МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Український державний університет науки і технологій**

Кафедра Електронні обчислювальні машини
(повна назва)

«ДО ЗАХИСТУ»

Завідувач кафедри
_____ Жуковицький І.В.
(підпис) (ПІБ)
«21» 12 2021р.

# ДИПЛОМНА РОБОТА

на здобуття освітнього ступеня «магістр»

Галузь знань 12 Інформаційні технології
(шифр) (назва)

Спеціальність 123 Комп'ютерна інженерія
(код) (повна назва)

Тема: Дослідження можливостей використання нових технологій при побудові локальної мережі кафедри ЕОМ

Theme: Research of possibilities of using new technologies at construction of a local network of computer department

| | | | |
|---|---|---|---|
| Керівник дипломного проекту | професор (посада) | _____ (підпис) | Жуковицький І.В. (ПІБ) |
| Консультант розділу з БЖД | доцент (посада) | _____ (підпис) | Саблін О.І. (ПІБ) |
| Нормоконтролер | доцент (посада) | _____ (підпис) | Шаповалов В.О. (ПІБ) |
| Студент групи | КС2021 (група) | _____ (підпис) | Чернов Д.В. (ПІБ) |
| Student | | | Chernov Dmytro (family name) |

Дніпро
2021

**Довідка**

**про відсутність плагіату у випускній кваліфікаційній роботі**

Міністерство освіти і науки України

Український державний університет науки і технологій

Кафедра ЕОМ

ДОВІДКА

За результатами перевірки випускної кваліфікаційної роботи здобувача вищої освіти Чернова Дмитра Віталійовича

*(прізвище, ім'я, по батькові)*

на тему: Дослідження можливостей використання нових технологій при побудові локальної мережі кафедри ЕОМ

в роботі не виявлено порушень академічної доброчесності.

Керівник ВКР Ігор ЖУКОВИЦЬКИЙ

20.12.21

**Український державний університет науки і технологій**

**Факультет** «Комп'ютерні технології і системи» **кафедра** ЕОМ
**Спеціальність** 123 "Комп'ютерна інженерія"

**ЗАТВЕРДЖУЮ:**
**Завідувач кафедри**
д.т.н., проф._____(Жуковицький І.В.)
'_____'_____**2021 р.**

# ЗАВДАННЯ

до дипломної роботи на здобуття освітнього ступеня магістр

студента групи КС2021 Чернова Дмитра Віталійовича

**1. Тема дипломної роботи**: Дослідження можливостей використання нових технологій при побудові локальної мережі кафедри ЕОМ

**затверджена наказом по університету від** « 09 » 11 2021 р. № 11ст.
**2. Термін подання студентом закінченої роботи** 15 грудня 2021 р.
**3. Вихідні дані до дипломної роботи** Існуюча структура локальної мережі кафедри ЕОМ

**4. Зміст пояснювальної записки (перелік питань до розробки)**
4.1 Вступ
4.2 Аналіз існуючої структури мережі
4.2.1 Аналіз існуючої структури мережі кафедри ЕОМ
4.3 Огляд можливих нових технологій
4.3.1 Технологія Wi-Fi та механізми її захисту
4.3.2 Хмарні сховища даних
4.4 Пропозиції щодо вдосконалення архітектури локальної мережі кафедри ЕОМ
4.4.1 Загальна структура
4.4.2 Налаштування Cisco ASA 5505
4.4.3 Налаштування сервера
4.4.4 Налаштування Wi-Fi
4.5 Організація хмари у локальній мережі кафедри для використання у навчальному процесі
4.5.1 Аналіз хмарних сховищ даних
4.5.2 Налаштування хмарного сховища
4.6 Охорона праці та безпека у надзвичайних ситуаціях
4.7 Висновки
**5. Перелік креслень (демонстраційного матеріалу)**
5.1 Структура існуючої локальної мережі кафедри ЕОМ

5.2 Структура нової локальної мережі кафедри ЕОМ

5.3 Комп'ютерна презентація

## 6. Розділи та консультанти

| Розділ | Консультант | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| Основна частина | Жуковицький І. В. | | |
| Охорона праці та безпека в надзвичайних ситуаціях | Саблін О.І. | | |

## КАЛЕНДАРНИЙ ПЛАН

| № п/п | Назва розділів дипломного проекту (роботи) | Термін виконання розділів проекту (роботи) | Примітки |
|---|---|---|---|
| 1 | Вступ | 3% | |
| 2 | Аналіз існуючої структури мережі | 10% | |
| 3 | Огляд можливих нових технологій | 15% | |
| 4 | Пропозиції щодо вдосконалення архітектури локальної мережі кафедри ЕОМ | 30% | |
| 5 | Організація хмари у локальній мережі кафедри для використання у навчальному процесі | 25% | |
| 6 | Охорона праці та безпека у надзвичайних ситуаціях | 5% | |
| 7 | Висновки | 2% | |
| 8 | Оформлення пояснювальної записки | 10% | |
| | | | |

Дата видачі завдання: «_____»_____20___ р.

Керівник дипломної роботи _____ Жуковицький І. В.
(підпис) (ПІБ)

Завдання прийняв до виконання _____ Чернов Д.В.
(підпис) (ПІБ)

# РЕФЕРАТ

**Чернов Д.В. Дослідження можливостей використання нових технологій при побудові локальної мережі кафедри ЕОМ.** – Український державний університет науки і технологій, кафедра електронних обчислювальних машин. – Дипломний проект. – 61 с., 24 рис., 5 табл., 18 джерел.

Об'єктом дослідження дипломного проекту є використання сучасних технологій при проектуванні чи модернізації локальних обчислювальних мереж.

Метою роботи є розробка рекомендацій щодо оптимізації та модернізації локальної обчислювальної мережі кафедри «Електронні обчислювальні машини».

Робота складається з вступу, п’яти основних розділів, висновку та списку використаних джерел. В першому розділі наведено аналіз існуючої структури локальної мережі кафедри. В другому розділі проведено огляд нових технологій та можливості їх впровадження до мережі. В третьому розділі надано пропозиції щодо вдосконалення архітектури локальної мережі. Проведено налаштування встановленого нового мережевого обладнання. В четвертому розділі надано обґрунтування та вибір платформи, а також описано її налаштування для організації хмарного сховища у локальній мережі кафедри. В п’ятому розділі розглянуто питання охорони праці та безпеки в надзвичайних ситуаціях. У висновках сформульовано основні результати дипломної роботи.

Отриманні результати роботи можуть бути використанні при проектуванні чи модернізації локальної обчислювальної мережі. Надані рекомендацій дозволять, при використанні невеликих вкладень, підвищити ефективність використання локальної мережі, збільшити рівень її безпеки та зручність адміністрування.

ЛОКАЛЬНА МЕРЕЖА, БЕЗДРОТОВІ ТЕХНОЛОГІЇ, ХМАРНІ СХОВИЩА, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, LAN, VLAN, WI-FI, CISCO.

# RESUME

**Chernov D.V. Research of possibilities of using new technologies at construction of a local network of computer department**. - Ukrainian State University of Science and Technology, Department of Electronic Computers. - Diploma project. - 61 p., 24 figs., 5 tables., 18 sources.

The object of study of the diploma project is the use of modern technologies in the design or modernization of local area networks.

The work consists of an introduction, five main sections, a conclusion and a list of sources used. The first section presents an analysis of the existing structure of the local network of the department. The second section provides an overview of new technologies and the possibility of their implementation in the network. The third section provides suggestions for improving the architecture of the local network. Installation of the installed new network equipment is carried out. The fourth section provides a rationale and choice of platform, as well as describes its settings for the organization of cloud storage in the local network of the department. The fifth chapter deals with health and safety in emergencies. The main results of the work are formulated in the conclusions.

The obtained results can be used in the design or modernization of a local area network. The provided recommendations will allow, with the use of small investments, to increase the efficiency of the local network, increase its security and ease of administration.

LOCAL NETWORK, WIRELESS TECHNOLOGIES, CLOUD STORAGE, SOFTWARE, LAN, VLAN, WI-FI, CISCO.

**ЗМІСТ**

# ПЕРЕЛІК СКОРОЧЕНЬ

| | |
|---|---|
| ASA | Adaptive Security Appliance |
| ASDM | Adaptive Security Device Manager |
| DNS | Domain Name System |
| RDP | Remote Desktop Protocol |
| SSL | Secure Sockets Layer |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WEP | Wired Equivalent Privacy |
| Wi–Fi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |
| WPA | Wi–Fi Protected Access |
| ЕОМ | Електронні обчислювальні машини |
| ІОЦ | Інформаційно обчислювальний центр |
| ЛОМ | Локальна обчислювальна мережа |
| ОС | Операційна система |
| ПЗ | Програмне забезпечення |
| ПК | Персональний комп’ютер |

# ВСТУП

В даний час комп'ютерні мережі виконують різні функції — від створення домашньої мережі для відтворення та зберігання мультимедійного контенту до розробки глобальної обчислювальної мережі з мільйонами учасників, що виконують зберігання та обробку інформації.

