# КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

УДК 004.72
DOI https://doi.org/10.32782/2521-6643-2024-2-68.7

**Киричек Г. Г.,** кандидат технічних наук, доцент,
доцент кафедри комп'ютерних систем та мереж
Національного університету "Запорізька політехніка"
ORCID: 0000-0002-0405-7122

**Пестов О. Д.,** студент факультету комп'ютерних наук
та технологій
Національного університету "Запорізька політехніка"
ORCID: 0009-0002-6092-3301

**Тягунова М. Ю.,** кандидат технічних наук, доцент,
доцент кафедри комп'ютерних систем та мереж
Національного університету "Запорізька політехніка"
ORCID: 0000-0002-9166-5897

## СИСТЕМА ВІДДАЛЕНОГО КЕРУВАННЯ ОБ'ЄКТАМИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

*Стаття присвячена актуальному питанню забезпечення віддаленого керування об'єктами критичної інфраструктури в умовах активних бойових дій, коли вони постійно піддаються ракетним ударам та атакам. Авторами визначено основне завдання із підтримки працездатності віддаленого об'єкту, виключаючи ризики для персоналу, який цей об'єкт обслуговує та наведено етапи реалізації та впровадження системи, не виключаючи виникнення аварійних відключень електрики та інших надзвичайних ситуацій. В роботі розглянуто процес організації віддаленого керування автоматизованими об'єктами застосовуючи накладену P2P мережу Yggdrasil, а також моделі, методи і програмні засоби забезпечення віддаленого керування об'єктами. Враховано, що при застосуванні технології Yggdrasil, кожен вузол мережі звертається до іншого за його внутрішньою мережевою IPv6-адресою, а трафік між ними проходить через інші вузли поки не досягне адресата. Маршрутизація пакетів відбувається на основі координат дерева мережі, розподіленої за допомогою хеш-таблиць (DHT) та таблиць маршрутизації на кожному вузлі. У статті проаналізовано наявні готові рішення віддаленого керування, виявлено їх недоліки та запропоновано алгоритм реалізації віддаленого керування із використанням мережі Yggdrasil. З'ясовано, що в системі є доцільним: використання мобільних телефонів із підтримкою протоколу RNDIS; застосування мереж мобільних операторів зв'язку та спеціального програмного забезпечення на боці клієнта. Авторами, з метою спрощення встановлення і налаштування клієнта Yggdrasil на кінцевих пристроях під управлінням операційних систем Windows, на мові програмування C реалізовано конфігураційну утиліту YggVPN. Запропонований в статті варіант системи віддаленого керування впроваджено і перевірено із використанням клієнтського/серверного програмного забезпечення TigerVNC, яке застосовується на робочих місцях персоналу, та додатку droidVNC-NG, що використовується для віддаленого керування телефонами. Мережеві інструменти Yggdrasil і парольний захист серверів VNC забезпечують конфіденційність зв'язку і запобігають несанкціонованому доступу до об'єкта. Зв'язок з об'єктом здійснюється через Інтернет, завдяки чому забезпечується мобільність віддалених операторів і робочих місць.*

Ключові слова: *мережа, система, клієнт, протокол, телефон, керування.*

***Kyrychek H. H., Pestov O. D., Tiahunova M. Yu. Remote control system of critical infrastructure objects***

*The article is devoted to the topical issue of providing remote control of critical infrastructure facilities in conditions of active hostilities when they are constantly exposed to missile strikes and attacks. The authors define the main task of maintaining the functionality of a remote object, excluding risks for the personnel that this object serves, and the stages of implementation and implementation of the system are given, not excluding the occurrence of emergency power outages and other emergencies. The paper considers the process of organizing remote control of automated objects using the Yggdrasil P2P network, as well as models, methods, and software for providing remote control of objects. It is taken into account that when applying Yggdrasil technology, each network node addresses another by its internal network IPv6 address, and the traffic between them passes through other nodes until it reaches the destination. Packet routing is based on the coordinates of the network tree distributed*

*using hash tables (DHT) and routing tables at each node The article analyzes available ready-made remote control solutions, identifies their shortcomings, and proposes an algorithm for implementing remote control using the Yggdrasil network. It has been found that the following is appropriate in the system: the use of mobile phones with support for the RNDIS protocol; application of networks of mobile communication operators and special software on the client side. The authors, to simplify the installation and configuration of the Yggdrasil client on end devices running Windows operating systems, implemented the YggVPN configuration utility in the C programming language. The version of the remote control system proposed in the article is implemented and tested using the client/server software TigerVNC, which is used at staff workplaces, and the droidVNC-NG application, which is used for remote control of phones. Yggdrasil network tools and password protection of VNC servers ensure communication confidentiality and prevent unauthorized access to the object. Communication with the object is carried out via the Internet, thereby ensuring the mobility of remote operators and workplaces.*

Key words: *network, system, client, protocol, telephone, control.*

**Постановка проблеми.** Задача підтримки працездатності віддаленого об'єкту із мінімальними ризиками для персоналу, який його обслуговує, є актуальною у сучасних реаліях і умовах проведення активних бойових дій, коли об'єкти критичної інфраструктури піддаються ракетним ударам та атакам [1]. При цьому це є системи, або частини цих систем чи їх сукупність, які є надзвичайно важливими для економіки, національної безпеки і оборони, тому порушення їх функціонування завдає проблем національним інтересам [2]. До таких об'єктів зазвичай відносять електричні (атомні) станції та підстанції, аеродроми, залізничні вузли, військові об'єкти, медичні заклади, тощо [1, 2].

