DOI 10.15276/imms.v12.no3.243
УДК 004.4

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 3, pp. 243-253

ОРГАНІЗАЦІЯ ДИСТАНЦІЙНОГО ДОСТУПУ ДО КОМП'ЮТЕРНОЇ НАВЧАЛЬНОЇ ЛАБОРАТОРІЇ ЗА ДОПОМОГОЮ ВЕБ-ТЕХНОЛОГІЙ

Г.О. Шеремет, О.А. Стопакевич

Національний університет "Одеська політехніка",
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: sheremet.heorhiy@gmail.com,
stopakevich@op.edu.ua

Зараз у світі відбувається цифрова трансформація суспільства. Більшість видів людської діяльності поступово переносяться у цифровий вимір. Така сфера життя, як освіта не є винятком. З кожним роком студенти все рідше відвідують заняття очно, причиною цього є різні фактори. Виникає необхідність переходу навчальних закладів на дистанційну форму навчання. У зв'язку з цим виникають складнощі у використанні комп'ютерних лабораторій, розташованих в навчальних закладах. Отже, на сьогоднішній день організація дистанційного доступу до комп'ютерів навчальної лабораторій є досить актуальним завданням. Метою роботи є створення системи віддаленого доступу до комп'ютерної навчальної лабораторії з комп'ютера будь-якого користувача по паролю за допомогою web технологій. У статті розглядається процес налаштування серверної частини віртуальної приватної мережі VPN на віртуальному виділеному сервері VPS. Розглянуто послідовність команд у терміналі для встановлення та налаштування серверної частини VPN. Описано процес підключення до віртуальної приватної мережі з комп'ютера навчальної лабораторії та розглянуто послідовність команд у терміналі для встановлення та налаштування клієнтської частини VPN. Розглянуто інсталяцію та налаштування програмного забезпечення для віддаленого доступу на комп'ютерах навчальної лабораторії. Змодельовано віддалений доступ, який надає можливість віддаленого керування комп'ютерною мишею та клавіатурою, віддаленого запуску програмного забезпечення, обміну файлами між комп'ютером студента та комп'ютером навчальної лабораторії.. Стороннє програмне забезпечення, яке використовується при створенні системи віддаленого доступу, є вільно розповсюджуваним та безкоштовним.

Ключові слова: віддалений доступ до комп'ютера, віртуальна приватна мережа, VPN, WireGuard, RustDesk, VPS.

Вступ

Структурні зміни у світовій системі освіти, що відбулися починаючи з другій половині XX століття, зумовлені розвитком науково-технічного прогресу, вплинули на всі сторони життя суспільства. Поява дистанційного навчання не є раптовою подією, за всіх часів потреба у освіті зберігалася високому рівні. Поява інтернету та прискорення темпів наукового прогресу лише сприяли поширення даного формату здобуття освіти. У світлі останніх подій в Україні дистанційне навчання набуває ще більшої актуальності.

Існує безліч готових рішень для віддаленого доступу до комп'ютера. Найпоширеніші і найбільш функціональні з них є платними чи частково платними. У статті розглядається організація дистанційного доступу до комп'ютерної навчальної лабораторії з використанням виключно безкоштовних рішень. При цьому запропоноване рішення є досить функціональним і забезпечує студентів всім необхідним для комфортного використання навчальної лабораторії дистанційно.

Аналіз досліджень та публікацій

Дистанційне навчання в сучасному розумінні сформувалося порівняно нещодавно і тому, беручи до уваги цю новизну, воно орієнтується на передовий

педагогічний і методичний досвід, акумульований різними освітніми інституціями світового простору, на застосовування новітніх і оперативних інформаційно-педагогічних технологій, що окликаються на запити сучасної освіти та соціуму в цілому. Дистанційне навчання – одна із форм навчання, яка виникла й удосконалювалася разом із розвитком інтернет-технологій, і на сьогодні має чіткі характерні ознаки, принципи і певні методичні напрацювання. Дистанційне навчання та освіта із застосуванням дистанційних освітніх технологій набуває все більшого поширення в Україні і здобуває власних рис [**1**].

