Список використаних джерел:

1. Дубко В. О. Стохастичні диференційні рівняння. Вибрані питання. Київ: Логос, 2012. URL: https://www.calameo.com/read/003168372374fa86544f4

2. Дубко В. О. Застосування індикаторних процесів при моделюванні та дослідженні показників систем із змінною структурою. *Вчені записки ТНУ ім. В. І. Вернадського. Серія: Технічні науки*. Том 36 (75) № 4 2025. Частина 2. С. 127–132.

3. Дубко В. О., Распопов В. Б. Дидактичні аспекти використання штучного інтелекту у викладанні математики студентам. *VI Міжнародна науково-практична конференція Таврійського національного університету імені В. І. Вернадського, до 107-ї річниці від дня заснування університету* (м. Київ, 16 жовтня 2025 р.). Львів – Торунь : Liha-Pres, 2025. URL: http://catalog.liha-pres.eu/index.php/liha-pres/catalog/book/443

DOI https://doi.org/10.36059/978-966-397-621-1-63

Киричек Г. Г.,
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних систем та мереж
Національного університету «Запорізька політехніка»
м. Запоріжжя, Україна

Тягунова М. Ю.,
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних систем та мереж
Національного університету «Запорізька політехніка»
м. Запоріжжя, Україна

Шлапік О. А.,
студент факультету комп'ютерних наук і технологій
Національного університету «Запорізька політехніка»
м. Запоріжжя, Україна

МЕТОД ДЕЦЕНТРАЛІЗОВАНОГО КЕРУВАННЯ КОМП'ЮТЕРНИМИ СИСТЕМАМИ

Об'єкти критичної інфраструктури є сукупністю систем, їх компонентів та взаємопов'язаних елементів [1], які мають ключове значення для забезпечення сталого функціонування економіки, національної

безпеки та обороноздатності держави [2], а порушення їх роботи здатне спричинити суттєву шкоду життєво важливим національним інтересам. В умовах сучасних воєнних загроз такі об'єкти зазнають підвищеного ризику ураження, що обмежує можливість постійної фізичної присутності персоналу, попри необхідність безперервного моніторингу та підтримки їх працездатності. Це зумовлює актуальність розв'язання науково-практичної задачі забезпечення безпечного функціонування об'єктів критичної інфраструктури із мінімізацією ризиків для життя та здоров'я обслуговуючого персоналу [3]. Метою роботи є підвищення надійності, безпеки та автономності процесів віддаленого керування об'єктами критичної інфраструктури шляхом розробки та реалізації децентралізованої системи доступу на основі оверлейної мережі з використанням відкритого програмного забезпечення. Об'єктом дослідження є процеси організації віддаленого доступу та керування комп'ютерними системами в умовах функціонування об'єктів критичної інфраструктури. Предметом є методи та засоби побудови децентралізованих систем віддаленого керування із застосуванням оверлейних мереж і програмних засобів віддаленого доступу. Основними завданнями є: проведення аналізу сучасних рішень віддаленого керування і визначення обмежень при застосуванні їх в критичних системах; формулювання вимоги до системи віддаленого керування з урахуванням критеріїв безпеки, відмовостійкості та незалежності від сторонніх сервісів; обґрунтування використання оверлейної мережі Yggdrasil для побудови децентралізованої архітектури; реалізація експериментальної моделі системи із застосуванням TigerVNC; перевірка працездатності і надійності системи; визначення перспектив її практичного застосування.

На сучасному етапі розвитку інформаційних технологій існує значна кількість програмних рішень для віддаленого доступу та керування комп'ютерними системами, зокрема AnyDesk, TeamViewer, RealVNC VNC Connect та GoToMyPC. Однак, попри простоту використання, вони характеризуються централізованою архітектурою, закритістю вихідного коду та наявністю платних або обмежених версій [4–5]. З огляду на зазначені обмеження, доцільним є підхід, за якого задача організації віддаленого керування розглядається як дві окремі підзадачі: забезпечення керування та організація доступу [6]. Реалізація підзадачі керування визначається архітектурними особливостями цільової системи. У випадку використання тонких клієнтів, як правило, вже застосовується відповідний протокол віддаленого доступу, зокрема SSH, VNC, RDP або NX, що зводить задачу до налаштування клієнтського програмного забезпечення та організації мережевого доступу [7–8]. У випадку товстих клієнтів із встановленням додаткового програмного забезпечення, функції керування реалізуються шляхом інсталяції відповідного серверного програмного забезпечення TigerVNC, яке забезпечує платформо незалежний доступ до графічного середовища робочого

