УДК 004.738.5 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.6

В. Д. БОЙКО
кандидат технічних наук, доцент,
доцент кафедри кібербезпеки
Національний університет «Одеська юридична академія»
ORCID: 0000-0001-5929-657X

В. І. БЕВЗА
магістр за спеціальністю 125 «Кібербезпека»
Національний університет «Одеська юридична академія»
ORCID: 0009-0007-2695-969X

В. М. СЛАТВІНСЬКА
доктор філософії, асистент кафедри кібербезпеки
Національний університет «Одеська юридична академія»
ORCID: 0000-0002-6082-981X

ІНІЦІЮВАННЯ МЕРЕЖЕВОЇ АКТИВНОСТІ В WINDOWS ЗА ДОПОМОГОЮ NETSTAT

Мета статті. Метою статті є створення комплексного підходу до ініціювання та аналізу мережевої активності в операційній системі Windows за допомогою утиліти netstat з урахуванням сучасних вимог, пов'язаних з відстеженням системи, та гарантуванням можливості інтерпретації результатів діагностичної активності найефективнішим чином. У рамках роботи також буде зроблено спробу стандартизувати використання Netstat, доповнити його іншими інструментами для автоматизації аналізу даних та перетворити його пропозиції на конкретні рекомендації для системних адміністраторів та експертів з кібербезпеки. Спеціальні програми для ідентифікації мережевих з'єднань, виявлення аномалій та аналізу навантаження також відіграють вирішальну роль у стабільності та безпеці інформаційних систем у динамічному мережевому середовищі.

Наукова новизна. Наукова новизна дослідження полягає у створенні класифікації станів TCP-з'єднань на основі даних, отриманих за допомогою netstat, що дозволяє ефективно інтерпретувати інформацію про мережеву активність у контексті діагностики системи. Архітектура системи моніторингу, що запропонована в цій роботі, включає чотири основні компоненти: збір первинних даних, обробку, аналіз та сповіщення про аномалії, розширює класичні підходи до використання утиліт Windows. Поєднання netstat із сучасними методами автоматизації та аналізу даних, особливо з часовими рядами та логуванням, надає нові можливості для виявлення трендів та аномалій.

Результати. В рамках дослідження було детально досліджено функціональність netstat, зокрема опції -a, -n, -o, -s та -r, які надають повний список активних з'єднань, IP-адрес, ідентифікаторів процесів, статистику для мережевих протоколів та таблиць маршрутизації. Було створено таблицю класифікації станів TCP-з'єднань (LISTENING, ESTABLISHED, TIMEWAIT, CLOSEWAIT) з описом діагностичних значень та рекомендаціями, згідно з якими можна ідентифікувати проблемні стани, наприклад, довгий CLOSE_WAIT. Результати, отримані з мережевих сеансів з IP-адресами 127.0.0.1 та 192.168.0.161 та портами 161:4147-4149, показані на рисунку 2, надають інформацію, пов'язану з інтенсивністю активності веб-застосунків, системними процесами, а також існуванням потенційних аномалій. Запропоновано способи написання сценаріїв для автоматизації збору даних та підключення до систем реєстрації даних для побудови часових рядів.

Висновки. Дослідження довело, що netstat ефективно запускає та моніторить мережеву активність у Windows та є корисним інструментом завдяки розширеним параметрам командного рядка та організованому методу збору даних для діагностики. Отримана архітектура моніторингу та класифікація стану з'єднання забезпечують основу для інтеграції традиційних утиліт із сучасними технологіями, такими як машинне навчання. Перспективи подальших досліджень включають розробку алгоритмів автоматичного виявлення аномалій, інтеграцію з хмарними системами, розробка адаптивних систем оповіщення, з практичними наслідками в галузі безпеки та оптимізації мережевих ресурсів (кібербезпека).

