УДК 378.147:004.713

НАВЧАННЯ МАЙБУТНІХ ПРОГРАМІСТІВ РОБОТІ ІЗ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ: ВИКОРИСТАННЯ SNMP ЯК ЗАСОБУ ДЛЯ ВЗАЄМОДІЇ ІЗ МЕРЕЖЕВИМ ОБЛАДНАННЯМ

Ірина Наумук, Олексій Наумук

Мелітопольський державний педагогічний університет імені Богдана Хмельницького

Анотація:
У сучасному світі, де інформація та комунікації відіграють ключову роль у розвитку бізнесу, ефективне управління мережею підприємства стає критично важливим фактором успіху. Мережа підприємства є складною системою, що складається з безлічі пристроїв і компонентів, які повинні працювати злагоджено і без збоїв. Одним із ключових елементів фізичної мережевої інфраструктури є керовані комутатори, які дозволяють організувати управління, фільтрацію та безпеку логічної частини мережі. У статті розглянуто процес розробки інструментів діагностики несправностей у роботі локальної мережі студентами-програмістами за допомогою мови програмування Python. Описано основні аспекти практичного застосування протоколу SNMP для створення програмних засобів, призначених для виявлення та усунення проблем у локальних мережах. Наведено приклади інструментів, що реалізують функції моніторингу мережевого трафіку, аналізу продуктивності, виявлення аномалій та гарантування безпеки мережі. Вибір протоколу для взаємодії з мережевими пристроями повинен враховувати найпоширеніші проблеми в їхній роботі, для діагностики яких необхідна наявність актуальних даних про наявність фізичного підключення, поточного стану порту, швидкості підключення, кількості вхідних та вихідних пакетів даних, пакетів даних з помилками. Висвітлено переваги використання Python, такі, як його простота, доступність великої кількості бібліотек та інструментів для мережевого програмування, що значно полегшує процес розробки та підвищує ефективність навчання.

Ключові слова:
комп'ютерна мережа; керовані комутатори; засоби діагностики; протокол SNMP; Python; EasySNMP; Django.

Resume:
Naumuk Iryna, Naumuk Oleksii. Teaching future programmers to work with computer networks: using snmp as a tool to interact with network equipment.
The authors of the article stresses that information and communication play a key role in business development, and effective management of business processes is a critical factor in success. The production process is a collapsible system, which consists of no devices and components that work smoothly and without failures. One of the key elements of the physical fencing infrastructure is the hardened switches, which are used for the management, filtering and security of the logical part of the fringe. The article examines the process of developing tools for diagnosing problems in a robot local network by student programmers using additional Python programming. The article describes the main aspects of the practical use SNMP for creating software features for identifying and solving problems in local networks. Applications of tools have been developed to implement the functions of monitoring border traffic, analyzing productivity, identifying anomalies and ensuring security of borders. The choice of protocol for interaction with edge devices is responsible for the most widespread problems in the operation of edge devices, for the diagnosis of which it is necessary to obtain up-to-date data on the presence of a physical connection, flow rate of the port, and connections, number of packages included. The advantages of Python have been highlighted, such as its simplicity, the availability of a large number of libraries and tools for edge-to-edge programming, which significantly facilitates the development process and promotes the effectiveness of the beginning.

Key words:
computer network; controlled switches; diagnostic methods; SNMP protocol; Python; EasySNMP; Django.

Постановка проблеми. У сучасних умовах функціонування комп'ютерних мереж забезпечення їхньої безперебійної та надійної роботи є критично важливим завданням. Збої та несправності у роботі локальних мереж можуть призводити до значних фінансових втрат та зниження продуктивності організацій. Тому питання своєчасного виявлення та усунення мережевих несправностей стає особливо актуальним.

Враховуючи наявність обладнання різних типів та виробників, взаємодія має здійснюватися за стандартним протоколом. Аналіз способів взаємодії дозволяє виокремити три основних напрямки, веб-інтерфейс, telnet і SNMP, враховуючи можливу необхідність організації доступу до даних тільки для читання, протокол SNMP є оптимальним. Нині існує безліч модулів, плагінів і розширень для різних мов програмування, тому вибір був зроблений на користь Python, оскільки він має досить широкий спектр різних бібліотек для взаємодії з мережевими пристроями за протоколом SNMP, обробки даних, підключення до різних баз даних і фреймворком Django, що дозволяє швидко розробляти веб-додатки. Слід також враховувати, що розроблений інструмент у більшості випадків працюватиме на пристроях від різних виробників, а в разі потреби може бути модифікований. Розробка подібних інструментів є актуальним та перспективним напрямом, оскільки розвиток та дослідження в галузі покращення мережевого обладнання не зупиняються. Однак підготовка фахівців у сфері мережевих технологій часто обмежується теоретичними знаннями без достатнього акценту на практичні навички. В результаті випускники навчальних закладів можуть не володіти необхідними інструментами та методами для ефективної діагностики й усунення несправностей у реальних умовах.

