DOI: 10.26565/2786-4995-2021-3-07
УДК 330.115:338.45

Олександр Тарасенко
к.т.н., доцент кафедри ІТММ, Навчально-науковий інститут
«Каразінський банківський інститут»
Харківського національного університету ім. В.Н. Каразіна (Україна);
проспект Перемоги, 55, Харків, Харківська область, 61000;
e-mail: tap-top@ukr.net
Владислав Христоєв
студент, Навчально-науковий інститут
«Каразінський банківський інститут»
Харківського національного університету ім. В.Н. Каразіна (Україна);
проспект Перемоги, 55, Харків, Харківська область, 61000;
e-mail: vladislav0572@gmail.com;
Данило Аксинін
студент, Навчально-науковий інститут
«Каразінський банківський інститут»
Харківського національного університету ім. В.Н. Каразіна (Україна);
проспект Перемоги, 55, Харків, Харківська область, 61000;
e-mail: daniilaksinin@gmail.com;

АДМІНІСТРУВАННЯ ТА МОНІТОРИНГ КОМП'ЮТЕРНИХ МЕРЕЖ ЯК МЕТОД ВИРІШЕННЯ СУЧАСНИХ ПРОБЛЕМ У ФІНАНСОВИХ СИСТЕМАХ

Анотація. У статті визначено роль адміністрування та моніторингу комп'ютерних мереж у фінансових системах. Головні цілі моніторингу - активності у мережі. Аналіз досліджень та постановка завдання полягають у моніторингу трафіку, як важливішого джерела інформації для ефективного управління мережею, приведення основних функцій адміністраторів мережи у фінансових системах. Ефективність моніторингу з використанням аналізаторів мережевого трафіку який залежить від топології досліджуваної мережі, її конфігурації, та від набору пристроїв, з яких мережа побудована. Результат дослідження у вигляді двох головних потреб - це моніторинг та аналіз. Ефективне управління мережі у сфері фінансів та у банківських системах, а також постійне вдосконалення програмного забезпечення у фінансових системах. Яким вимогам відповідає технологія програмних агентів. Основні функції та задачі адміністрування мережі- опис моніторингу, його засоби та аналіз мереж, які поділяються на певні класи: аналізатори протоколів (Protocolanalyzers), засоби управління системою (System Management), системи управління мережею (Network Management Systems), будовані системи діагностики і управління (Embedded Systems), багатофункціональні пристрої аналізу та діагностики, обладнання для діагностики і сертифікації кабельних систем, експертні системи. Основні функції моніторингу та аналізу мережевої активності у фінансових системах які полягають у вигляді 4 пунктів: аналіз продуктивності, облік роботи мережі, управління безпекою, обробка помилок. Головні аспекти, для розробки ПЗ для моніторингу мережевої активності, потреби, що виникають в ході роботі з мережею, особливості адміністрування цих мереж, проаналізовані вже існуючі ПЗ для моніторингу мережевої активності у фінансових системах. Приклад використання програмного забезпечення для адміністрування та моніторингу комп'ютерних мереж - опис можливостей і висвітлення переваг та недоліків даних програм у фінансових системах. В даній статті розглядаються такі програмне забезпечення: Total Network Monitor 2, Observium, Network Olympus, Zabbix.

Ключові слова: *програмне забезпечення (ПЗ), моніторинг, аспект, мережа, адміністрування, інформаційний захист, інтернет-комунікація, периферійне обладнання, конфігурація.*

Рис.: 4, бібл.: 7

Вступ. В наші часи важко уявити своє життя без комп'ютерів та мобільних пристроїв. Через це виникла велика кількість проблем, які потребують нашої уваги та часу. Сьогодні кількість мереж та комп'ютерів в цих мережах обчислюється тисячами, а іноді десятками мільйонів. В корпоративних мережах діяльність користувачів розподілена, проте складні задачі вирішуються групами користувачів. Через це проблеми адміністрування таких систем та контролю ресурсів є актуальними.