Спираючись на це, потрібно відрізняти між собою засоби віддаленого доступу і віддаленого керування. Під віддаленим доступом до об'єкту розуміємо лише організацію зв'язку між ним та віддаленим робочим місцем, тоді як віддалене керування є процесом спостереження та безпосереднього впливу оператора на віддалений об'єкт за допомогою спеціальних програмних та апаратних засобів [3]. Найчастіше для здійснення віддаленого керування об'єктом необхідно мати, як мінімум, віддалений доступ до нього. Тому логічно припустити, що віддалене керування застосовується лише для автоматизованих систем. Автоматизованим (комп'ютеризованим) об'єктом інфраструктури вважаємо об'єкт, робота якого відбувається за допомогою пристрою під управлінням операційної системи із спеціальним програмним забезпеченням [4]. Подібні автоматизовані робочі місця персоналу, зазвичай, є товстими або тонкими клієнтами.

Товстими клієнтами у цьому випадку є пристрої, до яких безпосередньо підключаються усі підсистеми, які потрібно контролювати [4]. Програмне забезпечення, для кожної конкретної системи, є специфічним і тому немає можливості встановлювати якесь стороннє програмне забезпечення [5]. Це, зазвичай, ускладнює задачу віддаленого керування та примушує використовувати зовнішні апаратні засоби, наприклад такі, як KVM-over-IP комутатори. Тонкі ж клієнти, за допомогою мережевих з'єднань, лише надають об'єкту доступ до сервера, який і контролює підключені до нього підсистеми [3]. Сам доступ, при цьому, здійснюється засобами мережевого програмного забезпечення, яке, відповідно, встановлюється на клієнті та сервері. Тому не важливо, яким є це програмне забезпечення, оскільки запуск процесу віддаленого керування об'єктом спирається на просте встановлення цього ж програмного забезпечення на віддалене робоче місце та організації зв'язку між клієнтом та сервером [5].

**Аналіз останніх досліджень та публікацій.** Поводячи аналіз готових програмних рішень, які на даний час можуть забезпечувати як віддалений доступ так і віддалене керування об'єктами інфраструктури, можемо приділити особливу увагу наступним, що найбільш часто застосовуються для вирішення подібних завдань: AnyDesk, Team Viewer, RealVNC VNC Connect та GoToMyPC [6, 7]. Усі ці програмні рішення прості у налаштуванні і часто вимагають тільки доступу до відкритої (глобальної) мережі, але їм характерні ряд недоліків, це: централізованість; закритість вихідного коду; не мають безкоштовних версій для комерційного використання та/або обмеження безкоштовної версії [3].

При цьому централізованість означає, що при використанні одного з таких рішень доводиться стикатися з певними умовами та обмеженнями конкретної компанії та застосовувати тільки її серверне програмне забезпечення, що, зазвичай може стати єдиною точкою відмови. Також закритий вихідний код, в свою чергу, практично унеможливлює відчуття підтримки конфіденційності зв'язку з об'єктом та відсутності втручання сторонніх осіб, що ставить під сумнів безпеку самого об'єкту [7].

В якості альтернативи розглянемо систему MeshCentral, яка є повноцінним, функціонально незалежним рішенням віддаленого керування, що використовує відкритий вихідний код для серверної і клієнтської частин системи [6]. Також вона є безкоштовною і дозволяє розгортати серверну частину на власному пристрої, до якого підключаються керовані об'єкти та віддалені робочі місця. При цьому керування підконтрольним об'єктом здійснюється з використанням вебінтерфейсу серверної частини, або за допомогою утиліт, а зв'язок між ними підтримується утилітою MeshRouter, шляхом перенаправлення портів. Увесь трафік є зашифрованим за замовчанням. Кінцеві користувачі реєструються адміністратором, автентифікація здійснюється за логіном та паролем із можливістю застосування при підключенні додаткової двофакторної автентифікації та апаратних ключів [6]. Використання MeshCentral вирішує проблеми, пов'язані із використанням закритого вихідного коду але потребує, для розгортання системи, застосування або власного серверу

з відкритою IP-адресою, або оренди віртуального приватного сервера (VPS), що зазвичай потребує фінансових витрат. До того ж проблема централізованості залишається, бо сервер є єдиною точкою відмови системи. При цьому ситуація погіршується, якщо сервер розміщено на території країни і він знаходиться в зоні виникнення постійних аварійних ситуації [3].

