DOI 10.34185/1562-9945-4-159-2025-09
УДК 004.8

О.М. Шопський, Р.Р. Головатий

ЗАСТОСУВАННЯ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ ДЛЯ РАННЬОГО ВИЯВЛЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ НА ОСНОВІ ПОТОКОВИХ ВЕЛИКИХ ДАНИХ

Анотація. Сучасні системи раннього виявлення надзвичайних ситуацій недостатньо оперативні та точні через використання традиційних методів обробки потокових даних. Це призводить до затримок у реагуванні на надзвичайні події, збільшуючи масштаби потенційних втрат. Мета - дослідити ефективність моделей машинного навчання (глибокого навчання) для раннього виявлення надзвичайних ситуацій на основі аналізу потокових великих даних із сенсорних мереж (IoT) та соціальних медіа. Використано класичні (порогові методи, SVM) та сучасні алгоритми глибокого навчання (LSTM, LSTM-CNN), проведено експериментальні дослідження на синтетичних та реальних потокових даних, виконано порівняльний аналіз моделей за такими метриками, як точність (Precision), повнота (Recall), F1-міра, час раннього виявлення та кількість хибних спрацювань. Основні результати досліджень - гібридна модель LSTM-CNN забезпечила найвищу точність (F1=0.90) у ранньому виявленні надзвичайних ситуацій. LSTM-CNN модель продемонструвала найменшу середню затримку спрацювання (≈ 5,5 с). Підтверджено переваги моделей глибокого навчання над традиційними методами (пороговими детекторами, класичними алгоритмами ML). Український досвід впровадження ML-моделей у системах раннього оповіщення показав практичну ефективність і високу надійність цих технологій.
Ключові слова: машинне навчання, глибоке навчання, надзвичайні ситуації, великі дані, потокові дані, LSTM, аномалії, раннє виявлення, моніторинг, соціальні медіа, Інтернет речей (IoT).

Вступ. Раннє виявлення надзвичайних ситуацій – важливий компонент ефективного реагування на природні катастрофи, техногенні аварії та інші критичні події. Чим швидше виявлено надзвичайну ситуацію, тим більше шансів запобігти жертвам та зменшити збитки [1]. Традиційно системи раннього оповіщення спираються на мережі фізичних датчиків (сейсмографи, датчики погоди, пожежні сигналізації тощо) та заздалегідь визначені порогові значення. Наприклад, сейсмічні датчики можуть ініціювати тривогу при перевищенні порогу прискорення ґрунту, а метеостанції – при різкому підвищенні рівня води. Однак такі правил-орієнтовані системи часто вимагають тонкого налаштування параметрів і балансування між чутливістю та кількістю хибних тривог [2]. Більш того, вони не завжди здатні обробляти великі обсяги гетерогенних

даних у режимі реального часу. З іншого боку, розвиток технологій Інтернету речей (Internet of Things, IoT) та соціальних мереж призвів до появи величезних потоків даних, які можна використовувати як своєрідні "сенсори" надзвичайних ситуацій [3]. Наприклад, користувачі соціальних мереж повідомляють про події (землетруси, пожежі, аварії) майже миттєво, перетворюючись на “соціальні датчики”. Це відкриває нові можливості для моніторингу НС: у режимі реального часу агрегувати дані з тисяч джерел і виявляти ознаки надзвичайних подій раніше за офіційні повідомлення. Так, у роботі [4] запропоновано фреймворк EDEE, що за допомогою глибокої нейронної мережі (BERT-Att-BiLSTM) вилучає з потоків повідомлень ті, що стосуються надзвичайних подій, і групує їх у події для раннього оповіщення. На прикладі спалаху невідомої пневмонії (COVID-19) у місті Ухань було продемонстровано, що система змогла зафіксувати перші ознаки епідемії 30 грудня 2019 року – за день до офіційного повідомлення влади [4]. Це підтверджує потенціал соціальних мереж у задачах раннього виявлення.

Паралельно, у сфері промислової безпеки та моніторингу навколишнього середовища, тисячі IoT-сенсорів генерують безперервні вимірювання (температура, тиск, вологість, хімічні показники тощо). Ці дані також можна використовувати для автоматичного виявлення аномалій, що сигналізують про надзвичайні ситуації (наприклад, витік газу, початок пожежі або повені). Застосування штучного інтелекту до таких даних здатне суттєво покращити ефективність раннього оповіщення [6]. Зокрема, інтеграція технологій IoT та методів машинного навчання вже продемонструвала свою корисність для систем раннього попередження про землетруси та інші лиха як на етапі до катастрофи, так і після неї [7]. Нещодавні дослідження показали, що глибокі нейронні моделі, навчені на потокових даних з датчиків або супутників, можуть значно скоротити час виявлення події порівняно з традиційними підходами. Наприклад, глибинна модель на основі супутникових даних дозволила суттєво зменшити затримку прогнозування параметрів сильних землетрусів [8].

