

DOI: <https://doi.org/10.36910/6775-2524-0560-2021-42-29>

УДК 004.7

Сіваковська Олена Миколаївна, к.т.н.,

<https://orcid.org/0000-0002-9300-0039>

Ящук Андрій Анатолійович, к.т.н.,

<https://orcid.org/0000-0003-4872-7949>

Андрущак Ігор Євгенович, д.т.н., професор,

<https://orcid.org/0000-0002-8751-4420>

Ліщина Наталія Миколаївна, к.т.н., доцент,

<https://orcid.org/0000-0002-5200-536X>

Ліщина Валерій Олександрович, к.т.н., доцент.

<https://orcid.org/0000-0002-2371-3850>

Луцький національний технічний університет, м. Луцьк, Україна.

## МОНІТОРИНГ ТА ДОСЛІДЖЕННЯ МЕРЕЖІ НА БАЗІ LINUX-МАШИН

**Сіваковська О. М., Ящук А. А., Андрущак І. Є., Ліщина Н. М., Ліщина В. О.** Моніторинг та дослідження мережі на базі Linux-машин. Здійснено аналіз проблематики моніторингу мереж. Обґрунтовано переваги та недоліки наявних UNIX-подібних операційних систем. Означено етапи створення мережі на базі Linux-машин. Розглянуто основні компоненти для побудови системи моніторингу та мережі на базі Linux-машин.

**Ключові слова:** системи, моніторинг, мережі, операційні системи, Linux, управління, маршрутизатори.

**Сиваковская Е. Н., Ящук А. А., Андрущак И. Е., Лищина Н. Н., Лищина В. А.** Мониторинг и исследования сети на базе Linux-машин. Осуществлен анализ проблематики мониторинга сетей. Обоснованно преимущества и недостатки имеющийся в UNIX-подобных операционных систем. Отмечено этапы создания сети на базе Linux-машин. Рассмотрены основные компоненты для построение системы мониторинга и сети на базе Linux-машин.

**Ключевые слова:** системы, мониторинг, сети, операционные системы, Linux, управление, маршрутизаторы.

**Olena Sivakovska, Andrii Yashchuk, Igor Andrushchak, Natalia Lishchyna, Valerii Lishchyna.** Network monitoring and research based on Linux machines. The analysis of network monitoring issues is carried out. The advantages and disadvantages of existing UNIX-like operating systems are substantiated. The stages of creating the network based on Linux machines are marked. The main components for creating the monitoring system and network based on Linux machines are considered.

**Keywords:** systems, monitoring, networks, operating systems, Linux, management, routers.

**Постановка проблеми.** На сучасному етапі розвитку цивілізації все важливішу роль відіграють електронні обчислювальні машини. При цьому, навіть найпотужніші суперкомп'ютери залишалися б неефективними центрами обробки інформації, якби не виникла ідея об'єднати комп'ютери у локальні мережі. Наступним етапом стало їх об'єднання у глобальну мережу Інтернет, результатом якої стало виникнення пошукової системи, зберігання інформації, а також практично миттєвого зв'язку.

На жаль будь-які апаратні засоби, в тому числі і мережеві, мають властивість виходити з ладу і це лише одна із багатьох можливих проблем, які можуть виникнути під час експлуатації мережі. В таких умовах для вирішення гіпотетичного пошкодження далеко не на останньому місці стоїть оперативність локалізації несправності. І лише після цього можна розпочинати діагностику та усунення проблеми. Автоматизовані системи моніторингу здатні допомогти забезпечити необхідний рівень оперативності.

