Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет Комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету )
Кафедра комп'ютерних наук
(повна назва кафедри)

# ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту (роботи)

магістр
(освітній ступінь (освітньо-кваліфікаційний рівень))

на тему: Мережевий моніторинг як засіб аналізу інформаційних процесів у локальній і глобальній мережах

Виконав: студент (ка) 6 курсу, групи СНнм-61
спеціальності (напряму підготовки) 122
Комп'ютерні науки
(шифр і назва спеціальності (напряму підготовки))

_____ Стеблик В. А.
(підпис) (прізвище та ініціали)

Керівник _____ Дмитроца Л. П.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Мацюк О. В.
(підпис) (прізвище та ініціали)

Рецензент _____ Петрик М. Р.
(підпис) (прізвище та ініціали)

м. Тернопіль – 2020

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)

Факультет комп'ютерно-інформаційних систем і програмної інженерії

Кафедра комп'ютерних наук

Освітній ступінь магістр

Напрям підготовки
(шифр і назва)

Спеціальність 122. Комп'ютерні науки
(шифр і назва)

**ЗАТВЕРДЖУЮ**
Завідувач кафедри к.т.н., доц. Боднарчук І. О.

«27» травня 2020 р.

# З А В Д А Н Н Я
## НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Стеблику Валентину Андрійовичу
**(прізвище, ім'я, по батькові)**

1. Тема проекту (роботи) Мережевий моніторинг як засіб аналізу інформаційних процесів у локальній і глобальній мережах

Керівник проекту (роботи) Дмитроца Л. П., к. т. н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від «_27_» грудня 2019 року №_4/7-1166

2. Термін подання студентом проекту (роботи) 28 травня 2020 року

3. Вихідні дані до проекту (роботи) Наукові літературні джерела

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1 Аналіз середовища та основних методів моніторингу. 1.1 Локальні та глобальні мережі. 1.2 Значення моніторингу в сфері інформаційних технологій. 1.3 Засоби моніторингу та аналізу Мережі. 1.4 Методи аналізу та моніторингу мережі. 2 Аналіз систем мережевого моніторингу та обгрунтування вибору для дослідження. 2.1 Система моніторингу Zabbix. 2.2 Моніторингова Система Nagios. 2.3 Система моніторингу Cacti. 2.4 Моніторингова система Paessler PRTG . 2.5 Порівняльна характеристика систем моніторингу. 2.6 Оптимальна для використання система моніторингу. 3 Реалізація системи моніторингу на сервері в умовах існуючого навантаження мережі. 3.1 Характеристика досліджувальної системи серверів. 3.2 Експлуатаційні показники підприємства при моніторингу серверів. 4 Спеціальна частина. 5 Обгрунтування економічної ефективності. 6 Охорона праці та безпека в надзвичайних ситуаціях. 7 Екологія. Висновки. Перелік Посилань. Додатки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1.Вступ. 2. Актуальність роботи 3. Мета та завдання. 4. Об'єкт та предмет дослідження5. Засоби Моніторингу та аналізу мережі 6. SNMP 7. RMON 8 Netflow.. 9. Zabbix. 10 Nagios. 11 Cacti 12 Paessler. 13 Порівняльна характеристика. 14. Оптимальна система моніторингу 15-20 Експлуатаційні показники. 21. Наукова новизна і практичне значення 22 Висновок

6. Консультанти розділів проекту (роботи)

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Спеціальна частина | Литвиненко Я. В., к.т.н. доцент | 06.04.20р | 12.04.20р |
| Обгрунтування ек. ефект. | Матійчук Л. П., к.е.н. доцент | 13.04.20р | 19.04.20р |
| Охорона праці | Дмитроца Л. П., к.т.н. доцент | 20.04.20р | 26.04.20р |
| Безпека в надз. ситуаціях | Стадник І. Я., д.т.н. професор | 20.04.20р | 26.04.20р |
| Екологія | Лясота О. М., к.т.н., доцент | 27.04.20р | 03.05.20р |
| | | | |

7. Дата видачі завдання 29 жовтня 2019 року

**КАЛЕНДАРНИЙ ПЛАН**

| № з/п | Назва етапів дипломного проекту (роботи) | Термін виконання етапів проекту (роботи) | Примітка |
|---|---|---|---|
| 1 | Затвердження теми дипломної роботи | 29.10.2019 р. | Виконано |
| 2 | Аналіз літературних джерел | 30.10.19 – 10.11.19 р. | Виконано |
| 3 | Обгрунтування актуальності дослідження | 11.11.19 – 18.11.19 р. | Виконано |
| 4 | Аналіз предмету дослідження та предметної області | 19.11.19 – 24.11.19 р. | Виконано |
| 5 | Оформлення розділу «Аналіз середовища та основних | 25.11.19 - 22.12.19 р. | Виконано |
| | методів моніторингу» | | |
| 6 | Оформлення розділу «Аналіз систем мережевого | 13.01.20 – 16.02.20 р. | Виконано |
| | моніторингу та обгрунтування вибору для дослідження» | | |
| 7 | Оформлення розділу «Реалізація систем моніторингу на | 17.02.20 – 01.03.20 р. | Виконано |
| | сервері в умовах існуючого навантаження мережі» | | |
| 8 | Оформлення розділу «Спеціальна частина» | 06.04.20 – 12.04.20 р. | Виконано |
| 9 | Оформлення розділу «Обгрунтування економічної | 13.04.20 - 19.04.20 р. | Виконано |
| | ефективності | | |
| 10 | Оформлення розділу «Охорона праці та безпека в над- | 20.04.20 – 26.04.20 р. | Виконано |
| | звичайних ситуаціях» | | |
| 11 | Оформлення розділу «Екологія» | 27.04.20 - 03.05.20 р. | Виконано |
| 12 | Нормоконтроль | 04.05.20 - 08.05.20 р. | Виконано |
| 13 | Перевірка дипломної роботи на плагіат | 13.05.20 р. | Виконано |
| 14 | Попередній захист дипломної роботи | 14.05.20 р. | Виконано |
| 15 | Захист дипломної роботи | 29.05.20 р. | |
| | | | |
| | | | |

Студент _____ Стеблик В. А
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ Дмитроца Л. П.
(підпис) (прізвище та ініціали)

# АНОТАЦІЯ

Мережевий моніторинг як засіб аналізу інформаційних процесів у локальній і глобальній мережах // Дипломна робота освітнього рівня "Магістр" // Стеблик Валентин Андрійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СНнм-61 // Тернопіль, 2020 // С. - 108, рис. - 38, табл. - 8, додат. - 10, бібліогра. - 50.

Ключові слова: ГЛОБАЛЬНА МЕРЕЖА, ЛОКАЛЬНА МЕРЕЖА, СИСТЕМА МОНІТОРИНГУ, ПРОТОКОЛ, ПАКЕТИ, ТРАФІК.

Дипломна робота призначена дослідженню систем моніторингу та аналізу інформаційних процесів у локальних та глобальних мережах.

У першому розділі було проведено аналіз наукових робіт та літератури, по темі дипломної роботи. Проаналізовано середовище та основні методи моніторингу мережі.

В ході виконання другого розділу було проведено аналіз існуючих систем мережевого моніторингу, проведено порівняльну характеристику даних систем. Обгрунтовано вибір оптимальної для використання системи моніторингу для подальшого дослідження.

В третьому розділі було реалізовано систему моніторингу на сервері. Проведено аналіз системи серверів, на яких проводиться дослідження. Проаналізовано експлуатаційні показники підприємства при моніторингу серверів.

Під час виконання спеціальної частини було проведено встановлення системи моніторингу, опис основних елементів даної системи та їх налаштування.

Основним завданням дипломної роботи є дослідження існуючих систем моніторингу, їх порівняння та вибір оптимальної під специфічні вимоги мережі, реалізація її на системі серверів, дослідження експлуатаційних показників реалізованої системи моніторингу на основі існуючого навантаження серверів.

# ANNOTATION

Network monitoring as an analysis tool of information processes in local and global networks // Diploma work degree “Master” // Steblyk Valentyn // Ternopil Ivan Pul`uj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Computer Science, group CSsm-61 // Ternopil, 2020 // p. - 108, fig. - 38, table - 8.

Keywords: GLOBAL NETWORK, LOCAL NETWORK, MONITORING SYSTEM, PROTOCOL, PACKETS, TRAFFIC.

Diploma work in intended for study of monitoring systems and analysis of information processes in local and global networks.

In the first section, there was conducted an analysis of scientific papers and literature on the topic of diploma work. The environment and main methods of network monitoring has been analyzed.

During the implementation of the second section there was carried out the analysis of existing network monitoring systems and comparative characteristic of these systems. The choice of the optimal monitoring system for further research is substantiated.

In the third section, the monitoring system was implemented on the server. Analysis was performed on the system of servers. The operational of the enterprise at monitoring server are analyzed.

During the special part there was implemented the installation of the monitoring system, the description of the main elements of the system and their settings.

The main task of the diploma work is to study and consider of existing monitoring systems, their comparison and selection of the optimal network for specific requirements, its implementation at different central nodes, cost-effectiveness and explore of performance of the implemented monitoring system based on real traffic.

# ПЕРЕЛІК СКОРОЧЕНЬ

ARPAnet (англ. Advanced Research Projects Agency Network) – мережа агентства передових досліджень у США.

CLNS (англ. Connection Less Network Protocol) – мережевий протокол передачі даних без встановлення з’єдання.

DDP (англ. Distributed Data Protocol) – клієнт-серверний протокол для запитів та оновлення серверної бази даних, а також синхронізації тих оновлень поміж усіма клієнтами.

DICOM (англ. Digital Images and Communication On Medicine) – стандарт для комунікації і управління медичною візуальною інформацією та суміжних даних.

ERP (англ. Entreprise Resource Planning System) корпоративна інформаційна система, призначена для автоматизації обліку й керування.

HL7 (англ. Health Level 7) – це міжнародний стандарт збереження, передачі медичної інформації та адміністративних даних у програмному забезпеченні.

ICMP (англ. Internet Control Message Protocol) – міжмережевий протокол керуючих повідомлень.

IETF (англ. Internet Engineering Task Force) відкрита міжнародна організація проектувальників, вчених, мережевих операторів та провайдерів.

iLO2 (англ. Integrated Lights-Out) – механізм керування серверами в умовах відсутності фізичного доступу до них.

InfiniBand – високошвидкісна комутована послідовна шина, що застосовується для внутрішніх та міжсистемних з’єднань.

IPFIX (англ. Internet Protocol Flow Information Export) – стандарт

IPMI (англ. Intelligent Platform Management Interface) – інтелектуальний інтерфейс управління платформою, призначений для автономного моніторингу і керування функціями, вбудованих у апаратні платформи.

IPX (англ. Internetwork Packet Exchange) – протокол мережевого рівня моделі OSI, призначений для передачі дейтаграм у системах, неорієнтованих на з’єднання.

iSCSI (англ. Internet Small Computer System Interface) – протокол, розроблений для взаємодії та управління системами зберігання даних, серверів і клієнтів.

JMX (англ. Java management Extensions) технології мови Java, призначені для контролю та керування додатками, приладами та комп'ютерними мережами.

MIB (англ. Management Information Base) – віртуальна база даних, яка використовується для управління об'єктами в мережі зв'язку.

MySQL – вільна реляційна система керування базами даних.

NAS (англ. Network Attached Storage) – сервер для збереження даних на файловому рівні.

NMS (англ. Network Management Systems) – система керування мережею.

NNTP (англ. Network News Transfer Protocol) – протокол поширення, запиту, розміщення і отримання груп новин при взаємодії з сервером або клієнтом.

OID (англ. Object Identifier) – механізм ідентифікації.

OSI (англ. Open Systems Interconnection Basic Reference Model) - абстрактна мережева модель для комунікацій і розробки мережевих протоколів.

PACS (англ. Picture Archiving and Communication System) – технологія, о використовується в медичній візуалізації для зберігання і доступу до зображень.

PDU (англ. Protocol Data Unit) – одиниця інформації яка транспортована через всю комп'ютерну мережу.

QNAP – компанія-виробник мережевих систем зберігання даних NAS.

QoS (англ. Quality of Service) – набір методів для керування ресурсами мережі.

RDMA (англ. Remote Direct Memory Access) – програмне рішення для забезпечення прямого доступу до оперативної пам'яті другого комп'ютера.

RMON (англ. Remote Network MONitoring) – протокол дистанційного моніторингу комп'ютерної мережі.

RTT (англ. Round-Trip Time) – це час, потрібний для пересилання сигналу від передавача до отримувача, а потім у зворотному напрямку.

SAS (англ. Serial Attached SCSI) – комп’ютерний інтерфейс, розроблений для обміну даними з жорсткими дисками та накопичувачами.

SCNM (англ. Self Configuring Network Monitor) – моніторинг мережі з власною конфігурацією для транспортування інформації з комутаторів та маршрутизаторів.

SMTP (англ. Simple Mail Transfer Protocol) – простий протокол передачі, призначений для передачі електронної пошти в мережі.

SNMP (англ. Simple Network Management Protocol) – протокол керування мережами зв’язку на основі архітектури TCP/IP.

SSL (англ. Secure Sockets Layer) – криптографічний протокол, який має хороший рівень безпеки.

TCP/IP (англ. Transmission Control Protocol, англ. Internet Protocol) – набір або стек протоколів мережі Інтернет.

TDP (англ. Thermal Design Power) – величина, яка показує, на відведення якої теплової енергії може бути розрахована система охолодження комп’ютера.

TOE (англ. TCP Offload Engine) – технологія реалізована в деяких мережевих адаптерах для розгрузки центрального процесора і перенесення функцій по обробці мережевих пакетів на мережевий адаптер.

UDP (англ. User Datagram Protocol) – протокол датаграм користувачів, один з протоколів стеку TCP/IP.

ULV (англ. Ultra Low Voltage) – технологія високої енергоефективності.

UNIX – сімейство багатозадачних і багатокористувацьких операційних систем, які розроблені в 1970-х роках.

VoIP (англ. Voice over IP) – технологія передачі медіа-даних у реальному часі за допомогою сімейства протоколів TCP/IP.

WMI (англ. Windows Management Instrumentation) – базова технологія для централізованого керування і стеження за роботою інфраструктури на Windows.

WREN (англ. Watching Resources from the Edge of the Network) – перегляд ресурсів на кінцях мережі.

**ЗМІСТ**

# ВСТУП

Актуальність теми. Однією з найважливіших проблем сучасних комп'ютерних мереж є швидке та ефективне виявлення несправностей передачі даних у мережі. Працюючи з мережевими сервісами чи пристроями, невелика втрата пакетів призводить до короткої затримки або ж пошкодження файлів, які можна відновити. При повному відключені даних сервісі або ж пристроїв, в залежності від діяльності, можливі великі втрати з боку підприємств або організацій. Саме для запобігання та прогнозування випадків затримки, простою або ж повного відключення даних сервісів та пристроїв використовують моніторингові системи. Системи моніторингу ведуть постійне спостереження за процесами, об'єктами та явищами з метою оцінки їх стану, контролю за ними та прогнозування. А також обробку великої кількості інформації для покращення процесів прийняття рішень.

Об'єкт дослідження. Моніторинг глобальної та локальної мережі і виявлення критичного стану пристроїв, або попередження про збій чи неполадки в мережі.

Предмет дослідження. Системи моніторингу які використовуються для збору інформації та аналізу інформаційних процесів у глобальних та локальних мережах.

Мета дослідження. Вибір оптимальної системи моніторингу під специфічні вимоги мережі, реалізація систем моніторингу на різних центральних вузлах, оптимізація затрат на встановлення та налаштування системи. Проведення дослідження експлуатаційних показників реалізованої системи моніторингу на основі системи серверів з метою зменшення навантаження на мережу. А також покращення швидкісних та якісних характеристик мережі..

Для досягнення мети потрібно виконати такі завдання:

1. Проаналізувати локальні та глобальні мережі, засоби та методи аналізу мережі;

2. Порівняти існуючі рішення систем моніторингу;

3. Обгрунтувати вибір оптимальної системи моніторингу під специфіку мережевих пристроїв.

4. Розробити розгортання та налаштування вибраної моніторингової системи на центральному вузлі.

5. Провести тестування та аналіз експлуатаційних показників.

Практичне значення. Отримання повноцінної системи моніторингу для спрощення керуванням мережею та процесами, діагностування і запобігання критичних станів мережі та удосконалення інформаційних процесів. Покращення якості і швидкості мережі та пристроїв системи.

# 1 АНАЛІЗ СЕРЕДОВИЩА ТА ОСНОВНИХ МЕТОДІВ МОНІТОРИНГУ

## 1.1 Локальні та глобальні мережі

### 1.1.1 Особливості глобальної та локальної мережі

До локальної мережі відноситься набір мережевих комп'ютерів, периферійних пристроїв (сканери, принтери, ручні комп'ютери) і комутаційних пристроїв, які розташовані недалеко один від одного, на невеликій території (в радіусі не більше 1-2 кілометри), які з'єднанні кабелями або ж підключені в один домен. В загальному випадку можна розглядати локальну мережу як одну з комунікаційних систем, яка належить одній організації. Локальні мережі ми поділяємо на два типи – це мережі із виділеними серверами або ж одноранговi мережі. Прикладом одноранговоï є комп'ютери, на основі Windows або ж іншої операційної системи, що не мають в мережі спеціального виділеного комп'ютера, що організовує доступ та роботу в мережі. Фактично кожен користувач може виділяти або ділитись певними ресурсами, тобто дисковим простором, або ж мережевими пристроями, а також кожен може підключатись до інших користувачів. Мережі з виділеним сервером - це ті мережі, що можуть здійснювати централізоване управління з використанням серверів.

Дивлячись на невеликі відстані між набором комп'ютерів та техніки в локальній мережі, використання високоякісних та дещо дорогих ліній зв'язку не є проблемою. Тим самим, локальні мережі дозволяють застосовувати просту передачу даних і досягати цим дуже високої швидкості передачі даних. У зв'язку з цим, ті послуги що входять до локальних мереж, відрізняються широкою різноманітністю, а також реалізацію їй в онлайн режимі [1].

Глобальними ж мережами називають об'єднання комп'ютерів, що по сутті територіально незалежні один від одного, і можуть розташовуватись на дуже далекій відстані один від одного, різних міста, країнах, а також і материках.

Коли глобальна мережа на рівні країни може спілкуватись між іншими мережами в цій країні або ж зарубіжними комп'ютерними мережами, та надає послуги міжнародного обміну, вона стає частиною Internet. Історія Internet починається з 60-их років, коли була створена на основі американської мережі ARPAnet. Її розробляли під замовлення міністерства оборони США. В основі цієї мережі було те, що кожен комп'ютер міг з'єднуватись із іншими і обмінюватись даними. Це стало поштовхом для багатьох організацій (а особливо урядовим та освітнім) для створення власних мереж за тим же ж принципом, які потім поєднувались з іншими.

Звичайно що така мережа на величезні відстані не є з дешевих, і обходиться вона досить дорого, часто для побудови цієї мережі використовувалися і існуючі лінії зв'язку, які були призначені для інших цілей. Багато ліній глобальної мережі були побудовані на основі загального призначення телефонних ліній, або ж телеграфних. Через великі відстані в цій мережі, швидкість та якісь цих ліній зв'язку можуть обмежуватись. Але щоб покращити стійкість та якість передачі даних, використовується спеціальне обладнання та методи, які характерно відрізняються від обладнання та методів, що характерні для локальних мереж. Зазвичай, це є складні процедури контролю, а також відновлення даних. Спотворення сигналів пов'язане із найбільш типовим режимом передачі даних [1].

### 1.1.2 Основні відмінності мереж

Локальна мережа складається з певного числа обчислювальної технік, а також розміщується вона на невеликій території, або ж підприємстві. Глобальна ж мережа складається з віддалених комп'ютерів та обчислювальної техніки, які не мають обмеження на розташування.

Отже, основні відмінності [1]:

- Протяжність комп'ютерних комунікацій та їх монтаж. Так як локальні мережі знаходять на досить невеликій відстані, в даних мережах можна використовувати більш дорожчі матеріали та комплектуючі, що підвищує якість

передачі даних. В свою ж чергу, так як користувачі глобальної мережі знаходяться в різних куточках світу, використання найдорожчих комплектуючих і матеріалів, це дуже дорого і потребує великих коштів. Тому для прокладання цієї мережі використовували наявні комунікаційні магістралі.

- Технічні засоби і методи передачі даних. При формуванні глобальних мереж використовуються не найнадійніші канали зв'язку, тому для цього потрібні більш вдосконалені методи передачі даних і технічний ресурс для подібних цілей.
- Швидкість відклику на запити та методи комунікації. В локальних мережах пакети даних приходять в лічені мілісекунди, тоді як в глобальній мережі показник відклику збільшується в десятки рази. Ця недостатня швидкість відклику на запити, може бути перепоною для сервісів які працюють онлайн.
- Масштабування. Конфігурація базової топології мережі обмежує масштабування локальних мереж. В разі розширення кількості користувачів, передача даних може погіршитись. Глобальна мережа відрізняється тим, що об'єднує велику кількість комп'ютерів на великій відстані, і це не впливає на її якісні показники.

Дані дві мережі є схожими за своїми технічними особливостями, але як видно із наведених відмінностей – вони є суттєві.

## 1.2 Значення моніторингу в сфері інформаційних технологій

Система моніторингу – це набір пристроїв та програмного забезпечення, що забезпечує постійний збір і подальшу обробку інформації, що використовується для покращення процесів та прийняття рішень, здійснення інформування відповідальних осіб або як інструмент зв'язку з метою вироблення політики, сценаріїв або ж оцінки програм. За допомогою моніторингу ми можемо стежити за процесами, що перебувають у системі. Можливі два підходи моніторингу: зіставлення результатів записів у спеціальному файлі протоколів або спостереження в режимі реального часу. Перший підхід використовується коли моніторинг налаштований на автоматичне виконання або ж віддалено. В такому

випадку всі отримані результати ми можемо передати службі технічної підтримки для виявлення причини помилок в роботі апаратного чи програмного забезпечення. Другий підхід використовують для підвищення ефективності та оптимізації роботи системи [2].

Моніторинг це концентрація уваги, на забезпечення стабільності вашої мережі, серверів та додатків. Це можливість стабільно працювати на піку апаратної і програмної можливості. Це означає не просто замітити що система вийшла з ладу, а можливість сказати коли саме ця система може вийти з ладу, а також втрутитись і запобігти раптовій зупинці всієї системи.

Досить недавно не було професіоналів з інформаційної безпеки, не було білих хакерів, а також пентестерів. Мережевою безпекою, такою якою вона була, зазвичай займався системний адміністратор. Зараз жодна з компаній не подумає виключити інформаційну безпеку із списку необхідних для підприємства. Те саме зараз відбувається і з професіоналами з моніторингу. В наш час існує багато рішень для моніторингу. Хоча багато різних підприємств не мають взагалі ніякого рішення, а інші розгортають системи моніторингу не замислюючись про сумісність, масштабованість чи стандарти [49].

Але в не дуже далекому майбутньому у нас буде світ, де ідея створити цілу команду моніторингу є такою ж реальною, як і команда з мережевих адміністраторів, адміністраторів баз даних, а також адміністраторів інформаційної безпеки, які у нас є сьогодні.

Якщо б пропрацювати в сфері IT хоча би день, можна дізнатись, що системи несподівано виходять з ладу, користувачі висловлюють твердження про те, наскільки інтернет повільний, комп’ютери несподівано перезагружаються через оновлення і т. п., або ж IT-спеціаліст витрачає половину дня на пошук помилки в звітах.

Відповідь на всі ці виклики полягає у ефективному моніторингу середовища, збиранні статистики та перевірці на помилки, щоб ви могли ефективно знайти і доповісти, коли це потрібно. Це виходить за рамки пасивного підходу до

моніторингу «переконайтесь, що все зелене», до такого, що включає оптимізацію ресурсів, оптимізацію продуктивності та активну профілактику та відновлення [3].

### 1.3 Засоби моніторингу та аналізу мережі

Безперервний контроль за станом і роботою мережі це є основа будь якої корпоративної локальної мережі. Він необхідний для підтримки працездатності та нормального стану. Тобто, при управлінні мережею початковим і потрібним етапом є контроль. Контроль часто відокремлюють від решти функцій спеціальними засобами, оскільки він є дуже важливою функцією. Такий поділ доцільно робити в малих або середніх за розміром мережах, оскільки повна систем керування є громіздка і не є економічно вигідною. Використання засобів з автономним контролем допомагає системному адміністратору виявити критичні місця мережі, а також налаштування. Хоча для переробки або ж відключення адміністратор має можливість зробити це вручну [4].

Зазвичай процес контролю мережевого середовища поділяють на два етапи – етап моніторингу та етап аналізу.

На етапі моніторингу виконується проста, але немало важлива процедура – процес збору даних про роботу мережі: статистика про кількість кадрів що є в даній мережі, і пакетів різноманітних протоколів; моніторинг стану портів мережевих пристроїв та їх доступність.

Після етапу моніторингу слідує етап аналізу, під ним ми розуміємо більш складніший і аналітично-розумовий процес розбору зібраної інформації, що прийшла з етапу моніторингу, зіставлення отриманих раніше даних, а також вироблення візуального уявлення про причини погіршення або ненадійності в роботі мережі.

Завдання моніторингу можна вирішити за допомогою програмних або апаратних засобів, приладами для тестування, інтегрованими засобами в пристроях мережі, мережевими аналізаторами, а також агентами систем керування. Аналіз в

свою чергу потребує участь людини і використання більш складніших засобів, таких як експертні системи, що обробляють досвід мережевих фахівців [47].

Розділення засобів та аналізу моніторингу мереж, відбувається на декілька великих класів [4]:

- Клас систем керування мережею. Це системи програмного рівня, які збирають дані про стан мережевих пристроїв та їх вузлів, а також отримують дані про трафік в даній мережі. Крім здійснення моніторингу і аналізу ці системи також виконують напів або повністю автоматичне управління мережею, тобто виключення або включення портів пристроїв, зміну параметрів адресних таблиць комутаторів і маршрутизаторів і т. п.
- Клас засобів керування системою. Це засоби які часто виконують функції, схожі системам управління, але стосовно інших об’єктів. Об’єктом керування у першому випадку є апаратне забезпечення або ж програмне забезпечення мережевих пристроїв, а в другому це устаткування комунікаційне. Поряд з цим, деякі функції в цих двох видах систем управління можуть бути схожими або взагалі дублювати один одного, наприклад, аналіз трафіку мережі засобами керування системою.
- Аналізатори протоколів. Вони являють собою запрограмовані або апаратно-налаштовані системи, що обмежуються лише функціями та аналізом моніторингу трафіку в мережах від систем управління. Ці аналізатори можуть ініціалізувати деяке забезпечення для перехоплення пакетів і розпочинають декодування перехоплених пакетів, тобто в зрозумілій формі зобразити для користувачів зміст цих пакетів різних рівнів один в одного з розшифруванням змісту певних полів.
- Клас вбудованих систем діагностики і управління. Це є системи що виконуються у вигляді апаратних і програмних модулів, і які встановлюються в обладнання комунікації. Також можливе у вигляді програмних модулів бути вбудованим в операційні системи. Ці модулі виконують функції діагностування і управління лише одним пристроєм, в чому є і їхня різниця між централізованими

системами. Зазвичай, вбудовані модулі виконують роль SNMP-агентів, які доводять про стан пристрою.

- Експертні системи. Ці системи поєднують емпіричний людський досвід у виявленні причин не зрозумілої роботи мережі і способи відновлення мережі у робочий стан. Ці системи є набором невеликих підсистем різних засобів моніторингу та аналізу мережі. Одним з простіших варіантів є система допомоги. Набагато складніші системи вже являють собою бази емпіричних знань, що мають елементи машинного штучного інтелекту.
- Клас багатофункціональних пристроїв аналізу та діагностики. В зв'язку з загальним поширення локальних мереж виникла і необхідність у розробці портативних приладів які поєднують в собі декілька пристроїв: аналізатори протоколів, кабельні сканери і певні можливості програмного забезпечення мережевого управління.

Майже всі класи відносяться до апаратних, програмних або ж апаратно-програмних рішень, крім експертної системи, в якій вона акумулює людські знання та досвід і накопичується у певні системи або ж бази знань.