Сучасні технології передачі даних дозволяють організувати обмін величезної кількості інформації на далекі відстані, дозволяючи великим компаніям, що володіють філіями по всьому світу, підтримувати оперативний обмін актуальною інформацією та виконувати свої завдання в строк, незалежно від географічного розташування [1].

Для будь-якої організації комп'ютерна обчислювальна мережа — це не самоціль, а засіб реалізації необхідних функцій. Будь-яка локальна мережа повинна бути спроектована виходячи з потреб і специфіки підприємства.

Основним завданням локальної обчислювальної мережі в освітній установі є управління інформаційними ресурсами, досягнення максимально швидкої взаємодії між відділами, спрощення роботи з документами, підтримка навчального процесу, а також оптимізація виробничих процесів.

Надійна та продуктивна локальна обчислювальна мережа забезпечує:

- централізований доступ до інформаційних ресурсів;
- інформаційну взаємодію між співробітниками та відділами;
- ефективний спосіб подання навчального матеріалу;
- скорочення обсягів паперової роботи, дозволяючи вивільнити трудові та матеріальні ресурси;
- оперативність і високу точність даних і результатів їх обробки;
- підвищення продуктивності праці співробітників.

Актуальність дослідження визначається тим, що локальна мережа є визначальним компонентом інформаційної стратегії організації та недостатня увага до оцінки її продуктивності та планування шляхів розвитку призводить до необхідності повної або часткової реконфігурації.

Об'єктом дослідження є використання сучасних технологій при проектуванні чи модернізації локальних обчислювальних мереж.

Предметом дослідження є варіанти сучасних бездротових та хмарних технологій та їх використання у локальних обчислювальних мережах.

Метою роботи є розробка рекомендацій щодо оптимізації та модернізації локальної обчислювальної мережі кафедри «Електронні обчислювальні машини».

Практична цінність. Реалізація проекту дозволить підвищити продуктивність та безпеку існуючої локальної обчислювальної мережі, скоротити час на обробку інформації, знизити обсяг мережевого трафіку, скоротити обсяг паперового документообігу, уникнути втрати критично важливої інформації..

Апробація та публікації. Основні результати роботи представлені в доповіді на міжнародній науково-практичній конференції 2021 р. «Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості та освіті».

Тези доповіді опубліковані.

# 1 АНАЛІЗ ІСНУЮЧОЇ СТРУКТУРИ МЕРЕЖІ

## 1.1 Аналіз існуючої структури мережі кафедри ЕОМ

Мережа кафедри ЕОМ базується на технічних засобах ПК та ЛОМ і являється підсистемою корпоративної мережі університету. Існуюча структура мережі кафедри ЕОМ представлено на рис.1.1.

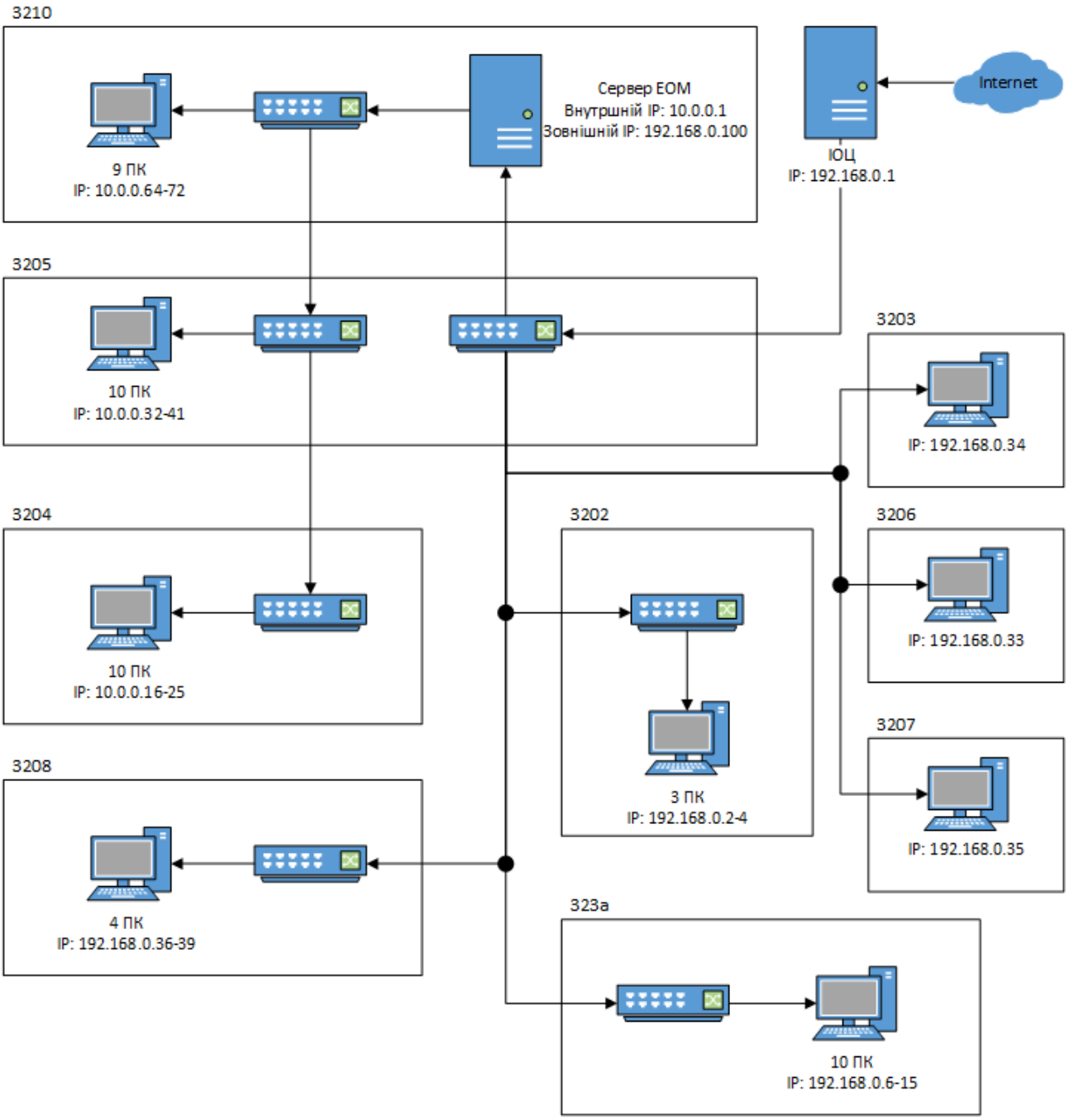


Рисунок 1.1 – Існуюча структура мережі кафедри ЕОМ

В цілому в мережі використовуються сорок вісім комп’ютерів, один сервер, сім комутаторів D-Link серії DES, кабелі UTP 5-ї категорії, а також конектори та розетки RJ-45.

Комп’ютери, що використовуються розділено на 3 групи:

1) комп’ютери для використання студентами;
2) комп’ютери для використання викладачами;
3) комп’ютер сервер.

Комп’ютери першої групи фізично розташовані в аудиторіях: 3210, 3205, 3204, 323а. В кожній навчальній аудиторії використовуються різні комп’ютери характеристики яких наведено у таблиці 1.1.

Таблиця 1.1 – Характеристики комп’ютерів в аудиторіях

| Аудиторія | Кількість ПК, шт. | Процесор | Обсяг оперативної пам’яті, Мб | Обсяг жорсткого диску, Гб | Операційна система |
|---|---|---|---|---|---|
| 3210 | 9 | Intel Core i3-7100, 3.9 ГГц | 8000 | 500 | Windows 10, Kali Linux |
| 3205 | 10 | Intel Pentium III | 4000 | 500 | Windows 7 |
| 3204 | 10 | Intel Core 2 Duo 4400 | 4000 | 500 | Windows 10 |
| 323а | 10 | Intel Celeron D | 2000 | 320 | Windows Xp |

Програмне забезпечення у всіх аудиторіях однотипне. Це зроблено для того, щоб кожну дисципліну можна було викладати у будь-якій аудиторій кафедри.

Комп’ютери другої групи розташовані в аудиторіях: 3202, 3203, 3206, 3207, 3208. В залежності від роду діяльності персоналу відповідні робочі станції мають доступ до додатковим інформаційним ресурсам, таким як, «Курсор» чи «Деканат».

Безпека кожного комп’ютера забезпечується локальною політикою безпеки, яка запобігає можливим небезпечним діям користувачів, примусовою зупинкою не

використовуваних служб, встановленням на кожний комп’ютер антивірусного програмного забезпечення.

Мережа побудована по стандарту 100BaseTX, який в якості середовища передачі використовує кабель UTP 5-ї категорії, що забезпечує пропуску здатність до 100 мбіт/с.