Коворкінг означає роботу двох або більше людей в одному місці, але не в одній фірмі. Це явище набуло значного розмаху в останні роки, включаючи зростання попиту у великих містах навколо світу та перспективи подальшого зростання в майбутньому. Характеристика фірм, розташованих у коворкінгах здається, змінилися з часом, оскільки сьогодні також зростає кількість великих нетехнологічних фірм, які обирають цей стиль [2].

У цілому нині з підприємницького погляду перебування у коворкінгу позитивно впливає на підприємницьку поведінку. Це засноване в основному на позитивних побічних ефектах та співпраці представників різних професій у рамках коворкінгу, що особливо вигідно молодим фірмам [2,3,4].

Коворкінг явище, яке проникло в організаційні структури, впливає на створення та обмін знаннями, покращує інноваційну поведінку та перебуває під впливом соціальних факторів, а також матеріального оснащення. Середовище, що нагадує коворкінг, робить людей більш щасливими та емоційно здоровими, компанії можуть розглянути можливість застосування набутого досвіду та знань у своїй організації, щоб співробітники з більшою готовністю залишалися з ними [5,6,7].

Мета і задачі роботи

Метою роботи є опис створення системи віддаленого доступу до комп'ютерної навчальної лабораторії з комп'ютера любого користувача по паролю за допомогою web технологій.

Для досягнення поставленої мети розроблена система має відповідати наступним основним вимогам:

- забезпечити реєстрацію та ідентифікацію, доступ по паролю користувачів та адміністраторів системи;
- комп’ютери лабораторії працюватимуть з використанням операційній системи Windows версії не нижче 8х;
- користувачі повинні мати доступ до управління курсором та клавіатурою, реалізувати віддалений запуск програм і отримання результатів їх роботи;
- забезпечити можливість обміну файлами з віддаленим комп’ютером.

Основна частина

Для організації дистанційного доступу до комп'ютерної навчальної лабораторії за допомогою веб-технологій необхідно виконати такі пункти:

1. Налаштувати серверну частину VPN на VPS.
2. Підключитись до VPN з комп'ютерної навчальної лабораторії.
3. Встановити та налаштувати програмне забезпечення для віддаленого доступу на комп'ютерах навчальної лабораторії.
4. Протестувати можливість віддаленого доступу.
5 Моделювання побудованої системи.

Налаштування серверної частини VPN на VPS.

VPN (virtual private network – віртуальна приватна мережа) — це узагальнена назва технологій, які дозволяють створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному пристрою чи користувачеві бути повноцінним

учасником віддаленої мережі та користуватися її сервісами — внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет. Безпека передавання інформації через загальнодоступні мережі реалізована за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. Технологія VPN дозволяє об'єднати кілька географічно віддалених мереж (або окремих клієнтів) у єдину мережу з використанням для зв'язку між ними спеціадьних каналів. Багато провайдерів пропонують свої послуги як з організації VPN-мереж для бізнес-клієнтів, так і для виходу в Інтернет. VPN є клієнт-серверною технологією [8].

Виртуальний виділений чи приватний сервер (virtual dedicated VDS or private VPS server) – послуга, у межах якої користувачеві надають віртуальний сервер. Це повноцінна альтернатива фізичного виділеного сервера з великою кількістю переваг, високою стабільністю, простотою в управлінні та налаштуванні, стійкістю до відмов та набагато меншими фінансовими витратами [9].

Можна обрати майже будь-який VPS, наприклад від digitalocean [10]. Операційною системою цього VPS є Ubuntu 22.10.

Для реалізації VPN використаємо WireGuard. WireGuard — це комунікаційний протокол та безкоштовне програмне забезпечення з відкритим вихідним кодом, яке реалізує зашифровані VPN [11]. Розглянемо послідовність команд у терміналі для встановлення та налаштування серверної частини WireGuard.

