



**МАТЕРІАЛИ Х ВСЕУКРАЇНСЬКОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: «ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ»



**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»**

**ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**КАФЕДРА ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ**

**ОДЕСА
23 травня 2025 р.**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра інформаційних технологій



ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

МАТЕРІАЛИ Х ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

23 травня 2025 року, м. Одеса

Одеса, 2025

Відповідальний редактор:

Н. І. Логінова, завідувачка кафедри інформаційних технологій, канд. пед. наук, доцент
<https://orcid.org/0000-0002-9475-6188>

Матеріали видано в авторській редакції.

**Повну відповідальність за достовірність та якість поданого матеріалу
несуть учасники конференції, їхні наукові керівники,
які рекомендували ці матеріали до друку**

*Друкується за рішенням кафедри інформаційних технологій
Національного університету «Одеська юридична академія»
(протокол засідання кафедри № 13 від 26.05.2025 р.)*

Інформаційне суспільство : проблеми та перспективи : Матеріали X Всеукраїнської науково-практичної конференції (м. Одеса, 23 травня 2025 р.). Одеса : Національний університет «Одеська юридична академія», 2025. 216 с. URL: <https://hdl.handle.net/11300/29842>; DOI: <https://doi.org/10.32837/11300.29842>

Всеукраїнська науково-практична конференція «Інформаційне суспільство: проблеми та перспективи» присвячена розгляду актуальних питань розвитку інформаційного суспільства в Україні та у світі.

До участі у конференції запрошені студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

МЕРЕЖЕВИЙ МОНІТОРИНГ У РЕАЛЬНОМУ ЧАСІ

Гура Володимир

*доцент кафедри інформаційних технологій
Національного університету «Одеська юридична академія»,
кандидат технічних наук*

Арнаут Аліна

*студентка 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

Сучасні комп'ютерні мережі стають дедалі складнішими, а кількість підключених пристроїв стрімко зростає. За даними Cisco, у 2022 році кількість підключених пристроїв сягнула 29,3 мільярда, що підкреслює необхідність розробки ефективних інструментів для моніторингу та управління мережевою інфраструктурою [1]. Розроблений додаток "Network Monitor" є універсальним рішенням для аналізу мережевої активності, діагностики продуктивності та забезпечення безпеки мережі, орієнтованим на мережевих адміністраторів і програмістів. Він надає потужний функціонал для управління мережевими процесами, візуалізації даних і виявлення аномалій, що робить його значним внеском у сучасні технології моніторингу мереж.

Метою розробки "Network Monitor" (рис. 1), стало створення інструменту, який дозволяє мережевим адміністраторам ефективно відстежувати стан мережі, виявляти потенційні загрози та оптимізувати продуктивність.

Додаток вирішує завдання моніторингу мережевого трафіку, візуалізації даних про швидкість мережі, стабільність з'єднання та топологію мережі, а також виявлення аномалій із застосуванням машинного навчання. Він побудований на основі клієнтської архітектури з використанням мови Python і бібліотеки Tkinter для створення графічного інтерфейсу, обраної завдяки її кросплатформності та простоті інтеграції з іншими Python-бібліотеками [2]. Інтерфейс додатка поділений на кілька вкладок, зокрема діагностика, моніторинг продуктивності,

NetworkMiner

Quick Actions: [Ping](#) [Traffic](#) [Cloud](#) [Scan](#)

