

ТЕХНІЧНІ НАУКИ

DOI: <https://doi.org/10.33216/1998-7927-2022-272-2-7-14>

УДК 004.77:004.031

ВПРОВАДЖЕННЯ СИСТЕМИ ВІДДАЛЕНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ КОМП'ЮТЕРНИХ ЛАБОРАТОРІЙ

Могильний Г.А., Семенов М.А., Кіреєв І.Ю.

IMPLEMENTATION OF A SYSTEM OF REMOTE ACCESS TO INFORMATION RESOURCES OF COMPUTER LABORATORIES

Mohylnyi H.A., Semenov M.A., Kiryeyev I.Yu.

Організація роботи навчальних комп'ютерних лабораторій в умовах дистанційного навчання пов'язане із низкою питань, зокрема з розробкою та впровадженням системи віддаленого доступу користувачів не лише до навчального контенту але й до ресурсів локальної мережі та сервісного обладнання: програмних засобів та середовищ, серверів, принтерів, цифрових приладів тощо. Тому одна з основних проблем, яка виникає при організації дистанційного навчання здобувачів освіти, зокрема ІТ спеціальностей, є створення умов для комфортного доступу здобувача освіти до комп'ютерної мережі університетської лабораторії – в ідеалі повна імітація роботи в комп'ютерній лабораторії університету при віддаленому доступі. Незважаючи на велику кількість праць, присвячених різним аспектам організації дистанційного навчання проблема створення віддалених навчальних комп'ютерних лабораторій досліджена не достатньо.

У роботі наведено аналіз існуючих підходів та принципів побудови типової інформаційної структури навчальної комп'ютерної лабораторії. На засадах практичного досвіду використання та модернізації такої системи запропоновано ряд технічних рішень спрямованих на організацію віддаленого доступу до внутрішніх інформаційних ресурсів навчальної комп'ютерної лабораторії. З багатьох можливих рішень по створенню інформаційної системи з віддаленим доступом у роботі окреслено три найпростіші та швидкі варіанти їх реалізації. Проаналізовано ряд варіантів організації віддаленого доступу до навчальної комп'ютерної лабораторії, яка побудована за допомогою технології перенаправлення окремих портів на один вузол локальної мережі із різноманітними інформаційними, апаратними та програмними ресурсами, або декілька вузлів, серед яких один сервер віддаленого робочого столу, web-сервер та інші ресурси з окремими IP адресами. Досліджено основні структурні компоненти системи віддаленого доступу на засадах VPN та наведено рекоме-

ндації по їх налаштуванню та застосуванню. Надано основні особливості застосування VPN з використанням роутеру MikroTik. Запропонований підхід дозволив реорганізувати роботу комп'ютерної навчальної лабораторії та створити нові можливості використання інформаційних ресурсів студентами та викладачами ЛНУ імені Тараса Шевченка в умовах запровадження дистанційної освіти в період COVID-19. Практичний досвід використання такого підходу у 2020-2021 рр. довів власну ефективність.

Ключові слова: VPN, Windows Server, навчальна комп'ютерна лабораторія, дистанційне навчання, комп'ютерна мережа, віддалений доступ, порт, протокол, PPTP.

Вступ. Одним із пріоритетних напрямів розвитку сучасної освіти є інформатизація всіх складових навчального процесу. Сучасний етап розвитку інформатизації системи освіти спрямований на подальше підвищення якості освіти, забезпечення конкурентоспроможності національної системи освіти на світовому ринку освітніх послуг, її інтеграцію у світовий освітній простір. Він передбачає реалізацію принципів відкритої освіти, підпорядкований сучасним освітнім парадигмам людиноцентризму та рівного доступу до якісної освіти [4].

Останнім часом в умовах COVID-19, та після 24 лютого 2022 р, коли наша держава була підвернута ворожій агресії зі сторони Російської Федерації та значна кількість навчальних закладів переведена на дистанційний режим роботи особливого значення набули різноманітні засоби інформаційних

комп'ютерних технологій та різноманітні методики їх впровадження у навчальний процес [2].

Безумовно, така складна ситуація, та соціально-економічні виклики суспільства сприяли підвищенню значимості дистанційної освіти в Україні.

Однак, в таких умовах ефективно використання сучасних інформаційних технологій та прогресивних педагогічних засобів навчання неможливе без створення спеціалізованих умов у навчальних комп'ютерних лабораторіях (НКЛ).

Різним питанням організації дистанційного та цифрового навчання присвячено багато наукових праць, зокрема роботи В. Бикова, Н. Морзе, В. Кухаренка, О. Щербини [3, 5, 6, 7]. Але робіт щодо використання віддалених віртуальних лабораторій в українському сегменті наукових досліджень майже немає. Серед світового досвіду заслуговує на увагу досвід університету DEUSTO [1] (м. Більбао, Іспанія). Це засвідчує актуальність цієї статті.

За таких умов, питання організації комп'ютерного середовища у навчальних лабораторіях та комп'ютерних класах ставить нові завдання до організації комп'ютерної мережі та програмно-технічного оснащення [5]. Основною метою цього процесу повинно бути розробка нових підходів до організації виконання лабораторних завдань для студентів та учнів, які знаходяться дома, за межами НКЛ (навчального закладу) шляхом створення умов аналогічних стаціонарній системі навчання.