Оскільки існуючі готові рішення потребують значних фінансових вкладень або є недостатньо надійними, процес організації віддаленого керування розбиваємо на менші за об'ємом задачі керування та організації доступу до об'єкту. При цьому вирішення задачі керування віддаленим об'єктом залежить від структури керованої системи (рис. 1).


Рис. 1. Віддалене керування

Якщо, як основа системи, застосовується тонкий клієнт то в системі, скоріш за все, вже використовується потрібний протокол віддаленого керування, один з: SSH, VNC, RDP, NX або інший спеціальний протокол обміну даними з сервером. Тому залишається тільки вирішити задачу доступу та установити спеціальне програмне забезпечення тонкого клієнта на віддалене робоче місце [8].

Якщо розглядати можливість використання стороннього програмного забезпечення при застосуванні товстого клієнта, то процес керування забезпечується встановленням відповідного серверного додатку із підтримкою одного з спеціальних протоколів, наприклад, TigerVNC, який є функціонально незалежним VNC-сервером та клієнтом, що підтримує відкритий вихідний код і забезпечує контроль над робочим столом сервера [7]. Якщо товстий клієнт не надає можливість встановлювати стороннє програмне забезпечення, то єдиним рішенням є встановлення та застосування зовнішнього пристрою, наприклад, комутатора KVM-over-IP, який емулює пристрої вводу/виводу і, водночас, є сервером, який підтримує спеціальні протоколи для віддаленого керування об'єктом [9]. Тому, в даному випадку, основним завданням є організація доступу віддаленого робочого місця до сервера [10].

Щоб забезпечити мобільність для операторів, які керують віддаленими об'єктами, потрібно забезпечити їм доступ до об'єкту інфраструктури через відкриту мережу, але реалізація такого доступу є достатньо складною і відповідальною. Навіть, якщо у об'єкта вже є вихід у глобальну мережу, скоріше за все, він знаходиться за пристроєм відповідного провайдера, який використовує технологію NAT. Тому, пристрої з приватними локальними адресами створюють вихідні з'єднання з кінцевими пристроями у глобальній мережі, але зворотні з'єднання підтримувати не можуть, бо пристрій за NAT не має унікальної відкритої адреси для встановлення зворотного зв'язку. Це можна вирішити застосуванням статичної відкритої IP-адреси, але ця послуга, у більшості провайдерів потребує сплати. Крім цього, для обходу NAT можна застосувати власний виділений VPN-сервер, хоча він також вимагає відкритої IP-адреси або VPS-хостингу і найчастіше має проблему централізованості [3].

Альтернативою VPN-серверу вважаємо P2P-мережу Yggdrasil, яка працює поверх протоколу IP. У випадку застосування технології Yggdrasil, кожен вузол мережі звертається до іншого за його внутрішньою мережевою IPv6-адресою, а трафік між ними проходить через інші вузли поки не досягне адресата [11]. Цій мережі властиві самоконфігурація та децентралізованість бо адреса, кожним вузлом, формується як частина хеш-суми відкритого ключа, яка випадково згенерована асиметричною парою ключів [5]. Маршрутизація пакетів відбувається на основі координат дерева мережі, розподіленої за допомогою хеш-таблиць (DHT) та таблиць маршрутизації на кожному вузлі. Перед відправленням увесь трафік мережі шифрується відправником і може бути розшифрований лише отримувачем, що і гарантує постійну підтримку конфіденційності зв'язку [8].

Вузли однієї локальної мережі знаходять один одного автоматично, використовуючи multicast-розсилку. Вузли, які розташовані за пристроєм, який підтримує NAT, підключаються до мережі через однин або декілька публічних вузлів, тому з точки зору самого NAT, подібне з'єднання завжди є вихідним [12]. Саме ця перевага технології Yggdrasil використовується для того щоб обійти NAT обмеження та встановити зв'язок

