

User name:
Volodymyr Matiiievskiy

Check date:
18.01.2023 19:53:08 EET

Report date:
18.01.2023 19:54:19 EET

Check ID:
1013537804

Check type:
Doc vs Internet

User ID:
100010994

File name: **3_Могильний_Г_А_123**

Page count: **78** Word count: **10535** Character count: **83371** File size: **2.09 MB** File ID: **1013300981**

Text modifications detected (similarity score might be affected)

6.17% Matches

Highest match: **1.39%** with Internet source (<https://www.hkepc.com/forum/viewthread.php?fid=12&tid=2666271&page=1>)

6.17% Internet sources 46

Page 80

No Library search was conducted

0% Quotes

No quotes found

Exclusion of references is off

0.32% Exclusions

Some exclusions were automatic (exclusion filters: matched word count less than **10 words** and **0%**)

0.32% Internet exclusions 184

Page 81

No Library exclusions

Modifind

Text modifications detected. Find more details in the online report.

Replaced characters 2

Suspicious formatting 21 Pages

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ЗАКЛАД
„ЛУГАНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА”

Навчально-науковий інститут фізики, математики та інформаційних
технологій

Кафедра інформаційних технологій та систем

Могильний Геннадій Анатолійович

**АНАЛІЗ ПРОГРАМНО-АПАРАТНИХ МЕТОДІВ ОРГАНІЗАЦІЇ
ВІДДАЛЕНОГО ДОСТУПУ ДО НАВЧАЛЬНИХ
КОМП'ЮТЕРНИХ ЛАБОРАТОРІЙ ДЛЯ ПІДТРИМКИ
ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ**

кваліфікаційна робота
здобувача вищої освіти другого (магістерського) рівня
освітньої програми «Комп'ютерні мережі»
за спеціальністю 123 Комп'ютерна інженерія

Особистий підпис – _____ Геннадій МОГИЛЬНИЙ

Науковий керівник – _____ доцент кафедри ІТС, кандидат
(підпис) **технічних наук,**
Юрій ТИХОНОВ
(посада, науковий ступінь, наук. звання, прізвище)

Зав. кафедри – _____ зав. кафедри ІТС, кандидат
(підпис) **педагогічних наук, доцент,**
Микола СЕМЕНОВ
(посада, науковий ступінь, наук. звання, прізвище)

Полтава – 2023

АНОТАЦІЯ

Могильний Г.А.

Тема: Аналіз програмно-апаратних методів організації віддаленого доступу до навчальних комп'ютерних лабораторій для підтримки виконання лабораторних робіт.

Спеціальність: 123 «Комп'ютерна інженерія».

Установа: ЛНУ імені Тараса Шевченка, 2023р.

Магістерська робота містить: 78 с., 53 рис. 20 джерел.

Об'єкт дослідження – програмно-апаратні засоби організації віддаленого доступу.

Предмет дослідження – програмно-апаратні засоби та методи організації віддаленого доступу для виконання лабораторних робіт.

Мета дослідження – на основі комплексного аналізу організації роботи комп'ютерних навчальних лабораторій та особливостей роботи сучасних роутерів запропонувати засоби та методи створення віддаленого доступу до інформаційних ресурсів, що дозволить організувати виконання лабораторних робіт в умовах дистанційного навчання.

Результати роботи – Проведено комплексний аналіз існуючих інформаційних структур, які запроваджено у закладах освіти. Розгледіти різноманітні засоби та методи організації віддаленого доступу до інформаційних ресурсів комп'ютерних навчальних лабораторій. Розроблено рекомендації щодо впровадження віддаленого доступу до інформаційних ресурсів на засадах використання найпростіших типів VPN з метою надання можливостей доступу до наявних засобів обчислювальної техніки. В результаті розроблених рекомендацій створено можливості для виконання лабораторних робіт з обчислювальної техніки в дистанційних умовах.

Ключові слова: навчальна комп'ютерна лабораторія, віддалений доступ, навчальний процес, VPN, віддалений робочий стіл, Radius, Microsoft AD, RDP.

ANNOTATION

Mohylnyi H.

Theme: Analysis of software and hardware methods for organizing remote access to educational computer laboratories to support the performance of laboratory work

Speciality: 123 "Computer engineering".

Institution: Luhansk Taras Shevchenko National University (LTSNU), 2023 year.

Master's work of: 78 p., 53 im, 20 sources.

A research object of – hardware and software tools for organizing remote access.

The article of research – hardware and software tools and methods of organizing remote access for performing laboratory work.

An aim of research is - on the basis of a comprehensive analysis of the organization of the work of computer training laboratories and the features of the operation of modern routers, to propose means and methods of creating remote access to information resources, which will allow to organize the performance of laboratory work in the conditions of distance learning.

Job performances - A comprehensive analysis of the existing information structures implemented in educational institutions was conducted. Understand various means and methods of organizing remote access to information resources of computer educational laboratories.

Recommendations have been developed for the implementation of remote access to information resources based on the use of the simplest types of VPNs in order to provide access to available computing equipment. As a result of the developed recommendations, opportunities have been created to perform laboratory work on computer technology in remote conditions.

Keywords: educational computer lab, remote access, educational process, VPN, remote desktop, Radius, Microsoft AD, RDP.

3

ЗМІСТ

ВСТУП.....	6
РОЗДІЛ 1. АНАЛІЗ ІНФОРМАЦІЙНИХ СТРУКТУР НАВЧАЛЬНИХ ЗАКЛАДІВ	9
1.1. Особливості сучасної освіти	9
1.2 Типові структури навчальних комп'ютерних лабораторій.....	11
Висновки до розділу 1.....	16
РОЗДІЛ 2. НАВЧАЛЬНІ КОМП'ЮТЕРНІ ЛАБОРАТОРІЇ З ВІДДАЛЕНИМ ДОСТУПОМ	17
2.1 Загальні підходи створення системи з віддаленим доступом	17
2.2 Апаратне забезпечення для системи з віддаленим доступом.....	19
WI-FI роутер Tp_link TL-WR840N	20
WI-FI роутер Mercusys AC12g	20
AX1500 Wi-Fi 6 Router	23
Роутер MikroTik RB750Gr3	25
2.3 Розгортання систем з віддаленим доступом до НКЛ	28
Варіант 1. Всі ресурси розташовані на одному вузлу локальної мережі НКЛ	28
Варіант 2. Ресурси різного типу розташовані на різних вузлах НКЛ.....	32
Варіант 3. Отримання віддаленого доступу до робочого столу всіх комп'ютерів НКЛ.....	39
Варіант 4. Отримання повного доступу до всіх ресурсів НКЛ	49
Висновки до розділу 2.....	55
РОЗДІЛ 3. ІНФОРМАЦІЙНА БЕЗПЕКА НКЛ З ВІДДАЛЕНИМ ДОСТУПОМ.....	57
3.1 Загальний огляд моделей безпеки	57
3.2 Особливості впровадження системи безпеки у навчальних закладах	61
3.3 Концептуальна модель безпеки НКЛ з віддаленим доступом	63
Висновки до розділу 3.....	69
ВИСНОВКИ	70
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	73

Додатки.....	76
Додаток А Перелік команд загального налаштування роутеру MikroTik....	76
Додаток Б Перелік команд налаштування роутеру MikroTik для налаштування Firewall	77
Додаток В Перелік команд налаштування роутеру MikroTik для налаштування PPTP.....	78

ВСТУП

Епідемію коронавірусної інфекції та ворожу агресію російської федерації можна однозначно вважати головними викликами не тільки для нашої країни та для економік різних країн, а і для суспільства в цілому. COVID-19 та заходи, вжиті для протидії його поширенню, мали сильний негативний вплив на нормальне функціонування організацій, які здійснюють свою діяльність у різних сферах та галузях. Самоізоляція, періоди, повне закриття установ та підприємств сфер культури, туризму та громадського харчування, дистанційна форма роботи, обмеження доступу третім особам на різні підприємства та виробничі майданчики, скасування робочих нарад та партнерських зустрічей – все це нові умови, до яких багатьом необхідно було пристосуватися в максимально короткі терміни.

Сфера освіти стала винятком. І хоча дистанційні форми навчання динамічно розвивалися та активно використовувалися до епідемії коронавірусної інфекції та військової агресії 2022 року ці ПОДІЇ змусили освітні заклади різних рівнів масово переходити на дистанційний формат навчання та впроваджувати у свою діяльність відповідні інструменти, до чого багато хто був просто не готовий.

Перехід на цей формат навчання супроводжувався різними проблемами, у тому числі технічного та організаційного характеру. Значно збільшилися навантаження як на викладачів, так і на студентів вищих навчальних закладів та учнів шкіл. Найбільш значну проблему та негативну оцінку дистанційного формату навчання визвали питання проведення лабораторних робіт та відсутності необхідного матеріально-технічного забезпечення у переміщених закладах освіти. Таким чином, питання організації проведення лабораторних робіт є своєчасним завданням та потребою подальшого дослідження.

Мета дослідження – на основі комплексного аналізу організації роботи комп'ютерних навчальних лабораторій та особливостей роботи сучасних роутерів запропонувати засоби та методи створення віддаленого доступу до

інформаційних ресурсів, що дозволить організувати виконання лабораторних робіт в умовах дистанційного навчання.

Об'єкт дослідження – програмно-апаратні засоби організації віддаленого доступу.

Предмет дослідження – програмно-апаратні засоби та методи організації віддаленого доступу для виконання лабораторних робіт.

Для досягнення цієї мети необхідно вирішити наступні завдання:

- Проаналізувати існуючий стан інформаційно-технічного забезпечення закладів освіти та відокремити типові інформаційні структури навчальних закладів освіти.
- Навести існуючі походи до створення умов для віддаленого доступу до інформаційних ресурсів навчальних закладів в умовах дистанційного навчання та провести аналіз їх складності впровадження.
- Виконати огляд необхідного матеріально-технічного та програмного забезпечення навчальних комп'ютерних лабораторій та запропонувати шляхи для його вдосконалення та модернізації з метою створення безпечних умов для організації віддаленого доступу до інформаційних ресурсів та підвищення ефективності проведення лабораторних робіт.

В цілому магістерська робота складається з трьох розділів.

В першому розділі проведено аналіз існуючих інформаційних структур навчальних закладів, вказано їх особливості, переваги та недоліки. В результаті виділено три типи інформаційних систем НКЛ, які відрізняються ступнем централізації та готовості к переходу до роботи у дистанційних умовах.

Другий розділ присвячено огляду особливостей порогового обладнання та його програмного забезпечення необхідного для впровадження технологій віддаленого доступу до існуючих інформаційних ресурсів навчальних

комп'ютерних лабораторій. На прикладах чотирьох різноманітних роутерів та запропонованих чотирьох найпростіших варіантів організації віддаленоГО доступу наведено докладний перелік дій та етапів переходу та впровадження технологій віддалено доступу з метою підвищення ефективності використання існуючого програмно-технічного забезпечення навчальних комп'ютерних лабораторій.

У третьому розділі наведено опис **моделей** інформаційних загроз, які існують при впровадженні найпростіших методів створення віддалено ДОСТУПУ до інформаційних ресурсів навчальних комп'ютерних лабораторій. Розглянуто особливості впровадження системи інформаційної безпеки у навчальних закладах та запропоновану концептуальну модель безпеки навчальних комп'ютерних лабораторій з віддаленим доступом.

РОЗДІЛ 1. АНАЛІЗ ІНФОРМАЦІЙНИХ СТРУКТУР НАВЧАЛЬНИХ ЗАКЛАДІВ

1.1. Особливості сучасної освіти

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 2022р, 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.

Про стан та перспективи організації дистанційного навчання в закладах загальної середньої освіти України пишуть Ю. Бигич, Ю. Богачков, А. Букач, В. Буренко, В. Кухаренко, Т. Літвінова, Т. Свистунова, В. Харківець. Проблему використання елементів дистанційної освіти у вищій школі розглядають у своїх розвідках (І. Адамова, Ю. Василенко, А. Гуржій, О. Дмитрієнко, М. Жалдак, Л. Карташова, А. Кожевникова, Ю. Кравченко, О. Кузьмінська, Н. Лотошникова, А. Самусенко, П. Стефаненко). 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).

Однак, в такій складній ситуації, в той час коли багато закладів освіти працюють у дистанційних умовах, ефективне використання сучасних інформаційних технологій та прогресивних педагогічних засобів навчання неможливе без створення спеціалізованих умов у навчальних комп'ютерних лабораторіях (НКЛ) .

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.

1.2 Типові структури навчальних комп'ютерних лабораторій

У закладах освіти існує багата кількість НКЛ, які відрізняються як рівнем оснащення обчислювальною технікою так і різноманіттям програмного забезпечення в залежності від спеціалізації та особливостей навчального процесу. Однак, з точки зору організаційної інформаційної та мережевої структури можна виділити найбільш поширені типові структури НКЛ, які використовуються у багатьох закладах середньої освіти та більшості вишів і, в багатьох випадках зовсім не пристосовано до завдань вирішення проблеми надання віддаленого доступу тим хто навчається дистанційно .