Головними цілями моніторингу активності у мережі є контроль роботи, виявлення некоректного використання ресурсів та забезпечення інформаційної безпеки [1].

В моніторингу та забезпеченні безпеки мережі за останні роки сталися суттєві зміни. До цих змін високий ступінь надійності мережі можна було забезпечити завдяки шифруванню, ідентифікації, розмежування доступу та автентифікації. Та зараз для того щоб забезпечити належний ступень надійності користувачі використовують міжмережеві екрани, антивірусні програми та системи виявлення атак.

Постійний контроль становить основу будь-якої корпоративної мережі, необхідний для її працездатності. Використання спеціального ПЗ допомагає адміністратору виявляти проблемні ділянки та усунути всі недоліки.

Ефективне управління мережі у сфері фінансів та у банківських системах, а також постійне вдосконалення програмного забезпечення, приводить до покращення працездатності, та поліпшенню основних показників діяльності, таких, як витрати ресурсів, оперативність і якість. В результаті, правильний моніторинг мережевої активності є головним параметром діяльності багатьох підприємств.

Аналіз досліджень та постановка завдання. Моніторинг трафіку – це важливіше джерело інформації для ефективного управління мережею. В результаті моніторингу трафіку, дані які були отримані беруться до уваги при розподілі ресурсів, плануванні обчислювальних потужностей для виконання корпоративних додатків, виявленні та локалізації відмов, розв’язанні питань безпеки.

У мережах шинної топології, завдяки наявності єдиного спільного середовища розповсюдження даних, моніторинг трафіку був відносно простим завданням. Для стеження за всім трафіком до такої мережі достатньо підключити єдиний пристрій для реєстрації трафіку, або використати мережевий інтерфейс і відповідний програмний засіб на одному з існуючих вузлів.

В ході подальшого розвитку мереж передачі даних, зростаючі вимоги до пропускної здатності мережі і розвиток технологій комутації пакетів зумовили швидкий перехід від єдиного середовища передачі, спільно використовуваного усіма вузлами, до сегментованих топологій. Та при цьому весь трафік вже неможливо «побачити» з однієї точки – і для отримання загальної картини необхідно виконувати моніторинг вхідного та вихідного трафіку окремо на кожному комп’ютері, що підключений до корпоративної мережі. Оскільки цей процес вимагає значних витрат обчислювальних потужностей персонального комп’ютера, то це може сповільнити саму роботу всієї системи в цілому. Окрім проблеми додаткового обчислювального навантаження (overhead), постають і інші проблемні питання: надійне зберігання логів (файлів чи баз даних з результатами моніторингу), збирання цих даних для подальшого їх аналізу, поновлення баз даних заборонених (недопустимих) з’єднань, і все це з урахуванням можливості збоїв у роботі обладнання та виходу частин мережі з ладу.

Очевидним є те, що ефективність моніторингу з використанням аналізаторів мережевого трафіку залежить від топології досліджуваної мережі, її конфігурації, та від набору пристроїв, з яких мережа побудована. У разі виникнення потреби організації спостереження за трафіком у мережі деякої компанії доведеться додавати чи замінювати обладнання та переналаштовувати системи відповідно до нової топології. Додаткові переналаштування необхідно буде зробити після кожної зміни складу та топології мережі, які можуть статися через підключення, відключення, заміну комп’ютерів або мережевої апаратури, або через відмови окремих апаратних елементів. Таким чином, складність задачі організації та підтримки дослідження трафіку зростає разом із зростанням складності структури мереж.

Ось чому нині є актуальною розробка алгоритмів моніторингу для вирішення вище перерахованих проблем і вибір для цього технології, яка вимагала б якомога менших витрат ресурсів комп'ютера, на якому реалізовано спостереження за трафіком.