### 1.4 Методи аналізу та моніторингу мережі

Приватні мережі в наший час розвиваються і ростуть невпинним темпом, тому надзвичайно важливо, щоб мережеві адміністратори вміли та знали як керувати мережевим трафіком та його типами, а також знаходили його в своїй мережі. Для ефективної діагностики та вирішення різного роду проблем з мережею коли вони виникають, потрібен моніторинг та аналіз трафіку. За допомогою моніторингу і аналізу адміністратори зводять період простою серверів або сервісів до мінімуму, або ж дозволяють запобігти їм взагалі.

Моніторинг мережі це складна задача, на яку потрібно витратити багато сили, але яка є надзвичайно необхідною частиною роботи в мережевих адміністраторів. Продуктивність у великих компаніях залежить від багатьох чинників, і тому якщо мережа «лежить» протягом не довгого періоду часу, ця

продуктивність скорочується. У зв’язку з цим мережевим адміністраторам потрібно стежити за трафіком що протікає і водночас за продуктивність всієї мережі [5].

В даному розділі розглянуто способи моніторингу, такі як: орієнтований на маршрутизатори та не орієнтований на маршрутизатори. Орієнтований на маршрутизатори моніторинг вбудований в них, та не потребує додаткових налаштувань чи встановлення програмного чи апаратного забезпечення. В свою ж чергу, не орієнтовані на маршрутизатори методи якраз таки потребують встановлення апаратного і програмного забезпечення, тому є гнучкими в розширені можливостей.

### 1.4.1 Протокол простого керування мережею

SNMP це протокол сьомого рівня моделі OSI, що є в наборі протоколів TCP/IP. Він дає змогу користувачу або ж адміністратору керувати ефективністю, виявляти і усувати знайдені помилки, а також розширювати ріст мережі. Збір статистики відбувається по збору трафіку кінцевого вузла, який проходить через пасивні датчики, що інтегровані з маршрутизаторами. Зараз існує три версії SNMP (SNMPv1, SNMPv2 та SNMPv3). Кожна з них має свої удосконалення порівняно з попередніми протоколами [15].

SNMPv1 це перша версія протоколу SNMP, що дала початок подальшим. Ця версія працює з великим набором мережевих протоколів. Вона отримала чимало критики через низький рівень безпеки. Аутентифікація користувачів відбувалась тільки з так званою «загальної строки», яка являла собою, по суті пароль. Так як він передавався у відкритому вигляді, проблеми з безпекою були очевидні. Розробка першої версії SNMP проводилась групою розробників у 80-их роках, і вони вважали що роботи які вони проводили можуть бути потенційно не робочі або не можливі до реалізації на платформах обрахунку того часу. SNMP був затверджений з твердженням, що це протокол проміжний, який необхідний для прийняття дій по розгортанню мережі Інтернет.

Друга версія SNMPv2 це переглянута перша версія яка доповнює покращеннями в області безпеки, конфіденційності, продуктивності та зв'язку між менеджерами. Також було введено новий запит GetBulkRequest як альтернативу використанню ітераційного GetNextRequest, в результаті чого можливе отримання більшої кількості керуючих даних в одному запиті. Однак система безпеки в SNMPv2 не отримала широкого поширення, тому що була дуже складною. Тому для цього було знайдено компроміс, який надавав більш високий рівень безпеки, але без надлишкової складності присутні в SNMPv2, це SNMPv2.

У версії SNMPv3 не було додано ніяких змін, окрім криптографічного захисту. Ця версія ж є покращенням за рахунок нових концепцій, текстових угод та термінології. Так як з самого початку основною і найбільшою проблемою SNMP була безпека, в третій версії SNMPv3 всі повідомлення мають в собі параметри безпеки, які закодовані як строки октетів. В залежності від моделі безпеки залежать і значення цих параметрів [10].

SNMPv3 представляє важливі особливості безпеки:

- Конфіденційність – для захисту від перехоплення шифруються пакети.
- Аутентифікація – виявлення джерела повідомлення.
- Цілісність – запобігання зміни повідомлень, а також захист від ретрансляції перехопленого пакету.

SNMPv3 є визнаним у IETF і описується в стандартах RFC в якості стандарту версії SNMP. Версії які були раніше є віджитими. Хоча на практиці в реалізаціях SNMP часто підтримуються декілька версій: SNMPv1, SNMPv2 та SNMPv3 [35].

Реалізація SNMP різноманітна в залежності від платформ представлення. В деяких випадках SNMP не вважаться достатньо серйозним для елементу основної розробки і тому є додатковою функцією.

Інколи запити цього протоколу при певному наборі даних можуть дати більшу, ніж очікується, навантаження на центральний процесор. Прикладом є великі таблиці маршрутизації BGP і IGP [34].

Для цього протоколу присутні три основні компоненти: Managed Devices, agents і Network Management Systems – NMSs. Вони показані на рисунку 1.1.

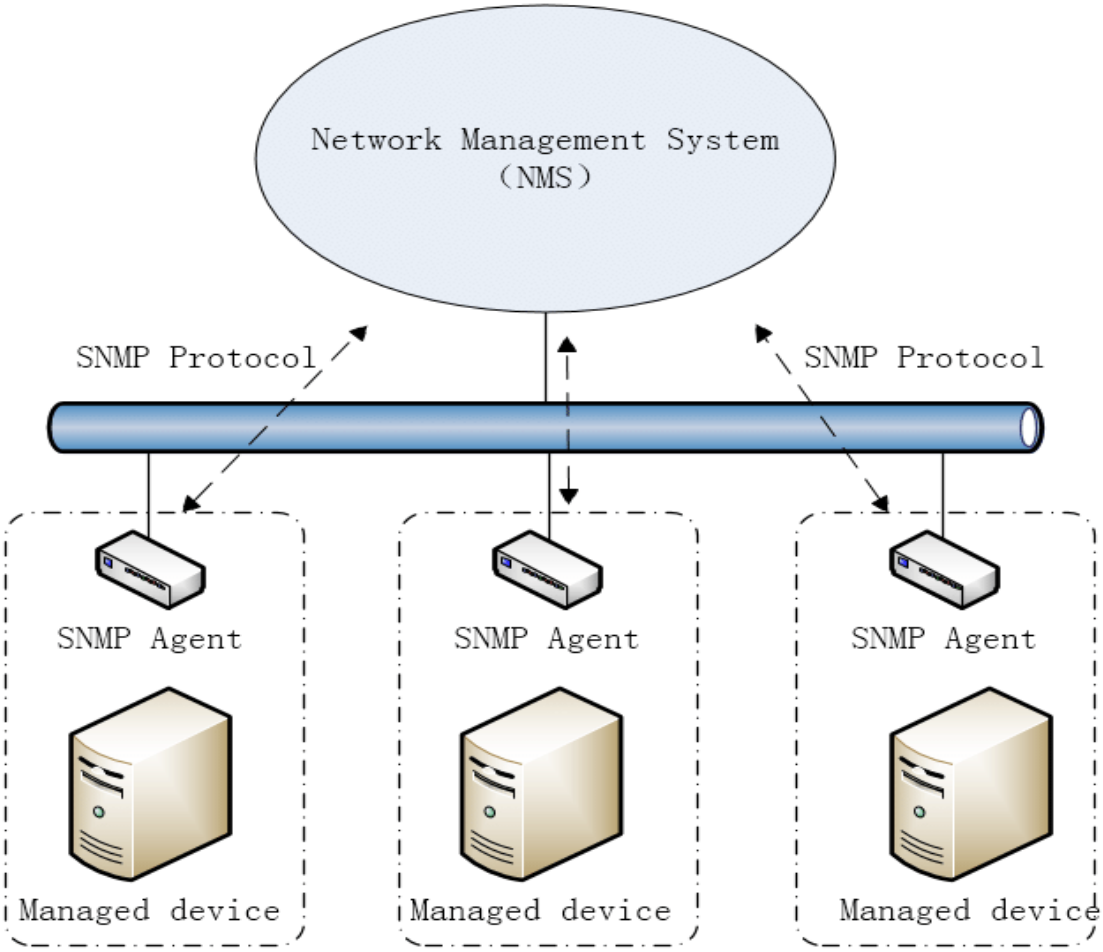



Рисунок 1.1 – компоненти протоколу простого керування

Пристрої керування вміщують в себе агент і можуть складатись із свічів, комутаторів, маршрутизаторів, принтерів, комп'ютерів та іншим. Саме агенти є тим що збирають інформацію та надають її для системи керування мережею (NMS).

Агенти є закритими для пристроїв керування. Вони містять в собі запрограмоване забезпечення, яке володіє інформацією по управлінні, а також переводить цю інформацію в форму, яка є зрозумілою з SNMP [45].

Системи керування мережею (NMS) відбувається за допомогою додатків, які включають моніторинг і контроль керуючих пристроїв. Процесорні ресурси і пам'ять які необхідні для керування надаються NMS. Для будь якої керуючої

мережі потрібно створення бодай одної системи керування. SNMP може працювати виключно як агент, чи NMS, чи може виконувати свої обо’язки або ж інші [6].

Існує чотири основні команди які використовуються в протоколі простого керування для контролю та моніторингу керуючих пристроїв: запис, читання, переривання і операція суміжності. Операція читання роздивляється зберігаючі в пристроях керування дані. Команда запису може змінювати значення цих змінних. Операція переривання, використовується в керуючих пристроях для того, щоб повідомити систему керування про відбування певної дії. Операція суміжності володіє інформацією про те, які змінні керуючих пристроїв підтримується, і збирають інформацію із керуючих таблиць змінних.

SNMP використовує сім протокольних одиниць обміну [6]:

- GetReguest. Запит до агента від менеджера, який використовується для отримання значення декількох або однієї змінної.
- SetRequest. Запит від агента до встановлення значення одної або декількох змінних.
- GetNextRequest. Запит до агента від менеджера, який використовує для отримання наступного значення змінної по ієрархії.
- GetBulkRequest. Запит від агента на отримання масиву даних.
- Response. Відповідь від агента менеджеру, який повертає запрошені значення змінних.
- InformRequest. Одностороннє повідомлення між менеджерами. Може використовуватися, наприклад для обміну інформації про MIB.
- Trap. Одностороннє повідомлення від агента до менеджера про якесь настання події.

Як було описано раніше, SNMP протокол це протокол рівня додатку, в якому використовуються пасивні сенсори, для спрощення відстеження трафіку мережі та її продуктивності, що надає допомогу мережевим адміністраторам. Цей протоколи має певні недоліки в загрозі безпеки, але також він є дуже корисним та продуктивним.

### 1.4.2 Віддалений моніторинг RMON

RMON це мережевий моніторинг віддаленого призначення. Він має в собі різні мережеві монітори і засоби для заміни даних, які отримує в процесі моніторингу. Це є розширенням для інформаційних баз даних (MIB) протоколу простого керування. На відмінну від SNMP, який змушений надсилати запити про представлення інформації, віддалений моніторинг може налаштовувати сигнали які будуть проводити постійне спостереження на основі заданого мірила. Він дає змогу керувати малими мережами, тобто локального призначення, на хорошому рівні. Монітори рівня мережі, можна побачити на рисунку 1.2.

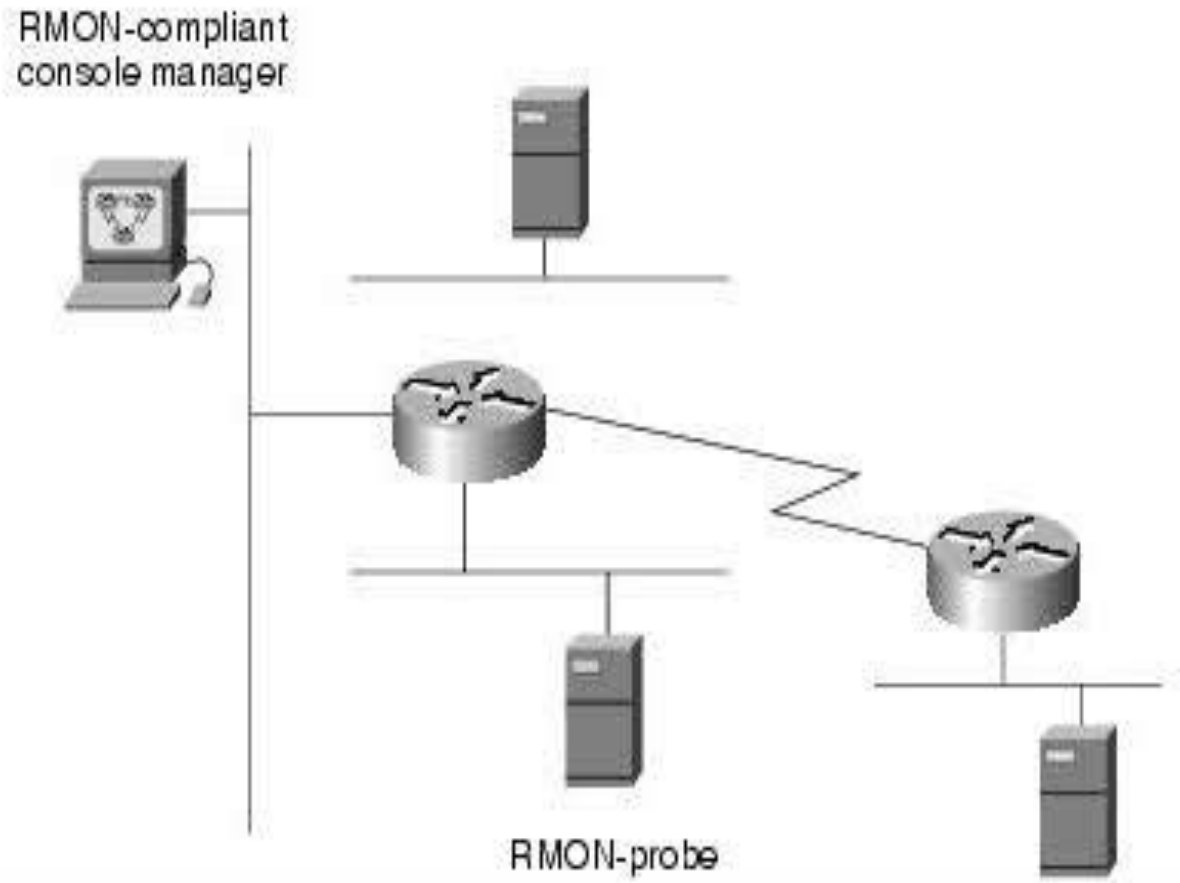



Рисунок 1.2 – Складові віддаленого моніторингу

Як видно на рисунку 1.2 є два компоненти RMON – датчик, або ж його можна ще назвати агент або монітор, і клієнт, який можна назвати як станція керування. На відмінну від SNMP агента, агент віддаленого моніторингу активно

проводить збір та зберігання мережевої інформації. Агент це вбудований в мережевий пристрій (наприклад пристрій маршрутизації або світч) програмне забезпечення. Датчик також має можливість запускатися і на персональних комп'ютерах. Датчик повинен міститись для кожного різного сегменту локальної чи глобальної мережі, так як він може збирати трафік тільки тоді коли саме через його канали трафік проходить. Тому за межами його каналу він не може знати про трафік [7].

Існує дві версії віддаленого моніторингу RMON та RMON2. RMON2 проводить мережевий моніторинг на всіх рівнях моделі OSI [33]. Але фокусується на IP-трафіку та трафіку прикладного рівня (рис. 1.3).

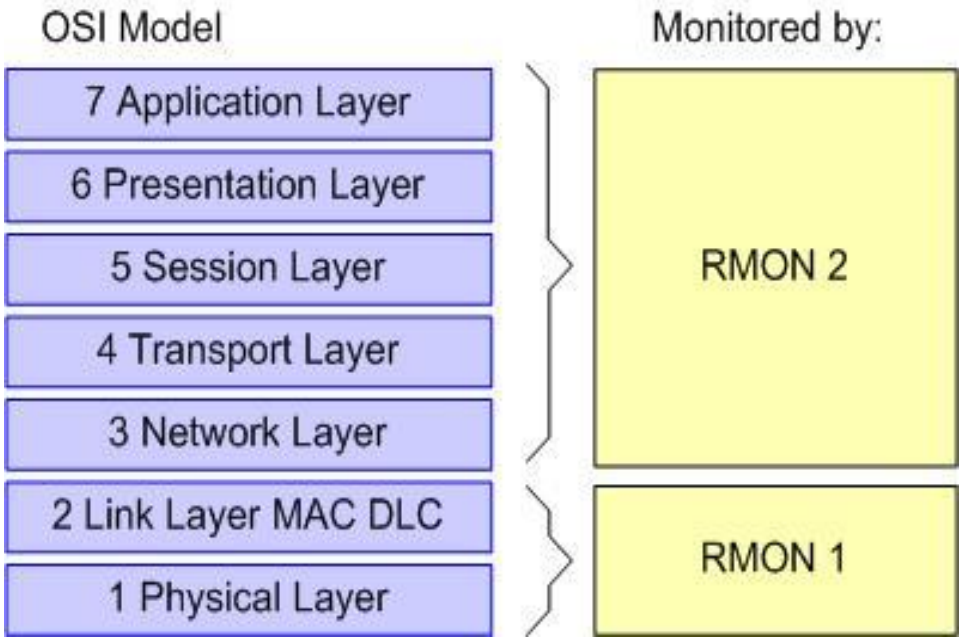



Рисунок 1.3 – RMON моніторинг рівнів моделі OSI

Клієнт це станція керування яка пов'язана з датчиком, яка використовує SNMP для отримання і кореляції RMON даних. Віддалений моніторинг має у використанні дев'ять груп моніторингу для отримання мережевої інформації:

- Statistics – виміряна статистика агентом для інтерфейсу моніторингу використовуваного пристрою.

- History – облік періодичної статистичної вибірки із мережі і збереження них для пошуку.
- Alarm – це періодичне порівняння статистичних образів з піковими значення, для генерації подій.
- Host – вміщує в собі дані по статистиці, які зв’язані з кожним приладом, знайдених в мережі.
- HostTopN – підготовлює табличні дані, для опису головного хоста.
- Filters – включає фільтрацію пакетів, беручи за основу рівняння фільтрації для захоплення подій.
- Packet capture – це перехоплення пакетів які проходять через даний канал зв’язку.
- Events – обліковує генерацію і реєстрацію подій в мережі.
- Token ring – підтримка кільцевих лексем.

Як можна замітити вище, RMON бере за основу протокол простого керування мережею. Хоча за допомогою цих методів можна виміряти моніторинг трафіку, аналітичні дані, отримані від простого керування мережею і віддаленого моніторингу мають низьку продуктивність. Утиліта Newflow, працює з великою кількістю аналітичних програм, щоб зробити роботу мережевого адміністратора набагато простішою [46].

### 1.4.3 Моніторинг на основі Netflow

Netflow – це протокол, що використовується в пристроях Cisco, які надають можливість моніторити та аналізувати трафік. При аналізі даних, які є в цих засобах, адміністратор мережі може виявити таке як: джерело і кінцевого користувача в мережі, причини перенавантаження, клас сервісів [39].

NetFlow включає в себе декілька компонентів:

- NetFlow Cache – зберігає IP потік інформації.
- FlowCollector – зберігає інформацію про потоки.

- NetFlow Export – експорт даних до колектора для подальшої аналізу та звітності.

Коли невідомий пакет даних входить в потік, і якщо маршрутизатор не бачив пакет раніше, він вирішує чи направляти датаграму чи ні. Якщо він пересилає датаграму, він робить запис у кешованому потоці (в маршрутизаторі) на основі критеріїв відповідності в пакеті.

Кожен пакет, що пересилається через маршрутизатор перевіряється на певний набір атрибутів, що ідентифікують цей пакет серед інших.

FlowCach аналізує та збирає дані про IP потоки, які входять в інтерфейс та перетворює дані для експорту [41].

На рисунку 1.4 ми можемо побачити інфраструктуру Netflow.

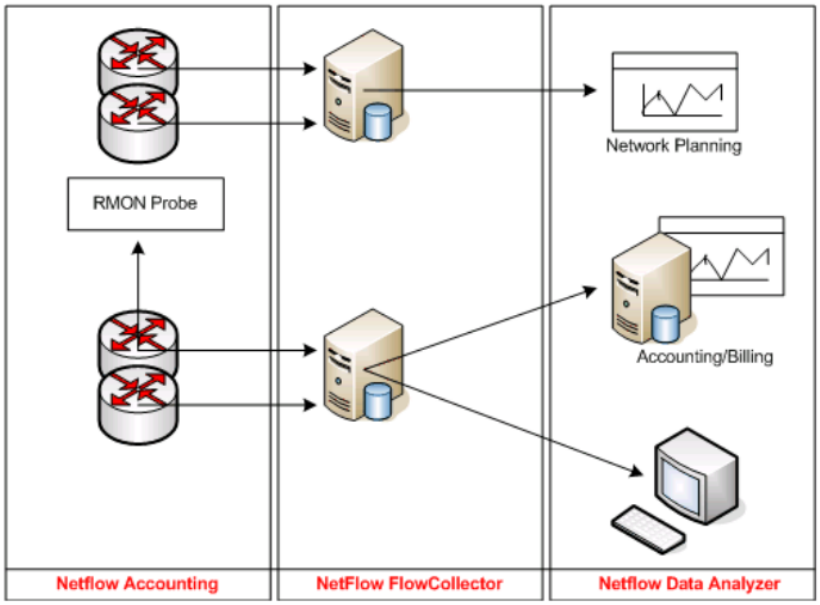



Рисунок 1.4 – Інфраструктура Netflow

FlowCach аналізує та збирає дані про IP потоки, які входять в інтерфейс та перетворює дані для експорту.

Із Netflow пакетів можна отримати набір такої інформації:

- Адресу відправника
- Адресу отримувача.
- Номер порту джерела

- Номер порту призначення.
- Кількість пакетів в потоці.
- Тип сервісу (TOS byte)
- Інтерфейс маршрутизатора або комутатора

Атрибути пакету об’єднуються у так званий потік (flow) і розміщуються : IP-адреса джерела / призначення, порти джерела / призначення, інтерфейс протоколу та клас обслуговування (рис. 1.5).

Визначення потоку є масштабованим, оскільки ці дані організовані в базу даних інформації Netflow, що називається Netflow Cache.

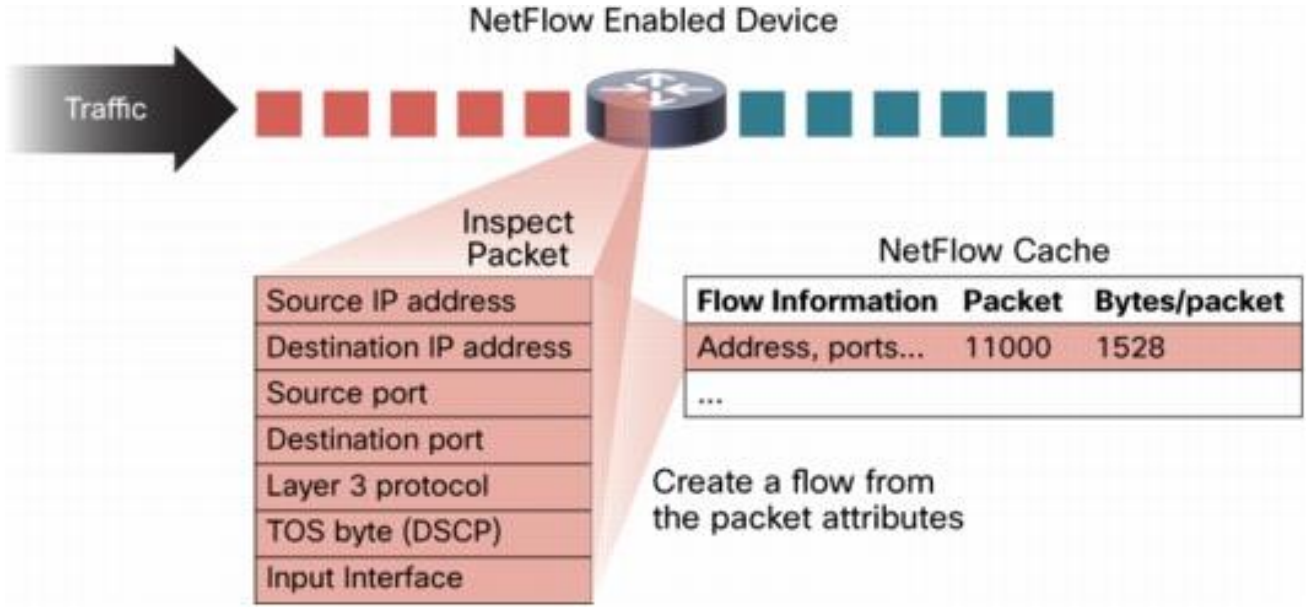



Рисунок 1.5 – Потік в Netflow Cache

Першочерговим що потрапляє на обробку для створення кешу є перший потік пакета. Потік зі схожими властивостями потрібні для утворення записів про пакети, які записуються в кеш для всіх наявних потоків. У відмітці є кількість байт та пакетів даних про кожен набір до поки з’єднання між хостом не буде розірвано. Коли потоки закінчуються вони експортуються в Flow Collector (колектор потоків), який буде аналізувати та архівувати потоки для подальшого використання. Колектор відповідає за збирання, фільтрацію та зберігання даних. Колектор потоків надає детальну інформацію про такі речі як, виявлені загрози, топологію мережі,

інтерфейси та графіки. Зниження кількості даних можна профільтрувати за допомогою фільтрів у Flow Collector. Netflow дев'ятої версії, яка зараз є стандартом IETF, відомим як IP Information Export (IPFIX), є стандартом для транспортування інформації з комутаторів та маршрутизаторів до колектора [8].

Перевагою цього протоколу над решту способами, тобто простий протокол керування і віддалений моніторинг, в тому, що в ньому є набір або пакет програмного призначення для різного роду збору і аналізу даних мережі, і які мають на меті представлення їх в більш дружелюбному для користувача вигляді.

### 1.4.4 Активний моніторинг мережі

Активний моніторинг це моніторинг що повідомляє про проблеми в мережі, на основі збору даних на двох кінцевих точках мережі. Активний вимір працює з деякими методами виміру: відгук, маршрути, packet loss, повтор пакетів, патерн пакетів, вимір кількості пройдених пакетів даних.

Ping це команда певного набору, яка дає змогу виміру втрати і затримки пакетів. Traceroute це команда за допомогою якої визначається топологія мережі, є основним зразком інструментів виміру. Два цих інструменти надсилають тестові пакети, до призначеного користувача і чекають відповіді. На рисунку 1.6 зображено як приклад, команда ping, яка виконує активний спосіб виміру, посилаючи Echo запит до кінцевого користувача через мережу.

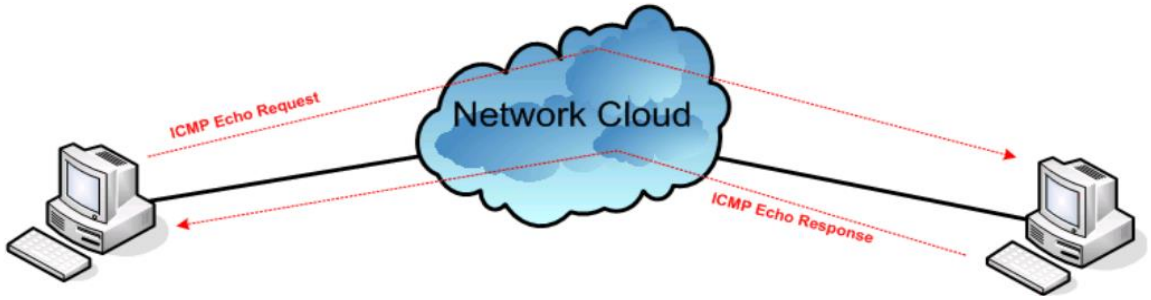



Рисунок 1.6 – Надіслана команда ping

Після цього отримувач відповідає Echo запитом у відповідь тому від кого прийшов запит.

Метод застосовується не тільки для збору одиничних метрик про активні виміри, но і може визначати мережеву топологію. Також важливим прикладом активного виміру є утиліта iperf. Це утиліта, яка визначає якість пропускної здатності траспортного і UDP протоколів. Вона дозволяє повідомити про пропускну здатність каналу, існуючі затримки і втрати пакетів [38].

Проблемою активного моніторингу є те, що представлені команди можуть вмішуватися в нормальний трафік. Часто активні спроби обробляються по іншому, ніж проста мережева активність, що надає сумніви важливості представленої інформації від цих спроб [9].

### 1.4.5 Пасивний моніторинг мережі

Основна відмінність пасивного і активного є те, що він не змінює і навантажує мережеве середовище. Ще однією відмінністю є те, що пасивний виконує збір інформації лише в одному місці мережі. Заміри є значно кращими, ніж при двох точках, як у активному. На рисунку 1.7 показано розміщення системи пасивного моніторингу, де агент розміщений на одинарному каналі між кінцями двох хостів і спостерігається трафік який проходить через канал зв’язку.