Під інформаційною структурою НКЛ будемо розуміти — комплекс програмно-технічних засобів, організаційних систем та нормативних документів, який забезпечує організацію взаємодії інформаційних потоків, функціонування та розвиток програмно-технічних засобів інформаційної взаємодії в межах комп'ютерної навчальної лабораторії. В межах цієї роботи основний аналіз будемо проводити з урахуванням тільки програмно-технічних засобів існуючих у НКЛ та її мережевої структури.

На засадах попереднього аналізу та досвіду можна виділити найбільш поширену найпростішу типову структуру НКЛ, яка використовується у багатьох закладах середньої освіти та більшості вишів (рис. 1.1).

Така типова структура ефективно працює при умовах її безпосереднього використання в аудиторії та може включати: мережеве обладнання, робочі станції (персональні комп'ютери), мультимедійне обладнання, 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. Таким

11

чином, основна спрямованість інформаційних потоків – це однонаправлений обмін інформацією «із нутрі – назовні». Тільки, за умови розгалуженої кабельної мережі, викладачі зможуть проводити онлайн лекції з лабораторії зі студентами та учнями, які працюють дистанційно (дома). Жодних можливостей використати наявну комп'ютерну техніку та програмне забезпечення із дому не передбачено.

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



Рис.1.1 Найпростіша інформаційна структура НКЛ

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.

У деяких навчальних закладах для підвищення ефективності інформаційної системи додатково використовують файловий сервер та друксервер. Більшість таких серверів створено на засадах використання розподіленого файлового доступу мережі Ms Windows (рис. 1.2).

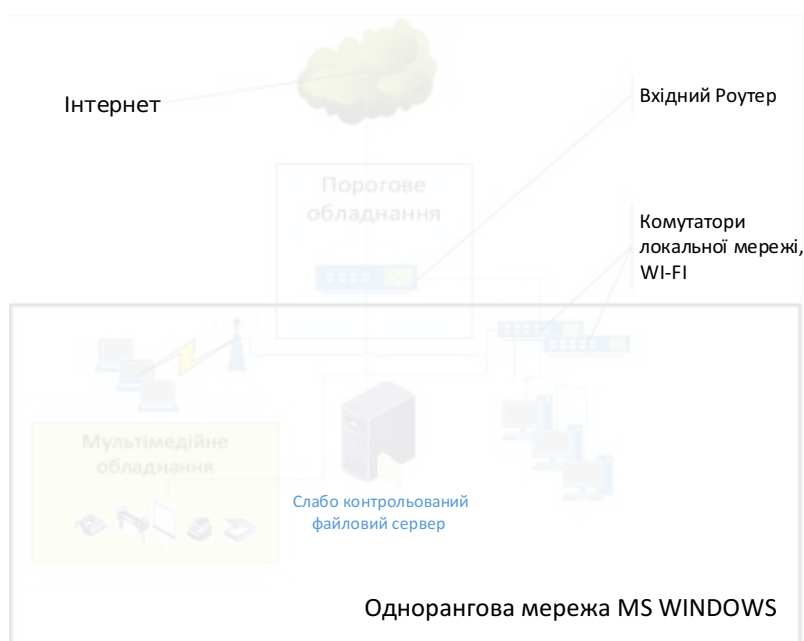


Рис.1.2. Типова схема найбільш поширеної інформаційної системи з підтримкою обміну файлами

При такому підході існують наступні недоліки:

- більшість файлових ресурсів буде слабо керуватись та працювати у режимі «тільки читання для ВСІХ» або обмеженого доступу «на запис» – для деяких користувачів;
- навчальні заклади зіштовхуються з багатьма питаннями безпеки, а в деяких випадках йдуть на організацію «неконтрольованої

файлової кучі» – будь хто може «покласти» файл та будь хто може його видалити.

На рисунку 1.3 показано спрощену схему НКЛ більш складної інформаційної –технічної структури, яка характерна для вищих навчальних закладів і дуже рідко використовується у закладах середньої освіти. Основною особливістю її є наявність розгалуженої мережі та окремо виділених обчислювальних машин великої продуктивності з серверними операційними системи (Microsoft Windows Server, linux server). Така структура дозволяє:

- створити умови для централізованого керування обчислювальними ресурсами за рахунок використання Microsoft Active Directory (Ms AD) або LDAP;
- забезпечити умови для подальшого розвитку інформаційної системи;
- використати програмного забезпечення віддалено доступу на засадах RDP до окремих серверів, принтерів, окремих робочих станцій;
- більш швидко запровадити перехід до дистанційних засобів навчання;
- створити умови для повної інтеграції усіх інформаційних ресурсів.

Однак, не багата кількість навчальних закладів перейшла на створення єдиного домену для всіх структурних підрозділів.

До недоліків системи створення єдиного домену Ms AD можна віднести наступне:

- потрібен навчально-допоміжний персонал більш високої кваліфікації;
- необхідне виділення окремих потужних обчислювальних машин для додаткових сервісів та служб;

- сервера Ms Windows є ядром такої системи, від якого залежить функціонування всієї інформаційної системи, тому необхідно створювати додатково систему резервного копіювання та підтримки;
- значна вартість ліцензійного програмного забезпечення для серверів;
- необхідність придбання додаткових ліцензій на користувачів (приладів);
- велика розгалуженість локальної мережі та структурних підрозділів та приладів, як правило, НЕ дозволяє повністю використовувати переваги домену, наприклад, особисті комп'ютери викладачів та студентів, спеціалізовані структурні підрозділи і таке інше.

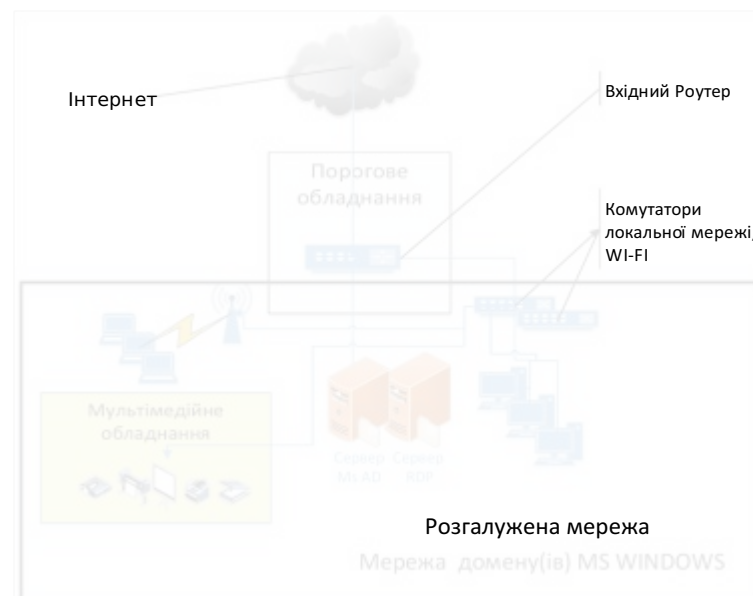


Рис.1.3. Типова схема керуємої інформаційної системи з підтримкою домену Ms AD

Висновки до розділу 1

Таким чином, загальний огляд існуючих інформаційних структур навчальних комп'ютерних лабораторій показав, що їх можна розподілити на 3 загальних типи:

1. Найпростіша інформаційна система, що характеризується слабкою централізацією та керованістю інформаційними ресурсами. Така система, як правило, має незначні програмно-технічні засоби, які потенційно можуть бути використані в режимі віддалено доступу та розрахована тільки на використання в аудиторному навчанні. Для переходу на режим використання в дистанційних умовах потрібно провести значне переналагодження порогових пристроїв та кожного комп'ютеру з урахуванням складності контролю за використаємиими засобами.
2. Інформаційна систем середнього класу характеризується наявністю деяких програмно-технічних засобів, які можуть бути використані при переході на дистанційний режим. Для переходу на дистанційний режим необхідно провести значне переналагодження порогових пристроїв, та часткове переналаштування внутрішніх сервісів.
3. Інформаційна система з доменом Ms AD характеризується великою степеню інтеграції, складною або розгалуженою мережею та у більшості випадків найбільш підготовлена для переходу на дистанційний режим роботи. Така система потребує переналагодження порогових приладів.

РОЗДІЛ 2. НАВЧАЛЬНІ КОМП'ЮТЕРНІ ЛАБОРАТОРІЇ З ВІДДАЛЕНИМ ДОСТУПОМ

2.1 Загальні підходи створення системи з віддаленим доступом

Важливим кроком у створенні системи з віддаленим доступом є етапи аналізу та планування переходу всієї інформаційної системи на використання віддаленого доступу. 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 віддаленому та безперервному (або необхідному) режимі, можливість їх переналадження 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 відповідно до завдань проекту EASMUS+ MoPED було проведено дослідження та впровадження різноманітних варіантів НКЛ з

17

віддаленим доступом. Досвід їх впровадження засвідчив той факт, що завдання аналізу та планування всієї інформаційної системи є складним, 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, наявність фінансування та кваліфікація навчально-допоміжного персоналу.

В окремих випадках необхідно приймати рішення спрямовані на першочергове виконання завдань, які можливо виконати та впровадити в існуючих умовах в стислий термін. 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 забезпечить її сталий розвиток.

Однак, з багатьох можливих рішень по створенню інформаційної системи з віддаленим доступом в межах цієї роботи 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 влаштовує.

- **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.** Ресурс одного типу, що використовує один порт але розташовані на різних вузлах НКЛ та за рахунок організаційних заходів може бути змінено.
- **Випадок 4.** 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.

2.2 Апаратне забезпечення для системи з віддаленим доступом

Одним з важливіших етапів створення НКЛ з віддаленим доступом є вибір засобу приєднання локальної мережі до мережі Інтернет. Існує декілька методів, однак всі вони поєднуються у два поширених підходи:

1. Створення порогового приладу на засадах виділеної обчислювальної машини з декількома мережевими адаптерами та налаштування системи доступу за рахунок можливостей певної операційної системи
2. Використання в якості порогового приладу окремого роутеру та налаштування його.

В межах цієї роботи розглянемо другий варіант. Безумовно, існує велика кількість роутерів, які можуть бути використані в якості порогового обладнання НКЛ. В межах цієї роботи розглянемо тільки деякі приклади:

- WI-FI роутер Tp_link TL-WR840N [11];
- WI-FI роутер Mercusys AC12g[12];
- WI-FI роутер Tp_link AX1500 Wi-Fi 6[13];
- Роутер MikroTik RB750Gr3 без підтримки WI-FI[14]

WI-FI роутер Tp_link TL-WR840N

Це недорогий роутер швидкістю до 300 МБ/с, який має 4 LAN порти зі швидкістю 100МБ/с та 1 WAN порт та відносно не дорогий – 700 грн, кількість антен – 2.

Для його налаштування використовується браузер, адреса за замовчанням 192.168.0.1 (на рис 2.4 адреса вже налаштована на 192.168.112.1).



Рис 2.4 Стан Tp_link TL-WR840N

Для його попереднього налаштування слід задати параметри зовнішнього підключення, локальної мережі та параметри DHCP серверу (рис.2.5).

WI-FI роутер Mercusys AC12g

Це більш сучасний роутер має загальну швидкість до 1200 Мбіт/с у двох діапазонах, який має 3 LAN порти зі швидкістю 1ГБ/с та 1 WAN порт та відносно не дорогий – 1500грн.



Рис. 2.5 Налаштування та підготовка до роботи

Для його налаштування використовується браузер, адреса за замовчанням 192.168.0.1 (на рис. 2.6 адреса вже налаштована на 192.168.113.1).



Рис.2.6 Стан роутеру Mercusys AC12g

Для його попереднього налаштування слід задати параметри зовнішнього підключення, локальної мережі та параметри DHCP серверу (рис.2.7-2.9).



Рис. 2.7 Зовнішня адреса



Рис. 2.7 Локальна адреса



Рис.2.9 Налаштування DHCP WI-FI роутер Mercusys AC12g

AX1500 Wi-Fi 6 Router

Це сучасний роутер має загальну швидкість до 1500 Мбіт/с у двох діапазонах, який має 4 LAN порти зі швидкістю 1ГБ/с та 1 WAN порт та відносно не дорогий – 2500грн.

Для його налаштування використовується браузер, адреса за замовчанням 192.168.0.1 (на рис 2.10).