Ключові слова: *netstat, мережа, моніторинг, Windows, діагностика комп'ютерних мереж, безпека комп'ютерних мереж, кібербезпека.*

V. D. BOYKO
PhD in Engineering, Associate Professor,
Associate Professor of Cyber Security
National University Odesa Law Academy
ORCID: 0000-0001-5929-657X

V. I. BEVZA
Master's Degree in Cybersecurity (Specialty 125)
National University Odesa Law Academy
ORCID: 0009-0007-2695-969X

V. M. SLATVINSKA
PhD, Assistant at the Cybersecurity Department
National University Odesa Law Academy
ORCID: 0000-0002-6082-981X

INITIATING NETWORK ACTIVITY IN WINDOWS USING NETSTAT

The purpose of the article. The aim of the article is to create a complex approach to the initiation and analysis of network activity in the windows operating system with the help of the netstat utility with references to the current demands related to tracking of the system and guaranteeing the opportunity to interpret the findings of diagnostic activities in the most effective way. The work will also try to standardize the use of Netstat, complement it with other tools to automate the analysis of the data and translate its proposals into concrete recommendations for the system administrators and the cybersecurity experts. Specific applications for identifying network connections, anomaly detection and load analysis also play a crucial role in the stability and security of information systems in a dynamic network environment.

Scientific novelty. The scientific novelty of the research is the creation of a classification of TCP connection states on the basis of data obtained using netstat that permits effective interpretation of the information about network activity in the context of system diagnostics. The architecture of the monitoring system proposed in this work, which features four major components: primary data collection, processing, analysis, and notification about anomalies, extends classical approaches to the usage of Windows utilities. The combination of netstat together with modern automation and data analysis techniques, especially with time series and logging, provides new possibilities for trend and anomaly detection.

Results. As part of the study, the functionality of netstat was explored in detail, particularly the -a, -n, -o, -s and -r options, which give a complete listing of active connections, IP address, process ID, statistics for network protocols and routing tables. The classification table of TCP connection states (LISTENING, ESTABLISHED, TIMEWAIT, CLOSEWAIT) with description of diagnostic values and recommendations was created, according to which problematic states can be identified, for example, long CLOSE_WAIT. The results obtained from the network sessions with IP addresses 127.0.0.1 and 192.168.0.161 and ports 161:4147-4149, shown in Figure 2, provide information related to the intensity of the activity of the web applications, system processes and also the existence of potential anomalies. Ways for scripting to automate the data collection and connection with logging systems for building time series are suggested.

Conclusions. The study has proven that netstat is efficient for starting and monitoring the network activity in windows and is a useful tool with its advanced command-line parameters and organized method to capture the data for diagnostics. The resulting monitoring architecture and connection state classification provides the foundations for integration of traditional utilities with modern technologies such as machine learning. Future work opportunities: development of algorithms for automatic anomaly detection, integration with cloud systems, development of adaptive alerting systems, with practical consequences in the field of security and optimization of network resources (cybersecurity).

Key words: *netstat, network, monitoring, Windows, computer network diagnostics, computer network security, cybersecurity.*

Постановка проблеми

Сучасні комп'ютерні системи характеризуються інтенсивною мережевою активністю, що потребує ефективних засобів моніторингу та діагностики. Операційна система Windows надає розгалужений інструментарій для аналізу мережевого трафіку, серед якого утиліта netstat займає особливе місце завдяки своїй універсальності та доступності. Проблема ефективного використання netstat для ініціювання комплексного моніторингу мережевої активності набуває особливої актуальності в контексті зростаючих вимог до системної безпеки та продуктивності. Традиційні підходи до використання netstat часто обмежуються базовими функціями, що не дозволяє повною мірою використати потенціал цього інструменту. Необхідність систематизації методів застосування netstat та розробки оптимальних стратегій інтерпретації результатів зумовлює актуальність даного дослідження.

Аналіз останніх досліджень і публікацій

Аналіз сучасних досліджень у галузі мережевого моніторингу демонструє широкий спектр підходів до оптимізації системних утиліт. Бойко В. Д., Бевза В. І., Слатвінська В. М. [1, с. 1263] розглядають питання використання

штучного інтелекту для оптимізації системного коду, що має пряме відношення до автоматизації роботи з мережевими утилітами. Дослідження системних збоїв та їх впливу на мережеву безпеку представлено у працях Бевза В. І., Слатвінська В. М. [2, с. 335], де аналізуються наслідки масштабних системних відмов. Продовження цього дослідження Бевза В. І., Слатвінська В. М. [3, с. 252] поглиблює розуміння взаємозв'язків між системними збоями та мережевою активністю.