Рисунок 1.7 – Моніторинг при пасивних замірах

Моніторинг при пасивних замірах володіє такою інформацією як:

- Мережеві протоколи;
- Мережевий трафік;
- Кількість біт переданих даних;

- Час прибуття та синхронізація пакетів.

Його можна виконати за допомогою будь якої програми, яка стягує дані пакети.

Хоч і в пасивному моніторингу не має затрат, які існують в активному моніторингу, у нього є також недоліки. З пасивним моніторингом виміри можуть бути проаналізовані тільки офлайн і вони не надаються колекцією. У цьому виникає проблема, пов'язаня із зібраними даними, які обробляються. Дані сигналів не потрапляють в мережеве середовище, тому пасивний кращий активного, але післяобробка спонукає додаткову кількість часових затрат. Для цього і було зроблено поєдання двох методів.[9].

### 1.4.6 Комбінований моніторинг мережі

На основі двох попередніх підрозділів, проаналізовано що комбінація двох видів моніторингу це найкраще поєднання ніж застосування одного або іншого по роздільності. Комбінація цих технік використовують позитивні якості обох видів. В комбінованій технології описано дві нові технології, це: перегляд ресурсів на кінцях мережі, та моніторинг мережі з власною конфігурацією.

WREN є використання комбінації технік двох типів моніторингу. Ця комбінація активно опрацьовує дані, коли дані мережі невеликі за розміром і пасивно опрацьовує дані коли на великому відрізку часу трафік великий. Він переглядає мережеві дані від початкового до кінцевого користувача, що дає змогу зробити акуратніші виміри. Для виміру своєї важливої пропускної здатності, ця техніка бере за використання трасування пакетів для існуючого від додатку трафіку. Він розділений на двоє: головний рівень швидкого опрацювання пакетів і аналізатор трасування користувацького рівня.

Для швидкої обробки пакетів потрібен основний рівень щоб відповідав за отримання інформації, пов'язаної з пакетами входу і виходу. На рисунку 1.8 показано інформацію, яка стягується для кожного всіх пакетів.

Об'єкт трасування пакетів має здатність до розподілення обрахунків поміж декількома машинами. Один пристрій дає старт роботі іншого пристрою, задаючи

прапорець в шапці вихідного пакету для старту опрацювання певного широкого простору даних, що трасуються. Друга машина розпочинає трасування пакетів як тільки вона бачить, що в шапці стоїть подібний прапорець. Така направленність дозволяє забезпечувати, що дані та інформація про схожість пакетів надається для зберігання кожному кінцевому користувачі в незалежності від того, що з ним відбувається.

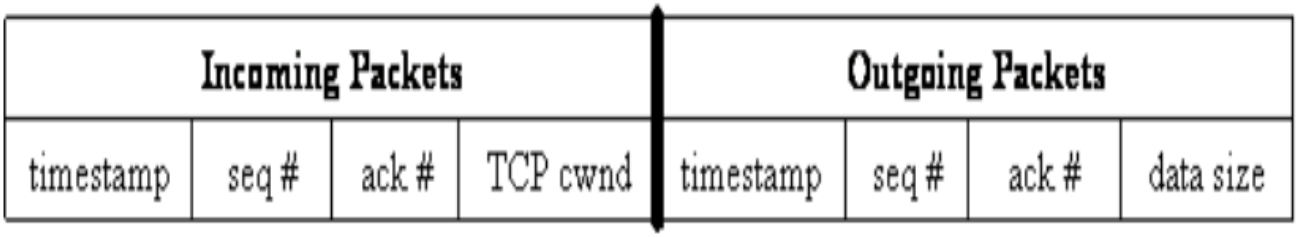



Рисунок 1.8 – інформація головного рівня трасування пакетів

Аналізатор трасування користувацького рівня – другий рівень в комбінаційному моніторингу. Це елемент, що дає початок трасування не важливо якого пакету, здійснює збір та обробку повернутих даних на операторському рівні ядра. З проектуванням, елементи користувацького рівня можуть не мати потреби в зчитуванні інформації з об’єкта за весь термін. Даний аналіз можливий і після закінчення етапу трасування, для розробки висновків, або ж висновки можуть зберігатись для майбутньої потреби в них.

При малому мережевому навантаженні, WREN задля збереження порядку потоків замірів, проводить введення трафіку в мережу. Після багаточисленних дослідів встановлено, що WREN проявляє подібні заміри в середовищах перенасиченості і протилежних.

В даній реалізації користувачі не змушені лише до захвату трасування, які були започатковані ними. Хоча кожен має можливість слідкувати за використаною мережею додатків других користувачів, доступ до інформаційних даних обмежений. В їхніх властивостях є можливість лише отримання зв’язності та аргументованості чисел, але доступу до «живих» даних із пакетів ні.

В загальному, WREN це дуже корисне поєднання, яке має в собі переваги і активного і пасивного моніторингу. Ця технологія розвивається і може надавати адміністраторам користі ресурси в моніторингу і аналізу мережі [9].

SCNM це моніторинг, що є поєднанням суміші двох вимірів, активних і пасивних, для надання інформації вихідних маршрутизаторів і інших ключових елементів мережевого середовища. Середовище має в собі і апаратний і програмний компонент.

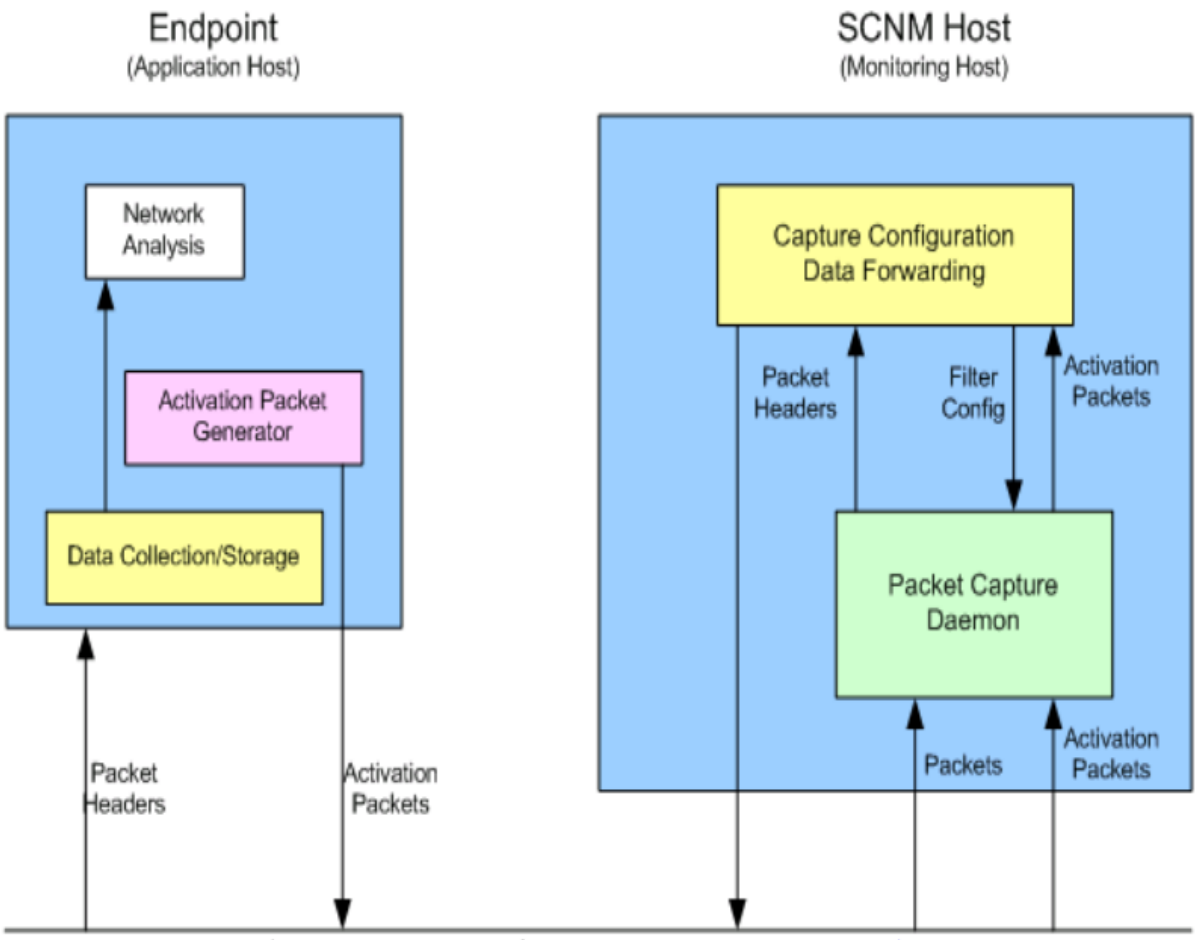



Рисунок 1.9 – Програмні компоненти SCNM

Апаратне середовище інсталюється в місцях критичної уваги мережі. Воно несе відповідальність за заголовки мережевих пакетів даних. Програма запускається на кінцевому хості мережі. Як показано на рисунку 1.9, програмне забезпечення запускається на кінцевому хості.

Відповідальність за створення і пересилання активних пакетів, які використовуються для початку моніторингу мережі лежить на програмному забезпечені. Властивості пакетів активації, які отримуються у відповідь на збір і моніторинг, посилаються користувачами. Учасники не обов'язково повинні знати місцезнаходження хоста беручи істиною те, що всі хости не закриті для «прослуховування» пакетів.

Завдяки даним, що знаходиться в змісті пакету активації, фільтр вміщується в потік аналізу даних, що є на кінцевому хості і знаходиться в робочому стані. Процес збору заголовків пакетів третього і четвертого рівня, які належать фільтру. Він вводиться в перерву на автоматі, після чітко заданого періоду часу, коли він отримає відмінні пакети додатку. Служба вибірки пакетів, що запускається на хості, користується командою tcpdump (подібне програмі вибірки) в порядку отримання записів і записи трафіку, які відповідають запиту.

Якщо завдяки інструментам пасивного моніторингу виявляється помилка, мережева активність може бути згенеровано активними інструментами моніторингу, таким чином, щоб дозволити отримувати дані які приходять для детального аналізу та вивчення помилки. При розгортувані цього монітора в мережі на кожному маршрутизаторів на протяжності шляху, ми можемо вивчати лише секції мережі, які мають проблеми [10].

SCNM визначається для встановлення і використання мережевими адміністраторами. Тим не менше звичайні користувачі здатні користуватись частиною переваг і можливостей.

### 1.5 Висновки до першого розділу.

В даному розділі розглянуто особливості глобальної та локальної мережі, їх відмінності. Проведено аналіз методів моніторингу та засобів моніторингу. В розділі описано протокол простого керування мережею, віддалений моніторинг RMON, моніторинг на основі NetFlow, комбінований, активний та пасивний моніторинг мережі.

# 2 АНАЛІЗ СИСТЕМ МЕРЕЖЕВОГО МОНІТОРИНГУ ТА ОБГРУНТУВАННЯ ВИБОРУ ДЛЯ ДОСЛІДЖЕННЯ

## 2.1 Система моніторингу Zabbix

Система моніторингу Zabbix це рішення для моніторингу мережевого середовища, яке можна сконфігурувати під окремі мережеві підсередовища. В основному це рішення для систем, які є інтегрованими з великою кількістю серверів. Ним підтримується сервери на основі Linux та Windows. Інтерфейс системи моніторингу можна побачити на рисунку 2.1.

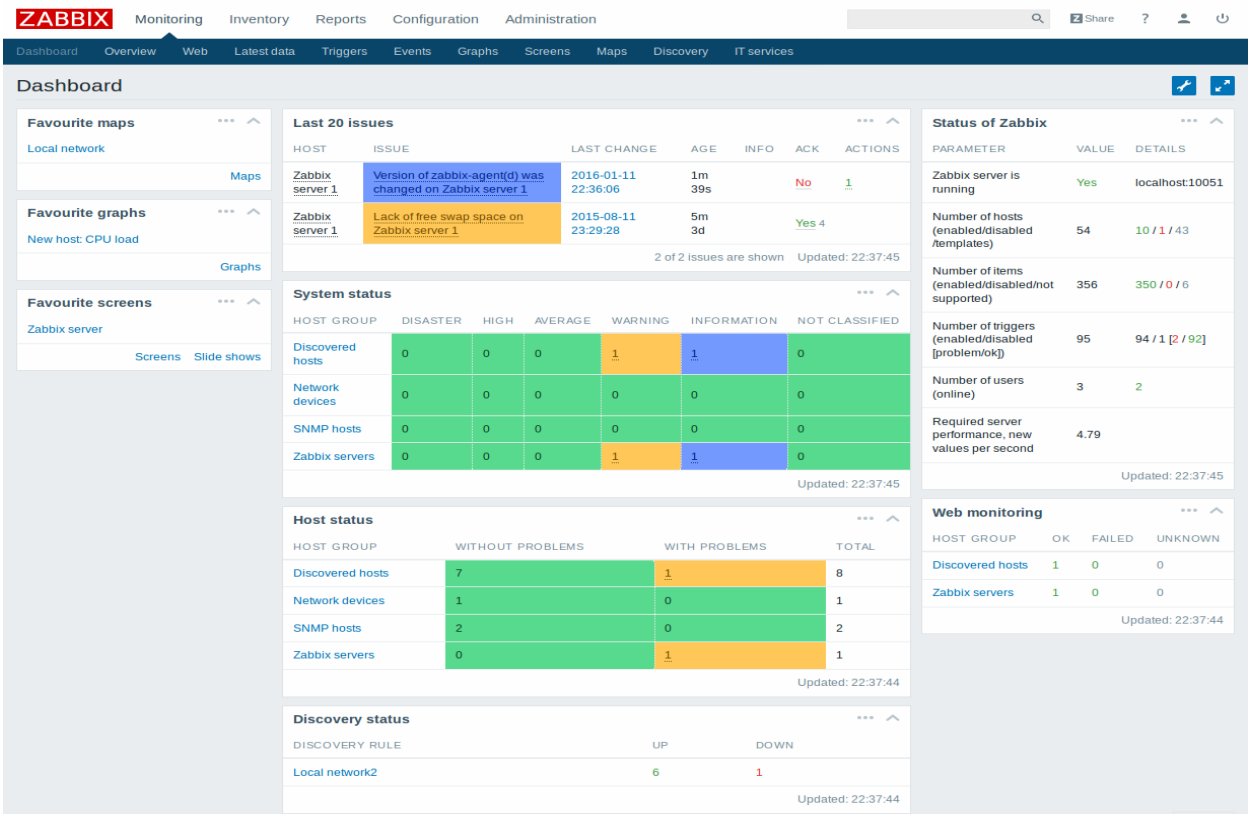



Рисунок 2.1 – інтерфейс програми Zabbix

Складається ця система моніторингу з чотирьох частин:

- Агент – спеціальний датчик для збору даних на фізичному сервері.
- Сервер моніторингу (ядро) це компонент який збирає та обробляє дані від всіх агентів.

- Веб-інтерфейс це візуалізація представлення графіків та даних в системі моніторингу.
- Проксі це компонент, який виконує ті ж самі функції, але з послідовною відправкою на центральний сервер.

Дана система моніторингу працює з різними варіаціями баз даних і може бути налаштована завчасно. Це такі як: MySQL, Oracle, SQLite, PostgreSQL та інші.

Також дана система підтримує майже всі види операційних систем (агентів та серверів). А також існують спеціальні агенти для операційних систем Windows.

Для керування певними сервісами або ж налаштуванням повідомленнями існують спеціальні тригери (рис. 2.2).

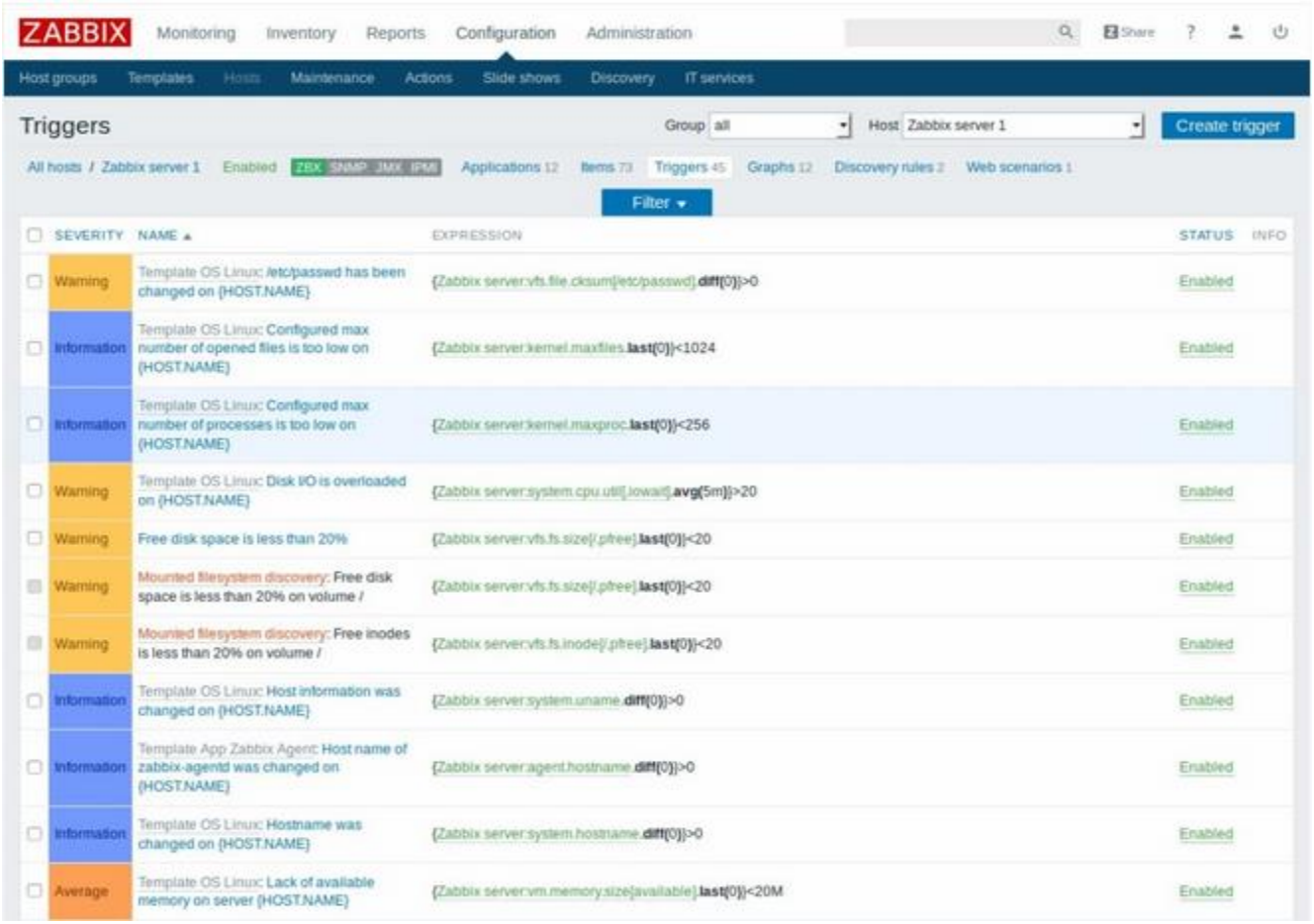



Рисунок 2.2 – Тригери в моніторинговій системі

Для активації їх, потрібно щоб значення пристрою перевищило заданий поріг, або його став був змінений.

Також в даній системі є функція об’єднання в групі, загальна інформація про які видно на панелі (рис. 2.3).

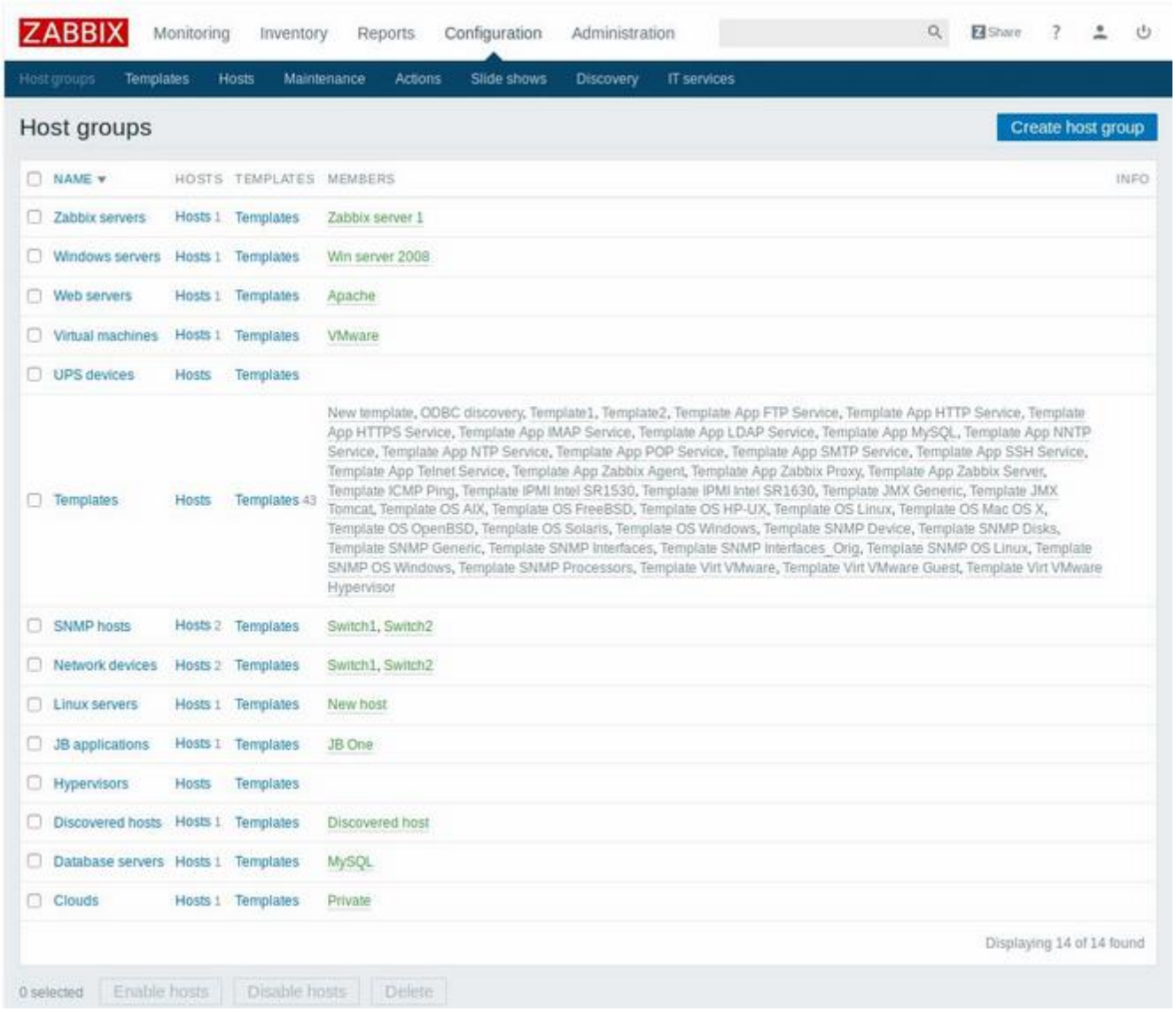



Рисунок 2.3 – Об’єднання в групи

До плюсів системи можна віднести те, що вона є дуже гнучка і достатня для практично будь якого завдання моніторингу. Також варто зазначити, що система є у вільному доступі і не потребує ліцензій. Також в ній є багатий вибір плагінів та потужні налаштування сповіщень.

До мінусів даної системи ми відносимо те, що дана система найчастіше керується UNIX системою, що доводить до інтеграції спеціальних агентів для

Windows системи. Також вона має громіздкий інтерфейс та високе навантаження на комп’ютер.

### 2.2 Моніторингова система Nagios

Система Nagios це хороше рішення для моніторингу, керування яким фокусується на веб інтерфейсі (рис. 2.4). З початку створення ця система була створена для операційних систем на базі Linux. Вона не є простою для оволодіння, однак має досить велику інтернет спільноту і добре сформовану документацію, тому освоєння не буде займати багато часу.

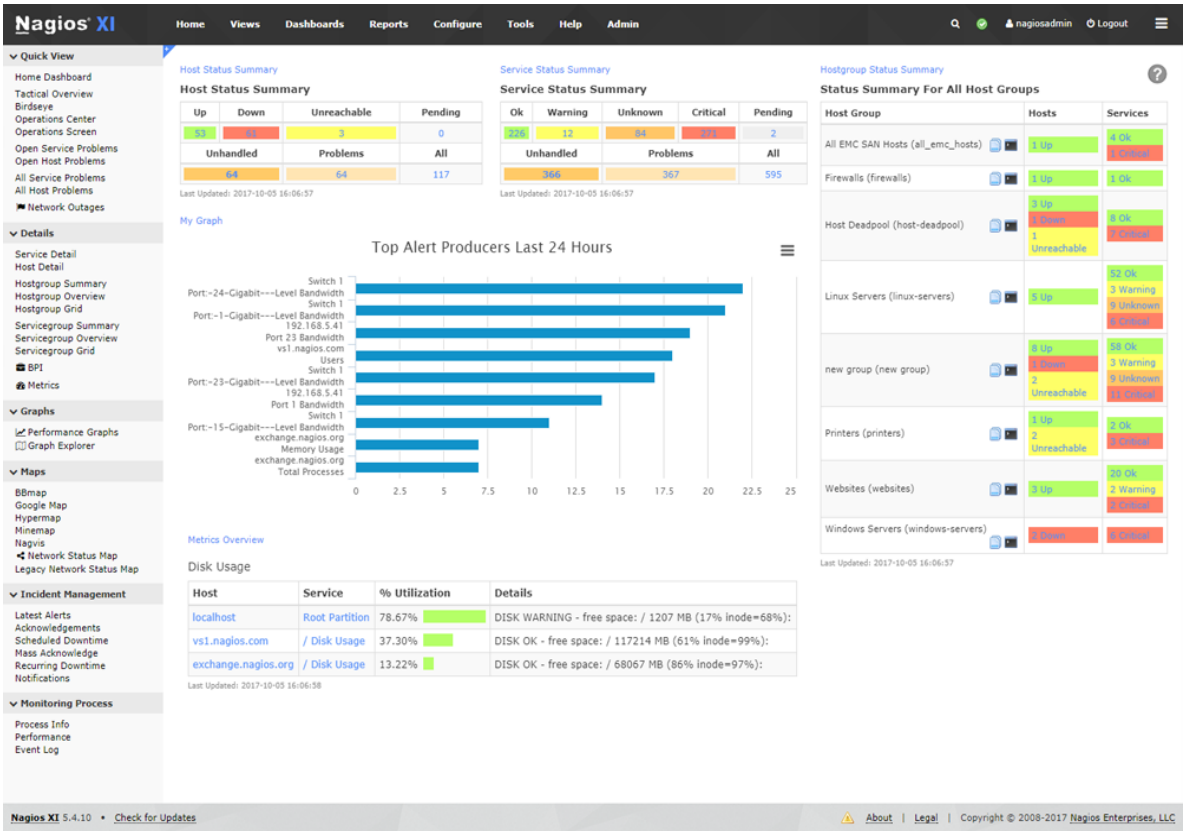



Рисунок 2.4 – система моніторингу Nagios

До можливостей даної системи можна віднести централізоване керування і аналіз мережевої інфраструктури, багатокористувацький доступ, запуск контролю додатків і сервісів за допомогою тригерів, проста до розширення архітектура а також велика кількість користувачів форумів.

Дана система може також підтримувати збір даних на основі агентів або ж без них.

При активній перевірці мережевих пристроїв, моніторинг здійснюється прямо із сервера де він встановлений.

При активному часто використовується техніка перевірки статусу. Даний метод здійснюється вже самою системою моніторингу.

При пасивній перевірка здійснюється зовнішньою програмою, а не самою системою. В кінцевому результаті після перевірки програмою, результати перевірки надаються програмі моніторингу.

Дивлячись на всі можливості даної системи до загальних плюсів у використанні її ми відносимо такі, як: висока гнучкість даної системи, містить в собі корисні шаблони та хорошу інтеграцію з іншими додатками.

До негативних сторін даної моніторингової системи ми відносимо: ціна за необмежену кількість сенсорів досить висока, трудомісткі та затратні налаштування даної мережі і необхідність наймання спеціалістів по даній системі.