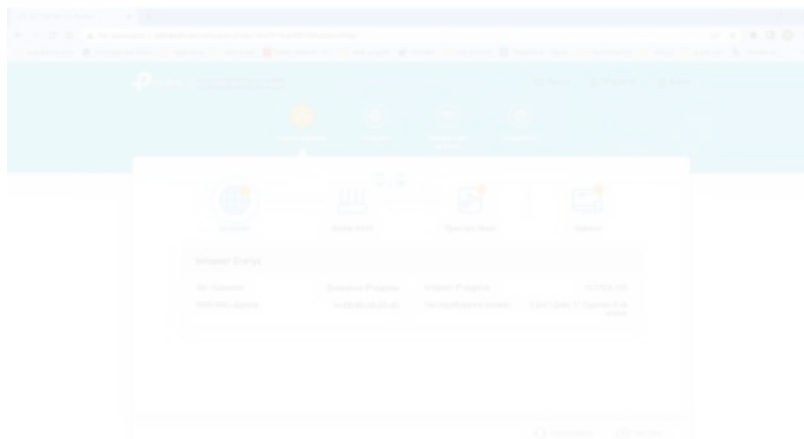


Рис. 2.10 Стан роутеру

Всі налаштування робляться аналогічно попереднім роутерам. Слід задати параметри зовнішнього підключення, локальної мережі та параметри DHCP серверу

Рис 2.11 Налаштування зовнішньої адреси

Рис 2.12 Налаштування зовнішньої адреси

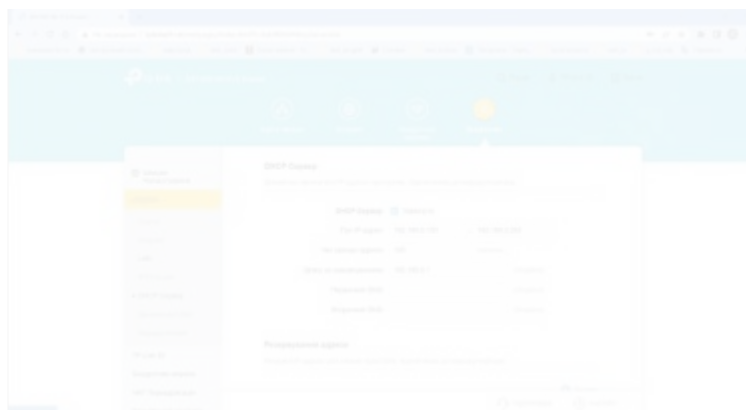


Рис 2.12 Налаштування DHCP

Роутер MikroTik RB750Gr3

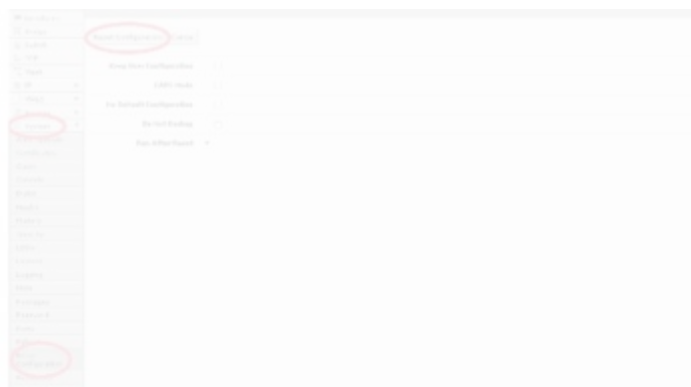
Налаштування цього роутеру суттєво відрізняється від попередніх. Роутер не має попередньо призначених інтернет портів та локальних портів.

Роутер має 5 рівноцінних портів зі швидкістю 1ГБ/с та ціну 2400грн.

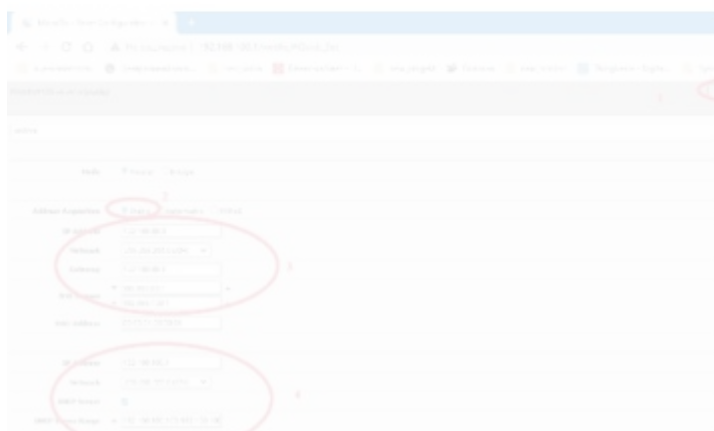
Для налаштування використовується браузер або спеціалізована програма WINBOX. Після очищення конфігурації (або за замовчанням) вважається, що 1 порт (ether1) – Інтернет з'єднання, а з 2 по 5 – локальна мережа. [15]

Слід відзначити, що роутери бренду MikroTik мають уніфікований принцип налаштування (внутрішня операційна система RouterOS) та відрізняються тільки характеристиками суцього технічного характеру: кількість портів, типи портів, швидкість маршрутизації пакетів, обсяг таблиці MAC адрес та інше. 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. 2.13, а) та налаштуємо її знову (так як показано на рис. 2.13, б).



а



б

Рис. 2.13. 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. 2.14).

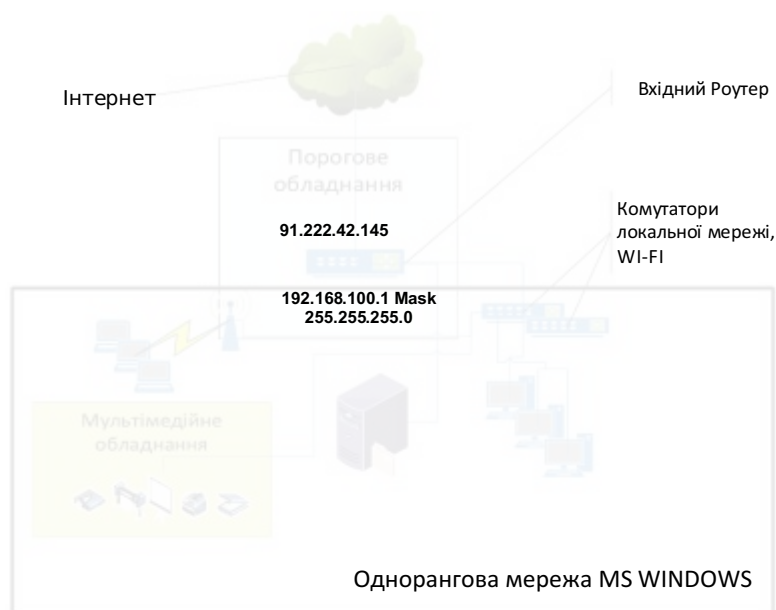
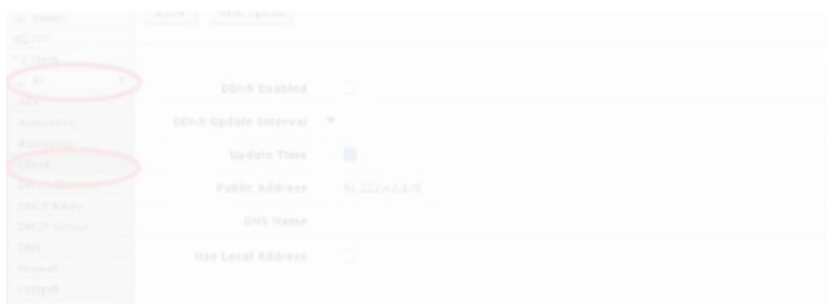
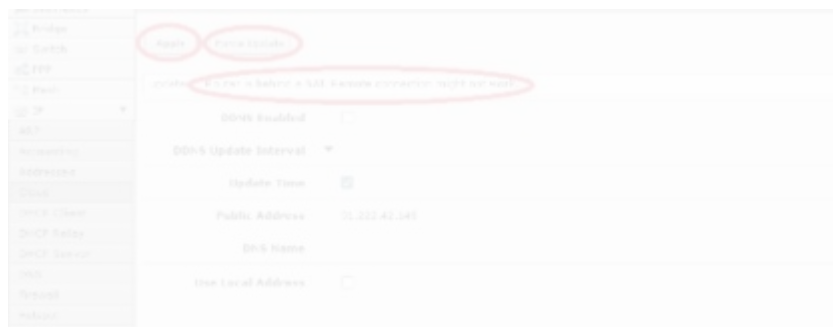


Рис. 2.14. Приклад адресації мережі НКЛ

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. 2.15, а) та переглянути отримане повідомлення у верхній частині вікна додатку (рис. 2.15,б).



а



6

Рис. 2.15. Перевірка порогового роутеру

Якщо у Вас є повідомлення, як на рис 2.15б: «Router is behind a NAT. Remote connection might not work.» або «...service might not work», то треба звернутись до провайдеру – 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.

2.3 Розгортання систем з віддаленим доступом до НКЛ

Варіант 1. Всі ресурси розташовані на одному вузлу локальної мережі НКЛ

Розглянемо деякі можливі ситуації. 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.

В цьому випадку на багатьох роутерах є можливість скористатися параметром DMZ. Слід зауважити, що адреса локального інформаційного ресурсу повинна бути статичного, тобто без використання DHCP.

DMZ (від англ. demilitarized zone) – це сегмент мережі, що містить загальнодоступні сервіси та відокремлює їх від приватних [8]. Як загальнодоступний може виступати, наприклад, вебсервіс: сервер, що його

28

забезпечує, який фізично розміщений у локальній мережі (Інтранет), повинен відповідати на будь-які запити із зовнішньої мережі (Інтернет), при цьому інші локальні ресурси (наприклад, файлові сервери, робочі станції) необхідно ізолювати від зовнішнього доступу. Мета DMZ — надати додатковий рівень безпеки в локальній мережі, який дозволяє мінімізувати збитки в разі атаки на один із загальнодоступних сервісів: зовнішній зловмисник має прямий доступ тільки до обладнання в DMZ [9].

На рисунках 2.16-2.18 показано як це зробити на роутерах:

- Tp_link TL-WR840N – адреса ще не вказано – треба замінити 0.0.0.0 на необхідну адресу вузла локальної мережі, перекинути «стан» в положення «включити» та натиснути кнопку «зберегти» (рис. 2.16);
- Mercusys AC12g – показано для вузла локальної мережі з адресом 192.168.113.100 та потім перекинути «DMZ Server» в положення «ON» (рис. 2.17);
- Tp_link AX1500 – показано для вузла локальної мережі з адресом 192.168.0.100 та потім встановити «DMZ» в положення «увімкнути» (рис. 2.18).

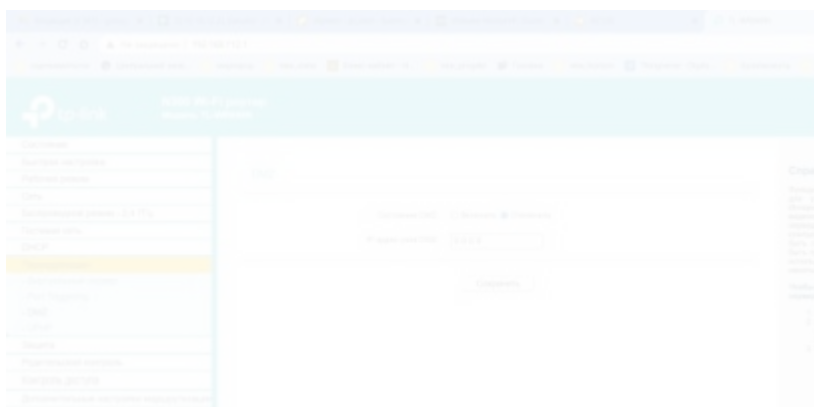


Рис. 2.16 Налаштування DMZ для Tp_link TL-WR840N



Рис. 2.17 Налаштування DMZ для Mercusys AC12g



Рис. 2.18 Налаштування DMZ для Tp_link AX1500

Найбільш складні налаштування для роутеру Mikrotik. Для цього необхідно: вибираємо «IP» – «FireWall», закладка «Nat» (рис. 2.19) та тиснемо кнопку “Add New” – відобразиться сторінка параметрів (рис 2.20), 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 роутеру), 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.

30

- Поле **In. Interface** – ether1 – зовнішній інтерфейс роутеру.
- 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. 2.19. Перехід до налаштування NAT

Рис. 2.20. Налаштування NAT для одного ресурсу

В результаті буде два правила Nat (рис. 2.21).



Рис. 2.21. Правила Nat для одного ресурсу

Якщо, налаштовуєте 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». Перелік команд наведено у Додатку А. (у меню «IP» – «FireWall», закладка «Filter Rules» (рис. 2.22).