Аналіз літератури та різноманітних методичних розробок показав, що в цьому напрямку слабо наведені організаційно-методичні засади використання та модернізації існуючого програмно-апаратного забезпечення НКЛ. Більшість авторів запроваджують різноманітні педагогічні підходи та моделі освітнього процесу і всебічно розглядають можливості використання додаткового програмного забезпечення спрямованого на підвищення ефективності взаємодії між учасниками освітнього процесу [3, 7]. Таким чином, передбачається, що всі учасники освітнього процесу використовують засоби особистої (домашньої) обчислювальної техніки.

Однак питання роботи існуючих НКЛ в таких умовах не достатньо розглянуті. В цей час, комп'ютерні класи (лабораторії) практично не готові до нових вимог освітнього процесу та в більшості випадків знаходяться у режимі простою або часткового використання. Безумовно, розробка засобів використання існуючих локальних інформаційних ресурсів НКЛ в умовах дистанційної освіти значно підвищить ефективність всього навчального процесу.

Мета роботи – комплексний аналіз та опис шляхів модернізації інформаційних ресурсів навчальних комп'ютерних лабораторій, спрямований на вирішення проблеми віддаленого доступу до них в умовах дистанційного навчання.

Викладення основних матеріалів. У закладах освіти існує багата кількість НКЛ, які відрізняються як рівнем оснащення обчислювальною технікою так

і різноманітним програмним забезпеченням в залежності від спеціалізації та особливостей навчального процесу. Однак, з точки зору організаційної та мережевої структури можна виділити найбільш поширену типову структуру НКЛ, яка використовується у багатьох закладах середньої освіти та більшості вишів і зовсім не пристосовано до завдань вирішення проблеми надання віддаленого доступу тим хто навчається дистанційно (рис. 1).

Така типова структура ефективно працює при умовах її безпосереднього використання в аудиторії та може включати: мережеве обладнання, робочі станції (персональні комп'ютери), мультимедійне обладнання, файловий сервер та друксервер, які зазвичай об'єднані на засадах однорангової мережі Microsoft. Така структура НКЛ дозволяє ефективно використовувати мережу Інтернет, локальні прилади та локальне програмне забезпечення, але зовсім не пристосована для використання учасниками освітнього процесу в дистанційних умовах.

При такому підході більшість інформаційних ресурсів є слабо керованими та потребують постійної присутності співробітників навчально-допоміжного персоналу.

Тим не менш, значною перевагою цієї інформаційної системи є мала вартість, незначні вимоги до кваліфікації обслуговуючого персоналу, мінімальна програмно-технічна підтримка та можливість забезпечити виконання основних завдань навчального процесу при роботі у стаціонарному (денному, очному) режимі.

Основним недоліком її є відсутність можливостей використати наявну обчислювальну техніку в дистанційних умовах, коли всі учасники освітнього процесу знаходяться поза межами НКЛ.

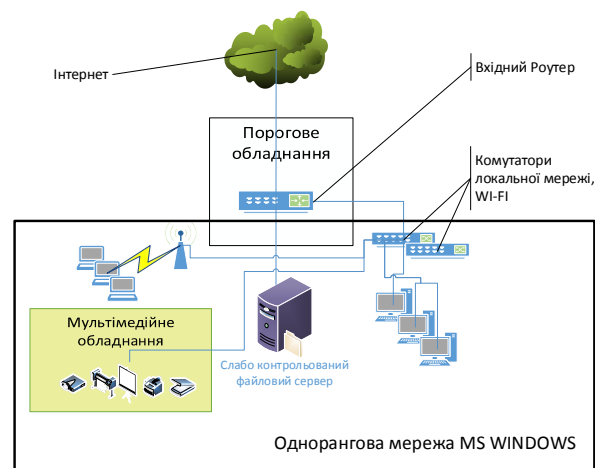


Рис. 1. Типова структура НКЛ

Результати досліджень. Важливим кроком у створенні системи з віддаленим доступом є етапи аналізу та планування всієї інформаційної системи з віддаленим доступом. У загальному випадку необхідно вирішити низьку завдань та обов'язково врахувати наступне:

1. Можливість отримання реальної IP адреси (пула адресів).

2. Кількість, типи та різноманітність інформаційних ресурсів, які повинні бути надані у віддаленому доступі. При цьому, потрібно врахувати необхідні умови основних завдань навчального процесу з метою забезпечення достатньої якості виконання лекційних занять та завдань до лабораторних робіт.

3. Реальний стан наявних інформаційних ресурсів, їх спроможність працювати у безперервному (або необхідному) режимі, можливість їх переналаштування та модернізації.

4. Фінансові можливості придбання додаткового програмного та апаратного забезпечення (комп'ютери, складові комп'ютерів, комплектуючі, програмне забезпечення, роутери, тип мережевої кабельної системи та інше).

5. Наявність та кваліфікація навчально-допоміжного персоналу, спроможного виконати монтаж, налаштування та обслуговування додаткового програмно-апаратного забезпечення.

6. Приблизний термін впровадження запланованих рішень.