Оновлюємо сервер:

```
apt update && apt upgrade -y
```

Ставимо wireguard:

```
apt install -y wireguard
```

Генеруємо ключі сервера:

```
wg genkey | tee /etc/wireguard/privatekey | wg pubkey | tee /etc/wireguard/publickey
```

Проставляємо права на приватний ключ:

```
chmod 600 /etc/wireguard/privatekey
```

Перевіримо назву мережного інтерфейсу:

```
ip a
```

Швидше за все, це буде eth0, але можливо й інший, наприклад, ens3 або якось інакше. Ця назва інтерфейсу використовується далі в конфігураційному файлі /etc/wireguard/wg0.conf, який буде створено нижче:

```
vim /etc/wireguard/wg0.conf
```

Вміст файлу wg0.conf

```
[Interface]
PrivateKey = <privatekey>
Address = 10.0.0.1/24
ListenPort = 51830
PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
```

У рядках PostUp і PostDown використаний саме мережевий інтерфейс eth0. Якщо інший, необхідно замінити eth0 на нього.

Вставляємо замість <privatekey> вміст файлу /etc/wireguard/privatekey

Налаштовуємо IP форвардинг:

```
echo "net.ipv4.ip_forward=1" >> /etc/sysctl.conf
sysctl -p
```

Включаємо systemd демон з wireguard:

```
systemctl enable wg-quick@wg0.service
systemctl start wg-quick@wg0.service
systemctl status wg-quick@wg0.service
```

Створюємо ключі клієнта:

```
wg genkey | tee /etc/wireguard/client_privatekey | wg pubkey | tee /etc/wireguard/ client_publickey
```

Додаємо в конфіг сервера клієнта:

```
vim /etc/wireguard/wg0.conf
[Peer]
PublicKey = <client_publickey>
AllowedIPs = 10.0.0.2/32
```

Замість <client_publickey> — замінюємо вміст файлу /etc/wireguard/ client_publickey

Перезавантажуємо systemd сервіс із wireguard:

```
systemctl restart wg-quick@wg0
systemctl status wg-quick@wg0
```

Підключення до VPN з комп'ютерної навчальної лабораторії

На локальній машині навчальної лабораторії створюємо текстовий файл із конфігом клієнта:

```
[Interface]
PrivateKey = <CLIENT-PRIVATE-KEY>
Address = 10.0.0.3/32
DNS = 8.8.8.8
[Peer]
PublicKey = <SERVER-PUBKEY>
Endpoint = <SERVER-IP>:51830
AllowedIPs = 0.0.0.0/0
PersistentKeepalive = 20
```

Тут <CLIENT-PRIVATE-KEY> замінюємо на приватний ключ клієнта, тобто вміст файлу /etc/wireguard/client_privatekey на сервері. <SERVER-PUBKEY> замінюємо на публічний ключ сервера, тобто вміст файлу /etc/wireguard/publickey на сервері. <SERVER-IP> замінюємо на IP сервер.

Цей файл відкриваємо у Wireguard клієнті (є для всіх операційних систем, у тому числі мобільних) – і тиснемо у клієнті кнопку підключення.

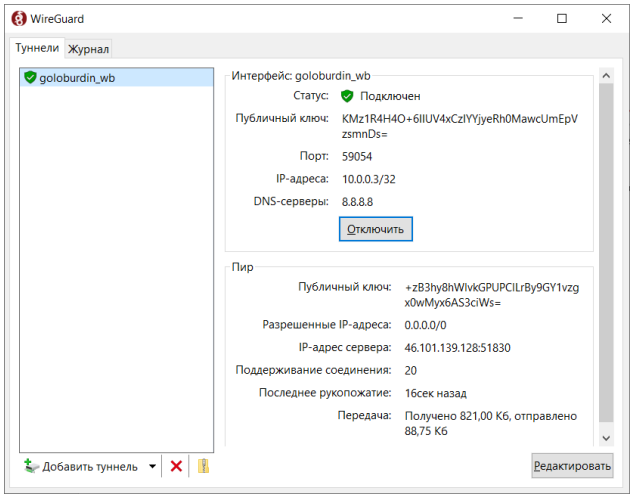

Рис. 1. Підключення до VPN

На цьому налаштування локальної машини навчальної лабораторії закінчено. Тепер вона має вихід в інтернет через білу IP-адресу. Це необхідно для можливості віддаленого доступу.

Встановлення та налаштування програмного забезпечення для віддаленого доступу на комп'ютері навчальної лабораторії.