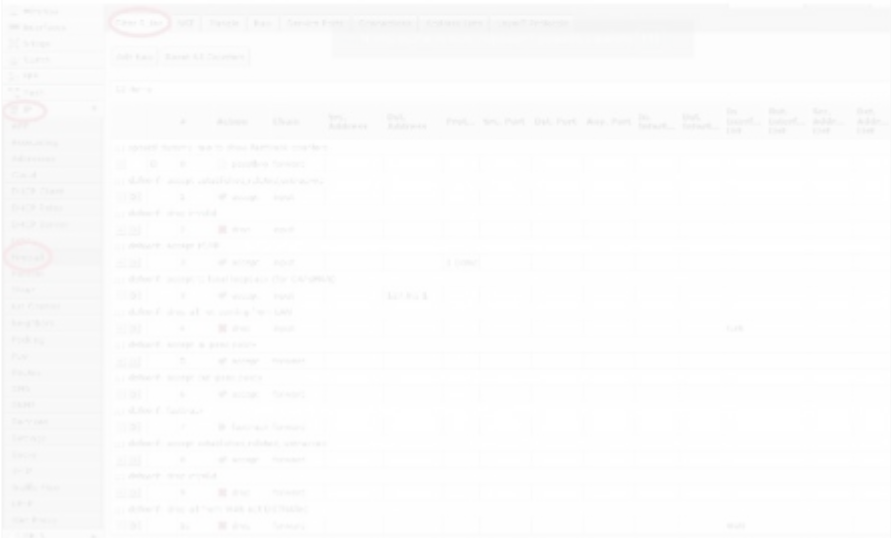


Рис. 2.22. Правила Filter Rules при першому налаштуванні

Варіант 2. Ресурси різного типу розташовані на різних вузлах НКЛ

Коли ресурси різного типу розташовані на різних вузлах НКЛ для задачі організації віддалено доступу треба ґрунтовно враховувати особливості протоколів (портів), що використовує кожний ресурс.

Треба врахувати три **особливості**:

1. З технічної документації встановити номери портів, що використовує кожна служба (ресурс), яка розташована на окремому вузлу локальної мережі.
2. Порти служб (ресурсів), що розташовані на різних вузлах локальної мережі не мають однакових номерів. Не може бути задіяно однакові порти на різних вузлах локальної мережі.
3. За рахунок організаційних заходів є можливість перевизначення співпадаючих портів на інші номери. Однак потрібно провести аналіз можливостей клієнтського програмного забезпечення для цих служб.

Наприклад, є ВЕБ сервер – 192.168.0.7 (порти 80 та 443), поштовий сервер – 192.168.0.8 (порти 25 та 110), FTP сервер – 192.168.0.9 (21,20 та 1024-1240).

Слід відзначити, що для багатьох роутерів ця задача вирішується приблизно однаково – за рахунок використання переадресування портів (меню – «віртуальний сервер» або «port forwarding»).

На рисунках 2.23-2.25 наведено меню роутерів Tp_link TL-WR840N, Mercusys AC12g та AX1500 Wi-Fi 6.

Детальне вирішення наведеного прикладу дано тільки для роутеру AX1500 Wi-Fi 6 на рисунках 2.26-2.27.

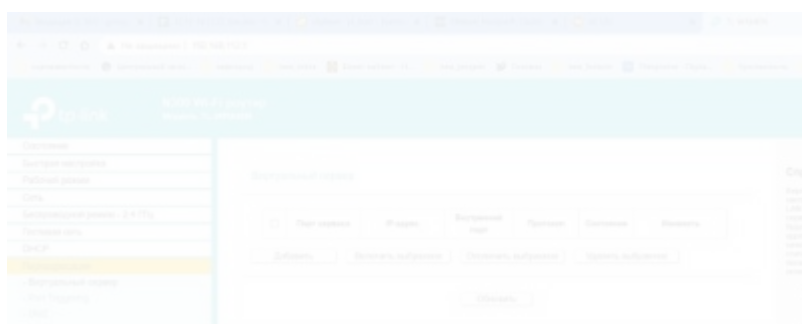


Рис. 2.23. Переадресування у роутері Tp_link TL-WR840N



Рис. 2.24. Переадресування у роутері Mercusys AC12g



Рис. 2.25 Переадресація у сервері AX1500 Wi-Fi 6



Рис. 2.26 Додавання ВЕБ – порт 80

Рис. 2.27 Загальна таблиця налаштувань переадресування

Для роутеру Mikrotik [16] задача переадресування портів вирішується в інший метод. Для прикладу, 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 перейти до правил NAT (рис. 2.19) та додати правило для ВЕБ серверу (рис. 2.28) 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).

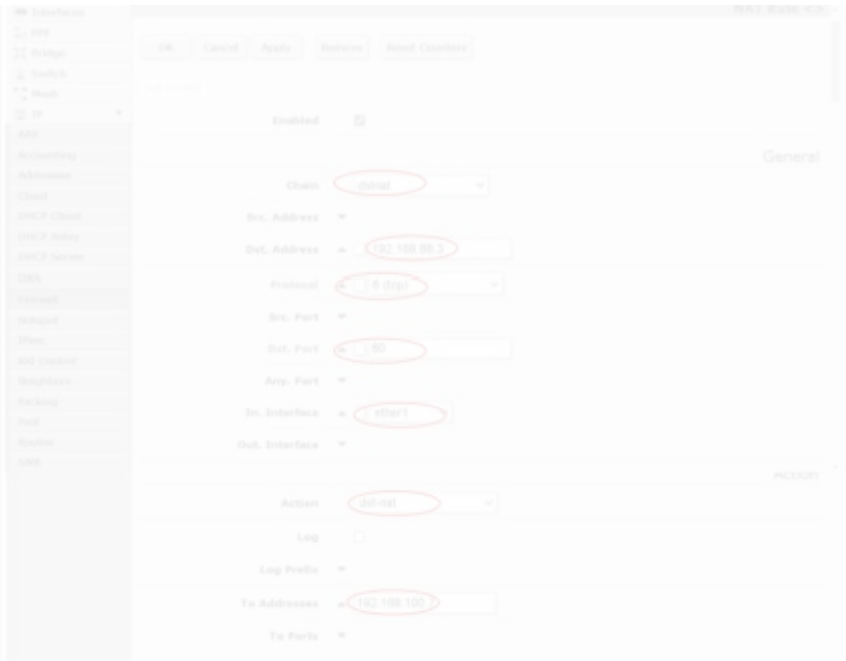


Рис. 2.28. Налаштування доступу до ВЕБ серверу

Потім , для другого вузлу, додаємо правило таке як у Варіанті 1. Таким чином призначаємо – всі інші порти – на адресу 192.168.100.2 .
У результаті повинно бути три правила (одно за замовчанням – masquerade) – дивись рис. 2.29.



Рис. 2.29. Набір правил NAT для двох ресурсів

Слід відзначити, що є можливість 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/>

Це правило буде мати номер 3, то перенесемо мишкою його вище на номер 2 (рис. 2.30) та отримаємо чотири правила.



Рис. 2.30. 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. 2.31).

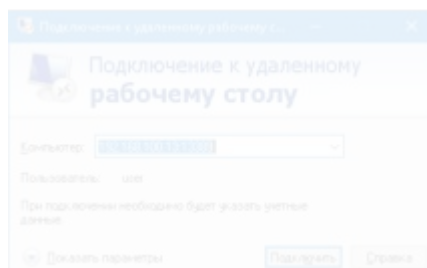


Рис. 2.31. Варіант підключення до віддаленого робочого столу

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.

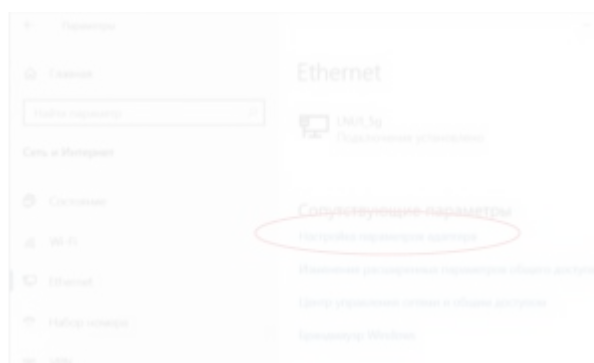
Таким чином, в результаті подібних дій, за рахунок організаційних заходів та принципу перепризначення портів є можливість створити віддалений доступ до всіх комп'ютерів НКЛ.

Варіант 3. Отримання віддаленого доступу до робочого столу всіх комп'ютерів НКЛ

В попередньому розділі розглянуто питання організації віддаленого доступу до НКЛ у випадку коли всі порти служб мають різноманітні номери. Однак більш ґрунтовний аналіз цього процесу дозволяє стверджувати, що за рахунок впровадження додаткових організаційних заходів є можливість надати доступ до віддалених робочих столів всіх комп'ютерів НКЛ.

Наприклад, у НКЛ використовується мережа 192.168.0.0/24, шлюз – 192.168.0.1, DNS – 192.168.0.1. Загальна методика впровадження цього процесу зводиться до наступних кроків:

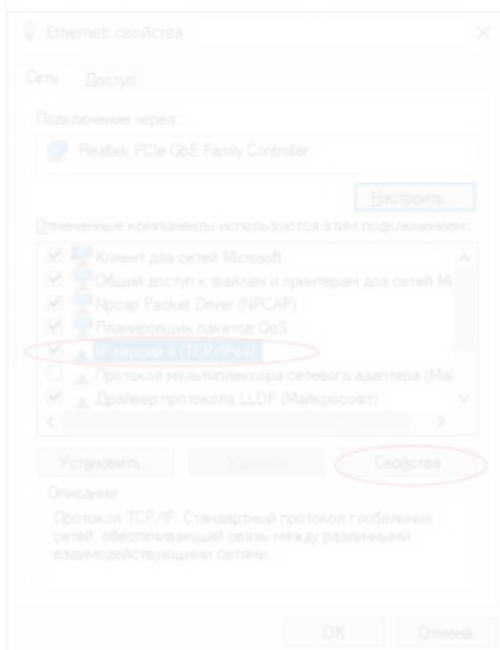
1. Переглянути систему адресації локальної мережі та відмовитись від використання DHCP.
 - а. Призначити статичні адреси всім комп'ютерам. Бажано ввести номера комп'ютерам та призначити подібні адреса (наприклад починаючи з 21). Комп'ютеру № 1 – 192.168.0.21, № 2 – 192.168.0.22 і так далі № 3 – 192.168.0.23 № 1 – 192.168.0.21. (Програма «Налаштування» – «мережа та Інтернет»



Обрати «Ethernet» «Налаштування параметрів адаптеру»



права кнопка на адаптері – «Властивості»



Обрати «IP версії 4 (TCP/IPv4) та натиснути «Властивості»



Рис. 2.32 Призначення статичної адреси

- б. Перевірити (або призначити) імена всіх комп'ютерів НКЛ. Наприклад, комп'ютеру № 1 з адресом 192.168.0.21 надати ім'я – comp1 комп'ютеру № 7 – 192.168.0.27 – comp7 і так далі



Рис. 2.33. Ім'я комп'ютера

2. Створити необхідну користувачів на кожному комп'ютері та додати до користувачів віддаленого робочого столу
 - а. Створення користувача (Права кнопка миші на програмі «Мій комп'ютер»)



Обрати меню «Керування»



Клацнути на пустому місці «Новий користувач»



Задати параметри користувача



Рис. 2.34 Створення користувача

- в. Призначити необхідних користувача – користувачем віддаленого робочого столу (Програма «Мій комп'ютер» – права кнопка

миші на пустому місці)



Обрати «Налаштування віддаленого доступу»



Вибрати «Вибрати користувачів»



Вибрати «Додати»



Вибрати «Додатково» та потім «Пошук»

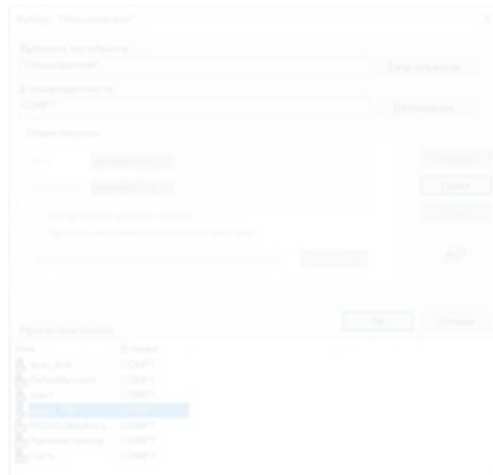


Рис. 2.35 Додавання користувача віддаленого робочого столу

3. Обрати зовнішні порти та створити необхідні налаштування роутеру

а. Вибрати схему призначення зовнішніх портів. Наприклад:

- i. для комп'ютеру № 1 - 192.168.0.21 3389+21=3410 приймаємо 3401,
- ii. для комп'ютеру № 2 – 3402,
- iii. Для комп'ютеру № 3 – 3403
- iv. і так далі

4. Створюємо необхідні відповідні записи на роутері.