У лабораторії ДІСЕНП кафедри ІТС Луганського національного університету імені Тараса Шевченка відповідно до завдань проекту EASMUS+ MoPED було проведено дослідження та впровадження різноманітних варіантів НКЛ з віддаленим доступом. Досвід їх впровадження засвідчив той факт, що завдання аналізу та планування всієї інформаційної системи є складним та багатоітераційним процесом та потребує повного комплексного підходу. Для цього необхідно окреслити основні показники ефективності системи НКЛ з віддаленим доступом. Серед мінімального набору таких показників є: відсоток реалізації елементів навчального плану за допомогою НКЛ, стабільність та наявність підключення, швидкість доступу до інформаційних ресурсів.

В окремих випадках необхідно приймати рішення спрямовані на першочергове виконання завдань, які можливо виконати та впровадити в існуючих умовах. Після їх виконання знову проводити комплексний аналіз. Таким чином вдається поступово досягнути значних результатів у досягненні проміжної мети. Цей процес не повинен зупинятися з метою постійного вдосконалення існуючих рішень інформатизації навчального процесу та підвищення якості дистанційної освіти. Це дозволяє створити передумови створення освітньої екосистеми (яка включає не лише НКЛ) та її сталий розвиток.

Однак, з багатьох можливих рішень по створенню інформаційної системи з віддаленим доступом в межах цієї статті окреслимо тільки декілька швидких та поширених випадків. При цьому будемо вважати, що в нас є реальна IP адреса, в наявності необхідний допоміжний персонал, достатньо фінансових коштів та термін впровадження нас влаштує.

• **Випадок 1.** Всі ресурси розташовані на одному вузлу локальної мережі НКЛ.

• **Випадок 2.** Ресурси різного типу (в кількості одного кожного типу) розташовані на різних вузлах НКЛ, які використовують різні порти TCP/IP. Іншими словами – один ВЕБ сервер, один принтер, один сервер RDP (віддаленого робочого стола) і так далі.

• **Випадок 3.** Повний доступ до всіх ресурсів НКЛ.

Слід зауважити, що перших два випадка можуть бути створені на багатьох типах порогових приладів. У третьому випадку треба проводити ґрунтовний попередній аналіз щодо можливостей наявного програмно-технічного забезпечення.

У межах цієї роботи в якості порогового приладу розглянемо роутер MikroTik RB750Gr3 з операційною системою RouterOS v6.49.6 (stable).

Попередньо, для достовірності даних, скинемо конфігурацію MikroTik (рис. 2, а) та налаштуємо її знову (так як показано на рис. 2, б).

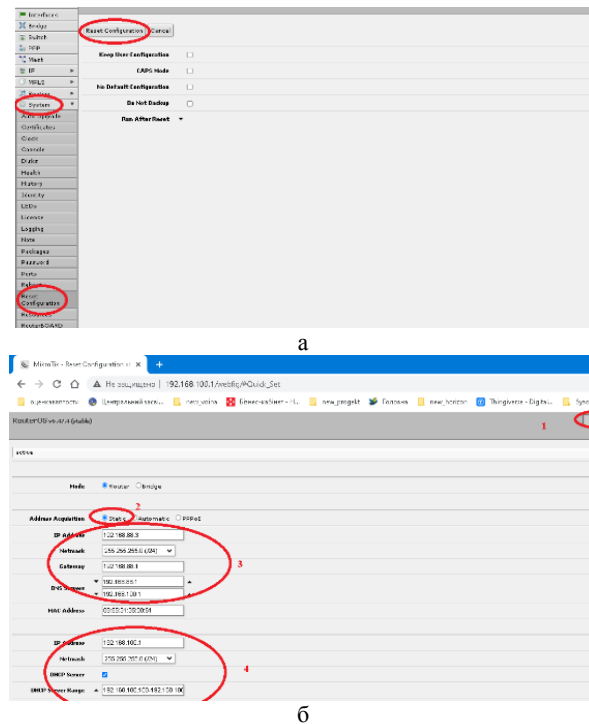


Рис. 2. Скидання конфігурації та попереднє налаштування

Таким чином, будемо вважати, що внутрішня локальна мережа має адресу 192.168.100.0 mask 255.255.255.0, внутрішня адреса порогового приладу (роутеру MikroTik) – 192.168.100.1, зовнішній інтерфейс (підключено Інтернет) – у першому порту – ether1 та має реальну IP адресу, наприклад 91.222.42.145, що надано провайдером за допомогою NAT на адресу 192.168.88.3 (рис. 3).

Один із засобів перевірити зовнішні налаштування роутера MikroTik це перейти із локальної мережі за адресом порогового роутера, в даному випадку, це: `hprpt://192.168.100.1` та обрати меню «IP» – «Cloud» потім кнопку «Force Update». Після чого

потрібно почекати поки відбудеться оновлення (рис. 4, а) та переглянути отримане повідомлення у верхній частині вікна додатку (рис. 4, б).

