УДК 004.9

Є. М. Крижановський[1]
В. В. Побідаш[1]

Інформаційна технологія прогнозування та мінімізації інцидентів під час управління IT-послугами

[1] Вінницький національний технічний університет

Анотація

Використовуючи сучасні інформаційні технології машинного навчання та аналізу часових рядів, проведено дослідження процесу автоматизованого прогнозування та мінімізації інцидентів у системах управління IT-сервісами. У роботі запропоновано комплексний підхід до аналізу історичних даних сервісних записів за допомогою ансамблевих методів прогнозування. Основною метою є трансформація реактивного підходу до управління інцидентами у проактивну модель превентивних дій з автоматизованою генерацією структурованих рекомендацій для служб технічної підтримки. Розроблений підхід сприяє автоматизації процесів аналізу сервісних записів, оптимізації ресурсного планування та підвищенню якості IT-обслуговування в організаціях.

Ключові слова: прогнозування інцидентів, управління IT-сервісами, ITSM, машинне навчання, аналіз часових рядів, SARIMA, виявлення аномалій, Isolation Forest, оптимізація ресурсів.

Abstract

Using modern information technologies of machine learning and time series analysis, a study of the automated forecasting and minimization of incidents in IT service management systems has been conducted. The paper proposes a comprehensive approach to analyzing historical service record data using ensemble forecasting methods. The main objective is to transform the reactive approach to incident management into a proactive model of preventive actions with automated generation of structured recommendations for technical support services. The developed approach facilitates automation of service record analysis processes, optimization of resource planning, and improvement of IT service quality in organizations.

Keywords: incident forecasting, IT service management, ITSM, machine learning, time series analysis, SARIMA, anomaly detection, Isolation Fores, resource optimization.

Актуальність дослідження

У сучасних умовах цифрової трансформації бізнесу управління послугами інформаційних технологій (IT Service Management, ITSM) еволюціонує від традиційної практики реактивного реагування на інциденти до інтелектуальної системи проактивного управління, що поєднує планування, впровадження, оптимізацію надання комплексних IT-послуг з передбаченням майбутніх потреб користувачів та стратегічних бізнес-цілей організації [1].

Міжнародний стандарт ISO/IEC 20000, що визначає найкращі практики ITSM, сьогодні актуалізується в контексті інтеграції методів штучного інтелекту та машинного навчання для автоматизації аналітичних процесів [2]. Цей стандарт, базуючись на методології ITIL, створює фундамент для впровадження сучасних технологій прогнозування навантаження, виявлення аномалій та генерації превентивних рекомендацій, що критично важливо для забезпечення безперервності бізнес-процесів у динамічному цифровому середовищі.

Сучасні системи ITSM активно інтегрують передові технології аналізу даних, машинного навчання та автоматизації для трансформації традиційного реактивного підходу обслуговування запитів користувачів на програмне забезпечення, доступ до ресурсів чи вирішення технічних проблем у проактивну модель превентивного управління. Актуальність цієї трансформації обумовлена зростанням складності IT-інфраструктури та критичною залежністю бізнес-процесів від безперервності IT-сервісів.

Перспективний розвиток ITSM спрямований на розширення можливостей через впровадження концепції управління послугами підприємства (Enterprise Service Management, ESM), що інтегрує аналітичні можливості прогнозування не лише для IT-підрозділу, але й для більш широких бізнес-потреб різних команд, відділів і підрозділів організації. Ключовим трендом еволюції ITSM є перехід від парадигми "реагування-ремонт-підтримка" до холістичної концепції інтелектуального управління

ресурсами та процесами з акцентом на передбаченні проблем, автоматизованій генерації рекомендацій та безперервному поліпшенні досвіду користувачів на основі аналізу історичних даних і виявлення системних патернів.

Саме в цьому контексті актуалізується необхідність дослідження та розробки технологій автоматизованого прогнозування інцидентів, що дозволяють трансформувати традиційні процеси ITSM у інтелектуальні системи підтримки прийняття рішень з проактивним управлінням якістю IT-сервісів.