Для віддаленого доступу використовується програма RustDesk. RustDesk – це безкоштовне програмне забезпечення для віддаленого ПК, створене RustDesk. Ця програма з відкритим вихідним кодом допомагає користувачам отримувати доступ та керувати своїми комп'ютерами. з будь-якого місця. Він служить і клієнтом, і

сервером, тому для його використання немає необхідності використовувати будь-які інші сторонні програми.[12]

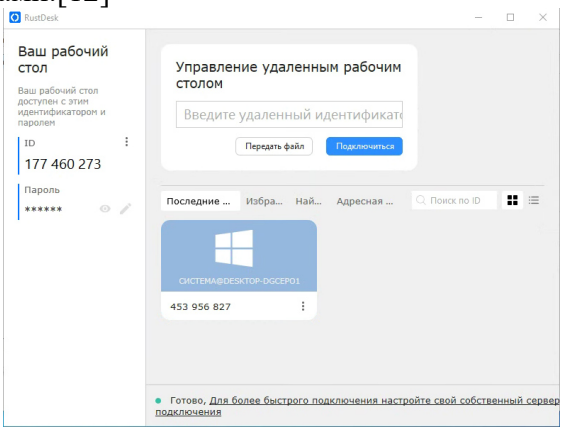

Рис. 2. Інтерфейс RustDesk

Цього достатньо для віддаленого доступу. Єдине, треба переконатися, що служба запущена.

Для віддаленого доступу необхідно надати студентам ID та пароль.

Тестування можливості віддаленого доступу.

Встановлюємо програму RustDesk на комп'ютер. У вікні «Керування віддаленим робочим столом» вводимо ID віддаленого комп'ютера навчальної лабораторії та натискаємо «Підключитися».

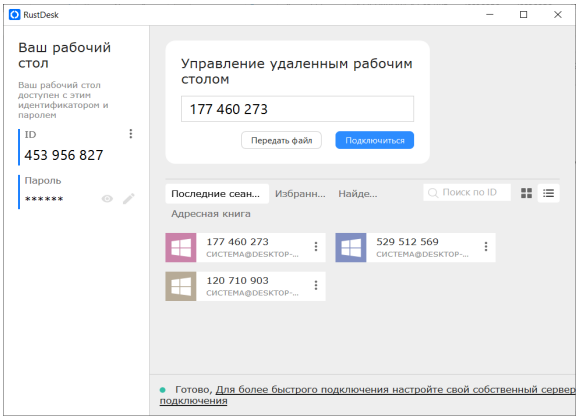

Рис. 3. Підключення до віддаленого комп'ютера

Далі програма попросить надати пароль. Вводимо пароль та натискаємо кнопку «ОК».

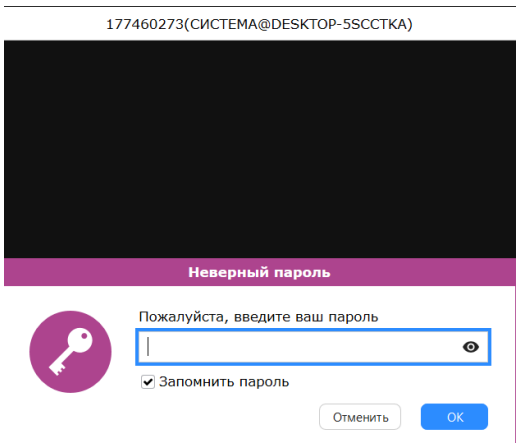

Рис. 4. Вікно введення пароля

Далі отримуємо віддалений доступ.

