УДК 614.8

Шклярук М. Б.

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ ПІД ЧАС НАДЗВИЧАЙНИХ СИТУАЦІЙ

Вінницький національний технічний університет

Анотація

У сучасному світі, де кількість надзвичайних ситуацій постійно зростає, надзвичайно важливою є роль інформаційних технологій у забезпеченні безпеки життєдіяльності населення. У тезах розглядаються основні напрями використання ІТ-рішень під час надзвичайних ситуацій природного, техногенного та соціального характеру.

Ключові слова: інформаційні технології, безпека життєдіяльності, надзвичайні ситуації, моніторинг, кібербезпека, штучний інтелект, геоінформаційні системи.

Abstract

In the modern world, where the number of emergencies is constantly growing, the role of information technologies in ensuring the safety of the population is extremely important. The theses consider the main directions of using IT solutions during emergencies of a natural, man-made and social nature.

Keywords: information technologies, life safety, emergencies, monitoring, cybersecurity, artificial intelligence, geographic information systems.

Вступ

У XXI столітті інформаційні технології стали невід'ємною частиною повсякденного життя людини. Вони не лише спрощують комунікацію, керування процесами й збереження даних, але й відіграють ключову роль у таких критичних галузях, як оборона, медицина, енергетика та безпека життєдіяльності. Особливо яскраво значення ІТ виявляється під час надзвичайних ситуацій — як природного, так і техногенного чи соціального походження. Своєчасна обробка даних, миттєва передача інформації, прогнозування небезпеки, організація евакуації, управління ресурсами — усе це можливе лише за умови ефективного використання сучасних цифрових інструментів.

Системи раннього оповіщення

У сучасному світі, де технології відіграють провідну роль у забезпеченні безпеки, системи раннього оповіщення стали критично важливим елементом інфраструктури життєдіяльності. Їхня головна мета — завчасно інформувати населення про наближення небезпеки: природного, техногенного або соціального характеру. Час, виграний завдяки такому повідомленню, може врятувати тисячі життів. Раніше такі системи асоціювались лише з сиренами чи радіо, однак сьогодні це цілісні комплекси, що використовують мережі сенсорів, супутниковий моніторинг, інтернет речей (IoT) та мобільні додатки.

Прикладом ефективної цифровізації систем раннього сповіщення в Україні є мобільний застосунок "Повітряна тривога", який став частиною повсякденного життя мільйонів українців у період активних бойових дій. Завдяки інтеграції з державними системами, додаток дозволяє миттєво сповіщати користувачів про небезпеку з урахуванням їхнього місцеперебування. Такі рішення — це вже не просто попередження, а стратегічна система захисту населення, що базується на точності, швидкості та автоматизації. У перспективі розвиток таких систем передбачає застосування штучного інтелекту, який буде не лише передавати, а й передбачати загрози ще до їхнього виникнення.

Геоінформаційні системи (GIS)

Геоінформаційні системи (GIS) стали невід’ємною частиною управління надзвичайними ситуаціями у світі [1]. Вони дозволяють об'єднувати та аналізувати просторові дані для прийняття рішень у реальному часі. У надзвичайних ситуаціях GIS допомагає створювати карти зон ризику, планувати евакуаційні маршрути, визначати критичні точки та координувати дії служб порятунку.

Саме точність і візуалізація — головні переваги таких систем, що дозволяють не лише бачити ситуацію в просторі, а й моделювати її розвиток.

У період повномасштабної війни в Україні, геоінформаційні системи використовувались для відстеження напрямків обстрілів, створення карт гуманітарної допомоги та координації логістики. Наприклад, інтерактивні карти укриттів, які стали доступними у багатьох містах, дозволяють мешканцям швидко знайти найближче безпечне місце. GIS активно застосовуються також в екологічному моніторингу: українська платформа "Ecomap" дозволяє візуалізувати забруднення і виявляти потенційні екологічні загрози. У надзвичайних ситуаціях час — вирішальний фактор, і саме GIS надає можливість швидко отримати критично важливу просторову інформацію для порятунку життя.