Одним з актуальних наукових завдань є розробка алгоритмів та ПЗ для програмного засобу моніторингу мережевої активності персональних комп'ютерів, який міг би працювати з мережею у будь-якої топології та дозволяв забезпечити постійний моніторинг трафіку мережі, навіть у випадках збоїв обладнання і при неможливості втручання адміністратора. Такий програмний засіб має бути розподіленою інтелектуальною системою, яка може самостійно приймати рішення відповідно до ситуації.

Цим вимогам відповідає технологія програмних агентів. Розробка системи моніторингу мережевого трафіку персональних комп'ютерів на основі технології програмних агентів дозволить забезпечити більш надійну інформаційну безпеку корпоративної мережі організації.

Метою статті є дослідження принципів та методів адміністрування та моніторингу комп'ютерних мереж з використанням певного програмного забезпечення.

Результати дослідження. При роботі в мережі можна видокремити дві головні потреби, це – аналіз і моніторинг.

Моніторинг полягає у зборі інформації про роботу мережі, стан комутаторів, кількість працюючих портів, коректність роботи маршрутизаторів.

На етапі аналізу виконується більш складний процес, який полягає в обробці отриманої інформації на етапі моніторингу. А саме зіставлення отриманої статистики зі статистикою отриманою раніше, формування припущень щодо сповільнення, або некоректності роботи мережі.[2]

Засоби моніторингу та аналізу мережі поділяють на класи:

1) Аналізатори протоколів (Protocolanalyzers) – апаратно-програмні системи, які використовуються для моніторингу і аналізу трафіку в мережі.

2) Засоби управління системою (System Management) – часто виконують ті ж самі функції, що й системи управління мережею, але засоби управління більш направлені на комунікаційне устаткування.

3) Системи управління мережею (Network Management Systems) – це програмні системи, що надають інформацію щодо трафіку в мережі та стан вузлів в мережі. Окрім надання інформацію ці системи можуть автоматично включати та відключати порти пристроїв при необхідності.

4) Вбудовані системи діагностики і управління (Embedded Systems) – програмно-апаратні модулі, що встановлюються в комунікаційне обладнання. Вони виконують діагностику і управління лише одним пристроєм.

5) Багатофункціональні пристрої аналізу та діагностики – дешеві портативні пристрої, які об'єднують в собі декілька пристроїв.

6) Обладнання для діагностики і сертифікації кабельних систем. Цей клас в свою чергу поділяється на чотири групи: мережеві монітори – для тестування кабелів, пристрої для сертифікації кабельних систем, кабельні сканери – для діагностики мідних кабельних систем, тестери – для перевірки кабелів на наявність фізичного розриву.

7) Експертні системи – це вид систем, що виявляють причини аномальної роботи мережі та можливі заходи для переведення мережі в працездатний стан.

Виділимо основні функції моніторингу та аналізу мережевої активності:

1) Аналіз продуктивності – на основі статистики допомагає виявити причини збоїв та некоректної роботи мережі, а також планувати розвиток мережі в майбутньому.

2) Облік роботи мережі – запис та управління ресурсами та пристроями мережі.

3) Управління безпекою – контроль та збереження цілісності даних.

4) Обробка помилок – виявлення та усунення некоректної роботи мережі.

Головною умовою успішної діяльності підприємства при роботі в мережі є комп'ютерна безпека. Дотримання основних правил дозволить захистити користувача, від можливих ризиків, таких як використання персональних даних, ураження шкідливою інформацією, або навіть

фінансових втрат.

Після того, як в нашому суспільстві масово поширилися мережеві технології з'явилося питання інформаційного захисту. Через те, що майже вся робота пов'язана з мережею, використання сервісів електронної пошти, так інших програм інтернет-комунікації, потреби безпеки необхідно було вирішувати негайно.

Масове поширення комп'ютерних вірусів та хакерських атак на функціонуючі мережі, стали причинами використання антивірусного програмного забезпечення.