столу. Таким чином, у загальному випадку задача організації віддаленого керування зводиться до побудови надійного та безпечного механізму доступу до відповідного сервера або керованого вузла, що реалізується із застосуванням мережевих та криптографічних технологій залежно від вимог до системи [9].

У роботі проведено аналіз сучасних програмних рішень віддаленого керування та встановлено їх обмеження при застосуванні в умовах об'єктів критичної інфраструктури: залежність від централізованих сервісів; обмежена прозорість механізмів безпеки та потенційна вразливість до відмов [10]. На основі отриманих результатів сформульовано вимоги до побудови надійної, відмовостійкої та безпечної системи віддаленого доступу. Запропоновано архітектурний підхід до реалізації системи віддаленого керування на основі децентралізованої оверлейної мережі Yggdrasil із використанням мобільних пристроїв, які підтримують протокол RNDIS та інфраструктури мобільних операторів зв'язку [11]. Для спрощення процесів розгортання і конфігурації клієнтських вузлів розроблено програмну утиліту YggVPN мовою C, яка забезпечує автоматизацію налаштування мережевої взаємодії та є сумісною із операційними системами сімейства Windows.

Практичну реалізацію запропонованого підходу для організації доступу до робочих станцій здійснено із застосуванням програмного забезпечення TigerVNC, а також для віддаленого керування мобільними пристроями застосовано droidVNC-NG. Взаємодію між компонентами системи забезпечено через публічні вузли мережі Yggdrasil, надійність яких підтверджено експериментальним шляхом у процесі тестування. При налаштуванні віддаленого керування у режимі модему телефон отримує IP адресу, яка є шлюзом за замовчанням. Це значення постійне і однакове для усіх версій Android та відкриває можливість звернення до телефону за цією адресою. На рисунку 1 наведено інтерфейс додатку droidVNC-NG.

Такі параметри використовуємо для віддаленого керування телефоном у разі необхідності. Для цього достатньо встановити на телефон droidVNC-NG, який є реалізацією VNC-сервера для Android і виконати перенаправлення портів за допомогою утиліти netsh. У додатку задаємо пароль для доступу, вмикаємо запуск при завантаженні системи та запускаємо службу. При першому запуску надаємо додатку дозволи додатків спеціальних можливостей.

Отримана система характеризується децентралізованою архітектурою, яка усуває єдину точку відмови та підвищує рівень відмовостійкості. Використання криптографічних механізмів оверлейної мережі та автентифікації VNC-серверів забезпечує належний рівень конфіденційності та захисту від несанкціонованого доступу. Додатковою перевагою є мобільність операторів і незалежність від конкретного каналу зв'язку, що дозволяє інтегрувати різнорідні мережеві середовища.

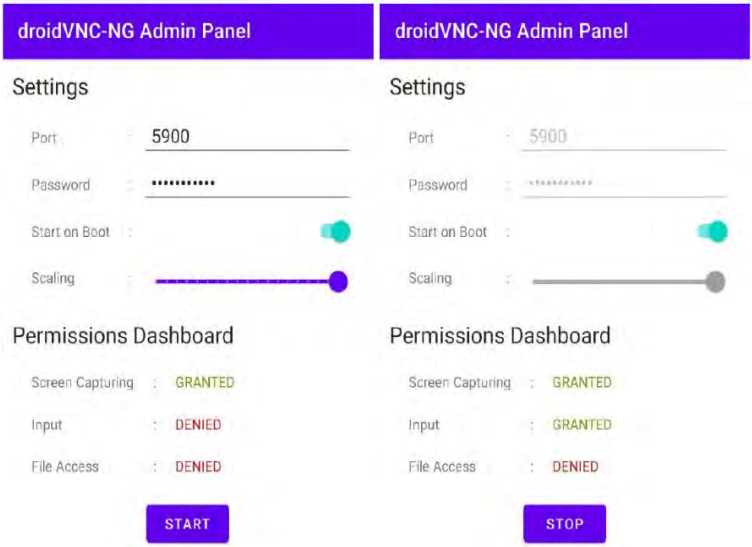

Рис. 1. Інтерфейс додатку

Таким чином, запропоноване рішення забезпечує ефективне поєднання безпеки, гнучкості та простоти експлуатації, що робить його придатним для використання у задачах віддаленого керування об'єктами з підвищеними вимогами до надійності та доступності.