з віддаленим об’єктом. При цьому зв’язок працює стабільно поки хоча б один публічний вузол є доступним. Все це підвищує надійність подібної системи порівняно з централізованими рішеннями. Клієнт Yggdrasil також є функціонально незалежним та має відкритий вихідний код [9]. Але окрім переваг така мережа може мати і недоліки до яких відносять незручність використання довгих IPv6-адрес та відсутність вбудованого фаєрволу, що обмежує доступу до кінцевого об’єкту. Проблему довжини адрес можна вирішити різними методами [5], або компенсувати використанням файлу hosts, який підтримується операційними системами і дозволяє поставити у відповідність логічним адресам зручні символьні імена. А для фільтрації трафіку можна застосовувати сторонні засоби, наприклад фаєрвол ip6tables в системах Linux або політики безпеки IPsec в системах Windows [4]. До того ж, оскільки адреси формуються криптографічно, у якості одного з кроків організації безпеки, разом з парольним захистом можна використовувати фільтрацію трафіку за адресою джерела. Але при наявності лише одного каналу зв’язку це стає єдиною точкою відмови, погіршуючи надійність всієї системи. Тому, для зберігання постійного доступу, необхідно мати резервні шляхи у відкриту мережу. Такі з’єднання надають мережі мобільних операторів зв’язку, підключення до яких можна організувати за допомогою локальних робочих місць віддаленого об’єкту, до яких підключаються або USB-модеми або звичайні мобільні телефони із підтримкою протоколу RNDIS, який дозволяє пристрою емулювати мережевий інтерфейс Ethernet поверх інтерфейсу USB [13].

**Постановка завдання.** Метою дослідження є реалізація та впровадження системи, яка призначена для віддаленого керування об’єктами критичної інфраструктури, враховуючи умови проведення активних бойових дій не виключаючи виникнення аварійних відключень електрики та інших надзвичайних ситуацій. Об’єктом дослідження є процес організації віддаленого керування автоматизованими об’єктами застосовуючи накладену P2P мережу Yggdrasil. Предметом дослідження є моделі, методи і програмні засоби забезпечення віддаленого керування об’єктами. В роботі потрібно проаналізувати готові рішення, які на даний час використовуються для віддаленого керування, визначити їх недоліки та запропонувати алгоритми та способи реалізації системи віддаленого керування із використанням сучасних методів та технологій. При цьому в системі планується використання мобільних засобів зв’язку з підтримкою потрібних протоколів, застосування мереж мобільних операторів та спеціального програмного забезпечення на боці клієнта. З метою спрощення процесів установлення і налаштування клієнтів на кінцевих пристроях планується, використовуючи мову програмування C, реалізувати утиліту конфігурації. Процеси роботи системи віддаленого керування потрібно протестувати із використанням клієнтського/серверного програмного забезпечення, яке потребує застосування на робочих місцях обслуговуючого персоналу та додатку, який планується застосовувати в процесі віддаленого керування телефонами.

**Виклад основного матеріалу.** Структуру наявної системи об’єкту наведено в першій частині рисунку 2. Керування підсистемами об’єкту здійснюється кінцевим пристроєм PC0 з робочих місць PC1, PC2 та PC3, які, у даному випадку є тонкими клієнтами при керуванні об’єктом PC0. В системі використовується KVM-over-IP комутатор, який підключено до об’єкту PC0 інтерфейсом VGA з метою отримання зображення та портом USB для емуляції миші і клавіатури. KVM-over-IP комутатор та робочі місця PC з першого по третій з’єднані у мережу за технологією FastEthernet інтерфейсу комутатора S1. Оскільки мережа, в якій розташовано сам об’єкт, є ізольованою від відкритої мережі, для підтримки віддаленого доступу потрібно в першу чергу забезпечити виходи у глобальну мережу. Як раз із цією метою і використовуємо три мобільні телефони під управлінням системи Android. Для підтримки високої надійності та оптимізації роботи системи, телефони використовують з’єднання через різних мобільних операторів зв’язку (Vodafone, Kyivstar, Lifecell). Вони підключаються до робочих місць за допомогою USB-to-microUSB кабелів. При цьому у налаштуваннях системи Android потрібно в ручну увімкнути режим модему (USB tethering). Таким чином на пристроях з’явиться мережевий адаптер із підтримкою технології Ethernet, що має назву Remote NDIS based Internet Sharing Device.

Із списку публічних вузлів мережі Yggdrasil, який наведений на сайті https://publicpeers.neilalexander.dev/ можна обрати потрібні, або ознайомитись із доступними. Хоча список містить лише ті вузли, які є доступними, його зручно використовувати при підключенні до мережі завдяки отриманню і іншій інформації про потрібні, або доступні вузли, а саме: географічному розташуванні вузла (у якій країні); необхідній версії клієнта; статусу вузла, який оновлюється щогодини (онлайн/офлайн) та орієнтовній надійності.

Для досліджуваної системи обрано чотири публічних вузла, вони відмічені як “reliable”: tls://193.111.114.28:1443 (Україна); tls://54.37.137.221:11129 (Польща); tcp://193.107.20.230:7743 (Німеччина); tls://185.165.169.234:8443 (Румунія). Ці вузли розташовано географічно віддалено один від одного, але вони є найближчими до об’єкту, з метою зменшення ймовірності їх одночасної відмови та мінімізації затримки. Для перевірки надійності вузлів створено bash-скрипт, який кожні 30 секунд перевіряє з’єднання з потрібним вузлом, пересилаючи йому ICMP-пакет. Якщо відповідь не отримана впродовж перших 20 секунд, система фіксує відсутність зв’язку. Інформація про активність вузла записується у файл.CSV, який в подальшому використовується для побудови графіку доступності. Окрім цього формується файл із параметрами перевірки зв’язку, а саме кількістю відправлених та отриманих пакетів. Процес завершується тільки після зупинки його користувачем.