Сучасні підходи до аналізу мережевих систем представлені у роботах Zhong Y., Zhang Y., Zhang J., Wan L. [4, с. 15], які досліджують стійкість мережевих командно-інформаційних систем. Аналітика мережевих даних у контексті 5G систем розглядається Romero M. L., Suyama R. [5, с. 8], що демонструє еволюцію підходів до мережевого моніторингу. Інноваційні методи контекстуалізації мережевих вимірювань за допомогою великих мовних моделей представлені Beltiukov R., Bhattaram K., Cheng E., Kanigicherla V., Singh A., Thampiratwong K., Gupta A. [6, с. 12].

Практичні аспекти аналізу мережевого трафіку висвітлені у дослідженні Jiang W., Zhang B., Zhu Q., Liao C., Wang W. [7, с. 3], які представили датасет реального мережевого середовища. Сучасні методи виявлення мережевих вторгнень розроблені Balakrishnapillai J., Ajayan A. K. P., Kurian A., Sabu A., Majeed A. [8, с. 020044] з використанням новітньої технології DSSTE. Альтернативний підхід до виявлення вторгнень на основі згорткових нейронних мереж запропонований S D. B., A Ms.D. [9, с. 5]. Інноваційні методи виявлення аномалій мережевих комутаторів представлені Nam S., Jeong E., Hong J. W. [10, с. 2], а прогнозування мережевого трафіку досліджене Lv Q., Chang Y., Li T., Ge J. [11, с. 111557].

Формулювання мети дослідження

Метою дослідження є розробка комплексної методології ініціювання та аналізу мережевої активності в Windows за допомогою netstat з урахуванням сучасних вимог до системного моніторингу та забезпечення оптимальної інтерпретації результатів діагностики.

Викладення основного матеріалу дослідження

Утиліта netstat являє собою фундаментальний інструмент операційної системи Windows для моніторингу мережевої активності. Її функціональність охоплює широкий спектр діагностичних можливостей, від базового відображення активних з'єднань до детального аналізу мережевих статистик. Досвід використання netstat у контексті системної оптимізації, як показано у дослідженнях Бойко В. Д., Бевза В. І., Слатвінська В. М. [1, с. 1265], демонструє важливість інтеграції традиційних утиліт з сучасними підходами до автоматизації.

Основні параметри командного рядка netstat забезпечують різноманітні режими моніторингу. Параметр -a відображає всі з'єднання та порти прослуховування, що критично важливо для комплексного аналізу системи. Використання -n замінює символьні імена хостів на IP-адреси, прискорюючи виконання команди та полегшуючи автоматизовану обробку результатів. Параметр -o додає ідентифікатори процесів до кожного з'єднання, що дозволяє точно визначити джерело мережевої активності.

Аналіз системних збоїв та їх впливу на мережеву активність, досліджений Бевза В. І., Слатвінська В. М. [2, с. 336], підкреслює важливість систематичного моніторингу мережевих з'єднань. Продовження цього дослідження [3, с. 254] демонструє кореляції між системними відмовами та аномальною мережевою поведінкою, що може бути ефективно виявлено за допомогою netstat.

Для аналізу результатів netstat розроблено таблицю основних станів TCP-з'єднань та їх інтерпретації в контексті системної діагностики:

Таблиця 1

Класифікація станів TCP-з'єднань у контексті netstat

Стан з'єднання	Опис	Діагностичне значення	Рекомендації
LISTENING	Очікування вхідних з'єднань	Активний сервісний порт	Перевірити необхідність сервісу
ESTABLISHED	Активне з'єднання	Нормальна комунікація	Моніторити тривалість
TIME_WAIT	Очікування закриття	Нормальне завершення	Контролювати кількість
CLOSE_WAIT	Очікування закриття додатком	Можлива проблема додатка	Перевірити код додатка

Як видно з таблиці 1, кожен стан TCP-з'єднання має специфічне діагностичне значення, що дозволяє системним адміністраторам ефективно інтерпретувати результати netstat для вирішення мережевих проблем.

