Міністерство освіти і науки України
Луцький національний технічний університет

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА АВТОМАТИЗОВАНІ СИСТЕМИ В ЦИВІЛЬНІЙ БЕЗПЕЦІ

Конспект лекцій
для здобувачів першого (бакалаврського) рівня
галузі знань К Безпека та оборона
спеціальності К10 Цивільна безпека
денної та заочної форм навчання

Луцьк-2025

УДК 004:331.445(076)
І-74

До друку
Голова вченої ради факультету цифрових, освітніх та соціальних технологій ЛНТУ _____ Г.А. Герасимчук

Затверджено вченою радою факультету цифрових, освітніх та соціальних технологій ЛНТУ, протокол № ____ від «____»_____ 2025 року.

Електронна копія друкованого видання передана для внесення в репозитарій ЛНТУ.
Директор бібліотеки _____ Н.П. Поліщук

Рекомендовано до видання на засіданні кафедри цивільної безпеки ЛНТУ,
протокол № _____ від «____»_____ 2025 року.
Завідувач кафедри цивільної безпеки _____ В.І. Федорчук-Мороз

Укладач: _____М.В. Рудинець, кандидат технічних наук, доцент, кафедри цивільної безпеки ЛНТУ.

Рецензент: _____Л.Ф. Бондарчук кандидат сільськогосподарських наук, доцент кафедри цивільної безпеки ЛНТУ.

Відповідальний за випуск:_____В.І. Федорчук-Мороз, кандидат технічних наук, доцент, завідувач кафедри цивільної безпеки ЛНТУ.

І-74 Інформаційні технології та автоматизовані системи в цивільній безпеці [Текст]: Конспект лекцій для здобувачів першого (бакалаврського) рівня галузі знань К Безпека та оборона спеціальності К10 Цивільна безпека денної та заочної форм навчання / уклад. М.В. Рудинець – Луцьк: ЛНТУ, 2025. – 88 с.

Конспект лекцій укладено згідно з чинною програмою курсу «Інформаційні технології та автоматизовані системи в цивільній безпеці» з метою надання методичної допомоги у процесі вивчення дисципліни.

Зміст

Тема 1. Інформаційні технології.....5
1.1. Поняття інформаційної технології. Етапи розвитку інформаційних технологій 5
1.2. Класифікація інформаційних технологій 6
1.3. Нейромережні технології 7
1.4. Технологія автоматизованих робочих місць 7
1.5. Гіпертекстова технологія. Технологія мультимедіа.....8
1.6. Мережні технології. Технології Internet 8
1.7. Технологія електронної пошти.....11
1.8. Інформаційних технології у цивільній безпеці.....13
Тема 2. Інформаційні системи моніторингу загроз природного та техногенного характеру 15
2.1. Метеорологічні інформаційні системи моніторингу.....15
2.2. Гідрологічні інформаційні системи моніторингу.....17
2.3. Інформаційні системи радіаційного моніторингу 18
2.4. Інформаційні системи хімічного моніторингу.....19
Тема 3. Геоінформаційні системи (ГІС) у цивільній безпеці.....22
3.1. Принципи роботи геоінформаційних систем (ГІС).....22
3.2. Картографування небезпек системами ГІС 22
3.3. Моделювання зон ураження за допомогою ГІС.....24
Тема 4. Дистанційне зондування Землі та його застосування у запобіганні НС.....26
4.1. Супутникові дані як елемент дистанційного зондування Землі у запобіганні надзвичайних ситуацій.....26
4.2. Дані, отримані за допомогою дронів 27
4.3. Фотограмметрія у системі запобіганні НС.....28
4.4. Аналіз зображень для забезпечення безпеки у системі цивільної безпеки.....28
Тема 5. Бази та банки даних у цивільній безпеці 31
5.1. Принципи проєктування баз даних 31
5.2. Моделі даних 32
5.3. Керування реляційними базами даних – SQL.....32
5.4. Збирання та зберігання даних про об’єкти підвищеної небезпеки.....33
5.5. Збирання та зберігання даних про укриття 33
5.6. Збирання та зберігання даних про ресурси реагування на НС.....34
5.7. Спеціалізовані державні та відомчі інформаційні банки даних: Єдина державна система цивільного захисту.....34
5.8. Реєстри ДСНС у системі цивільної безпеки України.....35
Тема 6. Системи підтримки прийняття рішень у цивільній безпеці.....39
6.1. Аналітичні моделі у цивільній безпеці.....39
6.2. Алгоритми оцінки ризиків у системі цивільної безпеки 40
6.3. Сценарне прогнозування, інформаційні панелі 41
Тема 7. Архітектура та класифікація автоматизованих систем у сфері цивільного захисту 43
7.1. Типи АСУ, принципи побудови 43
7.2. Компоненти АСУ 45
7.3. Рівні автоматизації АСУ у сфері цивільної безпеки України 46
Тема 8. Автоматизовані системи оповіщення населення та управління реагуванням на НС.....49
8.1. Принципи побудови автоматизованих систем оповіщення населення та управління реагуванням на надзвичайні ситуації 49
8.2. Канали передачі сигналів. 50
8.3. Цифрові системи оповіщення населення 51

Тема 9. Хмарні технології та цифрові платформи у системах цивільної безпеки.....53
9.1. Хмарна інфраструктура.....53
9.2. Сервіси для обробки великих даних.....56
9.3. Кіберстійкість платформ.....57
Тема 10. Мобільні застосунки та технології штучного інтелекту у прогнозуванні та реагуванні на надзвичайні ситуації.....60
10.1. Додатки для оповіщення. 60
10.2. Додатки для навігації.....60
10.3. Додатки для зв'язку, координації дій під час НС. 61
10.4. Машинне навчання. 62
10.5. Аналіз великих даних.....63
10.6. Алгоритми для оцінки загроз у системах цивільної безпеки 64
Тема 11. Інформаційна безпека та захист даних в автоматизованих системах цивільної безпеки 68
11.1. Кібербезпека.....68
11.2. Захист інформації. 69
11.3. Загрози інформаційним системам у сфері цивільної безпеки.....70
Тема 12. Віртуальна, доповнена реальність та перспективні цифрові технології у сфері цивільної безпеки 74
12.1. VR/AR-тренажери.....74
12.2. Симуляційні моделі 75
12.3. Практичні кейси навчання рятувальників 76
12.4. Інтернет речей (IoT) у сфері цивільної безпеки.....77
12.5. Сенсорні мережі.....78
12.6. Роботизовані системи у сфері цивільної безпеки.....79
12.7. Цифрові двійники об'єктів у системі цивільної безпеки.....79

Тема 1. Інформаційні технології

1.1. Поняття інформаційної технології. Етапи розвитку інформаційних технологій.
1.2. Класифікація інформаційних технологій.
1.3. Нейромережні технології.
1.4.Технологія автоматизованих робочих місць.
1.5. Гіпертекстова технологія. Технологія мультимедіа.
1.6. Мережні технології. Технології Internet.
1.7. Технологія електронної пошти.
1.8. Інформаційних технології у цивільній безпеці.

1.1. Поняття інформаційної технології. Етапи розвитку інформаційних технологій

Інформаційна технологія (ІТ) може бути визначена як поєднання процедур, які реалізують функції збору, накопичення, зберігання, обробки і передачі даних на основі застосування вибраного комплексу технічних засобів за участі управлінського персоналу [1; 2].

Тому інформаційні технології нерозривно пов'язані з технічним і програмним середовищем, в якому вони реалізовані.

Таким чином, автоматизована інформаційна технологія складається з технічних пристроїв (найчастіше – комп’ютерів, комунікаційної техніки), програмного забезпечення, організаційно-методичних матеріалів, персоналу, об’єднаних у технологічний ланцюжок. Цей ланцюжок забезпечує збір, передачу, накопичення, зберігання, опрацювання, використання і поширення інформації [3].

Основу технології обробки даних складають процеси перетворення вхідної інформації в результативну. *Мета будь-якої інформаційної технології* – отримати потрібну інформацію необхідної якості на заданому носії. Отже, кожна ІТ закінчується виробництвом *інформаційного продукту* [2].

Комп'ютерні інформаційні технології пройшли в своєму розвитку етап машинних ресурсів, етап програмування, етап нових інформаційних технологій, етап високих інформаційних технологій.

Функціональні обмеження і висока вартість ЕОМ цілком визначали головне завдання інформаційної технології **етапу машинних ресурсів** (50-ті – 60-ті рр.) – підвищення ефективності обробки даних за вже формалізованими алгоритмами або слабоформалізованими алгоритмами. Для прискорення кодування за алгоритмами були створені алгоритмічні мови Алгол, Фортран. Але загальні витрати на програмування складали декілька відсотків від вартості машино-години ЕОМ. Тому завданням ІТ на цьому етапі була *економія машинних ресурсів*, тобто необхідність при використанні мінімального об'єму оперативної пам’яті забезпечити максимальну кількість операцій, що виконуються за одиницю машинного часу.

Завданням другого етапу – етапу програмування (середина 60-х рр. до початку 80-х рр.) стає *економія людських ресурсів*, оскільки успіхи в розвитку електроніки привели до швидкого зниження вартості машинних операцій і біта оперативної пам'яті, тоді як витрати на розробку і супровід програм мали тенденцію до зростання [5].

В основі концепції третього **етапу новітніх інформаційних технологій** (початок 80-х рр.) лежать дві центральні ідеї: автоформалізація професійних знань користувачів в обчислювальному середовищі АРМ, інтелектуалізація всіх форм взаємодії користувачів з технічними засобами [1; 7].

Технічною базою на даному етапі розвитку інформаційної тех.нології став масовий випуск персональних ЕОМ (ПЕОМ). Користувачеві рекомендувалося автоматизувати все, що люди можуть описати, програмувати без програмістів. Головним завданням нових інформаційних технологій було створення типової технології автоматизації персональних знань. Метою на даному етапі була *економія роботи користувачів*. Елементом нової

інформаційної технології стає *автоматизоване робоче місце (АРМ)* фахівців різного профілю.

В основі концепції **високих інформаційних технологій** (четвертий етап) лежить ідея удосконалення засобів спілкування між людьми, глобалізація інформаційного простору до масштабів всієї планети.

Виникнення високих інформаційних технологій стало можливим завдяки здешевленню вартості ПЕОМ і широкому їх обхвату глобальними комп'ютерними мережами, заснованими на платформі [4].

Програмне забезпечення включає вже не тільки індивідуальні додатки, але і системи конференцій, підтримує мультимедіа і тривимірну графіку. Мультимедійні додатки полегшують спілкування людей. Інформаційне забезпечення побудоване на базі розподілених баз даних.

Головними завданнями високих інформаційних технологій є *досягнення універсальності методів комунікацій; підтримка систем мультимедіа і максимальне спрощення інтерфейсу «Людина-ЕОМ»*, заснованого на принципах інтуїтивного інтерфейсу; відкритість стандартів, тобто використання тих протоколів і програмних інтерфейсів, які гарантували б створення єдиного інтерфейсу для всіх взаємодій з ЕОМ: для доступу до файлів, повідомлень, Web-сторінок, документів, графіки і мультимедіа.

Метою даного етапу є *зниження вартості інформаційного контакту, необмеженість об'єму інформації,* доступної користувачеві, повноцінність використання як персональних машинних ресурсів, так мережних.

1.2. Класифікація інформаційних технологій

Технологія як процес властива будь-якій предметній області.

Технологія як процес властива будь-якій предметній області. Предметна технологія являє собою послідовність етапів перетворення первинної інформації у результативну відповідно до логіки конкретної діяльності [2].

Інформаційні технології, що використовуються як інструментарій у різних предметних областях для вирішення універсальних завдань обробки інформації, називають забезпечуючими технологіями. До них належать текстові процесори, системи управління базами даних, табличні та графічні процесори [3].

Сукупність забезпечуючих технологій, об’єднаних для автоматизації конкретної управлінської функції, формує функціональну інформаційну технологію, яка є складовою інформаційної системи [4].

Залежно від типу інформації, що обробляється, інформаційні технології поділяють на технології обробки даних, текстової, графічної інформації, знань та мультимедійних об’єктів реального світу.

Класифікація ІТ за видами інформації, яка обробляється

Види інформації, яка обробляється	Види інформаційних технологій	
Дані	СУБД, алгоритмічні мови, табличні процесори	Інтегровані пакети (об'єднання різних технологій)
Текст	текстові процесори	
Графіка	графічні процесори	
Знання	експертні системи	
Об'єкти реального світу	засоби мультимедіа	

За способом використання обчислювальної техніки виділяють інформаційні технології централізованих і децентралізованих автоматизованих інформаційних систем [4].

За ступенем охоплення управлінських завдань розрізняють інформаційні технології електронної обробки даних, автоматизації управління, підтримки прийняття рішень, електронного офісу та експертної підтримки [2].

Технології аналізу даних

Сховище даних (Data Warehouse) – це предметно-орієнтоване, прив'язане до часу і незмінне зібрання корпоративних даних для підтримування процесу прийняття управлінських рішень [2; 9]. Дані у сховище надходять з систем оперативного обліку підприємства, а також із зовнішніх джерел, (наприклад, зі статистичних звітів). Головним призначенням сховища є надання інформації для аналізу в одному місці та в інтуїтивно зрозумілій структурі.

Під сховищем не обов'язково розуміти велике скупчення даних. Для маленьких сховищ призначений окремий термін – **Data Marts (вітрини даних)**. Вітрина даних може являти собою спеціалізоване сховище, яке обслуговує один з напрямів діяльності компанії (наприклад, облік персоналу або маркетинг).

Сховища даних є джерелом інформації для засобів оперативного аналітичного оброблення даних OLAP (OnLine Analytical Processing).

OLAP-технології – це сукупність засобів багатовимірного аналізу даних, накопичених у сховищі даних. Користувачу OLAP надається інтуїтивно зрозуміла модель даних, організована у вигляді багатовимірних кубів (Cubes). Осями – *вимірами* (Dimensions) багатовимірної системи координат слугують основні атрибути аналізованого бізнес-процесу (наприклад, для процесу продажу – товар, регіон, тип покупця). На перетинах вимірів знаходяться дані, що кількісно характеризують процес, – *міри* (Measures) (наприклад, обсяги продажу, витрати). Значення, що відкладаються на осях кубу, називаються *членами виміру* (members). Члени виміру можуть утворювати ієрархії, що складаються з декількох рівнів. Наприклад, для виміру «Час» ієрархією може бути «Рік місяці тижні дні».

1.3. Нейромережні технології

Комп'ютерні технології, які отримали назву **нейромережних**, працюють за аналогією з принципами будови і функції нейронів головного мозку людини і дозволяють вирішувати широкий круг завдань: розпізнання мови людини і абстрактних образів, класифікація станів складних систем, управління технологічними процесами і фінансовими потоками, вирішення аналітичних дослідницьких, прогнозних завдань, зв'язаних великими інформаційними потоками [1; 2].

Нейромережні технології істотно полегшують процес ухвалення управлінських рішень у ситуаціях невизначеності, дефіциту часу та обмеженості інформації, що робить їх перспективним інструментом для систем підтримки прийняття рішень у різних галузях, зокрема у сфері цивільної безпеки [3].

Нейромережна технологія характеризується двома ключовими властивостями: здатністю до навчання на конкретних прикладах і вмінням стабільно розпізнавати та прогнозувати нові ситуації з високим рівнем точності, навіть за наявності неповних або суперечливих даних [2; 4].

1.4. Технологія автоматизованих робочих місць

Під автоматизованим робочим місцем розуміють професійно орієнтований програмно-апаратний комплекс, призначений для забезпечення ефективного виконання функціональних обов'язків користувача безпосередньо на його робочому місці із застосуванням сучасних інформаційних технологій [4].

Автоматизовані робочі місця забезпечують збір, організацію, обробку, зберігання та передачу інформації, залишаючи за фахівцем функції управління, контролю та ухвалення рішень. Користувач при цьому виступає як кінцевий користувач АРМу, що підвищує оперативність і якість управлінської діяльності [1].

АРМи застосовуються для вищих керівників і менеджерів різних рівнів управління, фахівців економічного, інженерного та технологічного профілю, а також для технічних

виконавців. Зокрема, АРМ інженера з охорони праці використовується для розроблення інструкцій з безпеки, контролю виконання вимог охорони праці, організації навчання персоналу та оформлення дозвільної документації.

1.5. Гіпертекстова технологія. Технологія мультимедіа

Звичайний текст виглядає як один довгий рядок символів, який читається в одному напрямі.

Під **гіпертекстом (Hypertext)** розуміють систему інформаційних об'єктів (статей, документів, сторінок), об'єднаних між собою направленими зв'язками (гіперпосиланнями), які утворюють мережу. Гіпертекст є формою організації інформації у вигляді системи взаємопов’язаних інформаційних об’єктів, об’єднаних гіперпосиланнями, що дозволяє користувачеві здійснювати нелінійну навігацію між фрагментами інформації [6]. Такий підхід забезпечує відкритість структури документа та можливість її постійного розширення без порушення логічної цілісності матеріалу.

Гіпертекстові технології знайшли широке застосування у побудові вебресурсів, електронних довідників, систем дистанційного навчання, електронних бібліотек і пошукових систем [1].

Мультимедіа є інтерактивною технологією, що поєднує роботу з текстом, графікою, звуком, відео, анімацією та тривимірною графікою, забезпечуючи високий рівень наочності й сприйняття інформації [2]. Мультимедійні технології широко застосовуються в освіті, професійній підготовці, комп’ютерному тренінгу, бізнесі та дистанційному навчанні, зокрема у створенні навчальних симуляторів і віртуальних тренажерів.

Поєднання гіпертекстових і мультимедійних технологій призвело до формування гіпермедіа, що забезпечує інтеграцію різних типів даних у єдиному інформаційному середовищі з використанням системи посилань [6].

1.6. Мережні технології. Технології Internet

Обчислювальна мережа визначається як територіально розподілена обчислювальна система, що складається з взаємодіючих електронно-обчислювальних машин і терміналів (вузлів мережі), поєднаних між собою каналами передачі даних з метою колективного використання апаратних, програмних та інформаційних ресурсів [1; 5].

За рангом обчислювальні мережі поділяють на локальні та глобальні. Локальні обчислювальні мережі (Local Area Network, LAN) забезпечують з’єднання терміналів із комп’ютерами або комп’ютерів між собою в межах обмеженої території (підприємство, установа, навчальний заклад). Глобальні обчислювальні мережі (Wide Area Network, WAN) реалізують міжмережну взаємодію, поєднуючи комп’ютери та локальні мережі, розташовані на значних відстанях [5; 6].

У розвитку обчислювальних мереж виділяють три покоління. Перше покоління мереж забезпечувало підключення терміналів до центральних обчислювальних машин. Друге покоління орієнтувалося на безпосереднє з’єднання комп’ютерів між собою. Третє покоління мереж характеризується інтеграцією мереж у глобальні обчислювальні системи, де відбувається з’єднання мереж між собою. Найбільш відомим і масштабним прикладом мережі третього покоління є Internet, який став основою глобального інформаційного простору [6].

Internet – це глобальна комп’ютерна мережа третього покоління, тобто мережа мереж.

Підключення до Internet виконується згідно зі схемою на рис. 1.1.

Рис. 1.1. **Схема підключення до Internet**

Усі електронно-обчислювальні машини, об'єднані в мережу, поділяються на основні та допоміжні. Основними є абонентські ЕОМ, або клієнти (робочі станції), які виконують інформаційно-обчислювальні операції та визначають функціональні можливості мережі. Допоміжні ЕОМ – сервери – призначені для зберігання, обробки, маршрутизації та передачі інформації між вузлами мережі. До серверів висуваються підвищені вимоги щодо продуктивності, надійності та безперервності роботи [1; 4].

Для підключення комп'ютерів і каналів зв'язку використовуються спеціальні апаратні засоби: мережні адаптери, мережні плати, маршрутизатори, модеми тощо. Їх призначення полягає у перетворенні цифрової інформації, що надходить від комп'ютера, в електричні, радіо- або оптичні сигнали для передавання каналами зв'язку і у виконанні зворотного перетворення [5].

Модем (модулятор-демодулятор) забезпечує перетворення цифрових сигналів комп'ютера (двійкового коду) в аналогові сигнали, придатні для передачі телефонними лініями, а також виконує зворотну функцію – перетворення аналогових сигналів у цифрові, зрозумілі електронно-обчислювальній машині. Використання таких пристроїв стало передумовою розвитку віддаленого доступу до мережі Internet та формування сучасних мережних сервісів [6].

Користувач повинен зв'язати свій локальний пристрій з регіональним провайдером (**провайдер** – організація, що надає послуги доступу до комп'ютерної мережі). Багато користувачів, що підключаються до Internet з установи, використовують для цього локальну мережу свого підприємства, що безпосередньо підключена до сервера регіонального провайдеру Internet. Такий механізм взаємодії з Internet можна охарактеризувати як класичний варіант системи «клієнт-сервер».

Завдання узгодження взаємодії ЕОМ клієнтів, серверів, ліній зв'язку й інших пристроїв вирішується шляхом установлення певних правил, які називають **протоколами**.

Для Internet створені такі протоколи:

1. **IP** (Internet Protocol) – це протокол нижнього рівня, що служить для встановлення зв'язку між ЕОМ. Спеціальні ЕОМ – вузли мережі – використовують IP для передачі інформації з Internet: для кожного пакета інформації зазначена IP-адреса ЕОМ, завдяки якому інформація потрапляє за призначенням.

IP-адреса – це унікальне ім'я, під яким ЕОМ відома всім іншим ЕОМ в Internet.

Наприклад, IP-адреса може мати такий вигляд: *10.192.113.6*

2. **TCP** (Transmission Control Protocol) – протокол управління передачею. Це протокол, що забезпечує надійне з'єднання між двома додатками, що працюють у мережі. TCP визначає, яким чином інформація розділяється на пакети і відсилається по Internet. Він контролює передачу даних і стежить за тим, щоб вони досягали свого місця призначення. Таким чином, TCP/IP виконує роль мосту між різними мережами та системами в мережах Internet, що розуміють всі ЕОМ і мережі незалежно від того, яку мову вони використовують для внутрішніх цілей.

3. **ftp** (file transfer protocol) – протокол передачі файлів.
4. **HTTP** (Hipertext Transfer Protocol) – протокол передачі гіпертексту.

Адреси в Internet можуть бути представлені як послідовністю цифр, так і ім'ям, побудованим за певними правилами. В Internet використовується **доменна система імен** (Domain Name System або **DNS**), що є системою ієрархічних імен і імен серверів. Кожний рівень у такій системі називається доменом. Домени відділяються один від одного крапкою, наприклад: *home.manager.company.ua*

Домен верхнього (першого) рівня *ua* вказує на те, що мова йде про українську частину Internet. Наступний рівень визначає організацію в Україні, який належить дана адреса: *company*. Всі ЕОМ, підключені до Internet у цій фірмі, поєднуються в групу, що має таку адресу. Підрозділу менеджерів у компанії виділений свій домен з ім'ям *manager***.** Одній з ЕОМ у даному підрозділі привласнено ім'я *home***.** В імені може бути будьяке число доменів, але найчастіше використовується від трьох до п'яти. Символьні імена використовуються в Internet тільки для зручності користувачів. ЕОМ, підключені до мережі, використовують цифрові імена (32-бітові адреси). Числа розділяються крапками, наприклад: *197.165.1.15*. Початок адреси визначає частину Internet, до якого підключена ЕОМ, а закінчення – адресу ЕОМ у цій частині мережі [2; 5].

Домени першого рівня можуть бути географічними: ua – Україна; ru – Росія; fr – Франція; ge – Німеччина; jp – Японія; uk – Великобританія та ін.

Але вони можуть позначати не тільки регіон, але й тип організації, якій цей сайт належить: gov – позначає урядовий заклад; com – будь-яку комерційну організацію; net – організацію, що має відношення до мережних послуг; mil – військову установу; int – міжнародну установу; edu – освітню установу.

Працюючи з мережею Internet, користувач зіштовхується з різними *сервісами*, які надає Internet. Для того, щоб скористатися деякими з них, цілком достатньо вбудованого в Windows набору програм – браузера Internet Explorer, програми для роботи з електронною поштою і групами новин Outlook Express, клієнта голосового зв'язку NetMeeting. А для деяких необхідно встановлювати додаткові програми. *Найпопулярнішими сервісами (їх ще називають службами) Internet* є такі:

WWW (World Wide Web) – робота з гіпертекстом і мультімедіа;

E-mail – електронна пошта;

ICQ – обмін короткими повідомленнями; **newsgroups** – групи новин;

ftp – передача файлів від одного комп'ютера до іншого.

Розглянемо докладніше найпопулярніший сервіс – систему гіпертекстових сторінок **World Wide Web** (дослівний переклад – всесвітня павутина).

WWW представляє із себе величезний гіпертекстовий документ. Точніше, безліч маленьких документів-сторінок, зв'язаних між собою спеціальними посиланнями (*гіперпосиланнями*).

Сторінка – це найменша одиниця інформаційного ресурсу всесвітньої павутини. На ній можуть бути розміщені текст, зображення, аудіо, відео, Java-аплети (програми, що виводять на екран картинки, що рухаються), посилання на інші сторінки та ін. Посилання зазвичай розташовуються у звичайних текстових рядках і словах (найчастіше підкреслених або виділених кольором) або в картинках, що розміщені на сторінці. Вибір посилання дозволяє перейти на наступну сторінку.

Програма, що використовується для перегляду web-сторінок називається **браузер** (browser). Найбільш популярними серед користувачів браузерами є Internet Explorer, Netscape Navigator, Opera, Mozilla.

Сайт – це група сторінок, що належать одній фірмі, організації або приватній особі і зв'язані між собою за змістом.

WWW-сервером називається підключений до мережі комп'ютер, на якому встановлено серверне програмне забезпечення та зберігаються сайти і сторінки. На одному WWW-сервері може бути один сайт (особливо якщо це дуже великий сайт). А може бути і

багато, наприклад, якщо ми маємо справу із сервером провайдеру (постачальника послуг Internet), що зберігає на своєму комп'ютері сотні й навіть тисячі маленьких «домашніх сторінок».

Інтернет-портали – групи сайтів з необхідними користувачу послугами, доступ до яких можна одержати з єдиної для всіх них титульної сторінки. Звичайно в межах одного порталу можна одержати доступ до: пошукової системи; стрічки новин, розбитої за категоріями, що відповідає специфіці порталу; каталогу сторінок Internet; електронного магазину або аукціону.

При роботі в Internet використовуються не просто доменні адреси, а **універсальні покажчики ресурсів (URL – Universal Resource Locator**).

URL – це адреса будь-якого ресурсу в Internet разом із вказівкою того, за допомогою якого протоколу треба до нього звертатися, яку програму для цього варто запустити на сервері та до якого конкретного файлу варто звернутися на сервері.

Стандартний URL складається із трьох частин: формат передачі, ім'я вузла, що містить необхідний файл, і шлях до цього файлу.

Основний формат URL: *protocol://host.name.com/path/filename.html*

Наприклад: *http://www.dataforce.net/index.htm*

Остання частина назви, що розташована після скісної риски («слеша»), указує на конкретну сторінку на вказаному сайті. Остання група букв, після крапки, – розширення файлу, що вказує на його тип – гіпертекстовий документ Internet.

1.7. Технологія електронної пошти

Технологія електронної пошти – це технологія комп'ютерного способу пересилки і обробки інформаційних повідомлень, що забезпечує оперативний зв'язок між різними користувачами.

Електронна пошта (e-mail) – спеціальний пакет програм для зберігання і пересилки повідомлень між користувачами ЕОМ. Цей пакет програм виконує такі функції, як редагування документів перед передачею, їх зберігання в спеціальному банку; пересилка кореспонденції; перевірка і виправлення помилок, що виникають при передачі; видача підтвердження про отримання кореспонденції адресатом; отримання і зберігання інформації в своїй «поштовій скриньці»; перегляд отриманої кореспонденції. Якщо раніше застосовувалися самостійні пакети електронної пошти, то зараз спостерігається тенденція включення її в інтегровані пакети.

Поштове повідомлення має таку структуру: заголовок (адресат, тема, дата відправки і ін.); тіло повідомлення (текст); електронний підпис.

При цьому заголовок включає адресу одержувача листа; зворотну адреса; тему листа; дату і час відправки листа; адресатів, які отримають копію листа; список файлів, що посилаються разом з листом.

Адреси e-mail складаються з двох частин, розділених символом @:

справа – адреса ЕОМ, на якій розташовується поштове відділення клієнта у вигляді доменного імені в мережі, зліва – ім'я абонента.

Технологія Intranet

Мережу, що працює в рамках окремої організації побудовану за принципами та на програмному забезпеченні Internet, називають **Intranet (Інтранет)** або **корпоративна мережа**.

Intranet-технологія виникла головним чином через те, що технологія «клієнт-сервер» не завжди відповідала вимогам щодо швидкості передавання даних, які висувались у реальних інформаційних системах.

Технологія Intranet розуміє під собою створення локальної інформаційної системи клієнт-серверної архітектури з урахуванням суворих обмежень (протоколів обміну даними – HTTP і FTP та основної форми подання інформації – HTML (XML)). Intranet забезпечує високу пропускну здатність каналів зв'язку (до 1000 Mbps) між клієнтом і сервером і використання як стандартних серверів і клієнтів (HTTP-сервер і браузер), так і стандартних

механізмів розширення можливостей системи, наприклад CGI. *HTTP-сервер* призначений для виконання таких функцій: прийом запиту від клієнта; можливий запуск CGI-прикладної програми; повернення файла, що вимагається у запиті (результату виконання CGI-прикладної програми), або повідомлення про помилку клієнту.

Системи Intranet приблизно у 2,5 рази дешевші за спеціалізовані клієнт-серверні прикладні програми.

Останнім часом технологія Intranet все частіше слугує середовищем та інструментом для побудови систем автоматизації підприємства. Сполучення централізованого зберігання інформації і розподілених комунікацій надає зручні можливості для створення корпоративних інформаційних систем. Прикладом системи, побудованої на базі Intranet, є система управління ресурсами підприємства Oracle Applications корпорації Oracle.

Суть розподілених технологій обробки і зберігання даних

Однією з найважливіших мережних технологій є *розподілена обробка даних*, коли ПК встановлені на робочих місцях – в місцях виникнення і використання інформації – і сполучені каналами зв'язку.

Це дає можливість розподілити їх ресурси за окремими функціональними сферами діяльності і змінити технологію обробки даних у напрямі децентралізації. Розподілена обробка даних дозволила підвищити ефективність задоволення інформаційних потреб працівника, і тим самим забезпечити гнучкість і оперативність ухвалюваних ним рішень. Перевагами розподіленої обробки даних є: велике число користувачів, що взаємодіють між собою, виконують функції збору, реєстрації, зберігання, передачі і видачі інформації; зняття пікових навантажень з централізованої бази даних (БД) шляхом розподілу, обробки і зберігання локальних БД на різних ЕОМ; забезпечення доступу працівника до обчислювальних ресурсів мережі ЕОМ; забезпечення обміну даними між віддаленими користувачами.

У розподілених системах використовуються три інтегровані технології: технологія «клієнт-сервер»; технологія універсального призначеного для користувача спілкування у вигляді електронної пошти; технологія сумісного використання ресурсів у рамках глобальних мереж.

Сьогодні межі між централізованою і розподіленою архітектурою починають розмиватися, оскільки багато компаній вважають за краще зберігати дані на невеликих серверах, але самі сервери розміщують на одній центральній обчислювальній установці. Якщо обробка даних виконується в різних місцях, то можна говорити про розподілену архітектуру; якщо в переважній більшості дані обробляються в єдиному місці, то архітектура – централізована [2; 5].

Технології «Файл-сервер» і «Клієнт-сервер»

У залежності від конфігурації використовуваних технічних і програмних засобів застосовуються різні концепції мережної обробки даних – **«Файл-сервер»** і **«Клієнт-сервер»**.

Клієнт – це однокористувальницька робоча станція, яка виконує функції взаємодії з користувачем, здатна здійснити необхідні обчислення і забезпечує приєднання до віддалених обчислювальних ресурсів з базами даних, до засобів їх оброблення і засобів організації інтерфейсів.

Сервер – одно- чи багатопроцесорний комп'ютер з розділюваними пам'яттю, обробленням даних, комунікаційними засобами та засобами управління периферійним обладнанням.

Концепція **«Файл-сервер»** припускає наявність комп'ютера, виділеного під файловий сервер, у якому знаходиться ядро мережної ОС і централізовано збережені файли. Для цієї архітектури характерний колективний доступ до загальної бази даних на файловому сервері. Від конкретного АРМа на сервер надходить запит, обробка якого приведе до передачі по мережі на дане АРМ всієї інформації запитаного файлу. Вибір же записів, що задовольняють умови запиту, буде здійснений на самому АРМі засобами СУБД.

Це призводить до того, що в момент передачі по мережі інформації файлу доступ до нього інших АРМів блокується.

Одночасний доступ багатьох користувачів до інтегрованої БД реалізується в концепції **«Клієнт-сервер»**. У даній концепції серверу надається більш активна роль. Запит на обробку даних посилається клієнтом (АРМом) по мережі на сервер баз даних. На сервері здійснюється пошук даних і їх обробка засобами СУБД, установленої на сервері. Оброблені дані передаються по мережі від сервера до клієнта (на АРМ). Специфікою архітектури **«Клієнт-сервер»** є використання мови структурованих запитів SQL (Structured Queries Language) для запитів до БД, що забезпечує роботу з загальними даними з різнотипних додатків у мережі [2; 5].