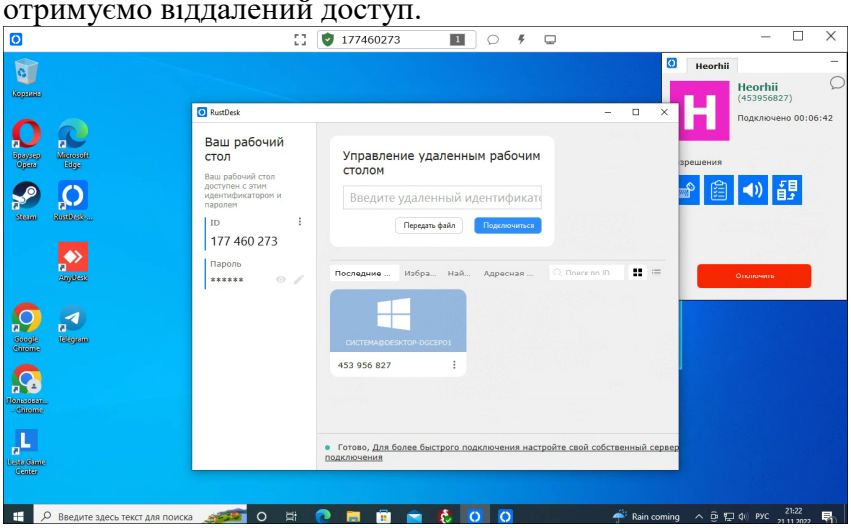

Рис. 5. Вікно віддаленого доступу

Тепер після успішного тестування ми можемо бути впевнені, що це рішення робоче і готове до використання.

Моделювання побудованої системи.

Панель адміністратора має вигляд як представлено рис. 6. У ній адміністратор системи може додавати, редагувати та видаляти комп'ютери.

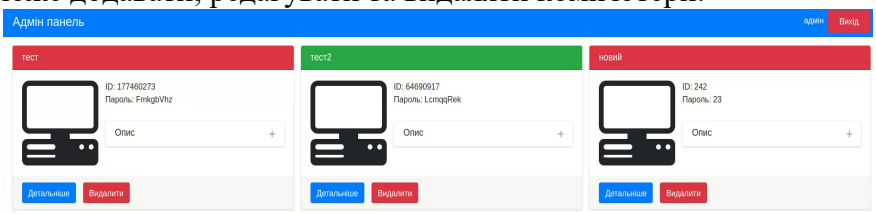

Рис. 6. Панель адміністратора.

Створимо новий комп'ютер з даними, представленими на рис. 7.

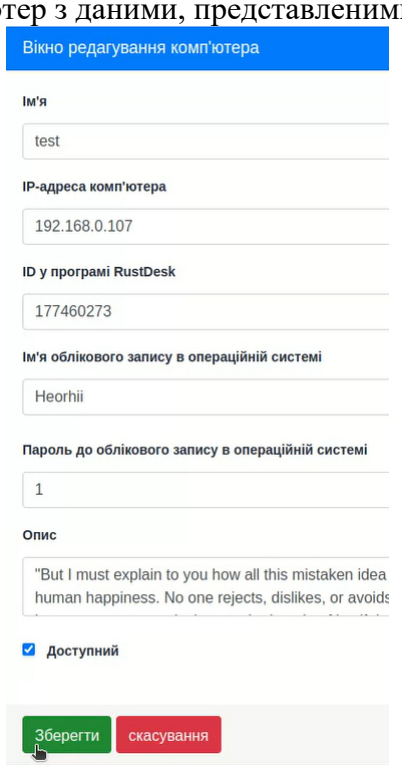

Рис. 7. Вікно редагування комп'ютера.

Тепер комп'ютер з ip-адресою 192.168.0.107 доступний для підключення студентів.

Для реєстрації необхідно надати електронну пошту та придумати пароль. Для користування системою також необхідно підтвердити адресу електронної пошти. Зареєструємось у системі. На рис.8 зображено вікно реєстрації.

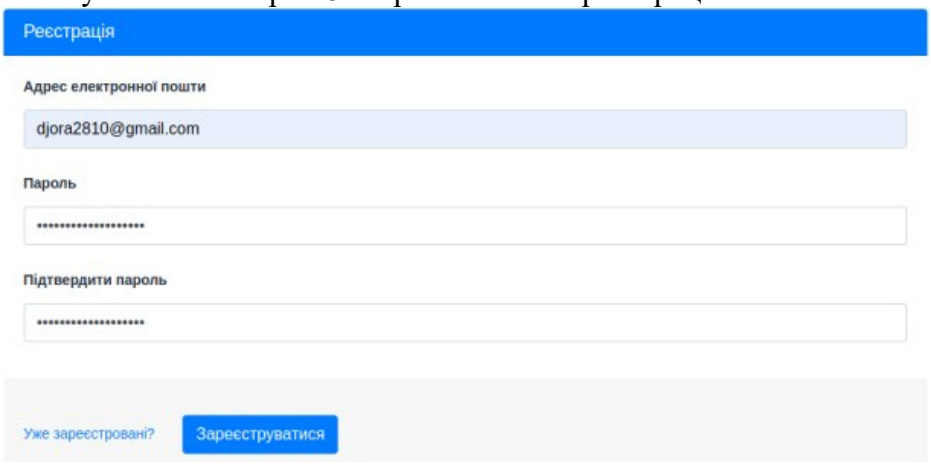

Рис. 8. Вікно реєстрація.