Сучасні підходи до аналізу мережевих систем, розроблені Zhong Y., Zhang Y., Zhang J., Wan L. [4, с. 18], підкреслюють важливість стійкості мережевих компонентів. Це безпосередньо пов'язано з можливостями netstat для виявлення потенційних проблем у мережевій інфраструктурі. Еволюція мережевих технологій, досліджена Romero M. L., Suyama R. [5, с. 10], вимагає адаптації традиційних інструментів моніторингу до нових реалій.

Інноваційні підходи до контекстуалізації мережевих вимірювань, представлені Beltiukov R., Bhattaram K., Cheng E., Kanigicherla V., Singh A., Thampiratwong K., Gupta A. [6, с. 14], демонструють перспективи інтеграції традиційних утиліт з сучасними технологіями машинного навчання. Це відкриває нові можливості для автоматизованого аналізу вихідних даних netstat.

Для візуалізації архітектури системи моніторингу мережевої активності на основі netstat розроблено структурну схему:

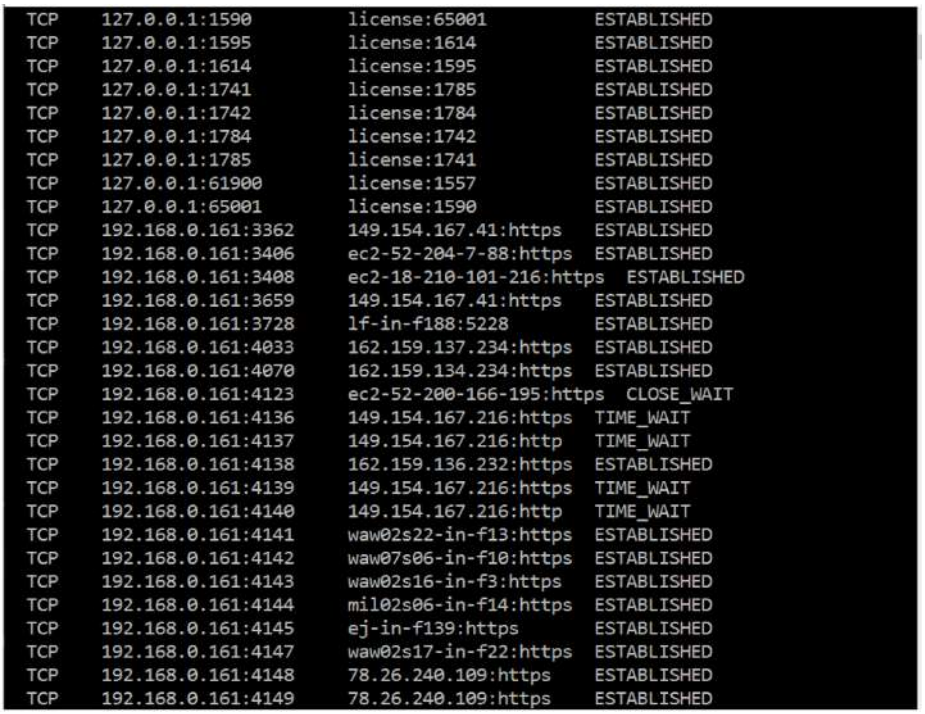
Рис. 1. Архітектура системи моніторингу на базі netstat

Джерело: авторська розробка

Як демонструє рисунок 1, архітектура системи моніторингу включає чотири основні компоненти, що забезпечують комплексний підхід до аналізу мережевої активності від збору первинних даних до генерації оповіщень про аномалії.