Однак впровадження моделей машинного навчання для аналізу потокових великих даних пов’язане з низкою викликів. По-перше, це висока швидкість та обсяг даних: алгоритми мають працювати в режимі реального часу, часто обробляючи тисячі повідомлень або вимірювань за секунду. По-друге, різнорідність даних: дані можуть надходити у вигляді числових показників датчиків, текстових повідомлень, зображень або звукових сигналів. Потрібні універсальні та стійкі моделі, здатні працювати з мультимодальними потоками. По-третє, існує проблема адаптації до змін (concept drift): з часом властивості потоку можуть змінюватися (наприклад, сезонні коливання сенсорних показників або зміни сленгу в соцмережах), що вимагає періодичного оновлення або онлайнового донавчання моделей. Нарешті, критичним є мінімізація хибних спрацювань – у контексті НС помилкова тривога теж небажана, адже може призвести до паніки або ігнорування системи.

Аналіз літературних джерел. Ранні системи оповіщення зазвичай реалізовані як системи з фіксованими правилами. Приклади включають порогові детектори

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

(спрацювання сигналізації при перевищенні певного рівня) та статистичні методи контролю рядів даних (наприклад, ковзне середнє, модель Холта-Вінтерса чи система EARS у епідеміологічному нагляді [5]. Такі методи відносно прості і зрозумілі, проте мають обмеження. Як зазначають дослідники [10], продуктивність цих алгоритмів визначається компромісом між чутливістю та рівнем хибних спрацювань, і для досягнення прийнятних результатів потрібне ретельне налаштування параметрів під конкретні умови. У швидкоплинних сценаріях надзвичайних ситуацій (наприклад, блискавична повінь, техногенна аварія) жорстко задані пороги можуть або не спрацювати вчасно, або ж створити надлишок помилкових тривог.

Зростання обсягів даних стимулювало перехід від правил до алгоритмів машинного навчання, які здатні автоматично навчатися на історичних даних і виявляти приховані залежності. У галузі виявлення аномалій в даних сенсорних мереж (що є технічно близьким до завдання виявлення НС) уже застосовуються різноманітні алгоритми МН. Ранні роботи використовували методи класичного навчання – наприклад, метод опорних векторів (SVM), класифікатори на основі правил або дерев рішень – для визначення відхилень у параметрах роботи обладнання чи інфраструктури. Проте такі алгоритми часто потребували побудови фіксованих ознак і не завжди справлялися з нелінійними динамічними патернами. На зміну їм прийшли методи глибокого навчання (ГН), які особливо добре зарекомендували себе у задачах з послідовними та часовими даними. Зокрема, рекурентні нейронні мережі (RNN) та їхні різновиди – довга короткочасна пам’ять (LSTM) та двонаправлена LSTM (Bi-LSTM) – здатні запам’ятовувати довгострокові залежності у часових рядах. Це дуже доречно для аналізу сенсорних потоків, де аномалія може проявлятися як специфічна послідовність сигналів. Автоенкодери (autoencoders) – ще один популярний підхід: мережа навчається відтворювати «нормальні» дані, і при появі аномальних ввідних сигналів помилка відтворення різко зростає, сигналізуючи про відхилення. Наприклад, Abusitta та ін. використовували денойзінг-автоенкодери для виявлення аномалій у IoT-системах [7]. З іншого боку, згорткові нейронні мережі (CNN) традиційно відомі успіхами в аналізі зображень, але їх можна застосувати і до часових рядів, перетворивши послідовність у «зображення» ознак або поєднавши з рекурентним шаром для вилучення локальних патернів. Комбінація LSTM і CNN продемонструвала високу результативність: зокрема, в науковій роботі [1] запропоновано гібридну модель LSTM-CNN для виявлення аномалій у потоках даних, яка перевершила за точністю звичайну LSTM та LSTM-автоенкодер. За результатами на наборі реальних даних Yahoo Webscope, LSTM-CNN показала найвищий F1-скор (міру), перевищивши автоенкодер на ~0.49 в одній зі серій експериментів [13], а звичайну LSTM – на 0.10 у іншій. Важливо, що при цьому час навчання збільшився несуттєво – додавання згорткового шару дещо ускладнило модель, але різниця в швидкодії була мінімальною. Це свідчить, що навіть складні глибокі моделі можуть бути застосовані в режимі майже реального часу за умови оптимізації та достатніх обчислювальних ресурсів.

Окрім числових показників сенсорів, важливим джерелом інформації є неструктуровані дані, зокрема тексти з соціальних мереж. Вже згаданий приклад раннього ви-

явлення епідемії через аналіз повідомлень у Weibo продемонстрував ефективність глибинного аналізу тексту [2]. Сучасні методи обробки природної мови (NLP) на основі глибокого навчання – такі як трансформери (BERT), рекурентні мережі з увагою та ін. – дозволяють класифікувати повідомлення з соціальних мереж з високою точністю.

У роботі [13] згаданий BERT-Att-BiLSTM класифікатор досяг високої повноти та точності при відборі постів, що стосуються НС, відсікаючи «фон» із маси даних. Автори поєднали машинне навчання із експертними правилами: їх метод (MRIM) інтегрує класифікатор, навчений на даних про повінь у м. Чженчжоу, з вручну заданими шаблонами, що дозволило покращити якість виділення релевантної інформації порівняно з чисто навченою моделлю. Цей результат цікавий тим, що підкреслює: для підвищення надійності в критичних системах інколи варто комбінувати нейронні мережі з правилорієнтованими методами, аби використати сильні сторони кожного.