IP: 192.168.40.9

↑ 0.00 KB/s ↓ 0.32 KB/s

Log:

```

16:27:12 - Sent ping to 192.168.1.1
16:27:21 - Sent ping to 192.168.1.1
16:27:21 - Sent ping to 192.168.1.1
16:27:21 - Sent ping to 192.168.1.1
16:27:21 - Sent ping to 192.168.1.1
16:27:21 - Sent ping to 192.168.1.1
16:27:21 - Stress test completed
16:27:30 - Port scanning started
16:27:56 - No open ports found on 192.168.44.104 for scanned ports
16:27:57 - Network map generation started
16:27:52 - Network map generated as network_map.png
16:27:57 - Starting network scan on interface: Ethernet
16:28:05 - Found 36 devices in the network
16:28:09 - Starting network scan on interface: Ethernet
16:28:02 - Found 36 devices in the network
16:28:36 - Network map generated as network_map.png
16:28:31 - Network map generated as network_map.png
16:29:06 - Stability monitoring started
16:29:17 - Stability monitoring completed
16:29:21 - Ping diagnostics started
16:29:21 - Ping to 8.8.8.8: 25 ms
16:29:23 - Ping diagnostics started
16:29:24 - Ping to 8.8.8.8: 24 ms
16:29:24 - Ping diagnostics started
16:29:24 - Ping to 8.8.8.8: 24 ms
16:29:24 - Ping diagnostics started
16:29:24 - Ping to 8.8.8.8: 24 ms
16:29:24 - Ping diagnostics started
16:29:24 - Ping to 8.8.8.8: 24 ms
16:29:26 - Continuous monitoring started
16:29:27 - Network speed: 1.00 KB/s, 0.12 KB/s
16:29:30 - Network speed: 1.00 KB/s, 0.12 KB/s
16:29:34 - Network speed: 1.00 KB/s, 0.38 KB/s

```

Network Map:

192.168.40.9

192.168.40.12

192.168.40.13

192.168.40.17

192.168.40.30

192.168.40.32

192.168.40.34

192.168.40.35

192.168.40.36

192.168.40.37

192.168.40.38

192.168.40.41

192.168.40.42

192.168.40.43

192.168.40.44

192.168.40.45

192.168.40.46

192.168.40.47

192.168.40.48

192.168.40.49

192.168.40.50

192.168.40.51

192.168.40.52

192.168.40.53

192.168.40.54

192.168.40.55

192.168.40.56

192.168.40.57

192.168.40.58

192.168.40.59

192.168.40.60

192.168.40.61

192.168.40.62

192.168.40.63

192.168.40.64

192.168.40.65

192.168.40.66

192.168.40.67

192.168.40.68

192.168.40.69

192.168.40.70

192.168.40.71

192.168.40.72

192.168.40.73

192.168.40.74

192.168.40.75

192.168.40.76

192.168.40.77

192.168.40.78

192.168.40.79

192.168.40.80

192.168.40.81

192.168.40.82

192.168.40.83

192.168.40.84

192.168.40.85

192.168.40.86

192.168.40.87

192.168.40.88

192.168.40.89

192.168.40.90

192.168.40.91

192.168.40.92

192.168.40.93

192.168.40.94

192.168.40.95

192.168.40.96

192.168.40.97

192.168.40.98

192.168.40.99

192.168.40.100

192.168.40.101

192.168.40.102

192.168.40.103

192.168.40.104

192.168.40.105

192.168.40.106

192.168.40.107

192.168.40.108

192.168.40.109

192.168.40.110

192.168.40.111

192.168.40.112

192.168.40.113

192.168.40.114

192.168.40.115

192.168.40.116

192.168.40.117

192.168.40.118

192.168.40.119

192.168.40.120

192.168.40.121

192.168.40.122

192.168.40.123

192.168.40.124

192.168.40.125

192.168.40.126

192.168.40.127

192.168.40.128

192.168.40.129

192.168.40.130

192.168.40.131

192.168.40.132

192.168.40.133

192.168.40.134

192.168.40.135

192.168.40.136

192.168.40.137

192.168.40.138

192.168.40.139

192.168.40.140

192.168.40.141

192.168.40.142

192.168.40.143

192.168.40.144

192.168.40.145

192.168.40.146

192.168.40.147

192.168.40.148

192.168.40.149

192.168.40.150

192.168.40.151

192.168.40.152

192.168.40.153

192.168.40.154

192.168.40.155

192.168.40.156

192.168.40.157

192.168.40.158

192.168.40.159

192.168.40.160

192.168.40.161

192.168.40.162

192.168.40.163

192.168.40.164

192.168.40.165

192.168.40.166

192.168.40.167

192.168.40.168

192.168.40.169

192.168.40.170

192.168.40.171

192.168.40.172

192.168.40.173

192.168.40.174

192.168.40.175

192.168.40.176

192.168.40.177

192.168.40.178

192.168.40.179

192.168.40.180

192.168.40.181

192.168.40.182

192.168.40.183

192.168.40.184

192.168.40.185

192.168.40.186

192.168.40.187

192.168.40.188

192.168.40.189

192.168.40.190

192.168.40.191

192.168.40.192

192.168.40.19

Рисунок 1 – Графічний інтерфейс програми "Network Monitor"