**Аналіз останніх досліджень та публікацій.** Питанням моніторингу та дослідження мереж займається дуже багато корпорацій. Зокрема, корпорація Майкрософт щорічно інвестує більше 1 млрд. доларів США в наукові дослідження і розробку рішень для забезпечення кібербезпеки та моніторингу мереж. Також проблематикою методів і алгоритмів моніторингу мереж займається к.т.н., доцент кафедри математичного забезпечення і застосування ЕОМ Санкт-Петербурзького державного електротехнічного університету «ЛЕТІ» ім В.І. Ульянова (Леніна) (СПбГЕТУ) Лавров А. О. Метою його дослідження є розробка методу і алгоритмів моніторингу ОС, заснованих на аналізі тимчасових закономірностей в роботі стека протоколів TCP / IP, і побудова системи моніторингу мережі на їх основі.

**Виклад основного матеріалу й обґрунтування отриманих результатів дослідження.** У широкому сенсі моніторинг — спеціально організоване, систематичне спостереження за станом об'єктів, явищ, процесів з метою їх оцінки, контролю або прогнозу [1]. Моніторингом називають систематичний збір і обробку інформації, яка використовується для поліпшення процесу прийняття рішення. З іншого боку – для інформування громадськості як інструмент зворотного зв'язку в цілях здійснення проектів, оцінки програм або вироблення політики.

Терміном «моніторинг мережі» визначають роботу системи, яка виконує постійне спостереження за комп'ютерною мережею у пошуках повільних або несправних систем і яка при виявленні збоїв –

повідомляє про них мережевого адміністратора. Ці завдання є підмножиною завдань управління мережею [2].

Комп'ютерна мережа або мережа передачі даних являє собою цифрову телекомунікаційну мережу, яка дозволяє вузлам розподіляти ресурси. У таких мережах обчислювальні пристрої здійснюють обмін даними один з одним, використовуючи з'єднання (передавання даних) між вузлами. Ці дані посилаються на кабельні носії ( до них відносимо провід або оптичні кабелі) або бездротові носії (для прикладу, Wi-Fi).

Не зважаючи на вищесказане, комп'ютерна мережа є вразливою до поломок окремих апаратних чи програмних компонентів. Для забезпечення надійності мережі застосовується резервування ресурсів, впереважності – апаратних.

В даному випадку може з'явитися певна «технічна суперечка», що пов'язана із бажанням досягнення високого рівня відмовостійкості шляхом спрямування трафіку через резервний канал (це може відбутися у разі відмови, наприклад, каналу зв'язку), а також бажанням досягнення щонайбільшого рівня утилізації. Тобто, здійснюється використання усіх ресурсів системи для виконання свого призначення, і, таким чином, досягнення максимальної фінансової вигоди. Із даного висновку випливає, що забезпеченням надійності мережі прирівнюється до фінансової вигоди, що приносять сервіси, побудовані на мережевій основі. Але насправді відмова мережі призведе до недоступності сервісів, що надто вплине на грошовий аспект.

Із вище вказаного, можна зробити висновок, що заходи щодо забезпечення відмовостійкості мережі сприяють отриманню зиску із роботи сервісів. Звідси актуальним постає питання удосконалення засобів та методів виявлення проблем та подальшого їх усунення.

Мережевий моніторинг – це використання системи, яка постійно здійснює контроль над комп'ютерною мережею для визначення повільних або несправних компонентів і повідомляє адміністратора мережі (за допомогою електронної пошти, SMS або інших сигналів) у разі виходу з ладу або виникненні інших проблем. Моніторинг мережі є частиною управління мережею. До найбільш поширених мережевих моніторів можна віднести наступні [3]:

1) мережевий монітор PRTG (графічний пристрій трафіку Paessler до версії 7) – це агентивне програмне забезпечення моніторингу мережі від Paessler AG. Він має властивість відслідковувати та класифікувати системні вимоги (наприклад, використання пропускну здатності або час безвідмовної роботи), а також збирати статистику з різних вузлів (наприклад, перемикачів, маршрутизаторів, серверів та інших пристроїв та програм);