### 2.3 Система моніторингу Cacti

Cacti – безплатна система моніторингу, яка дозволяє збирати статистичні дані за певний інтервал часу і відображати їх у вигляді графіків за допомогою утиліт, призначені для роботи з круговими базами даних (Round Robin Database), які використовуються для збереження інформації про зміни одної або декількох величин за певний проміжок часу. Стандартні шаблони збору даних включають в себе статистику по завантаженню процесора, виділенню оперативної пам’яті, кількістю запущених процесів, використання вхідного і вихідного трафіку.

Cacti написаний на інфраструктурі Apache-PHP-MySQL, що дозволяє налаштовувати збір і відображення даних моніторингу на основі веб-інтерфейсу, а також можливість дописати свій власний агент збору даних.

Інтерфейс відображення статистики, зібраної з пристроїв, представлення у вигляді дерева, структура якого задається самим користувачем. Як правило,

графіки групуються по певним критеріям. Є варіанти перегляду одного із набору графіків. Кожен з графіків може бути представлений за день, тиждень, місяць чи рік. Також можливо вибрати свій часовий проміжок.

До переваг даної системи ми відносимо: високу швидкість розгортання при мінімальному додатковому кодуванні, простоту та зручність інтерфейсу перегляду діаграм і їх налаштування, створення декількох користувачів і розмежування їх прав на управління даною системою, а також можливість встановлення загальної політики доступу.

До недоліків ми відносимо те, що: дана система може створювати графіки лише основних показників продуктивності, тоді як спроби створення нестандартних будуть знижувати продуктивність даного продукту, доволі старомодний інтерфейс системи моніторингу, досить швидше нарощування кількості однотипних налаштувань у випадку великого числа середовищ і серверів, обмежена продуктивність певних JMX рішень для системи.

### 2.4 Моніторингова система Paessler PRTG

Програмний компонент PRTG це проста у використанні і водночас гнучка і функціональна система моніторингу.

PRTG надає готові сенсори для моніторингу пристроїв і програм Citrix, Dell, HPE, HP, Cisco, NetApp, Fujitsu, QNAP, Oracle, VMware, Microsoft, Check Point, Fortinet і інші. Такі сенсори враховують особливості відповідних рішень і збирають дані швидше і з меншими навантаженнями на мережу.

В даній системі є декілька варіантів застосування системи. Першим є аналіз трафіку. PRTG відстежує мережевий (SNMP, xFlow, WMI) моніторить пакети даних, порти, пропускну здатність мережі (рис. 2.5). Фільтрує трафік по IP, протоколу і типу даних. Для аналізу якості використовуються сенсори QoS, які відстежують джитер, затримку пакетів (в мілісекундах), долі втрачених, пошкоджених, дубльованих пакетів, час прийому-передачі (RTT), Mean Opinion Score для тестування VoIP і інші параметри. Часто сенсори QoS використовують

для моніторингу параметрів VoIP. Також є спеціальний набір сенсорів для моніторингу VoIP рішень Cisco.

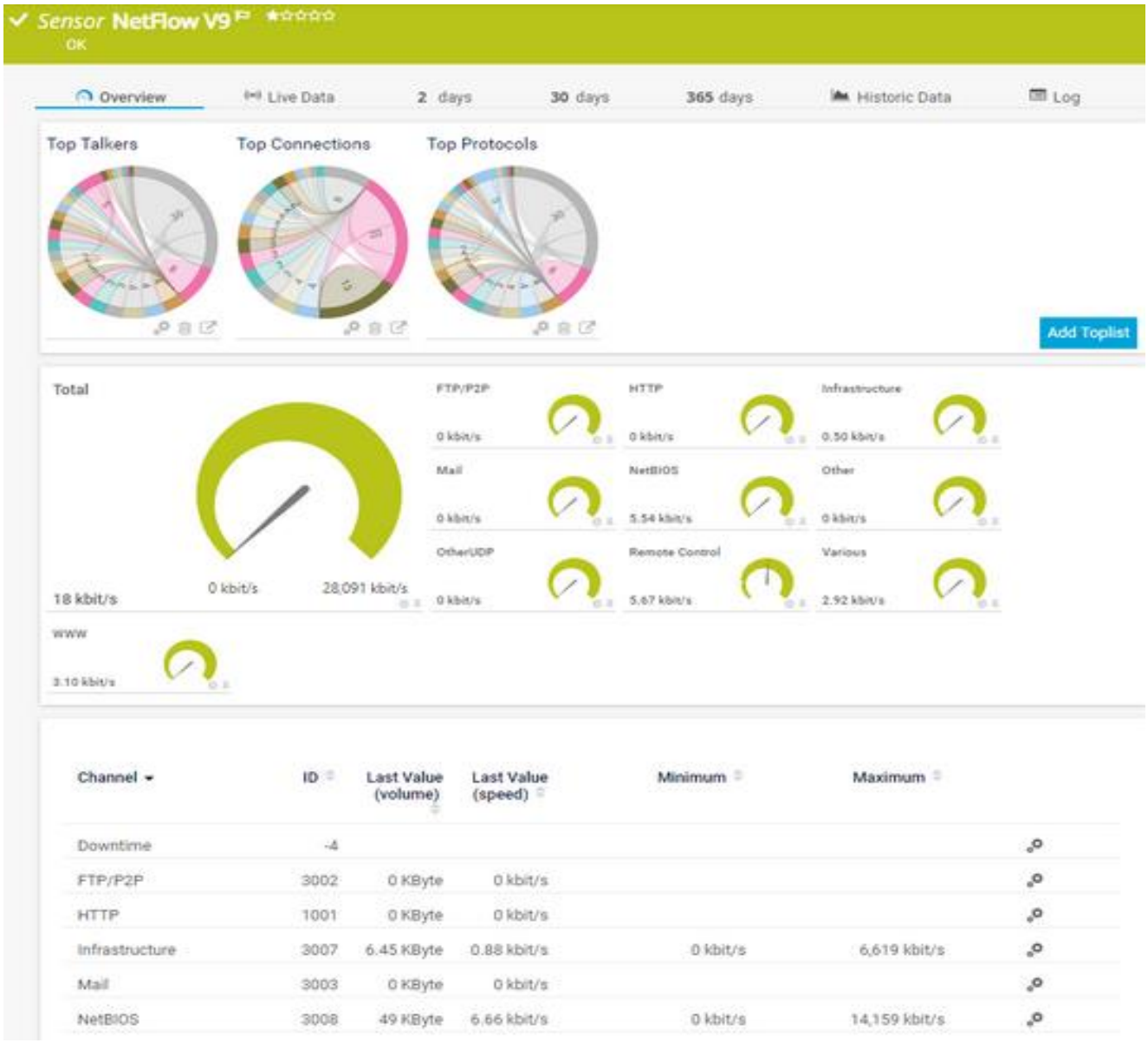



Рисунок 2.5 – сенсори NetFlow V9 у PRTG

Другий спосіб це попередження про перегрів. Система може відстежувати швидкість роботи вентилятора центрального процесора. Оскільки вихід з ладу, забруднення чи сповільнення кулера може призвести до перегріву, отже і до не стабільної роботи системи, в PRTG є сенсори, які дозволяють зреагувати завчасно.

Третім є контроль напруги мережі. Якщо ДБЖ підтримує SNMP, можна збирати дані про стан джерела живлення і контролювати ДБЖ у всій

інфраструктурі: стежити за вхідною і вихідною напругою, статусом батереї, напругою, статусом живлення (normal, bypass чи battery) і інші.

Четвертим є контроль приміщення. В систему PRTG можна добавити показники з датчиків температури, вологості, диму, відкривання дверей. Контролювати доступність камер відеоспостереження. Якщо приміщення велике, можна добавити на панель моніторингу схему будівлі в якості фону і для наочності розташувати на ній сенсори. У випадку збою можна швидко зрозуміти де саме знаходиться пошкоджений пристрій.

П’ятим є контролювання складу. В даній системі можна налаштувати її для керування складськими звітами на базі SAP або ж 1С. При зменшені певного товару на складі до критичної норми, система надсилає повідомлення.

Шостим є моніторинг онлайн сервісів. Більшість користувачів відстежують через PRTG доступність веб-серверів, трафік сайту і т.п. Багато великих онлайн магазинів почали завантажувати із ERP дані про різні надходження. Це дозволяє в реальному часі створити і порівняти динаміку відвідуваності сайтів.

Сьомим є моніторинг медичного обладнання. PRTG підтримує протоколи HL7 і DICOM. HL7 використовується для обміну медичними даними. Система моніторингу може допомогти контролювати доступність інтерфейсів, швидкість передачі даних між медичними інформаційними системами і лабораторними інформаційними системами. DICOM використовується для зберігання і передачі діагностичних зображень між обладнанням і системами архівації (PACS). За допомогою моніторингу відстежують коректність і цілісність зображень при передачі даних.

Дані сценарії можна реалізувати різними способами, не тільки за допомогою системи моніторингу. Але її головна цінність – в децентралізації. Показники інфраструктури і бізнесу контролюються через один додаток, в якому об’єднані збір, аналіз і представлення даних, розсилка повідомлень.

До основних плюсів даної системи ми відносимо: великий і широкий функціонал даної системи, можливість налаштовувати карти і панелі, гнучкий моніторинг, простий у розгортанні та використанні, можливість автоматично

розпізнавати пристрої мережі без втручання, містить готовий набір сенсорів і середовище для створення власних.

До мінусів даної системи ми відносимо: немає окремої бази даних в даній системі, можливість розгортання лише на операційній системі Windwos, доволі багато витрачається часу для налаштування системи сповіщення, висока ціна на дану систему і можливість лише тридцяти днів безкоштовної ліцензії.

### 2.5 Порівняльна характеристика систем моніторингу

Таблиці 2.1, 2.2, 2.3 дозволяють оцінити функціонал систем моніторингу комплексу IT-інфраструктури.

Таблиця 2.1 – Функціонал систем моніторингу

| Назва | Діаграми | Звіти SLA | Логічне групування | Події | Прогнозування подій |
|---|---|---|---|---|---|
| Cacti | + | + | + | + | + |
| Nagios | + | Через плагін | + | + | Через плагін |
| Zabbix | + | + | + | + | + |
| PRTG | + | + | + | + | + |

За пунктами таблиці 2.1, перевірялися наявність діаграм, звітування SLA, логічне угрупування, події та їх прогнозування.

В наступній таблиці 2.2 проводиться перевірка наявності автосканування пристроїв, агентів, доступності даної системи моніторингу, її ціна та підключення зовнішніх скриптів.

Таблиця 2.2 – Функціонал систем моніторингу

| Назва | Автосканування пристроїв | Агент | Open Source | Ціна | Зовнішні скрипти |
|---|---|---|---|---|---|
| Cacti | Через плагін | - | + | Безкоштовна | + |
| Nagios | Через плагін | + | - | 19 995 $ | + |
| Zabbix | + | Підтримується | + | Безкоштовна | + |
| PRTG | + | + | - | 15 500 $ | + |

В таблиці 2.3 ми досліджували плагіни та складність їх створення, наявність тригерів, підтримку Windows платформи та створення карти.

Таблиця 2.3 – Функціонал систем моніторингу

| Назва | Плагіни | Складність створення плагінів | Тригери | Підтримка Windows | Карти |
|---|---|---|---|---|---|
| Cacti | + | Середня | + | - | Через плагін |
| Nagios | + | Легкий | + | + | Динамічні і налаштовувані |
| Zabbix | + | Легкий | + | - | + |
| PRT*G | + | Легкий | + | + | + |

Кожна система має свої плюси і мінуси, хоча всі вони схожі за функціональними можливостями. Найбільше виділяються дві системи – Paessler PRTG та Nagios. Система моніторингу Cacti є найгіршою серед всіх показників.

## 2.6 Оптимальна для використання система моніторингу

Так як ця система моніторингу буде розгортатись на операційній системі Windows, тому такі системи як Cacti та Zabbix не є актуальними, оскільки не підтримують дану платформу. Порівнюючи системи Nagios та Paessler PRTG, плюси і мінуси даних систем, актуально використовувати моніторингову систему Paessler PRTG. Моніторингова система PRTG є простішою в налаштуванні для не досвідчених користувачів, має більшу кількість підтримуваних протоколів. Дана система дозволяє створювати діаграми та карти нашої мережевої інфраструктури, що надає візуальне представлення і допомагає у швидкому реагуванні на помилки. Для швидкості розгортання та налаштування в даній системі присутня функція автосканування всіх пристроїв у мережі. Також в ній присутнє логічне групування пристроїв і прогнозування подій. Ціна у Paessler PRTG, хоч і не набагато, але є нижчою і включає в себе безкоштовну підтримку, на відмінну від Nagios.

## 2.7 Висновки до другого розділу

В даному розділі було досліджено оптимальну для наших потреб та використання систему моніторингу серед існуючих рішень. Розглянуто такі системи моніторингу як Zabbix, Nagios, Cacti та Paessler PRTG. Для реалізації системи моніторингу на сервері буде використовуватися Paessler PRTG.

# 3 РЕАЛІЗАЦІЯ СИСТЕМИ МОНІТОРИНГУ НА СЕРВЕРІ В УМОВАХ ІСНУЮЧОГО НАВАНТАЖЕННЯ МЕРЕЖІ

## 3.1 Характеристики досліджувальної системи серверів

Дослідження та тестування для отримання реальних показників було проведено на основі двох Інтернет-провайдерів та ресурсів блейд-системи.

Для моніторингу мережі використовується система моніторингу Paessler PRTG, що встановлений на HP BladeSystem c7000 (рис. 3.1).

Це блейд-система в форма факторі 10U з підтримкою SFF дисків і можливістю встановлення серверів на базі процесорів Intel Xeon .

Одне шасі такого блейд сервера з висотою 10U (10-ти юнітів) вміщує до 16 двохпроцесорних або 8 чотирьохпроцесорних серверів із всією необхідною інфраструктурою живлення та охолодження, а також комутаційних модулів: комутаторів Fibre Channel, Ethernet, Infiniband.

Рисунок 3.1 – HP BladeSystem c7000

До основних характеристик блейд інфраструктури мможна віднести:

- Наявність двох форм-факторів – повнорозмірних блейд серверів до 8 на одній поличці, блейд серверів половинної висоти до 16 на одній поличці та Storage-blade (сервери зберігання даних) до 90 на одній поличці;
- Можливість підключити до шести блоків живлення з гарячою заміною і потужністю 2250 Вт;

- Керування за допомогою BladeSystem Insight Display або модуля керування Onboard Administrator.

В якості комутаційних модулів можуть виступати:

- Комутатори Ethernet (Gigabit і 10Gb Ethernet) і FC (4Gb Fiber Channel);
- Комутатор 4x DDR InfiniBand, який забезпечує дуже високу швидкість IB;
- Модулі патч-панелей при з'єднанні між серверами і мережею;
- Virtual Connect (Унікальний модуль віртуалізації вводу/виводу), який представляє простіше і найбільш потужніше середовище підключення до зовнішніх мереж;
- Два модулі керування Onboard Administrator

Вісім комутаційних відсіків дозволяють:

- Забезпечити до чотирьох резервних фабрик вводу/виводу;
- Використовувати Ethernet, Fibre Channel, iSCSI і InfiniBand;
- Зменшити використання кабелю до дев'яносто відсотків.

Використання блейд інфраструктури має високий рівень відмовостійкості за рахунок дублювання компонентів. Живлення в даній інфраструктурі може бути реалізовано по схемі n+n або ж n+1. Також використовується додаткова кількість вентиляторів системи охолодження. Всі серверні адаптери входу і виходу є двохпортовими, а модулі комунікації встановлюються парами.

Для використання в серверах пропонується високий вибір моделей серверів на базі двох або чотирьох ядерних процесорів Intel Xeon. Також використовуються сучасні серверні технології такі як: жорсткі диски SAS SFF, контролери Smart Array, процесор віддаленого керування iLO2, багатофункціональні мережеві адаптери з апаратною підтримкою iSCSI, TOE, RDMA.

Для ефективного керування даною системою в їх склад входять засоби, які дозволяють візуалізувати серверні полички і отримати наглядне уявлення про стан і конфігурацію блейд системи, контролювати параметри навколишнього середовища, налаштовувати підсистему охолодження та живлення.

### 3.2 Експлуатаційні показники підприємства при моніторингу серверів

Для середніх і великих підприємств якість та швидкість інтернет з'єднання є дуже важливим і необхідним. Воно необхідне для поштових служб, внутрішніх сервісів, програмами аудіо та відео зв'язку, обміну даними, зберігання та читання із файлових серверів і т. п. Тому для цього зазвичай до підприємства проводять два канали зв'язку. Щоб в разі будь якої аварії чи неполадок на стороні провайдера інтернету, автоматично включався резервний канал, і користувачі внутрішньої мережі не замітили різниці. Звичайно що це вимагає додаткових і не малих коштів, але це не є проблемою для підприємств які не можуть допустити простою у виробництві, простою у їх сервісах і т. п.

На нашому сервері встановлено систему моніторингу Paessler PRTG, яка включає в себе до тисячі хостів та 2242 сенсори, що зображено на рисунку 4.9.

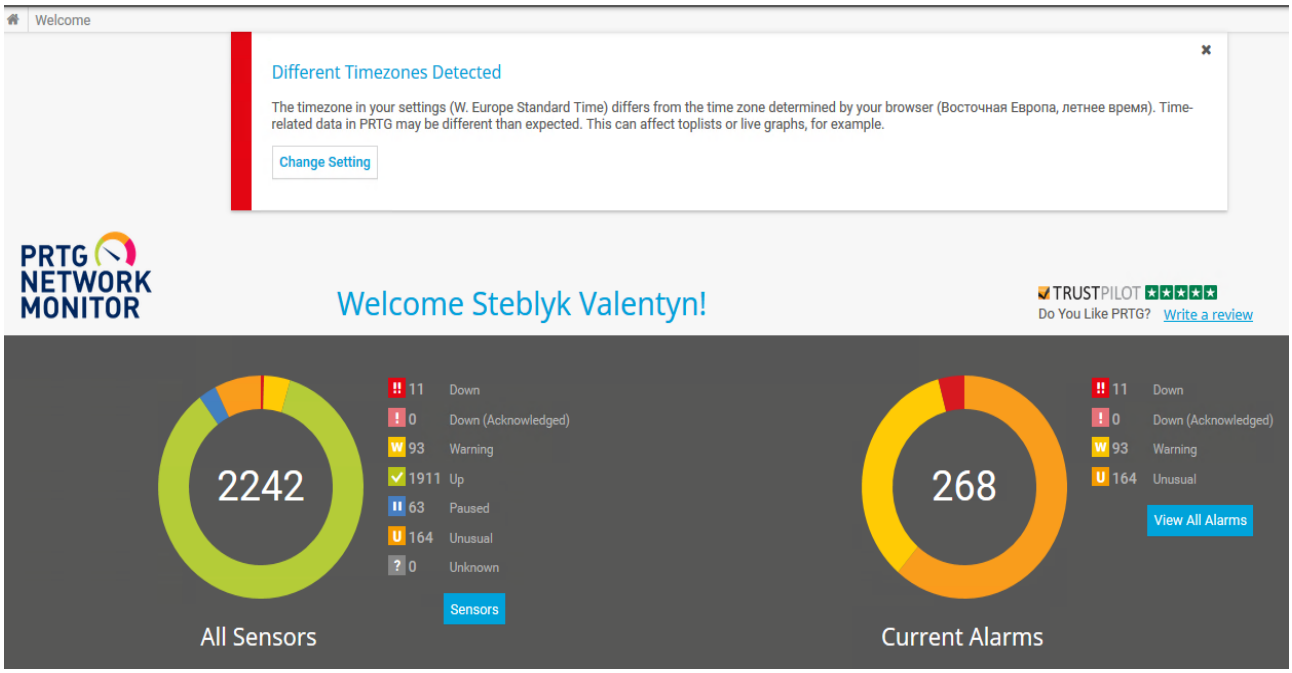



Рисунок 3.2 – Серверні сенсори та їх статус

Як зображено на рисунку 3.9, в даній системі є 1911 сенсорів що працюють в статусі добре. Також є 63 сенсори які тимчасово призупинені, у зв'язку з їх відключенням або ж роботами на них. До сенсорів які мають відхилення

відноситься 164 елементи. Це елементи системи які мають незвичайну поведінку, певні відхилення або ж певні оновлення. До сенсорів що мають статус попередження у нас відноситься 93 сенсори. Також у нас є 11 сенсорів які знаходять в статусі повного відключення.

Першим і важливим показником є трафік. На рисунку 3.3 у нас представлено тридцятиденний інтервал сканування трафіку кожні 60 секунд.

| | | | | |
|---|---|---|---|---|
| Last Scan:<br>57 s | Last Up:<br>57 s | Last Down:<br>15 d | Uptime:<br>100,0000% | Downtime:<br>0,0000% |
| Coverage:<br>99% | Sensor Type:<br>SNMP Traffic 64bit | Dependency:<br>Parent | Interval:<br>60 s | ID:<br>#21281 |

Рисунок 3.3 – Показники активного стану мережі

Сканування проводиться на основі сенсору SNMP. Час піднятої мережі і простою представлена у відсотках, і як видно з рисунку падіння мережі було 15 днів тому.

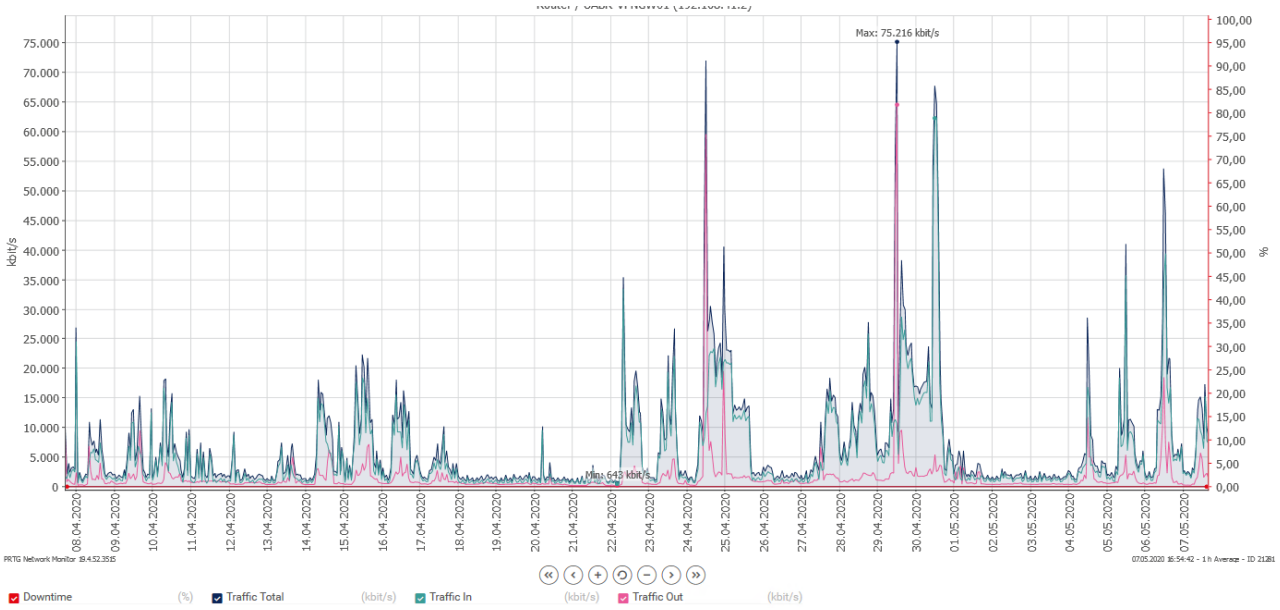



Рисунок 3.4 – Загальний трафік мережі

На рисунку 3.4 представлено загальний трафік мережі протягом 400 днів. На ньому ми можемо побачити мінімальний і максимальний піковий трафік. Мінімальним є трафік в 643 кілобіт на секунду, а максимальним 75 216 кілобіт на

секунду. Так як згадувалось раніше, наші сервера і сервіси працюють без зупинок, і комунікація між ними присутня завжди. Найменший трафік відбувається у вихідні дні, що можна помітити на графіку з другого травня до четвертого травня. Саме в ці дні крива графіку наближається до нуля. Пік припадає на такі дні як середа 29 квітня і до п’ятниці 1 травня.

Для порівняння ми візьмемо нашого резервного провайдера і його трафік, який ми можемо побачити на рисунку 3.5.

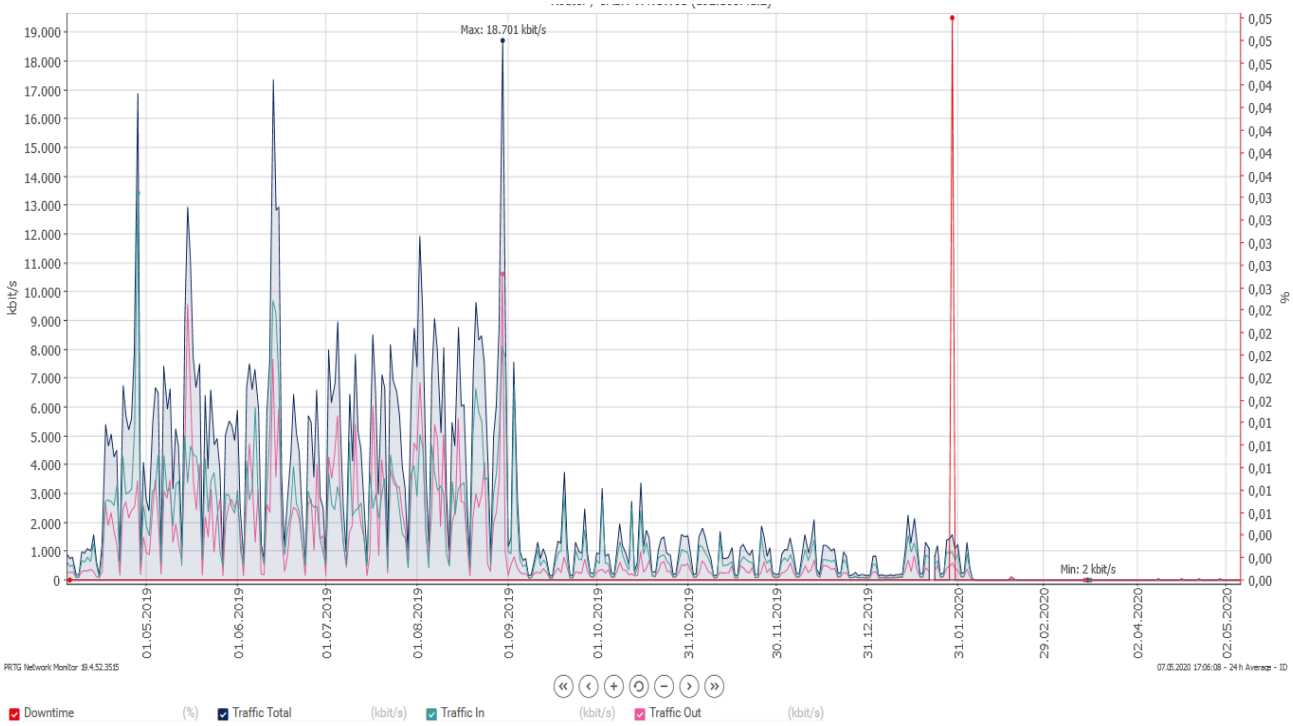



Рисунок 3.5 – трафік резервного провайдера

Так як за останні тридцять днів падіння мережі не було, тому графік за останній місяць буде фактично нульовим. Для наглядного представлення я беру графік за останні 400 днів. Звідси ми бачимо, що доволі довгий період часу дана мережа працювала в режимі основної.

Дане підприємство поділено на декілька зон з різними хостами і цілями. Воно розділене на виробництво, склад та офіси. На виробництві використовуються маленькі неттопи із програмним забезпеченням для сканування і роздруку етикет продукції яка виготовляється. Для даних операцій не потрібно великої швидкості

мережі а також системних вимог. Для складу використовуються термінали збору даних, які виконують інвентаризацію до складування, сортування і т. п.. Працюють вони через мережу WiFi і є вибагливими до якості і доступності мережі, але споживають досить малий трафік. В офісній зоні стоять повноцінні комп'ютери, які працюють постійно в мережевих папках, онлайн сервісах, програмах які потребують інтернету, відеоконференціях, тому для даної зони потрібно якісний та швидкий інтернет.

Отож, проаналізуємо трафік використання мережі на складі, дивлячись на рисунок 3.6.