В підсумку маємо, що протягом двох тижнів не відбулося жодної одночасної відмови всіх обраних публічних вузлів, з чого робимо висновок про їх достатню надійність. В другій частині рисунку 2 наведено структуру логічних з'єднань системи (маршрутів пересилання даних), де: PC є тонкими клієнтами; PP є обраними публічними вузлами, а RPC є віддаленими робочими місцями.

Маючи доступ у глобальну мережу, встановлюємо на локальні робочі місця серверну частину TigerVNC маючи за мету забезпечити, при необхідності, віддалене керування самими робочими місцями [7]. У контрольній панелі TigerVNC налаштовується пароль підключення до робочого місця. Також у вкладці Inputs потрібно увімкнути опцію Send raw keyboard events to applications. При цьому застосовувати окремо шифрування самого з'єднання не потрібно, оскільки всі з'єднання в мережі Yggdrasil підтримують шифрування за замовчанням [11]. З метою встановлення і налаштування клієнту мережі Yggdrasil використовуємо реалізовану утиліту YggVPN.

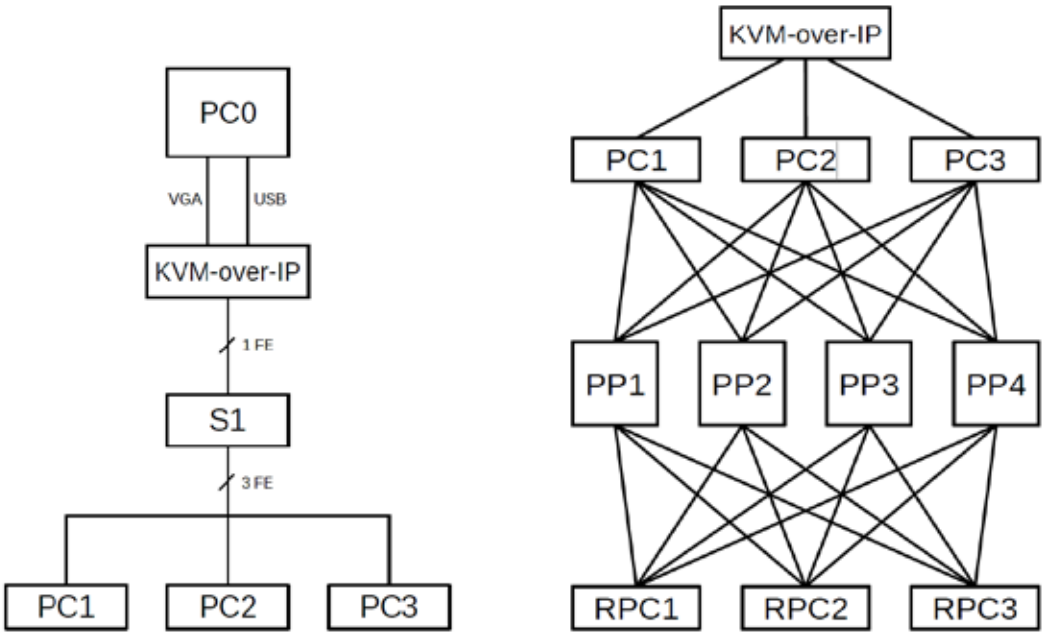


Рис. 2. Структура системи об'єкту та маршрутів пересилання даних

При цьому враховуємо, що деяке антивірусне програмне забезпечення може помилково сприймати її як загрозу, тому перед активуванням цю утиліту потрібно додати до списку винятків. При виконанні утиліти YggVPN на першому робочому місці, вводимо адреси обраних публічних вузлів та ім'я цього робочого місця – pc1.ygg. Далі всі кроки налаштування експортуються у файл yggvpn_export.conf, використовуючи команду "ec" і утиліта закривається командою "q". Налаштування другого робочого місця виконується аналогічно, але вже з файлом конфігурації, який експортується з налаштуваннями першого робочого місця. Тому вже не потрібно вводити адреси публічних вузлів, лише ім'я другого робочого місця – pc2.ygg та команду для експорту налаштувань. Аналогічним чином за допомогою yggvpn_export.conf з PC2 налаштовується і третє робоче місце. Таким чином, експортований файл конфігурації використовується для налаштування усіх віддалених робочих місць. Для того, щоб забезпечити надійне з'єднання з комутатором KVM-over-IP, використовуючи локальні робочі місця, на всіх PC необхідно налаштувати перенаправлення з локального порту 5990 на порт 5900 для всіх вхідних IPv6-з'єднань комутатора, використовуючи стандартний порт VNC та, наприклад, адресу 192.168.1.100. Для цього застосовуємо системну утиліту nesth і команду, яку слід виконувати від імені адміністратора:

netsh interface portproxy add v6tov4 listenport=5990 onnectaddress=192.168.1.100 connectport=5900