- а. Для більшості офісних роутерів це завдання вирішується приблизно однаково. Розглянемо для роутеру AX1500 Wi-Fi, переходимо на сторінку налаштувань (<http://192.168.0.1>) – «Додатково» – «NAT переадресація» – «Port Forwarding»



Обираємо «Додати» та заповнюємо відповідні поля згідно прийнятої схеми пере направлення портів



в результаті отримуємо



Створюємо інші записи та додаємо всі наявні комп'ютери

Рис. 2.36 Налаштування доступу до віддалених робочих столів у роутері AX1500 Wi-Fi

b. Особливий випадок – роутер Mikrotik. Розглянемо той же випадок та послідовність дій у налаштуванні за допомогою програми winbox. При налаштуванні цього роутеру необхідно враховувати зовнішню адресу, наприклад 176.105.190.38. Обираємо меню «IP» – «Firewall» (рис. 2.37)

Рис. 2.37 Налаштування роутеру Mikrotik у програмі Winbox

Обираємо закладку «NAT» та натискаємо на кнопку «+» (Add) –

у новому вікні – закладка «General» та заповнюємо поля:

Поле **Chain** – Dstnat (обов’язково).

Поле **Dst. Address** – 176.105.190.38 (зовнішній IP адрес роутеру).

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

Поле **Dst. Port** – 3401 – зовнішній порт для доступу до віддаленого робочого столу комп’ютеру № 1 (обов’язково).

Поле **In. Interface** – ether1 (ім’я зовнішнього інтерфейсу, до якого підключено Інтернет з’єднання (рис. 2.38) .

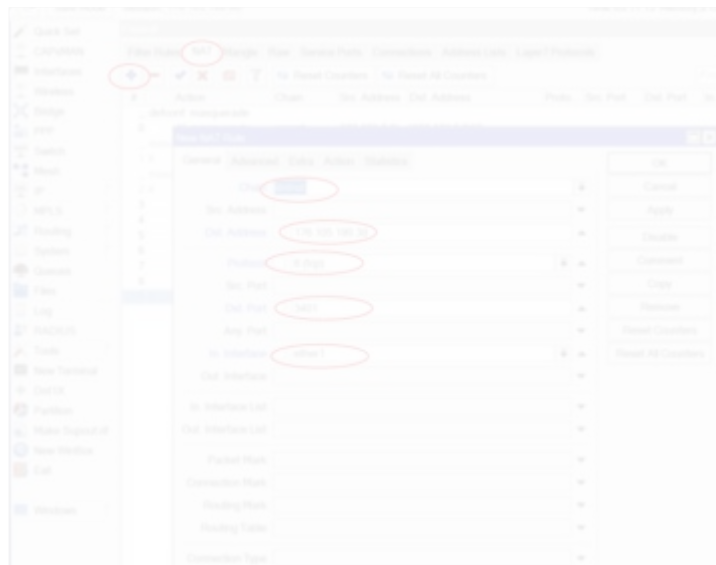


Рис. 2.38 Налаштування роутеру Mikrotik у програмі Winbox

Переходимо в закладку «Action» (рис.2.39)

Поле **Action** – Dst-nat.

Поле **To Addresses**– 192.168.0.21 – внутрішня адреса

комп'ютеру № 1 (обов'язково).
Поле **To Port**– 3389 – внутрішня адреса ввіддаленого робочого столу комп'ютеру № 1(обов'язково).

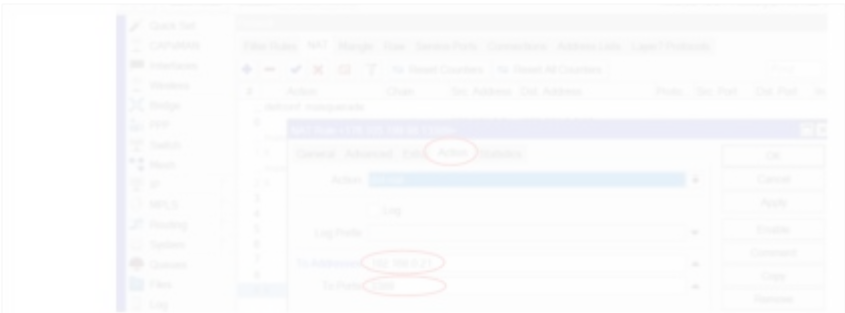


Рис. 2.39 Налаштування роутеру Mikrotik у програмі Winbox

Таким чином заповнюємо для всіх комп'ютерів з віддаленим робочим столом у НКЛ (рис. 2.40)

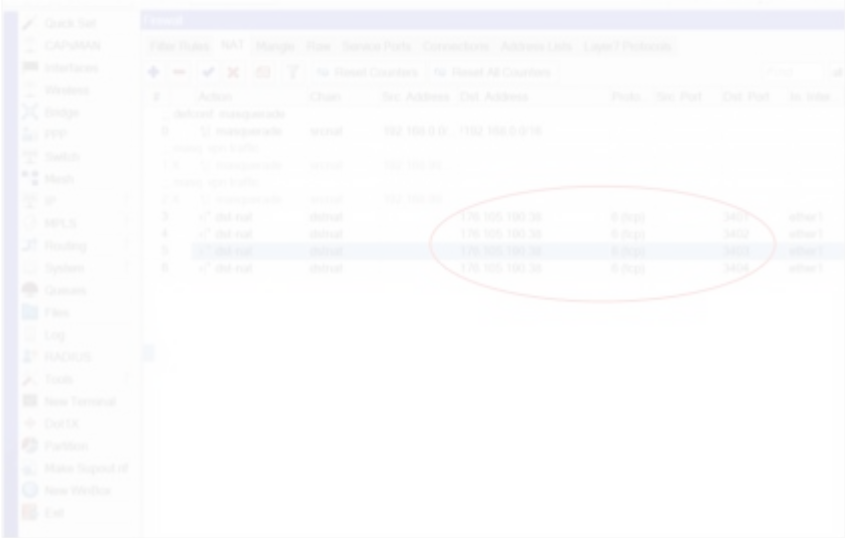


Рис. 2.40 Приклад створення доступу для комп'ютерів № 1-4

Варіант 4. Отримання повного доступу до всіх ресурсів НКЛ

Для отримання повного доступу до всіх мережевих ресурсів НКЛ найпростіше скористуватись VPN сервісом.

VPN буває декілька типів PPTP, L2TP, SSTP, OpenVPN та декілька типів тунелів. Це окреме питання, але в межах роботи розглянемо, як організувати найпростішу VPN типу PPTP. Ця VPN має безліч недоліків з питань безпеки, але її налаштування дуже швидке.

За рахунок використання цього сервісу вдається організувати доступ до всіх ресурсів НКЛ та досягти практично повної імітації присутності користувачів у НКЛ. Єдина різниця – здобувачі освіти не мають можливості використовувати консоль (клавіатура та миша) наявних комп'ютерів. Тому цей сервіс надає можливість використати саму мережу НКЛ (принтери, доступ до файлів та мережевих приладів) та надати доступ до всього програмного забезпечення, однак потребує переналаштування всіх комп'ютерів.

Отже, всіх перерахованих варіантів віддаленого підключення до НКЛ це найбільш ефективний.

Слід врахувати, що цей сервіс інтегровано у обжену кількість роутерів та їх вартість значно більша. Серед приладів-роутерів, які розглянуто в межах цієї роботи тільки два підтримують цю можливість:

- WI-FI роутер Tp_link TL-WR840N – не підтримує;
- WI-FI роутер Mercusys AC12g – не підтримує;
- WI-FI роутер Tp_link AX1500 Wi-Fi 6 – підтримує;
- Роутер MikroTik RB750Gr3 – підтримує

Безумовно, існують і інші засоби створення VPN, наприклад, на сервері Microsoft Windows. Для цього бажано мати сервер з двома мережевими платами та додатково інсталиювати роль «Сервер політики мережі» (NPAS).

Для створення VPN PPTP на роутері Tp_link AX1500 необхідно перейти на веб сторінку керування приладом та обрати меню «Додатково» –

«VPN Сервер» – «PPTP» (рис. 2.41). Включити «PPTP», налаштувати параметри підключення та призначити діапазон IP-адрес користувачів

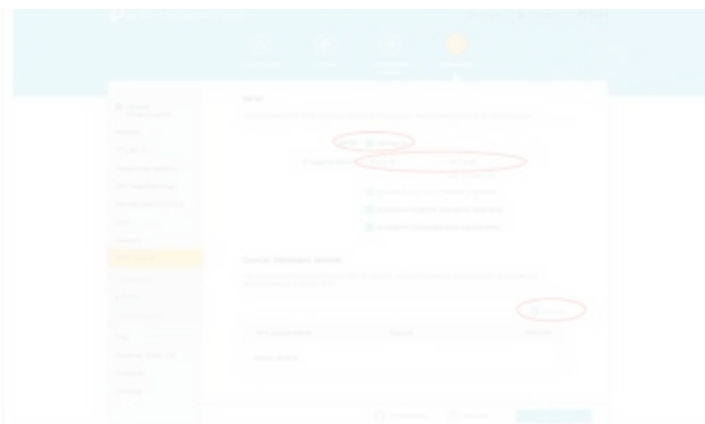


Рис. 2.41 Налаштування PPTP на роутері Tr-link AX1500

Після цього необхідно створити користувачів. Для цього натиснути кнопку «+»Додати та вказати ім'я користувача та пароль (рис.2.42)



Рис. 2.42 Додавання користувача VPN PPTP

Слід відзначити, що для цього роутеру є можливість створити до 16 користувачів, но одночасно можуть працювати тільки 10

Сервіс VPN PPTP є у системі роутеру MikroTik [17] та у випадку якщо роутер не приймав участі у багатьох налаштуваннях та переналаштування та ніколи не активізувався VPN практично все зробить система Mikrotik

RouterOS. Особливістю цього роутеру є те що кількість користувачів обмежена тільки продуктивністю роутеру.

Для початкового налаштування правил FireWale натисніть кнопку «Quick Set» в правому верхньому куті (рис.2.43), увімкніть «VPN Access» введіть пароль та натисніть кнопку «Apply Configuration», а потім «WebFig» – у правому верхньому куті.

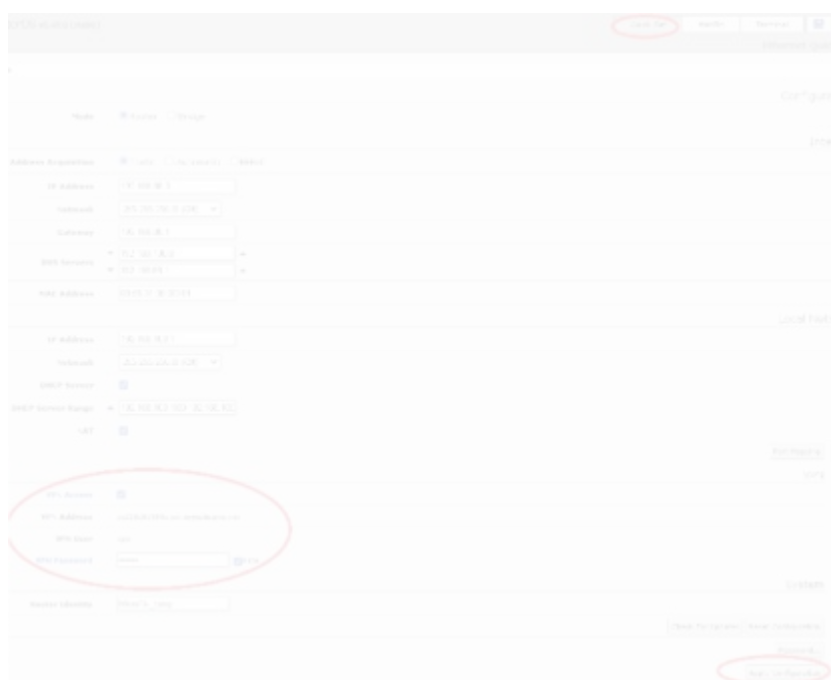


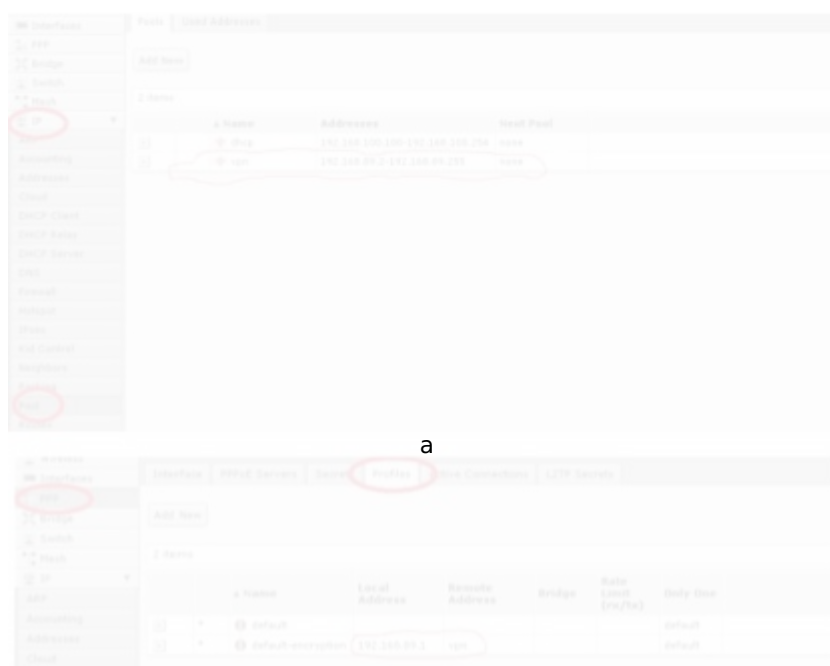
Рис. 2.43. Перехід до початкових налаштувань VPN

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 меню «PPP» закладка «PPTP Server» та перевіряємо параметр «Enable» – повинен бути включений (рис.2.44), звертаємо увагу на поле «Default Profile» – “default encryption”, тиснемо «OK».