Після реєстрації ми побачимо повідомлення про необхідність підтвердити адресу електронної пошти. На рис.9 зображено Сповіщення.

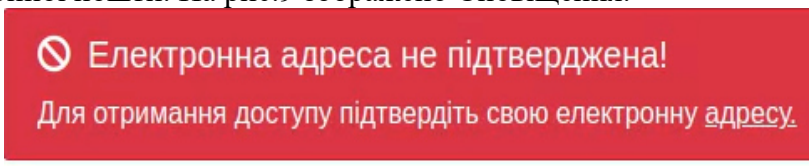

Рис. 9. Сповіщення.

Після підтвердження адреси це повідомлення зникне і ми зможемо скористатися системою. Завершивши реєстрацію, користувач побачить інтерфейс як представлено на рис.10.

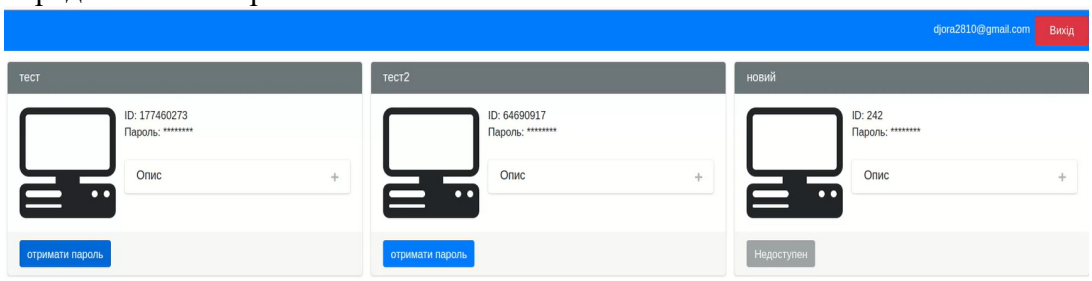

Рис. 10. Інтерфей користувача.

Користувач може вибрати комп'ютер та підключитися до нього. Підключимося до комп'ютера з іменем «test» натиснувши на кнопку «Отримати пароль». Після чого система надасть нам ID та пароль для підключення, як представлено на рис.11.

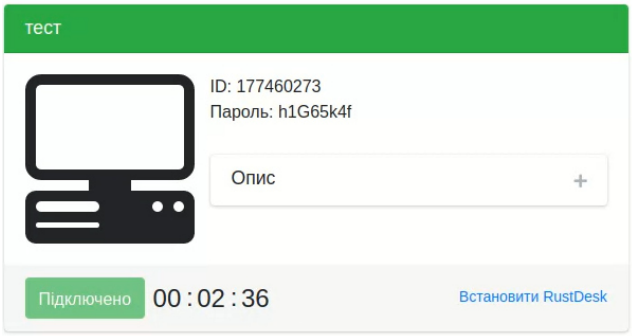

Рис. 11. Отримання пароля.

Далі заходимо в RustDesk і підключаємося за наданим ID, в нашому випадку це 177460273. RustDesk запросить пароль, вводимо раніше отриманий пароль, в нашому випадку це h1G65k4f.

Маючи віддалений доступ до комп'ютера, заходимо в консоль і вводимо команду ipconfig, щоб перевірити ip-адресу і переконатися в тому, що підключилися до потрібного комп'ютера. На рис. 12 зображено вікно віддаленого доступу.