В останні роки українські науковці зробили помітний внесок у розвиток ML-моделей для моніторингу надзвичайних ситуацій. Зокрема, у праці [13] запропоновано використовувати розподілене (федеративне) навчання для аналізу потокових даних в системах Industrial IoT. Автори показали, що федеративне навчання забезпечує вищу точність обробки даних навіть зі зростанням їх обсягів (у порівнянні з централізованими підходами), тоді як нерозподілені моделі ML працюють швидше при жорстких обмеженнях часу. Такий підхід відкриває можливості створення адаптивних самонавчальних систем, здатних підлаштовуватися під зміну параметрів середовища в реальному часі. Результати цих досліджень важливі для побудови стійких потокових платформ обробки великих даних, що актуально і для задач раннього оповіщення про НС.

Окремий напрямом виступає використання ML для комп’ютерного зору та аналізу відеопотоків у надзвичайних ситуаціях. Так, у науковій роботі [10] розроблено інтелектуальну систему для попередження дорожньо-транспортних аварій. Авторами дослідивши алгоритми глибинного навчання для реального часу. Ним проаналізовано низку сучасних моделей нейромереж (Transformer, CNN, R-CNN, GAN, HOG, YOLO) та проведено їх порівняльне оцінювання в задачі виявлення транспортних засобів і прогнозування аварійних ситуацій на дорозі. В результаті було запропоновано оптимальну модель на основі глибокого навчання, яка забезпечує підвищену точність і ефективність розпізнавання потенційно небезпечних сценаріїв руху. Інша робота [7] присвячена відеоспостереженню: автори реалізували прототип комп’ютеризованої системи, здатної автоматично виявляти нетипові (екстрені) ситуації на відео за допомогою методів ML. У праці розроблено архітектуру апаратно-програмного комплексу на базі мікроконтролера з камерою, а функція розпізнавання надзвичайної ситуації інтегрована шляхом навчання моделі на вибірках відео інцидентів. Подібні дослідження демонструють ефективність нейромережевих підходів для аналізу стрімінгового відео з метою виявлення аварій, пожеж, нестандартної поведінки тощо в режимі, близькому до реального часу.

Значним є інтерес і до використання ML у специфічних прикладних сферах безпеки. Приміром, у роботі [5] автори досліджували можливості експертних систем на

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

основі ML для підвищення безпеки авіації. Ними запропоновано концепцію системи підтримки прийняття рішень для аеропортів, що виявляє небезпечні ситуації на злітно-посадкових смугах. Як зазначається, машинне навчання дає змогу залучити великі обсяги історичних даних для навчання моделей, що забезпечує високу точність визначення небезпечних ситуацій. В поєднанні з правил-орієнтованими експертними модулями це рішення може генерувати рекомендації диспетчерам щодо запобігання інцидентам на летовищі. Таким чином, вітчизняні фахівці адаптують сучасні ML-методи під потреби авіаційної безпеки, де критично важливі і швидкість, і надійність виявлення загроз.

Варто відзначити, що в Україні розвиваються і промислові проєкти з впровадженням ML для раннього оповіщення про НС. Зокрема, інтегратори систем безпеки пропонують рішення СРВНС – системи раннього виявлення надзвичайних ситуацій на виробництвах, які поєднують мережі датчиків та програмні модулі з елементами штучного інтелекту. Наприклад, типова СРВНС для об’єктів підвищеної небезпеки (нафтобази, хімічні підприємства тощо) збирає показники з датчиків (температура, тиск, дим, газ, вібрація) і в режимі реального часу аналізує їх на відхилення від норми. Сучасні системи такого класу використовують алгоритми машинного навчання для підвищення точності аналізу даних, що дозволяє більш надійно виявляти ознаки аварійної ситуації на ранніх стадіях. У разі виявлення загрози система автоматично активує оповіщення (сигналізація, повідомлення) для персоналу та служб реагування, мінімізуючи затримку між виникненням події і реагуванням. Наявність подібних промислових впроваджень підтверджує практичну цінність дослідницьких розробок і демонструє готовність української індустрії використовувати ML-рішення для підвищення рівня безпеки.

Результати досліджень. Для оцінки ефективності моделей машинного навчання в задачі раннього виявлення надзвичайних ситуацій нами було побудувано експериментальну систему, що імітує обробку потокових даних і визначає момент спрацювання тривоги про НС. В ролі джерела числових потокових даних було використано публічний набір даних Yahoo! Webscope S5, який є загальновизнаним показником, що використовується для оцінки стану алгоритмів виявлення аномалій у часових рядах [1]. Цей набір містить синтетично згенеровані часові ряди з властивостями, подібними до реальних сенсорних даних (наприклад, метрика навантаження на сервер, показники температури тощо), до яких навмисно додано різного роду аномалії (сплески, стрибки, зміни тренду). Наявність розмітки аномальних інтервалів (ground truth) дозволяє точно оцінити момент спрацювання алгоритму відносно фактичного початку «надзвичайної ситуації» (аномалії). Для наших цілей ми трактуємо кожну аномалію в ряді як подію НС, яку слід виявити якомога раніше. Потік даних формується шляхом послідовної подачі точок часового ряду моделям, імітуючи реальний стримінговий режим: алгоритм отримує нові значення поступово і приймає рішення онлайн. Для ілюстрації можливостей моделей в текстовому домені було також зібрано експериментальний потік повідомлень з соціальної мережі “X”. за період кількох днів, що містив як спокійні періоди, так і час виникнення реальної події (наприклад, землетрус або великий вибух). Ці дані використовувалися переважно для якісного аналізу, оскільки для них не завжди є чітка "розмітка" часу початку події. Проте в рамках основного кількісного експери-

менту ми зосередилися на даних сенсорного типу (Yahoo S5), де можливо об'єктивно виміряти метрики.