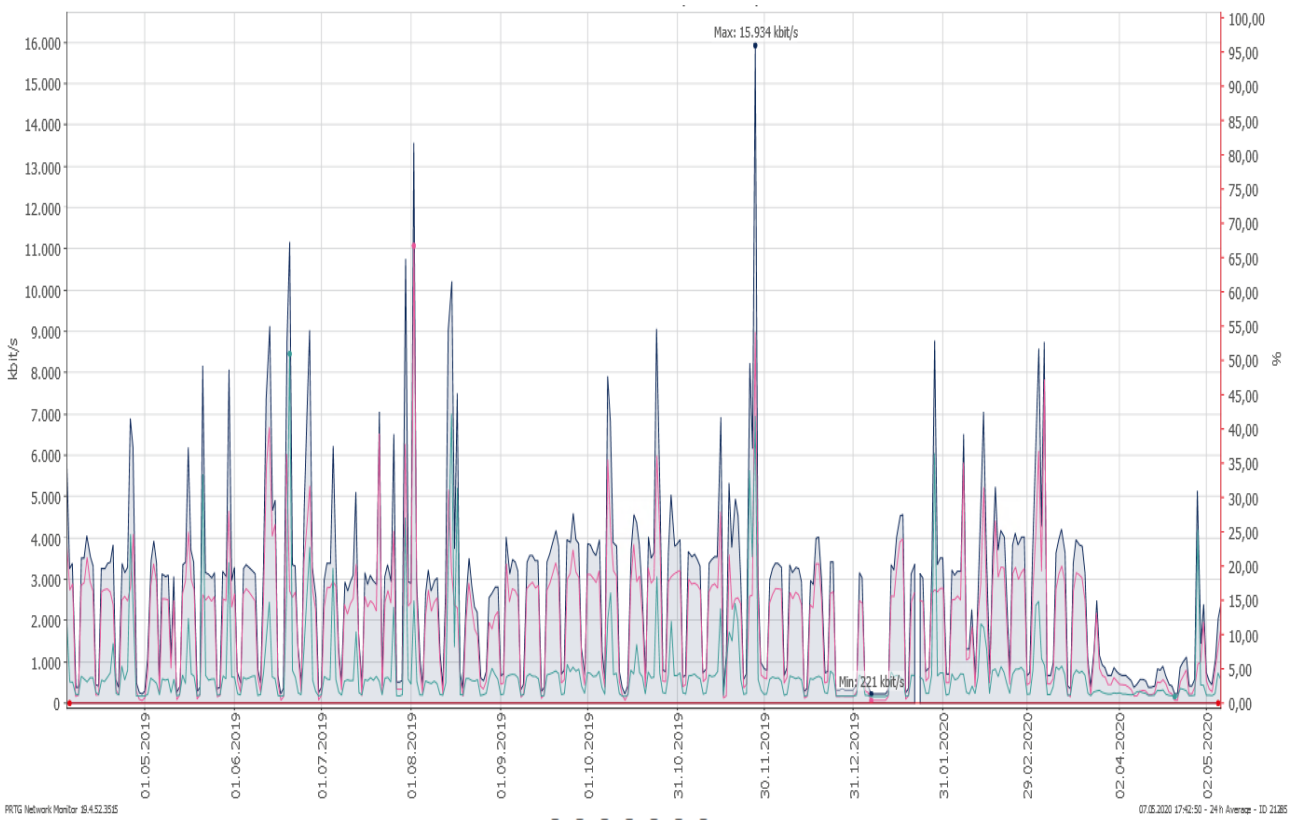



Рисунок 3.6 – трафік складського обладнання

Графік було взято за період останніх чотириста днів. Як ми бачимо з графіку, використання складським обладнанням трафік є малим і середнє значення приблизно три тисячі кілобіт на секунду. Все тому що термінали збору даних не використовують і не обробляють велику кількість даних, а лише підключаються до програми SAP та виконують базові операції в ній.

Наступним нашим графік для аналізу буде графік офісної мережі. Як зазначалось раніше, дана мережа повинна забезпечувати хорошу та безперебійну швидкість в даній зоні використання. Отож поглянемо на рисунок 3.7 і проаналізуємо трафік.

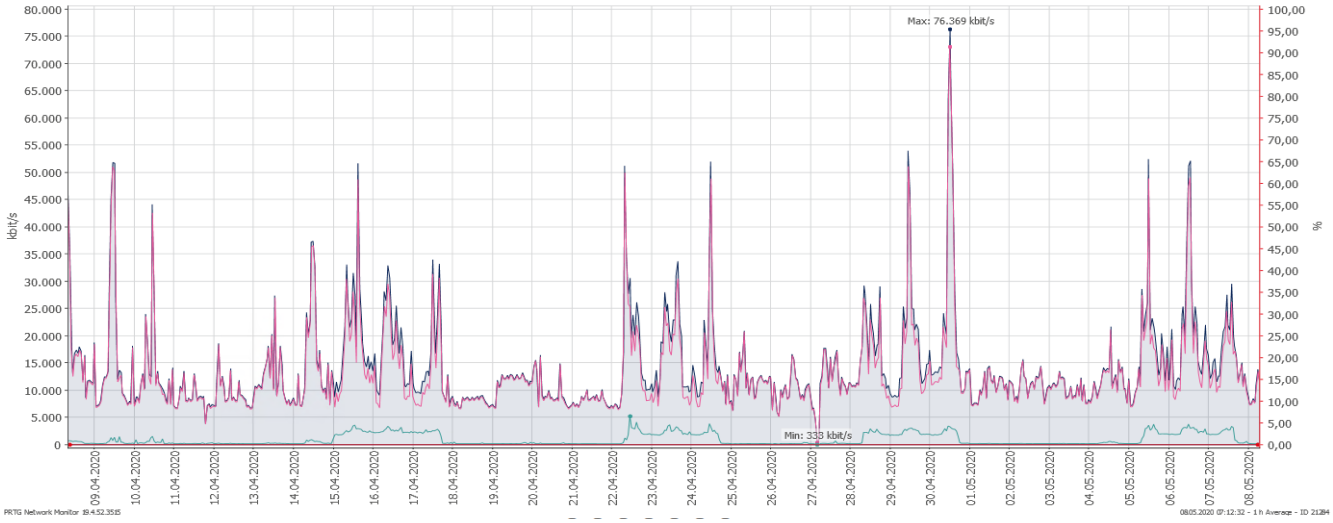



Рисунок 3.7 – трафік використання офісними працівниками

Як ми бачимо на цьому графіку за тридцять днів, працівники досить активно використовують дану мережу. Якщо взяти середнє значення трафіку за день, він складає приблизно 10 тисяч кілобіт в секунду. Це досить не мала кількість даних.

Наступним є графік трафіку VOIP пристроїв. Для хорошого та безпечного зв’язку на даному підприємстві є близько 200 телефонів Cisco.

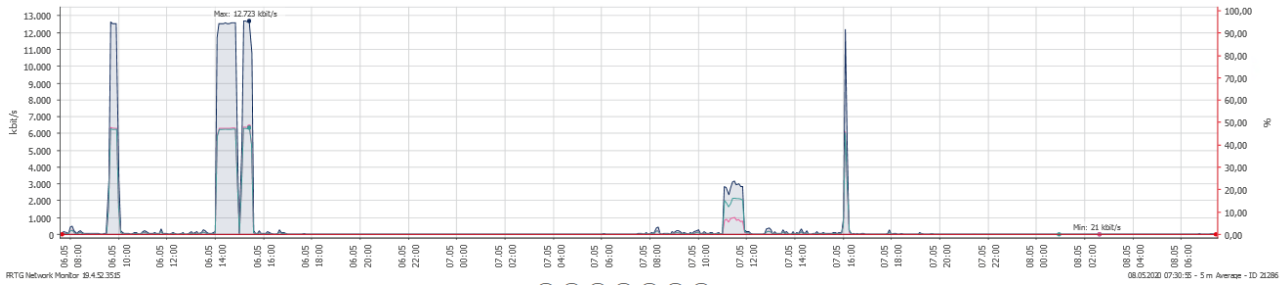



Рисунок 3.8 – графік використання VOIP за два дні

На рисунку 3.8 ми можемо побачити графік використання VOIP пристроїв за два дні. З графіку можна зрозуміти що цими пристроями користуються не так

часто як іншими сервісами. Хоча для даних пристроїв не властива велика кількість трафіку (рис. 3.9), якість з’єднання мережі повинна бути ідеальною, для можливості безперебійного спілкування з іншими абонентами.

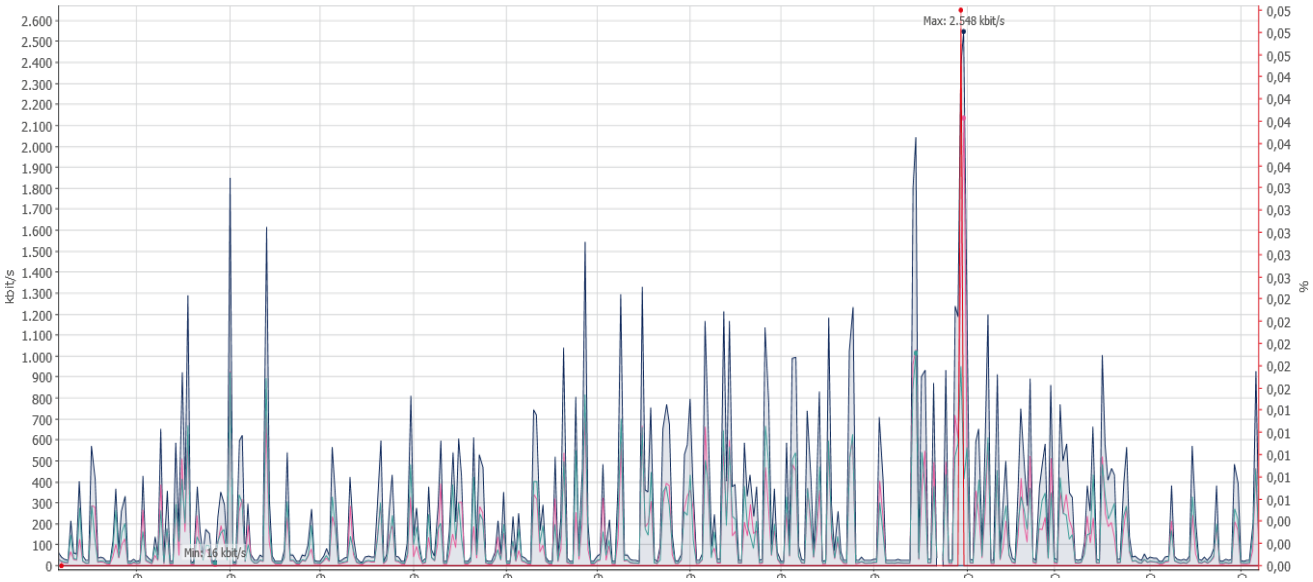



Рисунок 3.9 – трафік VOIP пристроїв за 400 днів.

Наступним на рисунку 3.10 ми можемо побачити трафік серверів.

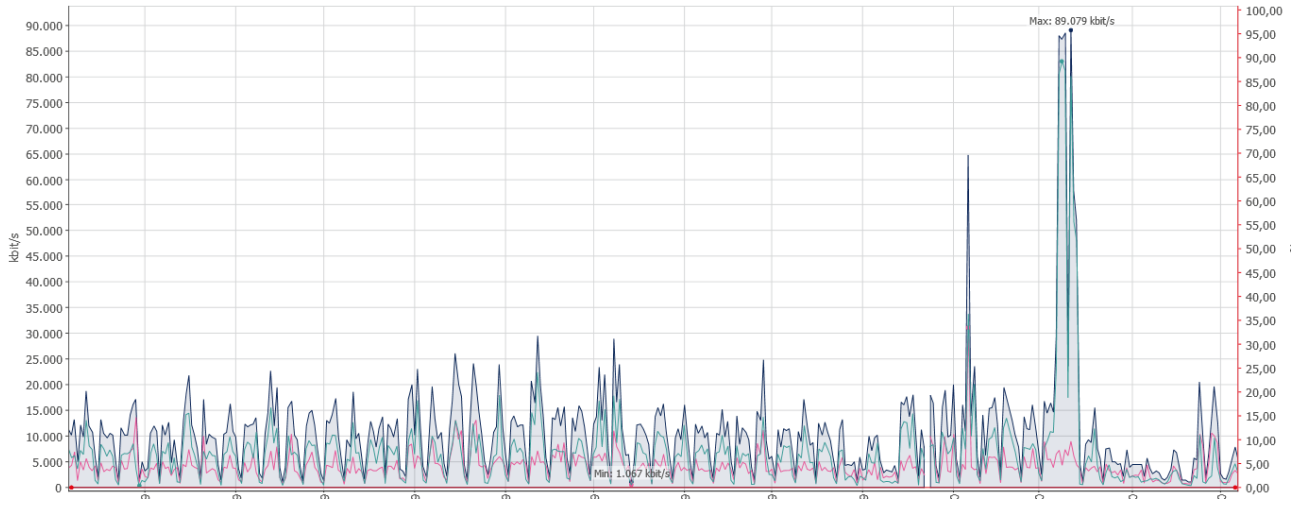



Рисунок 3.10 – трафік використаний серверами

Як видно на даному графіку за 400 днів, сервери знаходять в постійному споживані трафіку. Хоча він невеликий, але як видно що є певні часові зони в яких

він піднімається досить високо. Це може бути обумовлено з великою кількістю користувачів які взаємодіють з сервером, встановленням обновлень, або ж резервними копіюваннями.

Система моніторингу це є універсальна система спостереження за всіма можливими процесами в мережі, тому дальше аналізуємо серверні сенсори.

В додатку А, ми можемо спостерігати за сенсорами та їх станом на файловому сервері. Даних сенсорів є 11, але найбільш важливими є сенсори Disk Free, Dick_IO_Total і RDP.

Перший сенсор Disk Free відповідає за загальну кількість вільного місця. Оскільки це є файловий сервер, при заповнені всього вільного місця користувачі не зможуть обмінюватись, зберігати чи надсилати інформацію іншим користувачам, тому при наближені до відсоткового мінімуму, потрібно очищувати або ж збільшувати розмір дисків даного серверу.

Наступний сенсор Disk_I/O_Total визначає загальну кількість інформації, яка записується чи зчитується з даного сервера. Дана функція є корисною для візуалізації кількості даних яка записується чи зчитується з даного сервера, оскільки при незаконному проникненні на даний сервер буде великий скачок зчитуваних даних. В додатках ми можемо побачити графік читання і запису за 400 днів (додаток В), 30 днів (додаток Д), 2 дні (додаток Е) на даному сервері.

Сенсор RDP є також важливим сенсором. При активному стані даного сенсору у нас є можливість віддалено заходити на сервер і керувати ним. При вимкненні даної функції, у нас втрачається дана можливість, що є критично важливим, оскільки не завжди є можливість фізично зайти на даний сервер і керувати ним.

Наступним нашим сервером є сервер віддаленого підключення користувачів. Оскільки кількість користувачів є досить велика, даний сервер розподіляє користувачів між двома серверами USER1 та USER2.

В додаткуах ми можемо побачити які сенсори використовуються на даному сервері (додаток Є). Оскільки він призначений для використання користувачами,

основні властивості які він має мати це достатня кількість оперативної пам’яті, можливість підключення до RDP, та стабільність і постійну активність.

Першим і найголовнішим є кількість оперативної пам’яті. Оскільки до даного серверу підключається велика кількість користувачів, потрібна велика кількість оперативної пам’яті (додаток Ж). На даному сервері USER1 встановлено 32 гігабайти оперативної пам’яті. З рисунку ми можемо побачити що кількість вільної пам’яті є 15 гігабайт, що доволі небагато, враховуючи той факт, що дане дослідження розробляється у вихідний день.

Перейшовши на другий сервер USER2, ми можемо подивитись і порівняти наші сенсори. На додатку К ми можемо побачити кількість і схожість із сенсорами першого серверу. Оскільки даний сервер виконує ідентичну роль що і перший сервер, всі сенсори також дублюються. На додатку Л можна замітити, що даний сервер має таку ж кількість оперативної пам’яті як і в першому. Єдина відмінність в навантажені на нього. Кількість оперативної пам’яті яка вільна є на 9 гігабайт більша, тобто 23 гігабайти вільної. Це вказує на те, що кількість користувачів не збалансована і потрібно розробляти або ж переписувати скрипт розподілу навантаження на сервери.

### 3.3 Висновок до третього розділу

В даному розділі було описано основний блейд сервер, на якому проводились дослідження. Досліджено використання трафіку складськими пристроями, офісними працівниками та їх персональними комп’ютерами, пристроями VOIP та серверами. Проаналізовано основні сенсори, які використовуються на файловому сервері та сервері віддаленого доступу користувачів.

# 4 СПЕЦІАЛЬНА ЧАСТИНА

## 4.1 Встановлення системи моніторингу Paessler PRTG

Для того щоб ми могли скачати і встановити нашу систему моніторингу ми переходимо на головний сайт даної системи моніторингу. На головній сторінці ми можемо побачити посилання на завантаження даної системи, або ж знайти в меню скачування.

Після завантаження образу, ми запускаємо його. Дана програма має вшиту в файл інсталяції ліцензійний ключ, тому, як видно на рисунку 4.1, не потрібно вводити ключ ліцензії, вона автоматично підтягує його.


Рисунок 4.1 – Ініціалізація ліцензії PRTG

Після встановлення даної програми, нам автоматично відкриє у браузері за замовчуванням локальну адресу на яку встановлено систему моніторингу.

### 4.2 Основні елементи системи моніторингу Paessler PRTG

Усі об’єкти в моніторинговій системі PRTG розташовуються по ієрархії, що нагадує дерево. Об’єкти можуть групуватись по пристроях, сервісах чи певних місцях розташування. Цей ієрархічний порядок також використовується для визначення загальних параметрів для об’єктів більших груп. Наприклад, налаштування кореневої групи застосовуються до всіх інших об’єктів, що розташовані під ієрархією (рис. 4.2).

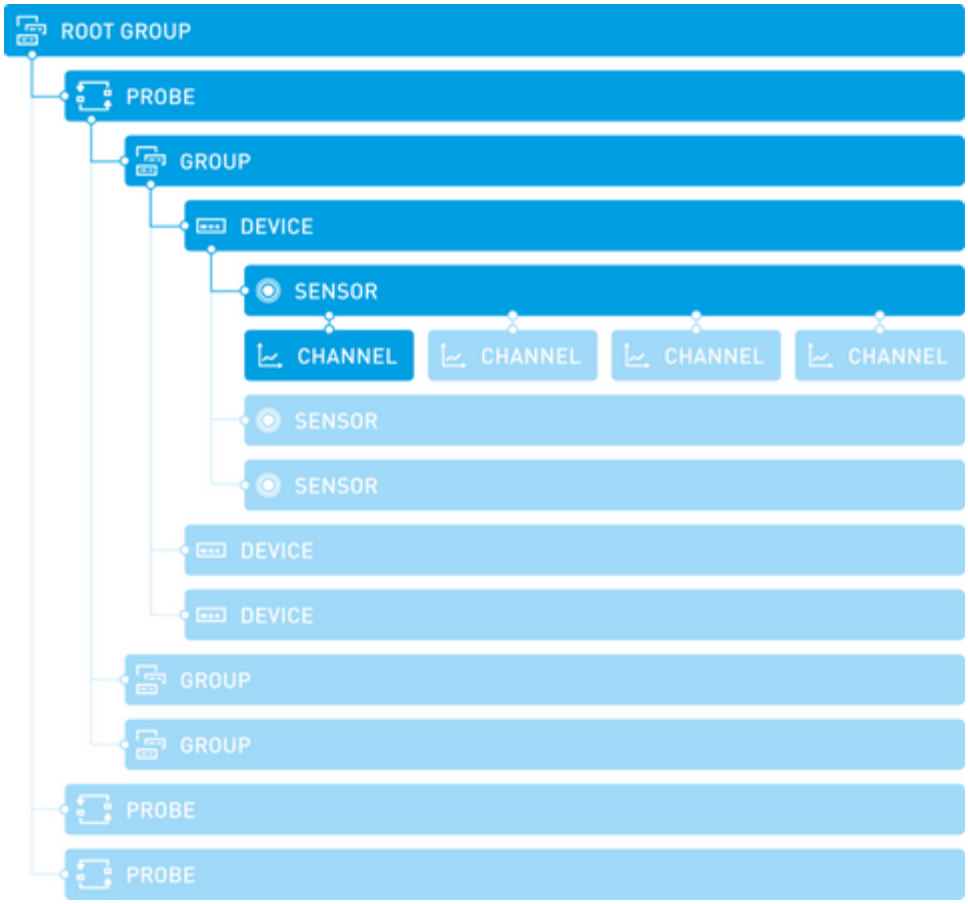



Рисунок 4.2 – Ієрархія об’єктів у PRTG

Probe це платформа, в зоні якої відбувається моніторинг пристроїв. Даних зон можна створювати декілька, в залежності від мережі яку потрібно сканувати.

На кожній зоні моніторингу є одна або декілька груп, які мають структурне призначення. Групи використовуються для розташування подібних елементів, щоб при налаштуванні всієї групи, вони успадковували однакові показники.

На рисунку 4.3 показано конфігурацію дерева пристрою із зоною моніторингом, кількома групами, пристроями та їх датчиками.

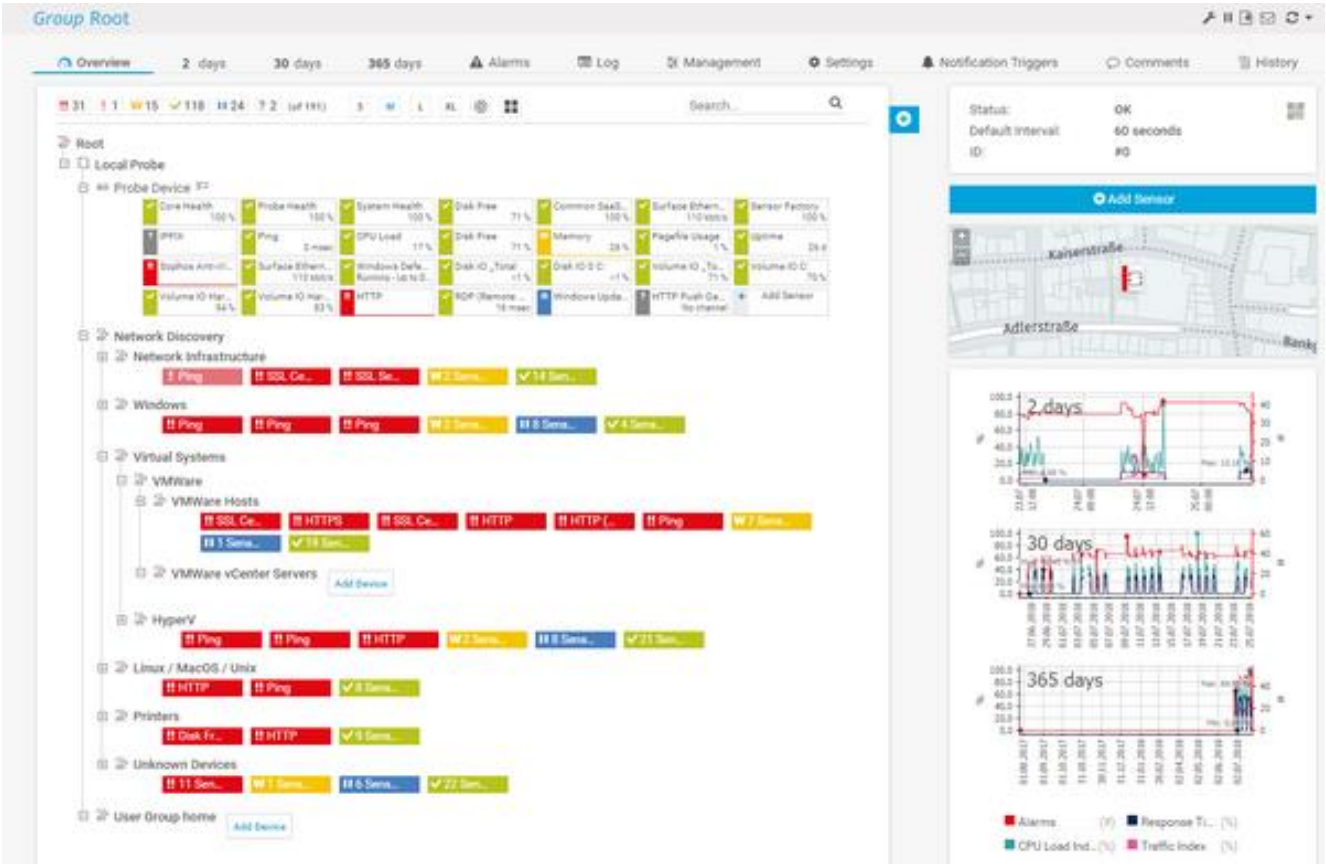



Рисунок 4.3 – зразок дерева з пристроями

Device це пристрій, відносно якого відбувається моніторинг. Кожен пристрій в конфігурації це реальне обладнання або віртуальний пристрій у мережі. Це може бути: веб або файловий сервер, клієнтські комп’ютери, маршрутизатори, практично кожен пристрій мережі.

Дана система автоматично аналізує додані пристрої та рекомендує датчики, які можливі для встановлення. Також можна додавати декілька разів один і той самий пристрій, для кращого огляду при використанні великої кількості датчиків.

На кожному пристрої можна створити ряд датчиків. Кожен датчик контролює один окремий аспект пристрою. Це може бути, наприклад:

- Мережеві послуги, такі як SNMP, FTP, HTTP та інші;
- Трафік мережевого комутатора;

- Навантаження процесора на пристрій;
- Завантаження пам’яті на пристрої;
- Трафік на мережевій карті;
- Пристрої NetFlow;
- Стан системи пристроїв;
- Та інші (бази даних, доступність файлів, електронної пошти і т.п.)

Кожен датчик має ряд каналів, через які він приймає різні потоки даних. Наявні канали залежать від типу датчика. Він може містити пробіг та час роботи пристрою, час завантаження веб-сторінки, час відповіді на запит ping на пристрої, час відгуку пристрою та інші (рис. 4.4).

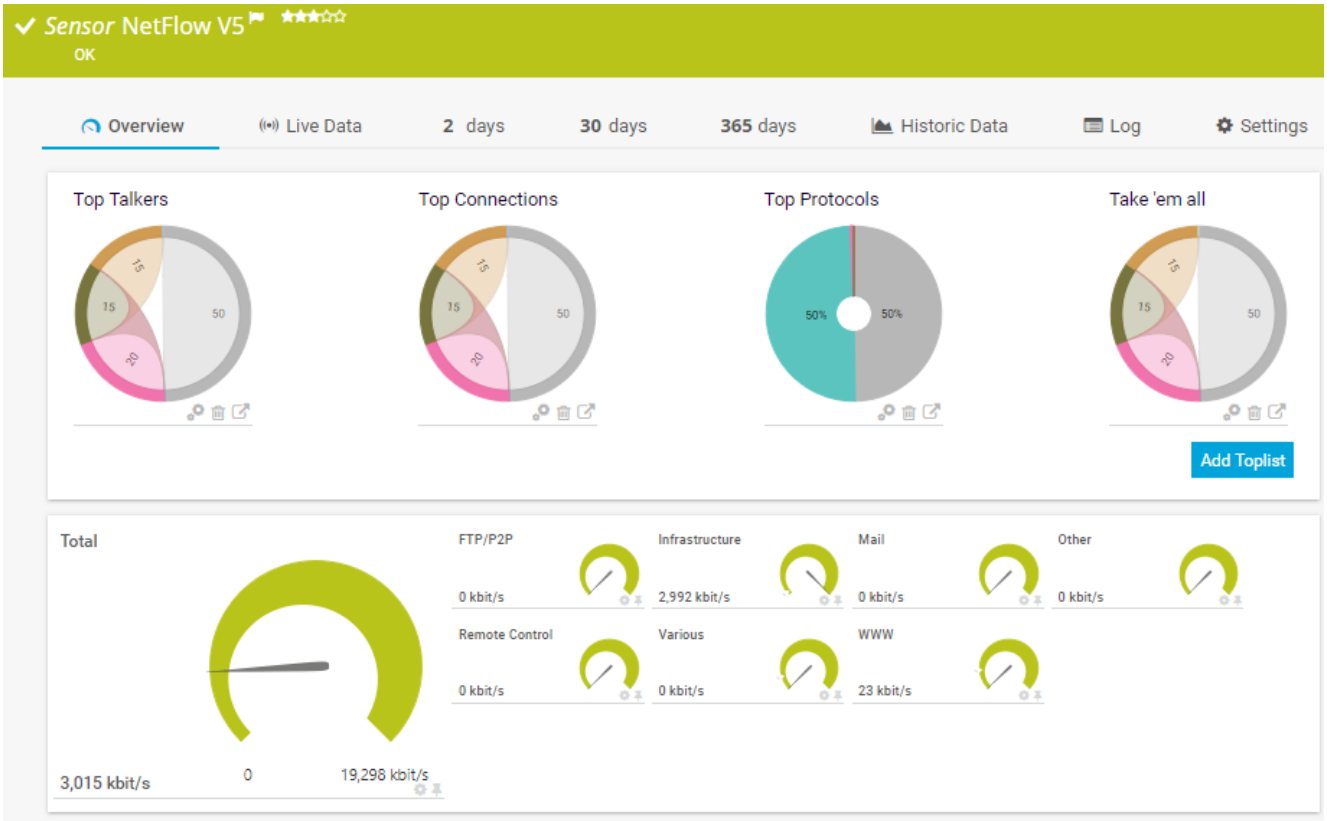



Рисунок 4.4 – датчики NetFlow v5

Щоразу, коли PRTG виявляє час простою, перезавантаження системи, порушення порогових значень (наприклад, заповнення вільного простору диска) або подібні ситуації, він може надсилати сповіщення. У сповіщеннях використовуються різні способи оповіщення про проблеми (наприклад, електронна

пошта, SMS, push-повідомлення тощо). Після створення шаблонів сповіщень у системних налаштуваннях їх можна вибрати у вкладці тригерів сповіщень зони моніторингу, груп пристроїв, датчиків, а також кореневої групи.