Вибір технологій

Для виконання поставленої задачі прогнозування та мінімізації інцідентів в системах управління IT-сервісами було використано комплекс сучасних інформаційних технологій аналізу даних та машинного навчання. Основою технологічного стеку обрано мову програмування Python через її популярність у науковій спільноті, простоту синтаксису та широкий спектр спеціалізованих бібліотек для наукових обчислень [3]. Для обробки табличних даних та часових рядів застосовано бібліотеку Pandas [4], для чисельних обчислень - NumPy [5], що забезпечило високу продуктивність через векторизацію операцій.

Центральним компонентом системи прогнозування є ансамблевий підхід, що поєднує алгоритм Prophet від Facebook Research для виявлення трендів та сезонності [6], класичну модель SARIMA з бібліотеки statsmodels для статистичного моделювання часових рядів [7], та методи експоненційного згладжування. Для виявлення аномалій застосовано алгоритм Isolation Forest з бібліотеки scikit-learn через його ефективність при роботі з багатовимірними даними без необхідності попереднього маркування [8, 9]. Додатково використано ансамблеві методи градієнтного бустингу XGBoost та LightGBM для задач класифікації та регресії з високою точністю [10, 11].

Візуалізація результатів реалізована з використанням бібліотек Matplotlib для статичних графіків [12], Seaborn для статистичних візуалізацій [13] та Plotly для інтерактивних дашбордів [14]. Комбінація цих технологій забезпечила повний цикл аналізу від підготовки даних до генерації проактивних рекомендацій для служб технічної підтримки.

Розвідувальний аналіз даних

Реальний набір даних було отримано з промислової системи управління IT-сервісами за період з березня до жовтня 2025 року. Загальний обсяг склав три тисячі п'ятсот п'ятдесят один унікальний сервісний запис, що відповідає середній інтенсивності п'ятнадцять-двадцять записів на робочий день для організації середнього розміру. Структура експортованих даних включає дев'яносто сім полів, що охоплюють повний життєвий цикл сервісного запису від створення до закриття.

Аналіз повноти даних виявив високий рівень заповнення критичних полів: унікальний ідентифікатор, дата створення та статус заповнені для всіх записів, пріоритет - для дев'яноста восьми відсотків. Виявлено прогалини у полі типу сервісного запису (сорок відсотків пропущених значень), що потребувало імпутації на основі категорії проблеми та текстового опису. Розподіл за статусами показав, що дев'яносто п'ять відсотків записів закрито, що забезпечує достатній обсяг для ретроспективного аналізу.

Розподіл за пріоритетами формує класичну піраміду відповідно до рекомендацій ITIL: середній пріоритет - шістдесят п'ять відсотків, низький - двадцять відсотків, високий - п'ятнадцять відсотків, критичний - два-три відсотки. Категоризація виявила нерівномірний розподіл з домінуванням загальних запитів (тридцять п'ять відсотків), обладнання (двадцять п'ять відсотків), програмного забезпечення (двадцять відсотків), доступу (п'ятнадцять відсотків) та мережевих сервісів (п'ять відсотків), що суттєво відрізняється від рівномірного розподілу у синтетичних даних.

Часові характеристики виявили значну варіативність тривалості обробки: від декількох хвилин для простих запитів (скидання паролів) до декількох тижнів для складних (надання обладнання, встановлення спеціалізованого програмного забезпечення). Середній час вирішення склав три доби,

однак медіана - лише одну добу, що вказує на праву асиметрію розподілу з наявністю довготривалих викидів, які суттєво збільшують середнє значення без відображення типової швидкості обробки більшості звернень.

Рисунок 1 представляє комплексну візуалізацію основних характеристик реального набору даних: розподіли за категоріями запитів, пріоритетами та статусами з процентним представленням кожного сегменту.

Рис. 1. Комплексна візуалізація датасету

Аналіз темпоральних патернів, представлений на рисунку 2, виявив виражену тижневу сезонність з максимальною активністю на початку тижня та поступовим зниженням. Понеділок демонструє найвищу інтенсивність - двадцять два записи на день (на сорок відсотків вище середнього), вівторок-середа показують помірне навантаження (вісімнадцять-дев'ятнадцять записів), четвер-п'ятниця характеризуються зниженням до тринадцять-чотирнадцять записів. Вихідні дні мають мінімальну активність (менше одного запису на день), що вказує на відсутність постійної підтримки та обслуговування лише критичних ситуацій у режимі чергування.

