприяють формуванню єдиного алгоритму роботи з подіями незалежно від географії та масштабу загроз.

3. Нормативно-правові рекомендації, розроблені у межах розділу, узгоджені з чинним законодавством України (зокрема, Кодексом цивільного захисту України, Законом України «Про захист населення від інфекційних хвороб», Постановою КМУ № 11 від 09.01.2014) та визначають напрями їхнього доповнення для інтеграції цифрових рішень, включно зі стандартизованими електронними формами повідомлень, визначенням часових регламентів, вимог до інтероперабельності та кіберзахисту.

4. Технічні рекомендації охоплюють базові вимоги до архітектури цифрової системи, принципи побудови функціональних модулів, механізми захисту даних, резервування та забезпечення безперервності роботи в умовах воєнних ризиків. Запропоновані підходи створюють передумови для формування стійкої, масштабованої та сумісної з іншими державними сервісами цифрової екосистеми.

5. Очікувані результати впровадження цифрового інструменту передбачають підвищення оперативності реагування, формування єдиного інформаційного простору, покращення міжвідомчої взаємодії, зростання якості управлінських рішень, зміцнення стійкості системи охорони здоров’я та забезпечення відповідності IHR (2005). Упровадження інструменту також створить можливість довгострокового зберігання та аналізу даних, що сприятиме розвитку доказової політики у сфері громадського здоров’я.

Таким чином, розроблені практичні рекомендації формують цілісний, узгоджений логічно та нормативно обґрунтований підхід до впровадження національного цифрового інструменту інформаційного забезпечення реагування

на надзвичайні ситуації у сфері громадського здоров’я. Вони забезпечують реалістичний і практично здійсненний шлях модернізації інформаційної підсистеми охорони здоров’я, що є ключовим чинником підвищення національної біобезпеки та стійкості держави в умовах сучасних загроз.

ЗАГАЛЬНІ ВИСНОВКИ

Результати проведеного дослідження підтверджують, що ефективне реагування на надзвичайні ситуації у сфері громадського здоров'я є критично залежним від якості, швидкості та узгодженості інформаційних процесів, а сучасні умови - зокрема воєнні дії, техногенні ризики та епідемічні загрози - висувають принципово нові вимоги до системи кризового управління. Виконання поставленої мети та всіх визначених завдань дозволило сформувати цілісне наукове бачення проблеми й обґрунтувати необхідність створення національної цифрової системи інформаційного забезпечення реагування на події, що становлять ризики для здоров'я населення.

1. Теоретико-методологічний аналіз довів, що інформаційні процеси є базовою складовою сучасного менеджменту громадського здоров'я та мають вирішальне значення на всіх етапах реагування - від первинного виявлення події до ухвалення управлінських рішень. У роботі обґрунтовано, що цифровізація, уніфікація даних, алгоритмізація оцінки ризику та міжвідомча інтеграція відповідають світовим тенденціям розвитку систем готовності та реагування на надзвичайні ситуації та вимогам ММСП.

2. Аналіз нормативно-правового та організаційного забезпечення в Україні засвідчив, що незважаючи на достатньо розвинену законодавчу рамку у сфері цивільного захисту та охорони здоров'я, в ній відсутні положення щодо використання єдиного обов'язкового цифрового інструменту для реєстрації, оцінки та обміну інформацією про небезпечні події. Виявлено ключові структурні прогалини: фрагментованість інформаційних потоків, відсутність стандартів електронних форм, часових регламентів інформування, нормативної моделі міжвідомчої цифрової взаємодії та механізмів автоматизованої оцінки ризику. Ці обмеження істотно знижують оперативність і якість реагування.

3. Вивчення міжнародного досвіду показало, що провідні інституції (WHO, ECDC, CDC) використовують інтегровані цифрові платформи раннього виявлення загроз, які забезпечують автоматизацію оповіщення, стандартизацію

даних, вбудовану оцінку ризику, ситуаційну аналітику, міжвідомчу взаємодію та захищеність інформаційних систем. Порівняння довело, що функціональні характеристики таких платформ є релевантними для адаптації в Україні й мають слугувати моделлю для формування національного інструменту.