2) Zabbix – це програмне забезпечення для моніторингу з відкритим кодом для різних компонентів ІТ, включаючи мережі, сервери, віртуальні машини (VM) та хмарні сервіси. Це ПЗ забезпечує показники моніторингу використання мережі, завантаження ЦП і споживання дискового простору. Конфігурацію Zabbix моніторингу можна виконати, використовуючи шаблони на основі XML, які містять елементи для моніторингу;

3) Pandora FMS – це ПЗ для моніторингу комп'ютерних мереж. Pandora FMS дозволяє візуально відслідковувати стан та роботу декількох параметрів з різних операційних систем, серверів, програм та систем обладнання (наприклад, брандмауери, проксі, бази даних, веб-сервери або маршрутизатори).

Оглянувши програмні продукти, що наведені вище, можна означити їх широкий функціонал та відповідні до нього системні вимоги та вимоги до апаратної частини. Можливість будування графіків та збереження даних на пристроях, забезпечення постійної пам'яті, перегляд завантаженості каналів зв'язку, що безумовно важливо для великих фірм. Аналіз опису даних програмних засобів для моніторингу мережі дав зробити висновок про їх орієнтування саме на великі підприємства, а не на малий бізнес. Для мереж такого рівня немає необхідності в цілодобовому моніторингу трафіку, перевірці доступності тисячі і більше вузлів мережі в кожен момент часу. Однак, мережі фірм малого бізнесу також потребують механізмів, що забезпечать їх надійність. Це стосується не лише системи моніторингу, а й мережі в цілому. Будь-який малий бізнес має на меті розвивати та примножувати свої потужності і, як наслідок, прибутки. А отже, такі мережі мають легко піддаватися масштабуванню, але при цьому залишатися працездатними. Тому виникає проблема створення та налаштування системи моніторингу мережі для малого бізнесу. В нашому дослідженні обґрунтуємо системи моніторингу мережі, побудованої на базі Linux-машин.

Для побудови системи моніторингу та мережі на базі Linux-машин необхідні наступні компоненти: операційна система маршрутизаторів, система віртуалізації операційної системи, система віртуалізації мережевих компонентів, мова програмування для опису сценарію, утиліта для регулярного запуску сценарію, система сповіщення.

Безумовно, що маршрутизатор (роутер) – один із найважливіших мережевих пристроїв. Саме тому особливу увагу необхідно приділити операційній системі, яка буде займатися маршрутизацією пакетів. На даний момент серед доступних варіантів можна виділити: RouterOS фірми MikroTik, Cisco IOS (Internetwork Operating System) фірми Cisco Systems, JUNOS фірми Juniper Networks. Ці операційні системи для маршрутизаторів добре зарекомендували себе на ринку. Однак в них існують суттєві недоліки при використанні у невеликих мережах. До таких можна віднести: висока вартість, можливість працювати лише на апаратних платформах тієї ж фірми-виробника та відсутність можливості кастомізації операційної системи під власні потреби. Враховуючи дані недоліки, вважаємо за потрібне розглянути альтернативи.

FreeBSD – UNIX-подібна операційна система, витоків якої тягнуться від AT & T UNIX, через Berkeley Software Distribution (BSD) гілку операційних систем 386BSD і 4.4BSD. Працює на Intel x86 (IA-32), сумісний з ПК системами (включно з Microsoft Xbox, а також DEC Alpha, Sun, Itanium (IA-64), AMD64, PowerPC і NEC PC-98 архітектурами. FreeBSD добре зарекомендувала себе як система для побудови інтернет-серверів. Вона надає достатньо надійні мережеві сервіси та ефективного управління пам'яттю [4].