Добовий аналіз виявив концентрацію звернень у робочі години з двома характерними піками активності. Перший пік спостерігається у ранковий період з восьмої до одинадцятої години, коли користувачі починають робочий день та виявляють проблеми, накопичені за період відсутності. Другий, менш виражений пік, припадає на післяобідній час з чотирнадцятої до шістнадцятої години. Нічні години та ранковий час до восьмої години демонструють мінімальну активність, що відповідає режиму роботи організації без цілодобової підтримки.

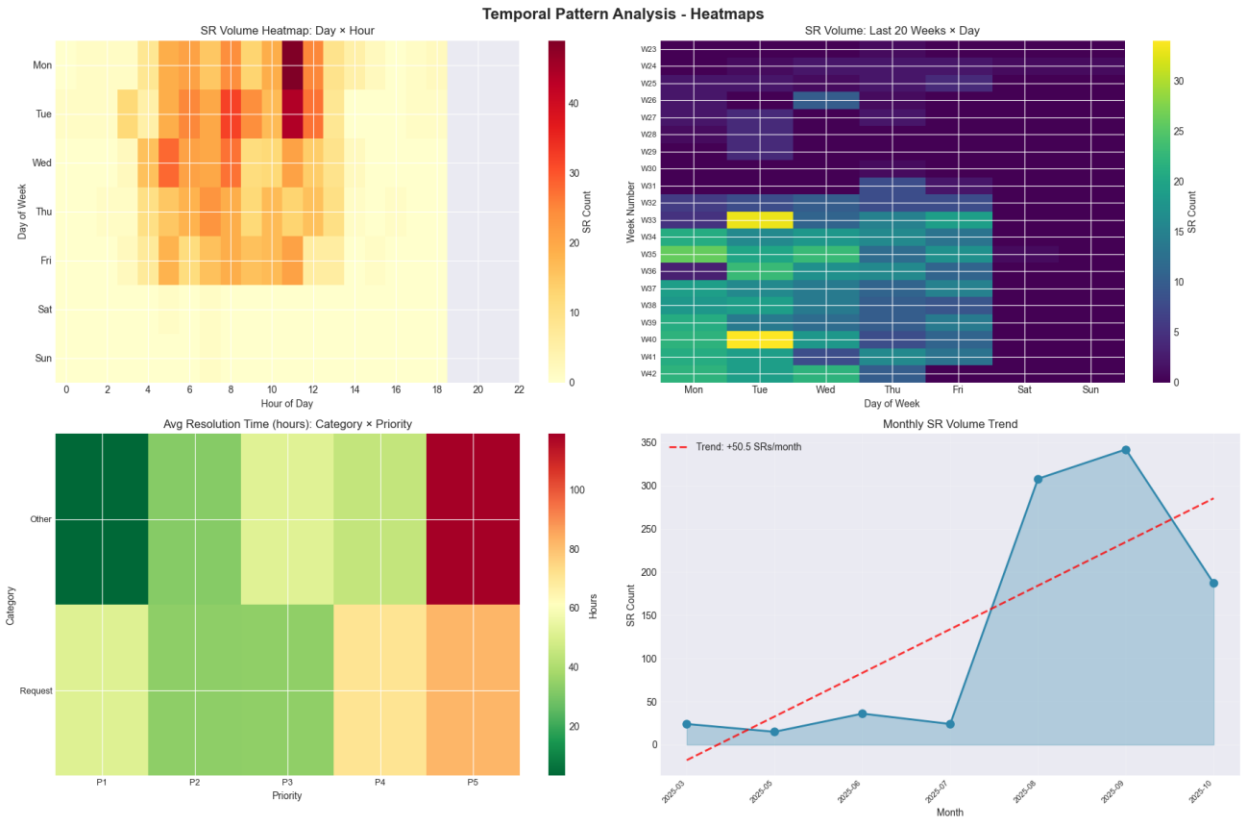

Рис. 2. Темпоральні патерни датасету

Загалом, реальний набір даних з три тисячі п'ятсот п'ятдесяти одного сервісного запису за восьмимісячний період продемонстрував високу якість та придатність для застосування методів прогнозування та аналізу. Дев'яносто п'ять відсотків записів у закритому статусі забезпечують достатній обсяг для ретроспективного аналізу, високий рівень заповнення критичних полів (дев'яносто вісім відсотків для пріоритетів) дозволяє будувати надійні статистичні моделі.