Концепція «Клієнт-сервер» може бути реалізована за дворівневою і багаторівневою архітектурою. При *дворівневій архітектурі* всі робочі станції посилають запити до сервера БД, на якому здійснюється вибірка даних і їхня попередня обробка. Одиницею обміну по мережі є запит і відповідь на запит. При *багаторівневій архітектурі* на робочій станції встановлено тільки програмне забезпечення, що підтримує інтерфейс користувача. Додатково виділений сервер додатків, на якому знаходиться програмне забезпечення загального користування, що виконує всю змістовну обробку інформації.

Сучасні інформаційні системи для організацій і підприємств здебільшого мають клієнт-серверну архітектуру.

1.8. Інформаційних технології у цивільній безпеці

Інформаційні технології є ключовим інструментом реалізації державної політики у сфері цивільної безпеки, оскільки забезпечують своєчасне отримання, оброблення, збереження та передавання інформації про загрози, надзвичайні ситуації та стан захищеності населення і територій. У сучасних умовах цифровізації управління інформаційні технології формують основу функціонування автоматизованих систем цивільного захисту, підвищуючи оперативність і обґрунтованість управлінських рішень [7; 8].

Однією з базових функцій інформаційних технологій у цивільній безпеці є інформаційно-аналітична функція. Вона полягає у зборі даних з різнорідних джерел (сенсорні системи, об’єктові та локальні автоматизовані системи, інформація від чергових служб), їх структуризації, обробленні та аналізі для оцінювання ризиків і прогнозування розвитку надзвичайних ситуацій. Автоматизовані інформаційні системи дозволяють інтегрувати просторові, часові та статистичні дані, формуючи єдине інформаційне поле управління цивільним захистом [1; 7].

Важливою є функція моніторингу та раннього виявлення загроз, яка реалізується через автоматизовані системи контролю параметрів небезпечних процесів і об’єктів. Згідно з вимогами ДБН В.2.5-76:2014, інформаційні технології забезпечують безперервний контроль за станом потенційно небезпечних об’єктів, інженерних споруд, природних середовищ та інфраструктури, що дозволяє виявляти загрозу виникнення надзвичайної ситуації на ранніх етапах [10]. Така функція є критичною для зменшення людських і матеріальних втрат.

Центральне місце в системі цивільної безпеки займає функція оповіщення населення та органів управління. Інформаційні технології забезпечують функціонування загальнодержавної автоматизованої системи централізованого оповіщення, яка призначена для доведення сигналів і повідомлень про загрозу або виникнення надзвичайних ситуацій у найкоротші терміни [8; 11]. Сучасні ІТ-рішення дозволяють використовувати багатоканальні способи оповіщення (сирени, телекомунікаційні мережі, мобільні додатки, цифрові платформи), що підвищує охоплення населення та надійність передачі інформації [12].

Не менш важливою є управлінська функція інформаційних технологій, яка полягає у підтримці процесів прийняття рішень. Інформаційні системи ДСНС та інших органів

управління цивільним захистом забезпечують керівників актуальною інформацією про обстановку, ресурси, сили і засоби реагування, а також варіанти дій у різних сценаріях розвитку подій [13]. Це сприяє реалізації принципів ситуаційного управління та координації дій між різними рівнями управління.

Інформаційні технології виконують також координаційно-комунікаційну функцію, забезпечуючи обмін інформацією між органами виконавчої влади, місцевого самоврядування, аварійно-рятувальними службами та іншими суб'єктами системи цивільного захисту. Єдині інформаційні платформи та автоматизовані канали зв'язку зменшують часові затримки та ризик втрати критично важливих даних під час ліквідації надзвичайних ситуацій [8; 13].

Окреме значення має навчально-тренувальна функція інформаційних технологій. Цифрові навчальні платформи, інформаційно-довідкові системи та моделювання сценаріїв надзвичайних ситуацій використовуються для підготовки фахівців цивільної безпеки, підвищення кваліфікації персоналу та інформування населення щодо правил поведінки у разі загрози або виникнення надзвичайних ситуацій [1; 14].

Інформаційні технології у цивільній безпеці виконують комплекс взаємопов'язаних функцій – від моніторингу та оповіщення до аналітичної підтримки управління і навчання. Їх системне впровадження є необхідною умовою підвищення стійкості держави та суспільства до надзвичайних ситуацій природного, техногенного і воєнного характеру.

Питання для контролю знань

1. Розкрийте сутність поняття «інформаційна технологія».
2. Дайте характеристику інформаційних технологій в умовах централізованої та децентралізованої обробки даних.
3. Наведіть приклади предметної, забезпечуючої, функціональної інформаційної технології.
4. Дайте характеристику інформаційних технологій робочого столу.
5. Визначте гіпертекстову та мультимедійну технології.
6. Наведіть характеристику основних мережних ІТ.
7. Дайте визначення розподілених технологій обробки і зберігання даних.
8. Що таке мобільні технології?
9. Дайте визначення електронної комерції.
10. Дайте визначення технології «клієнт-сервер».
11. Наведіть приклади сервісів Інтернет.
12. Охарактеризуйте етапи розвитку інформаційних технологій.
13. Які основні функції виконують інформаційні технології у системі цивільної безпеки держави?
14. Як інформаційні технології забезпечують моніторинг, прогнозування та оцінку ризиків надзвичайних ситуацій?
15. Яку роль відіграють автоматизовані інформаційні системи в управлінні силами та засобами цивільного захисту?
16. Як інформаційні технології використовуються для оповіщення населення про загрозу або виникнення надзвичайних ситуацій?
17. У чому полягає значення інформаційних технологій для підтримки прийняття управлінських рішень у сфері цивільної безпеки?
18. Які функції інформаційні технології виконують під час ліквідації наслідків надзвичайних ситуацій та відновлювальних робіт?
19. Яким чином інформаційні технології сприяють підвищенню рівня підготовки фахівців і населення у сфері цивільної безпеки?

Список використаних джерел

1. Виганяйло С. М. Інформаційне забезпечення професійної діяльності : навч. Посіб. Харків : ХНУВС, 2021. 108 с.
2. Інформаційні технології: навчальний посібник / О. І. Зачек, В. В. Сеник, Т. В. Магеровська та ін.; за ред. О. І. Зачека. - Львів: Львівський державний університет внутрішніх справ, 2022. - 432 с.
3. Інформаційні системи та технології : навчально-методичний посібник для здобувачів вищої освіти галузі знань 07-Управління та адміністрування спеціальності 073-Менеджмент / Уклад. Р.І. Чанишев. - Одеса: НУ «ОЮА», 2022. - 151 с.
4. ДСТУ ISO/IEC 2382:2017 Інформаційні технології. Словник термінів. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=75076
5. Комп'ютерні мережі : навч.-метод. посібник [Електронне видання] / О. В. Задерейко, Н. В. Багнюк, А. А.Толокнов. – Одеса : Фенікс, 2023. – 211 с. – Режим доступу: https://doi.org/10.32837/11300.25951
6. Комп'ютерні мережі. Книга 1. Технології комп'ютерних мереж [Електронний ресурс] : навч. посібник / Євсеєв С. П., Дженюк Н. В., Толкачов М. Ю. [та ін.]. – Електрон. текст. дані. – Харків – Львів : "Новий Світ – 2000", 2023. – 471 с. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/93100.
7. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=61937.
8. Кодекс цивільного захисту України. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text.
9. Kimball R., Ross M. The Data Warehouse Toolkit. 3rd ed. Wiley, https://darinadata.ir/wp-content/uploads/2025/02/Wiley_The_Data_Warehouse_Toolkit_The_Definitive_Guide_to_Dimensional.pdf.
10. ДБН В.2.5-76:2014. Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення. Київ : Мінрегіон України, 2014.
11. Деякі питання функціонування загальнодержавної автоматизованої системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій : постанова Кабінету Міністрів України від 29 берез. 2024 р. № 355. URL: https://zakon.rada.gov.ua/laws/show/355-2024-%D0%BF#Text.
12. Білоусов С. І. Об'єктові, локальні та спеціальні автоматизовані системи оповіщення цивільного захисту : навч. посіб. Одеса : ОНАЗ ім. О. С. Попова, 2013. 44 с.
13. Державна служба України з надзвичайних ситуацій. Офіційний сайт. URL: https://dsns.gov.ua/.

Тема 2. Інформаційні системи моніторингу загроз природного та техногенного характеру

1. Метеорологічні інформаційні системи моніторингу.
2. Гідрологічні інформаційні системи моніторингу.
3. Інформаційні системи радіаційного моніторингу
4. Інформаційні системи хімічного моніторинг.

2.1. Метеорологічні інформаційні системи моніторингу

У сучасних умовах цивільний захист населення значною мірою базується на своєчасному отриманні, обробці та передачі даних про стан довкілля, зокрема про атмосферні умови. Метеорологічні інформаційні системи моніторингу виступають

ключовим елементом у комплексі автоматизованих систем цивільного захисту, що дозволяють виявляти небезпечні синоптичні явища, прогнозувати їх розвиток та забезпечувати ефективне оповіщення населення про можливі метеорологічні надзвичайні ситуації (НС) [6].

Згідно з ДСТУ 2226-93, автоматизована система – це сукупність взаємопов'язаних технічних засобів, що забезпечують збір, оброблення, зберігання та передачу інформації з мінімальною участю людини із заданою точністю та швидкістю[6]. У контексті метеорологічного моніторингу такі системи інтегрують дані з метеостанцій, радарів, супутникових джерел та моделей прогнозу погоди для оперативного реагування на зміну погоди.

Основними завданнями метеорологічних систем моніторингу є: збір даних про атмосферні показники (температура, тиск, вологість, вітер, опади); визначення тенденцій змін погоди; формування прогнозів і попереджень щодо потенційних небезпек; передача інформації до систем цивільного захисту та органів управління надзвичайними ситуаціями.

В Україні метеорологічний моніторинг здійснюється за допомогою мережі наземних метеорологічних станцій, які збирають дані з території всієї країни, та інтеграції цих даних в Український гідрометеорологічний центр для їхньої обробки й прогнозування подальшої синоптичної ситуації [6].

Метеорологічні НС належать до природних надзвичайних ситуацій та охоплюють явища, пов'язані з атмосферними процесами, що створюють загрозу життю людей, об'єктам інфраструктури, довкіллю та економіці. Такі явища включають сильні зливи, град, буревії, смерчі, пилові бурі, сильні тумани, ожеледь, хуртовини, сильні морози та аномальну спеку[6].

Реальні приклади метеорологічних НС в Україні підтверджують актуальність створення та використання інформаційних систем моніторингу. У 2020 році на заході України відбулися сильні повені, спричинені інтенсивними тропічними зливами, що призвели до виходу річок з берегів, значних матеріальних збитків та жертв, і стали однією з наймасштабніших повеней за останні десятиліття[turn0search27]. Також у 2025 році в Одеській області сильні дощі спричинили масштабні повені, унаслідок яких були загиблі, евакуація мешканців і повністю перевантажені системи водовідведення та транспортні шляхи.

Окрім масштабних подій повеней, щорічно в Україні фіксують до 150 випадків стихійних метеорологічних явищ, серед яких сильні дощі, снігопади, ожеледі, тумани, пилові бурі та інші локальні НС, що потребують своєчасного оповіщення та реагування з боку органів цивільного захисту[1].

Важливість метеорологічних інформаційних систем полягає також у здатності передбачати такі явища на ранніх стадіях їх розвитку. Наприклад, сучасні автоматизовані системи моніторингу здатні виявляти формування шквалів та небезпечних опадів, що дозволяє фахівцям прогнозувати небезпеку та ініціювати попередження для населення чи зміну роботи інфраструктурних об'єктів у режимі реального часу.

В Україні законодавче питання функціонування загальнодержавної автоматизованої системи оповіщення врегульовано відповідно до Постанови Кабінету Міністрів України № 355 від 29 березня 2024 року «Деякі питання функціонування загальнодержавної автоматизованої системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій», яка передбачає організаційно-технічні засоби для передачі сигналів оповіщення у разі виникнення НС, у тому числі метеорологічних, з використанням усіх наявних каналів зв'язку та мереж звукового сигналу[2].

Одним з ключових елементів цивільного захисту є **система оповіщення населення**, яка розробляється й експлуатується Державної служби України з надзвичайних ситуацій (ДСНС). Ця система передбачає застосування технічних засобів для оперативної передачі сигналів та повідомлень про небезпеку, що дозволяє забезпечити інформаційне покриття

великих територій та своєчасно інформувати населення про виникнення метеорологічної НС[1; 5].

Важливим нормативно-технічним документом у сфері побудови таких систем є ДБН В.2.5-76:2014 «Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення», що визначає вимоги до побудови технічної архітектури, надійності передачі та інтеграції даних для забезпечення своєчасного реагування на надзвичайні події різного характеру, включно з метеорологічними[7].

Ефективність метеорологічних інформаційних систем моніторингу та оповіщення безпосередньо впливає на здатність суспільства своєчасно реагувати на погодні загрози та зменшувати наслідки НС для населення, інфраструктури та економіки країни. Забезпечення якісного функціонування таких систем – це не лише технічне завдання, а й важлива складова комплексної системи цивільного захисту в Україні, що має відповідати вимогам сучасних кліматичних викликів.

2.2. Гідрологічні інформаційні системи моніторингу

У системі цивільної безпеки важливе місце посідає моніторинг гідрологічних процесів, оскільки вода є одним із найбільш небезпечних природних чинників, здатних спричиняти масштабні надзвичайні ситуації. Повені, паводки, підтоплення, руйнування гідротехнічних споруд і дефіцит водних ресурсів становлять реальну загрозу для населення, інфраструктури та довкілля. У зв’язку з цим гідрологічні інформаційні системи моніторингу є ключовим інструментом прогнозування, попередження та мінімізації наслідків гідрологічних надзвичайних ситуацій [8].

Гідрологічні інформаційні системи моніторингу являють собою сукупність технічних, програмних та організаційних засобів, призначених для збору, оброблення, зберігання й аналізу даних про стан поверхневих і підземних водних об’єктів. Відповідно до положень ДСТУ 2226-93, такі системи належать до автоматизованих інформаційних систем, що функціонують із мінімальною участю людини та забезпечують оперативне отримання достовірної інформації для прийняття управлінських рішень у сфері цивільного захисту [4].

Основними об’єктами гідрологічного моніторингу є річки, озера, водосховища, канали, прибережні морські зони, а також підземні води. У процесі моніторингу фіксуються рівень і витрати води, швидкість течії, температура, льодові явища, мутність, хімічний склад води та інші показники, що можуть свідчити про загрозу виникнення надзвичайної ситуації [1].

В Україні гідрологічний моніторинг здійснюється в межах державної системи спостережень за довкіллям і координується спеціалізованими підрозділами, зокрема Українським гідрометеорологічним центром та Державною службою України з надзвичайних ситуацій. Отримані дані інтегруються в системи управління надзвичайними ситуаціями, що дозволяє прогнозувати розвиток паводкових процесів і своєчасно вживати заходів захисту населення [7].

Особливе значення гідрологічні інформаційні системи мають для прогнозування паводків і повеней. Сучасні системи поєднують дані наземних гідропостів, автоматизованих датчиків рівня води, супутникових спостережень та математичних моделей, що дає змогу оцінювати ризики підтоплення населених пунктів і об’єктів критичної інфраструктури. Такий підхід відповідає вимогам ДБН В.2.5-76:2014 щодо раннього виявлення загрози виникнення надзвичайних ситуацій [5].

Реальні гідрологічні надзвичайні ситуації в Україні підтверджують необхідність розвитку гідрологічних систем моніторингу. Значні паводки в басейнах річок Дністер, Прут і Тиса неодноразово призводили до підтоплення житлових будинків, руйнування доріг і мостів, евакуації населення та значних економічних збитків. Саме завдяки даним гідрологічного моніторингу можливе завчасне оповіщення населення та організація захисних заходів [2; 9].

Гідрологічні інформаційні системи тісно пов’язані із системами оповіщення населення. Згідно з Кодексом цивільного захисту України, інформація про загрозу або виникнення надзвичайної ситуації має оперативно доводитися до органів управління та населення із використанням централізованих і локальних систем оповіщення [8]. Дані гідрологічного моніторингу є підставою для формування попереджень і рішень щодо введення режимів підвищеної готовності або надзвичайної ситуації.

Сучасний розвиток цифрових технологій сприяє інтеграції гідрологічних інформаційних систем із геоінформаційними системами, мобільними додатками та онлайн-платформами, що підвищує доступність інформації та ефективність реагування.

2.3. Інформаційні системи радіаційного моніторингу

Радіаційна безпека є складовою національної безпеки та цивільного захисту населення, особливо в умовах наявності на території України ядерних енергетичних об’єктів, підприємств з використанням джерел іонізуючого випромінювання, а також з огляду на воєнні загрози та ризики техногенних аварій. Інформаційні системи радіаційного моніторингу забезпечують своєчасне виявлення змін радіаційного фону, прогнозування розвитку небезпечних ситуацій та підтримку управлінських рішень у сфері цивільного захисту [8].

Радіаційний моніторинг розглядається як цілеспрямована система спостережень, збору, обробки, збереження та аналізу даних про рівні іонізуючого випромінювання в навколишньому середовищі з метою оцінювання ризиків для населення і довкілля. Відповідно до міжнародних підходів, сформованих МАГАТЕ та ВООЗ, такі системи повинні бути безперервними, достовірними та інтегрованими з іншими підсистемами екологічного і техногенного моніторингу [11].

В Україні функціонування інформаційних систем радіаційного моніторингу регламентується Кодексом цивільного захисту України, законами у сфері використання ядерної енергії та радіаційної безпеки, а також підзаконними нормативними актами. Ключову роль у цій сфері відіграють Державна служба України з надзвичайних ситуацій, Державна інспекція ядерного регулювання України та гідрометеорологічна служба, які забезпечують спостереження за радіаційною обстановкою та інформування органів влади і населення [8; 12].

Структурно інформаційні системи радіаційного моніторингу включають мережу автоматизованих пунктів контролю, засоби вимірювання потужності дози гамма-випромінювання, системи передачі даних, серверні комплекси обробки інформації та програмні засоби візуалізації. Автоматизовані пости дозволяють у режимі реального часу фіксувати зміну радіаційного фону і передавати дані до центрів управління, що суттєво підвищує оперативність реагування на надзвичайні ситуації [4].

Особливе значення мають автоматизовані системи радіаційного контролю в зоні розміщення атомних електростанцій. Вони забезпечують постійне спостереження за радіаційною ситуацією в санітарно-захисних зонах і зонах спостереження, що дає змогу своєчасно виявляти відхилення від нормативних значень та запобігати негативним наслідкам для населення [11].

В умовах воєнного стану інформаційні системи радіаційного моніторингу набувають додаткового значення через ризики пошкодження ядерних об’єктів, диверсій або порушення технологічних процесів. Збройна агресія проти України актуалізувала необхідність підвищення стійкості таких систем, резервування каналів передачі даних та інтеграції з національними системами оповіщення населення [8; 13].

Сучасний розвиток інформаційних технологій сприяє впровадженню геоінформаційних систем у радіаційний моніторинг. ГІС дозволяють просторово відображати дані радіаційного контролю, моделювати поширення радіоактивних речовин, оцінювати зони можливого ураження та підтримувати прийняття управлінських рішень у сфері цивільного захисту [4].

2.4. Інформаційні системи хімічного моніторингу

Хімічна безпека є однією з ключових складових системи цивільного захисту держави, оскільки пов’язана з ризиками виникнення надзвичайних ситуацій техногенного та воєнного характеру, що супроводжуються викидом небезпечних хімічних речовин у навколишнє середовище. В умовах індустріалізації, розвитку хімічної промисловості, зростання обсягів транспортування небезпечних вантажів, а також з урахуванням воєнних загроз, актуалізується потреба у створенні та функціонуванні ефективних інформаційних систем хімічного моніторингу як інструменту раннього виявлення небезпек і підтримки управлінських рішень у сфері цивільної безпеки [8].

Інформаційні системи хімічного моніторингу являють собою сукупність технічних, програмних та організаційних засобів, призначених для безперервного або періодичного збору, оброблення, аналізу, зберігання та передачі даних про хімічний стан атмосферного повітря, водних об’єктів, ґрунтів і промислового середовища. Відповідно до національних стандартів, такі системи належать до автоматизованих інформаційно-вимірювальних систем, що забезпечують підтримку процесів моніторингу, прогнозування та оповіщення населення і органів управління [4].

Основною метою хімічного моніторингу є своєчасне виявлення перевищень гранично допустимих концентрацій небезпечних хімічних речовин, оцінка масштабів і динаміки забруднення, а також прогнозування можливих наслідків для здоров’я населення і довкілля. У системі цивільного захисту ці завдання безпосередньо пов’язані з функціями запобігання надзвичайним ситуаціям, мінімізації їх наслідків та організації захисних заходів [1].

Структурно інформаційні системи хімічного моніторингу включають мережу сенсорів і газоаналізаторів, пункти спостереження, канали передачі даних, центри оброблення інформації та програмні модулі візуалізації й аналізу. Первинні дані надходять від стаціонарних або мобільних постів контролю, які фіксують концентрації аміаку, хлору, оксидів азоту, сірчистого ангідриду, летких органічних сполук та інших небезпечних речовин [9; 10]. Отримана інформація в режимі реального часу передається до диспетчерських центрів або регіональних підсистем моніторингу.

В Україні функціонування систем хімічного моніторингу регламентується нормативно-правовими актами у сфері цивільного захисту, охорони довкілля та санітарно-епідеміологічного благополуччя населення. Координаційну роль у реагуванні на хімічні загрози відіграє Державна служба України з надзвичайних ситуацій, яка забезпечує збір та узагальнення інформації про хімічно небезпечні об’єкти, потенційні джерела аварій та наслідки надзвичайних подій [1], [8].

Практична значущість інформаційних систем хімічного моніторингу підтверджується реальними прикладами хімічних надзвичайних ситуацій, що мали місце в Україні. Так, у 2013 році на території ПАТ «Стирол» у місті Горлівка стався викид аміаку, який призвів до загибелі людей та ураження персоналу підприємства. Недостатня оперативність інформування та обмежені можливості автоматизованого контролю значно ускладнили ліквідацію наслідків аварії [1; 8].

Ще одним прикладом є аварії з витоком хлору на водоочисних станціях у різних регіонах України, зокрема у Вінницькій та Харківській областях, де хлор використовується для знезараження питної води. Такі інциденти створювали загрозу для населення прилеглих районів і вимагали негайного реагування з боку аварійно-рятувальних служб та систем оповіщення [10].

Особливе значення інформаційні системи хімічного моніторингу набувають у контексті воєнного стану, коли зростає ймовірність руйнування промислових об’єктів, складів хімічних речовин або об’єктів критичної інфраструктури. У таких умовах оперативний доступ до достовірної інформації дозволяє своєчасно приймати рішення щодо евакуації населення, введення режимів укриття, використання засобів індивідуального захисту та проведення аварійно-рятувальних робіт [10].

В умовах воєнних дій суттєво зросли ризики хімічних надзвичайних ситуацій, пов’язаних із обстрілами промислових об’єктів, складів із небезпечними хімічними речовинами та об’єктів критичної інфраструктури. Пошкодження нафтобаз, хімічних підприємств і транспортних комунікацій неодноразово призводили до локального забруднення атмосферного повітря та ґрунтів, що потребувало застосування мобільних засобів хімічного контролю та оперативного аналізу даних [10; 14].

Сучасні тенденції розвитку інформаційних систем хімічного моніторингу пов’язані з використанням геоінформаційних систем, хмарних технологій, інтеграцією з метеорологічними та гідрологічними даними, а також застосуванням елементів штучного інтелекту для прогнозування поширення хімічного забруднення. Такий підхід дозволяє підвищити точність оцінок ризику, ефективність управління та рівень захисту населення в умовах надзвичайних ситуацій [14].

Питання для контролю знань

1. Яке призначення метеорологічних інформаційних систем моніторингу в системі цивільного захисту населення?
2. Які основні джерела даних використовуються в метеорологічних інформаційних системах та як вони інтегруються в автоматизовані системи цивільного захисту?
3. Які види метеорологічних надзвичайних ситуацій є найбільш характерними для території України?
4. Яку роль відіграють автоматизовані системи раннього виявлення загроз у зменшенні наслідків метеорологічних НС?
5. Як функціонує система оповіщення населення про метеорологічні загрози відповідно до законодавства України?
6. Які приклади реальних метеорологічних надзвичайних ситуацій в Україні підтверджують необхідність впровадження сучасних інформаційних систем моніторингу?
7. Які основні вимоги нормативних документів (ДСТУ, ДБН, Кодекс цивільного захисту України) до побудови та експлуатації метеорологічних інформаційних систем?
8. Що розуміють під гідрологічними інформаційними системами моніторингу та яке їх призначення у системі цивільного захисту?
9. Які основні гідрологічні показники відстежуються за допомогою автоматизованих систем моніторингу водних об’єктів?
10. Охарактеризуйте структуру гідрологічної інформаційної системи та функції її основних компонентів.
11. Як здійснюється інтеграція даних гідрологічних інформаційних систем із системами оповіщення населення та управління надзвичайними ситуаціями?
12. Які проблеми та обмеження існують у функціонуванні гідрологічних інформаційних систем в Україні в умовах воєнного стану та зміни клімату?
13. Яке призначення інформаційних систем радіаційного моніторингу у системі цивільного захисту населення?
14. Які основні джерела радіаційної небезпеки контролюються в Україні за допомогою автоматизованих систем моніторингу?
15. Які типи датчиків і вимірювальних приладів використовуються в системах радіаційного моніторингу?
16. У чому полягає роль ДСНС та інших державних органів у функціонуванні систем радіаційного моніторингу?
17. Як інформаційні системи радіаційного моніторингу інтегруються з системами оповіщення населення про надзвичайні ситуації?
18. Які переваги надає використання автоматизованих та геоінформаційних технологій у радіаційному моніторингу?
19. Яке значення має оперативність і достовірність радіаційної інформації для прийняття управлінських рішень у разі надзвичайних ситуацій?

20. Яке призначення інформаційних систем хімічного моніторингу в системі цивільного захисту населення?

21. Які основні джерела хімічної небезпеки характерні для території України?

22. Які показники та параметри контролюються інформаційними системами хімічного моніторингу?

23. Які типи технічних засобів використовуються для автоматизованого контролю хімічного забруднення?

24. Яку роль відіграють інформаційні системи хімічного моніторингу у прогнозуванні та запобіганні хімічним надзвичайним ситуаціям?

25. Наведіть приклади реальних хімічних надзвичайних ситуацій в Україні та поясніть, як могли бути застосовані інформаційні системи моніторингу для мінімізації їх наслідків.

26. Яким чином результати хімічного моніторингу використовуються органами управління цивільного захисту для прийняття управлінських рішень?

Список використаної літератури

1. ДСНС України. Система оповіщення населення / Державна служба України з надзвичайних ситуацій – Режим доступу: https://dsns.gov.ua/.

2. Деякі питання функціонування загальнодержавної автоматизованої системи централізованого оповіщення… / Постанова КМУ № 355 від 29 березня 2024 р. – Режим доступу: https://zakon.rada.gov.ua/laws/show/355-2024-%D0%BF#Text.

3. Державна служба України з надзвичайних ситуацій (ДСНС) – інформація про управління надзвичайними ситуаціями – Режим доступу: https://dsns.gov.ua/.

4. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення. – К., 1993.

5. ДБН В.2.5-76:2014 Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення. – К., 2014.

6. Екологічний моніторинг: навчальний посібник / В.М Боголюбов, А.В.Сальнікова, О.О. Ракоїд // за ред. проф. В.М. Боголюбова. – Київ: НУБіПУ, 2023. – 200 с.

7. Український гідрометеорологічний центр. Гідрологічні спостереження та прогнози.

8. Кодекс цивільного захисту України. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text.

9. Воробієнко П. П., Білоусов С. І. Системи оповіщення цивільного захисту : навч. посіб. Одеса : ОНАС ім. О. С. Попова, 2013. 76 с.

10. Білоусов С. І. Об’єктові, локальні та спеціальні автоматизовані системи оповіщення цивільного захисту : навч. посіб. Одеса : ОНАЗ ім. О. С. Попова, 2013. 44 с.

11. International Atomic Energy Agency. Monitoring for Protection of the Public and the Environment. – Vienna : IAEA, 2025. URL: https://regelwerk.grs.de/sites/default/files/DS505%20Monitoring%20for%20Protection%20of%20the%20Public%20and%20the%20Environment%20-editing%20changes%20-%20for%20CSS%20silent%20approval_Step13_04.08.2025.pdf.

12. Державна служба України з надзвичайних ситуацій. Радіаційний захист та моніторинг [Електронний ресурс]. – Режим доступу: https://dsns.gov.ua/.

13. Положення про Державну інспекцію ядерного регулювання України. [Електронний ресурс] . – Режим доступу: https://zakon.rada.gov.ua/laws/show/363-2014-%D0%BF#Text.

14. World Health Organization. Chemical safety and public health. – Geneva : WHO, 2021. URL: https://www.who.int/publications/i/item/WHO-FWC-PHE-EPE-16-01.

Тема 3. Геоінформаційні системи (ГІС) у цивільній безпеці

1. Принципи роботи ГІС.
2. Картографування небезпек системами ГІС.
3. Моделювання зон ураження за допомогою ГІС.

3.1. Принципи роботи геоінформаційних систем (ГІС)

Геоінформаційні системи (ГІС) – це інтегровані інформаційні системи, які забезпечують збір, зберігання, обробку, аналіз і відображення даних, що мають просторову прив'язку. Основною метою ГІС є підтримка процесу прийняття рішень у різних сферах діяльності, включно з цивільним захистом, екологічним моніторингом, управлінням ресурсами та плануванням територій[1, 2].

ГІС базуються на принципах просторового аналізу, що дозволяє відображати зв'язки між об'єктами на карті та визначати їхні просторові закономірності. В основу роботи системи закладено концепцію цифрових шарів, де кожен шар містить окремий тип даних: рельєф, гідрологічні та метеорологічні показники, інженерну інфраструктуру, транспортні шляхи, об'єкти населення тощо. Шари можуть комбінуватися та аналізуватися для вирішення конкретних завдань[3, 4].

Одним із ключових принципів ГІС є геоприв'язка даних, тобто встановлення зв'язку між інформацією та її точним розташуванням у просторі за допомогою координатних систем. Це дозволяє виконувати точний просторовий аналіз, оцінювати ризики та прогнозувати розвиток надзвичайних ситуацій на основі географічних та атрибутивних даних[1, 5].

ГІС підтримують аналіз даних у режимі запитів та моделювання, що дозволяє прогнозувати поширення небезпечних явищ, наприклад повеней, хімічних аварій, радіаційних викидів або пожеж. Система може обчислювати зонування ризику, визначати потенційно уражені території та планувати маршрути евакуації, що робить її незамінним інструментом у цивільному захисті[2, 3, 6].

Технологічно ГІС складаються з трьох основних компонентів: апаратного забезпечення (сервери, робочі станції, датчики), програмного забезпечення (спеціалізовані ГІС-платформи та модулі для обробки даних), а також баз даних із географічною інформацією. Важливу роль відіграє інтерфейс користувача, який забезпечує візуалізацію даних на карті та доступ до інструментів аналізу[4, 5].

Іншим принципом роботи ГІС є інтеграція даних з різних джерел, включно з дистанційним зондуванням Землі, сенсорами, дрон-скануванням, державними та комерційними базами даних. Це забезпечує актуальність та точність інформації для прийняття оперативних рішень[3, 6].

ГІС використовуються для моніторингу надзвичайних ситуацій, управління ресурсами та планування заходів цивільного захисту. В Україні прикладом використання ГІС є інтеграція системи оповіщення населення ДСНС з даними метеорологічного та гідрологічного моніторингу для прогнозування повеней, буревіїв та інших НС[1, 2].

Крім того, ГІС дозволяє створювати карти ризиків, які відображають потенційні загрози для різних регіонів і населених пунктів.

За принципами роботи ГІС включають геоприв'язку даних, багатошарове відображення, інтеграцію різних джерел інформації, просторовий аналіз і моделювання, що робить ці системи ефективним інструментом для підтримки рішень у сфері цивільної безпеки.

3.2. Картографування небезпек системами ГІС

Картографування небезпек із використанням геоінформаційних систем (ГІС) є одним із ключових інструментів забезпечення цивільної безпеки, управління ризиками та підтримки прийняття рішень у сфері цивільного захисту. ГІС дозволяють здійснювати просторовий аналіз небезпечних природних і техногенних процесів, поєднувати різнорідні

дані та формувати наочні карти зон ризику для населення і критичної інфраструктури [1; 6].

У системі цивільного захисту картографування небезпек базується на інтеграції метеорологічних, гідрологічних, геологічних, радіаційних, хімічних та соціально-економічних даних. Такі дані подаються у вигляді тематичних шарів, що дозволяє здійснювати багатофакторний аналіз і виявляти території підвищеної небезпеки [3; 4]. Поєднання інформації про природні загрози з даними про щільність населення, об'єкти критичної інфраструктури та транспортні мережі є основою для оцінки ризиків надзвичайних ситуацій.

Важливим принципом картографування небезпек у ГІС є використання **просторового моделювання**. За допомогою геоалгоритмів визначаються зони можливого ураження під час повеней, пожеж, хімічних аварій, радіаційного забруднення або зсувів. Це дає змогу прогнозувати сценарії розвитку надзвичайних ситуацій, планувати евакуаційні заходи та оптимізувати дії аварійно-рятувальних служб [5].

В Україні картографування небезпек активно використовується органами ДСНС у межах автоматизованих систем оповіщення та моніторингу. Зокрема, карти зон підтоплення застосовувалися під час повеней у західних областях України у 2008 та 2020 роках, що дозволило завчасно ідентифікувати найбільш уразливі населені пункти та організувати заходи з мінімізації наслідків [6].