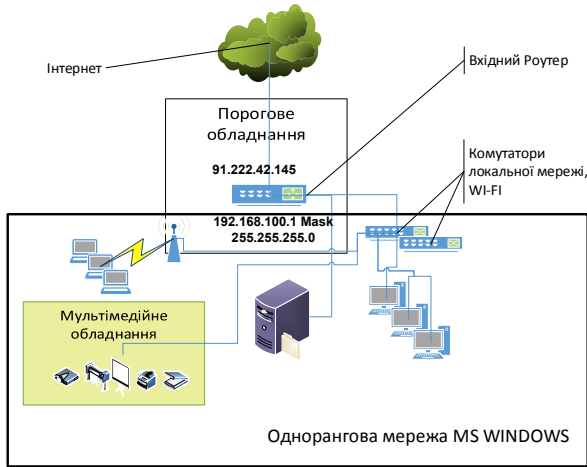


Рис. 3. Приклад адресації мережі НКЛ

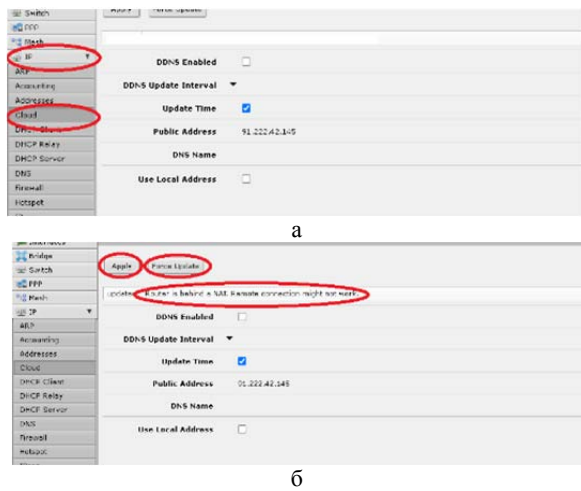


Рис. 4. Перевірка порогового роутера

Якщо у Вас є повідомлення, як на рис. 2.1, б: «Router is behind a NAT. Remote connection might not work» або «...service might not work», то треба звернутись до провайдера – у вас не має реальної IP адреси. У процесі практичного впровадження з’ясовано, що оновлення працює не стабільно та з великими затримками, а в деяких випадках – не видає помилки навіть в умовах повної відсутності реальної IP адреси.

Розглянемо деякі можливі ситуації. **Випадок перший.** Всі ресурси розташовані на одному вузлу локальної мережі НКЛ – наприклад, на внутрішній адресі – 192.168.100.2 . Це самий простий засіб організації віддаленого доступу до НКЛ та не потребує суттєвої переробки інформаційної структури.

Переходимо на сторінку порогового роутера та вибираємо «IP» – «FireWall», закладка «Nat» (рис. 5) та тиснемо кнопку «Add New» – відобразиться сторінка параметрів (рис 6), на якій вводимо:

Поле Chain – Dstnat (обов’язково) спрямованість пакету. У нашому випадку перенаправлення із зовнішньої мережі на внутрішню.

Поле Dst. Address – 91.222.42.145 (зовнішній IP адрес роутера), адреса призначення у пакеті. В деяких випадка, провайдер може надавати реальну IP адресу за допомогою свого NAT. В умовах експерименту це 192.168.88.3 – наш роутер використовує протокол NAT провайдера.

Поле In. Interface – ether1 – зовнішній інтерфейс роутера.

Поле Action – Dst-nat – переадресувати із зовнішньої мережі у внутрішню.

Поле To Addresses – 192.168.100.2 – внутрішня адреса вашого вузла з ресурсами (обов’язково).

Крім того, коли не задавати поля Dst. Address та In. Interface, то це правило буде працювати на всьому зовнішньому трафіку.

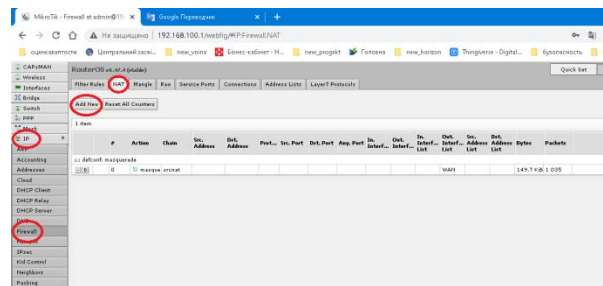


Рис. 5. Перехід до налаштування NAT

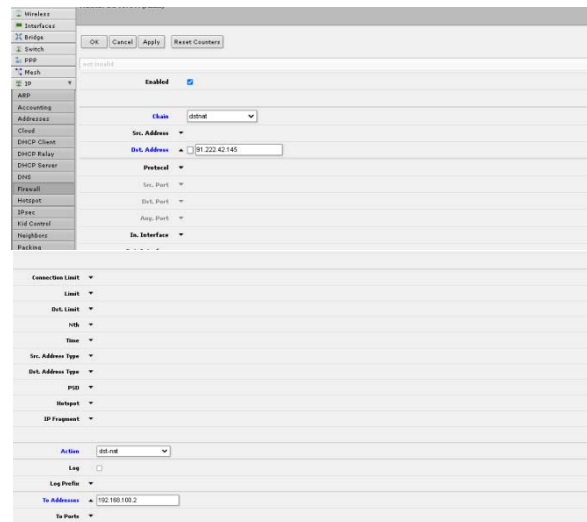


Рис. 6. Налаштування NAT для одного ресурсу

В результаті буде два правила Nat (рис. 7).