GNU / Linux - загальна назва UNIX-подібних операційних систем на базі аналогічного ядра. Це один з найвизначніших прикладів розробки вільного та відкритого (з відкритим кодом) програмного забезпечення. На відміну від власних операційних систем (на кшталт Microsoft Windows і MacOS X), їх вихідні коди доступні всім для використання, зміни та розповсюдження абсолютно вільно (в тому числі безкоштовно) [5]. Лінукс орієнтовано на досить велику кількість апаратних платформ. Цю операційну систему можна досить успішно використовувати як на основних і суперкомп'ютерах, так і на багатьох інших пристроях (наприклад, пристроях автоматички, смартфонах, планшетах, маршрутизаторах комп'ютерних мереж (роутерах), ПК, системи керування телевізорами та ігровими консолями тощо). Велика кількість спеціалізованих дистрибутивів Linux дозволяє застосовувати широкі можливості вибору програмного забезпечення. З вище сказаного можна зробити висновок, що Linux і FreeBSD мають приблизно одні і ті ж переваги та недоліки, але зупинемо вибір на Linux, оскільки саме ця операційна система має більше прихильників. Це насправді не означає, що FreeBSD гірша система, але при виникненні будь-якої проблеми, буде значно простіше знайти її вирішення, оскільки користувачі із дуже великою вірогідністю уже мали справу із такого типу проблемою.

Перед початком створення системи моніторингу, необхідно організувати мережеву лабораторію. Для цієї мети на основну інсталювану операційну систему Kubuntu 18.10 буде встановлено систему віртуалізації для підготовки та попереднього налаштування головного шаблону операційної системи маршрутизаторів. Спочатку потрібно завантажити файл інсталяції програми (рис.1).

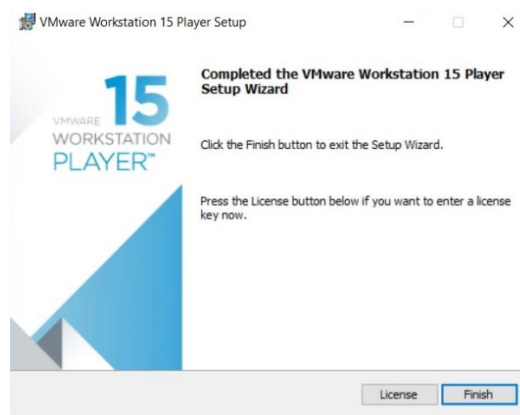


Рисунок 1 – Закінчення інсталяції VMware Player

На основній машині тепер встановлено систему віртуалізації, з допомогою якої можна в гостьовому режимі встановити операційну систему для маршрутизаторів. Для цього потрібно запустити процес інсталяції операційної системи. Наступним кроком стане заповнення попередніх даних користувача.

Важливий момент полягає в тому, що після встановлення, VMware Player додає віртуальні мережеві інтерфейси vmnet0, vmnet1, vmnet8 (рис. 2). Кожен із інтерфейсів відповідає трьом основним типам інтерфейсів bridge, host-only та NAT відповідно.

```
schistos@moosmachine:~$ ip -br a
lo                UNKNOWN    127.0.0.1/8  ::1/128
enp2s0           DOWN
wlp3s0           UP         192.168.0.107/24 fe80::d105:d29:e8ac:74cd/64
vmnet1           UNKNOWN    172.16.49.1/24 fe80::250:56ff:fec0:1/64
vmnet8           UNKNOWN    172.16.22.1/24 fe80::250:56ff:fec0:8/64
```

Рисунок 2 – Віртуальні інтерфейси

Наступний крок – це попередні налаштування Ubuntu server 18.04. Вказується звичайна інсталяція Ubuntu, хмарні технології для даного проекту не потрібні.

Налаштування мережевого інтерфейсу – ще один етап у створення системи моніторингу.

Наступний етап – вибір Проху-сервера, але оскільки в цьому випадку підключення «пряме», IP-адреса Проху-сервера не потрібна. Поле залишаємо пустим. Для проекту особлива розмітка віртуального жорсткого диску не потрібна, тому буде використовуватися весь віртуальний жорсткий диск з автоматичною розміткою основних розділів. Далі здійснюємо прийняття схеми розмітки віртуального жорсткого диску. Після усіх проведених налаштувань, необхідно надати дозвіл на інсталяцію операційної системи. Коли процес встановлення розпочато, – можна паралельно з ним Ubuntu-серверу дати можливість створити користувача та вказати пароль для аутентифікації користувача. Після закінчення процесу інсталяції операційної системи та перезавантаження віртуальної машини, можна встановлювати додаткове програмне забезпечення.