Доступ до мережі надається від головного сервера університету, який розміщено на інформаційно-обчислювальному центрі. Сервер кафедри ЕОМ розміщено в аудиторії 3210 і являє собою комп’ютер на базі двох ядерного процесора Intel Core 2 Duo E4400 з тактовою частотою 2 ГГц, чотирьома гігабайтами оперативної пам’яті та встановленою на ньому операційною системою Microsoft Windows Server 2003 R2. На сервері налаштовано маршрутизацію з зовнішньої мережі (мережі університету) у внутрішню (мережу кафедри). На даний час не всі комп’ютери підключені до внутрішньої мережі, що є недоліком існуючої архітектури.

Проведений аналіз, направлений на створення чіткого уявлення про працездатність, швидкодію, стабільність існуючої ЛОМ кафедри ЕОМ та її окремих вузлів, показав, що конфігурація мережі та сервера потребують модернізації, а саме:

- впровадження в мережу безпровідних точок доступу до Інтернету;
- для забезпечення стабільності, безпеки та швидкодії роботи операційної системи оптимальним варіантом є перехід на Windows 10, який стримується деякими наявними обмеженнями, а саме мінімальними вимогами до апаратного забезпечення, відсутність для ОС драйверів на застарілі периферійні пристрої;
- модернізація парку робочих станцій, тобто заміна комплектуючих для підвищення продуктивності ПК;
- вдосконалення архітектури мережі, переведення усіх ПК у внутрішню мережу кафедри;
- встановлення нового сервера з сучасним серверним програмним забезпечення дозволить коректно налаштувати внутрішню мережу.

## 1.2 Висновки за розділом

Локальна мережа кафедри постійно розвивається та модернізується з урахуванням появи нових мережевих та інформаційних технологій, а також потреб та можливостей кафедри.

Проведене дослідження мережі та її окремих вузлів, дозволило зробити висновки про її нинішній стан та розробити рекомендації щодо усунення наявних проблем мережі, а також шляхи її модернізації.

# 2 ОГЛЯД МОЖЛИВИХ НОВИХ ТЕХНОЛОГІЙ

## 2.1 Технологія Wi-Fi та механізми її захисту

Міцно влаштовані на робочих місцях, в наших будинках, освітніх установах, кафе, аеропортах та вуличних перехрестях, бездротові локальні мережі перетворилися на одну з найважливіших технологій доступу до Інтернету. Незважаючи на те, що у 1990-х роках велися розробки великої кількості технологій та стандартів для бездротових локальних мереж, переможцем цього змагання став лише один клас стандартів бездротових мереж: бездротова локальна мережа IEEE 802.11 WLAN, або просто Wi-Fi.

Існує кілька стандартів бездротових локальних мереж 802.11, у тому числі 802.11b, 802.11a та 802.11g. Крім того, сьогодні доступні пристрої, що працюють у подвійному (802.11a/g) і навіть потрійному (802.11a/b/g) режимах.

Між усіма трьома стандартами сімейства 802.11 є багато спільного. Так, наприклад, вони використовують однаковий протокол доступу до середовища передачі даних, CSMA/CA. Структури кадрів канального рівня всіх трьох стандартів також ідентичні. Всі три стандарти мають можливість зменшувати швидкість передачі з метою досягнення більш далеких відстаней.

Стандарт 802.11b має швидкість передачі даних 11 Мбіт/с і працює в діапазоні частот, що не ліцензується, 2400,0–2483,5 МГц, розділяючи його разом з телефонами, що працюють на частоті 2,4 ГГц, та мікрохвильовими печами. Швидкість передачі даних бездротової мережі 802.11a значно вища, як і робочий частотний діапазон. Працюючи у вищому частотному діапазоні, локальні мережі 802.11a мають меншу площу зони покриття та більше страждають від багатопроменевого ефекту поширення хвиль. Мережі типу 802.11g працюють у тому ж низькому діапазоні, що й мережі 802.11b, та мають з ними зворотну сумісність, тому багато користувачів оновлюють свої клієнтські пристрої 802.11b до стандарту 802.11g. Крім того, стандарт 802.11g надає вищу швидкість передачі даних, порівнянну зі швидкістю стандарту 802.11a.

Створений у 2009 році стандарт мереж Wi-Fi, 802.11n, передбачає використання антен множинного введення та множинного виведення (multipleinput & multiple-output – MIMO). Це означає, що з боку відправника та одержувача присутні по дві або більше антен, що передають або приймають сигнали. Залежно від використовуваного типу модуляції сигналу, стандарт 802.11n дозволяє досягти швидкості передачі даних до шести сотень мегабіт на секунду.

Технологія IEEE 802.11ac є розвитком технології стандарту 802.11n. Вона призначена замінити технологію 802.11n. Перехід із 2.4 ГГц на частоту 5,25 ГГц підвищує пропускну спроможність до 1,5 Гбіт/с. Ширина частотних 144 каналів розширено до 80-160 МГц (об'єднуються 2-4 канали). При перевищенні рівня перешкод на якомусь каналі передача перекладається на інші канали. Застосовуються нові методи модуляції та кодування сигналу.

Також використовується технологія Beamforming, що дозволяє змінювати діаграму спрямованості антен використовувати конкретні значення фази сигналу для певних пристроїв, враховуючи їхнє розташування. Формування діаграми спрямованості дозволяє збільшити дальність та швидкість передачі на відкритій території, а також долати перешкоди стін, що дозволяє передавати дані за межі приміщень.

Технологія IEEE 802.11ac має великі перспективи по застосуванню в корпоративному середовищі. Висока завадостійкість, швидкість та дальність передачі дозволяють впроваджувати її в приміщеннях великої площі, де потрібна підтримка багатьох клієнтів. Поширення технології призводить до переведення пристроїв з діапазону 2,4 ГГц до 5,25 ГГц. Мікросхеми для технології 802.11ac досить дорогі, тому не очікується масової заміни в портативні пристрої стандарту 802.11n на новий стандарт. Технологія забезпечує спільну роботу в змішаних мережах з колишніми стандартами в діапазоні 5,25 ГГц.

На відміну від дротових мереж, коли станції фізично з’єднані через кабель і наявна можливість контролю цих під’єднань, бездротова мережа є загальнодоступною. Контроль за під’єднанням станцій у цій мережі набагато

складніший. Перехоплення інформації, що циркулює по WLAN, можливе без використання складного обладнання [2].

Досить часто вразливості з'являються через некоректну конфігурацію станцій та точок доступу. Деякі функції, додані розробниками для полегшення роботи, призводять до появи недоліків та вразливостей захисту [2].

Можна виділити такі групи загроз:

- несанкціоноване під'єднання до приладів та мереж;
- перехоплення та розкриття трафіка (прослуховування, злам шифрування);
- модифікація трафіка(підробка повідомлень, ін'єкції в кадри);
- порушення доступності (завади, захоплення ресурсів мережі) [2].

В [3] описана вразливість бездротових клієнтів, згідно з якою зловмисник може від'єднати клієнтів від точки доступу, до якої вони під'єднані, і під'єднати до іншої точки доступу, менш безпечної.

Для протидії атакам на бездротові мережі, які засновані на вищеназваних загрозах, використовують стандарти безпеки, створені організацією Wi–Fi Alliance: WPA, WPA2, WPA3 [2]. Порівняння стандартів захисту мереж Wi–Fi наведено в таблиці 2.1.

Таблиця 2.1 - Порівняння стандартів захисту мереж Wi–Fi

| | WEP | WPA | WPA2 | WPA3 |
|---|---|---|---|---|
| Загальний опис | Перший протокол захисту мереж Wi–Fi | Посилення захисту без заміни обладнання. Нові протоколи автентифікації | Новий протокол шифрування | Посилення ключів. Заміна протоколу автентифікації PSK |
| На якому документі засновано | IEEE 802.11–1997 | Початкова версіяIEEE 802.11i | IEEE 802.11i–2004 | WPA3 Specification Version 1.0 |

Продовження таблиці 2.1

| | WEP | WPA | WPA2 | WPA3 |
|---|---|---|---|---|
| Автентифікація | Open system Shared key | Enterprise – 802.1X Personal – PSK | Enterprise – 802.1X Personal – PSK | Enterprise – 802.1X Personal –SAE |
| Шифрування | Шифр RC4 | TKIP (шифр RC4) | CCMP / GCMP(шифр AES) | CCMP / GCMP(шифр AES) |
| Ключ шифрування, біт | 64/128 | 128 | 128/256 | 128/256 |
| Захист цілісності (автентичності) даних | CRC–32 (32 біт) | Michael (64 біт) | CBC-MAC (64/128 біт)/GCM (128 біт) | CBC-MAC (64/128 біт)/GCM (128 біт) |
| Додатковий захист керуючих кадрів | – | Management Frame Protection (не обов’язково) | Management Frame Protection (не обов’язково) | Management Frame Protection |
| Управління ключами | – | 802.1X / 4-way handshake | 802.1X / 4-way handshake | 802.1X / SAE |
| Захист від атак повторення (reply) | – | Лічильник послідовності транзакцій (48 біт) | Номер пакета(48 біт) | Номер пакета(48 біт) |

Продовження таблиці 2.1

| | WEP | WPA | WPA2 | WPA3 |
|---|---|---|---|---|
| Можливі атаки | Відновлення ключа; атака фрагментації; Chop–Chop; DoS | Бека і Тьюза; Охігаші і Морі; KRACK; підбір пароля за словником; Hole196; DoS | KRACK; підбір пароля за словником; Hole196; DoS | Пониження до WPA2; пониження групи сторонніми каналами; DoS |
| Рівень безпеки | Не захищено | Слабкий/ Середній | Середній/ Високий | Високий |

Загальновідомо, що перший стандарт захисту WEP (IEEE 802.11) має багато вразливостей і не може бути рекомендований для застосування [2].