Як показано на рисунку 2, команда netstat з параметрами -a, -n та -o відображає всі мережеві сеанси в системі Windows, включаючи їхні числові адреси, ідентифікатори процесів та інші деталі. Існує багато TCP-з'єднань, здебільшого у стані ESTABLISHED, які відповідають двостороннім з'єднанням між локальним хостом (IP-адреса 127.0.0.1 та 192.168.0.161) та зовнішніми або внутрішніми серверами, що прослуховують порт 161, використовуючи протокол HTTPS на портах 4147-4149. Такі з'єднання, як CLOSE_WAIT та TIME_WAIT, представляють сеанси, що закриваються або очікують закриття (звичайний продукт динамічних мережевих транзакцій). З цієї інформації ми можемо зробити деякі висновки про інтенсивність мережевої активності веб-застосунків та системних процесів, а також надати уявлення про можливі аномалії, такі як стан CLOSE_WAIT, який може свідчити про проблему з правильним завершенням з'єднання.

Подальша оцінка даних на рисунку 2 може дозволити нам оцінити розподіл мережевих ресурсів та системне навантаження. Зокрема, той факт, що багато підключень пов'язані з однаковими ідентифікаторами процесів (наприклад, 149, 162), вказує на те, що кілька програм або служб, які взаємодіють з мережею, зайняті одночасно, і це може бути пов'язано з оновленнями програмного забезпечення у фоновому режимі або синхронізацією даних. Це робить ретельне



TCP	127.0.0.1:1590	license:65001	ESTABLISHED
TCP	127.0.0.1:1595	license:1614	ESTABLISHED
TCP	127.0.0.1:1614	license:1595	ESTABLISHED
TCP	127.0.0.1:1741	license:1785	ESTABLISHED
TCP	127.0.0.1:1742	license:1784	ESTABLISHED
TCP	127.0.0.1:1784	license:1742	ESTABLISHED
TCP	127.0.0.1:1785	license:1741	ESTABLISHED
TCP	127.0.0.1:61900	license:1557	ESTABLISHED
TCP	127.0.0.1:65001	license:1590	ESTABLISHED
TCP	192.168.0.161:3362	149.154.167.41:https	ESTABLISHED
TCP	192.168.0.161:3406	ec2-52-204-7-88:https	ESTABLISHED
TCP	192.168.0.161:3408	ec2-18-210-101-216:https	ESTABLISHED
TCP	192.168.0.161:3659	149.154.167.41:https	ESTABLISHED
TCP	192.168.0.161:3728	lf-in-f188:5228	ESTABLISHED
TCP	192.168.0.161:4033	162.159.137.234:https	ESTABLISHED
TCP	192.168.0.161:4070	162.159.134.234:https	ESTABLISHED
TCP	192.168.0.161:4123	ec2-52-200-166-195:https	CLOSE_WAIT
TCP	192.168.0.161:4136	149.154.167.216:https	TIME_WAIT
TCP	192.168.0.161:4137	149.154.167.216:http	TIME_WAIT
TCP	192.168.0.161:4138	162.159.136.232:https	ESTABLISHED
TCP	192.168.0.161:4139	149.154.167.216:https	TIME_WAIT
TCP	192.168.0.161:4140	149.154.167.216:http	TIME_WAIT
TCP	192.168.0.161:4141	waw02s22-in-f13:https	ESTABLISHED
TCP	192.168.0.161:4142	waw07s06-in-f10:https	ESTABLISHED
TCP	192.168.0.161:4143	waw02s16-in-f3:https	ESTABLISHED
TCP	192.168.0.161:4144	mil02s06-in-f14:https	ESTABLISHED
TCP	192.168.0.161:4145	ej-in-f139:https	ESTABLISHED
TCP	192.168.0.161:4147	waw02s17-in-f22:https	ESTABLISHED
TCP	192.168.0.161:4148	78.26.240.109:https	ESTABLISHED
TCP	192.168.0.161:4149	78.26.240.109:https	ESTABLISHED

Рис. 2. Процес ініціювання мережевої активності в операційній системі

Джерело: авторська розробка

дослідження поведінки таких процесів обов'язковим для оптимізації та безпеки. Тому результати, представлені на рисунку, використовуються як відправна точка для подальших досліджень початку мережевої активності та розробки методів її аналізу, які можна інтегрувати в автоматизовані системи моніторингу та реагування на мережеві загрози.