На основі огляду літератури, до експерименту було включено декілька моделей, що представляють різні покоління підходів:

Рисунок 1 - Графічне представлення моделей різного мокоління

Пороговий детектор представляє простий підхід, що встановлює статистично обґрунтований поріг для метрики і сигналізує про надзвичайні ситуації при виході показника за цей поріг. В наших експериментах як такий детектор використовувався контролер на основі ковзного середнього та трьох сигм ($\mu \pm 3\sigma$), що є аналогом класичних контролних карт. Цей метод не потребує навчання і слугує базою для порівняння. Щодо класичного ML-класифікатора - це навчена модель, що використовує вручну визначені ознаки. Нами було обрано метод опорних векторів (SVM) з радіально-базисною функцією ядра як приклад традиційного алгоритму машинного навчання. Для навчання SVM використовували згенеровані ознаки часових вікон (статистики за останні N точок: середнє, стандартне відхилення, градієнт тощо). Модель SVM навчалась розпізнавати "аномальне" вікно даних проти "нормального" на основі розмічених аномалій в навчальній підмножині даних. Глибока нейронна мережа LSTM представляє клас рекурентних мереж, здатних вловлювати часову структуру даних. У нашій роботі ми використали одномодульну LSTM-мережу, навчання якої було спрямоване на передбачення наступного значення часового ряду; рішення про наявність аномалії приймалося на основі величини помилки прогнозу, або ж модель напряму класифікувала стан як нормальний чи аномальний у кожен момент часу. Гіперпараметри, зокрема кількість нейронів у прихованому шарі та довжина вхідної послідовності, підбиралися експериментально на валідаційній вибірці. Альтернативним підходом є автоенкодер на основі

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

LSTM (LSTM-AE) — модель, що складається з енкодера та декодера, реалізованих за допомогою LSTM-структур і навчена відновлювати фрагменти нормального часового ряду. Внаслідок цього, при появі аномальних шаблонів у даних, модель демонструє значно вищу помилку реконструкції. Для виявлення аномалій встановлювався поріг на величину цієї помилки; його значення визначалося як певний перцентиль серед значень помилки на навчальних (нормальних) даних. Ще один варіант — гібридна модель LSTM-CNN, яка поєднує згортковий шар для вилучення локальних ознак із часової послідовності з подальшою обробкою цієї послідовності через LSTM-шар. Передбачається, що CNN дозволяє виявити короткотривалі шаблони або сплески, тоді як LSTM забезпечує врахування довгострокового контексту.

Оцінка ефективностей моделей оцінювалися за метриками, представленими в таблиці 1.

Таблиця 1

Метрики оцінки ефективності моделей

Точність позитивного передбачення (Precision)	Повнота виявлення (Recall)	F1 - міра	Час виявлення (затримка)	Пропуски та хибні спрацювання
частка реальних НС серед всіх спрацювань моделі. Низький Precision вказує на велику кількість хибних тривог	частка виявлених моделей надзвичайних сиутацій серед усіх фактичних. Низький Recall означає пропуски подій	гармонійне середнє precision та recall, використовується як інтегральний показник якості виявлення аномалій	різниця у часі між фактичним початком події та моментом, коли модель вперше згенерувала тривожний сигнал.	коли модель не видала сигнал під час події або видала сигнал, коли події не було

У випадку потокових даних оцінювання здійснювалося послідовно: на кожному кроці часу приймалося рішення (тривога чи спокій), яке потім порівнювалося з "істиною". Для забезпечення чесності оцінки, якщо модель видавала тривогу протягом події, вважалося, що подія виявлена (і подальші спрацьовування в її межах не рахувались як додаткові). Це моделює сценарій, коли система після першого спрацьовування по конкретній події вже сповіщує рятувальні служби, і повторні сигнали тієї ж події не так важливі.

Всі моделі було реалізовано в середовищі Python з використанням бібліотек машинного навчання (scikit-learn для SVM, TensorFlow/Keras для нейронних мереж). Потік даних подавався поетапно в модель: на кожному кроці надходило нове значення, після чого виконувалося оновлення внутрішнього стану (для рекурентних мереж) та, за

необхідності, видавався сигнал. Для простоти, моделі LSTM та LSTM-CNN реалізовано у вигляді міні-пакетної обробки: дані подавалися блоками по T кроків з перекриттям, де T – довжина вхідної послідовності для мережі. Це наближається до реального застосування, де дані можуть накопичуватися в буфері перед обробкою. Система оцінки в режимі реального часу відзначала часові мітки, коли генерувалася тривога, що дозволило потім обчислювати затримку.

Загальна продуктивність моделей. Результати по метриках Precision, Recall та F1-зведеній представлені в таблиці 2. Видно, що моделі, побудовані на методах глибокого навчання, перевершують як пороговий метод, так і класичний SVM у більшості показників. Найкращий сумарний баланс (виміряний F1-мірою) досягнуто гібридною моделлю LSTM-CNN – її F1=0.90, що трохи вище, ніж у чистої LSTM (F1=0.88) і суттєво вище, ніж у SVM (F1≈0.80). Пороговий метод продемонстрував найнижчу точність через велику кількість помилкових тривог (низький Precision 0.60), хоча його Recall був відносно прийнятним (0.75) завдяки чутливому налаштуванню.

