

### Список використаних джерел

1. Курепін В. М., Курепін Д. В., Іваненко В. С. Цивільний захист: навчальний посібник для здобувачів другого (магістерського) рівня вищої освіти денної та заочної форм здобуття вищої освіти. Миколаїв : МНАУ, 2025. 491 с. URL:<https://dspace.mnau.edu.ua/jspui/handle/123456789/20130>.
2. Курепін В. М., Самойленко О. О., Бацуровська І. В. Кібербезпека цифрового освітнього середовища як складова системи безпеки праці та життєдіяльності. Суспільство та національні інтереси: журнал. 2025. № 11(19). С 255-268. <https://dspace.mnau.edu.ua/jspui/handle/123456789/22584>.

## РОЛЬ МОНІТОРІНГУ, ВИЯВЛЕННЯ ВТОРГНЕНЬ ТА РЕАГУВАННЯ НА КІБЕРГІНЦИДЕНТИ

Мельничук Д.В.

*Миколаївський національний аграрний університет  
kypins@ukr.net*

В умовах воєнного стану моніторинг та кіберзахист систем оповіщення про загрози для населення набуває критичного значення. Ці системи стають потенційною метою для кібератак, спрямованих на дестабілізацію суспільства. Потрібне цілодобове відстеження стану серверів, каналів зв'язку та програмного забезпечення, які забезпечують передачу сигналів тривоги.

При різкому збільшенні мережевого трафіку система моніторингу може виявити ознаки DDoS-атаки на сервер, який відповідає за розсилку повідомлень про повітряну тривогу. Щоб не допустити зриву оповіщення населення автоматично активуються механізми обмеження трафіку або відбувається переключення на резервні канали.

Важливо захистити системи керування від спроб несанкціонованого доступу. Якщо обліковий запис оператора намагаються використати з нетипової геолокації або в незвичний час, система безпеки повинна заблокувати сесію та повідомити адміністратора про потенційний інцидент. Це дозволить запобігти ситуаціям, коли злодії могли б змінити налаштування системи або запустити фальшиві сигнали тривоги.

Елементом кіберзахисту є системи аналізу поведінки користувачів. Вони фіксують відхилення від звичних дій персоналу та сигналізують про можливу компрометацію доступу. Оперативне реагування на кіберінциденти відіграє окрему роль. У разі виявлення шкідливого програмного забезпечення серверні системи оповіщення негайно здійснюють ізоляцію враженого сегмента мережі. Управління переводиться на резервний центр, а відновлення працездатності відбуваються з резервних копій. В умовах воєнного стану, щоб не допустити перерв у передачі критичних повідомлень, такі дії виконуються за лічені хвилини.

Важливим є постійне тестування та удосконалення систем кіберзахисту. Проведення навчальних симуляцій атак дозволяє перевірити готовність персоналу та ефективність алгоритмів реагування. Також впроваджується практика дублювання каналів оповіщення. Інформація передається одночасно через мобільні застосунки, SMS та локальні системи гучномовців, це зменшує ризик повної втрати зв'язку навіть у разі успішної атаки на один із каналів.

При виявленні загроз у системах оповіщення алгоритми дій персоналу починаються з фіксації аномалії, яка може бути як технічною, так і кібернетичною. Дії мають бути чітко регламентованими, відпрацьованими та максимально автоматизованими, оскільки від швидкості та правильності реакції залежить безпека населення.

У такій ситуації першим кроком є верифікація загрози: перевірка журналів подій, аналіз джерела підключення, співставлення з типовими сценаріями роботи системи. Після підтвердження інциденту переходять до локалізації загрози. Якщо виявлено спробу несанкціонованого доступу, обліковий запис негайно блокується, сесії примусово завершуються, а відповідний сегмент мережі може бути тимчасово ізольований. У випадку з підозрою на вредоносне програмне забезпечення, заражений сервер відключається від мережі, щоб запобігти поширенню атаки. Водночас інші оператори можуть перевести управління системою оповіщення на резервний центр, щоб забезпечити безперервність передачі сигналів населенню.

Отже, ефективний моніторинг, своєчасне виявлення загроз та оперативне реагування на кіберінциденти забезпечують безперервність роботи систем оповіщення та належний захист критичної інфраструктури в умовах сучасних загроз воєнного часу.

## **ВПЛИВ МІНЕРАЛЬНОГО СКЛАДУ ПИТНОЇ ВОДИ НА ЗДОРОВ'Я НАСЕЛЕННЯ В УМОВАХ ВОЄННО-ТЕХНОГЕННОГО НАВАНТАЖЕННЯ В УКРАЇНІ**

**Міщенко Сергій Віталійович**

*асистент кафедри захисту України та безпеки життєдіяльності  
Полтавський національний педагогічний університет імені В. Г. Короленка  
sergeymishchenko777@gmail.com*

У сучасних умовах воєнного стану в Україні питання якості питної води є одним із ключових у системі цивільного захисту населення. Руйнування об'єктів водопостачання, пошкодження очисних споруд, забруднення водних джерел продуктами вибухів, паливно-мастильними матеріалами та важкими металами формують комплексну екологічну небезпеку. За даними досліджень, стан питної води прямо пов'язаний із рівнем захворюваності населення, зокрема серцево-судинної та шлунково-кишкової патології [1].

Мінеральний склад питної води є важливим чинником, що визначає функціональний стан організму. Зокрема, доведено, що дефіцит кальцію та магнію у воді пов'язаний із підвищенням ризику серцево-судинних захворювань і порушенням метаболічних процесів [2]. Водночас надлишок солей жорсткості може спричинити нефролітиаз і дисбаланс електролітів.

В умовах воєнних дій особливої актуальності набуває проблема використання альтернативних джерел водопостачання. Населення змушене споживати воду з колодязів, відкритих водойм або привізну воду невідомого складу, що підвищує ризик як хімічного, так і біологічного забруднення. За даними Центру громадського здоров'я, вживання води з нерегульованим мінеральним складом може призводити до порушення кислотно-лужної рівноваги та водно-солевого балансу [3].

Додаткову небезпеку становить техногенне забруднення води внаслідок бойових дій. Потрапляння у воду важких металів, нітратів, нафтопродуктів та хлорорганічних сполук може спричинити токсичні та канцерогенні ефекти [4]. У таких умовах особливого значення набуває моніторинг якості води та впровадження сучасних методів оцінки її впливу на організм, зокрема за допомогою біомаркерів (рН слини, буферна здатність).

Умови воєнного стану значно посилюють ризики, пов'язані з якістю питної води. Мінеральний склад води є критичним фактором впливу на здоров'я населення та має розглядатися як складова екологічної безпеки. Необхідно впроваджувати системи