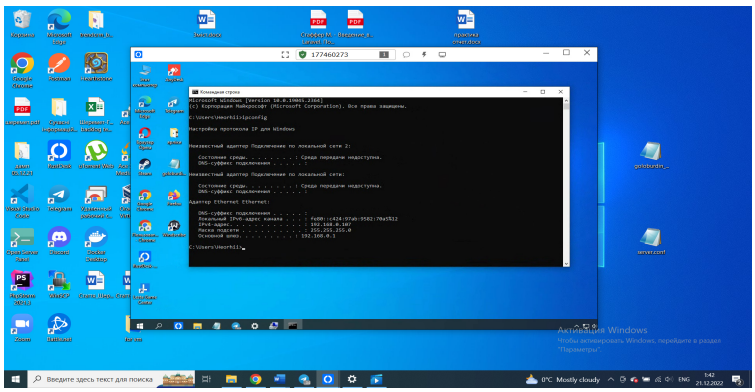

Рис. 12. Вікно віддаленого доступу.

Як видно на малюнку ip-адреса 192.168.0.107. Такий, як ми вказували при створенні комп'ютера в панелі адміністратора. Відтак система працює коректно та готова до використання.

Також у системі існує можливість зайняти чергу у разі коли потрібний нам комп'ютер зайнятий іншим користувачем. Зайнятий комп'ютер виглядає як на рис.13.

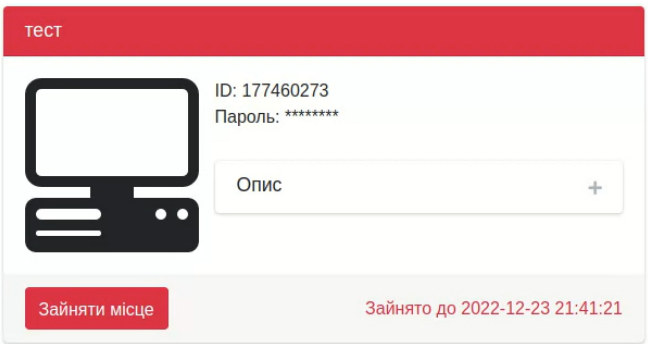

Рис. 13. Зайнятий комп'ютер.

При натисканні на кнопку "Зайняти місце" ми займемо місце в черзі. Перебування у черзі виглядає як представлено рис.14.

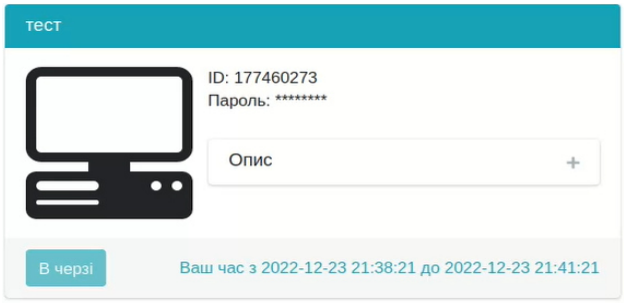

Рис. 14. Знаходження у черзі.

При настанні нашої черги система надасть нам пароль і ми зможемо отримати віддалений доступ.

Висновки

В межах статті виконана мета роботи – описано створення системи дистанційного доступу до комп'ютерної навчальної лабораторії за допомогою web-технологій.

При досягненні поставленої мети в роботі розв'язані наступні задачі:

- розроблено систему реєстрацію та ідентифікацію, доступ по паролю користувачів та адміністраторів системи;
- Розроблена система працює на операційній системи Windows версії не нижче 8х;
- Надана можливість управління курсором та клавіатурою, та віддаленого запуску програм і отримання результатів їх роботи;
- забезпечено можливість обміну файлами з віддаленим комп’ютером.

Проведено аналіз існуючих програм дистанційного доступу до комп'ютерних мереж. Серед них була обрана і взята за основу програма, що найбільш підходить за функціоналом і вимогами.

Розроблено програмний додаток який:

- забезпечує реєстрацію, автентифікацію та авторизацію користувачів у системі;
- надає можливість віддаленого керування курсором та клавіатурою;
- надає можливість віддаленого запуску програмного забезпечення;
- надає можливість обміну файлами між персональним комп'ютером користувача та комп'ютером навчальної лабораторії;
- забезпечує почергове використання комп'ютерів студентами.

Також проведено моделювання роботи системи дистанційного доступу до комп'ютерної навчальної лабораторії. Моделювання продемонструвало основні функції системи та підтвердило її працездатність.