Міжнародний досвід підтверджує високу ефективність використання ГІС для картографування небезпек. У Сполучених Штатах Америки широко застосовується система **HAZUS-MH**, розроблена Федеральним агентством з надзвичайних ситуацій (FEMA). Ця ГІС-платформа дозволяє моделювати ризики повеней, землетрусів, ураганів та інших стихійних лих, а також оцінювати потенційні людські й економічні втрати. Методологія HAZUS використовується не лише у США, але й адаптована в низці інших країн для аналізу регіональних ризиків [7].

На глобальному рівні важливу роль відіграє **Global Disaster Alert and Coordination System (GDACS)** – міжнародна система раннього попередження про катастрофи, створена за участі ООН та Європейської Комісії. GDACS використовує ГІС-технології та супутникові дані для оперативного картографування землетрусів, повеней, цунамі та тропічних штормів, забезпечуючи міжнародну координацію реагування на великомасштабні надзвичайні ситуації [8].

У країнах Європейського Союзу активно застосовуються сервіси Copernicus Emergency Management Service**,** зокрема European Flood Awareness System (EFAS) **та** Global Flood Awareness System (GloFAS)**.** Ці системи забезпечують прогнозування повеней і формування карт ризику на основі дистанційного зондування Землі та гідрологічних моделей, що використовується для попередження органів влади та населення про можливі загрози [9].

Досвід Швейцарії демонструє ефективність використання ГІС для картографування лавинної та зсувної небезпеки. Система RAMMS (Rapid Mass Movements) інтегрує цифрові моделі рельєфу, метеорологічні дані та фізичні моделі руху мас, що дозволяє створювати детальні карти небезпеки для гірських регіонів та планувати інженерні захисні заходи.

Сучасні тенденції розвитку картографування небезпек передбачають інтеграцію ГІС із даними дистанційного зондування, сенсорними мережами, безпілотними літальними апаратами та мобільними додатками. Це забезпечує оновлення карт ризику в режимі реального часу та підвищує ефективність управління надзвичайними ситуаціями [9].

Картографування небезпек системами ГІС є універсальним і науково обґрунтованим інструментом цивільної безпеки, який поєднує національний і міжнародний досвід, сприяє зниженню ризиків надзвичайних ситуацій та підвищує рівень захищеності населення.

3.3. Моделювання зон ураження за допомогою ГІС

У сучасних умовах зростання кількості природних, техногенних та воєнних загроз особливого значення набуває прогнозування наслідків надзвичайних ситуацій. Одним із ключових інструментів такого прогнозування є моделювання зон ураження з використанням геоінформаційних систем (ГІС), що дозволяє оцінювати просторові масштаби небезпек, визначати потенційні втрати та обґрунтовувати управлінські рішення у сфері цивільної безпеки [3; 5].

Моделювання зон ураження в ГІС ґрунтується на інтеграції просторових, статистичних і фізичних даних, що описують джерело небезпеки, характеристики середовища та параметри впливу уражальних факторів. До таких факторів належать ударна хвиля, теплове випромінювання, радіаційне забруднення, поширення хімічно небезпечних речовин, затоплення, зсуви та інші прояви надзвичайних ситуацій [1].

Геоінформаційні системи забезпечують можливість формування цифрових моделей територій, які включають рельєф місцевості, забудову, транспортну інфраструктуру, гідрографічну мережу та щільність населення. Використання цифрових моделей рельєфу дозволяє більш точно прогнозувати поширення уражальних факторів, зокрема при моделюванні повеней, селів або хмар токсичних речовин [2].

Процес моделювання зон ураження за допомогою ГІС зазвичай включає визначення сценарію надзвичайної ситуації, вибір математичної або емпіричної моделі, просторову прив’язку вихідних даних та візуалізацію результатів у вигляді тематичних карт. Такі карти можуть відображати зони різного рівня небезпеки, прогнозовані межі ураження та території, що потребують першочергової евакуації або захисних заходів.

Широке застосування в практиці цивільного захисту мають ГІС-моделі поширення хімічних речовин у повітрі, які враховують метеорологічні умови, швидкість і напрямок вітру, температуру та рельєф місцевості. Подібні моделі дозволяють оперативно оцінювати ризики для населення у разі аварій на хімічно небезпечних об’єктах або під час воєнних дій.

Важливим напрямом є моделювання зон радіаційного забруднення з урахуванням типу джерела випромінювання, потужності дози та тривалості впливу. ГІС у цьому випадку забезпечують аналіз просторового розподілу радіаційних полів і підтримку рішень щодо обмеження доступу до небезпечних територій та організації захисних заходів [10].

Міжнародний досвід підтверджує ефективність використання ГІС-моделювання у сфері управління ризиками. Зокрема, система **HAZUS-MH**, розроблена Федеральним агентством з надзвичайних ситуацій США (FEMA), використовується для оцінки наслідків землетрусів, повеней та ураганів, дозволяючи прогнозувати масштаби ураження та економічні втрати [11]. У країнах Європейського Союзу активно застосовуються інструменти Copernicus Emergency Management Service для моделювання зон стихійних лих із використанням супутникових даних і ГІС-аналізу [12].

Використання ГІС для моделювання зон ураження має важливе значення не лише на етапі реагування на надзвичайні ситуації, але й у процесі стратегічного планування, оцінки ризиків та підготовки населення і служб цивільного захисту. Інтеграція таких моделей у системи підтримки прийняття рішень сприяє підвищенню рівня безпеки та зменшенню негативних наслідків надзвичайних ситуацій [5].

Питання для контролю знань

1. Що таке геоінформаційна система (ГІС) та які її основні функції у сфері цивільної безпеки?
2. Які типи просторових даних використовуються в ГІС та в чому полягає різниця між векторними й растровими моделями даних?
3. Які основні компоненти входять до структури геоінформаційної системи та яку роль відіграє кожен з них?
4. У чому полягає принцип багатошарової організації даних у ГІС та як він використовується для аналізу небезпек?

5. Які основні методи просторового аналізу застосовуються в ГІС для оцінки ризиків надзвичайних ситуацій?
6. Як геоінформаційні системи інтегруються з даними дистанційного зондування Землі та автоматизованими системами моніторингу?
7. Які переваги та обмеження використання ГІС у процесі прогнозування та управління надзвичайними ситуаціями?
8. У чому полягає сутність картографування небезпек у системі цивільного захисту та яку роль у цьому процесі відіграють геоінформаційні системи (ГІС)?
9. Які основні типи просторових даних використовуються в ГІС для картографування природних і техногенних небезпек?
10. Поясніть принцип багатошарового аналізу в ГІС та його значення для оцінки ризиків надзвичайних ситуацій.
11. Які методи просторового аналізу застосовуються для моделювання зон ураження та прогнозування розвитку небезпечних процесів?
12. Охарактеризуйте міжнародний досвід використання ГІС для оцінки та картографування небезпек (HAZUS-MH, GDACS, EFAS, GloFAS). Які їхні основні переваги?
13. Як дистанційне зондування Землі та супутникові дані інтегруються з ГІС при картографуванні небезпек?
14. Яке практичне значення картографування небезпек системами ГІС для планування заходів реагування, евакуації населення та зниження наслідків надзвичайних ситуацій?
15. У чому полягає сутність моделювання зон ураження та яке його значення для системи цивільного захисту?
16. Які типи надзвичайних ситуацій найчастіше потребують моделювання зон ураження за допомогою ГІС?
17. Які просторові дані та інформаційні шари використовуються при побудові моделей зон ураження в ГІС?
18. Які основні методи просторового аналізу застосовуються в ГІС для визначення меж зон ураження?
19. Як ГІС використовується для моделювання поширення хімічного, радіаційного або вибухового ураження?
20. Яку роль відіграють сценарні та прогнозні моделі у процесі прийняття управлінських рішень під час НС?
21. Які переваги та обмеження має використання ГІС-моделювання зон ураження в реальних умовах надзвичайних ситуацій?

Список використаних джерел

1. Воробієнко П. П., Білоусов С. І. Системи оповіщення цивільного захисту: навчальний посібник. – Одеса: ОНАС ім. О. С. Попова, 2013. – 76 с.
2. Білоусов С. І. Об’єктові, локальні та спеціальні автоматизовані системи оповіщення цивільного захисту: навчальний посібник. – Одеса: ОНАЗ ім. О. С. Попова, 2013. – 44 с.
3. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення. – Київ, 1993.
4. ДБН В.2.5-76:2014 Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення. – Київ, 2014.
5. Кодекс цивільного захисту України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/5403-17#Text
6. ДСНС України. Система оповіщення населення / Державна служба України з надзвичайних ситуацій – Режим доступу: https://dsns.gov.ua/
7. FEMA. HAZUS-MH Technical Manual. Washington, DC, 2023.
8. Global Disaster Alert and Coordination System (GDACS). URL: https://www.gdacs.org/
9. Copernicus Emergency Management Service. URL: https://emergency.copernicus.eu/

10. Documentation of the Work of the International Atomic Energy Agency NMUN Simulation*: IAEA, 2024. https://www.nmun.org/assets/documents/conference-archives/new-york/2024/ny24-2-res-iaea.pdf.
11. Federal Emergency Management Agency. HAZUS-MH Technical Manual. – Washington, DC: FEMA, 2020.
12. European Commission. Copernicus Emergency Management Service: Mapping Guide. – Brussels, 2021.

Тема 4. Дистанційне зондування Землі та його застосування у запобіганні НС

1. Супутникові дані, як елемент Дистанційного зондування Землі у запобіганні НС.
2. Дані отримані за допомогою дронів у запобіганні НС,
3. фотограмметрія, аналіз зображень для безпеки.

4.1. Супутникові дані як елемент дистанційного зондування Землі у запобіганні надзвичайних ситуацій

Дистанційне зондування Землі (ДЗЗ) є одним із ключових інструментів сучасних інформаційних систем цивільної безпеки. Воно ґрунтується на отриманні інформації про стан земної поверхні, атмосфери та водних об’єктів без прямого контакту з ними, переважно за допомогою супутникових сенсорів. У системі запобігання надзвичайним ситуаціям супутникові дані забезпечують своєчасне виявлення небезпечних процесів, їх моніторинг і прогнозування, що є критично важливим для прийняття управлінських рішень [1; 2].

Супутникові системи ДЗЗ дозволяють отримувати просторово-часову інформацію про великі території, у тому числі важкодоступні або небезпечні для наземних спостережень зони. Залежно від типу сенсорів розрізняють оптичні, інфрачервоні та радіолокаційні супутникові дані. Оптичні супутники (Sentinel-2, Landsat-8/9) використовуються для оцінки стану рослинного покриву, виявлення пожеж, підтоплень і змін землекористування. Інфрачервоні канали дозволяють фіксувати теплові аномалії, що є важливим для раннього виявлення лісових та торф’яних пожеж.

Особливе значення для цивільної безпеки мають радіолокаційні супутники (Sentinel-1), які забезпечують отримання даних незалежно від погодних умов і часу доби. Це дозволяє здійснювати безперервний моніторинг паводків, зсувів, просідань ґрунту та деформацій інженерних споруд. Радіолокаційні дані активно застосовуються для аналізу наслідків надзвичайних ситуацій та оцінки ступеня ураження територій.

У системі запобігання надзвичайним ситуаціям супутникові дані використовуються для моніторингу метеорологічних і гідрологічних загроз. Метеорологічні супутники (Meteosat, NOAA) забезпечують спостереження за атмосферними процесами, розвитком циклонів, грозових фронтів і сильних опадів, що дозволяє прогнозувати небезпечні метеорологічні явища. Гідрологічний моніторинг за допомогою ДЗЗ використовується для визначення площ затоплення, динаміки рівнів води та оцінки ризику повеней [2; 3].

Супутникові дані є важливим елементом моніторингу техногенних небезпек. Вони застосовуються для виявлення наслідків аварій на промислових об’єктах, контролю стану хвостосховищ, нафтогазової інфраструктури та зон можливого хімічного чи радіаційного забруднення. У поєднанні з геоінформаційними системами супутникова інформація дозволяє створювати карти зон ураження та прогнозувати поширення небезпечних факторів.

Міжнародний досвід підтверджує ефективність використання супутникових даних у системах цивільного захисту. Зокрема, Європейська програма **Copernicus** забезпечує безкоштовний доступ до супутникових даних та сервісів Copernicus Emergency Management

Service, які використовуються для оцінки наслідків стихійних лих, збройних конфліктів та техногенних аварій. Дані Copernicus активно застосовуються й в Україні для аналізу повеней, пожеж і руйнувань інфраструктури [4].

Важливою особливістю сучасних підходів є інтеграція супутникових даних із ГІС, наземними сенсорами та автоматизованими системами оповіщення. Така інтеграція дозволяє створювати комплексні інформаційно-аналітичні платформи, що підтримують раннє попередження населення та органів управління про загрозу виникнення надзвичайних ситуацій відповідно до вимог Кодексу цивільного захисту України [1; 5].

Супутникові дані дистанційного зондування Землі підвищують точність прогнозів, забезпечують оперативність реагування та сприяють зниженню ризиків для населення і територій.

4.2. Дані, отримані за допомогою дронів

Сучасна система запобігання надзвичайним ситуаціям (НС) дедалі більше спирається на використання інноваційних інформаційних технологій, серед яких особливе місце займають безпілотні літальні апарати (БпЛА, або дрони). Вони є ефективним інструментом оперативного збору просторових даних, що дозволяє підвищити точність оцінки ризиків, своєчасність реагування та обґрунтованість управлінських рішень у сфері цивільного захисту [1].

Дрони забезпечують отримання високодеталізованих аерофотознімків і відеоданих у режимі реального часу, що є критично важливим під час моніторингу потенційно небезпечних територій. На відміну від супутникових систем, БпЛА можуть працювати за несприятливих метеорологічних умов, на малих висотах і з високою просторовою роздільною здатністю, що робить їх особливо корисними для локального аналізу загроз.

У системі запобігання НС дронові дані застосовуються для виявлення ознак розвитку небезпечних процесів, зокрема підтоплень, лісових і торф’яних пожеж, зсувів, руйнування дамб та інших елементів критичної інфраструктури. Використання тепловізійних камер дозволяє фіксувати осередки загорянь або витоки небезпечних речовин на ранніх стадіях, що суттєво зменшує масштаби можливих наслідків [3].

Важливою перевагою дронів є можливість інтеграції отриманих даних із геоінформаційними системами (ГІС)**.** Аерофотознімки використовуються для створення ортофотопланів, цифрових моделей рельєфу та поверхні, які слугують основою для картографування небезпек і моделювання сценаріїв розвитку НС. Це дозволяє визначати зони потенційного ураження, оцінювати вразливість територій та прогнозувати вплив небезпечних факторів на населення і довкілля.

Міжнародний досвід свідчить про ефективність використання БпЛА у системах цивільного захисту. Зокрема, у країнах Європейського Союзу дрони активно застосовуються в межах програм Copernicus Emergency Management Service для оперативної оцінки наслідків повеней, пожеж і техногенних аварій. Аналогічні підходи використовуються FEMA (США) для попереднього аналізу ризиків і підтримки рятувальних операцій [6].

В Україні дрони дедалі частіше застосовуються підрозділами ДСНС для моніторингу паводкової ситуації, пожеж у природних екосистемах та контролю промислово небезпечних об’єктів. Використання БпЛА дозволяє зменшити ризики для особового складу, підвищити швидкість отримання інформації та забезпечити більш точну координацію сил і засобів цивільного захисту [7].

Окрему увагу слід приділити питанню якості та надійності дронових даних. Для їх ефективного використання необхідне дотримання стандартів геопросторових даних, калібрування сенсорів, а також відповідна підготовка фахівців. У поєднанні з аналітичними можливостями ГІС та іншими джерелами інформації дрони формують важливий компонент сучасної системи управління ризиками НС.

Отримані дані за допомогою дронів сприяють підвищенню рівня безпеки населення, зменшенню матеріальних втрат і розвитку превентивного підходу у сфері цивільної безпеки.

4.3. Фотограмметрія у системі запобіганні НС

Фотограмметрія є сучасним методом отримання та обробки просторової інформації за допомогою фотографічних або цифрових зображень об'єктів і територій. Вона дозволяє створювати точні карти, тривимірні моделі місцевості та об'єктів, що є ключовими у системах запобігання надзвичайних ситуацій (НС) [8; 9].

Основним завданням фотограмметрії у цивільному захисті є моніторинг змін на території та оцінка потенційних ризиків. За допомогою фотограмметричних даних можна визначати рівень підтоплення територій, стан інфраструктури після стихійних лих, поширення хімічних або радіаційних забруднень, а також потенційні зони ураження в разі аварій [5; 10].

Сучасні підходи передбачають поєднання фотограмметрії з геоінформаційними системами (ГІС). Це забезпечує інтеграцію даних з різних джерел, таких як супутники, дрони та стаціонарні сенсори, що дозволяє проводити аналіз ризиків у реальному часі. Наприклад, створення цифрових моделей рельєфу (DEM) із використанням аерофотознімків дає змогу оцінити ймовірність повеней або зсувів ґрунту [11; 12].

Використання дронів значно розширює можливості фотограмметрії. Завдяки мобільності та оперативності безпілотних літальних апаратів можна отримувати свіжі дані навіть у важкодоступних районах, швидко оцінювати масштаби руйнувань та виявляти загрози для населення і критичної інфраструктури [13].

Реальні приклади застосування фотограмметрії в Україні включають оцінку пошкоджень після повеней у західних областях та моніторинг територій промислових підприємств для своєчасного виявлення потенційно небезпечних об'єктів. Міжнародний досвід показує, що фотограмметрія успішно застосовується для оцінки наслідків землетрусів у Японії, повеней у Німеччині та повітряного контролю радіоактивних зон після аварії на Фукусімській АЕС [14].

Фотограмметрія також використовується для моделювання зон ураження та планування евакуації, оскільки на основі високоточних тривимірних моделей території можна визначити маршрути евакуації, оптимальні місця розташування пунктів тимчасового розміщення та оцінити потенційні загрози для населення [9; 11].

Фотограмметрія є важливим елементом сучасної системи запобігання надзвичайним ситуаціям, який дозволяє отримувати високоточні просторові дані, інтегрувати їх із ГІС та іншими інформаційними системами, що сприяє ефективному плануванню, моніторингу і реагуванню на надзвичайні ситуації.

4.4. Аналіз зображень для забезпечення безпеки

Аналіз зображень є сучасним напрямом інформаційних технологій, який дозволяє автоматизовано обробляти фото- та відеоматеріали з метою оцінки ризиків, виявлення небезпек і моніторингу стану об'єктів та територій. У системах цивільної безпеки ця технологія використовується для раннього виявлення надзвичайних ситуацій, контролю критичної інфраструктури та підвищення оперативності реагування[9; 15].

Основою аналізу зображень є застосування алгоритмів комп'ютерного зору та штучного інтелекту. Вони дозволяють автоматично розпізнавати об'єкти, визначати їхні характеристики та відстежувати зміни у часі, що є важливим для оцінки небезпек, таких як пожежі, повені, хімічні викиди або радіаційні загрози [16].

Сучасні системи аналізу зображень інтегруються з геоінформаційними системами (ГІС) та дистанційним зондуванням Землі, що забезпечує просторову прив'язку даних та можливість створення карт ризику та зон ураження. Наприклад, обробка аерофотознімків або супутникових зображень дозволяє оцінювати масштаби повеней, руйнувань інфраструктури та виявляти потенційні загрози для населення [12].

Особливу увагу приділяють використанню дронів та безпілотних літальних апаратів, які дозволяють оперативно отримувати високоточні зображення важкодоступних територій. Це особливо важливо під час стихійних лих або техногенних аварій, коли швидкий аналіз зображень сприяє прийняттю рішень щодо евакуації, ліквідації наслідків і мінімізації шкоди.

Крім технічних аспектів, важливим є використання алгоритмів штучного інтелекту для виявлення аномалій, таких як нетипові рухи людей, присутність небезпечних предметів або димових і хімічних хмар. Це дозволяє службам цивільного захисту оперативно реагувати на потенційні загрози та підвищувати рівень безпеки населення.

Реальні приклади застосування аналізу зображень в Україні включають моніторинг пожеж у лісових масивах, контроль рівня води в річках та оцінку наслідків вибухів на промислових підприємствах. Міжнародний досвід показує, що подібні системи успішно застосовуються у США та Японії для контролю критичної інфраструктури, виявлення ризиків терористичних атак та прогнозування наслідків природних катастроф.

Питання для контролю знань

1. Що таке дистанційне зондування Землі (ДЗЗ) і яке місце в ньому займають супутникові дані?
2. Які основні типи супутникових сенсорів (оптичні, радіолокаційні, теплові) використовуються для моніторингу надзвичайних ситуацій?
3. Яким чином супутникові дані застосовуються для раннього виявлення природних і техногенних небезпек?
4. У чому полягає роль супутникових даних у прогнозуванні та моніторингу повеней, пожеж і посух?
5. Як інтеграція супутникових даних із геоінформаційними системами (ГІС) підвищує ефективність управління надзвичайними ситуаціями?
6. Які міжнародні супутникові програми та системи (Copernicus, Sentinel, Landsat тощо) використовуються для цілей цивільного захисту?
7. Які переваги та обмеження має використання супутникових даних у системах запобігання і реагування на надзвичайні ситуації?
8. Яку роль відіграють безпілотні літальні апарати (дрони) у системі запобігання та реагування на надзвичайні ситуації?
9. Які основні типи даних можуть бути отримані за допомогою дронів (оптичні, тепловізійні, мультиспектральні тощо) та для яких завдань цивільної безпеки вони використовуються?
10. У чому полягають переваги використання дронів порівняно з традиційними методами наземного та супутникового моніторингу?
11. Як дані з дронів інтегруються з геоінформаційними системами (ГІС) для аналізу ризиків і моделювання надзвичайних ситуацій?
12. Які приклади застосування дронів для моніторингу природних та техногенних небезпек в Україні можна навести?
13. Які обмеження та ризики пов’язані з використанням дронів у системі цивільного захисту (погодні умови, нормативно-правові аспекти, технічні обмеження)?
14. Яке значення має використання даних з дронів для підвищення оперативності прийняття управлінських рішень під час надзвичайних ситуацій?
15. Що таке фотограмметрія і яка її основна роль у системі запобігання надзвичайним ситуаціям?
16. Які види даних використовуються у фотограмметрії для оцінки ризиків НС?
17. Як інтеграція фотограмметрії з геоінформаційними системами (ГІС) підвищує ефективність моніторингу НС?
18. Які переваги використання дронів для збору фотограмметричних даних у важкодоступних районах?

19. Наведіть приклади реальних застосувань фотограмметрії в Україні для оцінки наслідків НС.
20. Яким чином фотограмметрія сприяє моделюванню зон ураження та плануванню евакуації?
21. Які міжнародні приклади ефективного використання фотограмметрії для запобігання наслідкам природних і техногенних катастроф існують?
22. Що таке аналіз зображень і яку роль він відіграє у системах цивільної безпеки?
23. Які алгоритми та технології використовуються для автоматичного розпізнавання об'єктів на зображеннях?
24. Як інтеграція аналізу зображень із геоінформаційними системами (ГІС) підвищує ефективність моніторингу надзвичайних ситуацій?
25. Які переваги використання дронів для збору зображень у системі цивільної безпеки?
26. Наведіть приклади реального застосування аналізу зображень в Україні для запобігання НС.
27. Як алгоритми штучного інтелекту допомагають виявляти аномалії та потенційні загрози на зображеннях?
28. Який міжнародний досвід застосування аналізу зображень для забезпечення безпеки населення та критичної інфраструктури існує?

Список використаних джерел

1. Кодекс цивільного захисту України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/5403-17#Text
2. ДСНС України. Інформація про управління надзвичайними ситуаціями. – Режим доступу: https://dsns.gov.ua/
3. World Meteorological Organization. Space-based observations in disaster risk management. Geneva, 2020.
4. Copernicus Emergency Management Service. – Режим доступу: https://emergency.copernicus.eu/
5. ДБН В.2.5-76:2014. Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення. – Київ, 2014.
6. Federal Emergency Management Agency (FEMA). *Use of Unmanned Aircraft Systems in Emergency Management*. Washington, 2020.
7. Державна служба України з надзвичайних ситуацій. Застосування безпілотних літальних апаратів у діяльності ДСНС. – Режим доступу: https://dsns.gov.ua
8. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. – Київ, 1993.
9. Воробієнко П. П., Білоусов С. І. Системи оповіщення цивільного захисту: навчальний посібник. – Одеса: ОНАС ім. О. С. Попова, 2013. – 76 с.
10. Білоусов С. І. Об'єктові, локальні та спеціальні автоматизовані системи оповіщення цивільного захисту: навчальний посібник. – Одеса: ОНАЗ ім. О. С. Попова, 2013. – 44 с.
11. Бутенко, О. С. Фотограмметрія та дистанційне зондування Землі [Текст] : навч. посіб. до виконання курсових робіт / О. С. Бутенко, С. І. Горелик, В. О. Ковальова. – Харків : Нац. аерокосм. ун-т ім. М. Є. Жуковського «Харків. авіац. ін-т», 2020. – 72 с.
12. ДСНС України. Система оповіщення населення / Державна служба України з надзвичайних ситуацій – Режим доступу: https://dsns.gov.ua/
13. Застосування безпілотних авіаційних систем у сфері цивільного захисту: монографія / Д.В. Бондар, А.В. Гурник, А.О. Литовченко, В.В. Хижняк, В.Л. Шевченко, Д.М. Ядченко. Київ, 2022, 312 с. https://indcz.dsns.gov.ua/upload/1/0/7/9/0/0/2/ljQ2PLY10IvuTptkblpjCibdMBdVh3TutyE5LM9Z.pdf.

14. United Nations Office for Disaster Risk Reduction. Global Assessment Report on Disaster Risk Reduction 2022. – Geneva, 2022. – 210 p.

15. ДСТУ 8302:2015. Документування науково-технічної інформації. – Київ, 2015.

16. Карамушка, Л., та Шевченко, А. (2022). Епіричне вивчення характеристик психічного здоров'я керівників і працівників навчальних закладів у умовах війни. Київський журнал сучасної психології та психотерапії, 3, 29-42. https://doi.org/10.48020/mppj.2022.01.02.

Тема 5. Бази та банки даних у цивільній безпеці

1. Принципи проектування БД.
2. Моделі даних.
3. SQL.
4. Збирання та зберігання даних про об’єкти підвищеної небезпеки.
5. Збирання та зберігання даних про укриття.
6. Збирання та зберігання даних про ресурси реагування на НС.
7. Спеціалізовані державні та відомчі інформаційні банки даних: Єдина державна система цивільного захисту.
8. Реєстри ДСНС.

5.1. Принципи проєктування баз даних

Проєктування баз даних (БД) є ключовим етапом у створенні інформаційних систем, що забезпечують збереження, обробку та аналіз даних у системах цивільної безпеки. Бази даних дозволяють систематизувати інформацію про надзвичайні ситуації, ресурси, персонал, об’єкти критичної інфраструктури та інші аспекти, що забезпечують ефективне реагування на НС [1; 2].

Основним принципом проєктування БД є структурованість даних, яка забезпечує логічну організацію інформації. Для цього використовуються концептуальні моделі даних, такі як ER-моделі (Entity-Relationship), що дозволяють визначити сутності, їхні атрибути та зв’язки між ними [3].

Важливим аспектом є нормалізація даних, яка полягає у структуризації таблиць бази даних таким чином, щоб зменшити дублювання даних та уникнути аномалій під час оновлення або видалення інформації. Нормалізація забезпечує цілісність даних та ефективне використання ресурсів БД.

При проєктуванні БД слід враховувати потреби користувачів та специфіку предметної області. Для систем цивільної безпеки важливо передбачати модулі для моніторингу ризиків, обліку ресурсів, планування заходів реагування та інтеграції з іншими інформаційними системами, такими як ГІС, системи моніторингу хімічної, радіаційної та метеорологічної обстановки [4; 5].

Сучасні підходи до проєктування БД також включають забезпечення безпеки та доступності інформації. Це передбачає управління доступом користувачів, шифрування даних, резервне копіювання та відновлення інформації після НС. Такий підхід дозволяє забезпечити стійкість інформаційних систем навіть під час надзвичайних ситуацій.

Інший важливий принцип – масштабованість та гнучкість БД, що забезпечує можливість інтеграції нових модулів, додавання нових типів даних та підтримку збільшеного навантаження без погіршення продуктивності системи [6].

Реальні приклади застосування принципів проєктування БД у цивільній безпеці включають єдині системи обліку рятувальних ресурсів, інтегровані системи моніторингу НС на регіональному та державному рівнях, а також бази даних для моделювання зон ураження та планування евакуації населення [7; 8].

Проєктування баз даних забезпечує структурованість, цілісність, безпеку та оперативний доступ до даних, що є критичним у процесі моніторингу, планування та реагування на надзвичайні ситуації.

5.2. Моделі даних

Модель даних є основним інструментом для опису структури інформації та її взаємозв'язків у базах даних та інформаційних системах. Вона визначає, яким чином дані організовуються, зберігаються та обробляються, що особливо важливо у системах цивільної безпеки, де інформація використовується для моніторингу, оцінки ризиків і прийняття рішень [1; 2].

Сучасні моделі даних поділяють на кілька основних типів. Ієрархічна модель організовує дані у вигляді дерева, де кожна сутність має лише одного «батька», а зв'язки між даними відображаються у вигляді ієрархічних структур. Вона застосовується для структурованих систем обліку ресурсів та об'єктів критичної інфраструктури [3].

Мережна модель дозволяє кожній сутності мати кілька зв'язків з іншими сутностями. Така модель ефективна для опису складних взаємозв'язків між об'єктами, наприклад, у системах управління ризиками та моніторингу надзвичайних ситуацій.

Найбільш поширеною у сучасних інформаційних системах є реляційна модель даних, де дані зберігаються у таблицях з рядками (записами) та стовпцями (атрибутами). Реляційні бази даних забезпечують гнучкий доступ до інформації за допомогою мови SQL і підтримують нормалізацію даних, що дозволяє уникнути дублювання та підвищує цілісність інформації [4].

Для складних та великих обсягів даних, характерних для інтегрованих систем цивільної безпеки, використовують об'єктно-орієнтовані моделі даних, які дозволяють зберігати дані разом із методами їх обробки. Такі моделі зручні для роботи з мультимедійними даними, зображеннями, відео та супутниковими даними [5].

При проєктуванні моделей даних важливо дотримуватися принципів структурованості, узгодженості та масштабованості, забезпечувати можливість інтеграції з іншими системами, такими як ГІС, системи радіаційного, хімічного та метеорологічного моніторингу. Це дозволяє створювати єдині інформаційні простори для обміну даними та оперативного прийняття рішень у випадку надзвичайних ситуацій [6].

Реальні приклади застосування моделей даних у системах цивільної безпеки включають облік рятувальних ресурсів, інтегровані системи моніторингу НС, бази даних зон ураження та моделювання евакуації населення [7; 8]. Моделі даних є фундаментом для побудови ефективних і надійних інформаційних систем, що дозволяють своєчасно оцінювати ризики та реагувати на надзвичайні ситуації.

5.3. Керування реляційними базами даних – SQL

Structured Query Language (SQL) є стандартною мовою програмування для роботи з реляційними базами даних (РБД). Вона дозволяє створювати, модифікувати та керувати даними, що зберігаються у таблицях, а також виконувати запити для їхнього вибіркового аналізу [1; 2].

Основними складовими SQL є DDL (Data Definition Language), DML (Data Manipulation Language) та DCL (Data Control Language). DDL використовується для визначення структури бази даних, створення, зміни та видалення таблиць і індексів [3]. DML забезпечує вставку, оновлення, видалення та вибірку даних, що є ключовим у роботі з інформаційними системами цивільної безпеки, наприклад для моніторингу надзвичайних ситуацій та ресурсів реагування [4]. DCL застосовується для управління доступом користувачів, що дозволяє забезпечити безпеку та конфіденційність інформації.

В SQL для вибірки даних використовується оператор SELECT, який дозволяє формувати запити різного рівня складності: від простих запитів до складних із об'єднанням таблиць, агрегуванням даних та використанням підзапитів [4]. Використання SQL у системах цивільної безпеки дозволяє швидко отримувати необхідну інформацію для прийняття оперативних рішень у разі надзвичайних ситуацій.

Важливою функціональністю SQL є підтримка транзакцій, що забезпечує цілісність даних. Транзакції дозволяють групувати операції так, щоб вони виконувалися як єдиний блок, а у разі помилки система автоматично відкотить зміни [5]. Це особливо важливо для систем обліку ресурсів, зон ураження та інших критичних даних, де втрата або пошкодження інформації може призвести до серйозних наслідків.

SQL також підтримує індексацію, обмеження цілісності та ключі, що забезпечує ефективне зберігання та швидкий доступ до великих обсягів даних. У системах цивільної безпеки це дозволяє оперативно проводити аналіз ризиків, моделювання зон ураження, моніторинг метеорологічних, хімічних та радіаційних загроз.

Сучасні СУБД (системи управління базами даних), такі як MySQL, PostgreSQL, Microsoft SQL Server та Oracle, реалізують стандарт SQL та додаткові розширення, що дозволяють інтегрувати бази даних з іншими інформаційними системами, ГІС та аналітичними платформами [6;7]. Така інтеграція забезпечує оперативність та надійність управління інформацією у системах цивільної безпеки.

SQL забезпечує збереження, обробку, аналіз та захист даних, що є критично важливим для ефективного функціонування систем цивільної безпеки.