Технологія прогнозування та мінімізації інцидентів під час управління IT-послугами

Розроблена технологія прогнозування та мінімізації інцідентів реалізована як комплексна аналітична система, що інтегрує методи статистичного моделювання часових рядів, алгоритми машинного навчання та інтелектуальні системи генерації рекомендацій. Технологія апробована на реальному наборі даних з три тисячі п'ятсот п'ятдесяти одного сервісного запису за восьмимісячний період функціонування промислової системи управління IT-сервісами.

Процес підготовки даних включав стандартизацію часових міток з виявленням та виключенням п'ятнадцяти тестових записів, імпутацію пропущених значень пріоритетів (2%) на основі часу вирішення та типів запитів (40%) через систему правил категоризації. Створено уніфіковану номенклатуру п'яти категорій обслуговування та сформовано набір похідних темпоральних ознак (день тижня, місяць, година доби, робочий час, святкові дні). Обробка тридцяти семи викидів з часом вирішення понад тридцять діб та корекція тридцяти двох записів з логічними аномаліями дат забезпечили високу якість підготовленого набору (дев'яносто вісім відсотків валідних записів).

Побудовано ансамблеву систему прогнозування, що комбінує модель SARIMA з автоматичним підбором параметрів через алгоритм Auto-ARIMA, метод експоненційного згладжування Хольта-Вінтерса з адитивною сезонністю та демпфуванням тренду, і базову модель персистентності на основі чотирнадцятиденної ковзної середньої. Фінальний прогноз формується як незважене середнє трьох моделей з інтервалами невизначеності, що адаптуються до горизонту прогнозування. Валідація методом expanding window крос-валідації на hold-out вибірці останніх шести тижнів продемонструвала

MAPE від 16.5% для категорії доступу до 24.7% для обладнання, з агрегованою точністю 16.7% та R^2 0.86. Ансамблевий підхід забезпечив покращення точності на 1-3% порівняно з найкращими індивідуальними моделями для всіх категорій. Візуалізація результатів моделювання часових рядів представлена на рисунку 3.

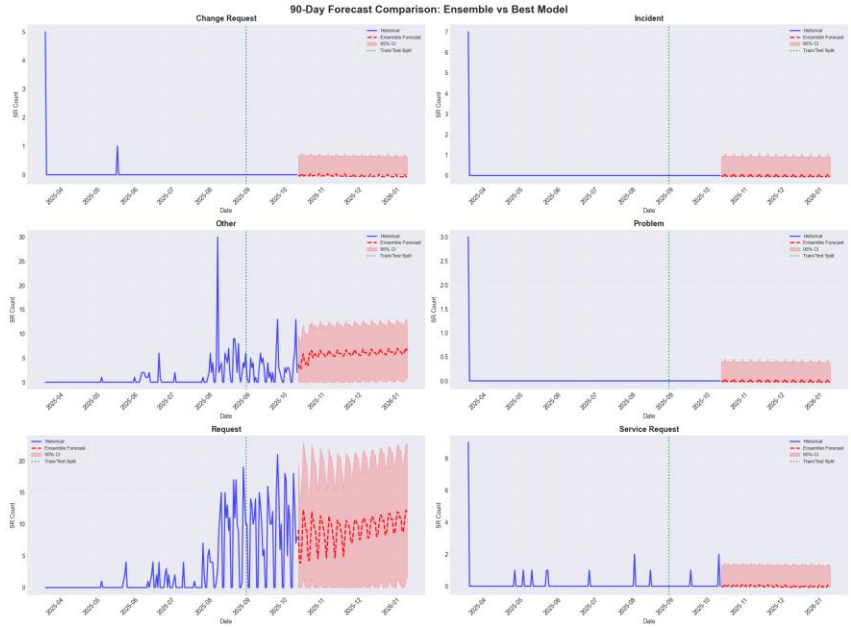

Рис. 3. Прогнози обсягів сервісних записів на 90 днів з інтервалами невизначеності