Практичні аспекти роботи з реальними мережевими середовищами, висвітлені Jiang W., Zhang B., Zhu Q., Liao C., Wang W. [7, с. 5], підкреслюють важливість валідації результатів netstat на основі емпіричних даних. Це особливо актуально для розробки ефективних алгоритмів фільтрації та аналізу.

Сучасні методи виявлення мережевих вторгнень, розроблені Balakrishnapillai J., Ajayan A.K.P., Kurian A., Sabu A., Majeed A. [8, с. 020045], можуть бути інтегровані з функціональністю netstat для створення комплексних систем безпеки. Альтернативні підходи, запропоновані S D. B., A Ms. D. [9, с. 7], демонструють можливості використання нейронних мереж для аналізу паттернів мережевої активності, виявлених за допомогою netstat.

Інноваційні методи виявлення аномалій, представлені Nam S., Jeong E., Hong J.W. [10, с. 4], базуються на аналізі логів мережевої активності, які можуть бути ефективно генеровані з використанням розширених можливостей netstat. Прогнозування мережевого трафіку, досліджене Lv Q., Chang Y., Li T., Ge J. [11, с. 111558], потребує якісних вхідних даних, які netstat може надати у структурованому вигляді.

Розширені можливості netstat включають параметр -s для відображення статистики по протоколах, що дозволяє аналізувати загальну ефективність мережевої підсистеми. Параметр -r відображає таблицю маршрутизації, що критично важливо для діагностики проблем з мережевою доступністю. Комбінування різних параметрів створює потужний інструментарій для комплексного аналізу мережевого стану системи.

Автоматизація роботи з netstat передбачає розробку скриптів для регулярного збору даних та їх подальшої обробки. Періодичне виконання команд netstat з різними параметрами дозволяє створювати часові ряди мережевої активності, що надає можливість виявляти тренди та аномалії. Інтеграція з системами логування забезпечує довгострокове зберігання історії мережевої активності для ретроспективного аналізу.

Висновки

Проведене дослідження демонструє фундаментальну важливість утиліти netstat для ініціювання та моніторингу мережевої активності в операційній системі Windows. Систематичний підхід до використання розширених параметрів netstat забезпечує комплексний аналіз мережевого стану системи. Розроблена класифікація станів TCP-з'єднань надає практичний інструментарій для інтерпретації результатів діагностики.

Запропонована архітектура системи моніторингу на базі netstat демонструє можливості інтеграції традиційних утиліт з сучасними підходами до автоматизації та аналізу даних. Методики автоматизованої обробки вихідних даних netstat створюють основу для розробки ефективних систем мережевого моніторингу.

Перспективи подальших досліджень включають розробку алгоритмів машинного навчання для автоматизованого виявлення аномалій на основі даних netstat, інтеграцію з хмарними системами моніторингу та створення адаптивних систем оповіщення. Результати дослідження мають практичне значення для системних адміністраторів та фахівців з мережевої безпеки, надаючи конкретні рекомендації щодо оптимального використання netstat у різних сценаріях діагностики.

Список використаної літератури

1. Бойко В. Д., Бевза В. І., Слатвінська В. М. Використання штучного інтелекту для оптимізації коду на Python з інтеграцією інструментів налагодження PDB / В. Д. Бойко, В. І. Бевза, В. М. Слатвінська // Наука і техніка сьогодні: Серія «Техніка». 2025. № 7 (48). С. 1258–1271. DOI: https://doi.org/10.52058/2786-6025-2025-7(48)-1258-1271

2. Бевза В. І., Слатвінська В. М. Вплив збою Crowdstrike на мега-витік паролів: чи є зв'язок? Ч. 1 / В. І. Бевза, В. М. Слатвінська // Вісник Хмельницького національного університету. Серія: Технічні науки. 2024. № 4. С. 332–338. DOI: https://doi.org/10.31891/2307-5732-2024-339-4-52 URL: https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/257