5.4. Збирання та зберігання даних про об’єкти підвищеної небезпеки

Об’єкти підвищеної небезпеки (ОПН) включають хімічні, радіаційні, енергетичні та промислові підприємства, транспортні вузли, об’єкти інфраструктури, де існує високий ризик виникнення надзвичайних ситуацій. Надійна інформація про такі об’єкти є ключовою для запобігання НС, планування заходів цивільного захисту та організації оперативного реагування [9; 10].

Збирання даних про ОПН здійснюється через офіційні державні реєстри, інформаційні системи підприємств, автоматизовані системи моніторингу та безпосередні обстеження об’єктів. До зібраних даних відносяться технічні характеристики, кількість та тип небезпечних речовин, наявність засобів пожежогасіння та аварійного реагування, план евакуації персоналу та населення, а також історія аварій та інцидентів [4; 5].

Особливу увагу приділяють електронному збиранню даних, яке забезпечує оперативне оновлення інформації, доступність для відповідальних структур та інтеграцію з іншими інформаційними системами цивільного захисту, включно з ГІС, системами радіаційного, хімічного та метеорологічного моніторингу [2; 6]. Застосування сучасних цифрових технологій, зокрема реляційних баз даних та SQL, дозволяє структуровано зберігати великі обсяги інформації та забезпечувати її швидкий доступ для аналізу та прийняття рішень [3].

Для підвищення безпеки інформації про ОПН застосовують різні рівні доступу, шифрування даних та системи резервного копіювання. Це забезпечує конфіденційність, цілісність та доступність інформації, що особливо важливо у випадку надзвичайних ситуацій.

Реальні приклади збору та зберігання даних про ОПН в Україні включають державні реєстри небезпечних об’єктів, інтегровані системи моніторингу на хімічних та енергетичних підприємствах, а також бази даних для обліку зон ураження та планів евакуації населення. Наприклад, автоматизована система обліку ОПН у ДСНС дозволяє у режимі реального часу відслідковувати стан об’єктів та надавати оперативну інформацію органам управління [11].

5.5. Збирання та зберігання даних про укриття

Укриття, як елементи цивільного захисту, призначені для захисту населення від наслідків надзвичайних ситуацій (НС), включаючи військові дії, хімічні, радіаційні та природні загрози. Надійна інформація про укриття необхідна для планування евакуації, організації швидкого доступу громадян до безпечних зон та забезпечення ефективного управління ризиками [9; 10].

Збирання даних про укриття включає отримання інформації про місцезнаходження споруд, їхню місткість, конструктивні особливості, наявність вентиляційних та

комунікаційних систем, запасів води та продуктів, а також технічного стану. Інформація збирається через державні та місцеві реєстри, обстеження об'єктів, автоматизовані системи моніторингу та опитування персоналу, відповідального за утримання укриттів [4; 5].

Сучасні підходи до збирання даних передбачають електронні бази даних та інтеграцію з геоінформаційними системами (ГІС), що дозволяє оперативно оновлювати інформацію, проводити аналіз доступності укриттів для населення та планувати дії у разі НС [2; 6]. Реляційні бази даних та мови запитів SQL забезпечують зручну структуризацію інформації, швидкий пошук необхідних даних та їх обробку для ухвалення рішень у реальному часі [3].

Для збереження конфіденційності та безпеки даних про укриття застосовують рівні доступу, шифрування та резервне копіювання інформації. Це особливо важливо в умовах воєнних дій або при загрозі цілеспрямованого порушення систем цивільного захисту.

В Україні приклади систем збирання та зберігання даних про укриття включають реєстри ДСНС, інтегровані ГІС міст та областей, а також спеціалізовані електронні платформи, що дозволяють моніторити стан укриттів та їх готовність до прийому населення. Дані системи забезпечують швидку передачу інформації органам управління цивільного захисту, планування евакуації та підтримку рішень в умовах надзвичайних ситуацій [11].

Завчасне збирання та зберігання даних про укриття за допомогою сучасних інформаційних технологій, їх інтеграція з ГІС та іншими системами моніторингу забезпечує швидке розміщення населення у захисних спорудах під час НС [2; 9].

5.6. Збирання та зберігання даних про ресурси реагування на НС

Ефективне реагування на надзвичайні ситуації значною мірою залежить від своєчасного та точного отримання інформації про наявні ресурси. До таких ресурсів відносяться людські, матеріально-технічні, транспортні та медичні засоби, а також спеціалізоване обладнання, яке залучається для ліквідації наслідків НС[9; 10].

Збирання даних про ресурси реагування передбачає реєстрацію наявності персоналу, спеціалізованих підрозділів, резервів техніки, матеріалів, медикаментів та інших засобів, необхідних для організації швидкої та ефективної допомоги. Джерелами такої інформації є державні та місцеві реєстри, обстеження підприємств та організацій, інтегровані інформаційні системи цивільного захисту[4; 5].

Сучасні підходи передбачають використання електронних баз даних та ГІС, що дозволяє вести облік ресурсів, здійснювати аналіз їх розташування та доступності, прогнозувати потреби в умовах надзвичайних ситуацій і планувати логістику реагування[5,6]. Інтеграція баз даних з геоінформаційними системами забезпечує оперативну візуалізацію ресурсів, що підвищує ефективність прийняття управлінських рішень [3].

Для забезпечення безпеки та достовірності даних застосовують рівні доступу, шифрування, резервне копіювання та регулярне оновлення інформації. Особлива увага приділяється актуалізації даних про технічний стан обладнання, наявність витратних матеріалів і готовність персоналу до дій у кризових умовах.

В Україні приклади систем збору та зберігання даних про ресурси реагування включають реєстри ДСНС, інтегровані платформи управління надзвичайними ситуаціями, а також автоматизовані системи обліку техніки та сил цивільного захисту. Такі системи дозволяють не лише оперативно визначати наявність ресурсів, а й планувати їх розподіл під час масштабних надзвичайних ситуацій [11].

5.7. Спеціалізовані державні та відомчі інформаційні банки даних: Єдина державна система цивільного захисту

У сучасних умовах зростання кількості природних, техногенних і воєнних загроз ефективне функціонування системи цивільного захисту неможливе без розвиненого інформаційного забезпечення. Інформація про потенційні небезпеки, сили і засоби реагування, стан інфраструктури та результати моніторингу є основою для прийняття

управлінських рішень у сфері запобігання надзвичайним ситуаціям та реагування на них. Саме тому в Україні сформовано систему спеціалізованих державних і відомчих інформаційних банків даних, інтегрованих у Єдину державну систему цивільного захисту.

Єдина державна система цивільного захисту України є комплексом органів управління, сил і засобів, а також інформаційних ресурсів, призначених для реалізації державної політики у сфері захисту населення і територій від надзвичайних ситуацій мирного часу та в особливий період. Відповідно до Кодексу цивільного захисту України, однією з ключових функцій ЄДСЦЗ є збирання, оброблення, зберігання та використання інформації про загрози і надзвичайні ситуації для забезпечення своєчасного реагування та координації дій органів влади і служб цивільного захисту [9].

Спеціалізовані державні та відомчі інформаційні банки даних у складі ЄДСЦЗ формуються за галузевим і функціональним принципом. Вони охоплюють інформацію про потенційно небезпечні об’єкти, об’єкти критичної інфраструктури, джерела підвищеної небезпеки, захисні споруди цивільного захисту, ресурси реагування, результати спостережень і моніторингу небезпечних процесів. Такі банки даних створюються і ведуться центральними органами виконавчої влади, зокрема ДСНС України, Міністерством внутрішніх справ, Міністерством охорони здоров’я, Міністерством енергетики та іншими відомствами в межах їх повноважень [12].

Важливе місце в системі інформаційних ресурсів ЄДСЦЗ посідають державні реєстри та автоматизовані інформаційні системи. До них належать, зокрема, банки даних про надзвичайні ситуації, інформаційні системи обліку захисних споруд, реєстри потенційно небезпечних об’єктів, системи моніторингу радіаційної та хімічної обстановки. Вони забезпечують накопичення структурованих даних, їх актуалізацію та доступ для органів управління цивільного захисту на державному, регіональному та місцевому рівнях [13].

Функціонування відомчих інформаційних банків даних передбачає використання сучасних інформаційно-комунікаційних технологій, геоінформаційних систем і автоматизованих систем управління. Інтеграція просторових даних у межах ЄДСЦЗ дозволяє візуалізувати загрози, прогнозувати розвиток надзвичайних ситуацій, оцінювати масштаби можливих уражень і планувати заходи з евакуації та ліквідації наслідків НС. Таким чином, інформаційні банки даних виконують не лише довідкову, а й аналітичну та прогностичну функцію.

Особливістю ЄДСЦЗ є міжвідомча взаємодія та обмін інформацією між державними і відомчими інформаційними ресурсами. Законодавством передбачено узгодження форматів даних, процедур доступу та механізмів інформаційного обміну з метою забезпечення цілісності інформаційного простору цивільного захисту. Це дозволяє уникати дублювання даних, підвищувати оперативність управлінських рішень і забезпечувати комплексний підхід до оцінювання ризиків [9; 14].

У сучасних умовах воєнного стану роль спеціалізованих інформаційних банків даних ЄДСЦЗ суттєво зростає. Вони використовуються для обліку наслідків надзвичайних ситуацій воєнного характеру, фіксації пошкоджень об’єктів інфраструктури, планування відновлювальних робіт і забезпечення захисту населення. Інформаційні ресурси стають важливим елементом національної безпеки, оскільки від їхньої повноти, достовірності та актуальності залежить ефективність функціонування всієї системи цивільного захисту [10].

5.8. Реєстри ДСНС у системі цивільної безпеки України

Функціонування системи цивільного захисту України неможливе без ефективного інформаційного забезпечення, ключовим елементом якого є державні та відомчі реєстри, що ведуться Державною службою України з надзвичайних ситуацій. Реєстри ДСНС забезпечують систематизований облік об’єктів, явищ і процесів, пов’язаних із виникненням надзвичайних ситуацій, потенційними загрозами та ресурсами реагування, і є основою для прийняття управлінських рішень у сфері цивільної безпеки.

Відповідно до Кодексу цивільного захисту України, ДСНС виконує функції щодо організації та здійснення державного нагляду, моніторингу небезпечних факторів, планування заходів реагування та інформування органів влади і населення про рівень ризиків [12]. Для виконання цих завдань формується система спеціалізованих реєстрів, які акумулюють актуальні дані про об’єкти підвищеної небезпеки, захисні споруди, потенційні джерела загроз і сили цивільного захисту.

Одним із ключових є Державний реєстр потенційно небезпечних об’єктів, який містить відомості про підприємства та об’єкти, діяльність яких може призвести до виникнення надзвичайних ситуацій техногенного або природного характеру. У реєстрі фіксуються характеристики об’єктів, види небезпечних речовин, можливі сценарії аварій та масштаби їх наслідків, що дозволяє здійснювати прогнозування ризиків і планування заходів запобігання [12].

Важливе місце в діяльності ДСНС посідає реєстр захисних споруд цивільного захисту, який включає інформацію про сховища, протирадіаційні укриття та інші інженерні споруди, призначені для захисту населення. Дані цього реєстру використовуються для оцінювання рівня забезпеченості територій укриттями, планування евакуаційних заходів та інформування населення про доступні захисні об’єкти, особливо в умовах воєнного стану [13].

У системі реагування на надзвичайні ситуації важливу роль відіграє облік сил і засобів цивільного захисту, що ведеться ДСНС у формі відомчих інформаційних баз і реєстрів. Вони містять відомості про аварійно-рятувальні формування, спеціальну техніку, засоби індивідуального захисту та матеріальні резерви, які можуть бути залучені під час ліквідації наслідків надзвичайних ситуацій. Актуальність цих даних є критичною для оперативного управління силами реагування.

Реєстри ДСНС тісно інтегровані з Єдиною державною системою цивільного захисту та іншими державними інформаційними ресурсами. Використання геоінформаційних систем і цифрових платформ дозволяє поєднувати реєстрові дані з просторовою інформацією, що підвищує точність аналізу ризиків, моделювання зон ураження та прийняття управлінських рішень у реальному часі [14].

Доступ до інформації регламентується законодавством, а обробка персональних та чутливих даних здійснюється з дотриманням вимог щодо кібербезпеки та захисту інформації. Це забезпечує баланс між відкритістю даних для органів управління та необхідністю збереження їх цілісності й конфіденційності [10].

Питання для контролю знань

1. Що таке база даних і яка її роль у системах цивільної безпеки?
2. Які основні етапи проєктування баз даних виділяють у сучасних інформаційних системах?
3. Що таке ER-модель і як вона допомагає структурувати дані?
4. У чому полягає нормалізація даних і чому вона важлива для цілісності бази даних?
5. Як забезпечується безпека та доступність інформації у базах даних цивільної безпеки?
6. Які принципи масштабованості та гнучкості застосовуються при проєктуванні БД для систем цивільної безпеки?
7. Що таке модель даних і яку роль вона відіграє у створенні інформаційних систем цивільної безпеки?
8. Які основні типи моделей даних існують і які особливості кожного типу?
9. У чому полягає особливість реляційної моделі даних і чому вона є найпоширенішою?
10. Як об’єктно-орієнтовані моделі даних допомагають працювати з мультимедійними та супутниковими даними?

11. Чому важлива інтеграція моделей даних із іншими системами моніторингу для цивільної безпеки?

12. Які принципи забезпечення узгодженості та масштабованості даних слід враховувати при проєктуванні моделей даних?

13. Що таке SQL і яку роль він відіграє у реляційних базах даних систем цивільної безпеки?

14. Які основні складові SQL і для чого використовується кожна з них (DDL, DML, DCL)?

15. Як оператор SELECT використовується для вибірки та аналізу даних у системах цивільної безпеки?

16. У чому полягає важливість транзакцій у SQL і як вони забезпечують цілісність даних?

17. Які механізми забезпечення цілісності та ефективності доступу до даних підтримує SQL?

18. Чому SQL вважається фундаментальним інструментом для збереження, обробки та захисту даних у системах цивільної безпеки?

19. Що відноситься до категорії об'єктів підвищеної небезпеки і чому їх моніторинг є критично важливим?

20. Які основні джерела інформації використовуються для збору даних про ОПН?

21. Як електронні системи збору даних підвищують ефективність моніторингу та реагування на НС?

22. Які заходи забезпечують безпеку та цілісність даних про ОПН[8,9]?

23. Як SQL та реляційні бази даних використовуються для зберігання та обробки інформації про ОПН?

24. Чому інтеграція даних про ОПН із ГІС та іншими інформаційними системами підвищує ефективність цивільного захисту?

25. Що відноситься до об'єктів укриття та яка їх роль у системі цивільної безпеки?

26. Які основні дані необхідно збирати про укриття для забезпечення безпеки населення?

27. Як електронні бази даних і ГІС підвищують ефективність моніторингу укриттів?

28. Які заходи забезпечують конфіденційність і безпеку інформації про укриття?

29. Як інтеграція даних про укриття з іншими інформаційними системами цивільного захисту підвищує ефективність реагування на НС?

30. Які переваги та обмеження використання реляційних баз даних і SQL при обліку укриттів?

31. Які основні види ресурсів залучаються для реагування на надзвичайні ситуації?

32. Які дані необхідно збирати про ресурси реагування для забезпечення ефективного управління НС?

33. Як електронні бази даних та ГІС підвищують ефективність моніторингу ресурсів реагування?

34. Які заходи забезпечують безпеку та достовірність інформації про ресурси реагування?

35. Які переваги та обмеження використання реляційних баз даних і SQL при обліку ресурсів реагування?

36. Яке призначення реєстрів ДСНС у системі цивільного захисту України?

37. Які основні види реєстрів ведуться Державною службою України з надзвичайних ситуацій?

38. Яку інформацію містить Державний реєстр потенційно небезпечних об'єктів і як вона використовується?

39. Яке значення має реєстр захисних споруд цивільного захисту для безпеки населення?

40. Як реєстри ДСНС інтегруються з Єдиною державною системою цивільного захисту та ГІС?

41. Які вимоги висуваються до захисту інформації в реєстрах ДСНС?

42. Яку роль відіграють реєстрові дані ДСНС у плануванні та ліквідації надзвичайних ситуацій?

Список використаних джерел

1. ДСТУ 8302:2015. Документування науково-технічної інформації. – Київ, 2015.
2. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. – Київ, 1993.
3. Трофименко О. Г. Організація баз даних : навч. посібник / О. Г. Трофименко, Ю. В. Прокоп, Н. І. Логінова, І. М. Копитчук. 2-ге вид. виправ. і доповн. – Одеса : Фенікс, 2019. – 246 с. https://dspace.onua.edu.ua/server/api/core/bitstreams/52f71d0e-d4a7-4a5b-bc54-1ebc66d3cecd/content.
4. Воробієнко П. П., Білоусов С. І. Системи оповіщення цивільного захисту: навчальний посібник. – Одеса: ОНАС ім. О. С. Попова, 2013. – 76 с.
5. Білоусов С. І. Автоматизовані системи раннього виявлення загроз: навчальний посібник. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 44 с.
6. ДБН В.2.5-76:2014 Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення. – Київ, 2014.
7. United Nations Office for Disaster Risk Reduction. Global Assessment Report on Disaster Risk Reduction 2022. – Geneva, 2022. – 210 p.
8. FEMA. HAZUS – GIS-based hazard analysis tool. – Washington, D.C., 2022.
9. Кодекс цивільного захисту України.– Режим доступу: https://zakon.rada.gov.ua/laws/show/5403-17#Text.
10. ДСНС України. Система оповіщення населення. – Режим доступу: https://dsns.gov.ua/.

14 Постанова КМУ № 355 від 29 березня 2024 р. «Деякі питання функціонування загальнодержавної автоматизованої системи централізованого оповіщення». – Режим доступу: https://zakon.rada.gov.ua/laws/show/355-2024-%D0%BF#Text.

12. Про затвердження Положення про Єдину державну систему цивільного захисту : Постанова Кабінету Міністрів України від 09.01.2014 № 11. – Режим доступу: https://zakon.rada.gov.ua/laws/show/11-2014-п.
13. Берко А.Ю., Верес О.М., Пасічник В.В. Системи баз даних та знань. Книга 2. Системи управління базами даних та знань: підручник. — 3-те вид., стер. — Львів : «Магнолія 2006», 2024.– 582 с. https://magnolia.lviv.ua/wp-content/uploads/2024/01/Systema-baz-danykh-knyha-2-pidruchnyk_zmist.pdf.
14. Донченко М. В. Геоінформаційні системи : навчальний посібник / М. В. Донченко, І. І. Коваленко. – Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2021. – 132 с.
15. Інформаційні системи і технології в міському просторі : монографія / [М. В. Новожилова, А. Л. Литвинов, В. Є. Зайцев та ін.] ; за заг. ред. М. В. Новожилової ; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2020. – 292 с. https://eprints.kname.edu.ua/56463/1/2019%20%D0%BF%D0%B5%D1%87.%2010_%D0%9C%D0%9D_.pdf.

Тема 6. Системи підтримки прийняття рішень у цивільній безпеці

1. Аналітичні моделі у цивільній безпеці.
2. Алгоритми оцінки ризиків.
3. Сценарне прогнозування, інформаційні панелі.

Сучасна система цивільної безпеки функціонує в умовах високої невизначеності, динамічності загроз та обмеженого часу на реагування. У таких умовах ключового значення набувають системи підтримки прийняття рішень (СППР), які забезпечують інтеграцію даних, аналітичну обробку інформації та формування обґрунтованих управлінських рішень. СППР у цивільній безпеці розглядаються як інформаційно-аналітичні комплекси, що поєднують бази даних, математичні моделі, алгоритми оцінки ризиків і візуальні інструменти для підтримки діяльності органів управління під час запобігання та реагування на надзвичайні ситуації.

6.1. Аналітичні моделі у цивільній безпеці

Аналітичні моделі є одним із ключових інструментів систем підтримки прийняття рішень у сфері цивільної безпеки, оскільки дозволяють формалізувати складні небезпечні процеси, оцінювати ризики надзвичайних ситуацій, прогнозувати їх розвиток і обґрунтовувати управлінські рішення щодо запобігання, реагування та ліквідації наслідків НС. У сучасних умовах зростання техногенних і природних загроз, а також воєнних ризиків, роль аналітичного моделювання суттєво зростає.

У теорії цивільної безпеки аналітична модель розглядається як формалізоване відображення реального об’єкта, процесу або явища з використанням математичних, статистичних, логічних чи імітаційних методів з метою аналізу, прогнозування та оптимізації управлінських рішень. Такі моделі дозволяють перейти від якісного опису небезпек до кількісної оцінки параметрів ризику, ймовірності виникнення подій та можливих наслідків, що відповідає сучасним підходам до управління ризиками у сфері безпеки [1].

Аналітичні моделі у цивільній безпеці застосовуються на всіх етапах управління надзвичайними ситуаціями: під час ідентифікації небезпек, оцінювання ризиків, планування заходів реагування, прогнозування розвитку НС та аналізу ефективності прийнятих рішень. Вони лежать в основі функціонування Єдиної державної системи цивільного захисту, систем моніторингу, прогнозування та інформаційно-аналітичного забезпечення органів управління [2].

За характером математичного апарату аналітичні моделі у цивільній безпеці поділяють на детерміновані та стохастичні. Детерміновані моделі описують процеси, параметри яких вважаються відомими та сталими, і застосовуються, зокрема, для розрахунку зон ураження при аваріях з викидом небезпечних хімічних речовин або для оцінювання параметрів пожежі за стандартних умов. Стохастичні моделі, навпаки, враховують імовірнісний характер небезпечних подій та невизначеність вихідних даних, що є особливо важливим під час аналізу природних загроз, масових аварій і катастроф.

Значне поширення у цивільній безпеці отримали ризик-орієнтовані аналітичні моделі, які базуються на поєднанні оцінки ймовірності виникнення небезпечної події та тяжкості її наслідків. Такі моделі використовуються для класифікації об’єктів підвищеної небезпеки, визначення пріоритетів захисних заходів, планування сил і засобів реагування, а також для обґрунтування управлінських рішень на державному та регіональному рівнях [4]. Відповідно до сучасних міжнародних підходів, ризик розглядається як функція небезпеки, вразливості та рівня впливу, що дозволяє комплексно оцінювати загрози для населення і територій [4].

Окрему групу становлять аналітичні моделі прогнозування розвитку надзвичайних ситуацій, які застосовуються для оцінки динаміки поширення небезпечних факторів у часі

та просторі. До таких моделей належать розрахунки поширення хмар токсичних речовин, прогнозування зон підтоплення, розповсюдження пожеж або вторинних небезпечних процесів. Застосування подібних моделей у поєднанні з геоінформаційними системами дозволяє наочно відображати результати аналізу та підвищує ефективність прийняття рішень.

У практиці цивільної безпеки широко використовуються також аналітичні моделі оцінювання наслідків надзвичайних ситуацій, які спрямовані на визначення можливих людських, матеріальних, екологічних і соціально-економічних втрат. Такі моделі застосовуються для обґрунтування планів евакуації, визначення потреб у ресурсах реагування, оцінки масштабів відновлювальних робіт і розроблення програм зниження ризиків [5].

Сучасний етап розвитку аналітичного моделювання у цивільній безпеці характеризується інтеграцією класичних математичних моделей з інформаційними технологіями, великими даними та елементами штучного інтелекту. Аналітичні моделі дедалі частіше реалізуються у вигляді програмних модулів систем підтримки прийняття рішень, інформаційно-аналітичних платформ і ситуаційних центрів, що забезпечує оперативність аналізу та адаптацію моделей до змін обстановки [6].

6.2. Алгоритми оцінки ризиків у системі цивільної безпеки

Алгоритми оцінки ризиків є одним із ключових інструментів аналітичного забезпечення управлінських рішень у сфері цивільної безпеки. Вони забезпечують системне виявлення, аналіз і кількісну або якісну оцінку небезпек, що можуть призвести до виникнення надзвичайних ситуацій природного, техногенного або соціального характеру. У сучасних підходах ризик розглядається як інтегральна характеристика, що поєднує ймовірність настання небезпечної події та тяжкість її можливих наслідків для населення, територій, об’єктів економіки й довкілля [7].

У теорії цивільної безпеки алгоритми оцінки ризиків ґрунтуються на класичній концепції «небезпека – вразливість – наслідки». Небезпека визначається як потенційне джерело шкоди, вразливість характеризує ступінь сприйнятливості об’єкта або системи до дії небезпечного чинника, а наслідки відображають масштаби можливих втрат. Поєднання цих складових дозволяє формувати об’єктивну картину ризиків і визначати пріоритетні напрями запобігання НС [2].

У практиці цивільного захисту широко застосовуються якісні, напівкількісні та кількісні алгоритми оцінки ризиків. Якісні алгоритми базуються на експертних оцінках і логічному аналізі можливих сценаріїв розвитку подій. До них належать матриці ризиків, чек-листи небезпек, методи ранжування загроз за рівнем небезпеки. Такі алгоритми є відносно простими у застосуванні та використовуються на початкових етапах аналізу або за умов обмеженої інформації.

Напівкількісні алгоритми поєднують експертні оцінки з умовними числовими шкалами. Наприклад, імовірність настання події та тяжкість наслідків оцінюються за бальною системою, після чого ризик визначається шляхом їх множення або агрегування. Цей підхід широко використовується в системах управління ризиками на об’єктах підвищеної небезпеки, у плануванні заходів цивільного захисту та під час розроблення паспортів ризику територій.

Кількісні алгоритми оцінки ризиків передбачають використання математичних моделей, статистичних даних та ймовірнісних методів. Вони дозволяють обчислювати індивідуальний, соціальний або територіальний ризик у числовому вираженні, наприклад у вигляді ймовірності загибелі людини протягом року або очікуваних економічних збитків. Такі алгоритми застосовуються під час аналізу промислових аварій, транспортних катастроф, радіаційних і хімічних загроз, а також у стратегічному плануванні безпеки.

Суттєву роль у сучасних алгоритмах оцінки ризиків відіграють геоінформаційні системи. Інтеграція алгоритмів оцінки ризиків із ГІС дозволяє враховувати просторовий розподіл небезпек, щільність населення, особливості інфраструктури та природні умови

території. Просторово орієнтовані алгоритми дають змогу формувати карти ризиків, визначати зони потенційного ураження та обґрунтовувати заходи з мінімізації наслідків НС.

У контексті цивільної безпеки особливого значення набувають сценарні алгоритми оцінки ризиків. Вони ґрунтуються на моделюванні можливих сценаріїв розвитку надзвичайних ситуацій з урахуванням різних вихідних умов і факторів впливу. Сценарний підхід дозволяє оцінити не лише найбільш імовірні, а й найнебезпечніші варіанти розвитку подій, що є важливим для підготовки органів управління та сил цивільного захисту [8].

Міжнародні підходи до оцінки ризиків у сфері цивільного захисту орієнтуються на концепцію ризик-орієнтованого управління, закріплену в документах ООН, ISO та Європейського Союзу. Зокрема, стандарт ISO 31000 визначає алгоритм оцінки ризиків як безперервний процес, що включає ідентифікацію небезпек, аналіз ризиків, їх оцінювання та вибір заходів реагування. Такий підхід активно впроваджується й у національну систему цивільного захисту України [3].

Алгоритми оцінки ризиків забезпечують науково обґрунтований підхід до прогнозування надзвичайних ситуацій, оптимізації заходів запобігання та підвищення рівня захищеності населення і територій.

6.3. Сценарне прогнозування, інформаційні панелі

Сценарне прогнозування у цивільній безпеці розглядається як метод системного аналізу можливих варіантів розвитку надзвичайних ситуацій з урахуванням впливу природних, техногенних і соціальних чинників. Його основною метою є не точне передбачення майбутніх подій, а формування кількох логічно обґрунтованих сценаріїв, що описують можливі наслідки за різних умов розвитку подій. У системі цивільного захисту сценарне прогнозування використовується для оцінювання ймовірних масштабів ураження населення, територій та інфраструктури, визначення потреб у силах і засобах реагування, а також для планування превентивних заходів.

У практиці цивільної безпеки сценарії зазвичай формуються на основі аналізу історичних даних про надзвичайні ситуації, результатів ризик-аналізу, математичного та імітаційного моделювання. Наприклад, при прогнозуванні паводків розглядаються сценарії нормального водопілля, критичного підвищення рівня води та катастрофічного затоплення з урахуванням кліматичних змін, стану гідротехнічних споруд і щільності забудови територій. Аналогічно, у разі хімічних або радіаційних аварій сценарії формуються з урахуванням типу небезпечної речовини, метеорологічних умов, рельєфу місцевості та часу реагування аварійних служб.

Важливою особливістю сценарного прогнозування є його тісний зв’язок із геоінформаційними системами. ГІС дозволяють візуалізувати сценарії розвитку надзвичайних ситуацій у просторовому вимірі, відображаючи зони можливого ураження, шляхи евакуації, розміщення укриттів і ресурсів реагування. Така візуалізація значно підвищує ефективність сприйняття інформації особами, що приймають рішення, та сприяє більш обґрунтованому плануванню дій у кризових умовах.

Інформаційні панелі (дашборди) є важливим інструментом реалізації результатів сценарного прогнозування та аналітичних розрахунків у системах підтримки прийняття рішень. Інформаційна панель являє собою інтерактивний візуальний інтерфейс, який у реальному або близькому до реального часі відображає ключові показники стану безпеки, ризиків і ресурсів реагування. У сфері цивільної безпеки такі панелі використовуються для моніторингу обстановки, оперативного аналізу даних і координації дій між різними суб’єктами Єдиної державної системи цивільного захисту.

Типова інформаційна панель цивільної безпеки може містити дані про кількість та типи надзвичайних ситуацій, рівні загроз, метеорологічні показники, стан критичної інфраструктури, готовність сил реагування та результати прогнозних сценаріїв. Важливо, що інформаційні панелі поєднують дані з різних джерел: сенсорних систем моніторингу, баз даних, результатів аналітичного та імітаційного моделювання, а також інформації від відомчих і міжвідомчих реєстрів [9].

Сучасні інформаційні панелі дедалі частіше використовують елементи інтелектуального аналізу даних та штучного інтелекту. Це дозволяє не лише відображати поточний стан обстановки, а й автоматично сигналізувати про перевищення порогових значень ризику, пропонувати рекомендовані варіанти дій або оновлювати сценарії розвитку подій з урахуванням нових даних. Такий підхід значно скорочує час на прийняття управлінських рішень та зменшує ймовірність людської помилки в умовах стресу та дефіциту часу.

Сценарне прогнозування та інформаційні панелі використовуються під час командно-штабних тренувань, навчань із реагування на надзвичайні ситуації та відпрацювання міжвідомчої взаємодії. Робота з такими інструментами формує у майбутніх спеціалістів системне мислення, здатність аналізувати складні ситуації та приймати обґрунтовані рішення на основі комплексної інформації [2].

Сценарне прогнозування та інформаційні панелі забезпечують перехід від реактивного до проактивного управління ризиками, підвищують рівень готовності до надзвичайних ситуацій та сприяють зниженню їхніх соціальних, економічних і людських втрат.

Питання для контролю знань

1. Що розуміють під аналітичною моделлю у сфері цивільної безпеки та яку роль вона відіграє у прийнятті управлінських рішень?
2. Які основні типи аналітичних моделей використовуються для аналізу небезпек і надзвичайних ситуацій?
3. У чому полягає відмінність між детермінованими та стохастичними аналітичними моделями?
4. Як аналітичні моделі застосовуються для прогнозування наслідків надзвичайних ситуацій?
5. Які вхідні дані необхідні для побудови аналітичних моделей у цивільній безпеці?
6. Які обмеження та похибки можуть виникати під час використання аналітичних моделей?
7. Яке значення мають аналітичні моделі для планування заходів цивільного захисту та реагування на НС?
8. Що таке ризик у контексті цивільної безпеки та які його основні складові?
9. Які етапи включає алгоритм оцінки ризиків надзвичайних ситуацій?
10. У чому полягає сутність якісної та кількісної оцінки ризиків?
11. Які показники використовуються для оцінювання ймовірності та тяжкості наслідків небезпечних подій?
12. Як алгоритми оцінки ризиків інтегруються у системи підтримки прийняття рішень?
13. Яку роль відіграють ГІС та інформаційні системи у реалізації алгоритмів оцінки ризиків?
14. Як результати оцінки ризиків використовуються для розробки превентивних заходів у цивільній безпеці?
15. Що таке сценарне прогнозування і чим воно відрізняється від традиційного прогнозування?
16. Які основні етапи побудови сценаріїв розвитку надзвичайних ситуацій?
17. Як сценарне прогнозування використовується для планування реагування на НС?
18. Яку роль відіграють інформаційні панелі (дашборди) у системах підтримки прийняття рішень?
19. Які показники та дані доцільно відображати на інформаційних панелях у сфері цивільної безпеки?
20. Як інтеграція сценарного прогнозування та дашбордів підвищує ефективність управління ризиками?

21. Які переваги та обмеження мають інформаційні панелі при прийнятті управлінських рішень у кризових ситуаціях?

Список використаних джерел

1. Бєгун В. В. Моніторинг безпеки на основі аналізу імовірнісних структурно-логічних моделей виробництва. [Електронний ресурс]. – Режим доступу: https://nasplib.isofts.kiev.ua/server/api/core/bitstreams/3d1d13cd-983f-4195-8295-ec151cef1e66/content.

2. Кодекс цивільного захисту України : Закон України від 02.10.2012 № 5403-VI (зі змін.).

3. ISO 31000:2018 Risk management – Guidelines. – Geneva : International Organization for Standardization, 2018. [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/65694.html.