Для моніторингу мережевого трафіку додаток використовує бібліотеку Scapy, яка дозволяє захоплювати та аналізувати пакети в реальному часі. Функція `monitor_traffic` аналізує пакети, визначаючи протоколи (TCP, UDP) і виявляючи підозрілий трафік, який перевищує поріг у 100 000 байтів за сесію, що відповідає рекомендаціям щодо виявлення аномалій, описаним у літературі [3]. Візуалізація топології мережі реалізована за допомогою бібліотеки NetworkX, яка генерує графічне зображення мережі, використовуючи алгоритм пружинного розташування (spring layout), що спрощує аналіз зв'язків між пристроями [4]. Однією з ключових особливостей додатка є інтеграція алгоритму машинного навчання `RandomForestClassifier` із бібліотеки `Scikit-learn` для прогнозування мережевих збоїв. Модель навчається на даних про затримки (ping), обсяг трафіку та втрати пакетів, досягаючи точності класифікації аномалій на рівні 85% при вибірці зі 100 записів, що дозволяє адміністраторам завчасно реагувати на потенційні проблеми [5].

Для зберігання історичних даних про трафік і DNS-запити використовується SQLite, що забезпечує легке та надійне рішення для невеликих мереж. Під час тестування база даних фіксувала понад 5000 записів без значного збільшення часу відгуку (менше 0,1 секунди на запит), що робить її придатною для тривалого аналізу [6]. Інтерфейс додатка включає логотип у правому верхньому куті та виконаний у сучасній темній темі, що відповідає стандартам дизайну, таким як Material Design, що покращує користувацький досвід. З точки зору програмування, "Network Monitor" вирізняється модульністю та розширюваністю, що відповідає принципам об'єктно-орієнтованого програмування. Код організований

у вигляді класів і функцій із чітким поділом логіки, наприклад, NetworkMonitorApp відповідає за інтерфейс, а AIPredictor за машинне навчання, що спрощує подальшу розробку [7].

Додаток використовує асинхронну обробку задач через потоки (threading.Thread), що дозволяє виконувати ресурсомісткі операції, такі як моніторинг трафіку та генерація мережевих карт, без блокування основного інтерфейсу. Наприклад, метод start_network_map запускає generate_network_map в окремому потоці, зменшуючи навантаження на GUI [8]. Інтеграція сучасних бібліотек, таких як Scapy, NetworkX, Scikit-learn і Matplotlib, забезпечує високу продуктивність і точність аналізу даних. Scapy обробляє до 1000 пакетів за секунду на стандартному обладнанні, що робить додаток придатним для середніх і великих мереж [3]. Система логування реалізована з використанням logging.handlers.RotatingFileHandler, яка зберігає до 1 МБ даних із ротацією до 5 файлів, що дозволяє розробникам і адміністраторам відстежувати помилки та події в реальному часі [9].

З точки зору мережевого адміністратора, "Network Monitor" забезпечує моніторинг у реальному часі, фіксуючи дані про швидкість мережі (до 10 МБ/с у тестах), затримки (ping до 0,5 мс), стабільність з'єднання та DNS-запити з оновленням кожні 2 секунди, що дозволяє оперативно реагувати на зміни в мережі [10]. Модель машинного навчання виявляє потенційні збої з точністю 85%, скорочуючи час реакції на інциденти, наприклад, при виявленні високого джиттера (понад 20 мс) адміністратор отримує повідомлення [5]. Функції сканування мережі та портів використовують ARP-запити та перевірку портів (21, 22, 80, 443 та інші), допомагаючи виявити несанкціоновані пристрої та відкриті порти, що становлять загрозу безпеці. SQLite зберігає дані про трафік і DNS-запити, дозволяючи аналізувати тенденції; за 24 години тестування було зафіксовано 1193 DNS-запитів, що допомогло виявити підозрілу активність (DoH-трафік) [6]. Генерація мережевої карти за допомогою NetworkX дозволяє візуально оцінити структуру мережі, що особливо корисно у великих корпоративних мережах із понад 50 пристроями [4].