Рис. 7. Правила Nat для одного ресурсу

Якщо, налаштуєте роутер у новому стані, без спеціалізованих налаштувань, то все повинно працювати. В іншому випадку треба переглянути та налаштувати правила «Firewall». В загальному випадку повинно бути 11 правил «Firewall» (у меню «IP» – «FireWall», закладка «Filter Rules» (рис. 8).

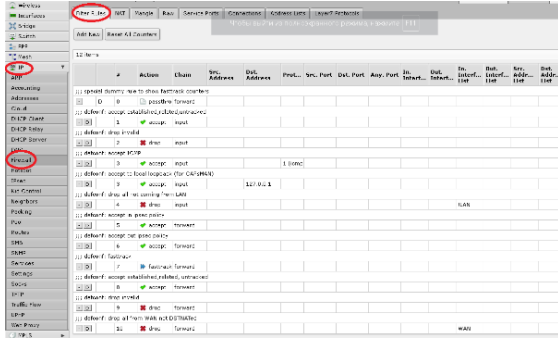


Рис. 8. Правила Filter Rules при першому налаштуванні

Випадак другий. Коли ресурси різного типу розташовані на різних вузлах НКЛ задача організації віддалено доступу вирішується аналогічно випадку 1, але треба ґрунтовно враховувати особливості протоколів (портів), що використовує кожний ресурс. Наприклад, є файловий ресурс мережі Microsoft на вузлу за адресом 192.168.100.2 та ВЕБ сервер – 192.168.100.7.

Файловий ресурс використовує багато портів, а ВЕБ сервер – порт 80. У такому випадку слід спочатку розташувати правило для ВЕБ серверу, а потім для файлового ресурсу. Слід враховувати, що порядок правил дуже важливий. Рекомендується більш «прості» ресурси розташовувати перед складними (менший номер правила). У будь-якому випадку є можливість змінити послідовність правил, перетягнув їх мишкою. Таким чином можна надати віддалений доступ багатьом ресурсам, якщо номери портів не співпадають.

Для виконання цього процесу треба знову перейти до правил NAT (рис.5) та додати правило для ВЕБ серверу (рис. 9) з наступними параметрами:

Поле Chain – Dstnat (обов’язково)

Поле Dst. Address – 192.168.88.3 (зовнішній IP адрес роутеру).

Поле Protocol – 6(tcp) – протокол ВЕБ серверу(обов’язково).

Поле Dst. Port – 80 – порт ВЕБ серверу (обов’язково).

Поле In. Interface – ether1 – зовнішній інтерфейс роутеру.

Поле Action – Dst-nat.

Поле To Addresses – 192.168.100.7 – внутрішня адреса ВЕБ серверу (обов’язково).

Потім додаємо правило таке як у Варіанті 1.

У результаті повинно бути три правила (одно за замовчанням –masquerade) – дивись рис. 10.

Для додавання другого ВЕБ серверу з адресом 192.168.100.9, якому теж потрібен порт 80 можна скористатися зміною порту на вхідному інтерфейсі,

наприклад, 8081. Для цього створюємо правило за такою схемою:

Поле Chain – Dstnat (обов’язково).

Поле Dst. Address – 192.168.88.3 (зовнішній IP адрес роутеру).

Поле Protocol – 6(tcp) – протокол ВЕБ серверу(обов’язково).

Поле Dst. Port – 8081 – порт ВЕБ серверу (обов’язково).

Поле In. Interface – ether1.

Поле Action – Dst-nat.

Поле To Addresses – 192.168.100.7 – внутрішня адреса ВЕБ серверу (обов’язково).

Поле To Port – 80 – внутрішня адреса ВЕБ серверу (обов’язково).

У такому випадку у строчці адреса браузера користувачі повинні набрати – <http://192.168.88.3:8081/>

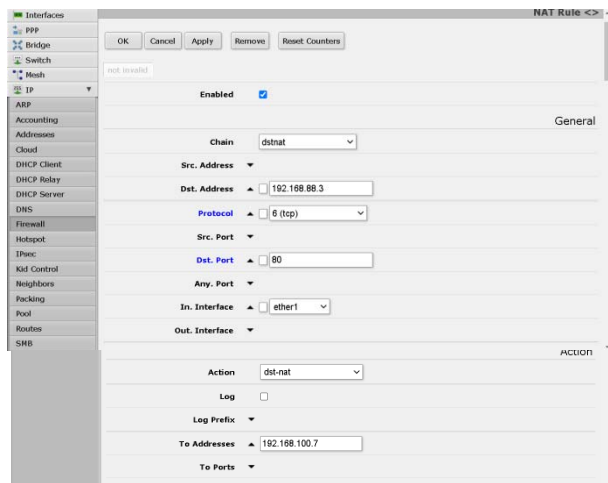


Рис. 9. Налаштування доступу до ВЕБ серверу

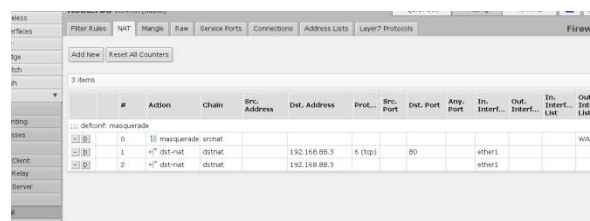


Рис. 10. Набір правил NAT для двох ресурсів

Це правило буде мати номер 3, то перенесемо мишкою його вище на номер 2 (рис. 11) та отримаємо чотири правила.