Стандарт WPA (WPA1) регламентує використання протоколу автентифікації IEEE 802.1X із сервером автентифікації й спрощеного режиму PSK. Протокол 802.1X, за використання ненадійних протоколів сімейства EAP (LEAP, EAP–FAST), уразливий до крадіжки пароля. Протокол PSK уразливий до декількох типів атаки на пароль та атаки перевстановлення ключа KRACK, яка дозволяє розшифровувати й підробляти пакети в мережі [2].

Стандарт WPA2 використовує протоколи автентифікації, аналогічні WPA, а також успадковує всі супутні вразливості. Стандарт регламентує використання блокових протоколів шифрування CCMP і GCMP. Кожний із протоколів забезпечує захист цілісності повідомлень і надійне шифрування. Багато дослідників указують на потенційні слабості протоколу GCMP. Використання атаки KRACK дозволяє реалізувати ці слабості, що веде до розкриття інформації, підроблення повідомлень [2].

Стандарт WPA3 регламентує використання механізму захисту кадрів керування, який раніше не був обов’язковим, що приводило до можливості маніпуляції зловмисником діями учасників мережі. Режим автентифікації PSK

може бути замінений на автентифікацію SAE. Протокол SAE дозволяє забезпечити високий рівень захищеності навіть заслабких паролів, а також запобігає вразливостям режиму PSK. Дослідники виявили ряд уразливостей цього протоколу (Dragonblood), однак усі ці вразливості не критичні [2].

### 2.2 Хмарні сховища даних

На сьогодні, кожна людина, яка активно використовує персональний комп'ютер так чи інакше стикалася з поняттям хмарних технологій. З'явившись близько 15 років тому, перші хмарні сховища суттєво змінили уявлення користувачів про збереження інформації. Хмарний сервіс для користувача представляє собою певний простір на віддаленому сервері, в якому він може працювати зі своїми файлами, завантажуючи та видаляючи їх, а також надаючи іншим користувачам у спільний доступ [4].

Хмарні сховища широко поширені серед користувачів, які працюють з інформацією, до якої часто потрібний доступ. Відмінність від інших способів зберігання інформації у тому, що користувач може працювати з інформацією з будь-якого пристрою (персональний комп'ютер, планшет та інші), що має доступ в інтернет [5].

Для користувача використання «хмари» є досить зручним, так як йому виділяється деякий обсяг пам'яті, представлений однією папкою. Користувач працює в «хмарі», при цьому він не знає, де саме зберігається його інформація. Для користувача "хмара" - це його папка. З вищевказаного випливає, що створення хмарних сховищ це найперспективніша технологія зберігання інформації [5].

Система зберігання даних у «хмарі» використовує розподілене зберігання даних на серверах. Звідси виникають загрози безпеці інформації, що зберігається, але, як правило, інформація користувачів не має особливої цінності, на відміну від корпоративної інформації [5].

Однак, зручність хмарних сервісів призводить до використання публічних хмарних сховищ користувачами у процесі роботи. Вони не замислюються про

забезпечення безпеки інформації. Такий стан справ, у кращому у разі викликає суперечки між різними службами компанії, а в гіршому – призводить до порушення системи безпеки. Крім загрози безпеці, використання працівниками публічних хмарних сервісів призводить до проблем, пов'язаних із законодавством. Простими заборонами виправити таку ситуацію досить складно. Компромісом може стати використання корпоративних хмарних сервісів як елемента інформаційної інфраструктури компанії [5].

Існує кілька способів організації хмарних сховищ.

Приватна хмара - інфраструктура, призначена для використання однією організацією, що включає кілька споживачів (наприклад, підрозділів однієї організації), можливо також клієнтами та підрядниками цієї організації. Приватна «хмара» може перебувати у власності, управлінні та експлуатації як самої організації, так і третьої сторони (або будь-якої їхньої комбінації), і вона може фізично існувати як усередині, так і поза юрисдикцією власника [6].

Публічна хмара — інфраструктура, призначена для вільного користування широкою публікою. Публічна «хмара» може перебувати у власності, управлінні та експлуатації комерційних, наукових та урядових організацій. Ця «хмара» є найбільш оптимальною у використанні з економічної точки зору[7].

Гібридна хмара - це комбінація з двох або більше різних хмарних інфраструктур, що залишаються унікальними об'єктами, але пов'язані між собою стандартизованими або приватними технологіями передачі даних та додатків [7].

Громадська хмара - вид інфраструктури, призначений для використання конкретним співтовариством споживачів з організацій, що мають спільні завдання. Громадська хмара може перебувати в кооперативній власності, управлінні та експлуатації однієї або більше організацій співтовариства або третьої, і вона може фізично існувати як усередині, так і поза юрисдикцією власника [7].

Доступ майже до всіх хмарних сховищ можна отримати через хмарний сервіс. Хмарні системи, що пропонуються ринком, є сервіс-орієнтованими: їх основне завдання — забезпечити користувача якісною послугою. Їх можна розділити на кілька основних видів залежно від послуг [7].

PaaS (платформа як послуга) — модель надання хмарних обчислень, при якій споживач отримує доступ до використання інформаційно-технологічних платформ: операційних систем, систем управління базами даних, що сполучає програмного забезпечення, засобів розробки та тестування, розміщених у хмарного провайдера. У цій моделі вся інформаційно-технологічна інфраструктура, включаючи обчислювальні мережі, сервери, системи зберігання, повністю керується провайдером. Провайдер також визначається набір доступних для споживачів видів платформ та його керованих параметрів. Споживачу може використовувати платформи на свій розсуд, створюючи їх віртуальні екземпляри, встановлюючи, розробляючи та тестуючи на них прикладне програмне забезпечення. При цьому існує можливість динамічної зміни кількості споживаних обчислювальних ресурсів [8].

Найчастіше, PaaS використовується програмістами, які спільно працюють над різними проектами. У цьому випадку всі або частина розробників отримують доступ до єдиного середовища розробки віддалено. Відповідно, всі вони потребують достатньої кількості системних ресурсів, а також інструментів спільної роботи.

SaaS (програмне забезпечення як послуга) - одна з форм хмарних обчислень, модель обслуговування, за якої передплатникам надається готове прикладне програмне забезпечення, що повністю обслуговується провайдером. Постачальник у цієї моделі самостійно керує додатком, надаючи замовникам доступ до функцій з клієнтських пристроїв, як правило через мобільний додаток або веб-браузер [9].

Основна перевага моделі SaaS для споживача послуги полягає у відсутності витрат, пов'язаних із встановленням, оновленням та підтримкою працездатності обладнання та працюючого на ньому програмного забезпечення. Прикладом SaaS може бути Microsoft Office 365. Корпорація Microsoft надає за моделлю SaaS доступ клієнтам до MS OfficeSuite (OfficeWebApps) поряд з SharePointServer, ExchangeServer та іншими сервісами та додатками.

IaaS (інфраструктура як послуга) надається як можливість використання хмарної інфраструктури для самостійного управління ресурсами обробки,

зберігання, мережами та іншими фундаментальними обчислювальними ресурсами, наприклад, споживач може встановлювати та запускати довільне програмне забезпечення, яке може включати в себе операційні системи, платформне та прикладне програмне забезпечення. Споживач може контролювати операційні системи, віртуальні системи зберігання даних та встановлені програми, а також мати обмежений контроль над набором доступних мережевих сервісів (наприклад, міжмережевим екраном, DNS). Контроль та управління основною фізичною та віртуальною інфраструктурою хмари, у тому числі мережі, серверів, типів використовуваних операційних систем, систем зберігання здійснюється хмарним провайдером [10].

Хмарних сховищ досить багато, і всі вони надають різноманітні можливості. Вони бувають: платними та безкоштовними, розраховані на великий обсяг інформації та на малий обсяг, підтримку різних операційних систем тощо. Єдине, у чому подібні між собою, - у способі обробки інформації.

Розглянемо деякі з найбільш популярних хмарних сховищ.