Мережева інфраструктура будь-якого підприємства – це сукупність технічних засобів та програмного забезпечення, призначених для обміну інформацією між комп'ютерами та іншими пристроями у межах організації. Вона забезпечує доступ до ресурсів, таких як дані, програми та інтернет, а також дозволяє співробітникам обмінюватися інформацією та співпрацювати

один з одним. Для ефективної роботи мережі необхідно забезпечити її надійність, безпеку та продуктивність. Це досягається шляхом правильного проектування, налаштування й керування мережевими пристроями.

Аналіз останніх досліджень і публікацій. Проблемою визначення причин збоїв та впровадження систем моніторингу IT-компонентів розглянуті у працях Ю. Хлапоніної та Г. Жирова, Н. Юрчук, Ю. Чернецької, А. Замулко. Проаналізовані дослідження спрямовані на вирішення проблеми шляхом впровадження системи моніторингу, можливості передбачити і запобігти збоям. Сучасні локальні мережі є основою функціонування багатьох організацій та підприємств, забезпечуючи доступ до інформаційних ресурсів і комунікацій. Однак збої та несправності у роботі мереж можуть призводити до значних проблем, зокрема зниження продуктивності, втрату даних та фінансові збитки. Виявлення та усунення цих несправностей є критично важливим завданням для забезпечення стабільної роботи мережі.

Формулювання цілей статті. Метою статті є розгляд процесу розробки інструментів діагностики несправностей у роботі локальної мережі студентами-програмістами за допомогою мови програмування Python. Описано основні аспекти практичного застосування протоколу SNMP для створення програмних засобів, призначених для виявлення та усунення проблем у локальних мережах. Наведено приклади інструментів, що реалізують функції моніторингу мережевого трафіку, аналізу продуктивності, виявлення аномалій та забезпечення безпеки мережі. Вибір протоколу для взаємодії з мережевими пристроями повинен враховувати найпоширеніші проблеми в роботі мережевих пристроїв, для діагностики яких необхідна наявність актуальних даних про наявність фізичного підключення, поточного стану порту, швидкості підключення, кількості вхідних та вихідних пакетів даних, пакетів даних з помилками. Висвітлено переваги використання Python, такі, як його простота, доступність великої кількості бібліотек та інструментів для мережевого програмування, що значно полегшує процес розробки та підвищує ефективність навчання.

Виклад основного матеріалу дослідження. На жаль, традиційні методи підготовки фахівців у галузі мережевих технологій часто не приділяють достатньо уваги практичним навичкам діагностики та усунення мережевих проблем. Випускники часто мають теоретичні знання, але не володіють необхідними інструментами та методами для ефективного вирішення реальних проблем у мережевій інфраструктурі. Тож основні компоненти мережі підприємства містять (Душко, & Петляк, 2023, с. 13):

- Сервери – потужні комп'ютери, на яких зберігаються дані та програми.
- Робочі станції – персональні комп'ютери або інші пристрої, з яких користувачі мають доступ до мережі.
- Мережне обладнання – маршрутизатори, комутатори та інші пристрої, які забезпечують передачу даних через мережу.
- Кабелі та мережеві адаптери – це фізичні засоби зв'язку між пристроями.

Комутатор – це пристрій, який з'єднує кілька комп'ютерів або інших мережних пристроїв у єдину мережу. Він виконує функцію «мосту» між ними, дозволяючи їм обмінюватися даними. Комутатори бувають різних типів та моделей, кожна з яких має свої особливості та переваги.

Основними функціями комутатора є (Переяслов, 2023, с. 10–12):

- Надсилання даних між підключеними пристроями.
- Фільтрування трафіку на основі MAC-адреса.
- Підтримка різних протоколів, таких як Ethernet, VLAN та QoS.
- Забезпечення безпеки мережі за допомогою таких функцій, як ACL і SSH.