Рис. 11. Налаштування Nat з двома ВЕБ серверами та файловим ресурсом

Так необхідно створювати правила для багатьох ресурсів. Наприклад, для служби віддаленого робочого столу (192.168.100.13) за такими параметрами:

Поле Chain – Dstnat (обов'язково).

Поле Dst. Address – 192.168.88.3 (зовнішній IP адрес роутеру).

Поле Protocol – 6(tcp) – протокол RDP серверу(обов'язково).

Поле Dst. Port – 13389 – порт RDP серверу (обов'язково).

Поле In. Interface – ether1.

Поле Action – Dst-nat.

Поле To Addresses – 192.168.100.13 – внутрішня адреса RDP серверу (обов'язково).

Поле To Port – 3389 – внутрішня адреса RDP серверу (обов'язково).

У такому випадку у програмі «Підключення до віддаленого робочого столу» треба вказати адресу як показано на малюнку (рис. 12).

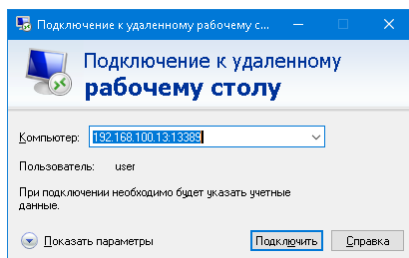


Рис. 12. Варіант підключення до віддаленого робочого столу

Таким чином можна продовжувати створювати правила для всіх ресурсів НКЛ та слідкувати за всіма використаними портами. Такий варіант можливий для простих ресурсів НКЛ, у яких відомо перелік портів та їх можна перенаправити.

Випадок третій. Для отримання повного доступу до всіх ресурсів НКЛ найпростіше скористуватись VPN сервісом. Цей сервіс є у системі роутеру MikroTik. Безумовно, існують і інші засоби створення VPN, наприклад, на сервері Microsoft Windows. Для цього бажано мати сервер з двома мережевими платами та додатково інсталиувати роль «Сервер політики мережі» (NPAS).

VPN буває декілька типів PPTP, L2TP, SSTP, OpenVPN та декілька типів тунелів. Це окреме питання, але в межах статті розглянемо, як організувати найпростішу VPN типу PPTP. Ця VPN має безліч недоліків з питань безпеки, але її налаштування дуже швидке. У випадку якщо ваш роутер не приймав участі у багатьох налаштуваннях та переналаштування та ніколи не активізувався VPN практично все зробить система Mikrotik Router OS.

Для початкового налаштування правил FireWale натисніть кнопку «Quik Set» в правому верхньому куті (рис. 13), увімкніть «VPN Access» введіть пароль та натисніть кнопку «Apply Configuration», а потім «WebFig» – у правому верхньому куті.

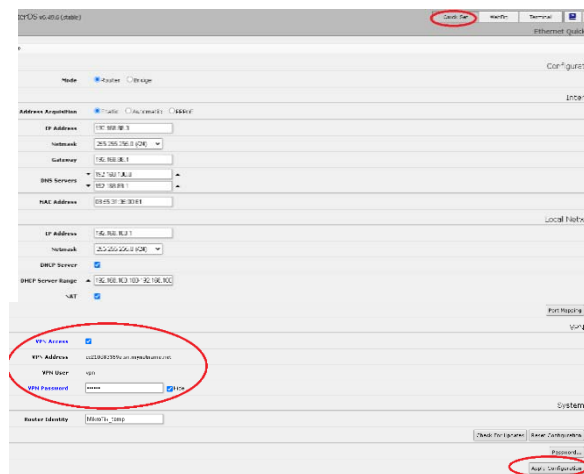


Рис. 13. Перехід до початкових налаштувань VPN

У меню «IP» – «FireWall», закладка «Filter Rules» повинно додатися декілька правил із загальною кількістю – не менш 17. А у меню «IP» – «FireWall», закладка «Nat» – на одно правило більше. Переходимо у «PPP» закладка «PPTP Server» та перевіряємо параметр «Enable» – повинен бути включений (рис.14), звертаємо увагу на поле «Default Profile» – “default encryption”, тиснемо «OK».

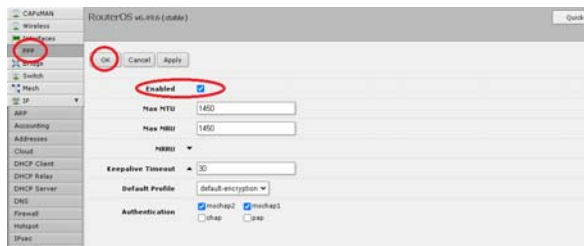


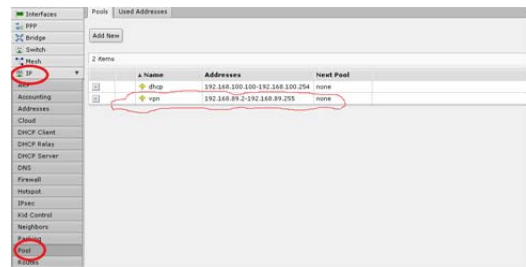
Рис. 14. Включити VPN Server

Потім, у цьому меню переходимо до «L2NP», «SSTP» та «OVPN Server» та їх статус «Enable» тимчасово відключаємо. Перевіряємо меню «IP» – «Pool», «IP» – «Routes» та «PPP» – закладка «Profiles» (рис. 15). Система Mikrotik RouterOS створить пул адрес 192.168.89.2 –192.168.89.255 та доддасть маршрутизацію на цю мережу 192.168.89.0/24. Важливо врахувати, що пул адрес з назвою VPN, не включає адресу «Profiles» “default-encryption” – 192.168.89.1, а маршрутизація повинна охоплювати всі адреси.