У налаштуваннях каналу датчика можна встановити обмеження для зміни стану датчика при порушенні певних меж. Таким чином, можна встановити датчик трафіку на стан Down (тобто відключений) , коли вимірюється значення пропускної здатності, яке вважається критичним.

У списку тривожних сигналів відображаються всі датчики, які перебувають у режимі Down, Warning або Unusual status. Це корисно для відстеження всіх порушень в мережевій системі.

У списку Logs відображається список з усіма подіями моніторингу. У типовому режимі виробляється величезна кількість даних цього журналу. Оскільки активність кожного об’єкту задокументовано, ці дані можна використовувати для точної перевірки даних системи.

### 4.3 Висновки до четвертого розділу

В даному розділі описано встановлення системи моніторингу Paessler PRTG. Описано основні елементи даної системи: кореневу групу, зони моніторингу, групування, пристрої, датчики та канали. Також описано налаштування пристроїв, тривожних сигналів та журнал змін.

# 5 ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Метою даного розділу є дослідження моніторингової системи для мережевих інформаційних процесів у локальній і глобальній мережах.

Щоб виконати оцінку економічної ефективності необхідно розрахувати трудомісткість реалізації проекту, витрати на оплату праці найманим працівникам, витрати апаратного і програмного забезпечення, амортизаційні відрахування, витрати енергоресурсів та інші витрати які є основними пунктами виконання обчислень, а також показники економічної ефективності розробки проекту.

## 5.1 Розрахунок норм часу на виконання науково-дослідної роботи

Розробка надійної і ефективної моніторингової системи вимагає значних затрат часу. Слід зауважити, що самі ж затрати напряму залежать від кваліфікації розробника та його професійних можливостей. Розробник системи та програмного забезпечення повинен у достатній мірі володіти навиками проектування та програмування, вміти адекватно та професійно використовувати математичні засоби та бути добре обізнаними з об’єктом дослідження.

Реалізація проекту моніторингової системи складається з низки послідовних та взаємопов’язаних етапів.

Кожен із етапів реалізації проекту характеризується метою та змістом, оцінкою часу виконання, кількістю та спеціалізацією виконавців, а також приблизною оцінкою вартості.

Для оцінки тривалості виконання окремих робіт використовуємо середній час виконання в годинах. Опираючись на досвід і нормативи, можемо сказати, що тривалість виконання операцій,  досить різна. В даному випадку, при досліджені моніторингової системи для мережевих інформаційних процесів у локальній і глобальній мережах, час операцій варіюється від 6 до 120 годин. Час виконання кожної операції приведений в таблиці 5.1.

Таблиця 5.1 – Операції технологічного процесу та їх час виконання

| № п/п | Назва операції (стадії) | Виконавець | Середній час виконання операції, год. |
|---|---|---|---|
| 1 | Постановка проблеми | Проектний менеджер | 6 |
| | | Інженер програміст | |
| 2 | Огляд існуючих рішень | Проектний менеджер | 8 |
| 3 | Аналіз сфери застосування | Інженер програміст | 8 |
| 4 | Збір потрібної інформації та її опрацювання | Інженер програміст | 11 |
| 5 | Створення технічного завдання | Інженер програміст | 20 |
| | | Проектний менеджер | |
| 6 | Проектування системи | Інженер програміст | 20 |
| 7 | Програмна реалізація системи | Інженер програміст | 120 |
| 8 | Тестування програмного продукту | Тестувальник | 30 |
| 9 | Створення документації | Інженер програміст | 25 |
| 10 | Заключна стадія | Інженер програміст | 8 |
| | | Проектний менеджер | |
| Всього | | | 256 |

В підсумку на реалізацію проекту моніторингової системи для мережевих інформаційних процесів у локальній і глобальній мережах необхідно 256 людино-годин, залучення трьох спеціалістів та виконання десяти різноманітних стадій реалізації проекту.

## 5.2 Розрахунок витрат на проведення НДР

Відповідно до Закону України «Про оплату праці» заробітна плата – це винагорода, обчислена, як правило, у грошовому виразі, яку за трудовим договором власник або уповноважений ним орган виплачує працівникові за виконану ним роботу.

Оплата праці залежить не тільки від результатів праці конкретного працівника, але також від результатів праці, прибутковості конкретного підприємства.

Основна заробітна плата нараховується за виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Згідно закону України «Про Державний бюджет України на 2020 рік», зокрема Статтею восьмою мінімальна заробітна плата у погодинному розмірі встановлена у розмірі 28,31 грн. Рекомендована тарифна ставка для проектного менеджера становить 96 грн./год., для інженера-програміста 137 грн/год., для тестувальника 68 грн/год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г, \tag{5.1}$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Оскільки всі види робіт виконує три спеціаліста, то основна заробітна плата буде розраховуватись за даною формулою:

$$З_{осн.} = (96 \cdot 25) + (137 \cdot 201) + (68 \cdot 30) = 31\ 977 \text{ грн.}$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \quad (5.2)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод} = 31\ 977\ \cdot 0{,}15 = 4\ 796{,}55 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.} \quad (5.3)$$

$$В_{о.п.} = 31\ 977\ + 4\ 796{,}55 = 36\ 773{,}55 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи:

– єдиний соціальний внесок ЄСВ (прибутковий податок) – 22%;

– військовий збір – 1,5%.

У сумі зазначені відрахування становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = Ф_{оп} \cdot 0{,}235 \quad (5.4)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$$В_{с.з.} = 36\ 773{,}55 \cdot 0{,}235 = 8\ 641{,}78 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці наведено у таблицю 5.2.

Таблиця 5.2 – Розрахунки витрат на оплату праці

| №з/п | Категорія працівників | Основна заробітна плата, грн. | | | Додаткова заробітна плата, грн. | Нарахув. на ФОП, грн. | Всього витрати на плату праці, грн. (6=3+4+5) |
|---|---|---|---|---|---|---|---|
| | | Тарифна ставка, | Кількість відпрацьованих | Фактично нарах. з/пл., грн. | | | |
| А | Б | 1 | 2 | 3 | 4 | 5 | 6 |
| 1. | Проектний менеджер | 96 | 25 | 2 400 | - | – | – |
| 2. | Інженер-програміст | 137 | 201 | 27 537 | - | – | – |
| 3. | Тестувальник | 68 | 30 | 2 040 | - | – | – |
| Всього | | | 256 | 31 977 | 4 796,55 | 8 641,78 | 45 415,33 |

З таблиці розрахунки витрат на оплату розробки моніторингової системи для мережевих інформаційних процесів у локальній і глобальній мережах видно, що всього витрати на оплату праці становить 45 415,33 грн.

### 5.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{ві} = q_i \cdot p_i \,, \qquad (5.5)$$

де: $q_i$– кількість витраченого матеріалу і–го виду; $p_i$ – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{вi}. \quad (5.6)$$

Розрахунки занесемо у таблицю 5.3.

Таблиця 5.3 – Розрахунки матеріальних витрат

| Найменування матеріальних ресурсів | Один. виміру | Норма витрат | Ціна за один., грн. | Затрати матер., грн. | Транспортно - заготівельні витрати, грн. | Загальна сума витрат на матер., грн. |
|---|---|---|---|---|---|---|
| 1. Основні матеріали | | | | | | |
| Місячна оплата межею Internet | грн | 199 | – | 199 | | 199 |
| Разом: | | | | | | 199 |

Згідно проведених розрахунків, матеріальні витрати становлять 199 грн.

## 5.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

$$З_в = W \cdot T \cdot S, \quad (5.7)$$

де $W$ – необхідна потужність, кВт; $T$ – кількість годин на реалізацію розробки; $S$ – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів. Отже, 1 кВт з ПДВ коштує 2,42 грн.

Потужність комп’ютера для створення моніторингової системи – 450 Вт, кількість годин роботи обладнання згідно таблиці 5.1 –256 годин.

Тоді,

$$З_в = 0{,}45 \cdot 256 \cdot 2{,}42 = 278{,}78 \text{ грн.}$$

Згідно формули затрати на електроенергію дорівнює 278,78грн.

### 5.5 Розрахунок суми амортизаційних відрахувань

Поняття "амортизація" або "амортизаційні відрахування" можна сформулювати як постійно накопичується в вартісному грошовому виразі знос основних засобів і нематеріальних активів для подальшого використання на реновацію, тобто на просте і розширене відтворення вартості відповідних активів.

Для визначення амортизаційних використовується формула:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \qquad (5.8)$$

де $A$ – амортизаційні відрахування за звітний період, грн.; $Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.; $Н_А$ – норма амортизації.

Комп’ютери та оргтехніка належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %).

Для даної роботи засобом розробки є комп’ютер. Його сума становить 25000 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 25000 \cdot 5\% / 100\% = 1250 \text{ грн.}$$

Оскільки робота виконувалась 256 годин, то амортизаційні відрахування будуть становити:

$$A = 1250 \cdot 256 / 100 = 3200 \text{ грн.}$$

Згідно формули для визначення амортизаційних, де $Б_В$ множиться $Н_А$ і ділиться на 100% амортизація розробки становить 3200 грн.

### 5.6 Обчислення накладних витрат

Накладні витрати пов’язані з обслуговуванням виробництва, утриманням апарату управління спілкою та створення необхідних умов праці. В залежності від організаційно-правової форми діяльності господарюючого суб’єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників.

$$Н_в = В_{о.п.} \cdot 0{,}2\ldots0{,}6\ , \qquad (5.9)$$

де $Н_в$ – накладні витрати.

Отже, накладні витрати:

$$Н_в = 36\ 773{,}55 \cdot 0{,}2 = 7\ 354{,}71 \text{ грн.}$$

Накладні витрати згідно розрахунку формули, становить 7 354,71 грн.

### 5.7 Складання кошторису витрат та визначення собівартості науково-дослідницької роботи

Результати проведених вище розрахунків зведемо у таблицю 5.4.

Таблиця 5.4 – Кошторис витрат на НДР

| Зміст витрат | Сума, грн. | В % до загальної суми |
|---|---|---|
| Витрати на оплату праці | 45 415,33 | 69,8 |
| Відрахування на соціальні заходи | 8 641,78 | 13,27 |
| Матеріальні витрати | 199 | 0,3 |
| Витрати на електроенергію | 278,78 | 0,42 |
| Амортизаційні відрахування | 3200 | 4,91 |
| Накладні витрати | 7 354,71 | 11,3 |
| Собівартість | 65 089,6 | 100,00 |

Собівартість ($С_в$) програмного продукту розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.з.} + З_{м.в.} + З_в + А + Н_в \text{ .} \qquad (5.10)$$

Отже, собівартість програмного продукту дорівнює:

Св = 45 415,33 + 8 641,78 + 199 + 278,78 + 3200 +7 354,71= 65 089,6 грн.

Загальний кошторис витрат та визначення собівартості науково-дослідницької роботи становить 65 089,6 грн.

## 5.8 Розрахунок ціни дослідження

Ціну науково-дослідної роботи можна визначити за формулою:

$$Ц = \frac{С_в \cdot (1 + Р_{рен}) + К \cdot В_{н.і.}}{К} \cdot (1 + ПДВ) \text{ ,} \qquad (5.11)$$

де $Р_{рен.}$ – рівень рентабельності, 30 %; $К$ – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних

систем); $В_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту); *ПДВ* – ставка податку на додану вартість, (20 %).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти К та Вн.і , оскільки їх в даному випадку не потрібно.

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_В \cdot (1 + Р_{рен}) \cdot (1 + ПДВ) \tag{5.12}$$

Звідси ціна на роботу складе:

$$Ц = 65\,089{,}6 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 101\,539{,}78 \text{ грн.}$$

Загальний розрахунок ціни дослідження становить 101 539,78 грн.

## 5.9 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

$$E_р = \frac{П}{C_В}, \tag{5.13}$$

де *П* – прибуток; $C_В$ – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_в \,. \tag{5.14}$$

Розраховуємо плановий прибуток:

$$П_{пл} = 101\ 539{,}78\ -\ 65\ 089{,}6\ = 36\ 450{,}18 \text{ грн.}$$

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_p = \frac{П_{пл}}{C_в}. \qquad (5.15)$$

Тоді,

$$E_p = 36\ 450{,}18 / 65\ 089{,}6\ = 0{,}56.$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень ($T_p$):

$$T_p = \frac{1}{E_p}\ , \qquad (5.16)$$

Термін окупності аналізу та створення інформаційної системи для дистанційного контролю мікроклімату житлових приміщень дорівнює:

$$T_p = 1 / 0{,}56 = 1{,}78 \text{ р.}$$

Згідно формул плановий прибуток від розробки становить 36 450,18 грн., економічна ефективність дорівнює 0,56 , а термін окупності становить 1,78 роки що вважається доцільним та економічно вигідним.

## 5.10 Висновки до п’ятого розділу

В розділі обґрунтування економічної ефективності було розраховано основні техніко-економічні показники при розробці програмного забезпечення для моніторингової системи мережевих інформаційних процесів у локальній і глобальній мережах.(див. таблиця 5.5).

Значення показника економічної ефективності становить 0,56 що є достатньо високим значенням, період окупності даної роботи становить 1,78 років, що є доцільним та економічно вигідним.

Таблиця 5.5 – Техніко-економічні показники науково-дослідної роботи

| №п/п | Показник | Значення |
|---|---|---|
| 1. | Собівартість, грн. | 65 089,6 |
| 2. | Плановий прибуток, грн. | 36 450,18 |
| 3. | Ціна, грн. | 101 539,78 |
| 4. | Економічна ефективність | 0,56 |
| 5. | Термін окупності, рік | 1,78 |

Отже, найбільша питома вага припадає на витрати для оплати заробітньої плати, а розрахунок електроенергії, амортизаційних відрахувань, затрати на матеріали є не значними. Тому усі ці показники значно підвищили економічну ефективність і термін окупності даної розробки. Система може бути реалізована та розвинена, оскільки вона є економічно вигідною по всіх основних технічних та економічних показниках.

# 6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

## 6.1 Значення охорони праці у роботі фахівців з комп'ютерних інформаційних технологій

Комп'ютерні технології вже давно є частиною нашого повсякденного життя, а норми роботи з ними добре вкоренилися в IT-компаніях, проте в нас на території України цей процес все ще триває, хоч і підходить до кінцевої завершальної стадії.

Звичайно, з першого погляду, робота за комп'ютером здається безпечною, але саме це зневажливе ставлення до неї може призвести до певних проблем для нашого здоров'я. Професія, яка вимагає сидячого, одноманітного положення, а отже програміста та інших фахівців IT-технологій пов'язана з колосальним розумовим напруженням. Розробники – це дуже зосереджені люди, навіть відволікаючись час від часу від роботи, вони продовжують думати про роботу. Нерідко відпочинком вони вважають заміну основної діяльності, наприклад, читання профільної літератури, верстку сайтів, вивчення нових мов програмування. Однак наший мозок не здатний до нескінченності сприймати виключно корисну інформацію, яку розробник прагне направляти в русло особистісного та професійного зростання.

Адже мозок людини не машина: він не може нескінченно зберігати і переробляти дані практично не втрачаючи продуктивності [26]. Людина програє ПЕОМ за багатьма показниками тому для підтримки її працездатності потрібно зовсім інші умови.

В наш час багато IT-компаній обладнують свої офіси кімнатами відпочинку та зонами відпочинку, в яких забезпечують психофізіологічну розгрузку працівників. Адже вже давно нікого не здивуєш окремим робочим столом з ноутбуком. Тому, бажаючи підвищити продуктивність працівників, міжнародні компанії змагаються, перетворюючи одноманітні та нудні офіси в креативні простори, де нові ідеї народжуються без неймовірних зусиль. Наприклад, деякі компанії створюють в офісі різноманітні декорації, іноді й казкові. Це може бути

гігантський гоночний трек, і пряниковий будиночок, і дуже реалістичний піратський корабель, на палубі якого розташувалися комп'ютерні столи, ніжками яких служать винні бочки. Робочі місця співробітників компанії Google в Цюріху нагадують гігантські вулики, а офіс шведського інтернет-провайдера Bahnhof розташувався в бомбосховищі часів холодної війни і походить на підземний притулок землян після глобальної катастрофи. А щоб співробітників не тягнуло додому, роботодавці створюють і можливість релаксувати, не відходячи від робочого місця, обладнавши басейни, ігрові кімнати та спортзали [27].

Можна цілий день просидіти біля монітора, а у вечорі відчути страшну втому, як від важкої фізичної праці. Однак це почуття помилкове і боротися з ним допоможе спорт. Відмінно бадьорить активний відпочинок, він розганяє кров, додає сил. Чимало програмістів відчувають потребу в активному відпочинку на підсвідомому рівні, вибираючи спорт як хобі для проведення вільного часу.

При цьому не варто забувати, що умови праці програмістів також характеризуються можливістю впливу на них наступних небезпечних і шкідливих виробничих факторів: шуму; тепловиділень, причому шкоди організму можуть завдати не тільки високі, але і низькі температури; іонізуючих і неіонізуючих випромінювань: рентгенівське, інфрачервоне, електромагнітне випромінювання ВЧ і СВЧ діапазону; статичної електрики; недостатнє штучне освітлення.

За таких умов зростає роль та значення охорони праці, як системи правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження здоров'я і працездатності людини в процесі праці. Адже в кінцевому рахунку плоди науково-технічного прогресу можуть бути ефективними лише в тій мірі, в якій вони забезпечують людині безпеку, комфортність і зручність трудової діяльності.

### 6.2 Охорона праці під час монтажу кабельних мереж

До виконання робіт з монтажу кабельних мереж допускаються робітники, які досягли 18 років та пройшли:

- медичний попередній огляд та визнані придатними виконувати монтажні роботи на висоті;

- навчання та перевірку знань з електробезпеки;

- навчання в закладах освіти для виконання робіт з підвищеною небезпекою за затвердженою програмою;

- спеціальне навчання та атестацію з питань пожежної безпеки;

- вступний інструктаж у службі охорони праці;

- первинний інструктаж безпосередньо на робочому місці.

Робітники повинні бути проінструктовані щодо розпорядку на робочому місці, порядку переміщення по території об'єкта, місце відпочинку під час технологічних та обідньої перерв, порядок закінчення роботи.

До початку робіт у комплексній бригаді проводиться первинний інструктаж з безпечного виконання робіт з основної та суміжних професій та ознайомлення з правилами надання першої допомоги.

Допущені мають виконувати тільки ті роботи, про безпечне виконання яких вони проінструктовані безпосередньо керівником.

Роботи на висоті (при підйомі над поверхнею вище, ніж 1,3 м) виконуються тільки з риштувань або помостів.

До початку робіт керівник зобов'язаний:

- перевірити ступінь готовності будівельних робіт;

- оцінити виробничі обставини, можливість взаємодії з іншими будівельно-монтажними організаціями у відповідності з проектом виконання робіт (ПВР); можливість безпечного застосування машин, механізмів, пристосувань, місця їх установки та порядок проїзду;

- узгодити з відповідними службами та, при необхідності, внести уточнення в ПВР.

- ознайомити працюючих з ПВР та технологічними картами на всі види робіт.

Керівник робіт повинен здійснити первинний інструктаж, який стосується:

- характеру та безпечних методів виконання робіт (у т.ч. за складних погодних умов); порядку проходів до кожного робочого місця;

- порядку розвантаження та складування матеріалів, устаткування та конструкцій;

- порядку і місця установки вантажних лебідок та інших механізмів у монтажній зоні; порядку роботи з гідропідйомників, риштувань, підмостків, драбин; наявності діючих електроустановок та заборонених зон;

- надання першої допомоги, виклику швидкої медичної допомоги, пожежної охорони, керівника робіт чи роботодавця, представника служби охорони праці.

Перевірити наявність та термін дії посвідчень з охорони праці, електро-пожежо-безпеки, посвідчень на право виконання спеціальних видів робіт. Видати наряд-допуск операторам на виконання робіт підвищеної небезпеки з проведенням цільового інструктажу та записом до журналу реєстрації інструктажів з питань охорони праці. Підписи інструкторів та інструктованих у журналі обов'язкові. Перевірити справність драбин. Вони повинні мати інвентарні номери, що відповідають реєстраційному обліку в журналі, а також тавро з датою наступного випробування.

Помости, риштування та площадки мостових кранів, які використовуються для монтажу силових та освітлювальних мереж, повинні мати по всьому периметру суцільні настили та захисну огорожу заввишки не менше 1,1 м.

Прокладання кабелів слід виконувати тільки в рукавицях.

Не дозволяється розміщувати кабель, барабан з кабелем та без нього, механізми, пристрої та інструменти безпосередньо біля бровки траншеї. Переміщувати барабан з кабелем слід після того, коли цвяхи із щік барабана вийнято, а кінці кабелю надійно закріплено. Перекочувати барабан з кабелем слід у напрямку стрілки, нанесеної фарбою на щоці барабана. Переміщувати барабан з кабелем вручну дозволяється тільки по твердому ґрунту або надійному настилу по горизонтальній поверхні на відстань не більше. Не дозволяється працюючим чи стороннім особам перебувати на шляху барабана, що переміщується. Під час

піднімання барабана необхідно слідкувати за тим, щоб не пошкодити щоки барабана та втулку.

Перед розмотуванням барабан встановити на. Підняти його на 0,15-0,20м над поверхнею землі, щоб барабан міг вільно. Барабан встановити так, щоб кабель розмотувався з його верхньої частини.

На трасах з поворотами робітники не повинні перебувати всередині кута повороту кабелю, а також підтримувати або відтягувати кабель руками.

Розміщення конструкцій і пристроїв для витягнення кабелю з барабана повинно бути таким, щоб забезпечити прохід робітника, який супроводжує кінець кабелю з тросом, без перепон і торкання раніше прокладених кабелів.

Під час виконання монтажних робіт на перетинах з автошляхами та інженерними мережами умови виконання робіт слід узгоджувати з їх власниками [28].

## 6.3 Організація оповіщення і зв'язку у надзвичайних ситуаціях техногенного та природного характеру.

Оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій організовується з урахуванням структури державного управління в Україні, максимально прогнозованого характеру і рівня надзвичайних ситуацій. Оповіщення може здійснюватися як централізовано, так і децентралізовано.

Оповіщення про загрозу або виникнення надзвичайних ситуацій забезпечується шляхом [24]:

1) функціонування загальнодержавної, територіальних, місцевих автоматизованих систем централізованого оповіщення про загрозу або виникнення надзвичайних ситуацій, спеціальних, локальних та об'єктових систем оповіщення;

2) централізованого використання телекомунікаційних мереж загального користування, у тому числі мобільного (рухомого) зв'язку, відомчих телекомунікаційних мереж і телекомунікаційних мереж суб'єктів господарювання в порядку, встановленому Кабінетом Міністрів України, а також мереж

загальнонаціонального, регіонального та місцевого радіомовлення і телебачення та інших технічних засобів передавання (відображення) інформації;

3) автоматизації процесу передачі сигналів і повідомлень про загрозу або виникнення надзвичайних ситуацій;

4) функціонування на об'єктах підвищеної небезпеки автоматизованих систем раннього виявлення надзвичайних ситуацій та оповіщення;

5) організаційно-технічної інтеграції різних систем централізованого оповіщення про загрозу або виникнення надзвичайних ситуацій та автоматизованих систем раннього виявлення надзвичайних ситуацій та оповіщення;

6) функціонування в населених пунктах, а також місцях масового перебування людей сигнально-гучномовних пристроїв та електронних інформаційних табло для передачі інформації з питань цивільного захисту.

Порядок організації оповіщення про загрозу або виникнення надзвичайних ситуацій та організації зв'язку у сфері цивільного захисту визначається положенням, яке затверджується Кабінетом Міністрів України захисту [24].

За рівнями системи оповіщення поділяються на загальнодержавну автоматизовану систему централізованого оповіщення, територіальні автоматизовані системи централізованого оповіщення, місцеві автоматизовані системи централізованого оповіщення, а також спеціальні, локальні та об'єктові системи оповіщення.

Методичне керівництво щодо створення та функціонування систем оповіщення всіх рівнів здійснюється ДСНС [25].

Загальнодержавна автоматизована система централізованого оповіщення функціонує на загальнодержавному рівні для оповіщення в автоматизованому режимі центральних і місцевих органів виконавчої влади, органів управління ДСНС та забезпечує доведення сигналів про загрозу виникнення або виникнення надзвичайних ситуацій загальнодержавного рівня та інформації з питань цивільного захисту.

Оповіщення та інформування центральних і місцевих органів виконавчої влади, органів управління ДСНС про загрозу виникнення або виникнення надзвичайних ситуацій здійснюється ДСНС через відповідну оперативно-чергову службу з використанням загальнодержавної автоматизованої системи централізованого оповіщення та системи автоматизованого виклику.

Утримання, реконструкція та підтримання у постійній готовності до використання за призначенням загальнодержавної автоматизованої системи централізованого оповіщення здійснюється ДСНС [25].

Спеціальні системи оповіщення створюються і функціонують:

- на атомних електростанціях;
- на гідротехнічних спорудах Дніпровського та Дністровського каскадів та в зонах їх можливого катастрофічного затоплення;
- на магістральних продуктопроводах.

Спеціальні системи оповіщення передбачають взаємодію з відповідними територіальними та місцевими автоматизованими системами централізованого оповіщення.

Проектування, створення (реконструкція) та забезпечення функціонування спеціальної системи оповіщення здійснюються на підставі рішення керівника об’єкта з її обов’язковою інтеграцією до відповідних територіальних та місцевих автоматизованих систем централізованого оповіщення [25].

Доведення сигналів, повідомлень про загрозу виникнення або виникнення надзвичайних ситуацій до населення, а також інформування здійснюється:

- через ПАТ “Національна суспільна телерадіокомпанія України”, державні і публічні телерадіокомпанії, комунальні, громадські та інші телерадіоорганізації незалежно від форми власності з використанням їх телемереж та мереж ефірного радіомовлення (із супроводженням інформації жестовою мовою та/або субтитруванням, якщо вона є голосовою, і аудіокоментуванням, якщо вона є візуальною);
- через операторів телекомунікацій із залученням телекомунікаційних мереж загального користування (телефонний зв’язок, текстові повідомлення);

- через Інтернет-ресурси (сайти, соціальні мережі).

Для передачі сигналів та повідомлень оповіщення використовуються сигнально-гучномовні пристрої, у тому числі встановлені на транспортних засобах, що залучаються для оповіщення, електронні інформаційні табло, електросирени та інші технічні засоби [25].

## 6.4 Забезпечення безпеки життєдіяльності при роботі з ПК.

Заходи щодо усунення небезпеки ураження електричним струмом зводяться до правильного розміщення устаткування та електричних кабелів. Інші заходи щодо забезпечення електробезпеки, збігаються з загальними заходами пожежо- та електробезпеки.