Вибір відповідного комутатора залежить від розміру та вимог мережі підприємства. Для невеликих мереж можна використовувати некеровані комутатори, які не потребують налаштування та забезпечують базову функціональність. Для середніх та великих мереж краще вибрати керовані комутатори, які надають ширші можливості для налаштування, керування та діагностики мережі.

Проблеми, пов'язані з підключенням до локальної мережі, це ситуації, коли мережне з'єднання між двома пристроями переривається. Причиною зникнення лінка можуть бути різні фактори, такі як (Карпенко, & Макогон, 2019., с. 95–97):

- обрив або пошкодження кабелю;
- несправність мережного обладнання;
- проблеми із живленням;
- навантаження мережі.

Для діагностики та усунення проблем з пропаданням лінків можна використовувати такі методи (Задерейко, Задерейко, & Задерейко, 2020, с. 59):

- перевірка стану мережного обладнання (комутаторів, маршрутизаторів тощо);
- тестування кабелю на наявність ушкоджень;
- аналіз лог-файлів мережного устаткування виявлення можливих проблем.

У більшості випадків доступ до мережних комутаторів здійснюється кількома способами.

Для управління комутатором, використовуючи протокол Telnet, необхідно, щоб на комутаторі був налаштований IPv4 або IPv6 адресу та хост з Telnet-клієнтом був доступний з комутатора (перебував в одній мережі з ним або доступний через маршрутизатор).

Для керування комутатором, використовуючи HTTP (WEB-інтерфейс), необхідно, щоб на комутаторі було налаштовано IPv4 або IPv6 адресу і хост з HTTP-клієнтом був доступний з комутатора (перебував в одній мережі з ним або був доступний через маршрутизатор).

Для управління комутатором по SNMP необхідно щоб на комутаторі був налаштований IPv4 або IPv6 адресу і хост з SNMP клієнтом був доступний з комутатора (перебував в одній мережі з ним або був доступний через маршрутизатор). Враховуючи, що для діагностики проблем у роботі мережі необхідно швидко отримувати лише певний тип інформації та обмежити доступ до функцій управління ідеальним варіантом використання протоколу SNMP (Simple Network Management Protocol) (Голубничий, & Коцюба, 2022, с. 16).

SNMP – це стандартний протокол, який широко використовується для керування мережевими пристроями. SNMP протокол працює за технологією клієнт-сервера. Як сервер виступає SNMP Агент, що працює на керованих пристроях, наприклад, комутаторах. Як клієнт NMS (Network Management Station) станція управління мережею. На комутаторах SNR підтримується лише функція SNMP агента (Голубничий, & Коцюба, 2022, с. 15).

Обмін інформацією між NMS та SNMP агентом здійснюється шляхом надсилання стандартизованих повідомлень. У SNMP визначено 7 типів повідомлень: Get-Request, Get-Response, Get-Next-Request, Get-Bulk-Request, Set-Request, Trap, Inform-Request

NMS може надсилати наступні повідомлення Агенту: Get-Request, Get-Next-Request, Get-Bulk-Request та Set-Request. Агент відповідає повідомленням Get-Response. Також Агент може надсилати Trap повідомлення на NMS для інформування про події, наприклад, UP/DOWN порту тощо. Повідомлення Inform-Request використовується для обміну інформацією між NMS.

Вся інформація, що є у певному пристрої, структурована як База керуючої інформації (MIB, Management Information Base). Ця MIB застосовує ієрархічний простір імен, що містить певний ідентифікатор об'єкта (OID, Object IDentifier) і представляє інформацію, яка може бути зчитана і повернена стороні, що запитує. Таким чином, MIB визначає набір стандартних об'єктів для керованих пристроїв. Для перегляду бази MIB можна використовувати спеціалізоване програмне забезпечення за найменуванням MIB Browser. Так OID дерева ifEntry SNMP буде виглядати так (рис. 1).