Якщо телефон при цьому отримує, наприклад, адресу 192.168.42.129 вона і буде використовуватися у якості шлюзу за замовчанням. Це значення є постійним і однаковим для усіх версій системи Android, що надає та підтримує можливість звернення до самого телефону за цією адресою. У разі необхідності цю можливість можна використати при віддаленому керуванні телефоном, для цього достатньо встановити на нього додаток droidVNC-NG (рис. 3), який є реалізацією VNC-сервера для системи Android [16], а також виконати перенаправлення портів за допомогою утиліти netsh.

У додатку задається пароль доступу, потім потрібно увімкнути запуск і при завантаженні системи запустити потрібну службу. Зауважте, що при першому запуску надаємо дозволи додатків спеціальних можливостей (Accessibility).

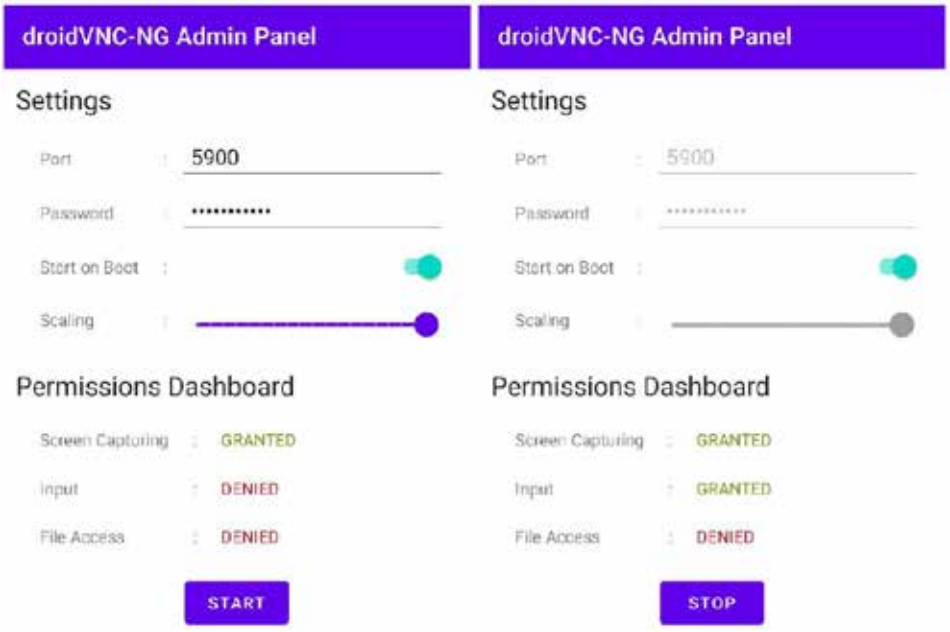


Рис. 3. Інтерфейс додатку droidVNC-NG

Далі наведемо команду для перенаправлення IPv6-з'єднань для порту 5909 кінцевого пристрою на порт 5900 підключеного телефону (192.168.42.129):

netsh interface portproxy add v6tov4 listenport=5909 connectaddress=192.168.42.129 connectport=5900

Віддалене керування об'єктом здійснюється із трьох віддалених робочих місць під управлінням системи Windows. Клієнт мережі Yggdrasil на них встановлюється та налаштовуються з використанням останнього експортованого файлу конфігурації. При додаванні потрібного робочого місця до системи, його Yggdrasil адресу вносимо до списку хостів на кожному із вже підключених локальних робочих місць за допомогою утиліти YggVPN. Потім достатньо встановити клієнт TigerVNC та перевірити з'єднання з об'єктом, використовуючи імена робочих місць та номери портів.

Структуру налаштованої системи наведено на рисунку 4, де додатково: P є мобільними телефонами; а CBS є базовою станцією коміркового зв'язку.

Для перевірки роботи системи виконуємо підключення до робочого столу першого робочого місця із одного з інших віддалених робочих місць. Для цього на клієнті TigerVNC вводимо адресу pc1.ygg:5900 та обираємо Connect. Далі вводимо попередньо встановлений пароль доступу. За портом 5990 отримуємо доступ безпосередньо до керованого об'єкту PC0 використовуючи комутатор KVM-over-IP. Також за портом 5909, аналогічним чином, можемо отримати доступ до першого телефону. Для інших віддалених об'єктів та локальних робочих місць результати перевірки є аналогічними. При цьому, навіть при зникненні з'єднання із відкритою мережею у двох із трьох локальних робочих місць, вони все одно будуть доступними завдяки автоматично організованого зв'язку між клієнтами Yggdrasil, завдяки маршруту через третє робоче місце.