Крім вірусного ПЗ та атак хакерів, небезпека може приховуватись в самому контакті з деякими видами інформації. Така інформація може завдати шкоди не тільки підприємству та мережі, що в ньому функціонує, а навіть здоров'ю та психіці користувача [1].

Важливо розуміти, що всі ці вище перелічені ризики, вони багаторазово зростають з кожним днем. Пов'язано це з тим, що розвиток комп'ютерного світу відбувається досить швидко, з кожним днем виникають тисячі нових проблем.

Саме тому в кожному підприємстві, яке пов'язано з роботою мережі, або навіть декількох мереж, необхідні такі люди як адміністратори. Які будуть контролювати інформацію, що передається в мережі, контролювати трафік, та вирішувати проблеми, що можуть виникнути під час праці [3].

Розглянемо основні функції та задачі адміністрування мережі:

1) об'єднання комп'ютерів в мережу;

2) розмежування прав користувачів;

3) впровадження антивірусного захисту;

4) управління конфігурацією (налаштування компонентів системи, мережевих адрес);

5) облік роботи мережі (контроль використовуваними ресурсами та пристроями мережі);

6) управління продуктивністю (збір інформації про роботу мережі, з метою оптимізації та мінімізації витрат ресурсів);

7) встановлення та налаштування програмного забезпечення;

8) підключення та налаштування обладнання (периферійного);

9) управління безпекою;

На різних підприємствах та в різних компаніях приведені вище функції можуть змінюватися. Задачі адміністратора поділяються на дві групи: контроль за роботою мережевого устаткування (відбувається заміна або налаштування мережевих приладів, усунення збоїв, шо виникають) та управління функціонування мережі в цілому (моніторинг та аналіз інформації для забезпечення інформаційної безпеки) [4].

Для того, щоб мінімізувати кількість системних адміністраторів, та полегшити їх працю доволі часто практикують віддалене адміністрування. Для цього використовують спеціальні утиліти, що надають можливість підключатися до мережі через інтернет в реальному часі. Таким чином можна отримати повний контроль над будь-яким ПК, що знаходиться в мережі, перебуваючи де завгодно. Сьогодні існує досить велика кількість утиліт від розробників програмного забезпечення. Відрізняються вони інтерфейсом, може бути консольним або графічним, та набором деяких інструментів [5].

ПЗ для моніторингу мережевої активності – це незамінні помічники системного адміністратора. Вони дозволяють бути в курсі всіх мережевих процесів. [6], [7]

Прикладами таких ПЗ є наступні програми:

1) Total Network Monitor 2 – доступне та дієве програмне забезпечення для мережевого моніторингу. Основним компонентом TNM 2 є монітори, що виконують перевірки з необхідною періодичністю. Ці перевірки дозволяють відстежити майже будь-який параметр, від доступності серверів в мережі, до перевірки стану сервісів.[8]

Дане ПЗ здатне самостійно усувати первинні неполадки – наприклад перезавантажувати пристрої користувачів, активувати антивірус. Майже всі ті функції, що раніше доводилось виконувати адміністратору самостійно. Приклад роботи програми наведений в рис. 1.

