проте вони є лише наочним прикладом роботи програмного засобу, а не готовим та безпечним рішенням для роботи в реальних умовах. Таким чином, існує необхідність у рішенні, яке б поєднувало в собі простоту інтеграції SaaS продуктів і доступність open-source програмного забезпечення.

## ПЕРЕЛІК ПОСИЛАНЬ


1. What is identity and access management? Guide to IAM [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system.
2. НД ТЗІ 1.1-003-99 [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.ua/assets/files/1.1_003_99.pdf.
3. What is Okta? [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://support.okta.com/help/s/article/What-is-Okta?language=en_US#:~:text=Okta%20features%20include%20Provisioning%2C%20Single,for%20organization%20security%20and%20control..
4. What is OpenIAM? [Електронний ресурс] – Режим доступу до ресурсу: https://docs.openiam.com/docs-4.2.0.8/getting-started/1-what_is_openiam.
5. Understand How You Can Use Auth0 [Електронний ресурс] – Режим доступу до ресурсу: https://auth0.com/docs/get-started/auth0-overview.
6. Ory Kratos Introduction [Електронний ресурс] – Режим доступу до ресурсу: https://www.ory.sh/kratos/docs/#:~:text=Ory%20Kratos%20is%20an%20API,application%20needs%20to%20deal%20with%3A&text=Admin%20APIs%3A%20Import%2C%20update%2C%20delete%20identities.
7. Keycloak - About [Електронний ресурс] – Режим доступу до ресурсу: https://www.keycloak.org/about#:~:text=Keycloak%20is%20an%20open%20source,with%20little%20to%20no%20code.&text=Trying%20Keycloak%20is%20quick%20and%20easy.



УДК [004.942+005.5]: 614.84



О.М. Шопський[1], О.В. Придатко[1], І.О. Малець[1]
[1]Львівський державний університет безпеки життєдіяльності ДСНС України, Львів


## АНАЛІТИКА ВЕЛИКИХ МАСИВІВ ДАНИХ ДЛЯ ПРОГНОЗУВАННЯ РИЗИКОВИХ СИТУАЦІЙ


**Анотація.** Описано процес узагальнення масиву даних для аналітики прогнозування ризикових ситуацій.



**Ключові слова.** *Система оперативно-диспетчерського управління, СОДУ, геоінформаційна система.*


**Вступ.** Техногенне навантаження та зміни клімату стимулюють до частого виникнення різного роду ризикових ситуацій: пожеж, ДТП, паводків тощо. Кожна подія супроводжується значними матеріальними збитками, а не

рідко і людськими жертвами. З метою оперативного реагування та координації дії рятувальних підрозділів з 2007 року в Головному управлінні Державної служби України з надзвичайних ситуацій у Львівській області впроваджено програмно-апаратний комплекс «Система оперативно-диспетчерського управління» (СОДУ), метою якої є максимальна оптимізація функцій оперативно-диспетчерського управління із використанням новітніх інформаційних технологій.

За час роботи інформаційною системою було зібрано велику базу даних щодо характеру та місця виникнення небезпечних подій, час обробки повідомлення про подію від заявника, час висилки сил та засобів, час доїзду рятувальних автомобілів, кількість задіяних ресурсів, час локалізації та ліквідації тощо. До цієї бази входять дані щодо розміщення і характеристики джерел водопостачання, оперативні плани пожежогасіння, картки на населені пункти, хімічно та потенційно небезпечні об'єкти, зони підтоплення, лісові господарства, гірські маршрути і стежки, торфополя, захисні споруди та інше.

Увесь цей масив даних потребує пошуку і очищення від помилок, опрацювання і глибокого аналізу, щодо визначення закономірностей виникнення тих чи інших ризикових ситуацій. Така аналітика дозволить створити модель швидкого прогнозування можливого виникнення тих чи інших подій в залежності від обраних критеріїв. На основі отриманих даних можливо буде приймати рішення щодо запобігання та унеможливлення виникнення таких подій, адже запобігти ризиковій ситуації легше, ніж долати її наслідки.