Список використаних джерел:

1. Киричек Г. Г., Тягунова М. Ю., Братчиков В. В. Система кешування даних в розгалуженій мікросервісній архітектурі. *Вчені записки Таврійського національного університету ім. В. І. Вернадського. Серія: Технічні науки.* 2024. С. 141–146. DOI: https://doi.org/10.32782/2663-5941/2024.1.1/21

2. Конституція України : Закон України «Про критичну інфраструктуру» від 21.09.2024 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 25.03.2026).

3. Cheruvu S., Kumar A., Smith N., Wheeler D. M. IoT software security building blocks. In: Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment. Berkeley, CA: Apress, 2019. P. 213–346. DOI: https://doi.org/10.1007/978-1-4842-2896-8_4

4. Kirichek G., Tymoshenko V., Rudkovskyi O., Hrushko S. Decentralized System for Run Services. In: CMIS. 2019. P. 860–872. URL: https://ceur-ws.org/Vol-2353/paper68.pdf. (дата звернення: 25.03.2026).

5. Kothari K., Palwankar T., Dubey A., Parate P. Tor vs Yggdrasil: Comparative Study of Two Different Communication System. In 2022

International Conference on Inventive Computation Technologies (ICICT). IEEE. 2022. P. 452–456. DOI: https://doi.org/10.1109/ICICT54344.2022.9850965

6. Tang W., Han Y., Ai T., Li G., Yu B., Yang X. Yggdrasil: Reducing Network I/O Tax with (CXL-Based) Distributed Shared Memory. Proceedings of the 53rd International Conference on Parallel Processing. 2024. P. 597–606. DOI: https://doi.org/10.1145/3673038.3673138

7. Tanenbaum A., Wetherall D. Computer networks. Pearson, 2021. 944 p.

8. Kurose J., Ross K. Computer Networking: A Top-Down Approach, Global Edition. Pearson Education; 2018. 856 p.

9. TigerVNC. URL: https://tigervnc.org/ (дата звернення: 25.03.2026).

10. Киричек Г. Г., Пестов О. Д., Тягунова, М. Ю. Система віддаленого керування об'єктами критичної інфраструктури. *Системи та технології*. 2024, 68 (2). С. 63–70. DOI: https://doi.org/10.32782/2521-6643-2024-2-68.7

11. Yggdrasil Network. URL: https://yggdrasil-network.github.io/ (дата звернення: 25.03.2026).

DOI https://doi.org/10.36059/978-966-397-621-1-64

Морозюк А. В.,
студент ІІ курсу магістратури факультету інформаційних технологій Хмельницького національного університету
м. Хмельницький, Україна

КІБЕРФІЗИЧНА СИСТЕМА ПРОЦЕСУ НАВІГАЦІЇ ПРИ ВИЗНАЧЕННІ НЕСПРАВНИХ ВУЗЛІВ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Розвиток сучасних телекомунікаційних мереж супроводжується стрімким зростанням їх складності: типова корпоративна або операторська мережа охоплює сотні взаємопов'язаних вузлів різного призначення. Це маршрутизатори, комутатори, шлюзи безпеки, сервери прикладних сервісів, віртуальні машини та контейнеризовані компоненти. Тому будь-яке, навіть локальне порушення нормального функціонування вузла здатне спричинити каскадну деградацію сервісів, фінансові втрати та зниження рівня доступності критичних ресурсів [1].

Забезпечення стійкості та безперебійної роботи телекомунікаційних мереж особливої актуальності набуло натепер – в сучасних умовах воєнних загроз. Періодичні відключення електроенергії, підвищене