Таблиця 2

Порівняння моделей за точністю (Precision), повнотою (Recall),
F1-мірою та середнім часом виявлення (затримкою) на тестових потоках

Модель	Precision	Recall	F1-міра	Середня затримка виявлення (с)
Пороговий детектор	0.60	0.75	0.67	15.0
SVM (класичний МН)	0.82	0.78	0.80	8.5
LSTM (нейронна мережа)	0.90	0.86	0.88	6.2
LSTM-AE (автоенкодер)	0.85	0.70	0.77	7.0
LSTM-CNN (гібридна)	0.92	0.88	0.90	5.5

Як видно з таблиці, LSTM-автоенкодер дещо поступився звичайній LSTM у Recall (0.70 проти 0.86). Це узгоджується зі спостереженнями інших дослідників, що автоенкодери не завжди добре захоплюють різноманітні шаблони нормальної поведінки і можуть пропускати деякі аномалії [1]. Натомість LSTM-класифікатор, який навчався явно розпізнавати аномалії, досягнув високого Recall. Додавання згорткового шару (модель

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

LSTM-CNN) дало невеликий, але помітний приріст точності: Precision підвищився до 0.92, а Recall до 0.88, що сумарно підняло F1 до 0.90. Ці кількісні результати відповідають тенденції, відзначеній у літературі [1], де гібридна модель перевищила звичайні у метриках, хоча й не драматично (різниця у кілька відсотків).

Останній стовпець таблиці 2 показує середню затримку спрацювання для кожної моделі. Тут перевага глибокого навчання проявилася ще виразніше. Пороговий метод, хоч і виявив більшість подій, робив це із середньою затримкою ~15 секунд після початку аномалії (в наших тестових даних одна "секунда" відповідає одному кроку дискретного часу або певному інтервалу залежно від природи датчика). SVM спрацьовував швидше (~8.5 с затримки), ймовірно через те, що він був налаштований на високу чутливість. LSTM-мережа показала затримку близько 6.2 с, що вже значно краще. Найшвидше зреагувала модель LSTM-CNN – в середньому через 5.5 с після початку події. В деяких випадках вона фактично випереджала інші моделі на кілька кроків часу, вловлюючи слабкі початкові ознаки. Наприклад, у одній з тестових серій LSTM-CNN згенерувала сигнал на 2 секунди раніше, ніж звичайна LSTM, завдяки розпізнаванню характерного “шуму” перед великим стрибком сигналу, який інші методи ігнорували. Ці результати підтверджують, що більш складні моделі можуть не лише підвищити точність, а й зменшити час спрацювання – ключовий показник для систем раннього оповіщення

Для практичного застосування важливо розуміти, які помилки роблять моделі. Пороговий метод генерував найбільше хибних тривог – приблизно 40% його спрацювань були помилковими, що збігається з його Precision = 0.60. Ці хибні сигнали виникали переважно через випадкові коливання сигналу, які перетинали встановлений поріг, але не були справжніми надзвичайними ситуаціями. SVM також видавав деяку кількість помилкових тривог (Precision≈0.82 означає ~18% хибних спрацювань), переважно у складних випадках, де патерни нормальної поведінки нагадували аномалію, але трохи не дотягували до порогу. LSTM та LSTM-CNN мали найвищий Precision, тобто найменше хибних спрацювань (~8-10%). Цікаво, що майже всі хибні тривоги LSTM-CNN співпадали з хибними тривогами LSTM – тобто обидві моделі помилялися на тих самих ділянках. Це можуть бути області даних, які були неоднозначними навіть для людини або відсутні у навчальній вибірці (невідомі патерни). Щодо пропусків (коли подія сталася, а сигналу немає), то найгірше справи були у LSTM-AE – він пропустив близько 30% подій (Recall 0.70). Пороговий метод пропустив 25% (Recall 0.75). SVM – 22%. LSTM – 14%. LSTM-CNN – 12%. Таким чином, глибинні моделі не лише рідше хибно спрацьовували, але й фіксували практично всі надзвичайні ситуації (пропускали не більше 1 з 8 подій), що є вирішальним для систем оповіщення.

В праці [8] наведено фрагмент часової серії з тестових даних зі штучно вставленою надзвичайною ситуацією (аномалією) та моменти спрацювання різних моделей. Видно, що як тільки починається стрімке зростання сигналу (імітація, наприклад, різкого підйому рівня води при повені), пороговий метод спрацьовує із запізненням, коли значення вже перейшло поріг (відмічено червоною точкою). SVM-алгоритм дав сигнал трохи раніше (синя точка), однак все ще після різкого стрибка. Натомість LSTM (зелена

точка) і LSTM-CNN (фіолетова точка) подають сигнал майже відразу після відхилення кривої від норми, випереджаючи простіші методи. У цьому прикладі LSTM-CNN першою згенерувала тривогу, випередивши пороговий детектор на ~3 секунд. Хоч даний графік ілюструє приватний випадок, подібна картина спостерігалася і в середньому по всіх тестових сценаріях.