В якості профілактичних заходів для забезпечення пожежної безпеки слід використовувати скриту електромережу, надійні розетки з пожежобезпечних матеріалів, силові мережі живлення устаткування виконувати кабелями, розрахованими на підключення в 3-5 разів більшого навантаження, включати й виключати живлення обладнання за допомогою штатних вимикачів. Треба регулярно робити очистку внутрішніх частин комп'ютерів, іншого устаткування від пилу, розташовувати комп'ютери на окремих неспалюваних столах. Для запобігання іскріння необхідно рідше встромляти і виймати штепсельні вилки з розеток.

Екран дисплея повинен бути розташованим перпендикулярно до напрямку погляду. Якщо він розташований під кутом, то стає причиною сутулості. Відстань від дисплея до очей повинна трохи перевищувати звичну відстань між книгою та очима. Перед екраном монітора, особливо старих типів, повинен бути спеціальний захисний екран. При його відсутності треба сидіти на відстані витягнутої руки від монітора. Ще одним моментом, який стосується зору, є необхідність створення неоднорідного поля зору. Для цього можна розвісити на поверхнях (стінах) плакати та картини, виконані у спокійних тонах. Наприклад, пейзажі.

Важливою є форма спинки крісла, яка повинна повторювати форму спини. Висота крісла повинна бути такою, щоб користувач не почував тиску на куприк або стегна. Крісло бажано обладнати бильцями. Його потрібно встановити так, щоб не треба було тягтися до клавіатури. Періодично користувачу необхідно рухатися, вчасно змінювати положення тіла і робити перерви у роботі [23].

При напруженій роботі за комп'ютером щогодини необхідно робити перерву на 15 хвилин через кожну годину і треба займатися іншою справою. Декілька разів на годину бажано виконувати серію легких вправ для розслаблення.

Режим праці та відпочинку при роботі з персональною електронно-обчислювальною машиною (ПЕОМ) залежить від категорії трудової діяльності. Всі роботи з ПЕОМ ділять на три категорії. Перша - епізодичне зчитування і робота з інформацією не більше 2-х годин за 8-годинну робочу зміну. Друга - зчитування інформації або творча робота не більше 4-х годин за восьми годинну зміну. Третя - зчитування інформації або творча робота тривалістю більше 4-х годин за зміну.

Якщо у приміщенні експлуатується більше одного комп'ютера, то треба врахувати, що на користувача одного комп'ютера можуть впливати випромінювання від інших, в першу чергу бокових, а також і задньої стінки сусіднього дисплея. Тому необхідний захист спеціальними фільтрами і щоб користувач розміщався від бічних і задніх стінок інших дисплеїв на відстані не ближче одного метра [23].

Отже, щоб запобігти негативним впливам необхідно знати й небезпечні сторони самого комп'ютера і правила безпечної роботи, знати засоби запобігання небезпек.

### 6.5 Висновки до шостого розділу

В даному розділі було розглянуто теми охорони праці, такі як: охорона праці під час монтажу кабельних мереж та значення охорони праці у роботі фахівців з інформаційних технологій. Засвоєні знання для подальшого використання у

монтажі кабельних мереж. А також усвідомлення ролі охорони праці як заходи та засоби спрямовані на збереження здоров’я і працездатності людини.

Також в даному розділі було розглянуто такі актуальні теми безпеки в надзвичайних ситуаціях такі, як: організація оповіщення і зв’язку у надзвичайних ситуаціях техногенного та природного характеру та забезпечення безпеки життєдіяльності при роботі з персональним комп’ютером. Отримано знання, які допоможуть в забезпечені зв’язку та розумінні оповіщень при надзвичайних ситуаціях різного характеру. Також були отримані знання про небезпеку спричинену різного роду заняттям з персональним комп’ютером.

# 7 ЕКОЛОГІЯ

## 7.1 Роль науково-технічного прогресу в забезпеченні якісного стану довкілля

Розвиток науки і техніки є однією з найважливіших умов для досягнення людством високого рівня розвитку цивілізації. Особливо гострою є проблема співвідношення науково-технічного прогресу і збереження довкілля, яке є єдино можливим середовищем життя людини. На сьогодні виділяють чотири головні чинники впливу науково-технічного прогресу на навколишнє природне середовище: збільшення населення земної кулі, скорочення природних мінеральних і паливних ресурсів, бурхливе зростання промислового виробництва та глобальне забруднення навколишнього природного середовища.

Екологічна діяльність є однією із основних складових будь-якої сфери народного господарства - сільське господарство, промислове виробництво, транспорт, військова діяльність тощо. Усі ці напрями діяльності зводяться до використання природних чи людських ресурсів, тобто відбувається втручання у процеси життєдіяльності біосфери. У зв’язку з цим об’єкт дослідження екології як науки про довкілля, особливо в даний час, включає в себе дослідження нових взаємозв’язків живих і неживих компонентів екосистеми, які проявляються під впливом природних і антропогенних факторів та суттєво впливають на функціонування екосистеми біосфери [29].

Вплив науково-технічного прогресу на стан навколишнього природного середовища не є однозначним, тобто завдяки його досягненням може посилюватись або зменшуватись техногенний антропогенний тиск на довкілля. Проте, на сьогоднішній день, негативні наслідки від використання досягнень науково-технічного прогресу переважають позитивні. З його розвитком людина отримала можливість значно впливати на навколишнє середовище, втручатися у природні процеси, кругообіг речовин та енергії, структури екосистем, що призвело до глобальної екологічної кризи на нашій планеті, оскільки підвищення обсягів

виробництва, різноманітності створюваної продукції та їх споживчих якостей на основі досягнень наукового прогресу відбулось при майже повному ігноруванні екологічного імперативу [31].

Основними джерелами антропогенного забруднення навколишнього середовища являються: ТЕС, АЕС, ГЕС, тисячі котельних, промислові об'єкти, військова промисловість, усі види транспорту, гірниче виробництво. Першоджерелом і першопричиною глобального розвитку екологічної кризи є демографічний вибух, який супроводжується збільшенням темпів використання і скорочення обсягів природних ресурсів, нагромадження величезної кількості відходів виробництва і побуту.

Найчастіше, наслідки науково-технічного прогресу найяскравіше проявляються відносно земельних ресурсів. Завдяки розвитку техніки людина отримала можливість зрошувати й осушувати великі земельні площі з метою сільськогосподарського використання, будувати канали та водосховища для більш раціональної організації території та ефективного використання земельних ресурсів. Проте гідромеліорація земель, використання засобів хімічного захисту рослин, надмірне застосування мінеральних добрив, що здійснювались без всебічного врахування їх впливу на ґрунтовий покрив, призвели до того, що високопродуктивні сільськогосподарські угіддя перетворились на малопродуктивні [31].

Розвивати техніку та виробництво без негативних наслідків для навколишнього середовища, зробити науково-технічний прогрес не тільки безпечним, але й сприятливим для природи, можливо вже в теперішній час, якщо принципи сталого розвитку посядуть належне місце в суспільній свідомості, дешевизна та прибуток не будуть самоціллю виробничої діяльності, а економічний механізм буде заохочувати науковців, підприємців, інженерно-технічних працівників та виробників до створення та впровадження екологічно безпечних, ресурсозберігаючих, мало- і безвідходних технологій, залучення нетрадиційних джерел енергії та продовольства [31].

Зарубіжні країни накопичують значний досвід використання адміністративно-правових та економічних інструментів регулювання природокористування і охорони навколишнього середовища. При цьому найкращого інструменту екологічного регулювання не існує, кожен з них спрямований на вирішення конкретних завдань і в певних випадках є більш доцільним, ніж інший.

В Україні існуючий механізм управління в екологічній сфері можна віднести до м'якого типу, який має за мету, в основному, боротьбу з негативними екологічними наслідками, а не з причинами виникнення екологічних деструктивних впливів [30].

Якщо проаналізувати, скільки зусиль інститутів спрямовано на те, щоб вирвати в природи її багатства, а скільки на встановлення меж «дозволеного» впливу на природу, то стає цілком очевидно, що таке порівняння далеко не на користь справі охорони навколишнього природного середовища [29].

Орієнтація на збереження природи має стати головним напрямом в науці. У зв’язку з цим наука повинна стати засобом екологічної безпеки, вирішувати екологічні проблеми, і бути не лише «виробничою силою», а мати більш вагоме значення [29].

## 7.2 Класифікація показників екологічності виробництва

Загальна класифікація еколого-економічних показників з метою оцінки й аналізу екологічності виробництва (ЕВ) у промисловості можу бути подана за такими ознаками: за змістом, за рівнем визначення, за часовим інтервалом, за об’єктом оцінки, за характером використання.

За змістом еколого-економічних показників [32]:

- Натуральні – показники екологічності (екобезпечності) технологічних процесів, техніки (включаючи природоохоронне устаткування), виробничо-господарської діяльності в цілому та її окремих складових. Наприклад, ступінь очищення промислових викидів, комплексність використання сировини (ресурсна

ефективність виробництва), обсяги викидів (скидів) шкідливих речовин у навколишнє середовище та інші;

- Натурально-вартісні – еколого-економічний збиток у розрахунку на одиницю товарної продукції в натуральному вираженні, збиткоємність маси викиду (скиду), екологічний результат у розрахунку на одну гривню капітальних вкладень;
- Вартісні – розмір економічного збитку в розрахунку на одиницю продукції у вартісному вираженні, повні екологічні витрати виробництва, екологічні платежі за забруднення довкілля;
- Локальні – показники вимірюють окремий параметр ЕЕРВ і можуть бути основою формування інтегральних показників, а також використовуватися для аналізу впливу екологічних чинників (показників) на узагальнюючі результати виробничо-господарської діяльності;
- Узагальнюючі – показники є головною, підсумковою і регулюючою оцінкою еколого-економічної ефективності технологічних процесів, забезпеченості підприємства природоохоронними фондами, рівня впливу виробництва на навколишнє природне середовище.

За рівнем визначення:

- Народногосподарський рівень – аналізуються макроекономічні показники екологічної спрямованості;
- Галузевий рівень – галузь розглядається в основному як сукупність підприємств, які об’єднуються за схожими характерними організаційно-технічними ознаками, оскільки сьогодні в основному відсутній дієвий галузевий організаційно-адміністративний розподіл матеріального виробництв:
- Регіональний рівень – область, район;
- Мікрорівень – підприємство;
- Рівень внутрішньовиробничих підрозділів підприємств.

За часовим інтервалом поділяються на: ретроспективні; поточні; фактичні; оперативні; прогнозні; планові.

За об’єктом оцінки:

- Виробництво в цілому, окремі етапи відтворювальних процесів (виробничо-технологічні, переробні, організаційні, природоохоронні, ресурсозбережні та інші);
- Виробництво конкретних видів продукції (послуг):
- Види (складові) виробничо-господарської діяльності підприємств (виробнича, інвестиційна та інші).

За характером використання:

- Регулюючі (дієві) – це показники, що безпосередньо застосовуються в процесі регулювання (управління) екологічності виробництва і якості навколишнього середовища, а також стану екосистем у процесі використання;
- Індикаторні – показники, за допомогою яких може здійснюватися узагальнююча характеристика ЕВ у процесі аналізу;
- Допоміжні показники забезпечують розрахунок комплексних, узагальнюючих еколого-економічних показників; можуть відігравати допоміжну роль при прийнятті складних, управлінських рішень [32].

Дані п’ять показників належать до екологічності виробництва.

## 7.3 Висновки до сьомого розділу

В даному розділі було розглянуто актуальні теми екології, такі як: роль науково-технічного прогресу в забезпеченні якісного стану довкілля та класифікація показників екологічності виробництва. Еколого-економічний аналіз грунтується на системі показників та інформації, необхідних для прийняття оптимальних управлінських рішень у сфері раціоналізації природокористування й охорони навколишнього середовища, екологізації та екологічності виробництва.

# ВИСНОВКИ

Під час виконання дипломної роботи було проаналізовано середовища моніторингу та його основні завдання, методи та засоби аналізу мережі. Описано основні особливості та відмінності глобальної та локальної мережі. Проаналізовано різні типи моніторингу мережі.

Здійснено порівняння існуючих систем мережевого моніторингу та досліджено позитивні сторони і недоліки даних систем. Проведено порівняльну характеристику систем моніторингу та їх особливості, на основі якої було вибрано досліджувану моніторингову систему для мережі та її пристроїв.

Розроблено розгортання системи моніторингу на центральному вузлі підприємства. Проаналізовано основні елементи системи моніторингу Paessler PRTG для подальшого налаштування і роботи з системою.

Розгорнуто моніторинг на системі серверів. Проведено тестування та налаштування пристроїв в мережі. Проаналізовано експлуатаційні показники мережі та системи серверів, що дало можливість удосконалити мережу для покращення її швидкості та якості.

Проаналізовано показники економічної ефективності, розраховано норми часу, матеріальні витрати та суми амортизаційних відрахувань. Обчислено накладні витрати та складено кошторис собівартості і розраховано ціну дослідження.

Обгрунтовано значення охорони праці у роботі з комп’ютерними технологіями та під час монтажу кабельних мереж. Проаналізовано організацію оповіщення і зв’язку у надзвичайних ситуаціях техногенного і природного характеру.

Проаналізовано роль науково-технічного прогресу в забезпечені якісного стану довкілля та класифікацію показників екологічності виробництва.

# ПЕРЕЛІК ПОСИЛАНЬ


1. Локальні і глобальні мережі [Електронний ресурс] – Режим доступу до ресурсу: http://matveev.kiev.ua/archnet/glava1/004.htm.

2. МОНІТОРИНГ ОБ‘ЄКТІВ В УМОВАХ АПРІОРНОЇ НЕВИЗНАЧЕНОСТІ ДЖЕРЕЛ ІНФОРМАЦІЇ / [Ю. Я. Бобало, Ю. Г. Даник, Л. О. Комарова та ін.]. – ЛЬВІВ, 2015. – 360 с.

3. Adato L. Networt Monitoring for Dummies, SolarWindws Special Edition / L. Adato, K. Yang, B. Hale., 2016. – (Brought to you by Solarwindws)

4. Засоби моніторингу та аналізу мережі [Електронний ресурс]. - https://wiki.cuspu.edu.ua/index.php/Засоби_моніторингу_та_аналізу_мережі,

5. Інформаційна технологія моніторингу та аналізу трафіку у комп’ютерних мережах [Електронний ресурс] / В. Кордяк, І. Дронюк, О. Федевич // Вісник Національного університету "Львівська політехніка". Комп’ютерні науки та інформаційні технології.. – 2015. - С. 35-42. – Режим доступу до ресурсу: http://nbuv.gov.ua/UJRN/VNULPKNIT_2015_826_8.

6. SNMP Operations [Електронний ресурс] – Режим доступу до ресурсу: https://docstore.mik.ua/orelly/networking_2ndEd/snmp/ch02_06.htm.

7. RMON: Remote Monitoring MIBs (RMON1 and RMON2)" [Електронний ресурс] – Режим доступу до ресурсу: http://www.networkdictionary.com/protocols/rmon.php?PHPSESSID=677dddf6927ec036f62817f8c29dc5ea.

8. NetFlow Services Solutions Guide, 1992-2006 [Електронний ресурс] – Режим доступу до ресурсу: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html

9. Чунарьова А. В. СУЧАСНІ ЗАСОБИ МОНІТОРИНГУ ІНФОРМАЦІЙНИХ ПОТОКІВ ІКСМ [Електронний ресурс] / А. В. Чунарьова, К. П. Сластенко, А. В. Чунарьов // Національний авіаційний університет (НАУ), Україна – Режим доступу до ресурсу: http://www.rusnauka.com/35_OINBG_2012/Informatica/4_123050.doc.htm.

10. A summary of Network Traffic monitoring and analysis techniques [Електронний ресурс] – Режим доступу до ресурсу: https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring/index.html#refs.

11. Algebra-Based Scalable Overlay Network Monitoring: Algorithms, Evaluation, and Applications. IEEE/ACM Transactions on Networking / Y.Chen, D. Bindel, R. Katz, H. Song., 2007

12. Shamsi J. PRINCIPLES OF NETWORK MONITORING / J. Shamsi, M. Brocmeyer. – Detroit, MI 48202, USA: Department of Computer Science, Wayne State University. – 40 с. – (Chapter 1).

13. Adato L. Monitoring 101 / Leon Adato.. – 25 с.

14. Wong E. Network Monitoring Fundamentals and Standarts / Edmund Wong.

15. Stallings W. SNMP, SNMPv2, and RMON Practical Network Management, Second Edition / William Stallings., 1996.

16. Уилсон Е. Мониторинг и анализ сетей. Методи виявления неисправностей / Ед Уилсон.. – 364 с.

17. Пасічник О. О. Класифікаційні ознаки об'єктів інформаційно-моніторингових систем на основі моделі OSI / О. О. Пасічник, О. І. Бурба. – 2015. – С. 116–118.

18. Гузій М. М. Аналіз моніторингу комп'ютерних мереж / М. М. Гузій, О. В. Станіславова, М. В. Кадет. – С. 1-5.

19. Remote Network Monitoring (RMON) [Електронний ресурс] – Режим доступу до ресурсу: https://networkencyclopedia.com/remote-network-monitoring-rmon/.

20. Best Network Monitoring Tools & Software of 2020 [Електронний ресурс] – Режим доступу до ресурсу: https://www.pcwdld.com/best-network-monitoring-tools-and-software.

21. Network Monitoring Basics [Електронний ресурс] – Режим доступу до ресурсу: https://www.comparitech.com/net-admin/network-monitoring-basics/.

22. Ultimate Guide to Network Monitoring [Електронний ресурс] – Режим доступу до ресурсу: https://www.dnsstuff.com/network-monitoring.

23. Мягченко О. П. Безпека життєдіяльності людини та суспільства : навчальний посібник / О. П. Мягченко. – Київ : Центр учбової літератури, 2010. – 384 с.

24. КОДЕКС ЦИВІЛЬНОГО ЗАХИСТУ УКРАЇНИ [Електронний ресурс] // Верховна рада України. – 204. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/5403-17.

25. Про затвердження Положення про організацію оповіщення про загрозу виникнення або виникнення надзвичайних ситуацій та зв'язку у сфері цивільного захисту [Електронний ресурс] // Постанова Кабінету Міністрів України №733. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/733-2017-%D0%BF.

26. Кальянов А. В. Психология безопасности труда / А. В. Кальянов., 2008. – 32 с. – (Донецкий областной совет профсоюза).

27. Конспект лекцій з курсу «Охорона праці в галузі» / Укладачі: Яскілка В.Я., Олійник М.З. –Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. –56 с.

28. ДНАОП. Інструкція з охорони праці під час монтажу кабельних мереж. [Електронний ресурс] – Режим доступу до ресурсу: https://dnaop.com/html/31931/doc-instrukcijaz-ohoroni-pracipid-chas-montazhu-kabelynih-merezh.

29. Дубовий О.В. Особливості екологічної культури в епоху науково-технічного прогресу [Електронний ресурс] / О.В. Дубовий. – Режим доступу: https://journal-knukim.com.ua/index.php/camw/article/viewFile/12/144.

30. Логачова О. В. Механізми регулювання антропогенних викидів парникових газів: автореф. дис. на здобуття ступеня канд. екон. наук: спец. 08.00.06 "Економіка природокористування та охорони навколишнього середовища" / О.В. Логачова. – Донецьк, 2008. – 21 с.

31. Суханова Е.Т. Економічні аспекти екологізації розвитку продовольчого комплексу регіону. – Ірпінь: Академія державної податкової служби України, 2002. – 77 с.

32. Тарасова В.В. Екологічна статистика.[Текст]/В.В.Тарасова.-Київ: «Центр учбової літератури», 2008 ро.-391с.

33. RMON 1 and RMON 2 MIBs [Електронний ресурс] – Режим доступу до ресурсу: http://etutorials.org/Networking/network+management /Part+II+Implementations+on+the+Cisco+Devices/Chapter+5.+RMON/RMON+1+and +RMON+2+MIBs/.

34. History of SNMP [Електронний ресурс] – Режим доступу до ресурсу: http://net-snmp.sourceforge.net/about/history.html.

35. История создания SNMP [Електронний ресурс] – Режим доступу до ресурсу: http://citforum.ru/internet/articles/art_10.shtml.

36. Nagios vs. Zabbix vs. PRTG vs. Spiceworks vs. Solarwinds Network Performance Monitor [Електронний ресурс] – Режим доступу до ресурсу: https://www.itcentralstation.com/product_reviews/zabbix-review-32935-by-it_user174738.

37. Back to Basics: What Is Network Monitoring? [Електронний ресурс] – Режим доступу до ресурсу: https://www.blackstratus.com/back-basics-network-monitoring/.

38. Network Monitoring and Measurements : Techniques and Experience [Електронний ресурс] – Режим доступу до ресурсу: http://www.netmode.ntua.gr/~csiat/Network-Measurement-And-Monitoring.pdf.

39. Introduction to Cisco IOS® NetFlow [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.pdf.

40. Using NetFlow/IPFIX for Network Management [Електронний ресурс] / [A. Pras, E. Sansre, A. Sperotto та ін.] // Springer Science+Business Media. – 2009.

41. Cisco Netflow Collection Engine [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html#wp1030039.

42. Basics of Network Monitoring [Електронний ресурс] – Режим доступу до ресурсу: https://www.manageengine.com/network-monitoring/basics-of-network-monitoring.html.

43. PRTG Network Monitor Manual [Електронний ресурс] – Режим доступу до ресурсу: https://www.paessler.com/manuals/prtg.

44. Nagios XI Documentation [Електронний ресурс] – Режим доступу до ресурсу: https://library.nagios.com/library/products/nagios-xi/documentation/?__hstc=118811158.149dbc5e2f99501d505bf920ab4bafa1.1589270940996.1589270940996.1589270940996.1&__hssc=118811158.1.1589270940997&__hsfp=2086609855.

45. Do You Understand SNMPv1, SNMPv2c, and SNMPv3? [Електронний ресурс] – Режим доступу до ресурсу: https://www.dpstele.com/snmp/v1-v2c-v3-difference.php.

46. A Winning Strategy in RMON vs. SNMP [Електронний ресурс] – Режим доступу до ресурсу: https://www.solarwindsmsp.com/content/rmon-vs-snmp.

47. Mikki M. NetworkMonitoring System (NMS) / M. Mikki, A. AbuSamra, A. Bader. // International Journal for Research in Applied Science & Engineering Technology. – 2017.

48. Network Monitoring: Everything you need to know [Електронний ресурс] – Режим доступу до ресурсу: https://www.opsview.com/resources/network/blog/network-monitoring-everything-you-need-know.

49. Стеблик В. А. Мережевий моніторинг як засіб аналізу інформаційних процесів у локальній і глобальній мережі / В. А. Стеблик, У. В. Поливана. // VII науково-технічна конференція «Інформаційні моделі, системи та технології».. – 2019.

50. Стеблик В. А. Розвиток мережевих технологій та їх вплив на навчання студентів комп’ютерних спеціальностей / В. А. Стеблик. // 52. Міжнародна наукова інтернет-конференція на тему "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення". – 2020. – №48.

# ДОДАТКИ

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ**
**ІМЕНІ ІВАНА ПУЛЮЯ**

**М А Т Е Р І А Л И**

**VII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ**

# «ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ »


**11–12 грудня 2019 року**

**ТЕРНОПІЛЬ**
**2019**

УДК 004.415.5
**В. Стеблик, У. Поливана**
Тернопільський національний технічний університет імені Івана Пулюя

## МЕРЕЖЕВИЙ МОНІТОРИНГ ЯК ЗАСІБ АНАЛІЗУ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ У ЛОКАЛЬНІЙ І ГЛОБАЛЬНІЙ МЕРЕЖІ

UDC 004.415.5
**V. Steblyk, U. Polyvana**
(Ternopil Ivan Puluj National Technical University, Ukraine)

## NETWORK MONITORING AS A WAY TO ANALYZE INFORMATION PROCESSES IN LOCAL AND GLOBAL NETWORK

Мережевий моніторинг в інформаційній структурі охоплює малі компанії та великі дата-центри. Моніторинг використовується, щоб системні адміністратори могли розрахувати спожитий трафік, стан безпеки мережі, а також були сповіщені про поломки та проблеми в інфраструктурі.

Раніше роль моніторингу здійснювали системні адміністратори, а інформацію про стан систем зберігались в неспеціалізованих програмах, або взагалі не зберігались. Практичний досвід роботи був єдиною інформацією про дану систему.

В теперішній час появилась велика кількість спеціалізованих систем моніторингу, які аналізують стан, оцінюють, збирають інформацію, а також обробляють її при необхідності.

Основною задачею системи моніторингу є представлення актуальної інформації для аналізу стану IT-інфраструктури і швидкого знаходження неполадок та їх оперативне усунення. Системи моніторингу дозволяють вчасно помітити зменшення продуктивності, відслідковувати дії користувачів в локальній комп'ютерній мережі та трафік з глобальної мережі. Постійний моніторинг дозволяє запобігти простою в роботі, підтримувати всі сервіси в активному робочому стані та дає можливість модернізації для покращення рівня якості. При виникненні проблеми в мережі відбувається надходження сповіщень-розсилок певним спеціалістам.

При відсутньому зв'язку з вузлом або елементом мережі, може використовуватись один з трьох типів систем моніторингу:

Базові системи моніторингу зазвичай працюють з протоколом ICMP. Стан елементів мережі проводиться періодично. Надається інформація про доступ та час відповіді.

Розширені системи моніторингу використовують протоколи, такі як SNMP, CDP, SSH. Завдяки їм, системи можуть отримувати практично всю інформацію про пристрої в мережі.

Системи моніторингу з активним контролем мають можливість керувати мережевими пристроями. За допомогою автоматичних сценаріїв, в цих системах можна побудувати алгоритм певних подій процедури.

При виборі, розробці чи розгортанні систем моніторингу спочатку потрібно визначити які об'єкти будуть відслідковуватись, а також критичні події і показники, які будуть надходити в сповіщеннях.

**Літератури**

1. Network Monitoring Fundamentals and Standards – [Електронний ресурс]. – Режим доступу: https://www.cse.wustl.edu/~jain/cis788-97/ftp/net_monitoring.pdf
2. Класифікаційні ознаки об'єктів інформаційно-моніторингових систем на основі моделі OSI – [Електронний ресурс]. – Режим доступу: http://stratcom.co.ua/klasifikatsijni-oznaki-ob-yektiv-informatsijno-monitoringovih-sistem-na-osnovi-modeli-osi/
3. Т. Лобур, О. Мацюк, Ю. Шилінська-Лобур Аналіз моніторингу трафіку в комп'ютерних мережах – [Електронний ресурс] – Режим доступу: http://elartu.tntu.edu.ua/handle/123456789/7840

Додаток Б

Архів конференцій >

## 2020/48 - 12 травня 2020 р.

# Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення"(випуск 48)

Перелік секцій, авторів і тем їх доповідей

Відображається 58 елементів

| Назва секції | Автор (автори) | Тема доповіді |
|---|---|---|
| Сортувати | Сортувати | Сортувати |
| 1. Інформаційні системи і технології | Яскевич С.С. | Дослідження систем контролю доступу до автомобіля |
| 1. Інформаційні системи і технології | Якимець В.С., Карпенко Ю.О. | Модернізація системи деканату |
| 1. Інформаційні системи і технології | Юрчишин В.М. | Проблеми підготовки спеціалістів вищої кваліфікації в області інформаційних технологій. |
| 1. Інформаційні системи і технології | Чуприна А.С., Руденко Д.Б. | Дослідження властивостей графових баз даних для вирішення транспортних задач |
| 1. Інформаційні системи і технології | Чемерис М.М. | Застосування кластерного аналізу в роботі web-сервісу обліку і планування громадських проєктів міста |
| 2. Економічні науки | Цуркан І.М., Савчук Д.Р. | Управління фінансовими результатами страхової компанії |
| 1. Інформаційні системи і технології | Терещенкова О.В., Стрелковская Л.А. | Использование видеоуроков для формирования компетенций судоводителей |
| 1. Інформаційні системи і технології | Таламанова І.С. | Огляд існуючих методів для прогнозування забруднення повітря |
| 1. Інформаційні системи і технології | Стеблик В.А. | Розвиток мережевих технологій та їх вплив на навчання студентів комп'ютерних спеціальностей |

***Стеблик В.А.***

*Тернопільський національний технічний університет імені Івана Пулюя, м. Тернопіль*

*Кафедра комп'ютерних наук, студент*

## РОЗВИТОК МЕРЕЖЕВИХ ТЕХНОЛОГІЙ ТА ЇХ ВПЛИВ НА НАВЧАННЯ СТУДЕНТІВ КОМП'ЮТЕРНИХ СПЕЦІАЛЬНОСТЕЙ

Швидкий та динамічний розвиток в галузі комп'ютерних мереж знайшов вплив у змінні значення комп'ютерної мережі. На початку свого розвитку мережі підключалися між обчислювальними машинами для комутації вузлів. При включені в мережі комп'ютерів, що підтримували сервіси обчислення інформації, під значенням комп'ютерної мережі почали розуміти всі технічні засоби, організаційні структури та програмне забезпечення, які утворюють спільну роботу усіх елементів системи та їх використання територіально розділеними користувачами.