Отримані в даній роботі результати можуть бути корисні не тільки для освіти, а й для дистанційного бізнес – коворкінга у невеликих фірмах, наукових установах. Результати роботи можуть служити основою для подальших розробок у цій галузі.

Список літератури

1. Гнатюк О.В. Дистанційне навчання: проблеми, пошуки, виклики. URL: https://lib.iitta.gov.ua/ Текст.pdf
2. Tim A. Haucke N., Östmarck A. An Analysis of the Co-working Space Industry in Stockholm from an Entrepreneurial Perspective. URL: https://kth.diva-portal.org/smash/get/diva2:1190270/FULLTEXT01.pdf
3. Fahrizal1 A., Jean C., Juan B.M., Ramdhani R., Hadiwirosa S., Hamdi E., Indradewa R., Abadi F. Strategic Formulation Analysis of Coworking Space Businesses Using Containers. URL: https://www.ijrrjournal.com/IJRR_Vol.9_Issue.3_March2022/IJRR022.pdf

4. Endrissat N., Vandelannoitte A.L. From sites to vibes: Technology and the spatial production of coworking spaces. URL: https://hal.archives-ouvertes.fr/hal-03332209/document
5. Kraus S.; Bouncken R.B.; Görmar L.; González-Serrano M.H., Calabuig F. Coworking spaces and makerspaces: Mapping the state of research. URL: https://www.econstor.eu/bitstream/10419/260976/1/1796986151.pdf
6. Hofeditz L., Mirbabaie M., Stieglitz S. Virtually Extended Coworking Spaces? *The Reinforcement of Social Proximity, Motivation and Knowledge Sharing Through ICT*. URL: https://arxiv.org/ftp/arxiv/papers/2012/2012.09538.pdf
7. Roche M., Oettl A., Catalina C. (Co-) Working in Close Proximity. *Knowledge Spillovers and Social Interactions*. URL: https://www.hbs.edu/ris/Publication%20Files/21-024rev2-11-22_4cf1fb54-e60b-41e6-8611-985031c999ba.pdf
8. Вікіпедія. VPN. URL: https://uk.wikipedia.org/wiki/VPN
9. Вікіпедія. Віртуальний виділений сервер. URL: https://uk.wikipedia.org/wiki/Віртуальний_виділений_сервер
10. DigitalOcean. Droplets. URL: https://www.digitalocean.com/products/droplets
11. Вікіпедія. WireGuard. URL: https://ru.wikipedia.org/wiki/WireGuard
12. RustDesk. URL: https://rustdesk.com/

ORGANIZING REMOTE ACCESS TO THE COMPUTER EDUCATIONAL LABORATORY USING WEB TECHNOLOGIES

G.O. Sheremet, O.A. Stopakevich

National Odesa Polytechnic University,
ave. Shevchenko, 1, Odesa, 65044, Ukraine; e-mail: sheremet.heorhiy@gmail.com,
stopakevich@op.edu.ua

Currently, the world is undergoing a digital transformation of society. Most types of human activity are gradually being transferred to the digital dimension. Such a sphere of life as education is no exception. Every year, students attend classes face-to-face less and less, the reason for this is various factors. There is a need for educational institutions to switch to distance education. In this connection, difficulties arise in the use of computer laboratories located in educational institutions. So, today, the organization of remote access to computers of educational laboratories is a very urgent task. The purpose of the work is to create a system of remote access to the computer training laboratory from any user's computer by password using web technologies. The article discusses the process of setting up the server part of a virtual private network VPN on a virtual dedicated VPS server. Considered the sequence of commands in the terminal to install and configure the VPN backend. The process of connecting to a virtual private network from a computer of the educational laboratory is described, and the sequence of commands in the terminal for installing and configuring the VPN client part is considered. The installation and configuration of software for remote access on the computers of the educational laboratory is considered. Remote access is simulated, which provides the possibility of remote control of a computer mouse and keyboard, remote start of software, file exchange between a student's computer and a computer of the educational laboratory. Third-party software used in creating a remote access system is free redistributable and free.
Keywords: remote computer access, virtual private network, VPN, WireGuard, RustDesk, VPS.