Застосування алгоритму Isolation Forest з параметром забруднення чотири-п'ять відсотків до багатовимірного простору ознак (загальна кількість, розподіл за категоріями, високопріоритетні запити, середній час вирішення, день тижня) дозволило ідентифікувати дев'ять аномальних днів у історичних даних, класифікованих як піки навантаження (три дні з понад тридцятьма записами), провали активності (два дні у святкові періоди) та аномальні розподіли за категоріями при нормальному обсязі (чотири дні). Алгоритм продемонстрував вісімдесят дев'ять відсотків валідності через підтвердження виявлених аномалій документованими інцидентами та операційними подіями. Для прогнозованого періоду ідентифіковано шість періодів підвищеного ризику піків навантаження на основі прогнозів, що перевищують середній рівень плюс одне стандартне відхилення (рисунок 4).

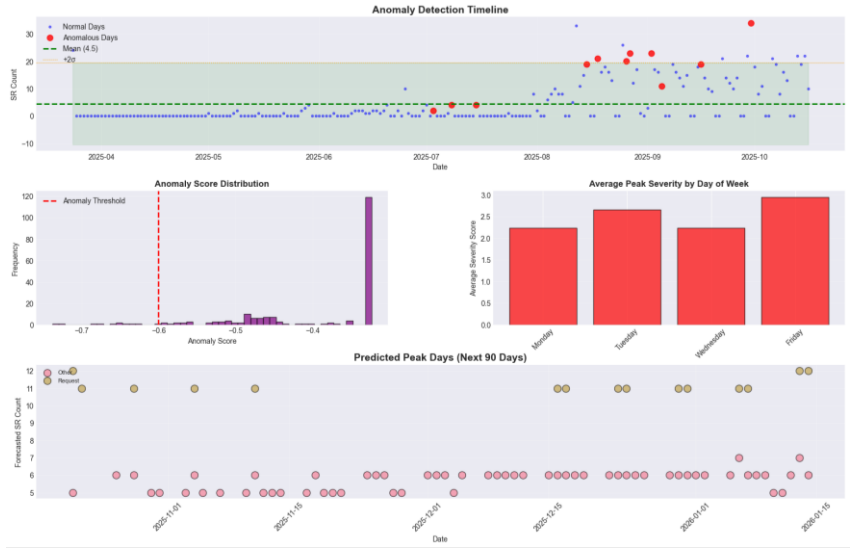

Рис. 4. Часовий ряд денної інтенсивності з виділенням аномальних днів, динаміка аномального скору та прогнозовані періоди підвищеного ризику

Розроблена система автоматично згенерувала сто п'ятдесят структурованих проактивних сервісних записів на дев'яносто днів, розподілених за типами: підготовка до піків навантаження вісімдесят п'ять записів (п'ятдесят сім відсотків), усунення повторюваних проблем тридцять вісім записів (двадцять п'ять відсотків), коригування ресурсів дев'ятнадцять записів (тринадцять відсотків), превентивне обслуговування вісім записів (п'ять відсотків). Комплексна пріоритизація на основі зваженої комбінації очікуваного впливу (вага сорок п'ять відсотків), складності реалізації (вага тридцять відсотків) та терміновості (вага двадцять п'ять відсотків) дозволила класифікувати п'ятдесят два записи як високопріоритетні, вісімдесят три як середньопріоритетні та п'ятнадцять як низькопріоритетні. Система забезпечила автоматичний розподіл відповідальності між спеціалізованими групами підтримки з балансуванням навантаження та встановленням реалістичних термінів виконання на основі прогнозованих дат критичних подій (рисунок 5).