4. UNDRR. Terminology on Disaster Risk Reduction [Електронний ресурс]. – Режим доступу: https://www.undrr.org/terminology.

5. Рубан І., Тютюник, В., Тютюник О. Особливості створення системи підтримки прийняття антикризових рішень в умовах невизначеності вхідної інформації при надзвичайних ситуаціях. Сучасні інформаційні технології у сфері безпеки та оборон. 2021. № 1(40) : Інформаційно-аналітична діяльність у сфері безпеки та оборони. С. 75–84.

6. Jung D, Tran Tuan V, Quoc Tran D, Park M, Park S. Conceptual Framework of an Intelligent Decision Support System for Smart City Disaster Management. Applied Sciences. 2020; 10(2):666. https://doi.org/10.3390/app10020666.

7. Підготовка органів управління до дій в надзвичайних ситуаціях: / В.Б. Лоїк, С.Д. Синельніков, Р.С. Яковчук, О.В. Лазаренко. Навчальний посібник – Львів: Львівський державний університет безпеки життєдіяльності, 2020. – 374 с.

8. UNDRR. **Global Assessment Report on Disaster Risk Reduction**. Geneva : United Nations, 2024. https://www.undrr.org/gar.

9. ISO 22320:2018. Security and resilience – Emergency management – Guidelines for incident management. – Geneva : International Organization for Standardization, 2018.

Тема 7. Архітектура та класифікація автоматизованих систем у сфері цивільного захисту

1. Типи АСУ.
2. Принципи побудови.
3. Компоненти АСУ, рівні автоматизації.

7.1. Типи АСУ, принципи побудови

Автоматизовані системи управління (АСУ) є ключовим елементом сучасної інфраструктури цивільного захисту, оскільки забезпечують збирання, оброблення, передавання та аналіз інформації, необхідної для ухвалення рішень щодо запобігання надзвичайним ситуаціям, реагування на них та організації оповіщення населення. Відповідно до ДСТУ 2226-93, автоматизована система визначається як система, що реалізує технологію оброблення інформації із застосуванням засобів обчислювальної техніки, методів та процедур управління об’єктами й процесами [1].

Застосування АСУ в цивільному захисті зумовлене потребою швидкої оцінки обстановки, координації сил, прогнозування розвитку подій та передачі сигналів оповіщення в режимі реального часу. Сучасні реалії, включно зі зростанням техногенних та природних ризиків, роблять автоматизацію невід’ємною складовою системи управління на державному, регіональному, місцевому та об’єктовому рівнях.

Типологія автоматизованих систем управління у сфері цивільного захисту ґрунтується на масштабі функціонування, призначенні, складі технічних засобів, а також на специфіці завдань, що вирішуються. У межах державної системи цивільного захисту можна виокремити кілька основних типів АСУ.

Одним із ключових типів є загальнодержавні автоматизовані системи, що забезпечують централізоване керування процесами оповіщення та реагування. До таких систем належить загальнодержавна автоматизована система централізованого оповіщення (ЗАСЦО), порядок функціонування якої визначено Постановою Кабінету Міністрів України № 355 від 29.03.2024. Система призначена для автоматизованого збору інформації про загрози, формування сигналів оповіщення та передачі їх до населення через електросирени, мобільні мережі, радіомовлення, телебачення та цифрові платформи [2]. Її структура включає центральний і регіональні вузли керування, мережі оповіщення, канали зв'язку та програмно-апаратні комплекси.

Другу групу становлять локальні та спеціальні АСУ оповіщення, які інтегруються на рівні окремих об'єктів підвищеної небезпеки, житлових районів, транспортних вузлів або промислових підприємств. Вони створюються для своєчасного інформування працівників і населення про небезпеку в межах певної території. За Воробієнком і Білоусовим, такі системи включають датчики контролю, підсистеми раннього виявлення НС, вузли керування, комплекси звукового та світлового сповіщення [3].

Особливої уваги заслуговують об'єктові АСУ, регламентовані нормами ДБН В.2.5-76:2014, де визначено вимоги до систем раннього виявлення надзвичайних ситуацій та оповіщення населення. Вони встановлюються у навчальних закладах, торговельних центрах, лікарнях, на підприємствах та промислових об'єктах. Такі системи поєднують автоматичні датчики (газу, диму, хімічних речовин), інтелектуальні модулі аналізу і цілу мережу виконавчих пристроїв для передачі сигналів. Їх функціонування має відповідати принципам безперервності, стійкості, дублювання та автономності джерел живлення [4].

У межах інформаційної інфраструктури цивільного захисту також функціонують автоматизовані системи моніторингу, що збирають і аналізують відомості про стан довкілля, гідрометеорологічну обстановку, сейсмічну активність, техногенні ризики. Такі системи забезпечують можливість прогнозування наслідків НС, формування превентивних заходів та координацію сил цивільного захисту. ДСНС України наголошує, що впровадження автоматизованих систем моніторингу дає змогу зменшити час реагування, підвищити точність оцінки ситуації та забезпечити інтеграцію даних із різних регіонів країни [5].

Принципи побудови АСУ у цивільній безпеці включають науково-технічні, організаційні та функціональні засади. Важливим є принцип ієрархічності, який передбачає наявність рівнів: державного, регіонального, місцевого та об'єктового. Це забезпечує обмін інформацією в обох напрямках і дає змогу ухвалювати рішення на відповідному рівні управління. Принцип інтегрованості полягає в об'єднанні різних підсистем – оповіщення, спостереження, моніторингу, прогнозування – у єдиний інформаційний простір. Принцип надійності передбачає дублювання каналів зв'язку, захист від кіберзагроз, резервне живлення та автоматичну діагностику працездатності системи.

Суттєве значення має також принцип автоматизації, відповідно до якого системи повинні виконувати основні функції без участі оператора: аналіз даних, формування попереджень, вибір сценарію реагування. Автоматизація дає змогу мінімізувати людський фактор, який особливо небезпечний у стресових або надзвичайних умовах. Принцип адаптивності вимагає, щоб АСУ могли змінювати свої параметри залежно від зовнішніх умов або технічного стану мережі.

Принципи побудови та функціонування АСУ також визначаються Кодексом цивільного захисту України, який встановлює завдання держави щодо створення системи управління, спостереження, моніторингу, прогнозування, оповіщення та реагування на надзвичайні ситуації [6].

Сучасні АСУ відіграють важливу роль у сфері цивільної безпеки, є багаторівневими, комплексними, інтегрованими системами, що забезпечують безперервне функціонування механізмів реагування та оповіщення населення. Вони становлять основу ефективного управління ризиками й формують технічне підґрунтя для збереження життя та здоров'я населення, сталого функціонування критично важливої інфраструктури й підвищення рівня безпеки держави.

7.2. Компоненти АСУ

Автоматизовані системи управління (АСУ) є важливою складовою сучасної інфраструктури цивільного захисту, оскільки забезпечують збирання, оброблення, збереження, передавання та використання інформації для прийняття рішень у надзвичайних ситуаціях. Відповідно до ДСТУ 2226-93, автоматизована система визначається як система, що поєднує персонал, технічні засоби, математичне забезпечення, організаційні заходи та інформаційні ресурси для автоматизації процесів управління об'єктами й процесами [1].

Компоненти АСУ формують цілісну, інтегровану структуру, у межах якої взаємодіють різні підсистеми, що забезпечують її функціонування. До ключових структурних складників АСУ належать технічні засоби, програмне забезпечення, інформаційне забезпечення, організаційне забезпечення, персонал системи, а також методичне й лінгвістичне забезпечення. Кожен з цих компонентів забезпечує виконання специфічних завдань і є необхідним для повноцінного функціонування системи управління.

Технічна частина АСУ охоплює апаратні ресурси, засоби зв'язку, інформаційно-вимірювальні комплекси, сервери, мережеве обладнання та кінцеві пристрої. Саме вони забезпечують збирання первинних даних, роботу каналів передачі інформації та функціонування елементів оповіщення. Згідно з ДБН В.2.5-76:2014, технічні компоненти систем оповіщення повинні включати датчики виявлення небезпечних факторів, центральні пункти керування, пристрої звукового оповіщення, джерела автономного живлення та дубльовані канали передачі інформації [4].

Програмне забезпечення АСУ охоплює операційні системи, прикладні програми, бази даних, алгоритми аналізу та прогнозування, а також спеціалізовані інтегровані модулі управління. Софт підвищує ефективність оброблення великих масивів даних, забезпечує оперативний аналіз і дозволяє автоматизувати значну частину функцій управління, зокрема формування сигналів оповіщення, їх розповсюдження, оцінку ризиків та управління ресурсами в умовах надзвичайних ситуацій.

Інформаційне забезпечення включає структури даних, формати повідомлень, довідники, бази даних та інформаційні потоки, що циркулюють у системі. У системах оповіщення, інформаційне забезпечення має ґрунтуватися на чітко визначених регламентах подання сигналів, стандартизованих повідомленнях про загрози та інструкціях для різних категорій населення [3; 7].

Чіткість і структурованість інформації є важливою умовою, оскільки від цього залежить своєчасність і правильність дій як органів управління, так і громадян.

Організаційне забезпечення АСУ включає структуру управління, розподіл функцій між органами цивільного захисту, правила взаємодії та нормативно-правові акти. Значна частина цих аспектів визначається Кодексом цивільного захисту України, який регламентує порядок функціонування органів управління, сил і засобів цивільного захисту, а також завдання щодо організації моніторингу, прогнозування, оповіщення та реагування [6].

На державному рівні порядок роботи загальнодержавної автоматизованої системи централізованого оповіщення визначений постановою Кабінету Міністрів України № 355, що деталізує склад технічних засобів, функції центрів управління, взаємодію регіональних і місцевих ланок та механізми надсилання сигналів [2].

Людський компонент АСУ – персонал – виконує функції контролю, технічної експлуатації, налаштування та прийняття рішень у нестандартних ситуаціях. Як підкреслює ДСНС України, ефективність автоматизованих систем управління значною мірою залежить від підготовки спеціалістів, які відповідають за інтерпретацію даних, технічну підтримку

обладнання, організацію оповіщення населення та координацію дій служб реагування [5]. Підготовка персоналу передбачає навчання роботі з програмними комплексами, знання нормативних документів і відпрацювання дій відповідно до планів реагування на НС.

Методичне забезпечення включає правила експлуатації, інструкції, алгоритми реагування, плани взаємодії та технологічні карти дій. В інфраструктурі цивільного захисту це особливо важливо, оскільки чіткі методичні документи дозволяють синхронізувати роботу системи на різних рівнях управління. Лінгвістичне забезпечення визначає стандарти формулювання сигналів, команд і повідомлень, що підвищує їх однозначність та точність.

Особливе місце серед компонентів АСУ займають системи оповіщення, які є критично важливими для збереження життя та здоров'я населення. ДСНС України описує систему оповіщення як комплекс технічних і організаційних засобів, що забезпечують передачу сигналів про небезпеку та інструкцій для населення у разі виникнення загроз. До складу таких систем входять локальні мережі оповіщення, сирени, мобільні та цифрові канали, телерадіомовлення, а також сучасні платформи екстрених повідомлень [5].

Науковці зазначають, що ефективність оповіщення залежить від злагодженої взаємодії всіх компонентів – технічних, програмних, інформаційних, організаційних і людських [3].

У системах централізованого оповіщення, згідно з постановою Кабінету Міністрів України № 355, основними компонентами є центральний пункт управління, регіональні вузли, апаратура аналізу загроз, сервісні платформи передачі повідомлень, канали зв'язку та спеціальні модулі оповіщення, здатні автоматично дублювати сигнали різними каналами [2].

Така багаторівнева структура забезпечує надійність і стійкість системи навіть у разі пошкодження окремих її елементів, оскільки компоненти АСУ формують складну інтегровану архітектуру, у якій технічні засоби забезпечують фізичну роботу системи, програмне забезпечення виконує інформаційно-аналітичні функції, організаційні та нормативні елементи визначають правила її роботи, а людський фактор забезпечує адаптивність і контроль.

7.3. Рівні автоматизації АСУ у сфері цивільної безпеки України

Автоматизовані системи управління (АСУ) – складні багаторівневі інформаційно-технічні структури, які використовуються для управління, моніторингу, аналізу та реагування на процеси, пов'язані з безпекою, цивільним захистом, оповіщенням населення, оперативним реагуванням тощо. У контексті цивільної безпеки, АСУ об'єднують технічні засоби, програмно-математичне забезпечення, організаційні процедури та людські ресурси, щоб забезпечити оперативність, надійність і ефективність дій під час надзвичайних ситуацій. [1]

Рівні автоматизації АСУ – важливий аспект її архітектури та функціонування. Розрізняючи рівні автоматизації, можна краще розуміти, які завдання виконує система, як взаємодіють її компоненти, і які можливості вона має для масштабування, інтеграції або дублювання функцій.

Один із підходів до поділу рівнів автоматизації визначає три основні рівні: нижній, середній та верхній. Нижній рівень охоплює датчики, контрольно-вимірювальні прилади, пристрої збору первинної інформації та виконавчі механізми. На цьому рівні забезпечується фіксація параметрів середовища (наприклад, тиск, дим, газ, температуру), моніторинг фізичних характеристик, а також – у разі потреби – безпосереднє втручання через виконавчі пристрої (сирени, сиренне оповіщення, аварійні системи). Інформація з цього рівня передається до середнього рівня для обробки. [1; 8]

Середній рівень – це обробка, аналіз і агрегування отриманих даних, програмно-апаратні комплекси, сервери, програмні системи збору й аналізу інформації. Саме тут формуються сигнали тривоги, оцінки стану, відбувається кореляція даних з різних датчиків, проводиться логіка прийняття рішень. У системах цивільного захисту середній рівень може відповідати за формування повідомлень, попереджень, вибір сценаріїв реагування,

передавання сигналів далі – на рівень верхній або безпосередньо до органів управління / оповіщення. [2; 6]

Верхній рівень автоматизації – це диспетчерські, аналітичні, керуючі центри, інформаційні пункти управління, інтеграція з базами даних, централізоване планування, координація дій, управління ресурсами. У контексті цивільної безпеки – це, наприклад, загальнодержавна автоматизована система централізованого оповіщення (ЗАСЦО), яка охоплює централізований вузол, регіональні підсистеми, канали передачі сигналів, інтеграцію з органами реагування та цивільного захисту. Така система має максимально широкий охоплення, здатна приймати рішення на основі зведених даних, поширювати сигнали масового оповіщення, координувати масштабну реакцію. [2].

Для систем цивільного захисту до цього трирівневого (або багаторівневого) підходу додається ще рівень інтеграції та взаємодії – коли різні АСУ (моніторингу, оповіщення, управління ресурсами, реагування) з'єднуються у єдиний інформаційний простір. Така інтегрована система забезпечує координацію між різними підсистемами, обмін даними, централізований контроль та комплексний аналіз. Наприклад, система оповіщення населення в Україні охоплює технології збору даних, обробки, прийняття рішень і поширення сигналів – що реалізовано на різних рівнях. [3; 9].

Переваги поділу на рівні автоматизації: ясність у структурі, можливість визначити відповідальність, розмежувати функції, забезпечити резервування та дублювання, підвищити надійність і стійкість. У випадку збою на нижньому рівні – датчиків чи виконавчих пристроїв – середній та верхній рівні можуть продовжити функціонувати, аналізувати ситуацію, визначати альтернативні сценарії. Якщо порушено канал зв'язку – верхній рівень може перенаправити сигнали іншими каналами або активувати резервні канали. Такі принципи забезпечують надійність та безперервність роботи систем цивільного захисту.

Законодавчо функціонування автоматизованих систем управління цивільним захистом в Україні регламентується на рівні загальнодержавного порядку. Зокрема, Постанова КМУ № 355 від 29 березня 2024 р. визначає порядок функціонування загальнодержавної автоматизованої системи централізованого оповіщення про загрозу або виникнення надзвичайних ситуацій. Це означає, що на «верхньому рівні» АСУ створено державний механізм централізованого реагування, який інтегрує регіональні й місцеві системи оповіщення та цивільного захисту [2].

Водночас, локальні або об'єктові системи – їх побудова відповідає нижньому або середньому рівню, залежно від масштабу і завдань. Наприклад, система оповіщення на підприємстві, навчальному закладі чи об'єкті інфраструктури або спеціалізований датчик/система моніторингу – це елементи нижнього/середнього рівня автоматизації, які можуть функціонувати автономно або бути інтегрованими у вищий рівень. [3; 7].

При проєктуванні АСУ для цивільної безпеки важливо враховувати потребу масштабованості, резервування та модульності: система має бути здатною працювати на різних рівнях – від локального об'єкта до загальнодержавного контролю. Це дає змогу гнучко адаптувати систему до конкретних умов, виду загрози, чисельності населення або об'єкта, та забезпечити стійкість до відмов. Організаційні та нормативні складові – відповідні положення, регламенти, інструкції, алгоритми реагування – мають відповідати обраному рівню АСУ. У цьому сенсі законодавчі документи, технічні норми, стандарти та нормативи відіграють ключову роль.

Забезпечення рівнів автоматизації АСУ в системах цивільної безпеки – це не лише технічне питання, а й стратегічне. Це основа для побудови ефективної, надійної та адаптивної системи захисту населення, оперативного реагування та управління ризиками.

Питання для контролю знань

1. Що таке автоматизована система управління (АСУ) та які її основні цілі у сфері цивільної безпеки?

2. Які основні типи АСУ виділяють за функціональним призначенням?
3. У чому полягає відмінність між АСУ технологічними процесами та організаційно-управлінськими АСУ?
4. Які принципи побудови АСУ є базовими (системності, ієрархічності, відкритості тощо)?
5. Як принцип ієрархічності реалізується в сучасних АСУ цивільної безпеки?
6. Яку роль відіграє принцип сумісності та стандартизації при створенні АСУ?
7. Чому принцип надійності є критично важливим для АСУ у сфері цивільного захисту?
8. Які основні компоненти входять до складу автоматизованої системи управління?
9. У чому полягає функціональне призначення технічного забезпечення АСУ?
10. Яку роль відіграє програмне забезпечення в роботі АСУ?
11. Що включає інформаційне забезпечення АСУ та які вимоги до нього висуваються?
12. Яке значення має організаційно-методичне забезпечення для ефективного функціонування АСУ?
13. Яку роль відіграє людський фактор (персонал) у складі АСУ?
14. Як взаємодіють між собою компоненти АСУ під час управління надзвичайною ситуацією?
15. Які рівні автоматизації АСУ виділяють у сфері цивільної безпеки України?
16. У чому полягають особливості локального рівня автоматизації?
17. Які функції реалізуються на регіональному рівні АСУ цивільного захисту?
18. Яку роль відіграє загальнодержавний рівень автоматизації в системі цивільної безпеки?
19. Як інформація передається між різними рівнями АСУ?
20. Які приклади автоматизованих систем оповіщення використовуються на різних рівнях?
21. Які перспективи розвитку рівнів автоматизації АСУ в умовах цифровізації та інтеграції з ІКТ?

Список використаних джерел

1. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
2. Деякі питання функціонування загальнодержавної автоматизованої системи централізованого оповіщення. Постанова Кабінету Міністрів України № 355 від 29.03.2024. URL: https://zakon.rada.gov.ua/laws/show/355-2024-п
3. Воробієнко П. П., Білоусов С. І. Системи оповіщення цивільного захисту: навчальний посібник. Одеса: ОНАС ім. О. С. Попова, 2013. 76 с.
4. ДБН В.2.5-76:2014 Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення.
5. Державна служба України з надзвичайних ситуацій. Управління надзвичайними ситуаціями. URL: https://dsns.gov.ua/.
6. Кодекс цивільного захисту України. URL: https://zakon.rada.gov.ua/laws/show/5403-17#Text.
7. Білоусов С. І. Об'єктові, локальні та спеціальні автоматизовані системи оповіщення цивільного захисту: навчальний посібник. Одеса: ОНАЗ ім. О. С. Попова, 2013. 44 с.
8. Рішення Кабінету Міністрів України від 29.03.2024 № 355 «Деякі питання функціонування загальнодержавної автоматизованої системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій». URL: https://zakon.rada.gov.ua/laws/show/355-2024-%D0%BF#Text.

9. Державна служба України з надзвичайних ситуацій – офіційна інформація про систему оповіщення населення. URL: https://dsns.gov.ua/ =9

10. Доклад про класифікацію та структуру АСУ: «Автоматизація систем управління: рівні, засоби, особливості та сфери застосування». URL: https://government.com.ua/nashi-hroshi/avtomatizatsiya-sistem-upravlinnya-rivni-zasobi-osoblivosti-ta-sferi-zastosuvannya.html.

Тема 8. Автоматизовані системи оповіщення населення та управління реагуванням на НС

1. Принципи побудови автоматизованих систем оповіщення населення та управління реагуванням на НС.
2. Канали передачі сигналів.
3. Цифрові системи оповіщення.

8.1. Принципи побудови автоматизованих систем оповіщення населення та управління реагуванням на надзвичайні ситуації

Автоматизовані системи оповіщення населення та управління реагуванням на надзвичайні ситуації є ключовим елементом функціонування системи цивільного захисту держави. Їх основним призначенням є своєчасне інформування органів управління, сил цивільного захисту та населення про загрозу або виникнення надзвичайної ситуації, а також забезпечення координації дій під час реагування. В умовах воєнного стану, техногенних аварій та природних катастроф роль таких систем істотно зростає, оскільки саме швидкість і достовірність інформації безпосередньо впливають на збереження життя і здоров’я людей.

Принципи побудови автоматизованих систем оповіщення формуються з урахуванням вимог законодавства України у сфері цивільного захисту, міжнародних рекомендацій, а також сучасних досягнень у галузі інформаційно-комунікаційних технологій. Одним із базових принципів є централізоване управління з можливістю децентралізованого використання. Це означає, що загальне керівництво системою здійснюється з єдиного центру (державного або регіонального рівня), водночас окремі її елементи можуть автономно функціонувати на місцевому рівні у разі втрати зв’язку з центральним пунктом управління. Такий підхід підвищує стійкість системи в умовах пошкодження інфраструктури або інформаційних каналів [1].

Важливим принципом є безперервність функціонування та цілодобова готовність. Автоматизовані системи оповіщення повинні працювати у режимі постійної готовності, забезпечуючи можливість негайного запуску сигналів оповіщення незалежно від часу доби чи умов зовнішнього середовища. Для цього передбачаються резервні джерела живлення, дублювання серверного обладнання та альтернативні канали зв’язку, що відповідає вимогам надійності та живучості систем цивільного захисту [2].

Наступним ключовим принципом є багатоканальність передачі сигналів оповіщення. Сучасні автоматизовані системи повинні використовувати одночасно кілька каналів комунікації: електросирени, радіо- і телемовлення, мобільний зв’язок, SMS- та Cell Broadcast-повідомлення, інтернет-платформи та мобільні застосунки. Це дозволяє охопити максимальну кількість населення та знизити ризик неповідомлення у разі виходу з ладу окремих каналів [3].

Принцип оперативності та мінімізації часу реагування передбачає автоматизацію процесів збору, обробки та передавання інформації. Інтеграція систем оповіщення з інформаційними системами моніторингу, диспетчерськими центрами та геоінформаційними системами дає змогу скоротити час між виявленням загрози і доведенням попереджувального сигналу до населення. Автоматичне формування

повідомлень та сценаріїв оповіщення зменшує залежність від людського фактора та ймовірність помилок [4].

Суттєвим є принцип адаптивності та масштабованості, який забезпечує можливість розвитку системи відповідно до змін у безпековому середовищі та технологічному прогресі. Автоматизовані системи оповіщення мають підтримувати розширення функціоналу, інтеграцію нових цифрових сервісів і модернізацію програмного забезпечення без повної заміни інфраструктури. Це особливо важливо в умовах динамічних загроз, характерних для сучасних надзвичайних ситуацій і воєнних дій [5].

Окрему увагу приділяють принципу доступності та зрозумілості інформації для населення. Повідомлення, що передаються через систему оповіщення, повинні бути чіткими, лаконічними та адаптованими до різних категорій населення, зокрема осіб з інвалідністю. Сучасні підходи передбачають використання не лише звукових сигналів, а й текстових, візуальних та мультимедійних повідомлень із рекомендаціями щодо дій у конкретній ситуації [6].

Побудова автоматизованих систем оповіщення населення та управління реагуванням на надзвичайні ситуації базуються на принципах поєднання централізованого управління, технічної надійності, багатоканальності, автоматизації та орієнтації на потреби населення.

8.2. Канали передачі сигналів.

Подання сигналів оповіщення є ключовим елементом систем цивільного захисту, оскільки від швидкості, надійності та доступності каналів передачі інформації безпосередньо залежить своєчасність реагування населення й органів управління на надзвичайні ситуації. Канали передачі сигналів в автоматизованих системах оповіщення формуються з урахуванням принципів багатоканальності, резервування та охоплення максимально широкої аудиторії незалежно від її місця перебування, технічних можливостей і стану інфраструктури.

Традиційно в системах цивільного захисту використовуються електросирени та гучномовці як первинні засоби масового оповіщення. Сигнал «Увага всім!» передається за допомогою електросирен і слугує універсальним попереджувальним знаком, після якого населення повинно отримати уточнювальну інформацію через інші канали зв’язку. Перевагою сиренного оповіщення є його висока чутність і незалежність від індивідуальних пристроїв користувачів, однак недоліком залишається обмежена інформативність та залежність від електропостачання [1].

Важливу роль у передачі сигналів оповіщення відіграють мережі проводового та ефірного мовлення. Телебачення і радіо використовуються для доведення розширених повідомлень про характер загрози, порядок дій населення, маршрути евакуації та інші інструкції. У межах Єдиної державної системи цивільного захисту України передбачено обов’язкове переривання теле- і радіоефіру для трансляції екстрених повідомлень органів управління цивільного захисту [2]. Цей канал є ефективним для охоплення великих територій, однак його результативність знижується за умов пошкодження телекомунікаційної інфраструктури або відсутності доступу населення до приймачів.

Сучасні автоматизовані системи оповіщення активно використовують телекомунікаційні мережі мобільного зв’язку. До таких каналів належать SMS-розсилки, голосові повідомлення та технологія Cell Broadcast, яка дозволяє передавати екстрені повідомлення на всі мобільні пристрої в межах визначеної зони без перевантаження мережі. Перевагою мобільних каналів є адресність, оперативність і можливість доставки текстової інформації з конкретними рекомендаціями щодо дій населення [3]. Разом з тим ефективність цих каналів залежить від стабільності роботи мобільних операторів і рівня покриття мережі.

Інтернет-канали передачі сигналів набувають дедалі більшого значення в умовах цифровізації суспільства. Офіційні вебсайти органів державної влади, сторінки ДСНС у соціальних мережах, мобільні застосунки та месенджери використовуються для оперативного інформування населення про надзвичайні ситуації. Перевагою цього каналу є можливість швидкого оновлення інформації, використання графічних матеріалів, карт і

рекомендацій у реальному часі. Водночас він є вразливим до кіберзагроз, перебоїв доступу до інтернету та інформаційного перевантаження користувачів [4].

Для підвищення надійності систем оповіщення застосовуються спеціалізовані канали зв'язку для органів управління та сил реагування. До них належать захищені цифрові радіомережі, відомчі системи зв'язку та супутникові канали, які забезпечують передачу сигналів навіть за умов повного руйнування наземної інфраструктури. Такі канали використовуються переважно для управління силами цивільного захисту та координації дій під час ліквідації наслідків надзвичайних ситуацій [5].

Ключовою вимогою до каналів передачі сигналів у цивільній безпеці є їх інтеграція в єдину автоматизовану систему. Це забезпечує синхронне доведення сигналів через різні канали, зменшує ризик втрати інформації та підвищує рівень готовності населення до реагування. Міжнародний досвід свідчить, що найбільш ефективними є гібридні моделі оповіщення, які поєднують традиційні та цифрові канали, забезпечуючи стійкість системи до технічних і організаційних збоїв [6].

Канали передачі сигналів в автоматизованих системах оповіщення населення мають багаторівневу структуру та виконують взаємодоповнюючі функції. Їх раціональне поєднання дозволяє забезпечити своєчасне, достовірне та доступне інформування населення і органів управління цивільного захисту, що є необхідною умовою ефективного реагування на НС.

8.3. Цифрові системи оповіщення населення

Цифрові системи оповіщення населення є ключовим елементом сучасної системи цивільного захисту, що забезпечує своєчасне інформування населення про загрози надзвичайних ситуацій та організацію адекватного реагування. Їх розвиток обумовлений переходом від аналогових і централізованих засобів сповіщення до інтегрованих цифрових рішень, здатних працювати в умовах високої динаміки подій, інформаційних перевантажень і багатоканального середовища.

Цифрові системи оповіщення базуються на використанні сучасних інформаційно-комунікаційних технологій, автоматизованих платформ управління та телекомунікаційних мереж. Вони забезпечують не лише передачу сигналу тривоги, а й доставку структурованих повідомлень із конкретними рекомендаціями щодо дій населення залежно від типу загрози, території та часу її розвитку. Такий підхід відповідає сучасним вимогам Єдиної державної системи цивільного захисту щодо адресності, оперативності та надійності інформування населення [1].

Однією з ключових особливостей цифрових систем оповіщення є їх інтеграція з автоматизованими системами управління, геоінформаційними системами та базами даних ризиків. Це дозволяє формувати повідомлення з урахуванням просторового аналізу небезпек, прогнозних моделей розвитку надзвичайних ситуацій та актуального стану інфраструктури. Наприклад, у разі хімічної або радіаційної аварії система може автоматично визначити зону можливого ураження та надіслати попередження лише тим категоріям населення, які перебувають у межах потенційного ризику [7].

В Україні цифрові системи оповіщення розвиваються в межах модернізації державної системи централізованого оповіщення з урахуванням досвіду воєнного стану. Застосовуються такі цифрові інструменти, як мобільні додатки, SMS-розсилки, push-повідомлення, інтеграція з мобільними операторами, офіційними вебпорталами органів влади та платформами електронного урядування. Прикладом є використання технології Cell Broadcast, яка дозволяє передавати екстрені повідомлення на всі мобільні пристрої в зоні покриття без перевантаження мережі [8].

Важливою перевагою цифрових систем оповіщення є можливість зворотного зв'язку. На відміну від традиційних сирен або радіоповідомлень, цифрові канали дозволяють отримувати підтвердження доставки повідомлень, аналізувати поведінку користувачів та коригувати подальші дії органів управління. Це підвищує ефективність реагування та дає змогу оперативно оцінювати рівень поінформованості населення [9].

Разом із тим, впровадження цифрових систем оповіщення пов’язане з низкою викликів. Серед них – нерівномірний рівень цифрової грамотності населення, залежність від електропостачання та мобільного зв’язку, ризики кібератак і поширення дезінформації. Тому сучасні наукові підходи наголошують на необхідності резервування каналів оповіщення, поєднання цифрових і традиційних засобів, а також захисту інформаційної інфраструктури систем оповіщення [10].

Міжнародний досвід свідчить, що найбільш ефективними є багаторівневі цифрові системи оповіщення, інтегровані з національними платформами управління надзвичайними ситуаціями. У країнах ЄС, США та Японії активно використовуються національні системи екстреного інформування населення, які поєднують мобільні технології, телебачення, інтернет-сервіси та соціальні мережі. Такий підхід дозволяє охопити максимальну кількість населення та знизити ризики несвоєчасного реагування [11].

Цифрові системи оповіщення населення забезпечують оперативне, адресне та інформативне доведення сигналів небезпеки для формування у населення навичок правильного реагування на цифрові сигнали оповіщення.

Питання для контролю знань

1. Які основні завдання виконують автоматизовані системи оповіщення населення у системі цивільного захисту?
2. У чому полягає принцип централізованого та децентралізованого управління системами оповіщення?
3. Як реалізується принцип безперервності та цілодобової готовності систем оповіщення?
4. Яке значення має принцип резервування елементів і каналів зв’язку в системах оповіщення?
5. Як принцип сумісності та інтеграції забезпечує взаємодію систем оповіщення з іншими інформаційними системами цивільного захисту?
6. Чому принцип адресності повідомлень є важливим для сучасних систем оповіщення населення?
7. Які вимоги висуваються до надійності та живучості систем оповіщення в умовах надзвичайних ситуацій і воєнного стану?
8. Які основні канали передачі сигналів оповіщення застосовуються в системах цивільного захисту?
9. У чому полягають переваги та обмеження використання дротових каналів зв’язку для оповіщення населення?
10. Яку роль відіграють радіо- і телевізійні канали в системах масового оповіщення?
11. Як мобільний зв’язок та SMS-оповіщення використовуються для адресного інформування населення?
12. Які особливості використання інтернет-каналів і мобільних додатків у системах оповіщення?
13. Чому важливим є поєднання кількох каналів передачі сигналів у єдиній системі оповіщення?
14. Які фактори впливають на надійність каналів передачі сигналів в умовах надзвичайних ситуацій?
15. У чому полягає сутність цифрових систем оповіщення населення та їх відмінність від традиційних аналогових систем?
16. Які основні технології використовуються в цифрових системах оповіщення (Cell Broadcast, IP-оповіщення тощо)?
17. Як цифрові системи оповіщення забезпечують адресність і персоналізацію повідомлень?
18. Яку роль відіграють геоінформаційні технології в цифрових системах оповіщення?

19. Які переваги цифрових систем оповіщення з точки зору швидкості реагування та охоплення населення?

20. Які кіберзагрози та ризики характерні для цифрових систем оповіщення і як їх мінімізують?

21. Які напрями розвитку цифрових систем оповіщення є найбільш перспективними для системи цивільної безпеки України?