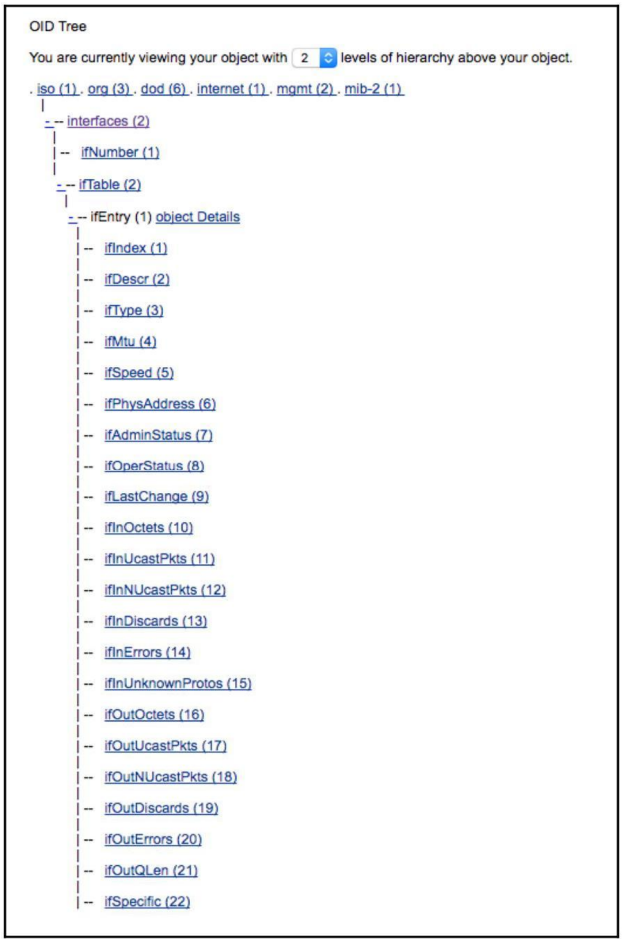

Рис. 1. Структура дерева ifEntry

MIB поділяються на громадські (public) та приватні (private). Public MIB визначаються RFC і є спільними для всіх Агентів, що підтримують їх, наприклад MIB для управління інтерфейсами – IF-MIB визначений в RFC 2863 (McCloghrie, & Kastenholz, 2000). Private MIB створюються виробниками обладнання і, відповідно, підтримуються тільки на обладнанні цього виробника.

Враховуючи типові проблеми з підключеннями до мережі та способи їхнього діагностування, можна визначити перелік даних, які необхідно отримувати від мережевого обладнання: стан порту (ifAdminStatus); статус порту (ifOperStatus), швидкість порту (ifSpeed), кількість октетів вхідних та вихідних пакетів даних (ifInOctets\ ifOutOctets), кількість октетів вхідних та вихідних пакетів даних з помилками (ifInErrors\ ifOutErrors), опис порту (ifAlias), опитування таблиці ARP (atPhysAddress).

Так для перевірки правильного налаштування можна виконати відповідний запит:

Snmpwalk – v 2c -c private 10.10.1.3 ifOperStatus

де – v 2c – 2 версія протоколу, -c private – ком'юніті, 10.10.1.3 – IP-адреса та значень поточного стану порту – ifOperStatus.

Як відповідь отримаємо список значень, підключено щось до порту в цей момент чи ні:

IF-MIB::ifOperStatus.1 = INTEGER: up (1)
IF-MIB::ifOperStatus.2 = INTEGER: up (1)
IF-MIB::ifOperStatus.3 = INTEGER: down (2)
IF-MIB::ifOperStatus.4 = INTEGER: up (1)
IF-MIB::ifOperStatus.5 = INTEGER: down (2)
IF-MIB::ifOperStatus.6 = INTEGER: down (2)
IF-MIB::ifOperStatus.7 = INTEGER: down (2)

Аналогічно відбувається отримання інших даних від мережевого устаткування. Однак формат, у якому надається відповідь, незручний і вимагає подальшої обробки, крім того, будь-яка мережа гетерогенна і може містити різні типи підключень, так і обладнання різних виробників, що значно ускладнює роботу з діагностування проблем. Таким чином, ще одним етапом є створення відповідних інструментів автоматизації, що дозволяють визначати тип пристрою й необхідний набір даних для створення запитів та декодування (Романов, & Нестеренко, 2012, с. 75).