Dropbox – хмарне сховище даних, яке дозволяє користувачам зберігати свої дані на серверах у хмарі та розділяти їх з іншими користувачами в Інтернеті. Його робота побудована на синхронізації даних. Додаток Dropbox можна завантажити та інсталювати на ПК, Mac, Linux або мобільний пристрій. Одна з головних переваг Dropbox – легкість та інтуїтивність у використанні – потрібно просто закачати файли до папки Dropbox, опублікувати її, або синхронізувати з потрібним пристроєм. На відміну від основних конкурентів, під час роботи з Dropbox редаговані файли не копіюються повністю на сервер — здійснюється передача лише зміненої частини інформації, попередньо стиснутої. Безкоштовно надається 5 Гб пам’яті.

Google Drive — хмарне сховище даних, яке дозволяє користувачам зберігати свої дані на серверах у хмарі та ділитися ними з іншими користувачами в Інтернеті. Після активації замінює Google Docs. У сервісі можна зберігати не лише документи, а й фотографії, музику, відео та багато інших файлів. Безкоштовно надається 15 Гб пам’яті.

OneDrive — це файловий хостинг, що надається компанією Майкрософт як частина набору онлайн-послуг. Він дозволяє користувачам зберігати файли, а також інші особисті дані, такі як налаштування Windows або ключі відновлення BitLocker у хмарі. Файли можна синхронізувати з ПК та отримувати доступ до них з веб-браузера або мобільного пристрою, а також ділитися публічно або з певними людьми. OneDrive пропонує 5 Гб вільного місця для зберігання. Додатковий обсяг пам'яті можна додати окремо або через підписку на інші служби Microsoft, включаючи Office 365 [11].

Хмарні технології мають як свої переваги, так і недоліки. До основних переваг можна віднести:

- доступність – доступ до інформації, що зберігається на хмарі, може отримати кожен, хто має комп'ютер, планшет, будь-який мобільний пристрій, підключений до Інтернету;
- мобільність – користувач не має постійної прихильності до одного робочого місця. З будь-якої точки світу менеджери можуть отримувати звітність, а керівники стежити за виробництвом;
- економічність – однією з важливих переваг називають зменшену затратність. Користувачеві не треба купувати дорогі, великі за обчислювальною потужністю комп'ютери та програмне забезпечення, а також він звільняється від необхідності наймати спеціаліста з обслуговування локальних IT-технологій;
- гнучкість – усі необхідні ресурси надаються провайдером автоматично.
- висока технологічність – великі обчислювальні потужності, які надаються у розпорядження користувача, які можна використовувати для зберігання, аналізу та обробки даних;
- надійність – деякі експерти стверджують, що надійність, яку забезпечують сучасні хмарні обчислення, набагато вища, ніж надійність локальних ресурсів;
- безпека – хмарні сервіси мають досить високу безпеку [12].

Незважаючи на переваги, саму концепцію хмарних технологій чимало критикують, виділяючи такі недоліки:

- постійне з'єднання з мережею – для отримання доступу до послуг хмари потрібне постійне з'єднання з мережею Інтернет;
- програмне забезпечення – є обмеження щодо ПЗ, яке можна розгортати на хмарах та надавати його користувачеві;
- конфіденційність – в даний час немає технології, яка б гарантувала 100% конфіденційність даних, що зберігаються;
- надійність – втрата інформації в хмарі означає неможливість її відновлення;
- безпека – хмара сама по собі є досить надійною системою, проте при проникненні на нього зловмисник отримує доступ до величезного сховища даних;
- дороговизна – безкоштовно надається обмежена кількість пам’яті [12].

## 2.3 Висновки за розділом

Інновації у сфері комп'ютерних мереж продовжують впроваджуватись швидкими темпами. Просування мережевих технологій нині відбувається усіма фронтами, зокрема у розгортанні високопродуктивних маршрутизаторів і збільшенні швидкостей передачі, як у магістральних мережах, так і у мережах доступу.

Мережі Wi-Fi є перспективними для їх застосування при проектуванні локальних мереж. Проаналізовано стандарти механізмів захисту, які використовуються в мережах Wi–Fi на різних етапах роботи, їх вразливості та наявні методики атак.

# 3 ПРОПОЗИЦІЇ ЩОДО ВДОСКОНАЛЕННЯ АРХІТЕКТУРИ ЛОКАЛЬНОЇ МЕРЕЖІ КАФЕДРИ ЕОМ

## 3.1 Загальна структура

У зв'язку із виявленими у розділі 1 недоліками та запровадженням нових технологій необхідно переглянути структуру існуючої локальної мережі. Нова структура мережі представлена на рисунку 3.1.

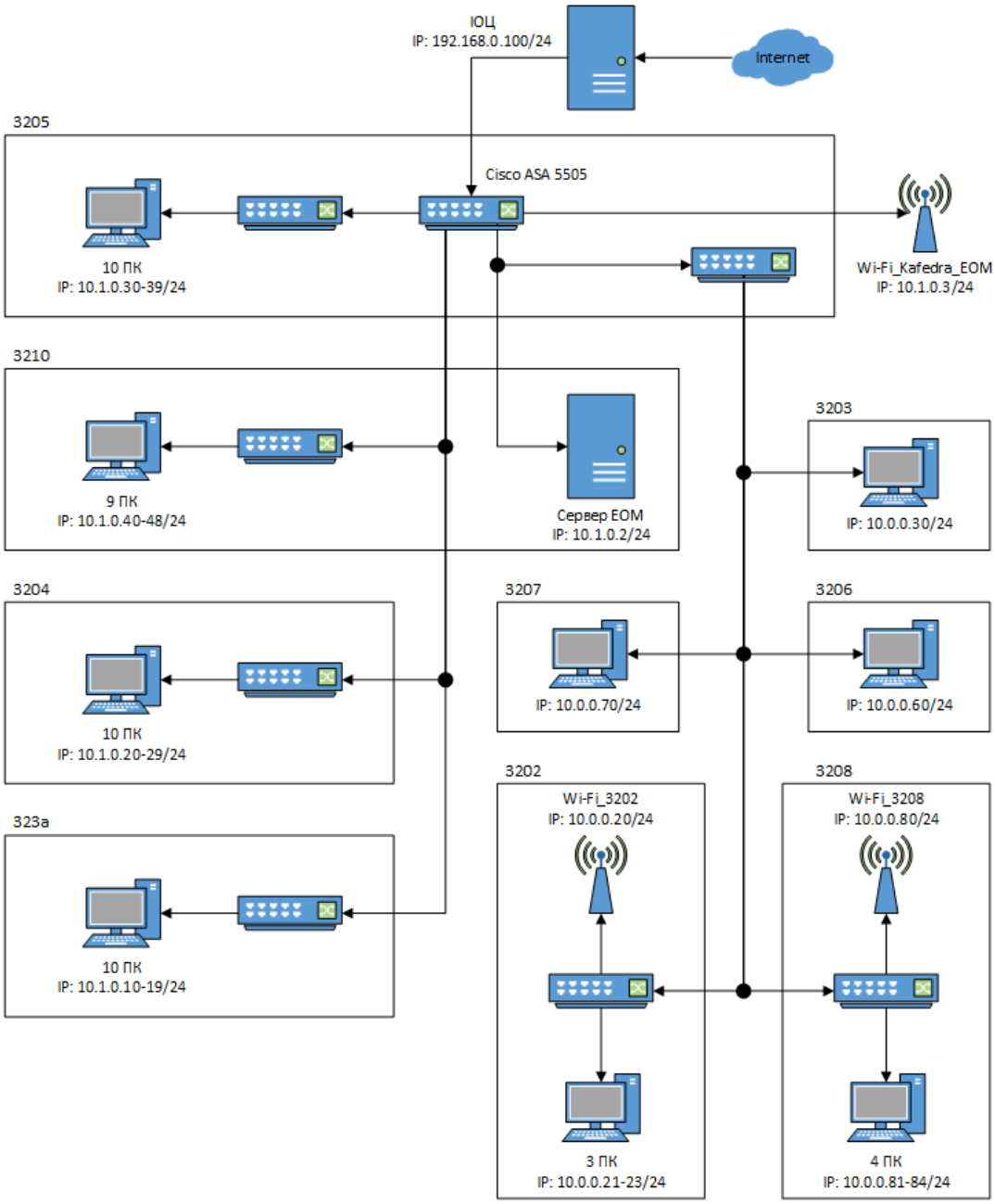


Рисунок 3.1 – Нова структура локальної мережі кафедри ЕОМ

В аудиторії 3205 встановлено міжмережевий екран Cisco ASA 5505, який є повнофункціональним комплексом захисту наступного покоління. Cisco ASA 5505 має високопродуктивний міжмережевий екран, SSL та IPsec VPN, а також велику кількість мережевих служб у модульному комплексі, що підтримує "plug-and-play". Використовуючи вбудований Cisco ASDM, міжмережевий екран Cisco ASA 5505 легко встановлюється та налаштовується. Cisco ASA 5505 має гнучкий комутатор на вісім портів, які можуть бути динамічно згруповані для створення трьох окремих віртуальних підмереж (VLAN), забезпечуючи вдосконалену мережну фрагментацію та безпеку.