Список використаних джерел

1. Кодекс цивільного захисту України : Закон України від 02.10.2012 № 5403-VI (зі змін.).
2. Про затвердження Положення про єдину державну систему цивільного захисту : Постанова Кабінету Міністрів України від 09.01.2014 № 11.
3. ДСНС України. Системи оповіщення та інформування населення у надзвичайних ситуаціях [Електронний ресурс]. – Режим доступу: https://dsns.gov.ua
4. Білоусов С. І. Об’єктові, локальні та спеціальні автоматизовані системи оповіщення цивільного захисту : навч. посіб. / С. І. Білоусов. – Одеса : ОНАЗ ім. О. С. Попова, 2013. – 44 с.
5. ISO 22320:2018. Security and resilience – Emergency management – Guidelines for incident management.
6. United Nations Office for Disaster Risk Reduction. Multi-hazard Early Warning Systems: A Checklist. – Geneva : 2020. URL: https://globalplatform.undrr.org/2022/sites/default/files/2022-02/Multi-hazard%20Early%20Warning%20Systems-%20A%20Checklist.pdf.
7. Закора О. В. Автоматизовані системи управління та зв'язок: підручник / А. Б. Фещенко, Л. В. Борисова, В. О. Собина, Д. В. Тарадуда, М. О. Демент, І. М. Неклонський. – Х.: НУЦЗУ, 2021. – 288 с.
8. Emergency Telecommunications Table-Top Simulation Guide. Geneva: International Telecommunication Union. ITU-D. 2020b. URL: https://www.itu.int/en/ITU-D/Emergency-Telecommunications/Documents/Publications/2020/TTX_Guide.pdf.
9. Cvetković V. M. Innovative solutions for disaster early warning and alert systems: a literary review. HOME. 2021. Т. 11 : Contemporary Security Challenges. С. 367–378. URL: https://eskup.kpu.edu.rs/dar/article/view/279/203.
10. ISO 22322:2015. Societal security – Emergency management – Guidelines for public warning. URL: https://www.iso.org/standard/53335.html.
11. European Commission. Emergency communication and public warning systems. – Brussels, 2022. URL: https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/emergency-communication-and-public-warning-systems.

Тема 9. Хмарні технології та цифрові платформи у системах цивільної безпеки

1. Хмарна інфраструктура.
2. Сервіси для обробки великих даних.
3. Кіберстійкість платформ.

9.1. Хмарна інфраструктура

Хмарна інфраструктура є одним із ключових елементів цифрової трансформації систем цивільної безпеки та управління надзвичайними ситуаціями. Вона забезпечує централізоване зберігання, обробку та доступ до великих обсягів даних у режимі реального часу, що є критично важливим для моніторингу небезпек, координації дій сил реагування та оперативного інформування органів управління і населення. У сучасних умовах, зокрема

під час воєнного стану та зростання кількості техногенних і природних загроз, хмарні технології розглядаються як основа стійкої, масштабованої та відмовостійкої інформаційної інфраструктури цивільного захисту.

Під хмарною інфраструктурою розуміють сукупність апаратних і програмних ресурсів, що надаються користувачам у вигляді сервісів через мережу Інтернет. До її складу входять центри обробки даних, віртуалізовані сервери, системи зберігання даних, мережеві ресурси та програмні платформи управління. Основною особливістю хмарної інфраструктури є використання технологій віртуалізації, які дозволяють ефективно розподіляти обчислювальні ресурси між різними користувачами та системами без необхідності створення власної фізичної IT-інфраструктури [1].

У системах цивільної безпеки хмарна інфраструктура застосовується для підтримки інформаційно-аналітичних систем, геоінформаційних платформ, реєстрів об'єктів підвищеної небезпеки, баз даних укриттів, ресурсів реагування та систем підтримки прийняття рішень. Використання хмарних сервісів дозволяє інтегрувати дані з різних джерел, зокрема сенсорних мереж, супутникового моніторингу, безпілотних літальних апаратів і відомчих інформаційних систем, у єдиному інформаційному просторі [2].

Залежно від моделі розгортання розрізняють публічні, приватні, гібридні та спільні хмари. Для систем цивільної безпеки найбільш доцільною є гібридна модель, яка поєднує переваги публічних хмар (масштабованість, доступність, економічність) і приватних хмар (підвищений рівень контролю та безпеки даних). Такий підхід дозволяє зберігати критично важливу інформацію в захищених державних сегментах, одночасно використовуючи публічні ресурси для обробки великих масивів відкритих або оперативних даних [3].

Важливою перевагою хмарної інфраструктури є її масштабованість, що дає змогу оперативно збільшувати або зменшувати обчислювальні ресурси залежно від рівня загроз та інтенсивності інформаційних потоків. У разі виникнення надзвичайної ситуації це дозволяє швидко нарощувати потужності для обробки даних моніторингу, моделювання сценаріїв розвитку подій і забезпечення безперебійної роботи цифрових платформ управління реагуванням [4].

Окрему увагу в хмарній інфраструктурі систем цивільної безпеки приділяють питанням надійності та безперервності функціонування. Хмарні платформи забезпечують резервування даних, географічне розподілення центрів обробки та автоматичне відновлення сервісів у разі збоїв. Це є критично важливим для підтримки управлінських рішень у кризових умовах, коли втрата доступу до інформації може призвести до значних соціальних і матеріальних втрат [5].

Разом із тим використання хмарної інфраструктури потребує врахування вимог інформаційної та кібербезпеки. Дані цивільного захисту можуть містити чутливу інформацію про критичну інфраструктуру, розташування укриттів, маршрути евакуації та ресурси реагування. Тому впровадження хмарних рішень має супроводжуватися дотриманням національних і міжнародних стандартів безпеки інформації, зокрема стандартів серії ISO/IEC 27000, а також нормативних вимог у сфері захисту інформації та персональних даних [6].

Таблиця 9.1.

Порівняльна таблиця моделей хмарних обчислень

Модель хмари	**Коротка характеристика**	**Рівень контролю користувача**	**Рівень безпеки**	**Переваги**	**Недоліки**	**Приклади застосування у цивільній безпеці**
Публічна хмара (Public Cloud)	Хмарна інфраструктура, що надається стороннім	Низький	Середній	Масштабованість, низька вартість, швидке розгортання	Обмежений контроль, залежність від провайдера	Оперативне інформування населення, відкриті ГІС-портали,

	провайдером і використовується багатьма користувачами					аналітика надзвичайних ситуацій
Приватна хмара (Private Cloud)	Інфраструктура, призначена для однієї організації	Високий	Високий	Повний контроль даних, підвищена безпека	Висока вартість, потреба у власному адмініструванні	Реєстри ДСНС, бази даних об’єктів підвищеної небезпеки
Гібридна хмара (Hybrid Cloud)	Поєднання публічної та приватної хмар	Середній–високий	Високий	Гнучкість, баланс між безпекою та вартістю	Складність інтеграції	Системи реагування на НС, аналітика великих даних з обмеженим доступом
Спільнотна хмара (Community Cloud)	Хмара для кількох організацій зі спільними завданнями	Середній	Високий	Спільне використання ресурсів, стандартизація	Обмежена масштабованість	Міжвідомча взаємодія органів цивільного захисту
IaaS (Infrastructure as a Service)	Надання обчислювальних ресурсів (сервери, мережі, сховища)	Високий	Залежить від налаштувань	Гнучкість, контроль інфраструктури	Потребує IT-фахівців	Розгортання систем моніторингу та оповіщення
PaaS (Platform as a Service)	Платформа для розробки та розгортання застосунків	Середній	Середній–високий	Швидка розробка, зниження навантаження на IT	Обмеження платформи	Розробка аналітичних систем НС
SaaS (Software as a Service)	Готові програмні рішення через інтернет	Низький	Середній	Простота використання, відсутність адміністрування	Обмежені налаштування	Онлайн-панелі управління, системи звітності
Модель хмари	Коротка характеристика	Рівень контролю користувача	Рівень безпеки	Переваги	Недоліки	Приклади застосування у цивільній безпеці
Публічна хмара (Public Cloud)	Хмарна інфраструктура, що надається стороннім провайдером і використовується багатьма користувачами	Низький	Середній	Масштабованість, низька вартість, швидке розгортання	Обмежений контроль, залежність від провайдера	Оперативне інформування населення, відкриті ГІС-портали, аналітика надзвичайних ситуацій

Для систем цивільної безпеки найбільш доцільним є використання гібридних хмарних моделей, які дозволяють поєднати високий рівень безпеки критичних даних із гнучкістю та масштабованістю публічних сервісів. Застосування моделей IaaS і PaaS є ефективним для створення та підтримки інформаційно-аналітичних систем реагування на

надзвичайні ситуації, тоді як SaaS-рішення доцільні для оперативного управління та інформування.

Хмарна інфраструктура є базовим технологічним компонентом сучасних систем цивільної безпеки, що забезпечує інтеграцію даних, оперативність управління та стійкість інформаційних процесів. Її впровадження створює передумови для розвитку цифрових платформ, використання аналітики великих даних і підвищення ефективності реагування на надзвичайні ситуації, за умови належного рівня кіберзахисту та нормативного регулювання.

9.2. Сервіси для обробки великих даних

У сучасних умовах цифровізації систем цивільної безпеки сервіси для обробки великих даних (Big Data) відіграють ключову роль у підвищенні ефективності запобігання, прогнозування та реагування на надзвичайні ситуації. Під великими даними розуміють масиви структурованої та неструктурованої інформації значного обсягу, які характеризуються високою швидкістю надходження, різноманіттям форматів і потребують спеціалізованих інструментів для зберігання, обробки та аналізу. У сфері цивільної безпеки такими даними є інформація з датчиків моніторингу, супутникові знімки, метеорологічні спостереження, геоінформаційні шари, телеметрія з технічних систем, оперативні звіти та повідомлення населення.

Сервіси для обробки великих даних у хмарному середовищі дозволяють централізовано накопичувати та аналізувати інформацію з різних джерел у режимі реального або близького до реального часу. Використання розподілених обчислювальних платформ (Hadoop, Spark, хмарні аналітичні сервіси) забезпечує масштабованість і гнучкість, що є критично важливим для систем цивільного захисту, які працюють в умовах різко змінюваного навантаження під час надзвичайних ситуацій [1].

У практиці цивільної безпеки сервіси Big Data застосовуються для аналізу ризиків виникнення надзвичайних ситуацій, прогнозування розвитку небезпечних процесів, оптимізації розміщення сил і засобів реагування, а також для оцінювання наслідків НС. Поєднання великих даних із геоінформаційними системами дозволяє формувати просторово-часові моделі небезпек, які враховують історичні дані, поточні показники та прогнозні сценарії [7].

В Україні елементи технологій Big Data поступово впроваджуються у діяльність Державної служби України з надзвичайних ситуацій. Зокрема, ДСНС використовує великі масиви даних метеорологічних спостережень, гідрологічної інформації та супутникових знімків для прогнозування паводків, підтоплень і лісових пожеж. Дані Державної служби з надзвичайних ситуацій інтегруються з інформаційними ресурсами Українського гідрометеорологічного центру, що дозволяє аналізувати динаміку небезпечних природних явищ і завчасно готувати заходи реагування [8].

Практичним прикладом використання підходів Big Data є аналіз статистики пожеж в екосистемах України. ДСНС накопичує значні обсяги інформації про місця, час, причини та наслідки пожеж, які в подальшому використовуються для виявлення просторових і сезонних закономірностей, визначення територій підвищеного ризику та планування профілактичних заходів. Поєднання цих даних із супутниковою інформацією (зокрема даними дистанційного зондування Землі) дозволяє оперативно виявляти осередки загорянь і оцінювати масштаби ураження [9].

Ще одним напрямом застосування великих даних у ДСНС є аналіз інформації про надзвичайні ситуації техногенного характеру та аварії на об’єктах підвищеної небезпеки. Агрегація історичних даних про аварійність, технічний стан об’єктів, результати перевірок і наглядової діяльності створює передумови для ризик-орієнтованого підходу в управлінні цивільною безпекою. У перспективі такі дані можуть використовуватися для побудови прогнозних моделей і підтримки прийняття управлінських рішень [10].

Важливу роль сервіси Big Data відіграють і в обробці інформації від населення, зокрема повідомлень про надзвичайні події, що надходять через лінію 101, мобільні додатки

або цифрові платформи. Аналіз великих масивів таких повідомлень дозволяє виявляти типові сценарії НС, оцінювати навантаження на підрозділи ДСНС та оптимізувати логістику реагування. У поєднанні з елементами штучного інтелекту ці сервіси можуть забезпечувати автоматичну класифікацію подій і пріоритезацію викликів [11].

Використання сервісів для обробки великих даних в діяльності ДСНС України створює передумови для переходу від реактивної моделі реагування до проактивного, прогнозно-аналітичного управління ризиками надзвичайних ситуацій. Подальший розвиток цих сервісів пов'язаний із розширенням інтеграції даних, підвищенням кіберстійкості платформ та підготовкою фахівців, здатних ефективно працювати з великими масивами інформації в умовах кризових ситуацій.

9.3. Кіберстійкість платформ

Цифрові платформи та хмарні сервіси відіграють критично важливу роль у забезпеченні безперервного управління, моніторингу надзвичайних ситуацій, оповіщення населення та підтримки прийняття рішень. Водночас зростання рівня цифровізації підвищує залежність цих систем від кіберпростору, що зумовлює необхідність забезпечення їх кіберстійкості як складової національної та громадської безпеки.

Кіберстійкість цифрових платформ у системі цивільної безпеки розглядається як здатність інформаційних систем протистояти кіберзагрозам, зберігати працездатність у разі кібератак, швидко відновлюватися після інцидентів та адаптуватися до нових ризиків. На відміну від традиційної кібербезпеки, що зосереджується переважно на запобіганні несанкціонованому доступу, кіберстійкість охоплює повний життєвий цикл інциденту – від підготовки та захисту до реагування, відновлення і вдосконалення системи [12].

Для систем цивільного захисту кіберстійкість має особливе значення, оскільки порушення роботи цифрових платформ у кризовий момент може призвести до затримок в оповіщенні населення, втрати оперативної інформації або неправильних управлінських рішень. Умови воєнного стану та гібридних загроз посилюють актуальність проблеми, адже кібердари можуть бути спрямовані саме на критичну інформаційну інфраструктуру органів управління та реагування на надзвичайні ситуації [13].

Основними принципами забезпечення кіберстійкості платформ цивільної безпеки є багаторівневий захист, резервування ключових компонентів, сегментація мережі, постійний моніторинг подій безпеки та управління ризиками. Багаторівневий підхід передбачає одночасне застосування технічних, організаційних і програмних засобів захисту, включаючи шифрування даних, багатофакторну автентифікацію, контроль доступу та регулярне оновлення програмного забезпечення [2].

Важливим елементом кіберстійкості є забезпечення безперервності функціонування платформ. Для цього використовуються механізми резервного копіювання даних, географічно розподілені дата-центри, дублювання серверів та автоматичне перемикання на резервні ресурси у разі відмови основних компонентів. У хмарних середовищах такі можливості реалізуються за допомогою концепцій high availability та disaster recovery, що дозволяють мінімізувати втрати даних і часу простою систем [14].

Суттєву роль у підвищенні кіберстійкості відіграє управління кіберризиками. Воно включає ідентифікацію потенційних загроз, оцінювання їх імовірності та наслідків, а також розроблення заходів реагування. Для систем цивільної безпеки характерними є ризики витоку персональних даних, підміни інформації про обстановку, блокування каналів зв'язку або втручання в роботу систем оповіщення. Застосування стандартів управління інформаційною безпекою, зокрема ISO/IEC 27001 та рекомендацій NIST, дозволяє системно знижувати ці ризики [12].

Окрему увагу слід приділяти людському фактору, який залишається одним із найвразливіших елементів кіберстійкості. Недостатній рівень цифрової та кіберграмотності персоналу може призвести до успішних фішингових атак, витоку облікових даних або ненавмисного порушення політик безпеки. Тому важливою складовою кіберстійкості є

регулярне навчання працівників органів цивільного захисту основам кібергігієни, правилам роботи з інформаційними системами та алгоритмам дій у разі кіберінцидентів [6].

У міжнародній практиці кіберстійкість цифрових платформ цивільної безпеки розглядається як інтегрований компонент управління надзвичайними ситуаціями. Європейський Союз і НАТО рекомендують поєднувати технічні засоби захисту з організаційними процедурами кризового управління та міжвідомчої взаємодії. В Україні питання кіберстійкості інформаційних систем державних органів, зокрема у сфері цивільного захисту, регулюються законодавством про захист критичної інформаційної інфраструктури та національну кібербезпеку [15].

Комплексною характеристикою, яка визначає здатність цифрових рішень ефективно функціонувати в кризових умовах і НС у системах цивільної безпеки є кіберстійкість платформ. Забезпечення кіберстійкості платформ потребує поєднання сучасних технологій, нормативно-правового регулювання, управління ризиками та підготовки персоналу.

Питання для контролю знань

1. У чому полягає сутність хмарної інфраструктури та її відмінність від традиційних IT-систем?
2. Які основні моделі розгортання хмар існують і в чому їх принципові відмінності?
3. Які переваги використання хмарних технологій у системах цивільної безпеки?
4. Які ризики та обмеження пов’язані з використанням публічних хмар для державних інформаційних систем?
5. У яких випадках доцільно застосовувати гібридну хмарну модель у цивільному захисті?
6. Чим відрізняються моделі IaaS, PaaS та SaaS з точки зору рівня відповідальності користувача?
7. Як хмарна інфраструктура сприяє підвищенню оперативності реагування на надзвичайні ситуації?
8. Що розуміється під поняттям Big Data та які основні характеристики великих даних (Volume, Velocity, Variety, Veracity, Value) є найбільш критичними для систем цивільної безпеки?
9. Які типи даних використовуються у системах цивільної безпеки для аналізу надзвичайних ситуацій (метеорологічні, геопросторові, сенсорні, оперативні тощо)?
10. Які хмарні сервіси та платформи застосовуються для збирання, зберігання й обробки великих даних у сфері реагування на НС?
11. Яким чином технології Big Data використовуються ДСНС України для прогнозування надзвичайних ситуацій та підтримки управлінських рішень?
12. Яку роль відіграє аналіз супутникових даних, даних з дронів та автоматизованих систем спостереження у формуванні аналітичних моделей ДСНС?
13. Які переваги та обмеження використання технологій Big Data в діяльності органів цивільного захисту України в умовах воєнного стану?
14. Які вимоги до інформаційної безпеки та захисту персональних даних необхідно враховувати при використанні сервісів Big Data у системах ДСНС?
15. Що розуміють під поняттям кіберстійкість цифрових платформ, і чим воно відрізняється від традиційної кібербезпеки?
16. Які основні загрози кіберстійкості характерні для інформаційних систем цивільної безпеки в умовах надзвичайних ситуацій та воєнного стану?
17. Яку роль відіграють резервне копіювання та відновлення даних (backup & recovery) у забезпеченні безперервності функціонування систем цивільного захисту?
18. Як принципи відмовостійкості, надлишковості та розподіленості ресурсів реалізуються у хмарних платформах цивільної безпеки?
19. Яким чином людський фактор впливає на рівень кіберстійкості інформаційних систем, і які заходи дозволяють мінімізувати ці ризики?

20. Які міжнародні стандарти та нормативні документи регламентують питання кіберстійкості та інформаційної безпеки критичної інфраструктури?
21. У чому полягають переваги використання хмарних і гібридних платформ для підвищення кіберстійкості систем управління реагуванням на надзвичайні ситуації?

Список використаних джерел

1. Сидор К. В., Щербина Ю. М. Технологія хмарних обчислень: архітектура, моделі та аспекти інформаційної безпеки. Інформаційні системи та мережі. 2025. Т. 18, (частина 2). С. 184 – 191. URL: https://doi.org/10.23939/sisn2025.18.2.184.
2. БІЛА КНИГА. Управління ризиками надзвичайних ситуацій та системи цивільного захисту в контексті пріоритетів Сендайської рамкової програми зменшення ризиків надзвичайних ситуацій. Archive.r2p.org.ua. 25.10.2020. URL: https://archive.r2p.org.ua/wp-content/uploads/2020/10/white_book_risks_3p-consortium.pdf.
3. Buyya R., Broberg J., Goscinski A. Cloud Computing: Principles and Paradigms. – Hoboken : Wiley, 2011. – 664 p.
4. «Програмні комплекси підтримки прийняття рішень у сфері цивільного захисту»: Монографія / Віталій НУЯНЗІН, Артем Биченко, Максим Удовенко, Михайло Пустовіт, Ігор Маладика − Черкаси: ЧІПБ, 2024. − 204 с.
5. Armbrust M. et al. A View of Cloud Computing // Communications of the ACM. – 2010. – Vol. 53, No. 4. – P. 50–58. https://www.researchgate.net/publication/220422375_A_View_of_Cloud_Computing.
6. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – Geneva : ISO, 2022.
7. Longley P. A., Goodchild M. F., Maguire D. J., Rhind D. W. Geographic Information Systems and Science. – 4th ed. – Hoboken : Wiley, 2015. – 560 p.
8. Державна служба України з надзвичайних ситуацій. Офіційний вебсайт : інформаційні матеріали та аналітика [Електронний ресурс]. – Режим доступу: https://www.dsns.gov.ua
9. Copernicus Emergency Management Service. Wildfire monitoring and assessment [Electronic resource]. – Mode of access: https://emergency.copernicus.eu.
10. Кодекс цивільного захисту України : Закон України від 02.10.2012 № 5403-VI (зі змінами).
11. McKinsey Global Institute. Big data: The next frontier for innovation, competition, and productivity. – McKinsey & Company, 2011. – 156 p. https://www.researchgate.net/publication/312596137_Big_data_The_next_frontier_for_innovation_competition_and_productivity.
12. National Institute of Standards and Technology. Cyber Resilience Engineering Framework. – Gaithersburg : NIST, 2022. – Режим доступу: https://www.nist.gov.
13. European Union Agency for Cybersecurity (ENISA). Cybersecurity and resilience of critical infrastructure. – Brussels, 2021.
14. Amazon Web Services. Disaster Recovery and Business Continuity in the Cloud. – Режим доступу: https://aws.amazon.com
15. Закон України «Про основні засади забезпечення кібербезпеки України». – Відомості Верховної Ради України. – 2017. – № 45.

Тема 10. Мобільні застосунки та технології штучного інтелекту у прогнозуванні та реагуванні на надзвичайні ситуації

1. Додатки для оповіщення.
2. Додатки для навігації.
3. Додатки для зв’язку, координації дій під час НС.
4. Машинне навчання.
5. Аналіз великих даних.
6. Алгоритми для оцінки загроз.

10.1. Додатки для оповіщення.

У сучасних умовах цивільної безпеки мобільні додатки для оповіщення населення відіграють ключову роль у своєчасному інформуванні громадян про надзвичайні ситуації, загрози та рекомендації щодо безпечної поведінки. Такі додатки дозволяють не лише швидко передавати сигнали тривоги, але й забезпечують інтерактивну взаємодію між органами управління та населенням, що особливо важливо в умовах воєнного стану або стихійних лих [1; 2].

Принцип роботи мобільних додатків для оповіщення базується на інтеграції з автоматизованими системами оповіщення, геолокаційними сервісами та каналами передачі повідомлень різного типу: push-повідомлення, SMS, голосові виклики або сповіщення у месенджерах. Важливою складовою є можливість таргетування повідомлень за географічними зонами ризику, що дозволяє забезпечити адресне сповіщення для населення, яке перебуває у зоні потенційної небезпеки [2; 3].

До прикладів українських мобільних додатків для оповіщення належать “Порятунок”, “Повітряна тривога” та “Дія. Цифрова безпека”. Ці сервіси забезпечують миттєве надходження інформації про загрозу обстрілу, хімічне або техногенне ураження, а також надають рекомендації щодо дій у критичних ситуаціях. Наприклад, додаток “Повітряна тривога” інтегрується з державними системами сповіщення та автоматично сповіщає користувачів про включення сирен у конкретному регіоні, визначеному через GPS-позицію [1].

Функціональні можливості таких додатків включають не лише отримання повідомлень, а й формування зворотного зв’язку: користувачі можуть надсилати інформацію про місце знаходження, стан об’єктів чи пошкоджень, що дозволяє підвищити ефективність реагування рятувальних служб. Також додатки можуть містити інтегровані карти безпечних зон, укриттів і маршрути евакуації, що сприяє мінімізації ризиків для життя та здоров’я населення [1].

Особлива увага приділяється інтерфейсу та доступності додатків. Вони повинні бути зрозумілими користувачам різного віку та рівня цифрової грамотності, підтримувати локалізацію українською мовою та працювати на різних типах мобільних пристроїв. Такі принципи забезпечують високу швидкість реагування та широку охоплюваність населення, що критично важливо у кризових ситуаціях [2].

Мобільні додатки для оповіщення населення забезпечують своєчасну, таргетовану та зрозумілу інформацію, сприяють підвищенню психофізичної безпеки громадян у надзвичайних ситуаціях інтегруючи автоматизовані канали передачі сигналів, геолокаційні сервіси та функції зворотного зв’язку.

10.2. Додатки для навігації.

Мобільні додатки для навігації є важливою складовою сучасних систем цивільного захисту, забезпечуючи оперативну орієнтацію населення та персоналу у надзвичайних ситуаціях. Основна мета таких сервісів полягає у наданні актуальної інформації про безпечні маршрути, локації укриттів, розташування пунктів надання допомоги, а також оптимальні шляхи евакуації з небезпечних зон. Завдяки використанню GPS, геоміток та цифрових карт користувачі можуть отримати точну інформацію про своє поточне розташування і навігаційні інструкції в реальному часі [4].

Сучасні додатки для навігації інтегруються з державними інформаційними системами цивільного захисту та платформами обміну даними, що дозволяє оперативно оновлювати карти ризиків, повідомлення про надзвичайні події та рекомендації щодо дій у конкретному районі. Вони можуть працювати як автономно, так і в комплексі з іншими сервісами, наприклад, додатками для оповіщення або цифровими панелями управління реагуванням на надзвичайні ситуації [2; 5].

Особливу увагу приділено забезпеченню доступності таких додатків для всіх категорій населення, включаючи осіб із обмеженими фізичними можливостями та людей з низьким рівнем цифрової грамотності. Інтерфейс додатків передбачає зрозумілі графічні індикатори маршрутів, кольорове маркування небезпечних зон, а також голосові інструкції для підвищення ефективності використання у стресових умовах [5].

Важливим аспектом є інтеграція даних від різних джерел, зокрема Державної служби України з надзвичайних ситуацій (ДСНС), геоінформаційних систем та громадських платформ. Це дозволяє побудувати комплексну систему навігаційного супроводу, яка враховує динамічні зміни ситуації на місцях, наприклад, перекриття шляхів, руйнування інфраструктури або нові загрози. Таке поєднання даних забезпечує більш точне прогнозування руху населення та оптимізацію дій рятувальних служб [7; 8].

Інтерактивність додатків для навігації полягає у можливості користувачів повідомляти про локальні небезпеки, стан доріг чи наявність постраждалих. Ця функція сприяє не лише підвищенню інформованості населення, а й покращує роботу служб реагування завдяки зворотному зв’язку в реальному часі [5].

Мобільні додатки для навігації забезпечують ефективну координацію дій, зменшення ризиків та підвищення безпеки населення в умовах надзвичайних ситуацій.

10.3. Додатки для зв’язку, координації дій під час НС.

Мобільні додатки для зв’язку та координації дій під час надзвичайних ситуацій є ключовим елементом сучасних систем цивільного захисту. Вони забезпечують оперативну комунікацію між населенням, рятувальними службами та органами управління, що критично важливо під час природних катастроф, техногенних аварій чи воєнних загроз [3].

Такі додатки дозволяють передавати повідомлення про небезпеку, координувати дії підрозділів, повідомляти про місце знаходження постраждалих та стан критичної інфраструктури. Важливою функцією є можливість групового зв’язку між службами реагування, а також між громадянами та екстреними службами, що підвищує ефективність координації та швидкість реагування [5; 7].

Особливості мобільних сервісів для координації включають інтеграцію з геолокаційними даними, що дозволяє відстежувати розташування ресурсів та людей у реальному часі, а також визначати найближчі доступні засоби допомоги. Завдяки цьому можна оптимізувати маршрути рятувальних підрозділів і евакуаційні шляхи, мінімізуючи час реагування та підвищуючи безпеку населення.

Для підвищення ефективності роботи додатків реалізуються інтерактивні функції, зокрема: формування спільнот користувачів для обміну оперативною інформацією, автоматичне сповіщення про зміни ситуації, а також інтеграція з державними інформаційними системами ДСНС. Це забезпечує єдиний інформаційний простір для об’єднання дій різних структур і створення цілісного механізму управління кризовими ситуаціями [1; 2; 5].

Додатки можуть містити алгоритми автоматичного розподілу повідомлень залежно від пріоритетності, територіальної прив’язки та групи користувачів. Наприклад, спеціальні сповіщення надсилаються рятувальникам, місцевим органам влади або мешканцям певних районів, які знаходяться в зоні підвищеного ризику. Це забезпечує точне і оперативне реагування без перевантаження системи непотрібною інформацією (Петрова, 2021).

Інтерактивні сервіси також підтримують функції оцінки ризиків і звітності, дозволяючи користувачам передавати фото, відео та текстові повідомлення про надзвичайні події. Ці дані автоматично інтегруються до аналітичних платформ управління цивільним

захистом, що забезпечує своєчасну обробку інформації та прийняття ефективних рішень [1; 2; 5].

Мобільні додатки для зв'язку та координації дій під час НС сприяють підвищенню швидкості реагування служб ЦЗ та інтеграції з аналітичними системами і виконують ключову роль у забезпеченні безпеки населення.

10.4. Машинне навчання.

Розвиток цифрових технологій та зростання складності надзвичайних ситуацій природного і техногенного характеру зумовлюють потребу у впровадженні інтелектуальних інструментів підтримки управлінських рішень у сфері цивільної безпеки. Штучний інтелект (ШІ) дедалі активніше використовується для прогнозування розвитку небезпечних подій, оцінки масштабів можливих наслідків та оптимізації процесів реагування. Його застосування дозволяє підвищити швидкість обробки інформації, зменшити вплив людського фактора та забезпечити більш обґрунтовані рішення в умовах дефіциту часу та невизначеності.

Машинне навчання є одним із ключових напрямів штучного інтелекту, що ґрунтується на здатності алгоритмів навчатися на основі накопичених даних та виявляти приховані закономірності. У цивільній безпеці методи машинного навчання застосовуються для прогнозування виникнення надзвичайних ситуацій, наприклад паводків, лісових пожеж, аварій на потенційно небезпечних об'єктах, а також для оцінки ймовірності їх ескалації. Алгоритми класифікації та регресії використовуються для аналізу метеорологічних, гідрологічних, технічних і соціальних показників, що дозволяє формувати прогностичні моделі ризику та визначати критичні порогові значення параметрів.

Технології машинного навчання у сфері цивільної безпеки доцільно розглядати як складову сучасної цифрової трансформації систем прогнозування та реагування на надзвичайні ситуації. Машинне навчання є напрямом штучного інтелекту, що передбачає створення алгоритмів, здатних навчатися на основі даних, виявляти приховані закономірності та формувати прогностичні або класифікаційні рішення без жорстко заданих правил. У системах цивільної безпеки такі підходи набувають особливого значення в умовах зростання обсягів інформації, обмеженого часу на ухвалення рішень і необхідності підвищення точності прогнозів.

У контексті управління надзвичайними ситуаціями машинне навчання використовується для аналізу великих масивів різнорідних даних, що надходять із сенсорних систем, автоматизованих систем раннього виявлення загроз, метеорологічних спостережень, супутникових знімків, реєстрів ДСНС та інформаційних систем органів влади. Відповідно до положень Кодексу цивільного захисту України, інформаційне забезпечення є базовим елементом функціонування Єдиної державної системи цивільного захисту, а впровадження сучасних аналітичних інструментів сприяє підвищенню ефективності управління ризиками та реагуванням на надзвичайні ситуації [8; 10].

Алгоритми машинного навчання у цивільній безпеці застосовуються для прогнозування розвитку небезпечних подій, оцінки ймовірності їх виникнення та визначення можливих наслідків. Наприклад, методи регресійного аналізу та нейронних мереж можуть використовуватися для прогнозування рівнів підтоплення, поширення пожеж або динаміки небезпечних метеорологічних явищ. Класифікаційні моделі дають змогу автоматично визначати тип надзвичайної ситуації за сукупністю ознак, що надходять від датчиків або з повідомлень населення. Такі підходи відповідають концепції автоматизованих систем, визначених у ДСТУ 2226-93, як систем, що забезпечують обробку інформації та підтримку управлінських рішень із мінімальною участю людини [11].

Важливим напрямом використання машинного навчання є підвищення ефективності систем оповіщення населення. Аналіз поведінкових моделей користувачів, просторового розподілу населення та історичних даних про реагування на сигнали тривоги дає змогу оптимізувати алгоритми формування повідомлень, визначати пріоритетні канали оповіщення та прогнозувати швидкість реагування населення. Це узгоджується з вимогами

ДБН В.2.5-76:2014, які передбачають використання автоматизованих систем раннього виявлення загроз і оповіщення населення на основі сучасних інформаційних технологій [14].

Постанова Кабінету Міністрів України № 355 від 29 березня 2024 року визначає правові та організаційні засади функціонування загальнодержавної автоматизованої системи централізованого оповіщення. У цьому контексті машинне навчання може застосовуватися для інтелектуального аналізу даних, що надходять до системи, з метою підвищення точності і своєчасності оповіщення, а також для адаптації алгоритмів реагування до конкретних регіональних умов [9].