Спершу необхідно оновити дані репозиторіїв та доступні пакети, встановити утиліти для роботи DHCP-сервера, DNS-сервера, VPN. Після встановлення усіх необхідних утиліт для роботи мережі – віддається команда на вимкнення Ubuntu server.

Наступний етап – інсталяція системи віртуалізації мережі EVE-NG. Після налаштування мережевого інтерфейсу EVE-NG здійснюємо імпорт збереженого раніше віртуального жорсткого диску Ubuntu server на EVE-NG-сервер. Окрім імпорту віртуального жорсткого диску необхідно створити новий зразок для маршрутизаторів. Для цієї мети потрібно створити файл конфігурації в директорії.

Після виконання приведених вище дій, для використання будуть доступні маршрутизатори з операційною системою Ubuntu server 18.04.

Наступним етапом стане побудова схеми мережі. Мережа буде складатися з трьох частин, а саме двох локальних мереж та мережі провайдера (рис. 3).

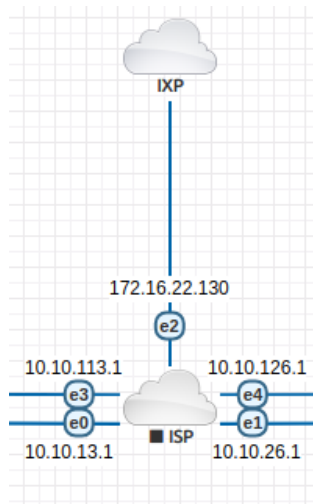


Рисунок 3 – Схема мережі провайдера

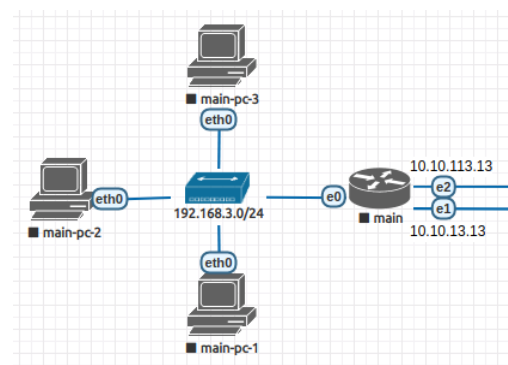


Рисунок 4 – Схема локальної мережі Main

Дана мережа складається із маршрутизатора ISP із підтримкою п'яти інтерфейсів та точки обміну інтернет-трафіком IXP (точки з'єднання мереж різних провайдерів). Технічно, IXP в даному випадку – це головний інтерфейс сервера EVE-NG, який, в свою чергу, підключений до мережевого інтерфейсу машини-хоста. Таким чином всі мережеві пристрої в даній мережевій лабораторії мають доступ до мережі Інтернет.

Перша із двох локальних мереж Main містить в собі три ПК, один комутатор та один маршрутизатор (рис. 4).

Аналогічним чином побудована друга локальна обчислювальна мережа Phialial. Як підсумок, глобальна мережа матиме такий вигляд (рис. 5).