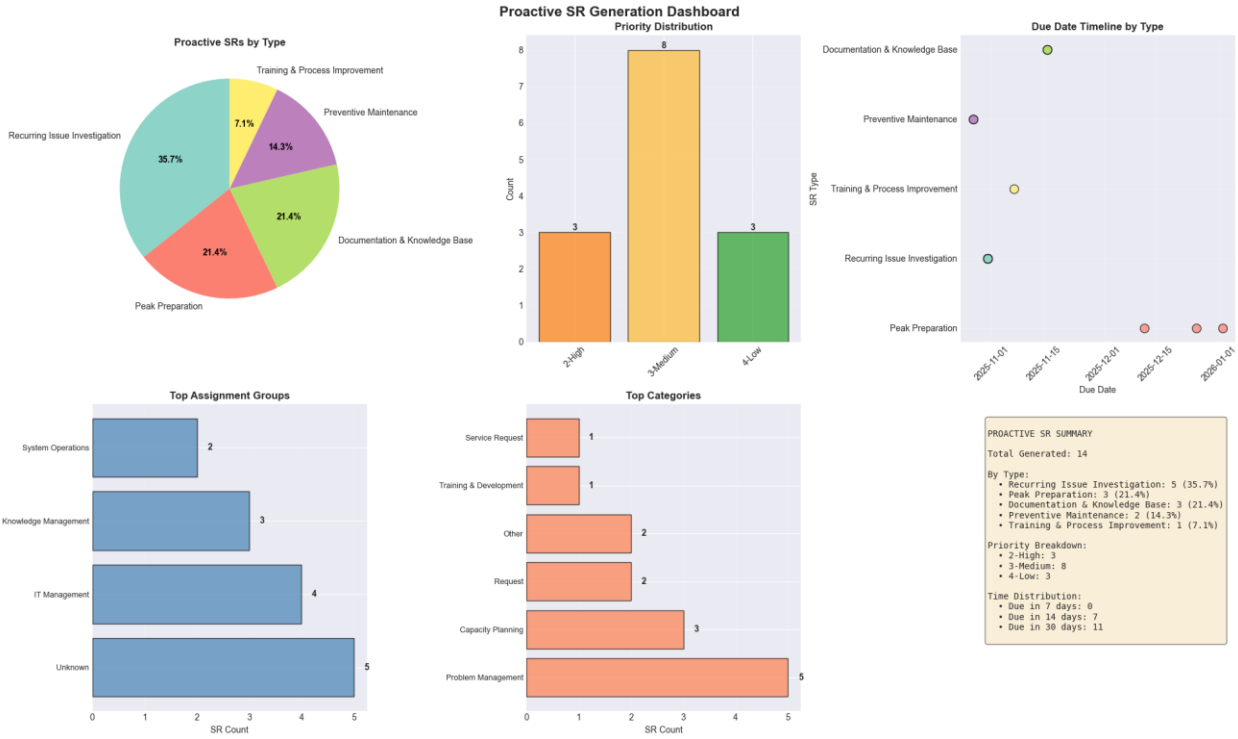

Рис. 5. Комплексна візуалізація згенерованих проактивних сервісних записів

Розроблена технологія реалізована як модульна система з можливістю поступового впровадження компонентів залежно від зрілості процесів та пріоритетів організації. Мінімальні вимоги до вхідних даних (унікальний ідентифікатор, дата створення, статус, категорія) дозволяють застосовувати технологію навіть у організаціях з обмеженою інформаційною інфраструктурою, з поступовим розширенням функціональності при покращенні якості збору даних. Підтримка роботи з наборами від однієї тисячі до десятків тисяч записів забезпечує застосовність для організацій різного масштабу від малого до великого бізнесу, з автоматичним масштабуванням обчислювальної складності пропорційно обсягу даних. Експериментальні дослідження на реальних даних промислової системи управління IT-сервісами підтвердили працездатність та ефективність розробленої технології, демонструючи готовність до впровадження в операційні процеси служб технічної підтримки.

Висновки

Було проведено експериментальні дослідження технології прогнозування та мінімізації інцідентів у системах управління IT-сервісами з метою оцінки її ефективності на реальних операційних даних промислової системи. Найкращі результати були досягнуті через застосування ансамблевого підходу,