Окрім кількісних результатів на синтетичних потоках, цікавим є аналіз роботи моделей на реальних даних. Ми проаналізували твіттер-стрічку під час землетрусу магнітудою ~3, що стався у Тернопільській області [14]. Було відмічено, що протягом перших хвилин після землетрусу в Twitter з'явилась кілька повідомлень від очевидців. Використовуючи попередньо навчену модель класифікації (спрощену версію BERT, натреновану на виявлення повідомлень про землетруси), вдалося ідентифікувати сплеск твітів, які згадують слово "землетрус" та описують поштовхи. Модель видала тривожний сигнал приблизно через 1–5 хвилини після фактичного початку землетрусу – задовго до офіційного повідомлення сейсмологічної служби (яка зазвичай публікує інформацію з затримкою кілька хвилин на обробку). Цей реальний кейс узгоджується з результатами роботи інших авторів, що соціальні мережі можуть суттєво випередити офіційні канали. На приклад, згадана китайська система EDEE з Weibo зафіксувала [2] спалах пневмонії за ~1 день до офіційного оголошення епідемії.

У статті досліджено застосування методів машинного навчання і глибокого навчання для задачі раннього виявлення надзвичайних ситуацій на основі потокових великих даних. Проведений аналіз літератури показав, що завдяки стрімкому розвитку IoT та популярності соціальних мереж з'явилися нові багаті джерела даних, які можна оперативно аналізувати з метою виявлення ознак надзвичайних подій. Традиційні методи, побудовані на фіксованих правилах або простих статистичних моделях, поступово доповнюються і замінюються алгоритмами машинного навчання, здатними навчатися на історичних даних та виявляти складні шаблони, що передують НС.

Експериментальне порівняння кількох моделей – від базових (пороговий детектор, SVM) до сучасних нейронних (LSTM, LSTM-AE, LSTM-CNN) – продемонструвало чіткі переваги глибокого навчання. Зокрема, гібридна модель LSTM-CNN досягла найвищої точності виявлення ($F1 \approx 0.90$) і забезпечила найменшу середню затримку спрацювання (~5.5 с) серед розглянутих варіантів. Це означає, що такі моделі можуть не лише більш надійно відрізнити надзвичайну ситуацію від фонових коливань, але й зробити це на кілька секунд швидше, що в контексті катастроф може бути вирішальним. Отримані результати узгоджуються з попередніми дослідженнями: наприклад, відомо, що поєднання різних архітектур (CNN+LSTM) дозволяє поліпшити показники в порівнянні з окремими компонентами [27], а якісно навчені глибокі моделі можуть вловлювати «тонкі» сигнали на ранніх стадіях розвитку події, які не видно менш складним алгоритмам.

Проведений нами кількісний експеримент був сфокусований на сенсорних даних, додатковий приклад з аналізом твіттер-стрічки під час землетрусу показав, що навіть з порівняно простим NLP-моделлю можна отримати виграш у часі щодо офіційних да-

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

них. Це відкриває шлях до мульти-модальних систем, де сигнали з різних джерел (датчики, соцмережі, відео) комбінуються для формування цілісної картини ситуаційної обстановки.

Результати дослідження можуть бути використані при побудові сучасних систем моніторингу надзвичайних ситуацій – від центрів управління кризами територіальних об'єднаних громад до промислових систем безпеки. Продемонстровано, що навіть відносно компактні нейронні моделі можуть працювати в реальному часі та виявляти події швидше і надійніше, ніж традиційні методи. Наприклад, впровадження LSTM-CNN моделі на потоках даних від сенсорної мережі дамби може дати додаткові хвилини на евакуацію завдяки більш ранньому розпізнаванню критичного підйому рівня води. Так само, інтеграція аналізу соцмереж до центрів реагування може забезпечити ранні сигнали про події, які інакше залишалися б непоміченими до офіційних повідомлень.

Водночас, слід відзначити кілька обмежень даного дослідження. По-перше, експерименти на синтетичних даних (наприклад Yahoo S5) не повністю відображають усю складність реальних даних сенсорних мереж, де можуть бути шум, збої, пропущені значення тощо. Тому наступним кроком є перевірка запропонованих моделей на реальних наборах даних (наприклад, вимірювання сейсмічних датчиків, телеметрія промислового обладнання) з реальними позначками інцидентів. По-друге, у випадку соціальних медіа існує виклик перевірки достовірності: моделі можуть реагувати на хвилю повідомлень, але серед цих повідомлень можуть бути чутки чи неправдива інформація. Вирішення цього потребує поєднання машинного аналізу з перевіркою надійних джерел або введення коефіцієнтів довіри. По-третє, питання описовості залишається відкритим: для практичного використання рятувальними службами система раннього оповіщення повинна не лише видати тривогу, але й надати певні інтерпретації – що саме сталося, який сенсор чи джерело даних спрацювало, який прогноз розвитку. Глибокі моделі в основі є "чорними ящиками", тому корисно досліджувати методи описового (пояснювального) штучного інтелекту для таких систем.

Підсумовуючи, наше дослідження підтверджує, що моделі машинного навчання – і особливо глибокого навчання – здатні суттєво підвищити ефективність раннього виявлення надзвичайних ситуацій. Вони забезпечують як більшу точність, так і швидкість реагування, використовуючи багатство даних сучасного цифрового світу. По мірі подальшого вдосконалення цих методів та вирішення супутніх викликів, можна очікувати появу нових поколінь інтелектуальних систем оповіщення, що допоможуть врятувати життя та мінімізувати збитки від надзвичайних ситуацій.