Мобільні додатки та платформи зв'язку

Мобільні додатки стали справжнім інструментом виживання у сучасному небезпечному світі. В умовах надзвичайних ситуацій мобільні платформи дозволяють не лише отримувати інформацію, а й повідомляти про своє місцезнаходження, подавати сигнали SOS, надавати дані про руйнування або потерпілих. Комунікація — один із ключових факторів у кризових умовах, і мобільні технології перетворюють кожен смартфон на персональний центр безпеки [2].

В Україні яскравим прикладом є додаток "єТривога", який інтегрований із застосунком "Дія", а також Telegram-боти, створені для оперативного повідомлення про обстріли, зниклих людей або необхідну допомогу. Крім того, застосунок TacticMedAid навчає цивільне населення наданню домедичної допомоги під час воєнних дій, що теж є елементом забезпечення безпеки. Платформи зв'язку також стають опорою для волонтерів, лікарів, працівників служб порятунку, бо дозволяють оперативно координувати дії в межах навіть найвіддаленіших регіонів. У майбутньому очікується ще глибша інтеграція таких додатків із державними системами та використання біометрії для персоніфікованого захисту.

Використання штучного інтелекту

Упродовж останнього десятиліття штучний інтелект (ШІ) вийшов за межі лабораторних досліджень і почав активно впроваджуватись у повсякденне життя [3]. Його застосування охоплює найрізноманітніші сфери — від медицини до фінансів, від транспорту до освіти. Однак особливо цінною є здатність ШІ бути корисним у критичних умовах, зокрема — під час надзвичайних ситуацій. Саме у стресових, швидкоплинних і непередбачуваних умовах ШІ виявляє свою головну силу — здатність швидко обробляти великі обсяги інформації, виявляти закономірності та прогнозувати розвиток подій у режимі реального часу.

Надзвичайні ситуації за своєю природою вимагають негайної реакції. В умовах обмеженого часу і постійно змінної ситуації, навіть найдосвідченішим фахівцям важко швидко приймати зважені рішення. Тут і вступає в гру штучний інтелект, який дозволяє автоматизувати аналіз загроз, оцінювати ймовірні сценарії розвитку подій, прогнозувати масштаби наслідків і навіть пропонувати найефективніші варіанти реагування [3]. Для прикладу, алгоритми машинного навчання можуть обробляти дані з супутників, дронів, метеостанцій, камер відеоспостереження, соціальних мереж та інших джерел, щоб оцінити ризики повеней, землетрусів, пожеж або радіаційного забруднення.

У світовій практиці застосування ШІ в безпекових цілях уже давно є нормою. Наприклад, у США ШІ використовується для передбачення поширення лісових пожеж, а в Індії — для виявлення заторів на дорогах під час масової евакуації. У Японії з допомогою ШІ моделюють сценарії землетрусів та оптимізують маршрути екстрених служб. Такі системи працюють на основі великих даних (Big Data), що зберігаються в хмарних сховищах та обробляються у режимі 24/7. ШІ також використовується для ідентифікації небезпечної поведінки людей у натовпі — наприклад, під час евакуації з будівель або підземних станцій — що дозволяє рятувальникам краще координувати свої дії.

Україна, попри складні обставини, також починає впроваджувати елементи ШІ у свої системи безпеки. Зокрема, технології комп'ютерного зору використовуються для автоматичного розпізнавання облич та автомобілів на блокпостах, контролю за дотриманням комендантської години, а також для аналізу відео з дронів з метою фіксації руйнувань або пошуку людей. В умовах війни такі інструменти мають вирішальне значення, оскільки дозволяють частково зменшити навантаження на людські ресурси, підвищити точність рішень і мінімізувати людський фактор. Команда українських IT-

волонтерів також працює над проєктами аналізу супутникових знімків та передбачення напрямків атак з використанням нейронних мереж.

ШІ активно впроваджується й у медичну сферу під час НС: він дозволяє проводити сортування потерпілих, прогнозувати розвиток ускладнень, визначати пріоритети в наданні допомоги, а також координувати доставку медичних засобів у найкритичніші точки. У поєднанні з дронами та роботизованими платформами ШІ забезпечує швидке реагування там, де присутність людини небезпечна або неможлива.