3. Бевза В. І., Слатвінська В. М. Вплив збою Crowdstrike на мега-витік паролів: чи є зв'язок? Ч. 2 / В. І. Бевза, В. М. Слатвінська // Вісник Хмельницького національного університету. Серія: Технічні науки. 2024. Том 341. № 5. С. 248–259. DOI: https://doi.org/10.31891/2307-5732-2024-341-5-36 URL: https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/300

4. Zhong Y., Zhang Y., Zhang J., Wan L. Research on resilience measurement and optimization of networked command information system / Y. Zhong, Y. Zhang, J. Zhang, L. Wan // Reliability Engineering & System Safety. 2025. Vol. 261. Art. 111048. DOI: https://doi.org/10.1016/j.ress.2025.111048 URL: https://www.sciencedirect.com/science/article/pii/S0951832025002492

5. Romero M. L., Suyama R. Towards Network Data Analytics in 5G Systems and Beyond (Version 1) / M. L. Romero, R. Suyama // arXiv. 2025. DOI: https://doi.org/10.48550/ARXIV.2506.04860 URL: https://arxiv.org/abs/2506.04860v1

6. Beltiukov R., Bhattaram K., Cheng E., Kanigicherla V., Singh A., Thampiratwong K., Gupta A. Leveraging Large Language Models to Contextualize Network Measurements (Version 2) / R. Beltiukov, K. Bhattaram, E. Cheng, V. Kanigicherla, A. Singh, K. Thampiratwong, A. Gupta // arXiv. 2025. DOI: https://doi.org/10.48550/ARXIV.2505.19305 URL: https://arxiv.org/abs/2505.19305v2

7. Jiang W., Zhang B., Zhu Q., Liao C., Wang W. A Real Network Environment Dataset for Traffic Analysis / W. Jiang, B. Zhang, Q. Zhu, C. Liao, W. Wang // Scientific Data. 2025. Vol. 12, No. 1. DOI: https://doi.org/10.1038/s41597-025-04876-2 URL: https://www.nature.com/articles/s41597-025-04876-2

8. Balakrishnapillai J., Ajayan A. K. P., Kurian A., Sabu A., Majeed A. Network intrusion detection using novel DSSTE / J. Balakrishnapillai, A. K. P. Ajayan, A. Kurian, A. Sabu, A. Majeed // AIP Conference Proceedings. 2025. Vol. 3260. Art. 020044. DOI: https://doi.org/10.1063/5.0259047 URL: https://is.gd/A27Mrf

9. Brindha S., Dhamayanthi A. Network Based Intrusion Detection using Convolutional Neural Network / S. Brindha, A. Dhamayanthi // International Journal of Scientific Research in Engineering and Management. 2025. Vol. 09, No. 03. P. 1–9. DOI: https://doi.org/10.55041/ijsrem42812 URL: https://is.gd/JMt6yI

10. Nam S., Jeong E., Hong J. W. Log-TF-IDF and NETCONF-Based Network Switch Anomaly Detection / S. Nam, E. Jeong, J. W. Hong // International Journal of Network Management. 2025. Vol. 35, No. 1. DOI: https://doi.org/10.1002/nem.2322 URL: https://onlinelibrary.wiley.com/doi/10.1002/nem.2322

11. Lv Q., Chang Y., Li T., Ge J. Betastack: Enhancing base station traffic prediction with network-specific Large Language Models / Q. Lv, Y. Chang, T. Li, J. Ge // Computer Networks. 2025. Vol. 270. Art. 111557. DOI: https://doi.org/10.1016/j.comnet.2025.111557 URL: https://www.sciencedirect.com/science/article/abs/pii/S1389128625005249

References

1. Boyko, V. D., Bevza, V. I., & Slatvinska, V. M. (2025). Vykorystannia shtuchnoho intelektu dlia optymizatsii kodu na Python z intehratsiieiu instrumentiv nalahodzhennia PDB [Use of artificial intelligence for Python code optimization with PDB debugging tools integration]. Nauka i tekhnika sohodni: Seriia “Tekhnika”, Science and Technology Today: Technical Series (7), 1258–1271. DOI: https://doi.org/10.52058/2786-6025-2025-7(48)-1258-1271 [in Ukrainian].