4. Обґрунтування необхідності створення національної цифрової системи показало, що в умовах значного зростання кількості небезпечних подій, складності міжвідомчої координації та високих ризиків воєнного часу чинна модель інформаційного забезпечення реагування не відповідає сучасним потребам. У роботі сформовано концептуальні цілі та принципи майбутньої системи, що базуються на стандартизації даних, централізації інформації, оперативності, автоматизації, інтероперабельності, кіберстійкості та відповідності міжнародним вимогам.

5. Практичні рекомендації щодо впровадження цифрового інструменту визначили комплекс управлінських, нормативних, організаційних та технічних заходів, які є необхідними для успішної реалізації проекту. Запропоновані рекомендації узгоджені з чинним законодавством, враховують специфіку функціональних підсистем МОЗ України та реалії воєнного стану. Окремо визначено очікувані результати впровадження системи - зростання оперативності реагування, підвищення якості даних, зміцнення міжвідомчої взаємодії, гармонізація з міжнародними стандартами й суттєве підвищення національної стійкості до біологічних, хімічних, радіаційних і техногенних загроз.

Комплексне дослідження підтвердило, що створення національного цифрового інструменту інформаційного забезпечення реагування на надзвичайні ситуації у сфері громадського здоров’я є науково обґрунтованою, практично необхідною та стратегічно важливою умовою посилення безпеки населення України. Розроблена концепція, сформований набір принципів та запропоновані практичні рекомендації створюють системний фундамент для побудови сучасної інтегрованої системи, яка забезпечить:

- уніфікацію та стандартизацію інформаційних процесів у галузі охорони здоров’я;
- оперативне та доказове ухвалення управлінських рішень на всіх рівнях влади;
- інтеграцію суб’єктів реагування у єдиний інформаційний простір**;**
- відповідність міжнародним стандартам та зобов’язанням України у сфері готовності та реагування на надзвичайні ситуації;
- реальне підвищення стійкості держави до надзвичайних ситуацій будь-якого походження.

Запропонована модель цифрової системи становить завершене та науково обґрунтоване рішення, що може бути використане як концептуальна основа для державних політик, нормативних ініціатив та практичної реалізації проектів у сфері громадського здоров’я та цивільного захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. World Health Organization. Health Emergency and Disaster Risk Management Framework. Geneva: WHO, 2019. 76 p.
https://www.who.int/publications/i/item/9789241516181

2. World Health Organization. International Health Regulations (2005). 3rd ed. Geneva: WHO, 2016. 74 p.
https://www.who.int/publications/i/item/9789241580496

3. Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту : постанова Кабінету Міністрів України від 27 вересня 2017 р. № 733.
URL: https://zakon.rada.gov.ua/laws/show/733-2017-%D0%BF
(дата звернення: 10.12.2025).

4. Epidemic Intelligence from Open Sources (EIOS). World Health Organization. URL: https://www.who.int/initiatives/eios

5. Early Warning and Response System (EWRS). European Centre for Disease Prevention and Control.
URL: https://www.ecdc.europa.eu/en/early-warning-and-response-system-ewrs

6. Epi-X: The Epidemic Information Exchange. Centers for Disease Control and Prevention. URL: https://www.cdc.gov/epix/

7. Кодекс цивільного захисту України від 02 жовтня 2012 р. № 5403-VI.
URL: https://zakon.rada.gov.ua/laws/show/5403-17
(дата звернення: 10.12.2025).

8. Про затвердження Положення про єдину державну систему цивільного захисту : постанова Кабінету Міністрів України від 09 січня 2014 р. № 11.
URL: https://zakon.rada.gov.ua/laws/show/11-2014-%D0%BF#Text
(дата звернення: 10.12.2025)

9. Про надання позачергових повідомлень Міністерству охорони здоров'я України : Наказ МОЗ України від 23 травня 2002 р. № 190.
URL: https://zakon.rada.gov.ua/go/v0190282-02
(дата звернення: 10.12.2025)

10. Про затвердження Положення про функціональну підсистему медичного захисту населення єдиної державної системи цивільного захисту : наказ Міністерства охорони здоров'я України від 23 березня 2023 р. № 542.
URL: https://zakon.rada.gov.ua/laws/show/z0590-23
(дата звернення: 11.12.2025)

11. Про затвердження Положення про функціональну підсистему забезпечення санітарного та епідеміологічного благополуччя населення єдиної державної системи цивільного захисту : наказ Міністерства охорони здоров'я України від 06 грудня 2022 р. № 2213.