ЛІТЕРАТУРА

1. Disaster and Pandemic Management Using Machine Learning: A Survey / V. Chamola et al. IEEE Internet of Things Journal. 2020. P. 1.
URL: https://doi.org/10.1109/jiot.2020.3044966.
2. Early detection of emergency events from social media: a new text clustering approach / L. Huang et al. Natural Hazards. 2022. Vol. 111, no. 1. P. 851–875.
URL: https://doi.org/10.1007/s11069-021-05081-1.

3. Luthfee, A. A., Abdulla, R., Thiruchelvam, V., Rana, M. E., Mukil, A., Bathich, A., Lau, C. Y. Early flood detection and avoidance using IoT and machine learning// *American Institute of Physics Conference Series*. – 2024. – Т. 3161. – Стаття № 020017.
URL: https://doi.org/10.1063/5.0230082.
4. Early Detection of Earthquakes Using IoT and Cloud Infrastructure: A Survey / M. S. Abdalzaher et al. *Sustainability*. 2023. Vol. 15, no. 15. P. 11713.
URL: https://doi.org/10.3390/su151511713.
5. Real-Time Fault Tracking and Ground Motion Prediction for Large Earthquakes With HR-GNSS and Deep Learning / J. Lin et al. Journal of Geophysical Research: Solid Earth. 2023. Vol. 128, no. 12. URL: https://doi.org/10.1029/2023jb027255.
6. Shen H., Ju Y., Zhu Z. Extracting Useful Emergency Information from Social Media: A Method Integrating Machine Learning and Rule-Based Classification. International Journal of Environmental Research and Public Health. 2023. Vol. 20, no. 3. P. 1862.
URL: https://doi.org/10.3390/ijerph20031862.
7. Duraj, A., Szczepaniak, P. S., Sadok, A. Detection of Anomalies in Data Streams Using the LSTM-CNN Model // *Sensors*. – 2023. – Т. 25, № 5. – Стаття № 1610.
URL: https://doi.org/10.3390/s25051610.
8. LT-FS-ID: Log-Transformed Feature Learning and Feature-Scaling-Based Machine Learning Algorithms to Predict the k-Barriers for Intrusion Detection Using Wireless Sensor Network / A. Singh et al. Sensors. 2022. Vol. 22, no. 3. P. 1070.
URL: https://doi.org/10.3390/s22031070.
9. Hashemi-Beni L., Puthenparampil M., Jamali A. A low-cost IoT-based deep learning method of water gauge measurement for flood monitoring. *Geomatics, Natural Hazards and Risk*. 2024. Vol. 15, no. 1. URL: https://doi.org/10.1080/19475705.2024.2364777.
10. A Review of Cutting-Edge Sensor Technologies for Improved Flood Monitoring and Damage Assessment / Y. Tao et al. *Sensors*. 2024. Vol. 24, no. 21. P. 7090. URL: https://doi.org/10.3390/s24217090.
11. Величко Д.В. Комп'ютеризована система відеонагляду з функцією ідентифікації екстрених ситуацій на основі штучного інтелекту : кваліфікаційна робота бакалавра за спеціальністю „123 — Комп'ютерна інженерія“ / Величко Діана Вадимівна. – Тернопіль: ТНТУ, 2023. – 80 с.
12. Струтовський М. І., Нескородєва Т. В. Експертна система для визначення небезпечних ситуацій на злітних смугах із використанням машинного навчання. Прикладні інформаційні технології. 2023. С. 326–328.
13. Поспєлов, Б. Б., Андронов, В. А., Рибка, Є. О., Мелещенко, Р. Г., Карпець, К. М., Горінова, В. В., & Самойлов, М. О. (2019). Система раннього виявлення надзвичайних ситуацій.
14. Сейсмічний моніторинг. Головний центр спеціального контролю.
URL: https://gcsk.gov.ua/sejsmichnij-monitoring (дата звернення: 09.03.2025).

REFERENCES

1. Disaster and Pandemic Management Using Machine Learning: A Survey / V. Chamola et al. IEEE Internet of Things Journal. 2020. P. 1.
URL: https://doi.org/10.1109/jiot.2020.3044966.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)