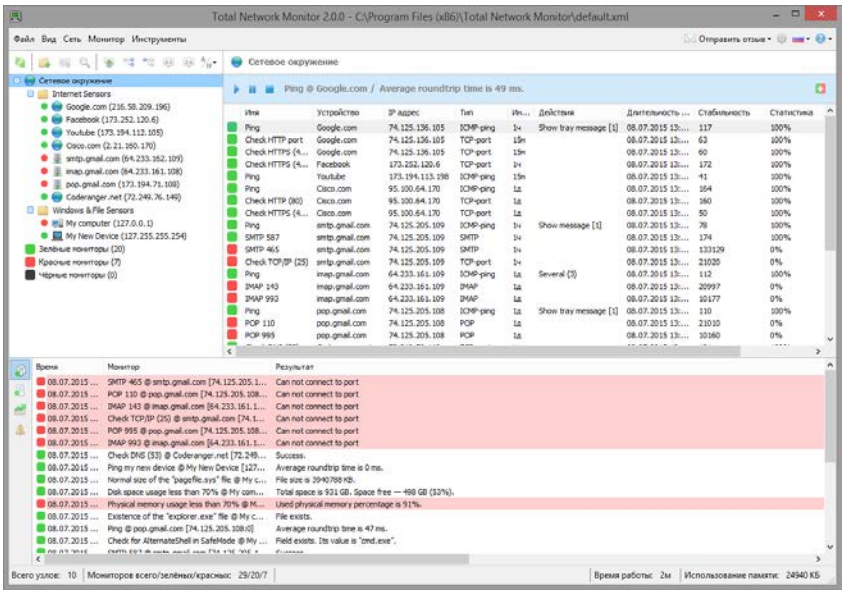

Рис. 1. Приклад функціювання ПЗ "Total Network Monitor 2"

До переваг даного програмного забезпечення можемо віднести:
a) Простий інтерфейс
b) Низька ціна
До недоліків належать:
a) Неможливість оновлення

2) Observium – програмне забезпечення яке засноване на використанні протоколу SNMP. Дозволяє "моніторити" стан мережі в реальному часі, аналізувати рівень продуктивності. Надає системним адміністраторам різні варіанти для налаштування. [9]

Крім того, адміністратори можуть в будь-який момент часу отримати доступ до даних характеристики обладнання, яке підключене до мережі. ПЗ може у вигляді графіків демонструвати слабкі сторони мережі. Приклад роботи даної програми наведений на рис. 2.

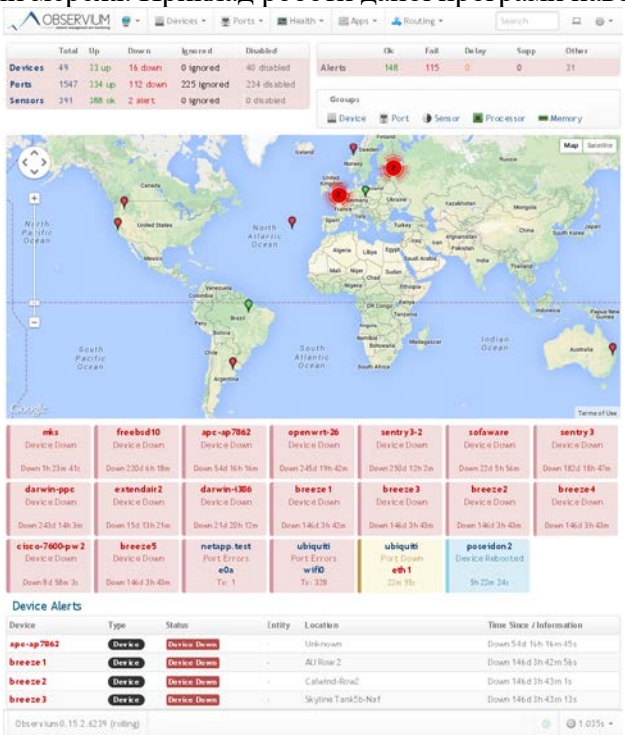

Рис. 2. Приклад роботи ПЗ "Observium"

До переваг даного програмного забезпечення можна віднести:

a) Автоматичне виявлення небезпек

b) Доступна безкоштовна версія

До недоліків належать:

a) Недоліки безкоштовної версії

b) Не призначене для малих мереж

3) Network Olympus – програмне забезпечення, що надає більшу гнучкість в роботі. Головною перевагою є конструктор сценаріїв, який надає змогу організувати схеми моніторингу будь-якої складності, для виявлення проблем та їх узгодження. Приклад роботи програми наведений на рис. 3.