Для остаточного налаштування переходимо у «PPP» – «Secrets» та за аналогією з користувачем VPN створюємо інших користувачів, а користувача VPN змінюємо ім'я з міркувань безпеки, а бо зовсім необхідно видалити (рис. 16).

Це ще не остаточне налаштування, але все повинно працювати. На цьому попереднє налаштування буде завершено. Всі створені користувачі у меню «PPP» – «Secrets» будуть в змозі використовувати VPN клієнта на своїх персональних комп'ютерах після відповідного їх налаштування у додатку «Пара-

метри» – «Мережа та Інтернет» – VPN – «+ Додати VPN підключення» (рис. 17, а) з параметрами, що вказані на рис. 17, б.



а



б



в

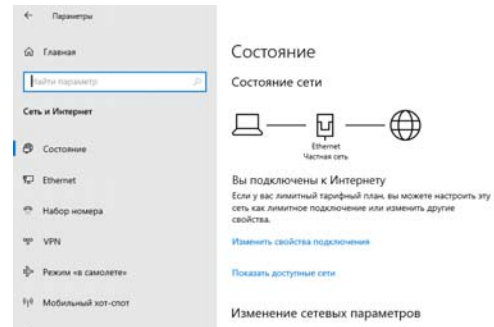
Рис. 15. Перевірка налаштувань



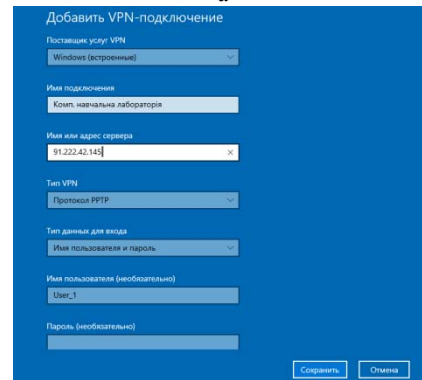
Рис. 16. Створення користувачів VPN у меню «PPP» – «Secrets»

У процесі впровадження цього рішення з'ясувалось ще одна особливість. При використанні VPN з'єднання у даному випадку шлюз за замовчанням буде налаштовано на адресу VPN – 192.168.89.1. Таким чином, в незалежності використовуються зараз користувачем ресурси НКЛ або ні – увесь трафік Інтернет буде спрямовано на ваш канал та запити на інші ресурси Інтернет будуть проходити через ваше з'єднання. З'ясувалось, що вирішити цей недолік можливо за рахунок використання спеціального додаткового пакету СМАК – пакет адміністратору.

Висновки. У процесі вирішення питання організації віддаленого доступу до навчальних інформаційних ресурсів НКЛ можливо скористатись декількома шляхами та ретельно провести основні етапи планування всієї інформаційної системи.



а



б

Рис. 17. Налаштування користувача

Один з ефективних шляхів – це використати в якості порогового приладу роутер MikroTik RB750Gr3 з оперативною системою RouterOS.

У випадку коли ресурси різного типу розташовані на різних вузлах НКЛ (або всі ресурси на одному вузлу) задача організації віддаленого доступу вирішується шляхом переназначення портів, але треба ґрунтовно враховувати особливості протоколів (портів), що використовує кожний ресурс та створити відповідні правила у «IP» – «FireWall», закладка «Filter Rules» та «NAT».

З іншого боку самий простий, але більш ефективний спосіб організації віддаленого доступу до основних ресурсів НКЛ – це скористатися системою VPN, яка швидко налаштовується на роутері MikroTik RB750Gr3.

Основний недолік цього засобу – це відсутність єдиного контрольованого доступу, створення умов використання тільки основних серверних машин та значні складності використання та контролювання локальних комп'ютерів НКЛ. Всі комп'ютери, окрім серверів, будуть простоювати.

Такий засіб є найпростішим, але далеко не єдиним та остаточним. Існує ще багато підходів заснованих на використанні Microsoft Windows Server та систем віртуалізації, наприклад рішеннях Vmware (ESXi, vsphere) або Citrix (XenServer). Однак вони потребують значних додаткових коштів та спеціалізованих фахівців для налаштування.