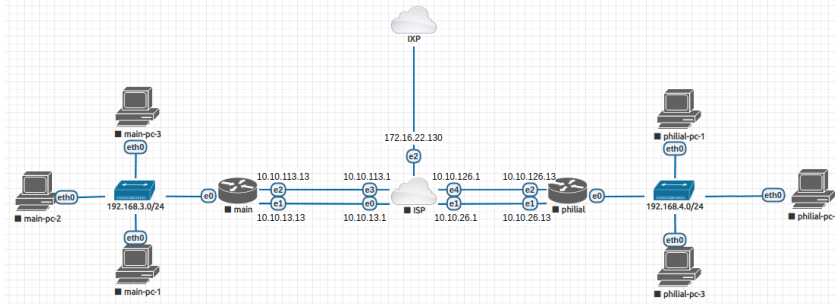


Рисунок 5 – Загальна схема мережі

Наступний етап проектування мережі – налаштування маршрутизаторів, яке буде відбуватися за наступним порядком: налаштування інтерфейсів; налаштування DHCP-сервера в сторону локальної мережі; налаштування DNS-серверу; налаштування NAT; налаштування VPN.

Після усіх налаштувань, які детально описувати не будемо, матимемо уже спроектовану функціонуючу мережу, у якій передбачено дві локальні мережі, які через мережу провайдера з'єднані з допомогою VPN-тунелювання. Маршрутизатори Main та Phialial підключені до мережі провайдера двома каналами, що збільшує надійність та відмовостійкість обох мереж. На обох маршрутизаторах щохвилини запускається сценарій, що перевіряє доступність критично важливих вузлів мережі та у випадку недоступності майже миттєво надсилає повідомлення у спеціально створений для цього чат. Таким чином, отримана мережа характеризується достатньо високим рівнем надійності, при відносно малих затратах ресурсів, що відводяться на систему моніторингу.

Дослідження результативності спроектованої системи доцільно проводити при наявності аналогічної комп'ютерної мережі із базовими налаштуваннями. Таким чином можна буде отримати результати, на основі яких буде здійснено висновок щодо ефективності побудованої системи у порівнянні із типовими аналогами.

Необхідними умовами для впровадження системи моніторингу мережі, побудованої на базі Linux-машин будуть: пристрої, які необхідно об'єднати в локальну мережу, наприклад, персональні робочі станції; комутатор для фізичного об'єднання кожної окремої локальної мережі; маршрутизатор для встановлення зв'язку з мережею Інтернет кожного окремого філіалу підприємства; програмні продукти для забезпечення необхідного базового функціоналу маршрутизаторів.

Кількість мережевих комутаторів потрібно обирати із кількості пристроїв, що необхідно об'єднати. Для функціонування представленої схеми мережі потрібно використовувати два комутатора – один для мережі Main та ще один для мережі Phialial. Як приклад буде розглянути наступний комутатор TP-LINK TL-SF 1005D із параметрами, що приведені в таблиці 1. Даний комутатор має можливість підключення п'яти локальних пристроїв, включно із маршрутизатором. Ethernet-порти мають можливість працювати із пропускнуою здатністю в 100 мегабіт на секунду в режимі повного дуплексу. Із мінімальною ціною складає цілком доступний комутатор для даної мети.

Таблиця 1 – Характеристики комутатора TP-LINK TL-SF 1005D

Тип	Комутатор локальної мережі (Switch)
Швидкість передачі даних	100 Мб/с
Стандарти	Auto MDI/MDIX
Роз'єми	RJ45 (авто-MDI/MDIX)
Протоколи	IEEE802.3, 802.3u, 802.3x, CSMA/CD, TCP/IP
Довжина	22 мм
Ширина	103,5 мм
Висота	70 мм
Кількість портів	5
Ціна	209 грн



Для апаратної частини маршрутизатора можна використати практично будь-яку комплектацію, але щоб при цьому апаратна частина відповідала мінімальним вимогам, приведеним в таблиці 2.

Таблиця 2 – Мінімальні апаратні вимоги Ubuntu server

Тип	Процесор	Оперативна пам'ять	Розмір жорсткого диску	
			Базове встановлення	Повне встановлення
Server	300 МГц	128 Мбайт	500 Мбайт	1 ГБайт

Також важливим фактором є наявність трьох мережевих інтерфейсів. За певних умов операційну систему можна встановити як прошивку для уже існуючого маршрутизатора з метою отримання доступу до більш широкого функціоналу.