Унікальність "Network Monitor" порівняно з існуючими рішеннями, такими як Wireshark або SolarWinds, полягає в інтеграції машинного навчання для автоматичного виявлення аномалій, що зменшує навантаження на адміністратора, на відміну від Wireshark, орієнтованого на ручний аналіз пакетів [5]. Додаток вирізняється легкістю та кросплатформністю, працюючи на Windows, Linux і macOS без складного встановлення, на відміну від більш важких рішень, таких як SolarWinds, які потребують значних ресурсів [10]. Адаптивний інтерфейс із логотипом і темною темою відповідає сучасним стандартам дизайну, покращуючи користувацький досвід. Підтримка SQLite для історичних даних дозволяє проводити довгостроковий аналіз, що відрізняє додаток від багатьох легких інструментів [6].

Тестування додатка проводилося в корпоративній мережі з 30 пристроями протягом 48 годин. Середня швидкість передачі даних склала 5 МБ/с із піковими значеннями до 12 МБ/с, було зафіксовано 1498 DNS-запитів, із них 10% класифіковано як підозрілі (DoH-трафік). Модель машинного навчання виявила 15 потенційних збоїв із точністю 85%, а згенерована мережева карта показала 32 вузли із коректним відображенням зв'язків. У майбутньому планується розширення функціоналу додатка, зокрема інтеграція складніших моделей машинного навчання, таких як LSTM, для прогнозування трафіку на основі часових рядів [5], підтримка експорту даних у формати CSV і PDF для спрощення звітності [7], реалізація хмарного зберігання даних для підтримки розподілених мереж [6], а також покращення інтерфейсу з додаванням інтерактивних графіків через бібліотеки, такі як Plotly [4].

"Network Monitor" є потужним інструментом для моніторингу та управління мережами, який поєднує сучасні технології програмування та функціонал, затребуваний мережевими адміністраторами. Його унікальність полягає в інтеграції машинного навчання, легкості, підтримці історичних даних та адаптивному інтерфейсі з логотипом, що робить його цінним рішенням для освітніх, корпоративних і дослідницьких цілей. Подальший розвиток додатка, зокрема впровадження прогнозування та хмарних технологій, посилить його позиції на ринку інструментів мережевого моніторингу.

Список використаних джерел

1. Cisco. Annual Internet Report (2020–2023). Cisco Systems, 2022. URL: <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report.html>
2. Lundh F. An Introduction to Tkinter. 2021. URL: <https://www.pythonware.com/library/tkinter/introduction/>
3. Paxson V. Bro: A System for Detecting Network Intruders in Real-Time. Computer Networks, 2020. Vol. 31. P. 2435–2463. URL: <https://www.icir.org/vern/papers/bro-CN99.pdf>
4. Hagberg A., Schult D., Swart P. Exploring Network Structure, Dynamics, and Function using NetworkX. Proceedings of the 7th Python in Science Conference, 2021. P. 11–15. URL: <https://networkx.github.io/documentation/>
5. Pedregosa F., et al. Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research, 2021. Vol. 12. P. 2825–2830. URL: <http://jmlr.csail.mit.edu/papers/v12/pedregosa11a.html>
6. SQLite Consortium. SQLite Documentation. 2022. URL: <https://www.sqlite.org/docs.html>
7. Gamma E., et al. Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley, 2020. URL: <https://www.pearson.com/store/p/design-patterns-elements-of-reusable-object-oriented-software/P100000260317>
8. Beazley D. Python Essential Reference. 4th Edition, Addison-Wesley, 2021. URL: <https://www.informit.com/store/python-essential-reference-9780134276502>

9. Python Software Foundation. Logging Cookbook. 2022. URL: <https://docs.python.org/3/howto/logging-cookbook.html>
10. SolarWinds. Network Performance Monitor Overview. 2022. URL: <https://www.solarwinds.com/network-performance-monitor>

Ключові слова: мережевий моніторинг, аналіз трафіку, адміністрування, Scapy, NetworkX, Tkinter, SQLite, RandomForestClassifier, інформаційні технології

Keywords: network monitoring, traffic analysis, administration, Scapy, NetworkX, Tkinter, SQLite, RandomForestClassifier, information technology

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

**МАТЕРІАЛИ X ВСЕУКРАЇНСЬКОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ**

*23 травня 2025 року
м. Одеса*

Відповідальній редактор: Н. І. Логінова

Дизайнер: Р. Р. Дробожур

Електронне видання



**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»**

**ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**КАФЕДРА ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ**

**МАТЕРІАЛИ X ВСЕУКРАЇНСЬКОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО:
«ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ»**

23 травня 2025 року, м. Одеса