Використання можливостей Cisco ASA 5505 дозволить об’єднати усі комп’ютери в одну мережу, при цьому розділити їх на дві віртуальні підмережі. Одна віртуальна підмережа для комп’ютерів, що використовуються студентами, інша для тих, що використовуються персоналом кафедри. Кожна віртуальна підмережа буде захищена та відокремлена одна від одної.

Для забезпечення бездротового підключення до мережі Internet встановлено три точки доступу. Дві встановлено в аудиторіях 3202 та 3208, а третю в коридорі кафедри.

Сервер, що знаходиться в аудиторії 3210 замінено на новий який побудований на базі материнської плати Supermicro MBD-X10SRI-F, в якості процесора використовує Intel Xeon E5-2600 v4 та має можливість підключати до дванадцяти жорстких дисків об’ємом до одного терабайта кожний.

### 3.2 Налаштування Cisco ASA 5505

Для налаштування VLAN на Cisco ASA 5505 визначено значення основних його параметрів та зведено їх до таблиці 3.1. Для вхідного підключення з інформаційно обчислювального центру на пристрої необхідно створити окрему віртуальну підмережу, тому загальна кількість VLAN становитиме три.

Таблиця 3.1 – Значення основних параметрів Cisco ASA 5505

| Параметр | Номер VLAN | Значення | Опис |
|---|---|---|---|
| nameif | 1 | PRIVAT | VLAN для використання персоналом |
| | 2 | outside | VLAN для підключення від ІОЦ |
| | 3 | PUBLIC | VLAN для користування студентами |
| ip address | 1 | 10.0.0.1/24 | IP адреса для VLAN 1 |
| | 2 | 192.168.0.100/24 | IP адреса від інтернет провайдера |
| | 3 | 10.1.0.1/24 | IP адреса для VLAN 3 |
| security-level | 1 | 100 | Рівень безпеки від 0 до 100 (від самого низького до самого високого) |
| | 2 | 0 | |
| | 3 | 50 | |
| interface Ethernet | 1 | 0/1, 0/2, 0/3 | Відповідність фізичного інтерфейсу (порту) до VLAN |
| | 2 | 0/0 | |
| | 3 | 0/4, 0/5, 0/6, 0/7 | |

Щоб провести налаштування Cisco ASA 5505 потрібно підключитися до нього через консольний кабель та ввести наступні команди:

1) Створюємо VLAN 1:
   - interface vlan 1
   - nameif PRIVAT
   - ip address 10.0.0.1 255.255.255.0
   - security-level 100
   - no shutdown
   - exit

2) Створюємо VLAN 2:
   - interface vlan 2
   - nameif outside
   - ip address 192.168.0.100 255.255.255.0
   - security-level 0

- no shutdown
- exit

3) Створюємо VLAN 3:

- interface vlan 3
- no forward interface vlan 1
- nameif PUBLIC
- ip address 10.1.0.1 255.255.255.0
- security-level 50
- no shutdown
- exit

4) Зв’язуємо кожний фізичний інтерфейс (порт) з відповідною VLAN:

- interface Ethernet0/0
- switchport access vlan 2
- no shutdown
- exit
- interface Ethernet0/1
- switchport access vlan 1
- no shutdown
- exit
- interface Ethernet0/2
- switchport access vlan 1
- no shutdown
- exit
- interface Ethernet0/3
- switchport access vlan 1
- no shutdown
- exit
- interface Ethernet0/4
- switchport access vlan 3
- no shutdown

- exit
- interface Ethernet0/5
- switchport access vlan 3
- no shutdown
- exit
- interface Ethernet0/6
- switchport access vlan 3
- no shutdown
- exit
- interface Ethernet0/7
- switchport access vlan 3
- no shutdown
- exit

5) Для маршрутизації пакетів до мережі Інтернет вказуємо шлюз за замовчуванням та інтерфейс, через який він доступний:

- route outside 0.0.0.0 0.0.0.0 192.168.0.1

6) Налаштування DNS:

- dns domain-lookup outside
- dns name-server 192.168.0.1

7) Для доступу з наявних VLAN до мережі Інтернет необхідно транслювати адреси з локальної мережі на публічну адресу:

- object network OBJ_NAT_PRIVAT
- subnet 10.0.0.0 255.255.255.0
- nat (PRIVAT,outside) dynamic interface
- exit
- object network OBJ_NAT_PUBLIC
- subnet 10.1.0.0 255.255.255.0
- nat (PUBLIC,outside) dynamic interface
- exit

8) Зберігаємо налаштування:

- write memory.

Після виконання налаштувань Cisco ASA 5505 готовий до використання у мережі.

### 3.3 Налаштування сервера

Серверна операційна система займається обслуговуванням запитів інших комп'ютерів, надає у спільне користування файли та принтери через мережу. Також керує програмами, що обслуговують користувачів мережі, - такими як сервери програм, системи управління базами даних (СУБД), служби каталогів, засоби управління мережами, Web-сервери, поштові сервери. Крім Windows Server на ринку серверних операційних систем також популярні різні версії Linux (Ubuntu, Debian, Gentoo).

Основні переваги серверів під керуванням Windows - відносна простота адміністрування, досить велика кількість інформації та ПЗ. Також можна виділити технологію RDP для доступу користувача до серверних програм та загальну універсальність системи. До недоліків Windows Server можна віднести одразу два параметри: вартість ліцензії та споживання ресурсів. Серед усіх серверних ОС Windows Server найбільш ресурсноємна і вимагає щонайменше одне ядро процесора і від півтора до трьох гігабайт оперативної пам'яті просто для роботи ядра та стандартних служб. Ця система не підходить для малопотужних конфігурацій, а також має ряд вразливостей, пов'язаних із RDP та політиками груп та користувачів.

Ubuntu - один з найбільш популярних дистрибутивів сімейства Linux. Сервери на базі Ubuntu використовують для розміщення веб-серверів на nginx або Apache (на противагу Microsoft IIS), для роботи з PostgreSQL та MySQL. На сервері з Ubuntu відмінно працюють служби маршрутизації та управління трафіком.

До переваг можна віднести менше споживання ресурсів, ніж у Windows Server, а також нативну для всіх unix-систем роботу з консоллю та пакетними менеджерами.

Основним недоліком Ubuntu можна вважати те що, для роботи з нею, особливо в повноцінній серверній конфігурації, тобто виключно через термінал, будуть потрібні певні навички. Крім того, Ubuntu більше орієнтована на персональне використання та не завжди підходить для вирішення корпоративних цілей.

Gentoo відрізняється від інших дистрибутивів Linux. Її особливістю є те що, користувачі самі вибирають встановлені функції. Саме тому Gentoo виступає як одна з кращих серверних операційних систем сімейства Linux.

Однією з головних переваг Gentoo є те що, кожна установка є унікальною, користувачі можуть самі скомпілювати ядро, що дає набагато більший контроль. Отже, такі аспекти, як споживання пам'яті, можуть контролюватися для сервера. Завдяки такій модульній конструкції та гнучкості системні адміністратори особливо цінують Gentoo.

Недоліком Gentoo вважається те що, компіляція пакетів займає більше часу ніж встановлення готових виконуваних файлів. Однак, як правило, користувачі миряться з повільною компіляцією в обмін на можливість задавати власні параметри установки.

В якості операційної системи на сервер встановлено Gentoo. Процес встановлення можна звести до послідовності з десяти кроків, кожний з яких призводить до певного стану, які зведено до таблиці 3.2.

Таблиця 3.2 – Послідовність встановлення Gentoo

| Номер кроку | Стан |
|---|---|
| 1 | Користувач знаходиться в робочому середовищі, готовому до встановлення Gentoo. |
| 2 | Підключення до Інтернету готове до встановлення Gentoo. |
| 3 | Жорсткі диски готові до встановлення Gentoo. |
| 4 | Підготовлено інсталяційне середовище, і користувач готовий переключитися у нове середовище. |
| 5 | Розгорнуті основні пакети, загальні для всіх систем Gentoo. |
| 6 | Встановлено ядро Linux. |

Продовження таблиці 3.2

| Номер кроку | Стан |
|---|---|
| 7 | Створено основну частину конфігураційних файлів системи. |
| 8 | Встановлено необхідні системні засоби. |
| 9 | Встановлено та настроєно вибраний початковий завантажувач. |
| 10 | Щойно встановлене оточення Gentoo готове до використання. |

Після встановлення ОС на сервер виконано встановлення деяких програмних засобів для більш зручного подальшого користування сервером:

- Cinnamon - це оточення робочого столу Linux, що пропонує гнучкість, швидкість і безліч можливостей.
- Htop - монітор процесів, написаний для Linux, створений замінити стандартну програму top. htop показує динамічний список системних процесів, список зазвичай сортується за використанням процесора. На відміну від top, htop показує всі наявні процеси в системі, а також час безперервної роботи, використання процесорів і пам'яті.
- PuTTY - вільно розповсюджуваний клієнт для протоколів SSH, Telnet, rlogin і чистого TCP.
- Cron - утиліта в операційних системах Unix і Linux, яка дозволяє користувачам виконувати команди або скрипти (групи команд) автоматично в заданий час.
- Iptables — утиліта командного рядка, стандартний інтерфейс керування роботою міжмережевного екрану (брандмауеру) Netfilter для ядер Linux.
- Rsyslog - це дуже швидкий сервіс, що розширюється, для управління логами з величезною кількістю можливостей. Серед його можливостей можна відзначити підтримку фільтрації контенту, а також передачі логів по мережах.