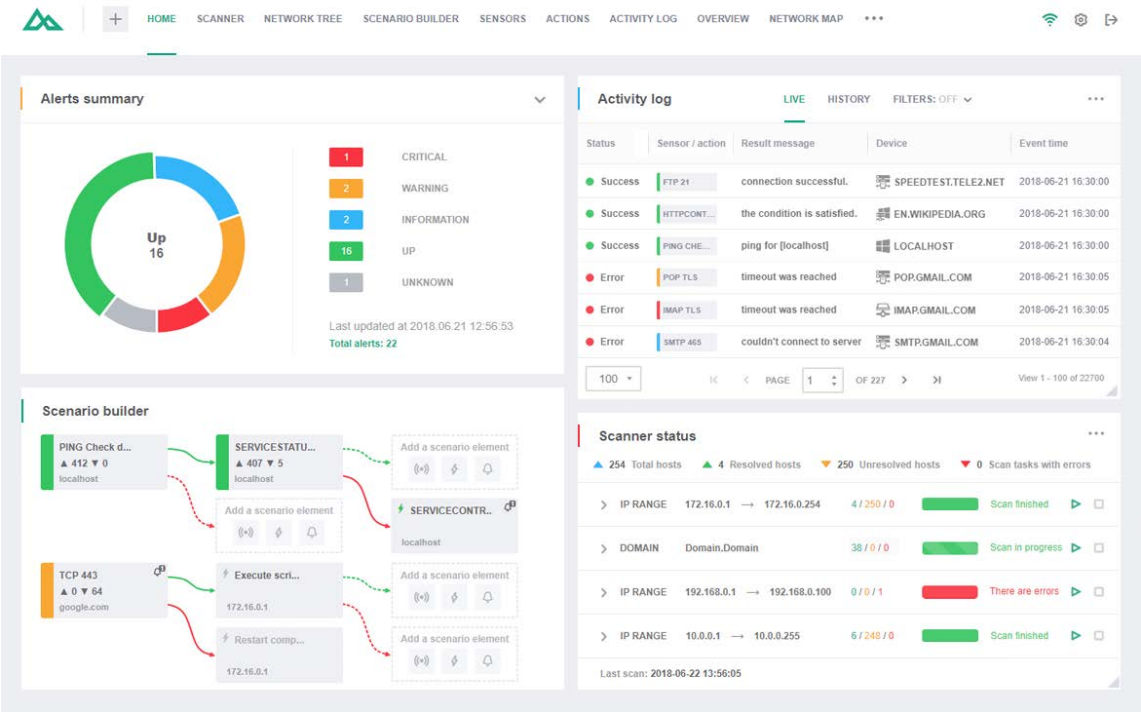

Рис. 3. Приклад роботи ПЗ "Network Olympus"

До переваг даного ПЗ можемо віднести:

a) Просте налаштування

b) Конструктор сценаріїв

До недоліків належать:

a) Відсутність багатокористувацького доступу

b) Призначене тільки для Windows

4) Zabbix – універсальне ПЗ для моніторингу з відкритим вихідним кодом, що дає змогу більш зручно налаштувати його під конкретну мережу. Надає можливість одночасно керувати сотнями мережевих вузлів. [10]

Крім того, дане програмне забезпечення надає набір інструментів для відстеження стану апаратної частини мережі. Приклад роботи програми наведений на рис. 4.