Практика діяльності ДСНС України свідчить про поступове впровадження елементів інтелектуальної аналітики в системи управління надзвичайними ситуаціями. На офіційному інформаційному ресурсі служби підкреслюється важливість використання сучасних цифрових технологій для підтримки управлінських рішень, координації сил і засобів та аналізу обстановки в режимі реального часу [10]. Машинне навчання в цьому контексті може розглядатися як інструмент переходу від реактивного до проактивного управління ризиками.

З теоретичної точки зору машинне навчання підсилює можливості традиційних методів аналізу, забезпечуючи більш глибоке опрацювання даних і зменшуючи суб'єктивний вплив людського чинника. Водночас його впровадження в системи цивільної безпеки потребує дотримання вимог до надійності, кібербезпеки та захисту інформації, а також нормативного узгодження з чинною правовою базою. Для майбутніх фахівців цивільної безпеки розуміння принципів машинного навчання є важливою передумовою ефективної роботи з сучасними автоматизованими системами прогнозування та реагування на надзвичайні ситуації.

10.5. Аналіз великих даних

У сучасних умовах зростання кількості надзвичайних ситуацій природного, техногенного та воєнного характеру особливого значення набуває використання аналізу великих даних (Big Data) як інструменту підтримки управлінських рішень у сфері цивільної безпеки. Великі дані дозволяють об'єднувати різнорідні інформаційні потоки, оперативно виявляти загрози, прогнозувати розвиток небезпечних подій та підвищувати ефективність реагування органів цивільного захисту [8].

Під великими даними розуміють масиви інформації, що характеризуються значним обсягом, високою швидкістю надходження та різноманітністю форматів, обробка яких традиційними методами є ускладненою. У сфері цивільної безпеки такими даними виступають оперативні зведення ДСНС, дані автоматизованих систем оповіщення, інформація з датчиків моніторингу, супутникові знімки, геоінформаційні дані, повідомлення з мобільних додатків та відкриті джерела інформації [11].

Нормативно-правові засади використання інформаційних та автоматизованих систем у цивільному захисті визначаються Кодексом цивільного захисту України, який передбачає створення і функціонування єдиних інформаційних систем для збору, обробки та аналізу даних про загрози і надзвичайні ситуації [8].

Важливу роль у цьому контексті відіграє загальнодержавна автоматизована система централізованого оповіщення, функціонування якої регламентується постановою Кабінету Міністрів України № 355 від 29 березня 2024 року, що прямо орієнтує систему на використання цифрових даних та аналітичних технологій [9].

Аналіз великих даних у цивільній безпеці реалізується через інтеграцію різних інформаційних джерел у межах інформаційно-аналітичних платформ. Такі платформи дозволяють здійснювати агрегацію даних у реальному часі, просторово-часовий аналіз, виявлення аномалій та закономірностей, що є критично важливим для раннього виявлення загроз та прогнозування розвитку надзвичайних ситуацій [12].

У практичній діяльності ДСНС України елементи аналізу великих даних використовуються для оцінювання оперативної обстановки, визначення пріоритетів

реагування, прогнозування зон ураження та ресурсного забезпечення аварійно-рятувальних робіт. Дані, отримані з автоматизованих систем раннього виявлення загроз, оповіщення населення та відомчих інформаційних ресурсів, формують єдине аналітичне середовище, що підвищує обґрунтованість управлінських рішень [13; 14; 15].

Важливою складовою аналізу великих даних є використання геоінформаційних технологій, які дозволяють поєднувати статистичні, оперативні та прогнозні дані з просторовою інформацією. Це забезпечує наочне відображення ризиків, зон можливого ураження, маршрутів евакуації та розміщення сил і засобів цивільного захисту, що відповідає вимогам сучасних інформаційних технологій у сфері безпеки та оборони [12; 14].

Аналіз великих даних тісно пов’язаний із розвитком алгоритмів машинного навчання та інтелектуального аналізу даних, які дозволяють автоматизувати процеси виявлення прихованих закономірностей і прогнозування. У системах цивільної безпеки такі підходи можуть застосовуватися для прогнозування кількості та масштабів надзвичайних ситуацій, оцінки ризиків для населення та об’єктів інфраструктури, а також оптимізації процесів оповіщення та реагування [12; 15].

Водночас використання великих даних у цивільному захисті потребує дотримання вимог інформаційної безпеки, захисту персональних даних та забезпечення надійності функціонування інформаційних систем. Це особливо актуально в умовах воєнного стану, коли інформаційні ресурси стають об’єктами кібератак і інформаційних впливів [8; 14].

Аналіз великих даних дає можливість підвищити оперативність, точність та ефективність управління надзвичайними ситуаціями, сприяє переходу від реактивного до превентивного управління ризиками, що є одним із пріоритетних напрямів розвитку сучасної системи цивільного захисту України.

10.6. Алгоритми для оцінки загроз у системах цивільної безпеки

Оцінка загроз є ключовим елементом управління цивільною безпекою та прийняття управлінських рішень у сфері запобігання і реагування на надзвичайні ситуації. В умовах зростання техногенних, природних і воєнних ризиків особливого значення набуває використання алгоритмів, здатних оперативно обробляти великі масиви різнорідних даних та формувати обґрунтовані прогнози щодо розвитку небезпечних подій. Алгоритмічні підходи дозволяють перейти від реактивної моделі управління до проактивної, орієнтованої на попередження загроз і мінімізацію їх наслідків.

У нормативно-правовому полі України оцінка загроз тісно пов’язана з функціонуванням Єдиної державної системи цивільного захисту, що передбачає моніторинг небезпечних факторів, аналіз ризиків та своєчасне оповіщення населення відповідно до Кодексу цивільного захисту України [15].

Сучасні алгоритми оцінки загроз інтегруються в автоматизовані системи оповіщення та управління реагуванням, визначені положеннями постанови Кабінету Міністрів України № 355 від 29 березня 2024 року [9].

Алгоритми для оцінки загроз у цивільній безпеці базуються на поєднанні математичних, статистичних, логічних та інтелектуальних методів. Класичні підходи включають детерміновані алгоритми, що використовують формалізовані правила та порогові значення показників небезпеки. Вони застосовуються, зокрема, у системах раннього виявлення надзвичайних ситуацій, регламентованих ДБН В.2.5-76:2014, де загроза визначається шляхом порівняння поточних параметрів із нормативно допустимими межами [14].

Поряд із детермінованими моделями широкого поширення набули ймовірнісні алгоритми оцінки загроз, які дозволяють враховувати невизначеність та випадковий характер розвитку подій. До таких алгоритмів належать методи статистичного аналізу, байєсівські мережі, дерева рішень і моделі Монте-Карло. Вони використовуються для оцінювання імовірності виникнення надзвичайної ситуації та можливих сценаріїв її розвитку з урахуванням різних чинників впливу, що є особливо актуальним у складних техногенних і природних системах [10].

Сучасний етап розвитку цивільної безпеки характеризується активним впровадженням інтелектуальних алгоритмів оцінки загроз, заснованих на методах штучного інтелекту та машинного навчання. Такі алгоритми здатні самонавчатися на основі історичних даних, інформації з сенсорних мереж, супутникового моніторингу та відомчих інформаційних ресурсів ДСНС України [10]. Вони забезпечують автоматизоване виявлення аномалій, класифікацію типів загроз і прогнозування наслідків надзвичайних ситуацій у режимі реального часу.

Важливим напрямом є використання алгоритмів багатокритеріальної оцінки загроз, які дозволяють одночасно враховувати технічні, природні, соціальні та просторові чинники ризику. Такі алгоритми формують інтегральні показники рівня загрози та використовуються в системах підтримки прийняття рішень органів управління цивільним захистом. Вони відповідають термінології та класифікації автоматизованих систем, визначених у ДСТУ 2226-93 [11].

У практиці ДСНС алгоритми оцінки загроз застосовуються для визначення необхідності запуску систем централізованого оповіщення населення, вибору каналів передачі сигналів та планування заходів реагування. Інформація, отримана в результаті алгоритмічної обробки даних, використовується для формування управлінських рішень щодо евакуації, локалізації аварій і координації дій аварійно-рятувальних підрозділів [13; 15].

Розвиток і впровадження алгоритмів для оцінки загроз забезпечує підвищення точності прогнозів, скорочення часу реагування та зменшення людських і матеріальних втрат у разі надзвичайних ситуацій, також сприяє процесу цифровізації систем управління ризиками.

Питання для контролю знань

1. Які основні функції виконують мобільні додатки для оповіщення населення у системі цивільної безпеки?
2. Як працює механізм геотаргетованого сповіщення у мобільних додатках для оповіщення?
3. Назвіть українські мобільні додатки для оповіщення населення та охарактеризуйте їхні основні функції.
4. Яку роль відіграє інтеграція додатків для оповіщення з автоматизованими системами цивільного захисту?
5. Які способи передачі сигналів використовуються мобільними додатками для оповіщення населення?
6. Як функції зворотного зв’язку у мобільних додатках підвищують ефективність реагування на надзвичайні ситуації?
7. Які вимоги до інтерфейсу та доступності мобільних додатків забезпечують їхню ефективність серед різних категорій користувачів?
8. Яку роль відіграють мобільні навігаційні додатки у забезпеченні безпеки населення під час надзвичайних ситуацій?
9. Які типи навігаційних даних використовуються у додатках для цивільного захисту та як вони оновлюються в умовах НС?
10. У чому полягає значення геолокаційних сервісів для планування маршрутів евакуації населення?
11. Які функціональні можливості навігаційних додатків є найбільш критичними для рятувальних підрозділів під час реагування на НС?
12. Як інтеграція навігаційних додатків з інформаційними системами ДСНС підвищує ефективність управління реагуванням?
13. Які ризики та обмеження існують при використанні навігаційних додатків у зонах зруйнованої інфраструктури або відсутності зв’язку?

14. Які напрями розвитку навігаційних мобільних застосунків є перспективними для системи цивільної безпеки України?

15. Яку роль відіграють мобільні додатки зв'язку в системі управління реагуванням на надзвичайні ситуації?

16. Які основні функції координації дій реалізуються в мобільних застосунках цивільного захисту?

17. Як використання геолокаційних сервісів у додатках підвищує ефективність реагування під час НС?

18. Які переваги має інтеграція мобільних додатків із державними інформаційними системами ДСНС?

19. Які типи інформації можуть передаватися користувачами через додатки для координації дій під час НС?

20. У чому полягає значення пріоритетної та адресної передачі повідомлень у кризових мобільних сервісах?

21. Які ризики та обмеження використання мобільних додатків для зв'язку й координації дій в умовах надзвичайних ситуацій?

22. Що таке машинне навчання та які його основні відмінності від традиційних алгоритмічних підходів в автоматизованих системах цивільного захисту?

23. Які типи машинного навчання (контрольоване, неконтрольоване, навчання з підкріпленням) можуть застосовуватися у прогнозуванні надзвичайних ситуацій?

24. Які джерела даних використовуються для навчання моделей машинного навчання у системах цивільної безпеки (з урахуванням діяльності ДСНС України)?

25. Як методи машинного навчання можуть підвищити ефективність систем раннього виявлення загроз та оповіщення населення відповідно до вимог Кодексу цивільного захисту України?

26. Яку роль відіграє машинне навчання в аналізі великих даних для підтримки управлінських рішень під час реагування на надзвичайні ситуації?

27. Які ризики та обмеження пов'язані з використанням машинного навчання у критичних системах цивільного захисту (помилки моделей, якість даних, кіберзагрози)?

28. Як нормативно-правові акти України (ДБН, ДСТУ, постанови КМУ) впливають на впровадження та використання технологій машинного навчання в автоматизованих системах оповіщення та управління НС?

29. Що розуміють під аналізом великих даних (Big Data) та які його ключові характеристики у сфері цивільної безпеки?

30. Які основні джерела великих даних використовуються ДСНС України для прогнозування та управління надзвичайними ситуаціями?

31. Яку роль відіграє аналіз великих даних у функціонуванні автоматизованих систем оповіщення населення?

32. Які методи та інструменти аналізу великих даних застосовуються для оцінки ризиків і наслідків надзвичайних ситуацій?

33. Як інтегрується аналіз великих даних з геоінформаційними системами та системами підтримки прийняття рішень у цивільному захисті?

34. Які нормативно-правові документи України регламентують використання інформаційних ресурсів і великих даних у сфері цивільного захисту?

35. Що розуміють під алгоритмами оцінки загроз у системі цивільного захисту та яке їх призначення?

36. Які основні етапи включає процес алгоритмічної оцінки загроз виникнення надзвичайних ситуацій?

37. Які типи даних використовуються алгоритмами оцінки загроз у діяльності ДСНС України?

38. У чому полягає відмінність між детермінованими та імовірнісними алгоритмами оцінки загроз?

39. Які переваги та обмеження використання алгоритмів штучного інтелекту для оцінки загроз у сфері цивільної безпеки?

Список використаних джерел

1. «MineFree» - новий мобільний застосунок дбає про безпеку громадян. Державна служба України з надзвичайних ситуацій. 08.08.2022. URL: https://dsns.gov.ua/news/ostanni-novini/minefree-novii-mobilnii-zastosunok-dbaje-pro-bezpeku-gromadyan.
2. Красномовець П. Увага! Екстрене сповіщення! ДСНС вперше застосувала нову систему для реальної загрози. Як вона працює. Forbes. 11.07.2023. URL: https://forbes.ua/innovations/uvaga-spovishchennya-dsns-testuvati-sistemu-zavershili-yak-vona-pratsyuvatime-29092022-8681.
3. Андрієнко М. В., Дячкова О. М., Борисов А. В., Соколенко О. І. Інформаційна система державного оповіщення при виникненні надзвичайних ситуацій в Україні. Державне управління: удосконалення та розвиток. 2019. № 5. – URL: http://www.dy.nayka.com.ua/?op=1&z=1428.
4. World Health Organization. Mental health in emergencies. Режим доступу: https://www.who.int/news-room/fact-sheets/detail/mental-health-in-emergencies
5. Мобільні додатки, що здатні допомогти під час небезпечної ситуації. Сильні. URL:https://cutt.ly/jtbYlSbK.
6. Інноваційні трансформації в сучасній освіті: виклики, реалії, стратегії: зб. матеріалів IV Всеукр. відкр. наук.-практ. онлайн-форуму, Київ, 27 жовт. 2022 р. / за заг. ред. І. М. Савченко, В. В. Ємець. — Київ : Національний центр «Мала академія наук України», 2022. — 588 с. ISBN 978-617-7945-04-7
7. Федорчук-Мороз В., Рудинець М. Підвищення рівня культури безпеки та зниження психосоціальних ризиків на підприємствах в умовах воєнного стану // Вісті Донецького гірничого інституту. – 2024. – № 2. – С. 128-137. URL: https://doi.org/10.31474/1999-981X-2024-2-128-137.
8. Кодекс цивільного захисту України : Закон України від 02.10.2012 № 5403-VI. – Режим доступу: https://zakon.rada.gov.ua/laws/show/5403-17#Text.
9. Деякі питання функціонування загальнодержавної автоматизованої системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій : постанова Кабінету Міністрів України від 29 березня 2024 р. № 355. – Режим доступу: https://zakon.rada.gov.ua/laws/show/355-2024-%D0%BF#Text
10. Державна служба України з надзвичайних ситуацій. Управління надзвичайними ситуаціями : офіційний сайт. – Режим доступу: https://dsns.gov.ua/.
11. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. – Київ : Держстандарт України, 1993. – 26 с.
12. Сучасні інформаційні технології у сфері безпеки та оборони [Електронний ресурс]. – Режим доступу: https://sit.nuou.org.ua/article/view/275444.
13. Білоусов С. І. Об’єктові, локальні та спеціальні автоматизовані системи оповіщення цивільного захисту : навч. посіб. / С. І. Білоусов. – Одеса : ОНАЗ ім. О. С. Попова, 2013. – 44 с.
14. ДБН В.2.5-76:2014. Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення. – Київ : Мінрегіон України, 2014. – 64 с.
15. ДСНС України. Система оповіщення населення. – Режим доступу: https://dsns.gov.ua/news/ostanni-novini/sistema-opovishhennia-naselennia-civilnii-zaxist-ta-borotba-iz-zagrozami-z-povitria-predstavniki-mvs-polshhi-iz-oficiinim-vizitom-vidvidali-ukrayinu.

Тема 11. Інформаційна безпека та захист даних в автоматизованих системах цивільної безпеки

1. Кібербезпека.
2. Захист інформації.
3. Загрози інформаційним системам.

11.1. Кібербезпека

В умовах цифровізації управління та зростання ролі інформаційно-комунікаційних технологій питання інформаційної безпеки набуває критичного значення, оскільки порушення цілісності, доступності або конфіденційності даних може призвести до збоїв у реагуванні на надзвичайні ситуації та створити загрозу життю і здоров'ю населення.

Кібербезпека в автоматизованих системах цивільної безпеки розглядається як комплекс організаційних, технічних та програмних заходів, спрямованих на захист інформаційних ресурсів, мереж і сервісів від кіберзагроз. Згідно з національними нормативно-правовими актами, кібербезпека є складовою національної безпеки та охоплює захист державних інформаційних ресурсів, критичної інформаційної інфраструктури та автоматизованих систем управління у сфері цивільного захисту. Для систем цивільної безпеки особливо важливими є вимоги до безперервності функціонування, стійкості до зовнішніх і внутрішніх впливів та здатності швидко відновлювати роботу після інцидентів кібербезпеки [1; 2].

У сучасних умовах цифровізації систем цивільного захисту кібербезпека набуває стратегічного значення, оскільки автоматизовані системи управління, оповіщення населення, моніторингу ризиків і підтримки прийняття рішень функціонують на основі інформаційно-комунікаційних технологій. Порушення їхньої цілісності, доступності або конфіденційності може призвести до дезорганізації реагування на надзвичайні ситуації та створити додаткові загрози життю і здоров'ю населення.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як захищеність життєво важливих інтересів людини, суспільства і держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та своєчасне виявлення, запобігання і нейтралізація кіберзагроз [1].

У сфері цивільної безпеки це поняття безпосередньо пов'язане з надійністю функціонування автоматизованих систем раннього виявлення загроз та централізованого оповіщення населення [3; 8].

Кібербезпека автоматизованих систем цивільного захисту базується на комплексному підході, що включає правові, організаційні та технічні заходи. Нормативно-правову основу становлять Кодекс цивільного захисту України, законодавство у сфері кібербезпеки, а також галузеві нормативні документи, зокрема ДСТУ 2226-93, який визначає термінологічні засади функціонування автоматизованих систем, і ДБН В.2.5-76:2014, що регламентує вимоги до систем раннього виявлення надзвичайних ситуацій та оповіщення населення [7–9].

Особливу роль у забезпеченні кібербезпеки відіграють автоматизовані системи централізованого оповіщення, які відповідно до постанови Кабінету Міністрів України № 355 від 29 березня 2024 року функціонують як загальнодержавна інформаційно-телекомунікаційна система з високими вимогами до захисту інформації та безперервності роботи [3]. Уразливість таких систем до кібератак може призвести до несвоєчасного або спотвореного інформування населення про загрозу, що істотно підвищує ризики негативних наслідків надзвичайних ситуацій.

Технічні заходи кібербезпеки в системах цивільної безпеки включають застосування захищених каналів передачі даних, криптографічних засобів захисту інформації, систем резервного копіювання та відновлення даних, а також багаторівневих механізмів автентифікації й авторизації користувачів. Важливим є також сегментування мереж та

ізоляція критичних компонентів системи від відкритого кіберпростору, що знижує ймовірність несанкціонованого доступу [4; 5].

Організаційні аспекти кібербезпеки передбачають визначення відповідальних осіб за захист інформації, розроблення планів реагування на кіберінциденти, регулярне проведення аудитів інформаційної безпеки та навчання персоналу. Для підрозділів ДСНС України це означає необхідність інтеграції кібербезпекових процедур у загальну систему управління надзвичайними ситуаціями, що підкреслюється у матеріалах офіційного вебпорталу служби [6].

У контексті гібридних загроз і воєнного стану кібербезпека систем цивільного захисту розглядається як складова національної безпеки. Кібератаки на інформаційні ресурси ДСНС, системи оповіщення або аналітичні платформи можуть мати ознаки цілеспрямованого впливу з боку противника, що вимагає тісної координації між суб'єктами сектору безпеки і оборони [1; 4].

Кібербезпека в автоматизованих системах цивільної безпеки забезпечує стійке функціонування систем оповіщення та управління реагуванням на надзвичайні ситуації, що є ключовою умовою захисту населення і територій.

11.2. Захист інформації.

Захист інформації в автоматизованих системах цивільної безпеки базується на принципах законності, комплексності, безперервності та адекватності рівня захисту реальним загрозам. Інформація, що обробляється в таких системах, може мати різний рівень доступу – від відкритої до службової або такої, що містить обмежений доступ. Захист інформації передбачає реалізацію заходів криптографічного та технічного захисту, ідентифікації та автентифікації користувачів, розмежування прав доступу, резервного копіювання та архівування даних. Особлива увага приділяється захисту персональних даних, а також інформації про об'єкти критичної інфраструктури, укриття, маршрути евакуації та системи оповіщення населення [3; 4].

Захист інформації є однією з ключових складових функціонування автоматизованих систем цивільної безпеки, оскільки ці системи забезпечують збирання, оброблення, зберігання та передавання критично важливих даних про загрози, надзвичайні ситуації, ресурси реагування та оповіщення населення. Порушення цілісності, конфіденційності або доступності такої інформації може призвести до збоїв в управлінні, несвоєчасного оповіщення та зростання ризиків для життя і здоров'я населення, що прямо суперечить завданням цивільного захисту, визначеним Кодексом цивільного захисту України.

У нормативно-правовому полі України захист інформації тісно пов'язаний із забезпеченням кібербезпеки та інформаційної безпеки держави. Закон України «Про основні засади забезпечення кібербезпеки України» визначає захист інформації як комплекс організаційних, правових та технічних заходів, спрямованих на запобігання несанкціонованому доступу, знищенню, модифікації або блокуванню інформації в інформаційно-комунікаційних системах, у тому числі тих, що використовуються в системах цивільного захисту [1]. Відповідно до цього підходу, автоматизовані системи оповіщення та управління реагуванням на НС мають функціонувати з урахуванням вимог захисту інформації на всіх етапах їх життєвого циклу.

Теоретично захист інформації ґрунтується на класичній тріаді безпеки: конфіденційність, цілісність і доступність. Конфіденційність передбачає обмеження доступу до службової та персональної інформації, що обробляється в системах цивільної безпеки, зокрема даних про об'єкти критичної інфраструктури, плани реагування та канали оповіщення. Цілісність означає збереження достовірності інформації та недопущення її несанкціонованої зміни, що є критично важливим для аналітичних моделей і алгоритмів оцінки загроз. Доступність полягає в забезпеченні безперервного доступу уповноважених користувачів до інформаційних ресурсів навіть в умовах надзвичайних ситуацій або кіберінцидентів, що прямо пов'язано з надійністю систем оповіщення та управління [10; 11].

У практиці цивільної безпеки захист інформації реалізується через поєднання організаційних, технічних і програмних заходів. Організаційні заходи включають розмежування прав доступу до інформаційних ресурсів, визначення відповідальних осіб, розроблення політик інформаційної безпеки та проведення навчання персоналу ДСНС і інших суб'єктів Єдиної державної системи цивільного захисту. Саме людський фактор часто залишається найуразливішою ланкою в системі захисту інформації, тому підвищення інформаційної культури та дисципліни користувачів є важливим елементом профілактики інцидентів [13; 15].

Технічні заходи захисту інформації охоплюють використання апаратних і програмно-апаратних засобів, таких як міжмережеві екрани, системи виявлення вторгнень, засоби резервного копіювання та фізичний захист серверного обладнання. У контексті автоматизованих систем оповіщення населення, вимоги до технічного захисту інформації узгоджуються з положеннями ДБН В.2.5-76:2014, які передбачають надійність каналів передавання сигналів, резервування елементів системи та захист від несанкціонованого втручання [8]. Аналогічні вимоги містяться й у положеннях ДСТУ 2226-93, який визначає базові терміни та принципи функціонування автоматизованих систем [7].

Програмні засоби захисту інформації відіграють особливо важливу роль у сучасних цифрових платформах цивільної безпеки. До них належать засоби автентифікації та авторизації користувачів, криптографічний захист інформації, журнали подій безпеки, а також механізми контролю цілісності даних. У навчальних посібниках з інформаційної безпеки наголошується, що криптографічні методи є ключовими для захисту інформації під час передавання даних між елементами автоматизованих систем, зокрема між центральними пунктами управління та об'єктами оповіщення [10; 12; 13; 14].

Особливого значення захист інформації набуває в загальнодержавній автоматизованій системі централізованого оповіщення, функціонування якої регламентовано постановою Кабінету Міністрів України № 355 від 29 березня 2024 року. Цей документ передбачає вимоги до захисту інформаційних ресурсів системи, стійкості до технічних збоїв і протидії несанкціонованому доступу, що є складовою загальної безпеки держави в умовах воєнних і техногенних загроз [3].

Захист інформації в автоматизованих системах цивільної безпеки слід розглядати як комплексну проблему, що поєднує правові, організаційні та технічні аспекти. Ефективна реалізація заходів захисту інформації забезпечує надійність функціонування систем оповіщення та управління реагуванням на надзвичайні ситуації, підвищує стійкість Єдиної державної системи цивільного захисту та сприяє зниженню ризиків для населення і територій.

11.3. Загрози інформаційним системам у сфері цивільної безпеки

В умовах цифровізації процесів управління цивільним захистом інформаційні системи стають критично важливими елементами забезпечення безпеки населення, функціонування систем оповіщення, управління реагуванням на надзвичайні ситуації та координації дій сил цивільного захисту. Водночас зростання ролі автоматизованих систем супроводжується збільшенням спектра загроз, які можуть порушити їхню працездатність, достовірність інформації та безперервність управління.

Згідно із Законом України «Про основні засади забезпечення кібербезпеки України», загрози інформаційним системам охоплюють сукупність факторів і умов, що створюють небезпеку несанкціонованого доступу, порушення цілісності, конфіденційності та доступності інформації, а також стабільності функціонування інформаційно-телекомунікаційних систем держави [1]. Для систем цивільної безпеки такі загрози мають особливу вагу, оскільки їх реалізація може призвести до несвоєчасного оповіщення населення, помилкових управлінських рішень або зриву заходів реагування на надзвичайні ситуації.

У науковій та нормативній літературі загрози інформаційним системам класифікуються за джерелом виникнення, характером впливу та рівнем реалізації [10; 11; 14].

За джерелом походження виокремлюють зовнішні та внутрішні загрози. Зовнішні загрози пов'язані з діяльністю кіберзлочинців, хакерських угруповань, диверсійних структур, а також із поширенням шкідливого програмного забезпечення через глобальні та корпоративні мережі [12; 15]. Внутрішні загрози зумовлені помилками персоналу, низьким рівнем інформаційної культури, зловживанням службовими повноваженнями або порушенням регламентів експлуатації інформаційних систем [13].

За характером впливу загрози поділяються на загрози конфіденційності, цілісності та доступності інформації [10; 14]. Порушення конфіденційності проявляється у витоку службової, персональної або критично важливої інформації, зокрема даних про об'єкти підвищеної небезпеки, захисні споруди цивільного захисту чи маршрути евакуації. Загрози цілісності пов'язані з несанкціонованою модифікацією даних, підміною сигналів оповіщення або спотворенням інформації в системах підтримки прийняття рішень. Загрози доступності полягають у блокуванні доступу до інформаційних ресурсів або виведенні з ладу автоматизованих систем, що є критично небезпечним під час надзвичайних ситуацій [15].

Окрему групу становлять кіберзагрози, що реалізуються через цілеспрямовані атаки на інформаційно-телекомунікаційні системи. До них належать атаки типу DDoS, впровадження шкідливого програмного забезпечення, фішингові кампанії, атаки на ланцюги постачання програмного забезпечення та експлуатація вразливостей програмно-апаратних компонентів [1; 14]. У системах цивільної безпеки такі атаки можуть призводити до порушення функціонування автоматизованих систем оповіщення та управління реагуванням, що регламентуються ДБН В.2.5-76:2014 і постановою Кабінету Міністрів України № 355 від 29 березня 2024 року [9; 13].

Суттєвим джерелом загроз є також технічні та технологічні чинники. До них належать фізичний знос обладнання, відмови апаратних засобів, перебої електроживлення, а також вплив надзвичайних ситуацій природного чи техногенного характеру на елементи інформаційної інфраструктури [5; 7]. У контексті цивільного захисту ці загрози мають комплексний характер, оскільки часто поєднуються з іншими небезпечними факторами та ускладнюють процес управління реагуванням [9].

Людський фактор залишається одним із найбільш уразливих елементів системи інформаційної безпеки. Недостатній рівень підготовки персоналу, ігнорування вимог захисту інформації, використання слабких паролів, необережна робота з електронною поштою та зовнішніми носіями інформації значно підвищують імовірність реалізації загроз [10; 13]. Дослідження у сфері інформаційної безпеки підкреслюють, що саме помилки користувачів часто стають початковою ланкою складних кіберінцидентів [14; 15].

У сфері цивільної безпеки загрози інформаційним системам мають системний вплив і можуть призводити до порушення виконання функцій Єдиної державної системи цивільного захисту, визначених Кодексом цивільного захисту України [9]. Саме тому їх ідентифікація, аналіз і мінімізація є складовою державної політики у сфері національної, інформаційної та кібернетичної безпеки [1].

Загрози інформаційним системам у цивільній безпеці мають багатовимірний характер і охоплюють кібернетичні, технічні, організаційні та людські аспекти. Розуміння природи цих загроз є необхідною передумовою формування ефективних систем захисту інформації, забезпечення стійкості автоматизованих систем управління та надійного функціонування механізмів оповіщення і реагування на надзвичайні ситуації.

Питання для контролю знань

1. У чому полягає сутність кібербезпеки як складової національної та цивільної безпеки?

2. Які основні об’єкти кіберзахисту в автоматизованих системах цивільної безпеки?
3. Які принципи забезпечення кібербезпеки визначені Законом України «Про основні засади забезпечення кібербезпеки України»?
4. Які типові кіберзагрози характерні для автоматизованих систем оповіщення та управління реагуванням на НС?
5. Яку роль відіграють ДСНС України та інші суб’єкти сектору безпеки у забезпеченні кібербезпеки?
6. Які організаційні та технічні заходи застосовуються для підвищення кіберстійкості систем цивільного захисту?
7. Як кіберінциденти можуть впливати на ефективність реагування на надзвичайні ситуації?
8. Що розуміють під захистом інформації в автоматизованих системах цивільної безпеки?
9. Які основні властивості інформації підлягають захисту відповідно до класичної моделі (конфіденційність, цілісність, доступність)?
10. Які нормативно-правові акти України регламентують захист інформації в інформаційних системах цивільного захисту?
11. Які методи та засоби технічного захисту інформації застосовуються в автоматизованих системах оповіщення?
12. У чому полягає різниця між організаційними, програмними та криптографічними заходами захисту інформації?
13. Які вимоги до захисту інформації встановлюються для державних та відомчих інформаційних ресурсів ДСНС?
14. Яку роль відіграє захист інформації у забезпеченні надійності та безперервності функціонування систем цивільної безпеки?
15. Які основні класи загроз інформаційним системам виділяють у теорії та практиці інформаційної безпеки?
16. У чому полягає відмінність між зовнішніми та внутрішніми загрозами інформаційним системам цивільної безпеки?
17. Які кіберзагрози є найбільш критичними для автоматизованих систем оповіщення та управління реагуванням на надзвичайні ситуації?
18. Як впливають людський фактор і помилки персоналу на рівень загроз інформаційним системам?
19. Які види програмних загроз (шкідливе ПЗ, атаки типу DoS/DDoS, фішинг тощо) становлять небезпеку для систем цивільного захисту?
20. Яким чином порушення цілісності, конфіденційності та доступності інформації може вплинути на функціонування систем цивільної безпеки?
21. Які нормативно-правові акти України регламентують ідентифікацію та нейтралізацію загроз інформаційним системам у сфері цивільного захисту?

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19.
2. ДСНС України. Система оповіщення населення : офіційний вебпортал. – Режим доступу: https://dsns.gov.ua/.
3. Деякі питання функціонування загальнодержавної автоматизованої системи централізованого оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій : постанова Кабінету Міністрів України від 29 березня 2024 р. № 355. – Режим доступу: https://zakon.rada.gov.ua/laws/show/355-2024-%D0%BF#Text.
4. Сучасні інформаційні технології у сфері безпеки та оборони : науковий журнал. – Режим доступу: https://sit.nuou.org.ua/article/view/275444.

5. Білоусов С. І. Об’єктові, локальні та спеціальні автоматизовані системи оповіщення цивільного захисту : навч. посіб. / С. І. Білоусов. – Одеса : ОНАЗ ім. О. С. Попова, 2013. – 44 с.

6. Державна служба України з надзвичайних ситуацій : інформація про управління надзвичайними ситуаціями. – Режим доступу: https://dsns.gov.ua/.

7. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення. – Чинний від 1994-01-01. – Київ : Держстандарт України, 1993.

8. ДБН В.2.5-76:2014. Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення. – Київ : Мінрегіон України, 2014.

9. Кодекс цивільного захисту України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/5403-17#Text

10. Полторак В. П. Інформаційна безпека та захист даних в комп’ютерних технологіях і мережах [Електронний ресурс] : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с. URL: https://ec.lib.vntu.edu.ua/DocumentView?doc_id=335470.