Наведені результати дозволяють зробити висновки, що засобами мережі Yggdrasil із захистом VNC-серверів забезпечується конфіденційність зв'язку та виключається несанкціонований доступ до віддаленого об'єкту.

**Висновки.** У роботі проведено дослідження актуальних на сьогодні методів та алгоритмів реалізації систем віддаленого керування, виявлено їх недоліки та запропоновано варіант реалізації віддаленого керування об'єктом критичної інфраструктури використовуючи накладену децентралізовану мережу Yggdrasil. В процесі виконання роботи авторами проаналізовано наявні готові рішення, визначено вимоги до системи віддаленого керування об'єктом і запропоновано її реалізацію через Yggdrasil при використанні мобільних телефонів із підтримкою протоколу RNDIS та мереж мобільних операторів зв'язку, а також спеціального клієнтського програмного забезпечення. Для оптимізації процесу коректного встановлення та налаштування клієнта мережі Yggdrasil на кінцевих пристроях, мовою C реалізовано конфігураційну утиліту YggVPN, яку також можна використовувати і поза сценарієм віддаленого керування інфраструктурним об'єктом. Тестований екземпляр системи реалізовано на конкретному прикладі з використанням клієнтського/серверного програмного забезпечення TigerVNC для робочих місць та додатку droidVNC-NG для віддаленого керування телефонами. Для забезпечення зв'язку робочих місць з віддаленим об'єктом обрано чотири публічні вузли мережі Yggdrasil. Надійність вузлів протестована шляхом перевірки зв'язку протягом наведеного часу. Усі залучені програмні компоненти мають відкритий вихідний код. Система є децентралізованою – для

віддаленого керування об’єктом достатньо мати в доступі публічний вузол та одне віддалене і локальне робоче місце. Засобами мережі Yggdrasil та парольним захистом VNC-серверів забезпечується конфіденційність зв’язку та виключається несанкціонований доступ до об’єкту. Зв’язок з об’єктом здійснюється через глобальну мережу, тим самим забезпечуючи мобільність віддалених операторів та робочих місць, при цьому система підтримує будь-які додаткові канали зв’язку самого об’єкта через мережу.

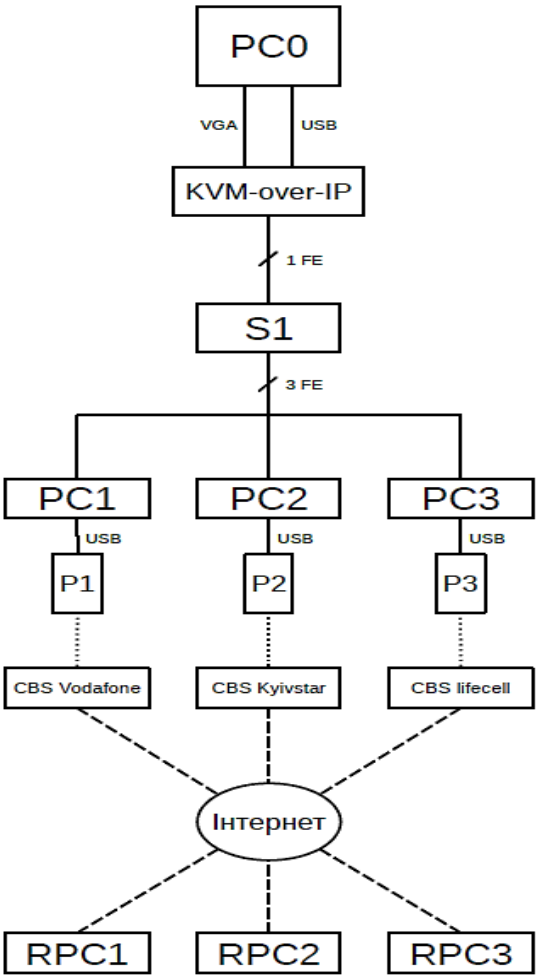


Рис. 4. Структура налаштованої системи

Ненадійність централізованих ієрархічних систем зв’язку, вимагає нового підходу до сітчастої мережі, де межа між маршрутизацією та кінцевими пристроями стає розмитою. В подальшому планується проведення дослідження того, наскільки схема маршрутизації Yggdrasil підходить для розгортання великомасштабних децентралізованих комунікаційних мереж. Маршрутизації, в якій вузли самостійно генерують свої адреси, використовуючи для адресації асиметричне наскрізне шифрування з однаковими ключами. При цьому частини об’єднаної мережі можна з’єднувати через будь-які інші мережі IPv4/6, в яких ці кінцеві вузли розташовані.

**Список використаних джерел:**

1. Конституція України: Закон України “Про критичну інфраструктуру” від 21.06.2024 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 05.09.2024).