Рис. 2.44. Включити VPN Server

Потім, у цьому меню переходимо до «L2TP», «SSTP» та «OVPN Server» та їх статус «Enable» тимчасово відключаємо. Перевіряємо меню «IP» – «Pool», «IP» – «Routes» та «PPP» – закладка «Profiles» (рис. 2.45). Система Mikrotik RouterOS створить пул адрес 192.168.89.2 – 192.168.89.255. Важливо врахувати, що пул адрес з назвою VPN, не включає адресу «Profiles» “default-encryption” – 192.168.89.1.



б

Рис. 2.45. Перевірка налаштувань

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. 2.46).

Будьте уважні, з'ясовано, що ім'я користувачів слід використовувати з урахуванням регістру.



Рис. 2.46. Створення користувачів VPN у меню «PPP»–«Secrets»

Це ще не остаточне налаштування, але все повинно працювати. На цьому попереднє налаштування буде завершено. Поступово створюємо інших користувачів (рис. 2.47)

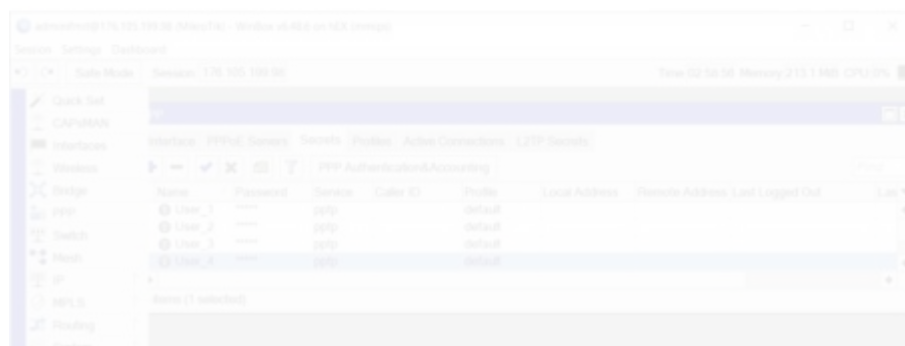


Рис. 2.47 Користувачі PPTP у роутері Mikrotik

Всі створені користувачі у меню «PPP» – «Secrets» будуть в змозі використовувати VPN клієнта на своїх персональних комп'ютерах після відповідного їх налаштування у додатку «Параметри» – «Мережа та Інтернет»

– VPN – «+ Додати VPN підключення» (рис. 2.48, а) з параметрами, що вказані на рис. 2.48, б.

a

6

Рис. 2.48. Налаштування користувача

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

використаються 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 можливого за рахунок використання спеціального додаткового пакету СМАК – пакет адміністратору.

Висновки до розділу 2

У процесі вирішення питання організації віддаленого доступу до навчальних інформаційних ресурсів НКЛ можливо скористатись декількома шляхами, однак необхідно ретельно провести основні етапи планування всієї інформаційної системи та етапів переходу до впровадження віддалено доступу.

Серед поширених роутерів далеко не всі мають можливості створення ефективної системи з віддаленим доступом. В роботі розглянуто 4 роутери. Один з ефективних шляхів – це використати в якості порогового приладу роутер MikroTik RB750Gr3 з оперативною системою RouterOS.

У випадку, коли всі ресурси розташовані на одному вузлі НКЛ, задача організації віддаленого доступу до нього вирішується практично на всіх роутерах за рахунок використання DMZ.

У випадку коли ресурси різного типу розташовані на різних вузлах НКЛ задача організації віддаленого доступу вирішується шляхом прокидання портів. Цей варіант організації підтримують практично всі існуючі роутери, але треба ґрунтовно враховувати особливості протоколів (портів), що використовує кожний ресурс. 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. Однак, за рахунок застосування додаткових організаційних заходів, можливо задіяння інших

комп'ютерів шляхом переназначення портів до їх віддаленого робочого столу. Цей варіант підтримують практично всі роутери.

Для використання цього варіанту самим складним, але ефективним приладом є MikroTik.

З іншого боку найпростіший, але більш ефективний спосіб організації віддаленого доступу до основних ресурсів НКЛ – це скористатися системою VPN. Серед досліджених роутерів тільки 2 мають таку можливість. Слід відзначити, що обмеження на кількість користувачів відсутні у MikroTik . VPN PPTP швидко налаштовується. Для цього необхідно створити відповідні правила у «IP» – «FireWall», закладка «Filter Rules» та «NAT».

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.

РОЗДІЛ 3. ІНФОРМАЦІЙНА БЕЗПЕКА НКЛ З ВІДДАЛЕНИМ ДОСТУПОМ

3.1 Загальний огляд моделей безпеки

Важливим питанням є розгляд та створення різних моделей інформаційної безпеки [18-20], які можуть застосовуватися під час побудови системи інформаційної безпеки. Існує кілька моделей, кожна з яких дозволяє відповісти на поставлені перед нею питання.

Можна виділити три основні моделі інформаційної безпеки, це:

- концептуальна модель,
- математична модель,
- функціональна модель.

Концептуальна модель дозволяє сформулювати найбільш загальні процеси створення системи безпеки вона створюється на першому етапі моделювання. Ця модель інформаційної безпеки відповідає на загальні питання і схематично відбиває загальну структуру моделі інформаційної безпеки, на ній як на стрижні будуються інші моделі і концепції інформаційної безпеки.

Математична модель – це формалізований опис сценаріїв у вигляді логічних алгоритмів представлених послідовністю дій порушників і заходів у відповідь. Розрахункові кількісні значення параметрів моделі характеризують функціональні залежності, що описують процеси взаємодії порушників із системою захисту та можливі результати дій. Саме такий вид моделі найчастіше використовується для кількісних оцінок уразливості об'єкта, побудови алгоритму захисту оцінки ризиків та ефективності вжитих заходів.

При побудові даних моделей необхідно спиратися на такі найважливіші обставини:

- Вибір критеріїв для оцінки важливості (пріоритетності) інформаційних ресурсів;

- створення кількісних показників різноманітних видів вразливостей об'єктів;
- вибір критеріїв оцінки запропонованих напрямків, методів та засобів захисту;
- створення кількісних показників різноманітних підсистем захисту;
- вибір критеріїв оптимальності системи захисту інформації для даної архітектури інформаційної системи;
- чітке математичне формулювання завдання побудови моделі засобів захисту інформації, що враховує задані вимоги до системи захисту та дозволяє побудувати засоби захисту інформації відповідно до цих критеріїв.

Вибір методу, який використовується в межах певної математичної моделі, відбувається за законами і правилами математики, тобто йдеться, наприклад, про метод оцінювання, про метод перевірки гіпотези, про метод доказовості теореми [10].

Безумовно з математичною моделлю на пряму пов'язана функціональна модель.

У подальшому, в межах функціональної моделі, розробляються і досліджуються алгоритми щодо практичного застосування і доказовості наведених припущень.[10]. Ця модель визначає потоки інформації, дозволені в системі, та правила керування доступом до інформації.

Існує декілька основних типів функціональних моделей:

1. Модель дискреційного доступу (DAC) – контролюється доступ суб'єктів (користувачів або додатків) до об'єктів, що становлять різні інформаційні ресурси: файли, додатки, пристрої виведення тощо. Класичний варіант – закрита система, тобто спочатку об'єкт не доступний нікому, і в списку прав доступу описується набір дозволів. У «відкритій» системі–за умовчанням усі мають повний доступ до об'єктів, а у списку доступу

описується набір обмежень. Реалізована в операційних системах Windows та Linux. Недолік моделі DAC полягає в тому, що суб'єкт, який має право на читання інформації, може передати її іншим суб'єктам, які цього права не мають, без повідомлення власника об'єкта.

2. Модель безпеки Белла-ЛаПадули – є одна з найвідоміших моделей безпеки (модель мандатного управління доступом). У ній визначено безліч понять, пов'язаних із контролем доступу. Даються визначення суб'єкта, об'єкта та операції доступу, а також математичний апарат для їх опису. Ця модель переважно відома двома основними правилами безпеки: одне відноситься до **ЧИТАННЯ**, а інше – до запису даних. на випадок, коли в системі необхідно мати декілька рівнів доступу – розрізняються нетаємні, конфіденційні, секретні та секретні дані. Користувач з рівнем допуску до секретних даних може читати несекретні, конфіденційні та секретні документи, а створювати лише секретні та конфіденційні. Таким чином, користувачі можуть читати лише документи, рівень секретності яких не перевищує їх допуску, і можуть створювати документи нижче за рівень свого допуску але прочитати їх вони не мають права. Недоліком є те, що ігнорується проблема зміни класифікації (рівня доступу): передбачається, що всі відомості відносяться до відповідного рівня таємності, але трапляються випадки, коли користувачі повинні працювати з даними, які вони не мають права побачити.

3. Рольова модель контролю доступу (RBAC) – контролює доступ користувачів до інформації на основі типів їх дій у системі. Під роллю розуміється сукупність дій та обов'язків, пов'язаних із певним видом діяльності. При цьому з кожним об'єктом зіставлено набір дозволених операцій доступу кожної ролі, а не певного користувача. Кожному користувачеві зіставлені ролі (у деяких – декілька ролей), які може виконувати. Модель широко використовується для управління привілеями користувача в межах єдиної системи або програми, наприклад у, Microsoft Active Directory, VMware Vsphere, FreeBSD, Solaris, СУБД Oracle, PostgreSQL 8.1, SAP R/3 та інших.

Системи розмежування доступу (СРД) – це сукупність реалізованих правил розмежування доступу у засобах обчислювальної техніки чи автоматизованих системах, більшість з яких базуються на концепції диспетчера доступу – абстрактної машини (захищений, відокремлений процес), яка виступає посередником при всіх зверненнях суб'єктів до об'єктів. Диспетчер доступу використовує базу даних захисту, в якій зберігаються правила розмежування доступу і на підставі цієї інформації дозволяє або не дозволяє суб'єкту доступ до об'єкта, а також фіксує інформацію про спробу доступу в окремому журналі. Ця база будується з урахуванням матриці доступу чи однієї з її перетворень. Таким чином матриця доступу – це таблиця, в якій рядки відповідають суб'єктам, стовпці – об'єктам доступу, а на перетині рядка та стовпця містяться правила (дозвіл) доступу суб'єкта до об'єкта.

Основними недоліками такої матриці є надмірно велика розмірність і складність адміністрування і для подолання цих складнощів матриця доступу в СРД часто замінюється деякими її перетвореннями:

- Списки керування доступом (access control lists, ACL). Для кожного об'єкта задано список суб'єктів, які мають ненульові повноваження доступу до них (із зазначенням цих повноважень).
- Списки повноважень суб'єктів. Аналогічно ACL, але для кожного суб'єкта заданий список об'єктів, доступ яких дозволено із зазначенням повноважень доступу. Таке уявлення називається профілем суб'єкта.
- Атрибутні схеми. Засновані на присвоєнні суб'єктам та/або об'єктам певних міток, що містять значення атрибутів. Елементи матриці доступу не зберігаються у явному вигляді, а динамічно обчислюються при кожній спробі доступу конкретної пари суб'єкт-об'єкт на основі їх атрибутів.

3.2 Особливості впровадження системи безпеки у навчальних закладах

Важливим питанням у створенні систем з віддаленим доступом є аналіз системи безпеки та створення різних моделей інформаційної безпеки, які можуть застосовуватися під час розробки та впровадження різноманітних програмно-технічних та організаційних заходів щодо забезпечення збереження інформації. Безумовно питання стабільності роботи обладнання, організації захищеного середовища даних та програмних розробок мають цілу низьку особливостей у навчальній комп'ютерній лабораторії. Ці питання межують між вимогами:

- відкритість навчального процесу та студентоцентроване навчання;
- забезпечити комфортні умови доступу до всіх матеріалів навчального процесу
- жорсткими положеннями до витоку конфіденційної та службової інформації.

Попередній аналіз діяльності НКЛ свідчить, що важною особливістю впровадження системи захисту у навчальних закладах є відсутність окремих відділів по захисту інформації.