Щоб отримати відповідь на запит про стан комутатора за протоколом SNMP, можна використовувати бібліотеку EasySNMP. Використання об'єкта Session найбільше підходить, коли планується запитувати клька фрагментів даних SNMP з джерела, або можна використовувати простий інтерфейс, призначений для одноразових операцій, коли ви хочете вказати всі деталі в запиті (Alawi S., Zahary A.).

```
def check_ports(host_ip, oid_dict):
    try:
        session = Session(
            hostname=host_ip, community="public",
version=2, timeout=1, retries=1
        )

        result = {}
        item_list = []
        for oid in oid_dict.values():
            item_list.append(oid)
        description = session.get(item_list)
        oid_value = []
        for item in description:
            oid_value.append(item.value)
        result = oid_value
    except:
        oid_value = []
        for oid in oid_dict:
            oid_value.append("0")
        result = oid_value
    else:
        result = oid_value
    return result
```

Рис. 2. Функція опитування комутатора

У випадку, якщо пристрій, до якого здійснюється звернення, не відповідатиме списку елементів, на виході функції матиме значення 0. Як параметри передаються IP-адреса комутатора, а також перелік SNMP OIDs. На виході буде сформовано відповідний список значень, який надалі може бути імпортований у текстовий файл або базу даних, для подальшої обробки та подання.

Django – це фреймворк, тобто набір готових інструментів та функцій. З його допомогою можна швидше та простіше реалізовувати на Python сайти та програми. Створення веб-сервісу на Python можливе і без Django, але тоді дуже багато доведеться писати і налаштовувати з нуля самостійно. Під час програмування на Django можна зосередитись лише на унікальних функціях веб-сервісу. Ось основні можливості, які дає цей фреймворк (Holovaty, & Kaplan-Moss, 2009; Forcier, Bissex, & Chun, 2008):

- Налаштовано веб-сервер, який обробляє запити від користувачів до веб-сервісу.
- Готові механізми авторизації користувачів.
- Прості шаблони веб-сторінок.
- Адміністративний інтерфейс для керування контентом сервісу – наповнення, зміни, оновлення даних, що використовуються.
- Система кешування для збільшення швидкості завантаження та відкриття сторінок через браузери, зовнішні клієнти або програми.
- Інтерфейси та адаптери для підключення до різних типів баз даних.

Використовуючи можливості фреймворку, створюються відповідні шаблони та уявлення, які при отриманні в якості параметра IP-адреса комутатора та всіх необхідних значень для опитування в залежності від моделі комутатора передаються в скрипт. Після того, як скрипт відпрацює дані, вони заносяться в базу даних і використовуються для формування сторінки з усією необхідною інформацією по кожному порту комутатора (рис. 3).

У цьому випадку при зверненні до обладнання користувач може отримати вичерпну інформацію про опис порту, стан порту (включено/вимкнено), статус порту, кількість пакетів, кількість пакетів з помилками, що може бути використане для діагностики та усунення проблем з підключенням до локальної мережі підприємства.

port	description	admin state	oper state	trafic In\Out
1	LIGHT	Off	down 100 Mbt/s	0 / 0
2	PORT_FLAP	Off	down 100 Mbt/s	0 / 0
3		On	Up 100 Mbt/s	673247400 / 559537185 erorrs: 151\0
4		On	down 100 Mbt/s	0 / 0
5		On	Up 100 Mbt/s	948711628 / 2747742371
6	LIGHT	Off	down 100 Mbt/s	0 / 0
7		On	Up 100 Mbt/s	632231418 / 1616680673
8		On	down 100 Mbt/s	0 / 0
9		On	down 100 Mbt/s	0 / 0

Рис. 3. Інтерфейс перевірки стану портів комутатора

Висновки. Таким чином, ефективність роботи мережі підприємства є ключовим фактором успіху в сучасному світі. Для цього необхідно забезпечити надійність, безпеку та продуктивність мережі. Одним із ключових елементів цієї системи є своєчасна діагностика та виявлення проблем у роботі обладнання.

Подальше вивчення теми може містити більш глибоке занурення в принципи роботи комутаторів, налаштування та управління ними, а також вивчення інших аспектів управління мережею підприємства, таких як безпека, доступність та відмовостійкість.

Список використаних джерел

Голубничий, Д.Ю., & Коцюба, В.П. (2022). *Застосування технологій моніторингу та аналізу стану IP-мережі на основі використання протоколу SNMP*.

Душко, Д.О., & Петляк, Н.С. (2023). Метод та система управління інформаційною безпекою підприємства // *Тези доповідей*.

Задерейко, О.В., Задерейко, О.В., & Задерейко, А.В. (2020). *Методичні вказівки до виконання лабораторних та самостійних робіт з дисципліни «Комп'ютерні мережі» для здобувачів вищої освіти галузі знань 12 «Інформаційні технології»*.