2. Collier K., Grudinin A. Ukraine’s top mobile internet company says it has been hit by Russian cyberattack. NBC News. URL: https://www.nbcnews.com/tech/security/ukraines-top-mobile-internet-company-blames-russian-cyberattack-rcna129253 (date of access: 05.09.2024).

3. Пестов О. Д. Розробка системи віддаленого управління об’єктами критичної інфраструктури. Національний університет «Запорізька політехніка», 2023.

4. Kirichek G., Kyrychek D., Hrushko S., Timenko A. Implementation the Protection Method of Data Transmission in Network. *In: ATIT-2019*. P. 29–132.

5. Рудьковський О.Р., Киричек Г.Г. Програмний комплекс з підтримки розподіленої взаємодії мережевих пристроїв та додатків. *Вчені записки ТНУ ім. В.І. Вернадського. Серія «Технічні науки».* 2021. Вип.32(71). № 2. С. 229–234.

6. Cheruvu S., Kumar A., Smith N., Wheeler DM. IoT software security building blocks. Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment. 2020. P. 213-346.

7. TigerVNC. URL: https://tigervnc.org/ (дата звернення: 05.09.2024).

8. Yggdrasil Network. URL: https://yggdrasil-network.github.io/ (дата звернення: 05.09.2024).

9. 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.

10. Киричек Г.Г., Щетінін М.О. Конфігурація серверів з використанням Ansible. *Publishing House "Baltija Publishing"*. 2021. P. 15–17.

11. 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.

12. Киричек Г.Г., Гаркуша В.Ю. Віртуалізація хостів на основі Proxmox VE в умовах надлишкового використання ресурсів. *Вчені записки ТНУ імені В.І. Вернадського. Серія «Технічні науки».* 2021. Вип. 32 (71). № 1. С. 78–84.

13. Costa PA, Rosa A., Leitão J. Enabling Wireless Ad Hoc edge systems with yggdrasil. Proceedings of the 35th Annual ACM Symposium on Applied Computing. 2020. P. 2129-2136.

**References:**

1. Konstytutsiia Ukrainy: Zakon Ukrainy "Pro krytychnu infrastrukturu" [Constitution of Ukraine: Law of Ukraine «On Critical Infrastructure»] dated June 21, 2024 No.1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (date of access: 05.09.2024) [in Ukrainian].

2. Collier K., Grudinin A. Ukraine's top mobile internet company says it has been hit by Russian cyberattack. NBC News. URL: https://www.nbcnews.com/tech/security/ukraines-top-mobile-internet-company-blames-russian-cyberattack-rcna129253 (date of access: 05.09.2024).

3. Pestov O. D. (2023). Rozrobka systemy viddalenoho upravlinnia obiektamy krytychnoi infrastruktury [Critical infrastructure objects remote control system development]. *Zaporizhzhia Polytechnic National University* [in Ukrainian].

4. Kirichek, G., Kyrychek, D., Hrushko, S., Timenko, A. Implementation the Protection Method of Data Transmission in Network. In: ATIT-2019, P. 29–132.

5. Rudkovskyi O.R., Kyrychek H.H. (2021) Prohramnyi kompleks z pidtrymky rozpodilenoi vzaiemodii merezhevykh prystroiv ta dodatkiv [A software complex supporting the distributed interaction of network devices and applications]. *Scientific notes of TNU named after V.I. Vernadskyi. Series «Technical Sciences»,* 32(71), 2, 229–234 [in Ukrainian].

6. Cheruvu S., Kumar A., Smith N., Wheeler DM. (2020). IoT software security building blocks. Demystifying Internet of Things Security: Досвідчений IoT Device/Edge and Platform Security Deployment, 213-346.

7. TigerVNC. URL: https://tigervnc.org/ (date of access: 05.09.2024).

8. Yggdrasil Network. URL: https://yggdrasil-network.github.io/ (date of access: 05.09.2024).

9. Kothari K., Palwankar T., Dubey A., Parate P. (2022). Tor vs Yggdrasil: Comparative Study of Two Different Communication System. In 2022 International Conference on Inventive Computation Technologies (ICICT), 452-456.

10. Kyrychek H.H., Shchetinin M.O. (2021). Configuring servers using Ansible. Publishing House "Baltija Publishing", 15–17.

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

12. Kyrychek H.H., Harkusha V.Yu. (2021) Virtualizatsiia khostiv na osnovi Proxmox VE v umovakh nadlyshkovoho vykorystannia resursiv [Virtualization of hosts based on Proxmox VE in conditions of excessive use of resources]. *Scientific notes of TNU named after V.I. Vernadskyi. Series «Technical Sciences».* 32 (71), 1, 78–84 [in Ukrainian].

13. *Costa* PA, Rosa A., Leitão J. (2020). Enabling Wireless Ad Hoc edge systems with yggdrasil. Proceedings of the 35th Annual ACM Symposium on Applied Computing, 2129-2136.