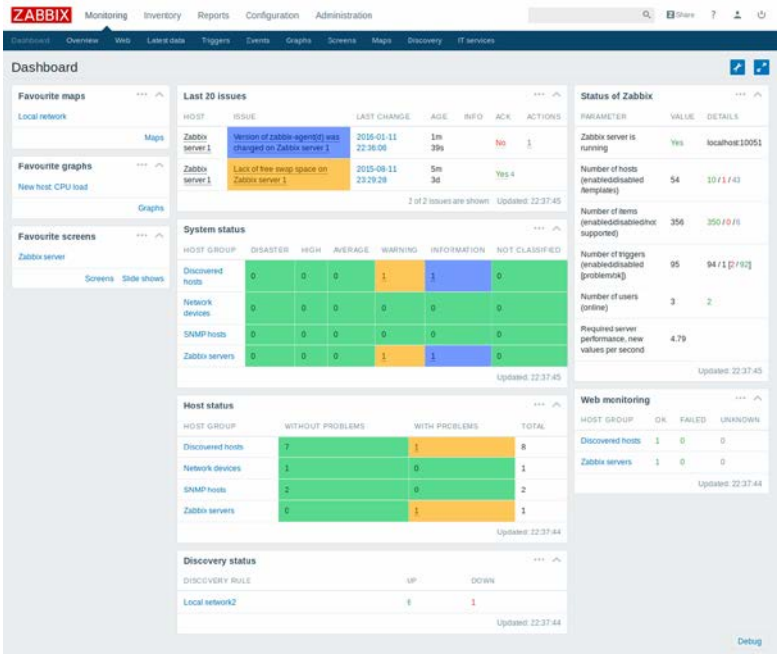

Рис. 4. Приклад роботи ПЗ "Zabbix"

До переваг даного ПЗ можемо віднести:

a) Безкоштовне

b) Велика кількість плагінів

До недоліків належать:

a) Не призначене для Windows

b) Громіздкий інтерфейс

c) Велике навантаження на комп'ютер

Висновки. Отже, аналізуючи сучасні проблеми, з якими стикаються власники комп'ютерних мереж та їх користувачі, можна сказати, що фокусування на адмініструванні та моніторингу є головною перспективою для покращення та оптимізації роботи КМ. І так як коректний моніторинг мережевої активності є головним параметром діяльності багатьох підприємств, слід звернути увагу на якісне ПЗ для адміністрування та моніторингу комп'ютерних мереж, кожна з яких має свої певні переваги та недоліки. Проаналізувавши кожну з них, є можливість вибрати певну ПЗ для вирішення певних задач які потребує мережа.

Список використаної літератури

1. Проблеми інформатизації та управління [Електронний ресурс]. – Режим доступу до ресурсу: http://jrnl.nau.edu.ua/index.php/PIU/article/view/7250/8135.
2. Інформаційна технологія моніторингу та аналізу трафіку у комп'ютерних мережах [Електронний ресурс]. – Режим доступу до ресурсу: https://docplayer.net/71333630-Informaciyna-tehnologiya-monitoringu-ta-analizu-trafiku-u-komp-yuternih-merezhah.html.
3. Системний адміністратор – Вікіпедія [Електронний ресурс]. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Системний_адміністратор.
4. Адміністрування мережі [Електронний ресурс]. – Режим доступу до ресурсу: https://hi-news.pp.ua/internet/10013-admnstruvannya-merezh-ce-scho-take.html.
5. Адмістрування мережі необхідне для забезпечення її ефективної роботи [Електронний ресурс]. – Режим доступу до ресурсу: https://studopedia.su/10_122752_administruvannya-merezhi.html.
6. Моніторингові програмні продукти – Вікіпедія [Електронний ресурс]. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Моніторингові_програмні продукти.
7. Топ програм для моніторингу мережі [Електронний ресурс]. – Режим доступу до ресурсу: https://www.softinventive.ru/best-network-monitoring-tools/.
8. Документація total network monitor [Електронний ресурс]. – Режим доступу до ресурсу:https://docs.softinventive.ru/tnm/rukovodstvo-pol-zovatelya/nastrojki.
9. Документація Observium [Електронний ресурс]. – Режим доступу до ресурсу: https://docs.observium.org/
10. Документація Zabbix [Електронний ресурс]. – Режим доступу до ресурсу: https://www.zabbix.com/ru/manuals