В більшості випадків завдання по забезпеченню кібербезпеки покладено навчально допоміжний персонал. Крім того, слід враховувати дуже складну ситуацію у закладах середньої освіти. Всіма питаннями по налаштуванню роботи обчислювальної техніки, забезпеченню захисту інформації та організацію освітнього середовища у більшості випадків покладено на викладачів інформатики. У системі вищої школи та закладах середньої освіти не передбачено окремі посади, які відповідають за питання кіберзлочинності.

Значною особливістю вишів є велика різниця у кваліфікації викладачів та студентів. Навчальний процес більшості спеціальностей та освітніх програм містить освітні компоненти спрямовані на використання обчислювальної техніки та програмного забезпечення певної (дуже різноманітної) галузі знань.

НКЛ використовують як спеціальності з великим обсягом комп'ютерних дисциплін, так спеціальності, у яких знання засобів обчислювальної техніки та методів програмування не включено до основних компетентностей.

В результаті, процеси створення моделей захисту, впровадження певних заходів по їх удосконаленню, аналізу спроб несанкціонованою використання інформаційних ресурсів практично не виконуються або підтримуються на дуже слабкому рівні.

Таким чином, особливостями впровадження системи захисту інформації у НКЛ є:

- Відсутність відділів та осіб відповідальних за систему інформаційної безпеки;
- Недостатній рівень підготовки навчально-допоміжного персоналу в напрямку інформаційної безпеки;
- Значна різниця у кваліфікації користувачів: здобувачів освіти та викладачів;
- Відсутність системи моніторингу питань інформаційної безпеки;
- Недостатнє фінансування;
- Необхідність підтримки дистанційної освіти;
- Швидкий перехід на інформаційно-комунікаційні технології;
- Необхідність підтримки «відкритості» навчального процесу, всіх його складових та впровадження нових засобів розповсюдження інформації;
- Необхідність створення умов для використання різноманітних обчислювальних пристроїв (особистих комп'ютерів, мобільних пристроїв, планшетів та інше) викладачів та здобувачів освіти;
- Використання спеціалізованого програмного забезпечення для налаштування, моніторингу, обслуговування різноманітних обчислювальних приладів у навчальному процесі;

- Відсутність необхідного матеріально-технічного забезпечення в умовах швидкого впровадження рішень спрямованих на впровадження дистанційної освіти.

3.3 Концептуальна модель безпеки НКЛ з віддаленим доступом

Для побудови концептуальної моделі інформаційної безпеки незалежно від того, наскільки проста чи складна інформаційна система, необхідно як мінімум відповісти на три питання:

- що захищати;
- від кого захищати;
- як захищати.

Це обов'язковий мінімум, якого може бути достатньо невеликих інформаційних систем. Однак, беручи до уваги можливі наслідки, то краще виконати побудову повної концептуальної моделі інформаційної безпеки, в якій необхідно визначити (Рис. 3.1):

- джерела інформації,
- пріоритет чи ступінь важливості інформації,
- джерела загроз,
- цілі загроз,
- загрози,
- способи доступу,
- напрями захисту,
- засоби захисту,
- методи захисту.

При побудові моделі слід враховувати особливості діяльності структурного підрозділу. В межах цієї роботи розглянемо концептуальну модель за умови, що інші структурні підрозділи навчального закладу

знаходяться у відокремленому, окремому та захищеному інформаційному середовищі. Тому до моделі включено тільки інформацію, яка може бути розташована або використана у НКЛ.



Рис.3.1 Загальна концептуальна модель інформаційної безпеки

З врахуванням особливостей діяльності НКЛ та особливостей сучасного стану системи захисту інформації у навчальних закладах при побудові концептуальної моделі системи захисту інформації необхідно врахувати та планувати наступні дії:

1. Провести попередній моніторинг існуючої (або відсутньої) системи захисту інформації. За необхідністю, створити тимчасову комісію з питань інформаційної безпеки.
2. Призначити відповідальних осіб за систему захисту інформації.
3. Провести попередній аналіз доцільності впровадження системи з віддаленим доступом до НКЛ в умовах наявності/відсутності системи захисту інформації.
4. Відокремити першочергові заходи.
5. Провести попередній аналіз необхідних коштів для впровадження систем з віддаленим доступом та забезпечення певних мінімальних вимог до захисту інформації.

Безумовна концептуальна модель інформаційної безпеки НКЛ (рис.3.2) включає основні положення загальної моделі. В процесі її розробки необхідно проаналізувати та провести уточнення основних положень.

Джерела інформації НКЛ це:

- Навчально-методичні матеріали, які використовуються у навчальному процесі. Особливу увагу необхідно надати їх цілісності та створити умови для цілодобового використання. Слід зауважити, що матеріали комп'ютерних дисциплін можуть мати спеціальну навчально-технічну інформацію.
- Кабельна мережа, мережа Wi-Fi, її структура та адресування, імена користувачів та паролі. Дуже велике значення можуть мати «відкриті» імена користувачів та паролі, які використовуються у навчальних цілях.
- Співробітники, викладачі та студенти, які мають можливість випадково (або навмисно) повідомляти о наявних інформаційних ресурсах та шляхах їх використання.
- Серверні, локальні та особисті накопичувачі. Слід враховувати, що особисті накопичувачі слабо контролюються та можуть бути

джерелами вірусів або використовуватись для несанкціонованого доступу до інформації.

- Спеціалізоване програмне забезпечення, яке використовується у навчальному процесі. Особливу увагу слід приділити ПЗ, яке орієнтовано на налаштування, моніторинг та обслуговування обчислювальної техніки і використовується у навчальному процесі комп'ютерних спеціальностей.
- Мобільні пристрої та ноутбуки викладачів та студентів – це пристрої які можуть бути використані для створення різноманітних атак на інформаційну систему.
- Особисті документи викладачів, які зберігаються на інформаційних ресурсах

Пріоритетність інформації НКЛ має значні особливості в залежності від спрямованості самої НКЛ її структури. Попередній аналіз показав необхідність врахування інформації яка може створити умови для порушення системи безпеки, наприклад:

- Структура та адресування мережі, розташування серверних машин та мережевих приладів – це одна з найважливіших складових, використання якої може надати зловмиснику вагомі переваги у створенні загрози. Слід враховувати, що більшість НКЛ розповсюджує цю інформації в процесі виконання певних лабораторних робіт.
- Пріоритетні користувачі, їх імена, паролі та права доступу.
- Навчально-методичні матеріали можуть бути використані з метою особистої вигоди, впливу на оцінювання.
- Спеціалізоване програмне забезпечення **МО**же бути використано для організації атаки. Особливу загрози створюють спеціалізовані

програми спрямовані на вивчення та моніторинг комп'ютерного та мережевого обладнання.

- Загальне програмне забезпечення може бути непрацездатним та перешкодити проведенню навчальних занять.
- Особисті документи викладачів – ця інформація найменшого пріоритету для НКЛ.

Джерела загроз у НКЛ мають незначні особливості

- Інтернет – загроза, вплив якої значно зростає зі створенням системи віддаленого доступу і дає вплив на НКЛ постійно. Крім того, ця загроза надає можливість впливати на діяльність НКЛ багатьом користувачам, які підключені до Інтернет.
- Внутрішня мережа, яка в багатьох випадках «відкрита» для використання викладачами, гостями та здобувачами освіти.
- Прилади студентів та викладачів, які використовуються в межах «відкритого навчального середовища»
- Спеціалізовані прилади та ПЗ навчального процесу, яке може бути використано для несанкціонованого доступу.
- Інші відвідувачі, які відвідують навчальний заклад.

Цілі загроз у НКЛ в цілому співпадають з багатьма іншими підрозділами: ознайомлення, дублювання, модифікація, знищення, порушення працездатності. Слід відзначити, що треба додатково врахувати специфічні для НКЛ: цікавість, випадковість, порушення авторського права, використання в особистих цілях.

Загрози у НКЛ не відрізняються від інших установ та складаються з: доступність інформації, непрацездатність приладів та ПЗ, цілісність ПЗ та інформації, конфіденційність

До засобів доступу у НКЛ відносяться: розголошення, витік, особисті прилади, несанкціонований доступ.

Напрями захисту це: програмно – апаратний, організаційний, інженерно-технічний. Однак практично не можливо використати правовий (юридичний) напрям захисту, тому що більшість учасників освітнього процесу не пов'язано трудовими відносинами.

До методів захисту слід віднести: попередження, роз'яснення, запобігання. Більш слабкі методи у НКЛ: аналіз та вивчення випадків, припинення, протидія тому що вони потребують створення спеціалізованого підрозділу з безпеки інформації.

Таким чином, концептуальну модель інформаційної безпеки можна представити у вигляді схеми, що зображена на рис. 3.2.



Рис.3.2 Концептуальна модель безпеки НКЛ

Висновки до розділу 3

В результаті проведеного дослідження літературних джерел наведено огляд та класифікацію різноманітних моделей, які використовуються в процесах створення системи інформаційної безпеки. Встановлено, що першим важливим кроком є створення концептуальної моделі безпеки інформації.

Аналіз системи інформаційної безпеки у НКЛ показав, що більшості навчальних закладів необхідно більше уваги приділити процесам підвищення захищеності інформації. Важливу складову додає необхідність швидкого впровадження дистанційних методів навчання. Встановлено та наведено особливості процесу впровадження цієї системи. До основних, з яких, відносяться:

- відкритість навчального процесу та необхідність забезпечення доступу до всіх матеріалів навчального процесу;
- відсутність відділів та осіб відповідальних за систему інформаційної безпеки;
- значна різниця у кваліфікації користувачів: здобувачів освіти та викладачів;
- недостатнє фінансування;
- використання спеціалізованого програмно-технічного забезпечення у навчальному процесі та дозвіл на використання особистої техніки учасників навчального процесу.

З урахуванням цих особливостей розроблено концептуальну модель безпеки, на засадах якої можна розробити першочергові заходи спрямовані на підвищення інформаційної безпеки у навчальних закладах.

ВИСНОВКИ

Останні роки (2020-2022) суттєво вплинули на загальні підходи до організації освітнього середовища. Дуже важливу роль у цьому процесі відіграли коронавірусна інфекція (COVID-19) та військова агресія російської федерації, в умовах яких велика кількість навчальних закладів були вимушені перейти до інтенсивного використання дистанційних методів навчання. Більшість навчальних закладів доволі ефективно впровадили нові інформаційно-комунікаційні технології спрямовані організацію процесів спілкування та взаємодії типу «викладач— здобувач освіти». Однак, в такій складній ситуації, ефективне використання сучасних інформаційних технологій та прогресивних педагогічних засобів навчання неможливе без створення спеціалізованих умов у НКЛ.

Найбільш значну проблему визвали питання проведення лабораторних робіт та відсутності необхідного матеріально-технічного забезпечення у НКЛ.

В роботі на основі комплексного аналізу організації роботи НКЛ та запропоновані засоби та методи створення віддаленого доступу до інформаційних ресурсів, що дозволить організувати виконання лабораторних робіт в умовах дистанційного навчання.

Загальний огляд існуючих інформаційних структур навчальних комп'ютерних лабораторій показав, що їх можна розподілити на 3 загальних типи, які мають різні можливості для створення інформаційної системи з віддаленим доступом:

1. Найпростіша інформаційна система.
2. Інформаційна систем середнього класу.
3. Інформаційна система з доменом Ms AD та значною степеню інтеграції.

Важливим кроком у створенні НКЛ з віддаленим доступом є етапи аналізу та планування переходу всієї інформаційної системи на використання віддаленого доступу. Встановлені особливості переходу до цієї структури, однак, одним з важливіших – є вибір засобу приєднання локальної мережі до мережі Інтернет – вибір порогового приладу . У більшості випадків для цього використовуються спеціалізовані роутери.

В межах цієї роботи розглянуто тільки деякі приклади:

- WI-FI роутер Tp_link TL-WR840N;
- WI-FI роутер Mercusys AC12g;
- WI-FI роутер Tp_link AX1500 Wi-Fi 6;
- Роутер MikroTik RB750Gr3 без підтримки WI-FI

З багатьох можливих рішень по створенню НКЛ з віддаленим доступом в межах цієї роботи окреслено та надано комплекс заходів по їх розгортанню декілька поширених випадків:

- **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.** Ресурс одного типу, що використовує один порт але розташовані на різних вузлах НКЛ та за рахунок організаційних заходів може бути змінено.
- **Випадок 4.** Повний доступ до всіх ресурсів НКЛ.

Встановлено, що для підтримки всіх варіантів самим складним, але ефективним приладом є MikroTik.

Важливим питанням у створенні систем з віддаленим доступом є аналіз системи безпеки та впровадження різноманітних програмно-технічних та

організаційних заходів щодо забезпечення збереження інформації. Ці питання мають цілу низьку особливостей у НКЛ та межують між вимогами до відкритості навчального процесу, необхідністю забезпечення доступу до всіх матеріалів навчального процесу та жорсткими положеннями до витоку конфіденційної та службової інформації.