Усі програмні продукти, що приведені в проектуванні мережі поширюються безплатно, тому їх отримання не пов'язане із фінансовими проблемами.

Із приведених даних можна зробити висновок, що впровадження даного проекту не має чітких рамок реалізації, що дає можливість вільного підбору апаратних компонентів, оскільки програмна частина не прив'язана до конкретної архітектури чи фізичних приладів. Завдяки чому, спроектована мережа легко масштабується та здатна до оптимізації під різноманітні потреби. А система моніторингу, що практично не навантажує операційну систему забезпечує оперативне сповіщення про мережеві неполадки, таким чином збільшуючи загальний рівень надійності та відмовостійкості мережі.

**Висновки та перспективи подальших досліджень.** Комп'ютерна мережа, що побудована на базі операційної системи Linux легко піддається масштабуванню та оптимізації під існуючі апаратні можливості підприємства із мінімальним добром комплектуючих пристроїв.

Такий різновид систем є хорошим рішенням для встановлення у місцях, що не мають чіткої структури та схильні до частих змін та перебудов, оскільки система легко адаптується під актуальні потреби та легко переноситься на практично будь-яку апаратну частину. Такі показники дозволяють виконувати модернізацію та адаптацію під конкретну задачу. Система моніторингу, що не навантажує ні апаратну частину, ні операційну систему, не заважає проводити дані дії, забезпечуючи при цьому оперативне сповіщення про неполадки, що суттєво полегшує проведення діагностики та подальшого усунення проблеми, таким чином збільшуючи загальний рівень надійності та відмовостійкості комп'ютерної мережі.

#### Список бібліографічного опису

1. Б. Стогній, М. Сопель (2013) Основи моніторингу в електроенергетиці. Про поняття моніторингу. Техн. Електродинаміка. №1, URL : [http://previous.techined.org.ua/2013\\_1/st9.pdf](http://previous.techined.org.ua/2013_1/st9.pdf) (дата звернення: 10.03.2021). АСМ.
2. М. Гузій, О. Станіславова, М. Кадет (2012) Аналіз технологій моніторингу кмп'ютерних мереж. Наукові технології. №4 (16), URL : <http://jrn1.nau.edu.ua/index.php/SBT/article/viewFile/5091/5353#:~:text=%D0%A2%D0%B5%D1%80%D0%BC%D1%96%D0%BD%D0%BE%D0%BC%20%D0%BC%D0%BE%D0%BD%D1%96%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96%20%D0%B2%D0%B8%D0%B7%D0%BD%D0%B0%D1%87%D0%B0%D1%8E%D1%82%D1%8C%20%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D1%83.%D1%94%20%D0%BF%D1%96%D0%B4%D0%BC%D0%BD%D0%BE%D0%B6%D0%B8%D0%BD%D0%BE%D1%8E%20%D0%B7%D0%B0%D0%B2%D0%B4%D0%B0%D0%BD%D1%8C%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D1%8E> (дата звернення: 10.03.2021). АСМ.
3. Networking monitoring tools (2021) National Acceleratory Laboratory SLAC, URL: <https://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html> (дата звернення: 10.03.2021). АСМ.
4. Ю. Тарнавський, М. Кузьменко (2018) Організація комп'ютерних мереж: підручник для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки», Київ: КПІ ім. Ігоря Сікорського, 259 с. АСМ.
5. Linux (2020) Матеріал з Вікіпедії — вільної енциклопедії, URL : [https://uk.wikipedia.org/wiki/Linux#:~:text=%D0%9B%D1%96%CC%81%D0%BD%D1%83%D0%BA%D1%81%20%D0%B0%D0%BD%D0%B3%D0%BB.,%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20\(software\)](https://uk.wikipedia.org/wiki/Linux#:~:text=%D0%9B%D1%96%CC%81%D0%BD%D1%83%D0%BA%D1%81%20%D0%B0%D0%BD%D0%B3%D0%BB.,%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20(software)) (дата звернення: 11.03.2021). АСМ.