**Основний зміст роботи.** Для побудови моделі обробки великих масивів даних, окреслено виконання таких етапів:

1. Кластеризація даних з бази та побудова нових структур (таблиці представлення).

2. Перевірка коректності даних. На цьому етапі потрібно відібрати події що не відповідають критеріям. Наприклад ті в котрих різниця часу між отриманням повідомлення і ліквідацією більше доби (лісові, торф'яні пожежі). Для цих даних пропонується формувати окрему вибірку. Також в окрему вибірку слід вносити дані щодо проведення пожежно-технічних та інших навчань особового складу (перевірка боєздатності, заняття).

3. Окремим блоком опрацювання даних є геокодування місця події в географічні координати. Для цього потрібно використати інструмент для пошуку OSM даних - Nominatim. Це також дозволить виявити типові помилки при введенні адреси. Маючи координати, всі події будуть розміщені на цифровій векторній карті, а з допомогою PostGIS буде проведено аналіз щодо зосередження подій в певній локації, в розрізі часових показників, класифікації подій та інших критеріїв. Шари з оперативними планами пожежогасіння, джерелами водопостачання, торфополями, хімічно-небезпечними об’єктами дозволяють проаналізувати їх взаємозв’язок із подіями. Шар з електронними сиренами дозволяє визначити можливість оповіщення населення біля об'єктів по підвищених номерах виклику. Дані часових показників виїзду і прибуття аварійно рятувальної техніки, місця події і шари районів виїзду дають

можливість перевірки коректності меж зон обслуговування і визначення нормативного часу доїзду до конкретного населеного пункту.

4. Розробити алгоритми сортування слабко-структурованих даних за визначеними критеріями.

5. Розробити алгоритми пошуку та відбору даних за певними класифікаційними ознаками.

6. Провести регресійних аналіз та визначити рівень впливу аналізованих даних на показник ймовірності виникнення надзвичайних подій.

**Висновки.** В результаті, аналітика великих масивів даних надасть можливість сформувати базу знань щодо прийняття оперативних рішень. Також це дозволить обгрунтувати потребу створення добровільних та місцевих пожежних команд.

## ПЕРЕЛІК ПОСИЛАНЬ

1. Грицевич В. С. Статистичні ознаки та характеристики їхньої центральної тенденції: тексти лекцій / В. С. Грицевич. − Львів: Видавничий центр ЛНУ імені Івана Франка, 2008. − 52 с.

2. Гуліда Е.М. Завдання та методичні вказівки для виконання розрахунково-графічної роботи № 1 з дисципліни методологія та організація наукових досліджень для підготовки магістрів зі спеціальності 8.092801 «Пожежна безпека» / Е.М. Гуліда. – Львів: ЛДУ БЖД, 2013. – 19 с.

3. https://postgis.net/ Spatial and Geographic objects for PostgreSQL

УДК 004.46

Ю.А. Мілінчук[1], Р.С. Глушан[1]
[1]Національний технічний університет «Дніпровська політехніка», Дніпро, Україна

## АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРИ АТАКАХ НА ПЛАТІЖНЕ ТЕРМІНАЛЬНЕ ОБЛАДНАННЯ

**Анотація.** Розглянуто основні види термінального обладнання та проаналізовано атаки на термінальне обладнання, що здійснюються шкідливими програмами Tyupkin та Skimer.

***Ключові слова****: термінальне обладнання, Tyupkin, атаки на термінальне обладнання, ОС термінального обладнання* .

**Вступ.** Застосування термінального обладнання, яке включає в собі об’єднання різноманітних рішень, та сучасних технологій, забезпечує комфорт, зручність отримання послуг та раціональне споживання ресурсів для користувачів. Наразі інфраструктура термінального обладнання розвивається швидше, ніж засоби її захисту, що залишає великий простір для діяльності зловмисників, і це, в свою чергу, потребує пошуку нових засобів безпеки. На