Стаття надійшла до редакції 09.12.2021
Статтю рекомендовано до друку 25.12.2021

References

1. Problemy informatyzatsii ta upravlinnia. Retrieved from: http://jrnl.nau.edu.ua/index.php/PIU/article/view/7250/8135.
2 Informatsiina tekhnolohiia monitorynhu ta analizu trafiku u kompiuternykh merezhakh. Retrieved from: https://docplayer.net/71333630-Informaciyna-tehnologiya-monitoringu-ta-analizu-trafiku-u-komp-yuternih-merezhah.html.
3. Systemnyi administrator – Vikipediia. Retrieved from: https://en.wikipedia.org/wiki/System_Administrator.
4. Administruvannia merezhi. Retrieved from: https://hi-news.pp.ua/internet/10013-admnstruvannya-merezh-ce-scho-take.html.
5. Admistruvannia merezhi neobkhidne dlia zabezpechennia yii efektyvnoi roboty. Retrieved from: https://studopedia.su/10_122752_administruvannya-merezhi.html.
6. Monitorynhovi prohramni produkty – Vikipediia. Retrieved from: https://en.wikipedia.org/wiki/Monitoring_program products.
7. Top prohram dlia monitorynhu merezhi. Retrieved from: https://www.softinventive.ru/best-network-monitoring-tools/.
8. Dokumentatsiia total network monitor. Retrieved from: https://docs.softinventive.ru/tnm/rukovodstvo-pol-zovatelya/nastrojki.
9. Dokumentatsiia Observium. Retrieved from: https://docs.observium.org/.
10. Dokumentatsiia Zabbix. Retrieved from: https://www.zabbix.com/ru/manuals.

The article was received by the editors 09.12.2021
The article is recommended for printing 25.12.2021

Oleksandr Tarasenko
Candidate of Technical Sciences, Associate Professor of the Department of ITMM of the Educational and Scientific Institute «Karazin Banking Institute» V.N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine,
e-mail: tap-top@ukr.net
Vladislav Khristoev
student of the Educational and Scientific Institute «Karazin Banking Institute» V.N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine;
e-mail: vladislav0572@gmail.com;
Danilo Aksynin
student of the Educational and Scientific Institute «Karazin Banking Institute»
V.N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine;
e-mail: daniilaksinin@gmail.com;

ADMINISTRATION AND MONITORING OF COMPUTER NETWORKS AS A METHOD OF SOLVING MODERN PROBLEMS IN FINANCIAL SYSTEMS

Abstract. The article defines the role of administration and monitoring of computer networks in financial systems. The main objectives of monitoring are network activities. Research analysis and task setting are to monitor traffic as an important source of information for effective network management, bringing the main functions of network administrators in financial systems. The effectiveness of monitoring using network traffic analyzers depends on the topology of the network under study, its configuration, and the set of devices from which the network is built. The result of the study in the form of two main needs is monitoring and analysis. Effective network management in the field of finance and banking systems, as well as continuous improvement of software in financial systems. What are the requirements for software agent technology? The main functions and tasks of network administration - a description of monitoring, its tools and network analysis, which are divided into certain classes: protocol analyzers (Protocolanalyzers), system management tools (System Management), network management systems (Network Management Systems), built diagnostic and management systems (Embedded Systems), multifunctional devices for analysis and diagnostics, equipment for diagnostics and certification of cable systems, expert systems. The main functions of monitoring and analysis of network activity in financial systems are in the form of 4 items: performance analysis, network accounting, security management, error handling. The main aspects for the development of software for monitoring network activity, the needs that arise during the work with the network, the peculiarities of the administration of these networks, analyzed the existing software for monitoring network activity in financial systems. An example of the use of software for the administration and monitoring of computer networks is a description of the capabilities and highlighting the advantages and disadvantages of these programs in financial systems. This article discusses the following software: Total Network Monitor 2, Observium, Network Olympus, Zabbix.

Keywords: *software, monitoring, aspect, network, administration, information protection, Internet communication, peripherals, configuration.*

Formulas: 4, bibl .: 7

JEL Classification: P34