Окремо варто згадати роль штучного інтелекту у створенні віртуальних симуляцій — цифрових копій об'єктів, міст чи регіонів (так званих "цифрових двійників"). Ці моделі дозволяють тестувати сценарії поведінки систем у разі різних надзвичайних ситуацій: вибухів, атак, природних катастроф. Таким чином, ШІ стає не лише інструментом реагування, а й ефективним засобом підготовки до криз.

Проте впровадження ШІ у сферу безпеки супроводжується і низкою викликів. Це — потреба у захисті конфіденційних даних, запобігання хибним спрацьовуванням, обмеження пов'язані з недостатньою якістю вхідних даних або відсутністю стандартизації в інфраструктурі. Саме тому роль ІТ-фахівців полягає не лише у створенні алгоритмів, а й у забезпеченні їхньої надійності, прозорості та етичності.

Отже, використання штучного інтелекту в надзвичайних ситуаціях — це вже не футуристична ідея, а реальна потреба часу. ШІ стає ключовим гравцем у збереженні людського життя, зменшенні наслідків катастроф та побудові безпечного середовища. Для фахівців у сфері інформаційних технологій це відкриває нові можливості — не лише у професійному розвитку, а й у безпосередньому впливі на захист суспільства. У сучасному світі майбутнє безпеки все більше залежить не від кількості людей у штабах, а від точності алгоритмів, які вони створюють і якими керують.

Кібербезпека під час надзвичайних ситуацій

Під час надзвичайних ситуацій особливо вразливою стає цифрова інфраструктура: енергетичні системи, системи зв'язку, банківські сервіси, водопостачання, транспортні вузли. Кібератака у критичний момент може призвести до колапсу не меншого масштабу, ніж фізичний удар. Саме тому кібербезпека — це не лише про захист даних, а про реальний захист життя та функціонування суспільства [4].

В умовах воєнного стану в Україні питання кіберзахисту стало особливо актуальним. Держава активно співпрацює з ІТ-компаніями, волонтерами та хактивістами, щоб забезпечити стійкість до атак з боку противника. Національний центр кібербезпеки під егідою Держспецзв'язку координує роботу по відбиттю атак на об'єкти критичної інфраструктури, включаючи електростанції, лікарні, урядові сервери. Українські компанії, такі як Hacken, активно залучені до побудови систем проактивного захисту.

Під час НС важливо забезпечити не лише технічну стійкість, а й інформаційну гігієну. Фейкові повідомлення, паніка, дезінформація — це частина кіберзагроз, що можуть дестабілізувати суспільство. Саме тому цифрова грамотність, багатофакторна аутентифікація, захист паролів, регулярне оновлення систем — усе це сьогодні є основами особистої безпеки, нарівні з аптечкою чи засобами зв'язку. У майбутньому саме баланс між відкритістю систем і їхнім захистом стане основним викликом для фахівців з безпеки життєдіяльності.

Висновки

Проаналізовані напрямки застосування інформаційних технологій — системи раннього оповіщення, геоінформаційні платформи, мобільні додатки, штучний інтелект і кібербезпека — доводять, що ІТ-інфраструктура вже давно перестала бути допоміжним інструментом у системах безпеки. Натомість вона стала їхнім ядром. Цифрові рішення дозволяють не лише швидко реагувати на загрози, але й попереджати їх, координувати рятувальні операції, зберігати дані, навчати населення і забезпечувати стабільність у критичних умовах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Грищенко Л. А. Геоінформаційні системи в безпеці життєдіяльності. Львів: Видавництво ЛНУ, 2021. 240 с.
2. Коваленко О. П. Інформаційні технології в управлінні кризовими ситуаціями. Київ: Техніка, 2023. 320 с.
3. Іванов С. О. Штучний інтелект у прогнозуванні катастроф. Київ: BHV, 2024. 360 с.
4. Сидоренко В. М. Кібербезпека в умовах надзвичайних ситуацій. Харків: Фабрика знань, 2022. 280 с.

Шклярук Марія Богданівна — студентка групи 2ПІ-22б, Факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: mariia.shkliiaruk@gmail.com

Shkliaruk Mariia — student of group 2PI-22b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: mariia.shkliiaruk@gmail.com