#### References

1. B. Stogniy, M. Sopol (2013) Power Monitoring in Electricity. Concepts of Monitoring. Tech. Electrodynamics. N 1, available at: [http://previous.techined.org.ua/2013\\_1/st9.pdf](http://previous.techined.org.ua/2013_1/st9.pdf) (accessed 10.03.2021). АСМ.
2. M. Guziy, O. Stanislavova, M. Cadet (2012) Analysis of Monitoring Technologies of Computer Networks. Science-intensive Technologies N 4 (16), available at: [http://jrn1.nau.edu.ua/index.php/SBT/article/viewFile/5091/5353#:~:text=%D0%A2%D0%B5%D1%80%D0%BC%D1%96%D0%BD%D0%BE%D0%BC%20%D0%BC%D0%BE%D0%BD%D1%96%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96%20%D0%B2%D0%B8%D0%B7%D0%BD%D0%B0%D1%87%D0%B0%D1%8E%D1%82%D1%8C%20%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D1%83.%D1%94%20%D0%BF%D1%96%D0%B4%D0%BC%D0%BD%D0%BE%D0%B6%D0%B8%D0%BD%D0%BE%D1%8E%20%D0%B7%D0%B0%D0%B2%D0%B4%D0%B0%D0%BD%D1%8C%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F%20\(software\)](http://jrn1.nau.edu.ua/index.php/SBT/article/viewFile/5091/5353#:~:text=%D0%A2%D0%B5%D1%80%D0%BC%D1%96%D0%BD%D0%BE%D0%BC%20%D0%BC%D0%BE%D0%BD%D1%96%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96%20%D0%B2%D0%B8%D0%B7%D0%BD%D0%B0%D1%87%D0%B0%D1%8E%D1%82%D1%8C%20%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D1%83.%D1%94%20%D0%BF%D1%96%D0%B4%D0%BC%D0%BD%D0%BE%D0%B6%D0%B8%D0%BD%D0%BE%D1%8E%20%D0%B7%D0%B0%D0%B2%D0%B4%D0%B0%D0%BD%D1%8C%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F%20(software))

[%B3%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96%20%D0%B2%D0%B8%D0%B7%D0%BD%D0%B0%D1%87%D0%B0%D1%8E%D1%82%D1%8C%20%D1%80%D0%BE%D0%B1%D0%BE%D1%82%D1%83.%D1%94%20%D0%BF%D1%96%D0%B4%D0%BC%D0%BD%D0%BE%D0%B6%D0%B8%D0%BD%D0%BE%D1%8E%20%D0%B7%D0%B0%D0%B2%D0%B4%D0%B0%D0%BD%D1%8C%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F%20%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D1%8E](#) (accessed 10.03.2021). ACM.

3. Networking monitoring tools (2021) National Acceleratory Laboratory SLAC, available at: <https://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html> (accessed 10.03.2021). ACM.

4. Yu. Tarnavsky, M. Kuzmenko (2018) Organization of Computer Networks: Textbook for Students Specialty 121 Software Engineering and 122 Computer Sciences, Kyiv: National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 259 pp. ACM.

5. Linux (2020) Materials from Wikipedia – the free encyclopedia, available at: [https://uk.wikipedia.org/wiki/Linux#:~:text=%D0%9B%D1%96%CC%81%D0%BD%D1%83%D0%BA%D1%81%20\(%D0%B0%D0%BD%D0%B3%D0%BB,\)%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20\(software\)](https://uk.wikipedia.org/wiki/Linux#:~:text=%D0%9B%D1%96%CC%81%D0%BD%D1%83%D0%BA%D1%81%20(%D0%B0%D0%BD%D0%B3%D0%BB,)%20%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE%20%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F%20(software)) (accessed 11.03.2021). ACM.