2. Bevza, V. I., & Slatvinska, V. M. (2024). Vplyv zboiu Crowdstrike na meha-vytik paroliv: chy ye zviazok? Ch. 1 [Impact of the Crowdstrike outage on the mega password leak: Is there a connection? Part 1]. Visnyk Khmelnytskoho natsionalnoho universytetu. Seriia: Tekhnichni nauky, Bulletin of Khmelnytskyi National University. Technical Sciences, (4), 332–338. DOI: https://doi.org/10.31891/2307-5732-2024-339-4-52 Retrieved from https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/257 [in Ukrainian].

3. Bevza, V. I., & Slatvinska, V. M. (2024). Vplyv zboiu Crowdstrike na meha-vytik paroliv: chy ye zviazok? Ch. 2 [Impact of the Crowdstrike outage on the mega password leak: Is there a connection? Part 2]. Visnyk Khmelnytskoho natsionalnoho universytetu. Seriia: Tekhnichni nauky. Bulletin of Khmelnytskyi National University. Technical Sciences, 341(5), 248–259. DOI: https://doi.org/10.31891/2307-5732-2024-341-5-36 Retrieved from https://heraldts.khmnu.edu.ua/index.php/heraldts/article/view/300 [in Ukrainian].

4. Zhong, Y., Zhang, Y., Zhang, J., & Wan, L. (2025). Research on resilience measurement and optimization of networked command information system. Reliability Engineering & System Safety, 261, 111048. DOI: https://doi.org/10.1016/j.ress.2025.111048 Retrieved from https://www.sciencedirect.com/science/article/pii/S0951832025002492 [in English].

5. Romero, M. L., & Suyama, R. (2025). Towards network data analytics in 5G systems and beyond (Version 1). arXiv. DOI: https://doi.org/10.48550/ARXIV.2506.04860 Retrieved from https://arxiv.org/abs/2506.04860v1 [in English].

6. Beltiukov, R., Bhattaram, K., Cheng, E., Kanigicherla, V., Singh, A., Thampiratwong, K., & Gupta, A. (2025). Leveraging large language models to contextualize network measurements (Version 2). arXiv. DOI: https://doi.org/10.48550/ARXIV.2505.19305 Retrieved from https://arxiv.org/abs/2505.19305v2 [in English].

7. Jiang, W., Zhang, B., Zhu, Q., Liao, C., & Wang, W. (2025). A real network environment dataset for traffic analysis. Scientific Data, 12(1). DOI: https://doi.org/10.1038/s41597-025-04876-2 Retrieved from https://www.nature.com/articles/s41597-025-04876-2 [in English].

8. Balakrishnapillai, J., Ajayan, A. K. P., Kurian, A., Sabu, A., & Majeed, A. (2025). Network intrusion detection using novel DSSTE. AIP Conference Proceedings, 3260, 020044. DOI: https://doi.org/10.1063/5.0259047 Retrieved from https://is.gd/A27Mrf [in English].

9. Brindha, S., & Dhamayanthi, A. (2025). Network based intrusion detection using convolutional neural network. International Journal of Scientific Research in Engineering and Management, 9(3), 1–9. DOI: https://doi.org/10.55041/ijsrem42812 Retrieved from https://is.gd/JMt6yI [in English].

10. Nam, S., Jeong, E., & Hong, J. W. (2025). Log-TF-IDF and NETCONF-based network switch anomaly detection. International Journal of Network Management, 35(1). DOI: https://doi.org/10.1002/nem.2322 Retrieved from https://onlinelibrary.wiley.com/doi/10.1002/nem.2322 [in English].

11. Lv, Q., Chang, Y., Li, T., & Ge, J. (2025). Betastack: Enhancing base station traffic prediction with network-specific large language models. Computer Networks, 270, 111557. DOI: https://doi.org/10.1016/j.comnet.2025.111557 Retrieved from https://is.gd/8bjNkw [in English].

Дата першого надходження рукопису до видання: 26.09.2025
Дата прийнятого до друку рукопису після рецензування: 22.10.2025
Дата публікації: 28.11.2025