11. Інформаційна безпека та захист даних в комп’ютерних технологіях і мережах. Вибрані розділи [Електронний ресурс] : навч. посіб. / уклад. В. П. Полторак, О. В. Савчук. Київ : КПІ ім. Ігоря Сікорського, 2021. 385 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/90931384-5ce9-4adf-a32f-37210eebd3cb/content

12. Технології захисту інформації в інформаційно-телекомунікаційних системах [Електронний ресурс] : навч. посіб. / А. В. Жилін та ін. Київ : КПІ ім. Ігоря Сікорського, 2021. 213 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/d99a0045-e907-4d17-afc1-5431f67d2444/content

13. Півоварова С. В., Виганяйло С. М. Безпека та захист в інформаційних системах // Міжнародна та національна безпека: теоретичні і прикладні аспекти : матеріали VIII Міжнар. наук.-практ. конф. Дніпро : ДДУВС, 2024. Ч. ІІ. С. 377–378.

14. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с. https://files.znu.edu.ua/files/Bibliobooks/Inshi84/0063833.pdf.

15. Костюк Ю. В. Системи захисту інформації : підручник / Ю.В. Костюк, П.М. Складанний, Г.М. Гулак, Б.Т. Бебешко, К.В. Хорольська, С.Л. Рзаєва. – Київ : Київський столичний університет імені Бориса Грінченка, 2025. – 887 с. https://elibrary.kubg.edu.ua/id/eprint/51359/1/Kostiuk_Y_Skladannyi_P_Hulak_H_Bebeshko_B_Khorolska_K_Rzaieva_S_SZI_2025_FITM.pdf.

Тема 12. Віртуальна, доповнена реальність та перспективні цифрові технології у сфері цивільної безпеки

1. VR/AR-тренажери.
2. Симуляційні моделі.
3. Практичні кейси навчання рятувальників.
4. Інтернет речей (IoT).
5. Сенсорні мережі.
6. Роботизовані системи.
7. Цифрові двійники об’єктів.

12.1. VR/AR-тренажери

Сучасний етап розвитку системи цивільної безпеки характеризується активним упровадженням цифрових технологій у процес підготовки фахівців, зокрема технологій віртуальної (Virtual Reality, VR) та доповненої реальності (Augmented Reality, AR). VR/AR-тренажери є інноваційним навчальним інструментом, що забезпечує моделювання складних, небезпечних або рідкісних надзвичайних ситуацій у контрольованому віртуальному середовищі, без ризику для життя і здоров’я учасників навчання [8].

Віртуальна реальність створює повністю імерсивне цифрове середовище, у якому користувач взаємодіє з моделлю надзвичайної ситуації як з реальною, тоді як доповнена реальність накладає цифрові об’єкти, підказки та сценарії на реальний фізичний простір. Поєднання цих технологій дозволяє формувати комплексні VR/AR-тренажери для підготовки рятувальників, диспетчерів, керівників підрозділів цивільного захисту та фахівців з управління ризиками [2].

Наукові дослідження підтверджують високу ефективність VR-тренажерів у навчанні реагуванню на надзвичайні ситуації. Зокрема, систематичний огляд Abdulmajeed Alshowair та співавторів доводить, що VR-вправи підвищують рівень ситуаційної обізнаності, швидкість прийняття рішень і стресостійкість персоналу під час підготовки до катастроф та масових інцидентів [1]. Аналогічні висновки отримано у роботах, присвячених навчанню перших реагувальників при масових ураженнях, де VR-тренажери дозволяють відпрацьовувати складні сценарії з великою кількістю постраждалих [3].

У сфері цивільної безпеки VR/AR-тренажери використовуються для моделювання пожеж, вибухів, хімічних і радіаційних аварій, повеней, руйнувань будівель, дорожньо-транспортних пригод, а також для тренування дій у зоні бойових уражень та техногенних катастроф. Віртуальні сценарії дозволяють багаторазово відпрацьовувати алгоритми евакуації, пошуку і рятування постраждалих, взаємодію між службами та роботу з автоматизованими системами оповіщення [4; 9].

Доповнена реальність набуває особливого значення у практичній підготовці, оскільки дозволяє поєднувати реальні об’єкти з цифровими інструкціями, підказками та маркерами небезпек. За допомогою AR-технологій фахівці можуть відпрацьовувати дії з реальним обладнанням, отримуючи візуалізовану інформацію про небезпечні зони, послідовність операцій або можливі помилки. Це суттєво підвищує якість практичної підготовки та знижує ризик помилок у реальних умовах [7].

Українські дослідження підтверджують доцільність використання VR/AR-тренажерів у проєктах системи захисту населення від надзвичайних ситуацій. Зокрема, у роботах М. В. Рудинця та В. І. Федорчук-Мороз обґрунтовано застосування віртуальної реальності як інноваційного елементу підвищення готовності персоналу до реагування на НС та управління ризиками [5]. Також доведено ефективність використання 3D-ігрових та VR-середовищ у формуванні проєктних і управлінських компетентностей студентів спеціальностей безпекового профілю [6].

Важливою перевагою VR/AR-тренажерів є можливість адаптації сценаріїв до вимог національного законодавства та нормативної бази у сфері цивільного захисту. Тренажери можуть бути інтегровані з положеннями Кодексу цивільного захисту України, а також з

практиками і стандартами, які застосовуються в діяльності Державної служби України з надзвичайних ситуацій [9; 10]. Це забезпечує відповідність навчання реальним умовам функціонування Єдиної державної системи цивільного захисту.

Використання VR/AR-тренажерів сприяє поєднанню імерсивності, інтерактивності і практичної спрямованості у фахівців цивільної безпеки, а також формуванню професійних компетентностей, підвищенню готовності до дій у надзвичайних ситуаціях та розвитку навичок управління ризиками в умовах високої невизначеності.

12.2. Симуляційні моделі

Симуляційні моделі є важливим інструментом сучасної системи підготовки фахівців цивільної безпеки, оскільки забезпечують можливість відтворення складних, динамічних та потенційно небезпечних процесів у контрольованому навчальному середовищі. В умовах цифровізації управління ризиками та надзвичайними ситуаціями симуляційне моделювання дозволяє поєднувати теоретичні знання з практичними навичками прийняття рішень, аналізу обстановки та координації дій служб реагування [1; 2].

Симуляційна модель у сфері цивільної безпеки розглядається як формалізоване відображення реальних процесів виникнення, розвитку та ліквідації надзвичайних ситуацій із використанням математичних, інформаційних і візуалізаційних засобів. Такі моделі забезпечують імітацію дій персоналу, функціонування інфраструктури, поширення небезпечних факторів та впливу зовнішнього середовища, що є особливо актуальним для підготовки рятувальників і управлінського складу [3; 9].

У наукових дослідженнях підкреслюється, що симуляційні моделі значно підвищують ефективність навчання за рахунок інтерактивності та сценарного підходу. Вони дозволяють створювати різні варіанти розвитку подій, змінювати вихідні умови, рівень ризику та часові параметри, формуючи у здобувачів освіти системне бачення надзвичайних ситуацій [2; 4]. Особливу цінність мають моделі, інтегровані з технологіями віртуальної та доповненої реальності, які забезпечують ефект присутності та підвищують психологічну готовність до дій в екстремальних умовах [5].

Симуляційні моделі широко застосовуються для відпрацювання реагування на масові ураження, техногенні аварії, пожежі, повені та інші загрози. Дослідження доводять, що використання високодеталізованих VR-симуляцій сприяє підвищенню швидкості прийняття рішень, точності виконання процедур та ефективності командної взаємодії серед рятувальників [4; 5]. Це особливо важливо в умовах, коли реальні тренування обмежені високими ризиками або значними матеріальними витратами.

Окремим напрямом є використання симуляційних моделей у навчанні управлінських рішень та інформаційного забезпечення діяльності органів цивільного захисту. Моделювання потоків інформації, роботи центрів управління, систем оповіщення та координації дозволяє оцінювати ефективність організаційних рішень і вдосконалювати алгоритми взаємодії між суб’єктами Єдиної державної системи цивільного захисту [1; 10].

Симуляційні моделі також застосовуються у формуванні проєктного мислення та навичок управління безпекою. Залучення студентів до розроблення та використання ігрових 3D-середовищ і симуляторів сприяє розвитку аналітичних здібностей, креативності та практичної орієнтації навчання [7; 8]. Такі підходи відповідають сучасним освітнім тенденціям і вимогам підготовки фахівців цивільної безпеки.

Застосування симуляційних моделей у підготовці фахівців цивільної безпеки узгоджується з положеннями Кодексу цивільного захисту України, який визначає необхідність професійної підготовки та постійного вдосконалення навичок осіб, залучених до реагування на надзвичайні ситуації [11]. У цьому контексті симуляційне моделювання виступає важливим засобом забезпечення готовності до дій у кризових умовах.

Симуляційні моделі є ефективним інструментом інтеграції теорії та практики у підготовці фахівців цивільної безпеки. Вони забезпечують безпечне середовище для відпрацювання складних сценаріїв, підвищують якість навчання та сприяють формуванню

професійних компетентностей, необхідних для захисту населення і територій від надзвичайних ситуацій.

12.3. Практичні кейси навчання рятувальників

Сучасна система підготовки фахівців цивільної безпеки перебуває в умовах трансформації, зумовленої зростанням кількості надзвичайних ситуацій, ускладненням їх характеру та підвищенням вимог до оперативності й обґрунтованості управлінських рішень. Відповідно до Кодексу цивільного захисту України, одним із ключових завдань є забезпечення готовності органів управління та сил цивільного захисту до дій у надзвичайних ситуаціях різного походження [11]. У цьому контексті практичні кейси навчання рятувальників, побудовані на основі віртуальної реальності, доповненої реальності та комп'ютерного моделювання, набувають особливого значення.

Практичні кейси являють собою комплексні навчальні сценарії, що відтворюють реальні або наближені до реальних умови надзвичайних ситуацій і дозволяють відпрацьовувати професійні дії без ризику для життя та здоров'я персоналу. За результатами досліджень, застосування VR-сценаріїв у підготовці рятувальників підвищує рівень засвоєння матеріалу, стресостійкість та здатність до прийняття рішень в умовах невизначеності [1].

Одним із найбільш поширених практичних кейсів є навчання діям під час пожеж у житлових, промислових та громадських будівлях. Використання VR-симуляторів дозволяє моделювати різні типи загорянь, зміну температурного режиму, задимлення, обмежену видимість і непередбачувану поведінку вогню. Наприклад, VR-симулятор вогнегасника «СИМ 3» дає можливість відпрацювати алгоритм гасіння пожеж різних класів, оцінювати помилки користувача та формувати навички правильного вибору засобів пожежогасіння [12]. Подібні кейси широко використовуються як у підготовці особового складу ДСНС, так і у навчальному процесі закладів вищої освіти.

Важливе місце займають практичні кейси, пов'язані з реагуванням на масові ураження та надзвичайні ситуації з великою кількістю постраждалих. Дослідження, присвячені високоточним VR-тренажерам для first responders, доводять ефективність таких рішень у формуванні навичок сортування постраждалих, координації між підрозділами та роботи в умовах інформаційного перевантаження [3]. Завдяки високому рівню занурення користувачі отримують досвід, максимально наближений до реальних умов, що складно або неможливо відтворити під час традиційних навчань.

Практичні кейси навчання рятувальників також активно застосовуються для підготовки до ліквідації наслідків техногенних аварій і промислових катастроф. VR-орієнтовані сценарії дозволяють моделювати вибухи, витоки небезпечних хімічних речовин, руйнування конструкцій та порушення інженерних мереж. За даними сучасних досліджень, такі кейси сприяють формуванню просторового мислення, прогнозуванню розвитку небезпечних факторів і зниженню кількості помилок під час реальних операцій [4].

Значну роль відіграють інтегровані навчальні кейси, що поєднують VR/AR-технології з елементами ігрового моделювання та командної взаємодії. У роботах українських і зарубіжних авторів доведено, що застосування 3D-ігрових середовищ у навчанні майбутніх фахівців цивільної безпеки підвищує мотивацію студентів, сприяє розвитку навичок управління ризиками та прийняття колективних рішень [5; 6]. Такі кейси особливо ефективні для підготовки керівного складу та диспетчерських служб.

Доповнена реальність активно використовується у практичних кейсах польової підготовки рятувальників. AR-технології дозволяють накладати цифрову інформацію на реальні об'єкти, забезпечуючи підказки щодо алгоритмів дій, розташування небезпечних зон або технічних характеристик обладнання. За результатами досліджень, використання AR у професійній підготовці зменшує час виконання операцій і підвищує точність дій персоналу [7].

Практичні кейси навчання рятувальників реалізуються з урахуванням вимог чинного законодавства та функціональних завдань Державної служби України з надзвичайних

ситуацій, яка визначає пріоритети підготовки персоналу та впровадження інноваційних освітніх технологій [8]. Інформаційне забезпечення таких кейсів базується на сучасних підходах до управління знаннями та професійною діяльністю у сфері безпеки [11].

Практичні кейси навчання рятувальників із використанням VR/AR і симуляційних технологій забезпечують поєднання теоретичних знань і практичних навичок, сприяють підвищенню готовності до дій у надзвичайних ситуаціях та відповідають сучасним вимогам підготовки фахівців цивільного захисту.

12.4. Інтернет речей (IoT) у сфері цивільної безпеки

Сучасний розвиток цифрових технологій зумовив активне впровадження Інтернету речей (Internet of Things, IoT) у сферу цивільної безпеки, що суттєво трансформує підходи до моніторингу, попередження та реагування на надзвичайні ситуації. IoT розглядається як сукупність взаємопов'язаних фізичних об'єктів, оснащених датчиками, засобами збору, передавання та обробки даних, які функціонують у єдиному інформаційному середовищі. Такі системи забезпечують безперервний обмін даними між технічними засобами та аналітичними платформами, що підвищує рівень ситуаційної обізнаності органів управління цивільним захистом.

У контексті цивільної безпеки IoT виконує функцію інформаційної основи для раннього виявлення загроз техногенного, природного та соціального характеру. Сенсори температури, диму, газу, сейсмічної активності, рівня води або радіаційного фону дозволяють у режимі реального часу фіксувати небезпечні відхилення від нормативних параметрів і передавати дані до центрів управління або автоматизованих систем оповіщення. Це відповідає вимогам Кодексу цивільного захисту України щодо забезпечення своєчасного інформування населення та органів влади про загрози надзвичайних ситуацій [10].

Важливою складовою IoT є інтеграція з інформаційно-аналітичними системами підтримки прийняття рішень. Зібрані дані обробляються з використанням хмарних технологій, елементів штучного інтелекту та машинного навчання, що дає змогу прогнозувати розвиток небезпечних подій і оцінювати можливі наслідки. Як зазначає С. М. Виганяйло, інформаційне забезпечення професійної діяльності фахівців безпеки має ґрунтуватися на достовірних, оперативних і структурованих даних, що є ключовою перевагою IoT-систем [11].

Практичне застосування IoT у сфері цивільної безпеки охоплює системи «розумного міста», автоматизований контроль стану критичної інфраструктури, моніторинг пожежної безпеки на промислових об'єктах і транспортних вузлах, а також спостереження за станом навколишнього середовища. У діяльності Державної служби України з надзвичайних ситуацій перспективним є використання мереж датчиків для контролю пожежонебезпечних територій, підтоплень, аварій на об'єктах підвищеної небезпеки, що сприяє підвищенню ефективності реагування та зниженню ризиків для особового складу [9].

Окремого значення IoT набуває у поєднанні з імерсивними технологіями навчання. Дані, отримані з реальних IoT-пристроїв, можуть використовуватися для формування сценаріїв VR/AR-тренувань і симуляційних моделей, що забезпечує наближення навчального процесу до реальних умов надзвичайних ситуацій. Дослідження зарубіжних авторів свідчать, що інтеграція реальних даних у віртуальні середовища підвищує ефективність підготовки рятувальників і рівень їх готовності до дій у кризових ситуаціях [1].

Разом із перевагами впровадження IoT у сфері цивільної безпеки актуалізуються питання кібербезпеки та захисту інформації. Велика кількість підключених пристроїв створює потенційні вразливості, що можуть бути використані для несанкціонованого доступу або спотворення даних. Тому проєктування IoT-систем повинно передбачати багаторівневий захист інформації, автентифікацію пристроїв і резервування каналів зв'язку, що є важливою складовою підготовки майбутніх фахівців цивільної безпеки.

У перспективі розвиток IoT тісно пов’язаний із концепцією цифрових двійників, роботизованих систем і автономних безпілотних платформ. Поєднання сенсорних даних з цифровими моделями об’єктів і територій дозволяє здійснювати комплексний аналіз ризиків і планування заходів цивільного захисту, що відповідає сучасним світовим тенденціям цифрової трансформації безпекової сфери [14; 15].

12.5. Сенсорні мережі

Сенсорні мережі є ключовим елементом сучасних цифрових технологій у сфері цивільної безпеки, оскільки забезпечують безперервний збір, передачу та аналіз даних про стан навколишнього середовища, техногенних об’єктів і потенційних джерел небезпеки. У контексті цивільного захисту сенсорні мережі розглядаються як інтегрована сукупність апаратних та програмних засобів, що функціонують у режимі реального часу та підтримують ухвалення управлінських рішень органами реагування [9; 10; 11].

Бездротові сенсорні мережі (Wireless Sensor Networks, WSN) складаються з великої кількості автономних сенсорних вузлів, які вимірюють фізичні, хімічні або біологічні параметри, зокрема температуру, тиск, вологість, рівень задимлення, концентрацію токсичних газів, радіаційний фон чи вібраційні коливання. Отримані дані передаються до центрів обробки інформації або диспетчерських пунктів, де здійснюється їх аналіз і візуалізація для подальшого реагування [11].

У системах цивільної безпеки сенсорні мережі широко застосовуються для раннього виявлення надзвичайних ситуацій природного та техногенного характеру. Зокрема, датчики диму та температури використовуються для виявлення пожеж у промислових зонах і лісових масивах, гідрологічні сенсори – для прогнозування повеней, а сейсмічні датчики – для моніторингу небезпечних геодинамічних процесів. Такий підхід відповідає превентивній концепції цивільного захисту, закріпленій у Кодексі цивільного захисту України [10].

Суттєвою перевагою сенсорних мереж є можливість їх інтеграції з іншими цифровими технологіями, зокрема Інтернетом речей, геоінформаційними системами, аналітичними платформами та цифровими двійниками об’єктів. Завдяки цьому формується єдиний інформаційний простір, у якому дані з сенсорів використовуються для моделювання сценаріїв розвитку надзвичайних ситуацій, прогнозування наслідків та оптимізації дій рятувальних підрозділів [15].

Важливим напрямом застосування сенсорних мереж є підтримка навчання та підготовки фахівців цивільної безпеки. Дані, отримані від реальних сенсорних систем, можуть бути інтегровані у віртуальні та симуляційні середовища, що дозволяє відтворювати реалістичні умови надзвичайних ситуацій у навчальному процесі. Такий підхід підвищує якість підготовки майбутніх рятувальників і диспетчерів, формує навички аналізу інформації та прийняття рішень у складних умовах [1; 2; 5].

Сенсорні мережі також активно використовуються у поєднанні з роботизованими та безпілотними системами. Датчики, встановлені на безпілотних літальних апаратах або наземних роботах, дозволяють здійснювати моніторинг зон підвищеної небезпеки без ризику для життя персоналу. Це особливо актуально під час ліквідації наслідків аварій, пожеж, вибухів або хімічного забруднення [14].

Разом із тим, впровадження сенсорних мереж у сфері цивільної безпеки супроводжується низкою викликів, зокрема проблемами енергоспоживання, надійності зв’язку, кібербезпеки та захисту інформації. З огляду на це особливого значення набувають питання стандартизації, резервування каналів зв’язку та забезпечення інформаційної безпеки даних, що передаються сенсорними системами [10; 11].

Сенсорні мережі є невід’ємною складовою сучасних автоматизованих систем цивільної безпеки, забезпечуючи оперативний моніторинг, прогнозування ризиків і підвищення ефективності реагування на надзвичайні ситуації. Їх розвиток і впровадження створюють передумови для формування інтелектуальних систем захисту населення та територій, що відповідають сучасним викликам і вимогам безпеки.

12.6. Роботизовані системи у сфері цивільної безпеки

Роботизовані системи є одним із найбільш перспективних напрямів розвитку цифрових технологій у сфері цивільної безпеки, оскільки вони забезпечують виконання небезпечних, складних і ресурсоємних завдань без безпосередньої участі людини. Їх застосування спрямоване на зменшення ризиків для життя рятувальників, підвищення оперативності реагування та точності прийняття управлінських рішень під час надзвичайних ситуацій [10; 11].

У сучасних умовах роботизовані системи використовуються для моніторингу територій, пошуково-рятувальних робіт, розвідки зон ураження, ліквідації наслідків техногенних аварій, пожежогасіння, роботи з небезпечними матеріалами та оцінювання рівня загроз. Вони поєднують апаратні компоненти (мобільні платформи, маніпулятори, безпілотні літальні апарати) з програмними засобами управління, системами технічного зору, штучного інтелекту та сенсорними мережами [14].

Особливе значення у цивільній безпеці мають мобільні наземні роботи, які здатні діяти в умовах руйнувань, задимлення, високих температур і радіаційного забруднення. Такі системи оснащуються відеокамерами, тепловізорами, газоаналізаторами та лазерними далекомірами, що дозволяє отримувати достовірну інформацію про стан об’єкта або території без ризику для персоналу [9; 10]. Отримані дані інтегруються в інформаційно-аналітичні системи управління силами цивільного захисту.

Важливу роль відіграють безпілотні літальні апарати, які застосовуються для аеророзвідки, картографування зон надзвичайних ситуацій, пошуку постраждалих та оцінювання масштабів лісових і промислових пожеж. Дослідження свідчать, що автономні дрони з елементами колективної поведінки та штучного інтелекту здатні значно підвищити ефективність реагування у складних динамічних середовищах [14]. Вони забезпечують швидке охоплення великих площ і передачу даних у режимі реального часу.

Роботизовані системи тісно пов’язані з технологіями віртуальної та доповненої реальності, які використовуються для підготовки фахівців цивільної безпеки. VR- і AR-середовища дозволяють моделювати управління роботами у різних сценаріях надзвичайних ситуацій, формувати навички дистанційного керування та прийняття рішень в умовах стресу [1; 3; 7]. Такий підхід сприяє підвищенню рівня професійної готовності персоналу без ризику для життя.

У контексті управління проєктами цивільної безпеки роботизовані системи розглядаються як складові комплексних інформаційно-технічних рішень. Їх ефективне впровадження потребує інтеграції з цифровими двійниками об’єктів і територій, що дає змогу прогнозувати розвиток надзвичайних ситуацій, оптимізувати маршрути руху роботів і оцінювати наслідки управлінських рішень [15]. Такий підхід забезпечує системність і наукову обґрунтованість заходів захисту населення.

Нормативно-правові засади використання роботизованих систем у цивільному захисті визначаються законодавством України, зокрема Кодексом цивільного захисту України, який передбачає застосування сучасних технічних засобів для запобігання надзвичайним ситуаціям і ліквідації їх наслідків [10]. Практична діяльність Державної служби України з надзвичайних ситуацій поступово інтегрує роботизовані комплекси у систему реагування, що відповідає світовим тенденціям цифровізації сфери безпеки [9].

Роботизовані системи поєднують автоматизацію, інтелектуальний аналіз даних і дистанційне управління, що сприяє підвищенню рівня безпеки рятувальників та ефективності реагування на надзвичайні ситуації.

12.7. Цифрові двійники об’єктів у системі цивільної безпеки

Цифрові двійники об’єктів є однією з найбільш перспективних цифрових технологій у сфері цивільної безпеки, оскільки поєднують можливості моделювання, прогнозування та управління ризиками в режимі реального часу. Поняття «цифровий двійник» (Digital Twin) означає віртуальну динамічну модель реального фізичного об’єкта, процесу або системи,

яка постійно оновлюється на основі даних, що надходять із сенсорів, інформаційних систем та результатів аналітичних розрахунків [15].

У контексті цивільної безпеки цифрові двійники застосовуються для підвищення готовності до надзвичайних ситуацій, оцінювання техногенних і природних ризиків, планування заходів захисту населення та підтримки управлінських рішень. Вони дозволяють створювати віртуальне середовище, у якому відтворюється поведінка реальних об'єктів інфраструктури – будівель, промислових підприємств, транспортних вузлів, гідротехнічних споруд – за різних сценаріїв впливу небезпечних факторів [14; 15].

Функціонально цифровий двійник складається з трьох взаємопов'язаних компонентів: фізичного об'єкта, його цифрової моделі та інформаційного каналу обміну даними між ними. Сенсорні мережі та технології Інтернету речей забезпечують безперервне надходження інформації про стан об'єкта, параметри середовища, навантаження та відхилення від нормативних показників [11; 15]. На основі цих даних цифровий двійник може відображати поточний стан об'єкта, прогнозувати розвиток аварійних процесів і оцінювати ефективність превентивних заходів.

Важливою перевагою цифрових двійників у цивільній безпеці є можливість моделювання надзвичайних ситуацій без ризику для життя та здоров'я людей. За допомогою цифрових двійників можна відпрацьовувати сценарії пожеж, вибухів, обвалів, хімічних аварій або затоплень, аналізувати поведінку об'єкта та навколишнього середовища, а також оцінювати наслідки для населення і персоналу [14]. Такий підхід значно підвищує якість планування заходів цивільного захисту та аварійно-рятувальних робіт.

У навчальному процесі цифрові двійники тісно інтегруються з технологіями віртуальної та доповненої реальності. Це дозволяє створювати інтерактивні навчальні середовища, у яких здобувачі освіти можуть працювати з реалістичними моделями об'єктів цивільного захисту, аналізувати ризики та приймати рішення в умовах, максимально наближених до реальних [1; 3; 9]. Такі підходи сприяють формуванню системного мислення, професійних компетентностей та навичок управління безпекою.

Цифрові двійники також активно використовуються для управління життєвим циклом об'єктів критичної інфраструктури. Вони дозволяють прогнозувати зношення конструкцій, виявляти потенційно небезпечні зони та своєчасно планувати ремонтні або захисні заходи. У сфері цивільної безпеки це має особливе значення для мінімізації ймовірності техногенних аварій та зниження масштабів можливих збитків [14; 15].

Перспективи розвитку цифрових двійників пов'язані з використанням штучного інтелекту, машинного навчання та великих даних. Поєднання цих технологій дозволяє не лише відображати поточний стан об'єктів, а й автоматично формувати рекомендації щодо підвищення рівня безпеки, оптимізації евакуаційних маршрутів та управління ресурсами під час ліквідації надзвичайних ситуацій [3; 13]. Таким чином, цифрові двійники стають ключовим елементом сучасних автоматизованих систем цивільної безпеки.

Питання для контролю знань

1. У чому полягає сутність VR- та AR-тренажерів і які їхні ключові відмінності у підготовці фахівців цивільної безпеки?
2. Як VR-тренажери сприяють формуванню навичок прийняття рішень в умовах стресу та обмеженого часу?
3. Які обмеження та ризики використання VR/AR-технологій у професійній підготовці рятувальників?
4. Яким чином застосування VR/AR-тренажерів узгоджується з вимогами Кодексу цивільного захисту України щодо підготовки персоналу?
5. Що розуміють під симуляційними моделями у сфері цивільної безпеки та чим вони відрізняються від VR-тренажерів?
6. Які види симуляційних моделей застосовуються для підготовки рятувальників до дій у надзвичайних ситуаціях?

7. Яку роль відіграють симуляційні моделі у прогнозуванні розвитку надзвичайних ситуацій?
8. Які дані та параметри є критично важливими для побудови достовірної симуляційної моделі НС?
9. У чому полягають переваги використання комп'ютерних симуляцій порівняно з традиційними навчально-тренувальними заняттями?
10. Що розуміють під практичними кейсами навчання рятувальників у контексті використання VR і симуляційних технологій?
11. Які типові сценарії надзвичайних ситуацій використовуються у практичних кейсах для підготовки рятувальників?
12. Як практичні кейси сприяють формуванню професійних компетентностей майбутніх фахівців цивільної безпеки?
13. Яку роль відіграє аналіз помилок і зворотний зв'язок після проходження симуляційного кейсу?
14. Які перспективи розвитку практичних кейсів навчання рятувальників із використанням VR/AR та штучного інтелекту?
15. Що таке Інтернет речей (IoT) та які його ключові складові в системах цивільної безпеки?
16. Які типи IoT-пристроїв застосовуються для моніторингу небезпечних факторів у надзвичайних ситуаціях?
17. Яку роль відіграють хмарні технології та аналітика даних у функціонуванні IoT-систем?
18. Які основні ризики інформаційної та кібербезпеки пов'язані з використанням IoT у цивільній безпеці?
19. Які перспективи розвитку IoT у системі цивільного захисту України?
20. Які типи сенсорів застосовуються для контролю фізичних, хімічних та біологічних загроз?
21. У чому полягає відмінність сенсорних мереж від окремих IoT-пристроїв?
22. Які проблеми енергоспоживання та надійності характерні для сенсорних мереж?
23. Як інтеграція сенсорних мереж із геоінформаційними системами підвищує ефективність управління НС?
24. Яке значення сенсорних мереж для автоматизованих систем управління цивільною безпекою?
25. Що розуміють під роботизованими системами у сфері цивільної безпеки?
26. Які завдання можуть виконувати наземні, повітряні та морські роботизовані платформи?
27. Як роботизовані системи зменшують ризик для життя рятувальників?
28. Які обмеження та етичні проблеми існують при використанні роботизованих систем у НС?
29. Що таке цифровий двійник та які його основні характеристики?
30. Які етапи створення цифрового двійника потенційно небезпечного об'єкта?
31. Як цифрові двійники використовуються для прогнозування аварій та надзвичайних ситуацій?
32. Які перспективи впровадження цифрових двійників у системі цивільної безпеки України?

Список використаних джерел

1. Alshowair A., Bail J., AlSuwailem F., Mostafa A., Abdel-Azeem A. Use of virtual reality exercises in disaster preparedness training: A scoping review // SAGE Open Medicine. – 2024. – Режим доступу: https://pmc.ncbi.nlm.nih.gov/articles/PMC11017811/
2. Khanal S., Medasetti U. Sh., Mashal M. Virtual and Augmented Reality in Disaster Management Technology: A Literature Review // Frontiers in Virtual Reality. – 2022. – Режим

доступу: https://www.frontiersin.org/journals/virtual-reality/articles/10.3389/frvir.2022.843195/full.

3. Heldring S., Jirwe M., Wihlborg J. Using High-Fidelity Virtual Reality for Mass-Casualty Incident Training by First Responders: A Systematic Review. – 2024. – Режим доступу: https://www.researchgate.net/publication/390636909.

4. Vercelli G., Iacono S. та ін. From Risk to Readiness: VR-Based Safety Training for Industrial Hazards. – 2024. – Режим доступу: https://arxiv.org/abs/2412.13725.

5. Рудинець М. В., Федорчук-Мороз В. І. Обґрунтування застосування віртуальної реальності як інноваційного елементу проектів системи захисту населення від надзвичайних ситуацій // Український журнал будівництва та архітектури. – 2022. – № 3. – С. 75–83.

6. Sivakovska O., Rudynets M., Yashchuk A., Redko R., Zabolotnyi O. Project Safety Management Systems of Students with 3D Game Development // EAI/Springer Innovations in Communication and Computing. – 2022. – P. 459–468. – Режим доступу: https://doi.org/10.

7. Kashkanov V. A. Використання технології доповненої реальності у підготовці фахівців // Вісник машинобудування та транспорту. – 2023. – Режим доступу: https://vmt.vntu.edu.ua/index.php/vmt/article/view/314.

8. Віртуальна реальність // Українська електронна енциклопедія освіти (EduGlos). – Режим доступу: https://eduglos.iitta.gov.ua/index.php/Віртуальна_реальність.

9. Державна служба України з надзвичайних ситуацій. Офіційний сайт. – Режим доступу: https://dsns.gov.ua/.

10. Кодекс цивільного захисту України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/5403-17#Text.

11. Виганяйло С. М. Інформаційне забезпечення професійної діяльності : навч. посіб. – Харків : ХНУВС, 2021. – 108 с. – Режим доступу: https://cutt.ly/SVuI8n1.

12. VR-симулятор вогнегасника «СИМ 3». – Режим доступу: https://www.novator-sim.org.ua/.

13. Floreano D., Wood R. J. Science, technology and the future of small autonomous drones // Nature. 2015. Vol. 521. P. 460–466.

14. Grieves M., Vickers J. Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems // Transdisciplinary Perspectives on Complex Systems. 2017. P. 85–113.

15. Tao F., Zhang H., Liu A., Nee A. Y. C. Digital twin in industry: State-of-the-art // IEEE Transactions on Industrial Informatics. 2019. Vol. 15, No. 4. P. 2405–2415. https://www.researchgate.net/publication/345078627_Digital_Twin_in_Industry_State-of-the-Art.

Інформаційні технології та автоматизовані системи в цивільній безпеці [Текст]: Конспект лекцій для здобувачів першого (бакалаврського) рівня галузі знань К Безпека та оборона спеціальності К10 Цивільна безпека денної та заочної форм навчання / уклад. М.В. Рудинець – Луцьк: ЛНТУ, 2025. – 88 с.

Комп’ютерний набір М. В. Рудинець
Редактор М. В. Рудинець

Підп. до друку 2025р.
Формат 60х84/16. Папір офс. Гарнітура Таймс.
Ум. друк. арк. 2,5.
Тираж 50 прим. Зам. ___.

Відділ іміджу та промоції
Луцького національного технічного
університету 43018, м. Луцьк,
вул. Львівська,75
Друк – Відділ іміджу та промоції ЛНТУ