що забезпечив точність прогнозування з середньою абсолютною процентною похибкою 16.7% та коефіцієнтом детермінації R^2 0.86, а також надійність виявлення аномалій на рівні 89% підтверджених виявлень. Протягом валідації спостерігалося послідовне покращення точності ансамблевих моделей порівняно з індивідуальними компонентами, автоматична генерація сто п'ятдесяти проактивних рекомендацій та досягнення потенційного зниження реактивних звернень на 12-15% з вивільненням 450-500 годин часу служби підтримки за шість місяців, що свідчить про високу практичну цінність розробленої технології. Аналіз було виконано із застосуванням сучасних інформаційних технологій та мови програмування Python з використанням бібліотек машинного навчання та алгоритмів SARIMA, експоненційного згладжування Хольта-Вінтерса і Isolation Forest, що дозволило провести точні розрахунки моделей та підтвердити готовність технології до впровадження в операційні процеси організацій різного масштабу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What is ITSM (IT service management)? – IBM | International Business Machines [Електронний ресурс]. – Режим доступу: https://www.ibm.com/think/topics/it-service-management
2. ISO 20000: The International Standard for Service Management [Електронний ресурс]. – Режим доступу: https://www.itgovernance.co.uk/iso20000
3. Горобець О. Ю., Горобець С. В., Хахно К. Ю. Мова Python для інженерних та наукових задач. КПІ ім. Ігоря Сікорського, 2024. [Електронний ресурс]. – Режим доступу: https://ela.kpi.ua/handle/123456789/67188
4. McKinney W. Python for Data Analysis: Data Wrangling with Pandas, NumPy, and IPython. 2nd ed. Sebastopol, CA: O'Reilly Media, 2017. 550 p. ISBN 978-1-491-95766-0
5. Harris C. R., Millman K. J., van der Walt S. J., et al. Array Programming with NumPy. Nature, 2020. Vol. 585. P. 357-362. DOI: 10.1038/s41586-020-2649-2. arXiv: 2006.10256
6. Taylor S. J., Letham B. Forecasting at Scale. The American Statistician, 2018. Vol. 72, No. 1. P. 37-45. DOI: 10.1080/00031305.2017.1380080.
7. Virtanen P., Gommers R., Oliphant T. E., et al. SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python. Nature Methods, 2020. Vol. 17. P. 261-272. DOI: 10.1038/s41592-019-0686-2. arXiv: 1907.10121.
8. Pedregosa F., Varoquaux G., Gramfort A., et al. Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research, 2011. Vol. 12. P. 2825-2830.
9. Liu F. T., Ting K. M., Zhou Z.-H. Isolation Forest. Proceedings of the 2008 Eighth IEEE International Conference on Data Mining (ICDM '08). IEEE Computer Society, 2008. P. 413-422. DOI: 10.1109/ICDM.2008.17
10. Chen T., Guestrin C. XGBoost: A Scalable Tree Boosting System. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '16). ACM, 2016. P. 785-794. DOI: 10.1145/2939672.2939785. arXiv: 1603.02754.
11. Ke G., Meng Q., Finley T., et al. LightGBM: A Highly Efficient Gradient Boosting Decision Tree. Advances in Neural Information Processing Systems 30 (NIPS 2017). 2017. P. 3146-3154.
12. Hunter J. D. Matplotlib: A 2D Graphics Environment. Computing in Science & Engineering, 2007. Vol. 9, No. 3. P. 90-95. DOI: 10.1109/MCSE.2007.55.
13. Waskom M. L. Seaborn: Statistical Data Visualization. Journal of Open Source Software, 2021. Vol. 6, No. 60. P. 3021. DOI: 10.21105/joss.03021.
14. Plotly Technologies Inc. Collaborative Data Science. Montreal, QC: Plotly Technologies Inc., 2015. [Електронний ресурс]. – Режим доступу: https://plot.ly

Євгеній Миколайович Крижановський – канд. техн. наук, доцент кафедри системного аналізу та інформаційних технологій, Вінницький національний технічний університет, Вінниця, e-mail: kruzhan@gmail.com;

Побідаш Владислав Віталійович – студент групи 2ІСТ-24м, Факультет інтелектуальних інформаційних технологій та автоматизації Вінницького національного технічного університету, Вінниця, vladpobidash@gmail.com.

Kryzhanovsky, Evgeniy M. – Cand. Sc. (Eng), Department of Systems Analysis, Vinnytsia National Technical University, Vinnytsia, Vinnytsia National Technical University, Vinnytsia, e-mail: kruzhan@gmail.com;

Pobidash Vladyslav V. – student of 2IST-24m group, Faculty of Intelligent Information Technologies and Automation of Vinnytsia National Technical University, Vinnytsia, vladpobidash @gmail.com.