Карпенко, М.Ю., & Макогон, Н.В. (2019). *Конспект лекцій з курсу «Комп'ютерні мережі» (для студентів усіх форм навчання спеціальностей 122–Комп'ютерні науки, 151–Автоматизація та комп'ютерно-інтегровані технології, 126–Інформаційні системи та технології)*.

Переяслов, А.О. (2023). *Комутатор пакетів для локальної мережі* (дисертація). Сумський державний університет.

Романов, А.І., & Нестеренко, Н.Н. (2012). *Аналітична модель інтенсивності службового трафіку згідно SNMP-протоколу*. 2. С. 75.

Alawi S., Zahary A. Intrusion Inspector and Detector in Local Area Network using SNMP and MMC Techniques (IIDLAN).

Forcier J., Bissex P., Chun W.J. Python web development with Django. Addison-Wesley Professional, 2008.

Holovaty A., Kaplan-Moss J. The definitive guide to Django: Web development done right. Apress, 2009.

McCloghrie K. RFC 2863 The Interfaces Group MIB [Електронний ресурс] / K. McCloghrie, F. Kastenholz // The Internet Society. 2000. Режим доступу до ресурсу: https://2rfc.net/2863

References

Golubnychy, D.Yu., & Kotsiuba, V.P. (2022). Application of technologies for monitoring and analyzing the state of the IR network based on the use of the SNMP protocol. [in Ukrainian]

Dushko, D.O., & Petliak, N.S. (2023). Method and system of management of enterprise information security. Abstracts of reports, 11. [in Ukrainian]

Zadereyko, O.V., Zadereyko, O.V., & Zadereyko, A.V. (2020). Methodical instructions for performing laboratory and independent work in the discipline "Computer networks" for students of higher education in the field of knowledge 12 "Information technologies". [in Ukrainian]

Karpenko, M.Y., & Makogon, N.V. (2019). Synopsis of lectures on the course "Computer Networks" (for students of all forms of education, majors 122-Computer Science, 151-Automation and computer-integrated technologies, 126-Information systems and technologies). [in Ukrainian]

Pereyaslov, A.O. (2023). Packet switch for local network (Master's thesis, Sumy State University). [in Ukrainian]

Romanov, A.I., & Nesterenko, N.N. (2012). Analytical model of service traffic intensity according to the SNMP protocol. Issue 2, 75. [in Ukrainian]

Alawi, S., & Zahary, A. Intrusion Inspector and Detector in Local Area Network using SNMP and MMC Techniques (IIDLAN). [in English]

Forcier, J., Bissex, P., & Chun, W. J. (2008). *Python web development with Django*. Addison-Wesley Professional. [in English]

Golovaty, A., Kaplan-Moss, J. (2009). The Complete Guide to Django: Proper Web Development . Apress. [in English]

McCloughrey, C. and Kastenholtz, F. (2000). RFC2863: Interface Group MIB. [in English]

Відомості про авторів:
Наумук Ірина Миколаївна
naumuk_iryna@mspu.edu.ua
Мелітопольський державний педагогічний університет імені Богдана Хмельницького
Наукове Містечко, вулиця, 59, Запоріжжя, Запорізька обл., 69000, Україна

Information about the authors:
Naumuk Iryna Mykolaivna
naumuk_iryna@mspu.edu.ua
Bohdan Khmelnytsky Melitopol State Pedagogical University
Scientific Town, Street 59, Zaporizhzhia, Zaporizhzhia region, 69000, Ukraine

Наумук Олексій Володимирович
Мелітопольський державний педагогічний
університет імені Богдана Хмельницького
Наукове Містечко, вулиця, 59, Запоріжжя,
Запорізька обл., 69000, Україна

doi: 10.33842/22195203-2024-2-33-203-208

Матеріал надійшов до редакції 23. 08. 2024 р.
Прийнято до друку 12. 09. 2024 р.

Naumuk Oleksii Volodymyrovych
Bohdan Khmelnytsky Melitopol
State Pedagogical University
Scientific Town, Street 59, Zaporizhzhia,
Zaporizhzhia region, 69000, Ukraine

doi: 10.33842/22195203-2024-2-33-203-208

Received at the editorial office 23. 08. 2024.
Accepted for publishing 12. 09. 2024.