### 3.4 Налаштування Wi-Fi

В аудиторіях 3202 та 3208 встановлено Wi-Fi роутери компанії TP-Link. Налаштування Wi-Fi роутерів:

1) В браузері за адресом tplinklogin.net переходимо до сторінки входу до налаштувань роутера. Вводимо логін та пароль і потрапляємо на налаштувань.

2) В цілях безпеки змінюємо пароль від сторінки налаштувань. В меню переходимо до вкладки «Системные инструменты», а в ній обираємо пункт «Пароль» після чого з’явиться сторінка яку зображено на рисунку 3.2. Вводимо попередні та нові данні у відповідні поля після чого натискаємо кнопку «Сохранить».

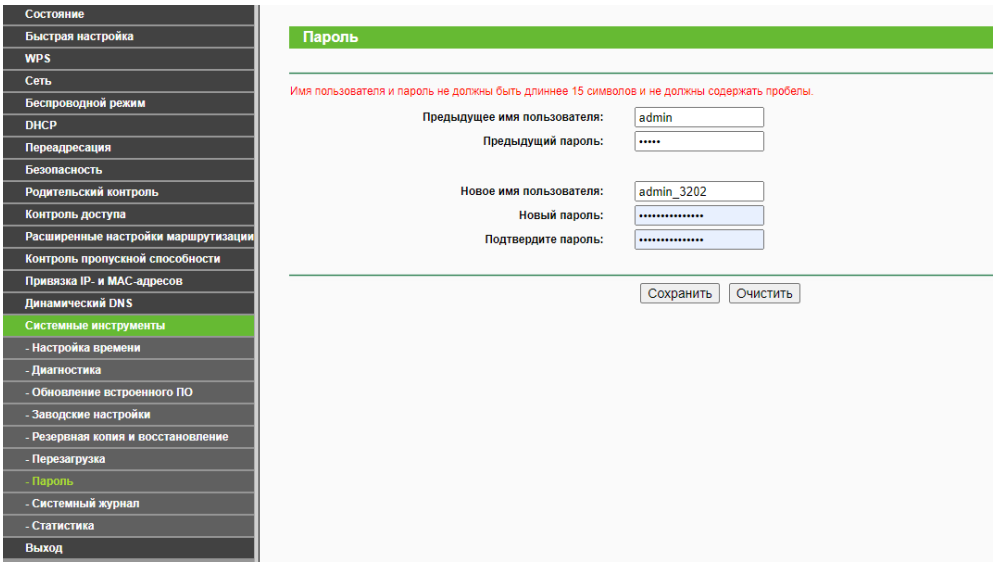


Рисунок 3.2 – Сторінка зміни даних для входу до налаштувань

3) Налаштовуємо доступ до мережі. Переходимо до вкладки «Сеть» та обираємо пункт «WAN» (рисунок 3.3). Для роутера в аудиторії 3202 ip адреса – 10.0.0.20, а в 3208 – 10.0.0.80.

4) Для налаштування бездротового режиму обираємо вкладку «Беспроводной режим» та переходимо до пункту «Настройки беспроводного режима» (рисунок 3.4). Вводимо ім’я мережі та знімаємо відмітку біля пункту «Включить широковещание SSID» після чого пристрої перестануть бачити Wi-Fi мережу. А щоб до неї підключитися, потрібно буде вказати не тільки пароль, а й ім'я мережі (SSID),що надає додаткового захисту мережі.

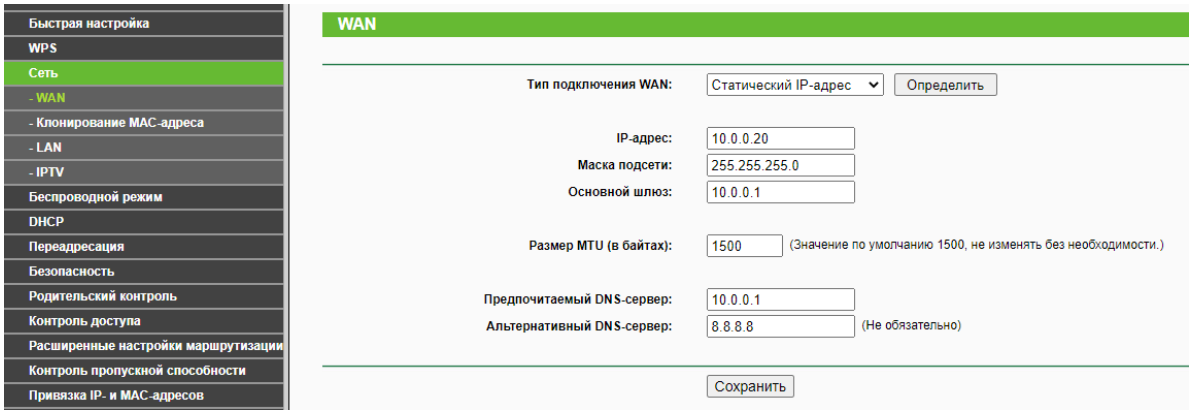


Рисунок 3.3 – Налаштування доступу до мережі

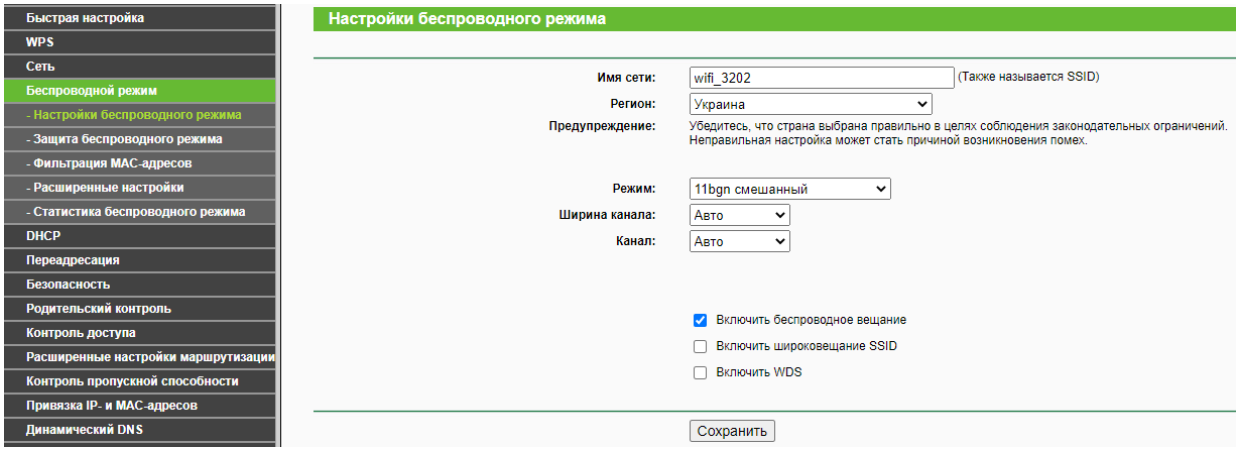


Рисунок 3.4 – Налаштування бездротового режиму

5) Переходимо до вкладки «Защита беспроводного режиму» (рисунок 3.5) та встановлюємо надійний пароль бездротової мережі.

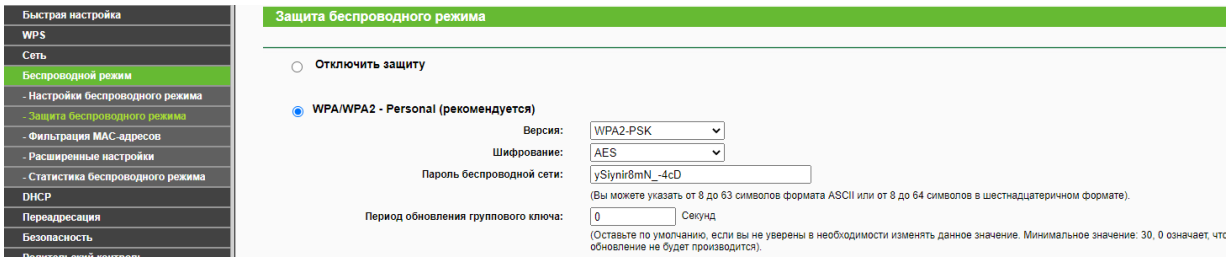


Рисунок 3.5 – Захист бездротової мережі

6) Відключення WPS. За допомогою WPS можна швидко та без введення пароля підключати пристрої до бездротової мережі. Тому для захисту роутера від злому цю функцію краще відключити. Переходимо на вкладку WPS та натискаємо кнопку «Отключить» (рисунок 3.6).