Досліджено та виявлено загальні особливості впровадження системи захисту інформації у НКЛ та розроблено концептуальну модель безпеки, на засадах якої можна запропонувати першочергові заходи спрямовані на підвищення інформаційної безпеки у навчальних закладах

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [illegible]

- 6)#cite_ref-FOOTNOTE%D0%A1%D0%BC%D1%96%D1%822006_2-0 (дата звернення: 21.12.2022)
- 10.Юлія Кожедуб. Функціональна модель системи забезпечення інформаційної безпеки.// Information technology and security. July-december 2018. Vol. 6. Iss. 2 (11) DOI: 10.20535/2411-1031.2018.6.2.153488
- 11.TL-WR840N V6.20 URL: <https://www.tp-link.com/uk-ua/home-networking/wifi-router/tl-wr840n/> (дата звернення: 21.12.2022)
- 12.AC1200 Двухдиапазонный гигабитный Wi-Fi роутер URL: <https://www.mercusys.com/ru/product/details/ac12g> (дата звернення: 21.12.2022)
- 13.AX1500 Wi-Fi 6 маршрутизатор URL: <https://www.tp-link.com/uk-ua/home-networking/wifi-router/archer-ax10/> (дата звернення: 21.12.2022)
- 14.Маршрутизатор MikroTik hEX (RB750Gr3) URL: <https://www.mikrotik.ua/product/mikrotik-hex-rb750gr3> (дата звернення: 21.12.2022)
- 15.Каталог приладів MikroTik URL <https://xn----7sba7aachdbqfnhtigr.xn--j1amh/katalog-ustroystv/nastrojka-mikrotik-hex-rb750gr3/> (дата звернення: 21.12.2022)
- 16.RouterOS URL: <https://xn----7sba7aachdbqfnhtigr.xn--j1amh/kategoriya-ustroystva/vse-kategorii/routeros/> (дата звернення: 21.12.2022)
- 17.Налаштування VPN через MikroTik URL: <https://deps.ua/ua/nowegable-base/samples-of-the-technical-solutions/7990.html> (дата звернення: 21.12.2022)
- 18.Оpirsky, I. Класифікація моделей захисту інформації в інформаційних мережах держави. Науковий вісник НЛТУ України, 25(10), 329-335. <https://doi.org/10.15421/40251050>
- 19.Trofymenko, O., Loginova, N., Serhii, M., & Dubovoi IY. (2022). Кіберзагрози в освітньому секторі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(16), 76-84. <https://doi.org/10.28925/2663-4023.2022.16.7684>

20. Avtushenko, O., Hyrda, V., Kozhedub, Y., & Maksymets, A. (2022). Аналіз методів, способів, механізмів, інструментів теорії прийняття рішень для моделювання систем захисту інформації. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(16), 159-171. <https://doi.org/10.28925/2663-4023.2022.16.159171>

Додатки

Додаток А Перелік команд загального налаштування роутеру MikroTik

```

# створення bridge
/interface bridge
add admin-mac=DC:2C:6E:5D:1D:50 arp=proxy-arp auto-mac=no comment=defconf \
    name=bridge

# призначення IP адрес для локальної мережі (192.168.100.0/24)
/ip address
add address=192.168.100.1/24 interface=bridge network=\
    192.168.100.0

# додаткове налаштування інтерфейсів
/interface ethernet
set [ find default-name=ether1 ] arp=proxy-arp
set [ find default-name=ether2 ] arp=proxy-arp
set [ find default-name=ether3 ] arp=proxy-arp
set [ find default-name=ether4 ] arp=proxy-arp
set [ find default-name=ether5 ] arp=proxy-arp
# необов'язкове створення переліку інтерфейсів: LAN - локальний та WAN - до
# Інтернет
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
# призначення членів до переліків інтерфейсів до WAN - один до LAN bridge
/interface list member
add interface=bridge list=LAN
add interface=ether1 list=WAN
# створення пулів адрес для зручності конфігурування
/ip pool
add name=dhcp ranges=192.168.100.100-192.168.100.254
add name=vpn ranges=192.168.98.2-192.168.98.254

# налаштування двох DHCP серверів
/ip dhcp-server
add address-pool=dhcp disabled=no interface=bridge lease-time=24m name=dhcp

# налаштування мережі DHCP серверу
/ip dhcp-server network
add address=192.168.100.0/24 dns-server=\
    192.168.100.8,176.105.220.22,209.244.0.3 gateway=192.168.100.1

```

Додаток Б Перелік команд налаштування роутеру MikroTik для налаштування Firewall

```
# " дозволити masquerade"
/ip firewall nat add chain=srcnat out-interface-list=WAN \
ipsec-policy=out,none action=masquerade

# налаштування фільтрів
/ip firewall
# далі йде набір фільтрів, які мінімально необхідні
# " приймати established,related,untracked"
filter add chain=input action=accept \
connection-state=established,related,untracked
# " блокувати invalid"
filter add chain=input action=drop connection-state=invalid

# " приймати ICMP"
filter add chain=input action=accept protocol=icmp

# " приймати to local loopback (for CAPsMAN)"
filter add chain=input action=accept dst-address=127.0.0.1

# " блокувати all not coming from LAN"
filter add chain=input action=drop in-interface-list=!LAN
# " приймати in ipsec policy"
filter add chain=forward action=accept ipsec-policy=in,ipsec
# " приймати out ipsec policy"
filter add chain=forward action=accept ipsec-policy=out,ipsec
# використовувати fasttrack"
filter add chain=forward action=fasttrack-connection \
connection-state=established,related
# " приймати established,related, untracke>
filter add chain=forward action=accept connection-
state=established,related,untracked
# " блокувати invalid"
filter add chain=forward action=drop connection-state=invalid
# " блокувати all from xpm dstnat
filter add chain=forward action=drop \
connection-state=new connection-nat-state=!dstnat in-interface-list=WAN

# блокувати непотрібні сервіси
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set ssh disabled=yes
```

Додаток В Перелік команд налаштування роутеру MikroTik для налаштування PPTP

```
# дозволити masquerade всіх мереж але блокувати їх з'єднання з WAN
/ip firewall nat
add action=masquerade chain=srcnat comment="defconf: masquerade" \
dst-address=!192.168.0.0/16 ipsec-policy=out,none out-interface-list=WAN \
src-address=192.168.0.0/16
# дозволити використовувати порт 1723
/ip firewall filter
add action=accept chain=input comment="allow pptp" dst-port=1723 \
in-interface-list=WAN protocol=tcp
```

Matches

Internet sources

46

2	https://www.hkepc.com/forum/viewthread.php?fid=12&tid=2666271&page=1	4 Sources	1.39%
3	http://elartu.tntu.edu.ua/bitstream/123456789/18982/2/2017_Opir_spezkyrs_Lekzii.PDF		1.28%
4	https://ivinas.gov.ua/publikatsiji/novi-vydannia-instytutu/download/1309_2c48241fd575bb7118cc72a7474c2bff.html		1.05%
5	https://uk.wikipedia.org/wiki/%D0%94%D0%B5%D0%BC%D1%96%D0%BB%D1%96%D1%82%D0%B0%D1%80%D0%B8%D0%...		1.02%
6	http://hnpu.edu.ua/sites/default/files/files/Kaf_vsesv_hist/Zb_Shodoznastvo/Shodoznastvo_2019.pdf	2 Sources	1%
7	https://education-trost.at.ua/print/Br_18.pdf		0.93%
8	http://dspace.wunu.edu.ua/bitstream/316497/41763/1/dis_tereschuk.pdf		0.84%
9	https://spw.ru/forum/threads/dostup-k-mikrotik-izvne.3633		0.82%
10	https://ela.kpi.ua/bitstream/123456789/33827/1/ITS2018-6-2_03.pdf		0.49%
11	https://kneu.edu.ua/userfiles/fupstap/Tr_ta_N_26_02_2020.pdf		0.42%
12	https://support.unet.by/knowledge_base/item/264413?sid=58365		0.41%
13	https://forummikrotik.ru/viewtopic.php?t=10979		0.38%
14	https://market.yandex.ru/product--wi-fi-router-tp-link-tl-wr1043nd-2010/6120422		0.34%
15	https://philarchive.org/archive/FEDTCO-6		0.2%
16	https://www.lnu.edu.ua/wp-content/uploads/2019/06/dis_pylypyuk.pdf		0.19%
17	https://chmnu.edu.ua/wp-content/uploads/disGavrichenko.pdf		0.18%
18	http://nbuv.gov.ua/node/5652		0.16%
19	https://www.uzhnu.edu.ua/uk/infocentre/get/48086		0.16%
20	https://topnet.com.ua/nastrojka-mikrotik-routeros		0.16%
21	https://lib.iitta.gov.ua/716487/1/%D0%9F%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%20%D0%93%D1%8...		0.15%

22	https://www.academia.edu/94688911/%D0%94%D0%BE%D1%81%D0%BB%D1%96%D0%B4%D0%B6%D0%B5%D0%BD%	6 Sources	0.15%
23	https://ivet.edu.ua/component/k2/item/download/196_4cf100c714a7ac2b8a4a693841af12cb		0.15%
24	http://elibrary.kdpu.edu.ua/xmlui/bitstream/handle/123456789/4050/%d0%b4%d0%b8%d0%bf%d0%bb%d0%be%d0%bc%20...		0.15%
25	https://www.technotrade.com.ua/Articles/mikrotik_router_setup.php		0.15%
27	http://mir.dspu.edu.ua/issue/download/15549/8588	5 Sources	0.13%
28	https://deps.ua/knowegable-base-ru/primery-tehnicheskikh-reshenij/7989.html	2 Sources	0.12%
29	http://elibrary.kdpu.edu.ua/bitstream/0564/2508/1/%D0%A6%D0%B8%D1%81%D1%8C_%D0%A1%D0%9D%D0%94.pdf	2 Sources	0.1%
30	https://www.freelancer.com/job-search/router-is-behind-a-nat.-remote-connection-might-not-work-mikrotik		0.09%
31	https://zakon.rada.gov.ua/go/1490-2022-%D0%BF	3 Sources	0.09%

Internet exclusions

5 Sources 1.56%

Page 81 of 82

https://visnyk.fem.sumdu.edu.ua/media/attachments/2020/02/15/10_pavlenko_1_2019.pdf	2 Sources	0.08%
https://www.ecofa.fr/livredor.php?msg=1		0.08%
https://lib.iitta.gov.ua/2170/1/%D0%91%D0%BE%D0%B9%D0%BA%D0%BE_%D0%A1_%D0%A2_2011.pdf	7 Sources	0.08%
http://phd.znu.edu.ua/page//dis/07_2020/Shcherbyna.pdf	11 Sources	0.08%
https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/31618/1/%D0%9C%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84...		0.08%
http://eprints.zu.edu.ua/27531/1/dys_Bosa.pdf		0.08%
http://eprints.zu.edu.ua/25852/1/dys_Solodovnyk.pdf	9 Sources	0.08%
https://www.lnu.edu.ua/wp-content/uploads/2018/03/dis_rozvod.pdf	8 Sources	0.08%
https://pedagogy.lnu.edu.ua/wp-content/uploads/2020/03/Jankovich_Osvit_tex.pdf		0.08%
https://uabio.org/wp-content/uploads/2016/04/position-paper-uabio-15-ua.pdf	7 Sources	0.08%
https://elearn.nubip.edu.ua/pluginfile.php/190079/mod_page/content/5/Lekcii/Lekcija_2.pdf	2 Sources	0.08%
https://kegt.rshu.edu.ua/images/dustan/2020/l_p_02.pdf	14 Sources	0.08%
https://www.uzhnu.edu.ua/uk/infocentre/get/13861		0.08%
https://dspace.library.khai.edu/xmlui/bitstream/handle/123456789/776/lvashchenko_A_M.pdf?sequence=1		0.08%
https://eprints.ugd.edu.mk/14774/1/2%20%D0%9A%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%	12 Sources	0.08%
https://www.edufuture.biz/index.php?title=%D0%92%D1%96%D0%B4%D0%B1%D0%B8%D0%B2%D0%B0%D0%BD%D0%BD%D1%		0.08%
https://www.edufuture.biz/index.php?title=%D0%9C%D0%BE%D0%BB%D1%8C%D1%94%D1%80_%E2%80%94%D0%BA%D0%	3 Sources	0.08%
https://repo.knmu.edu.ua/bitstream/123456789/5236/1/%D0%A5%D0%B8%D0%B6%D0%BD%D1%8F%D0%BA%20%D0%9D%	3 Sources	0.08%
https://dspace.hnpu.edu.ua/bitstream/123456789/7306/1/Dissertacia_Serhii_Kozin.pdf	2 Sources	0.08%