Література

1. Deusto LearningLab. URL: <https://learninglab.deusto.es/> (date of access: 02.05.2022).
2. Sysoieva S. DIGITALIZATION OF EDUCATION: PEDAGOGICAL PRIORITIES. Education: Modern Discourses. 2021. No. 4. P. 14–22. URL: <https://doi.org/10.37472/2617-3107-2021-4-02> (date of access: 04.05.2022).
3. Морзе Н.В. Моделі ефективного використання інформаційно-комунікаційних та дистанційних технологій навчання у вищому навчальному закладі. Інформаційні технології і засоби навчання. 2008. № 2 (6).
4. Стратегія розвитку вищої освіти в Україні на 2022 – 2032 роки. Міністерство освіти і науки України. URL: <https://mon.gov.ua/storage/app/media/news/2022/04/15/VO.plan.2022-2032/Stratehiya.rozv.VO-23.02.22.pdf> (дата звернення: 01.05.2022).
5. Теорія та практика змішаного навчання: монографія / В.М. Кухаренко та ін. Харків. Міськдрук, НТУ «ХП», 2016. 284 с.
6. Технологія розробки дистанційного курсу: навч. посіб. / В. Биков та ін. Київ: Міленіум, 2008. 324 с.
7. Щербина О.А. Нові засоби для оцінювання компетентностей в Moodle. Інформаційні технології і засоби навчання. 2016. № 55 (5). С. 96 – 104.

References

1. Deusto LearningLab. (2022). <https://learninglab.deusto.es/>
2. Sysoieva, S. (2021). DIGITALIZATION OF EDUCATION: PEDAGOGICAL PRIORITIES. Education: Modern Discourses, (4), 14 – 22. <https://doi.org/10.37472/2617-3107-2021-4-02>
3. Morze, N.V. (2008). Modeli efektyvnoho vykorystannia informatsiino-komunikatsiinykh ta dystantsiinykh tekhnolohii navchannia u vyshchomu navchalnomu zakladi. Informatsiini tekhnolohii i zasoby navchannia, 2 (6).
4. Stratehiia rozvytku vyshchoi osvity v Ukraini na 2022 – 2032 roky. (2022). Ministerstvo osvity i nauky Ukrainy. <https://mon.gov.ua/storage/app/media/news/2022/04/15/VO.plan.2022-2032/Stratehiya.rozv.VO-23.02.22.pdf>
5. Kukharenko, V., Berezenska, S., Buhaichuk, K., Oliinyk, N., Oliinyk, T., Rybalko, O. (2016). Teoriia ta praktyka zmishanoho navchannia: monohrafiia. Miskdruk. NTU “KhPI”, 2016. 284 p.
6. Bykov, V., Kukharenko, V., Syrotenko, N., Rybalko, O., Bohachkov, Yu. (2008). Tekhnolohiia rozrobky dystantsiinoho kursu: navch. posib. Milenium. 2008. 324 p.
7. Shcherbyna, O.A. (2016). Novi zasoby dlia otsiniuvannia kompetentnosti v Moodle. Informatsiini tekhnolohii i zasoby navchannia, 55 (5), pp. 96 – 104.

Mohylnyi H. Semenov M., Kiryeyev I. Implementation of a system of remote access to information resources of computer laboratories

The organization of learning computer laboratories in conditions of distance learning is associated with a number of issues, including the development and implementation of remote access to not only educational content but also resources of local network and service equipment: software and environments, servers, printers, digital devices, etc. Therefore, one of the main challenges in organization of distance learning for students, including IT specialties, is to create conditions for convenient access of students to the computer network of the university laboratory - ideally a complete simulation of work in the university computer laboratory with remote access. Despite the large number of papers dedicated to various aspects of distance learning, the problem of creating remote learning computer labs has not been sufficiently studied. The paper presents an analysis of existing approaches and principles of building a typical information structure of the learning computer laboratory. Based on the practical experience of using and modernizing such a system, a number of technical solutions aimed at organization of remote access to internal information resources of the learning computer laboratory are proposed. Of the many possible solutions for creating an information system with remote access, the three simplest and fastest options for their implementation are outlined. A number of options for organization of remote access were analyzed, in which the learning computer laboratory is built using the technology of redirection of individual ports to one node of the local network with various information, hardware and software resources, or several nodes, including one remote desktop server, web server and other resources with individual IP addresses. The main structural components of the remote access system based on VPN are studied and recommendations for their configuration and application are provided. The main features of VPN application using MikroTik router are given. The proposed approach allowed to reorganize the work of the learning computer laboratory and create new opportunities for the use of information resources by students and teachers of Luhansk Taras Shevchenko National University in conditions of distance learning that was introduced during the COVID-19 pandemic. The practical experience of using such an approach in 2020-2021 has proved its effectiveness.

Keywords: VPN, Windows Server, computer training lab, distance learning, computer network, remote access, port, protocol, PPTP.

Могильний Геннадій Анатолійович – к.т.н., доц., директор Навчально-наукового інституту фізики, математики та інформаційних технологій, Луганський національний університет імені Тараса Шевченка (м. Старобільськ), g.mogilnyi@gmail.com

Семенов Микола Анатолійович – к.пед.н., доц., завідувач кафедри інформаційних технологій та систем Навчально-наукового інституту фізики, математики та інформаційних технологій, Луганський національний університет імені Тараса Шевченка (м. Старобільськ), nick@luguniv.edu.ua

Кіреєв Ігор Юлійович – к.т.н., доц., доцент кафедри інформаційних технологій та систем Навчально-наукового інституту фізики, математики та інформаційних технологій, Луганський національний університет імені Тараса Шевченка (м. Старобільськ)