URL: https://zakon.rada.gov.ua/laws/show/z1601-22

(дата звернення: 11.12.2025)

12. Про затвердження Форм первинної облікової документації з інфекційної, дерматовенерологічної, онкологічної захворюваності та інструкцій щодо їх заповнення : наказ Міністерства охорони здоров'я України від 31 жовтня 2006 р. № 686.

URL: https://zakon.rada.gov.ua/laws/show/z0686-06#Text

(дата звернення: 11.12.2025)

13. Про затвердження Плану реагування на надзвичайні ситуації Міністерства охорони здоров'я України у сфері медичного захисту населення та санітарного і епідеміологічного благополуччя населення : наказ Міністерства охорони здоров'я України № 2172 від 21 грудня 2023 р.

URL: https://moz.gov.ua/uk/decrees/nakaz-moz-ukraini-vid-21122023--2172-----pro-zatverdzhennja-planu-reaguvannja-na-nadzvichajni-situacii-ministerstva-ohoroni-zdorov%E2%80%99ja-ukraini-u-sferi-medichnogo-zahistu-naselennja-ta-sanitarnogo-ta-epidemiologichnogo-blagopoluchchja-naselennja

(дата звернення: 11.12.2025)

14. Про затвердження Інструкції щодо організації взаємодії між Державною службою України з надзвичайних ситуацій і Міністерством охорони здоров'я України в разі виникнення надзвичайних ситуацій : постанова Кабінету Міністрів України від 28 червня 2000 р. № 879.

URL: https://zakon.rada.gov.ua/laws/show/z0479-18#Text

(дата звернення: 11.12.2025)

15. Про затвердження Порядку проведення оцінки ризиків для здоров'я та санітарно-епідемічного благополуччя населення та здійснення за її результатами профілактичних, обстежувальних, консультаційних та інших заходів : наказ Міністерства охорони здоров'я України від 01 вересня 2025 р. № 1373.

URL: https://moz.gov.ua/uk/decrees/nakaz-moz-ukrayini-vid-01-09-2025-1373-pro-zatverdzhennya-poryadku-provedennya-ocinki-rizikiv-dlya-zdorov-ya-ta-sanitarno-epidemichnogo-blagopoluchchya-naselennya-ta-provedennya-26366

(дата звернення: 11.12.2025)

16. Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями : постанова Кабінету Міністрів України від 17 березня 2004 р. № 368.

URL: https://zakon.rada.gov.ua/laws/show/368-2004-%D0%BF#Text

(дата звернення: 11.12.2025)

17. Ayebare R., Moriyón O.J., Grant L., et al. Event-based surveillance for outbreak detection in low-resource settings: opportunities and challenges. BMC Public Health. 2024;24:18466.

Available at: https://agritrop.cirad.fr/609204/1/s12889-024-18466-1-1.pdf

(Accessed: 10 December 2025).

18. Artificial intelligence in epidemic intelligence systems: improving early detection of public health threats. BMC Public Health, 2025.

URL: https://doi.org/10.1186/s12889-025-21998-9

(дата звернення: 12.01.2025).

19. European Centre for Disease Prevention and Control. European Surveillance System (TESSy). - https://www.ecdc.europa.eu/en/surveillance-and-disease-data/surveillance-systems/tessy

(Accessed: 10 December 2025)

20. Про захист населення від інфекційних хвороб : Закон України від 06 квітня 2000 р. № 1645-III.

URL: https://zakon.rada.gov.ua/laws/show/1645-14#Text

(дата звернення: 12.12.2025)

21. Основи законодавства України про охорону здоров’я : Закон України від 19 листопада 1992 р. № 2801-XII.

URL: https://zakon.rada.gov.ua/laws/show/2801-12

(дата звернення: 12.12.2025)

22. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем : постанова Верховної Ради України від 18 червня 2025 р. № 712-IX.

URL: https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text

(дата звернення: 12.12.2025)

23. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05 липня 1994 р. № 80/94-ВР.

URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

(дата звернення: 12.12.2025)

24. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05 жовтня 2017 р. № 2155-VIII.

URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

(дата звернення: 12.12.2025)