Необхідно зазначити, що в наш час активно розвиваються технології локальних мереж, мобільні, бездротові та оптоволоконні мережі. Тому ці мережі потребують для свого обслуговування висококваліфікованих спеціалістів. Для підготовки даних спеціалістів потрібна якісна та повноцінна професійно-технічна освіта.

Результати наукових досліджень в галузі мережевих технологій з метою вдосконалення теоретичного матеріалу, можна розділити на декілька напрямів:

1. Обумовлення змісту матеріалів програмними засобами мережі;
2. Вибір однієї мережевої технології та комп'ютерної мережі, для взяття за основу та удосконалення її змісту;
3. Удосконалення змісту на основі виділення окремого елементу мережевої технології, а саме програмі засоби, принципи маршрутизації, апаратні засоби глобальних чи локальних мереж та інші;
4. Виділення одного із стеку протоколів як основного для подальшого удосконалення змісту матеріалів.

Відмінність цих напрямів лежить у цілях навчання мережевих технологій.

Проаналізувавши перший напрям, ми можемо зробити висновок, що він дозволяє підготувати студентів до використання конкретних програмних засобів, з метою облегшення керування та роботі з мережами, але цілями навчання майбутніх інженерів передбачає формування вмінь та знань у сучасних умовах, без використання спеціалізованого забезпечення.

Другий напрям дозволяє вивчити мережеві технології окремо згідно з наведеною класифікацією, при чому виникає проблема відповідності класифікацій під сучасні вимоги. Тому що мережі змінюються, а технології старіють і замінюються сучасними.

В досліджені третього напряму передбачається виділення окремого елементу технології, згідно якого розглядаються і інші. Це не є ефективним підходом для підготовки, тому що він позбавляє студентів можливості у розвитку та можливості у повній мірі досягти цілей навчання.

У четвертому напрямі спираються на один із стеку протоколів. Хоча він дозволяє повноцінно орієнтуватися в різноманітних технологіях глобальних чи локальних мережах, даний підхід не повинен обмежуватись лише одним відомим стеком протоколів.

В результаті можна стверджувати, що підготовку теоретичного та практичного матеріалу доцільно акцентувати увагу на використання різноманітних стеків протоколів, проектування мереж на основі різних технологій та створення єдиного інформаційного простору.

Література:

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учеб. пособ. для студентов / В. Г. Олифер, Н. А. Олифер. – 2. изд. – М. [и др.] : Питер, 2003. – 863 с. – (Учебник для вузов).

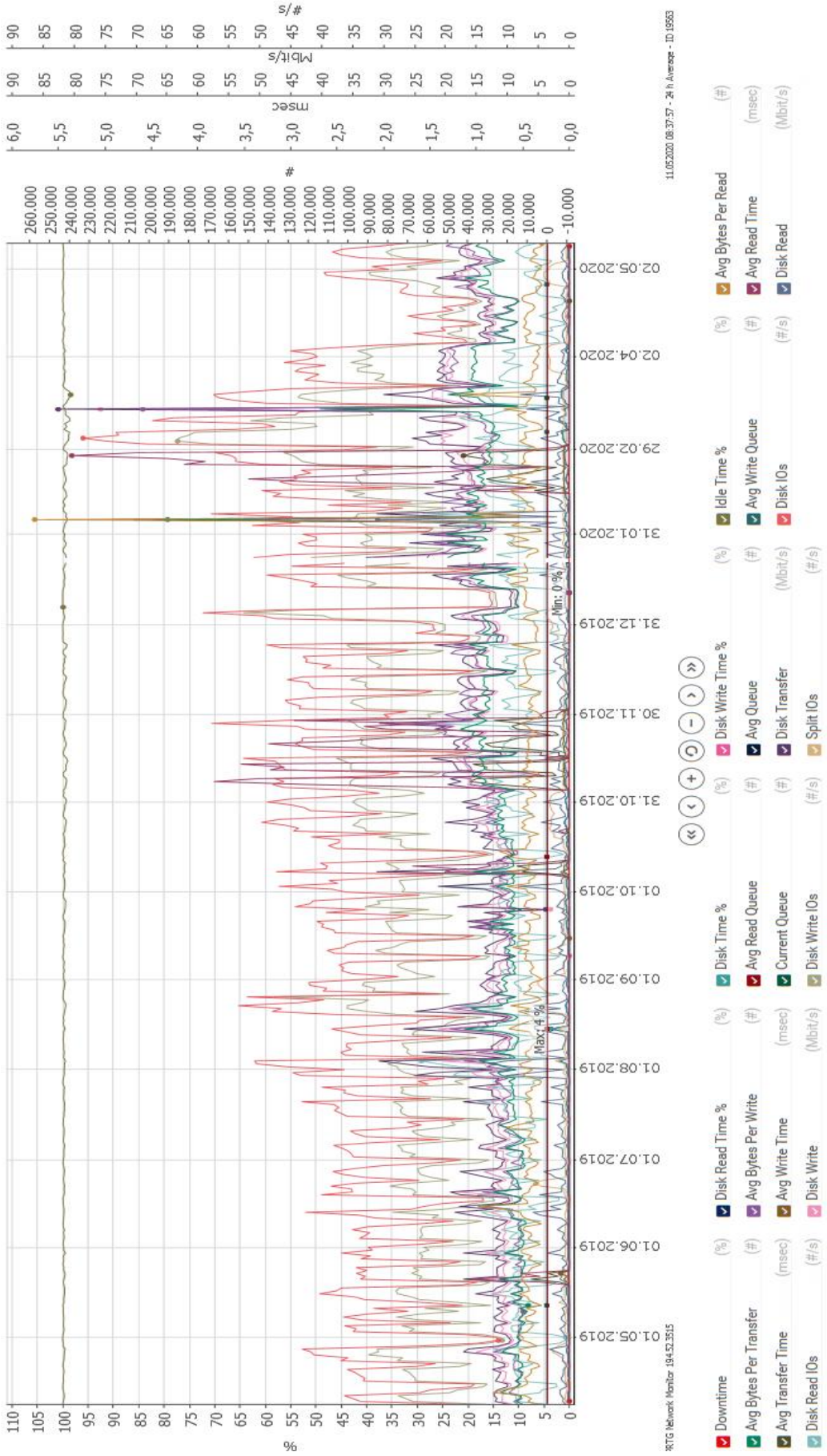
2. . Бутрименко А. В. Разработка и эксплуатация сетей ЭВМ / Александр Васильевич Бутрименко. – М. : Финансы и статистика, 1981. – 256 с.

3. Павленко М. Теоретичні та методичні засади навчання майбутніх інженерів-педагогів мережевих технологій / Максим Павленко. – Бердянськ, 2017. – 194 с

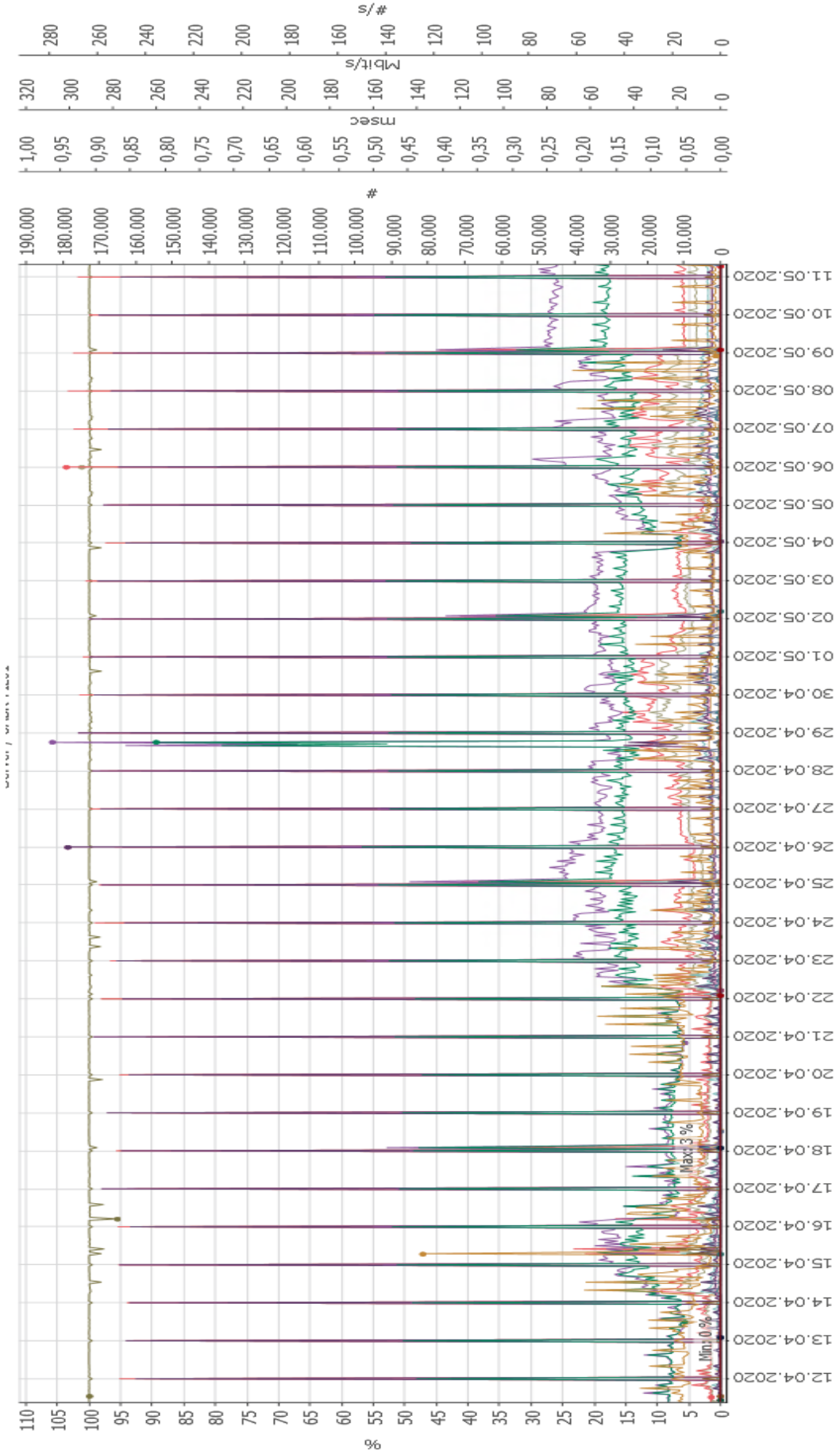
| Pos | Sensor | Status | Message | Graph | Priority | |
|---|---|---|---|---|---|---|
| 1. | PING 481 | Up | OK | Ping Time 0 msec | ★★★★★ | |
| 2. | CPU Load 280 | Up | OK | Total 0,50 % | ★★★★☆ | |
| 3. | Disk Free 209 | Warning | 20 % (Free Space D:) is below the war... | Free Space C: 28 % | ★★★★☆ | |
| 4. | Memory 222 | Up | OK | Percent Availi 76 % | ★★★★☆ | |
| 5. | Pagefile Usage 212 | Up | OK | Total 21 % | ★★★★☆ | |
| 6. | Uptime 269 | Up | OK | System Uptim 7 d 12 h | ★★★★☆ | |
| 7. | Disk IO _Total | Up | OK | Disk Read Tin <1 % | ★★★☆☆ | |
| 8. | Microsoft Network Adapter M... | Unusual | 1 hour interval average of 56 kbit/s (T... | Total 2,671 kbit/s | ★★★☆☆ | |
| 9. | Volume IO _Total | Up | OK | Free Space % 62 % | ★★★☆☆ | |
| 10. | Volume IO C: | Up | OK | Free Space % 28 % | ★★★☆☆ | |
| 11. | RDP (Remote Desktop) 173 | Up | OK | Response tim 14 msec | ★★★☆☆ | |

1 to 11 of 11

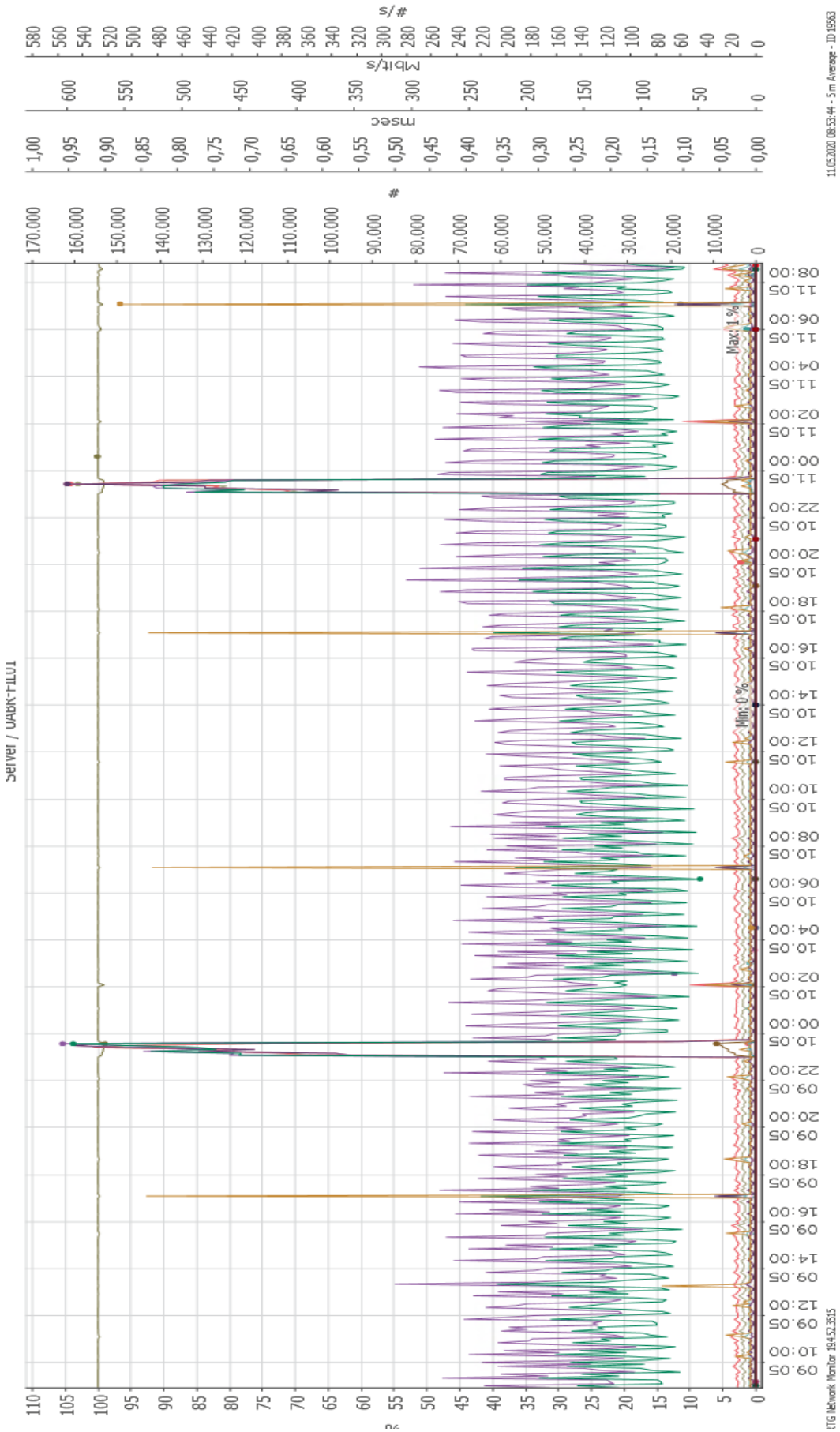
Додаток Г


PRTG Network Monitor 194.52.35.15
11.05.2020 08:37:57 - 24 h Average - ID 19563
Max: 4 %
Min: 0 %
Downtime
Disk Read Time %
Disk Time %
Disk Write Time %
Idle Time %
Avg Bytes Per Read
Avg Bytes Per Transfer
Avg Bytes Per Write
Avg Read Queue
Avg Queue
Avg Write Queue
Avg Read Time
Avg Transfer Time
Avg Write Time
Current Queue
Disk Transfer
Disk IOs
Disk Read
Disk Read IOs
Disk Write
Disk Write IOs
Split IOs

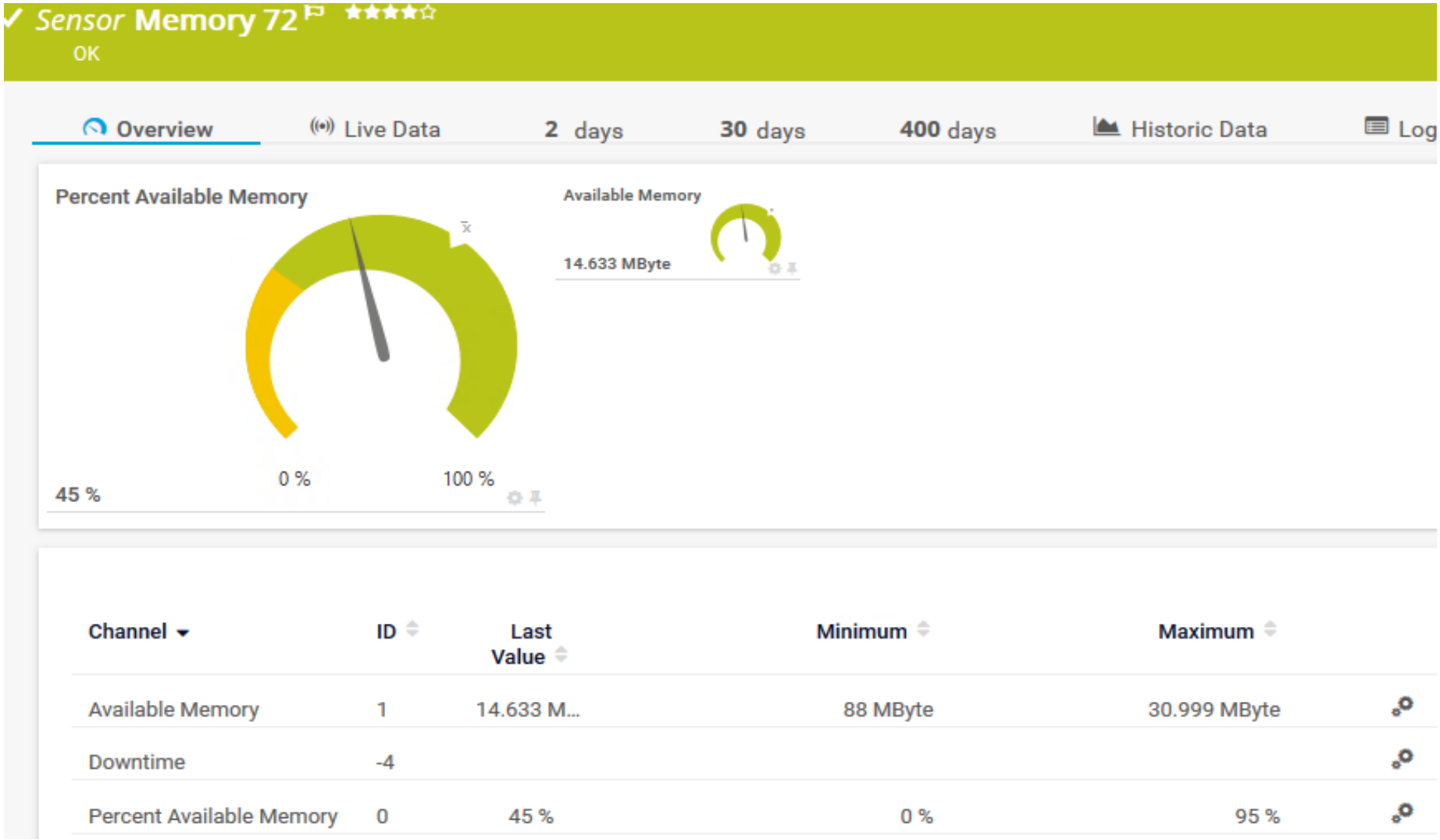
Додаток Д


%
#
msec
Mbit/s
#/s
Max: 3 %
Min: 0 %
12.04.2020
13.04.2020
14.04.2020
15.04.2020
16.04.2020
17.04.2020
18.04.2020
19.04.2020
20.04.2020
21.04.2020
22.04.2020
23.04.2020
24.04.2020
25.04.2020
26.04.2020
27.04.2020
28.04.2020
29.04.2020
30.04.2020
01.05.2020
02.05.2020
03.05.2020
04.05.2020
05.05.2020
06.05.2020
07.05.2020
08.05.2020
09.05.2020
10.05.2020
11.05.2020

Додаток Е

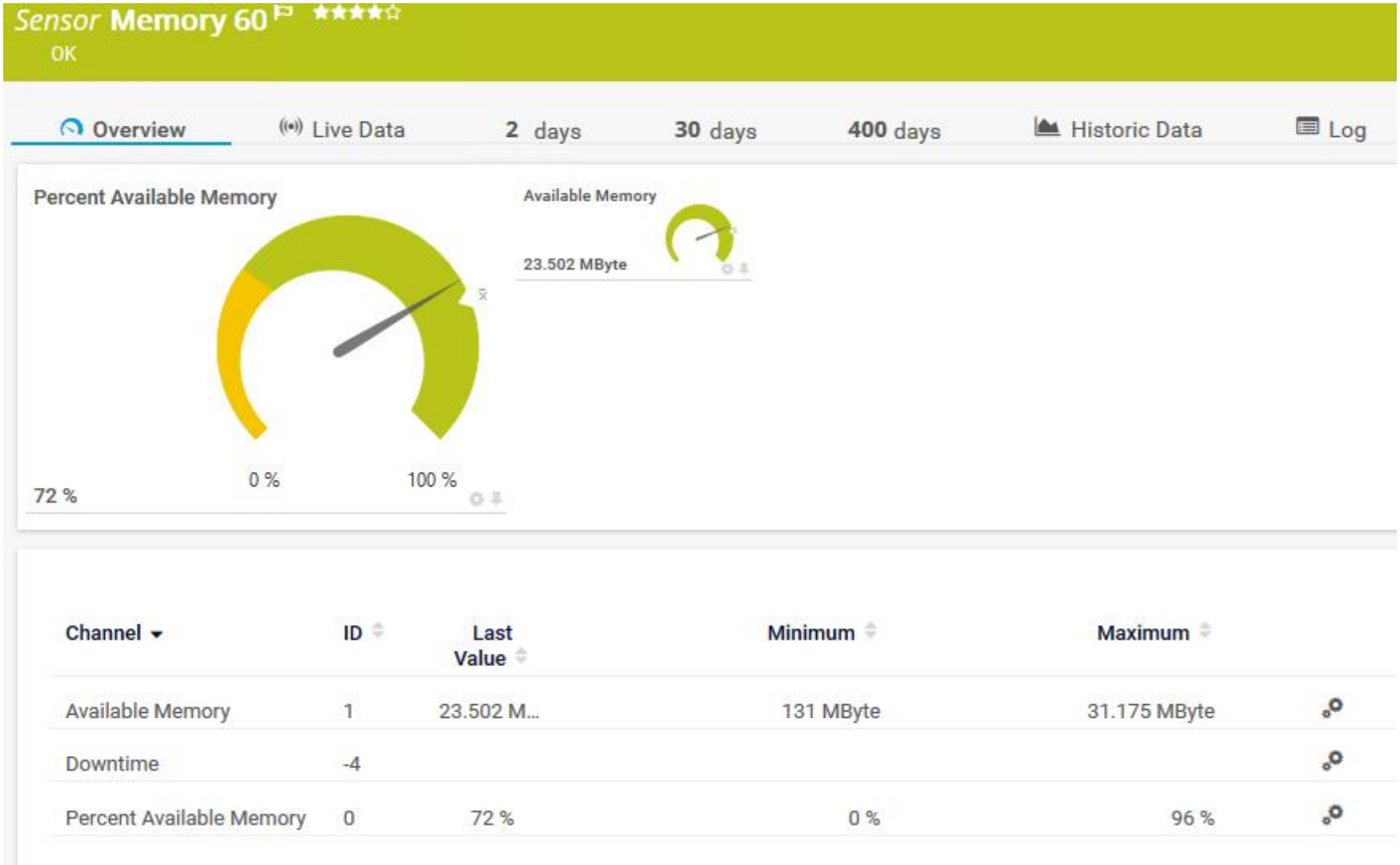

Server / UABK-TITU1
Max: 1 %
Min: 0 %
#/s
Mbit/s
msec
#
ITG Network Monitor 194.52.3515

| Pos | Sensor | Status | Message | Graph | Priority | |
|---|---|---|---|---|---|---|
| 1. | PING 323 | Up | OK | Ping Time 0 msec | ★★★★★ | |
| 2. | CPU Load 88 | Up | OK | Total 11 % | ★★★★☆ | |
| 3. | Disk Free 92 | Up | OK | Free Space C: 94 % | ★★★★☆ | |
| 4. | Pagefile Usage 92 | Up | OK | Total 10 % | ★★★★☆ | |
| 5. | Uptime 253 | Up | OK | System Uptim 7 d 5 h | ★★★★☆ | |
| 6. | Disk IO _Total | Up | OK | Disk Read Tin <1 % | ★★★☆☆ | |
| 7. | Disk IO 0 C: | Up | OK | Disk Read Tin <1 % | ★★★☆☆ | |
| 8. | Microsoft Network Adapter M... | Up | OK | Total 7.727 kbit/s | ★★★☆☆ | |
| 9. | Volume IO _Total | Up | OK | Free Space % 95 % | ★★★☆☆ | |
| 10. | Volume IO C: | Up | OK | Free Space % 94 % | ★★★☆☆ | |
| 11. | RDP (Remote Desktop) 66 | Up | OK | Response tim 14 msec | ★★★☆☆ | |
| 12. | Memory 72 | Up | OK | Percent Availi 45 % | ★★★★☆ | |


Sensor Memory 72
OK
Overview
Live Data
2 days
30 days
400 days
Historic Data
Log
Percent Available Memory
0 %
100 %
45 %
Available Memory
14.633 MByte
Channel
ID
Last Value
Minimum
Maximum
Available Memory 1 14.633 M... 88 MByte 30.999 MByte
Downtime -4
Percent Available Memory 0 45 % 0 % 95 %

| Pos | Sensor | Status | Message | Graph | Priority | |
|---|---|---|---|---|---|---|
| 1. | PING 297 | Up | OK | Ping Time 0 msec | ★★★★★ | |
| 2. | CPU Load 45 | Up | OK | Total 0.32 % | ★★★★☆ | |
| 3. | Disk Free 59 | Up | OK | Free Space C: 94 % | ★★★★☆ | |
| 4. | Memory 60 | Up | OK | Percent Availi 72 % | ★★★★☆ | |
| 5. | Pagefile Usage 50 | Up | OK | Total 0 % | ★★★★☆ | |
| 6. | Uptime 30 | Up | OK | System Uptim 7 d 14 h | ★★★★☆ | |
| 7. | Disk IO _Total | Up | OK | Disk Read Tin <1 % | ★★★☆☆ | |
| 8. | Disk IO 0 C: | Up | OK | Disk Read Tin <1 % | ★★★☆☆ | |
| 9. | Microsoft Network Adapter M... | Up | OK | Total 262 kbit/s | ★★★☆☆ | |
| 10. | Volume IO _Total | Up | OK | Free Space % 95 % | ★★★☆☆ | |
| 11. | Volume IO C: | Up | OK | Free Space % 93 % | ★★★☆☆ | |
| 12. | RDP (Remote Desktop) 45 | Up | OK | Response tim 15 msec | ★★★☆☆ | |
| 13. | Service: FastBackClient | Up | OK | Sensor Execu 59 msec | ★★★☆☆ | |

<< < 1 to 13 of 13 > >>


Sensor Memory 60
OK
Overview
Live Data
2 days
30 days
400 days
Historic Data
Log
Percent Available Memory
0 %
100 %
72 %
Available Memory
23.502 MByte
Channel
ID
Last Value
Minimum
Maximum
Available Memory 1 23.502 M... 131 MByte 31.175 MByte
Downtime -4
Percent Available Memory 0 72 % 0 % 96 %