2. Early detection of emergency events from social media: a new text clustering approach / L. Huang et al. Natural Hazards. 2022. Vol. 111, no. 1. P. 851–875.
URL: https://doi.org/10.1007/s11069-021-05081-1.
3. Luthfee, A. A., Abdulla, R., Thiruchelvam, V., Rana, M. E., Mukil, A., Bathich, A., Lau, C. Y. Early flood detection and avoidance using IoT and machine learning// *American Institute of Physics Conference Series*. – 2024. – Т. 3161. – Стаття № 020017.
URL: https://doi.org/10.1063/5.0230082.
4. Early Detection of Earthquakes Using IoT and Cloud Infrastructure: A Survey / M. S. Abdalzaher et al. *Sustainability*. 2023. Vol. 15, no. 15. P. 11713.
URL: https://doi.org/10.3390/su151511713.
5. Real-Time Fault Tracking and Ground Motion Prediction for Large Earthquakes With HR-GNSS and Deep Learning / J. Lin et al. Journal of Geophysical Research: Solid Earth. 2023. Vol. 128, no. 12. URL: https://doi.org/10.1029/2023jb027255.
6. Shen H., Ju Y., Zhu Z. Extracting Useful Emergency Information from Social Media: A Method Integrating Machine Learning and Rule-Based Classification. International Journal of Environmental Research and Public Health. 2023. Vol. 20, no. 3. P. 1862.
URL: https://doi.org/10.3390/ijerph20031862.
7. Duraj, A., Szczepaniak, P. S., Sadok, A. Detection of Anomalies in Data Streams Using the LSTM-CNN Model // *Sensors*. – 2023. – Т. 25, № 5. – Стаття № 1610.
URL: https://doi.org/10.3390/s25051610.
8. LT-FS-ID: Log-Transformed Feature Learning and Feature-Scaling-Based Machine Learning Algorithms to Predict the k-Barriers for Intrusion Detection Using Wireless Sensor Network / A. Singh et al. Sensors. 2022. Vol. 22, no. 3. P. 1070.
URL: https://doi.org/10.3390/s22031070.
9. Hashemi-Beni L., Puthenparampil M., Jamali A. A low-cost IoT-based deep learning method of water gauge measurement for flood monitoring. *Geomatics, Natural Hazards and Risk*. 2024. Vol. 15, no. 1. URL: https://doi.org/10.1080/19475705.2024.2364777.
10. A Review of Cutting-Edge Sensor Technologies for Improved Flood Monitoring and Damage Assessment / Y. Tao et al. *Sensors*. 2024. Vol. 24, no. 21. P. 7090.
URL: https://doi.org/10.3390/s24217090.
11. Velychko D.V. Kompiuteryzovana systema videonahliadu z funktsiieiu identyfikatsii ekstrenykh sytuatsii na osnovi shtuchnoho intelektu : kvalifikatsiina robota bakalavra za spetsialnistiu „123 — Kompiuterna inzheneriia“ / Velychko Diana Vadymivna. – Ternopil: TNTU, 2023. – 80 c.
12. Strutovskyi M. I., Neskorodieva T. V. Ekspertna systema dlia vyznachennia nebezpechnykh sytuatsii na zlitnykh smuhakh iz vykorystanniam mashynnoho navchannia. Prykladni informatsiini tekhnolohii. 2023. S. 326–328.
13. Pospielov, B. B., Andronov, V. A., Rybka, Ye. O., Meleshchenko, R. H., Karpets, K. M., Horinova, V. V., & Samoilov, M. O. (2019). Systema rannoho vyiavlennia nadzvychainykh sytuatsii.
14. Seismichnyi monitorynh. Holovnyi tsentr spetsialnoho kontroliu.
URL: https://gcsk.gov.ua/sejsmichnij-monitoring (date of access: 09.03.2025)

Received 05.05.2025.
Accepted 07.05.2025.

Application of machine learning models for early detection of emergency situations based on streaming big data

The article addresses the pressing issue of early detection of emergency situations, such as natural disasters, industrial accidents, or epidemics, through the application of machine learning and deep learning models. The focus is on analyzing streaming big data sourced from Internet of Things (IoT) sensor networks and social media platforms, which provide real-time information. Traditional early warning systems, relying on methods like threshold detectors or statistical models, often lack the speed and precision needed to process large volumes of heterogeneous data in real time. To overcome these limitations, the study explores the effectiveness of advanced machine learning techniques, with an emphasis on deep learning. A hybrid LSTM-CNN model is proposed, integrating convolutional neural networks (CNN) for extracting local features from time series data with long short-term memory (LSTM) networks for capturing long-term dependencies. This model was evaluated using synthetic data from the Yahoo Webscope S5 dataset and real-world streams, such as Twitter posts during an earthquake in the Ternopil region. Experimental results revealed that the hybrid LSTM-CNN model achieves high accuracy (F1=0.90) and the shortest average detection latency (≈5.5 s), significantly outperforming traditional methods like threshold detectors (F1=0.67, latency 15 s) and support vector machines (SVM, F1=0.80, latency 8.5 s). Comparative analysis also included LSTM and LSTM-autoencoder models, which yielded slightly lower performance (F1=0.88 and F1=0.77, respectively) but still surpassed classical approaches. The advantages of deep learning are evident not only in higher accuracy but also in the models' ability to detect subtle anomaly signals at early stages, which is critical for timely emergency response. Additionally, the potential of social media as a data source was demonstrated: Twitter analysis enabled earthquake detection within 1-5 minutes of its onset, outpacing official reports. These findings highlight the promise of the proposed models for emergency monitoring systems, such as industrial safety platforms or crisis management centers, where speed and reliability are paramount. The study also outlines limitations, including the need for broader testing on real-world datasets and addressing false positives in social media data.

Шопський Орест Михайлович - ад'юнкт кафедри інформаційних технологій та систем електронних комунікацій, Львівський державний університет безпеки життєдіяльності

Головатий Роман Русланович - к.т.н., доцент, кафедра інформаційних технологій та систем електронних комунікацій, Львівський державний університет безпеки життєдіяльності.

Shopskyi Orest - Phd of the Department of Information Technologies and Electronic Communication Systems, Lviv State University of Life Safety.

Golovatiy Roman - Candidate of Technical Sciences, Associate Professor, Department of Information Technologies and Electronic Communication Systems, Lviv State University of Life Safety.

ISSN 1562-9945 (Print)
ISSN 2707-7977 (Online)