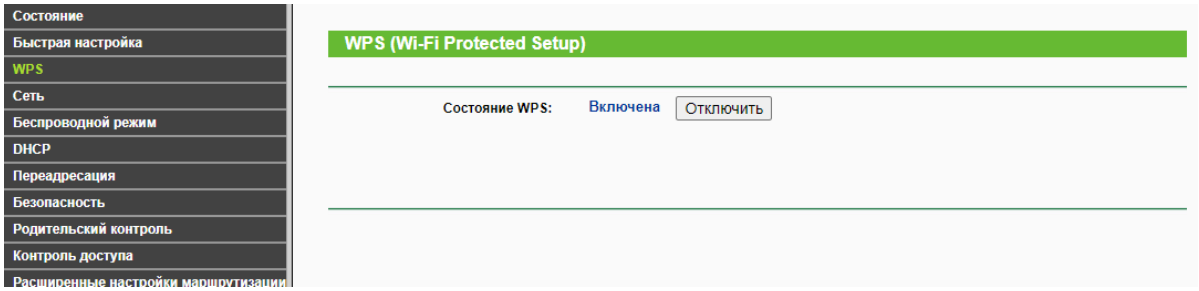


Рисунок 3.6 – Вимкнення функції WPS

В коридорі кафедри, для загального використання, встановлено бездротову точку доступу Ubiquiti UniFi AP. Ubiquiti UniFi є компактною бездротовою точкою доступу для використання всередині приміщення, яка дозволяє передавати зі швидкістю до 300 Мбіт/с по радіоканалу на відстань в 150м.

Перевагою UniFi є потужний програмний комплекс, який дає можливість здійснювати ефективне налаштування та керування пристроєм, у тому числі декількома пристроями одночасно, а також керувати мережами, трафіком та переглядати різноманітну статистичну інформацію у графічному вигляді.

Для налаштування точки доступу завантажуємо з офіційного сайту утиліту для налаштувань:

1) У вікні, що відкрилося обираємо країну та часовий пояс та нажимаємо «Next» (рисунок 3.7).


Рисунок 3.7 – Вікно налаштувань UniFi

2) Обираємо пристрій який будемо конфігурувати та натискаємо «Next» (рисунок 3.8).


Рисунок 3.8 – Вікно вибору пристрою

3) Вводимо назву та пароль бездротової мережі та натискаємо «Next» (рисунок 3.9).


Рисунок 3.9 – Вікно створення бездротової мережі

4) У наступному вікні вводимо данні для доступу до панелі адміністратора (рисунок 3.10).


Рисунок 3.10 – Налаштування доступу до панелі адміністратора

5) Натискаємо кнопку «Finish» на чому закінчуємо базове налаштування точки доступу.

6) Переходимо до панелі адміністратора, вводимо данні для входу та потрапляємо до конфігурування пристрою. Вибираємо мережу яку було створено та переходимо до її редагування. Вводимо ip адрес – 10.1.0.3/24 (рисунок 3.11).

Рисунок 3.11 – Налаштування бездротової мережі

Після виконання налаштувань на кафедрі працюють три бездротові мережі. Дві використовуються лише викладачами та персоналом кафедри. Інша, загальнодоступна мережа, яку можуть використовувати всі хто до неї підключиться.

### 3.5 Висновки за розділом

У цьому розділі надано пропозиції щодо вдосконалення структури локальної обчислювальної мережі кафедри. Проведено встановлення нового мережевого обладнання та описано його налаштування.

Реалізація наданих пропозицій дозволить підвищити ефективність використання локальної мережі, збільшити рівень її безпеки та зручність адміністрування.

# 4 ОРГАНІЗАЦІЯ ХМАРИ У ЛОКАЛЬНІЙ МЕРЕЖІ КАФЕДРИ ДЛЯ ВИКОРИСТАННЯ У НАВЧАЛЬНОМУ ПРОЦЕСІ

## 4.1 Аналіз хмарних сховищ даних

На ринку програмного забезпечення є багато рішень, які дозволяють організувати власне хмарне сховище даних. Серед всіх можна виділити два найбільш популярних та функціональних сервісів Nextcloud та Owncloud. Вони досить схожі між собою, але мають деякі функціональні відмінності. Порівняння сервісів зведено до таблиці 4.1.

Таблиця 4.1 – Порівняння характеристик Nextcloud та Owncloud

| Характеристика | Nextcloud | Owncloud |
|---|---|---|
| Функції файлового сховища | Завантаження, синхронізація, теги, коментування, різні версії, переміщення файлів у веб-інтерфейсі | |
| Файловий обмін | Можливість ділитися через e-mail, користувача, посилання, соцмережі. Термін дії та захист паролем. Редагування документа через e-mail, без створення облікового запису | Можливість ділитися через e-mail, користувача, посилання, соцмережі. Термін дії та захист паролем. Редагування без облікового запису недоступне. |
| Обмін папками | Можна ділитися через користувача, e-mail, посилання, соцмережі, встановлювати термін дії та захист, завантажувати та переглядати вміст | |
| Онлайн-інтеграція LibreOffice | Доступна | |
| Додаток Календар | Передбачено | |

Продовження таблиці 4.1

| Характеристика | Nextcloud | Owncloud |
|---|---|---|
| Додаток Контакти | Передбачено | |
| Переглядач PDF | Вбудований | Окрема програма |
| Контроль доступу | Передбачено | Тільки Enterprise Edition |
| Мобільні додатки | Безкоштовні клієнти для Android та iOS | Платні клієнти для Android та iOS |
| Чати (аудіо/відео) | Є додаток | Немає додатку |
| Лімітування швидкості | Передбачено | Не передбачено |
| Моніторинг ресурсів | Доступний | Недоступний |

Головною відмінністю даних сервісів є підхід до розповсюдження програмного забезпечення. Так Owncloud пропонує дві ліцензії, для користувача – безкоштовна, а для корпоративних – комерційна. Nextcloud розповсюджується під єдиною безкоштовною ліцензією. Ексклюзивні корпоративні функції для користувачів Owncloud доступні лише при покупці розширених пакетів. Nextcloud пропонує повний функціонал для спільнот та корпоративних клієнтів, а преміальна передплата включає лише технічну допомогу при розгортанні та консультативну підтримку.

### 4.2 Налаштування хмарного сховища

Для створення хмарного сховища у локальній мережі кафедри обрано платформу Nextcloud так як, вона є повноцінним, а саме головне безкоштовним

рішенням, яке може замінити загальновідомі продукти, такі як Dropbox, Google Drive і Microsoft 365.

Процес встановлення Nextcloud на сервер:

1) Завантажуємо останню версію програми:

- wget https://download.nextcloud.com/server/releases/nextcloud-23.0.0.tar.bz2

2) Завантажуємо файл з контрольною сумою:

- wget https://download.nextcloud.com/server/releases/nextcloud-23.0.0.tar.bz2.md5

3) Завантажуємо цифрові підписи:

- wget https://download.nextcloud.com/server/releases/nextcloud-23.0.0.tar.bz2.asc
- wget https://nextcloud.com/nextcloud.asc

4) Перевіряємо контрольну суму:

- md5sum -c nextcloud-23.0.0.tar.bz2.md5 < nextcloud-23.0.0.tar.bz2
- nextcloud-13.0.4.tar.bz2: OK

5) Розархівовуємо завантажений архів:

- tar -xjf nextcloud-13.0.4.tar.bz2

6) Копіюємо каталог на веб-сервер:

- cp -r nextcloud /var/www

7) Створюємо за допомогою текстового редактора конфігураційний файл та відкриваємо його:

- vi /etc/apache2/sites-available/nextcloud.conf

8) Вносимо наступні рядки:

Alias /nextcloud "/var/www/nextcloud/" <Directory /var/www/nextcloud/> Options +FollowSymlinks AllowOverride All <IfModule mod_dav.c> Dav off </IfModule> SetEnv HOME /var/www/nextcloud SetEnv HTTP_HOME /var/www/nextcloud </Directory>

9) Створюємо символьне посилання:

- ln -s /etc/apache2/sites-available/nextcloud.conf /etc/apache2/sites-enabled/nextcloud.conf

10) Для коректної роботи Nextcloud запускаємо такі модулі:

- a2enmod rewrite
- a2enmod headers
- a2enmod env
- a2enmod dir
- a2enmod mime
- a2enmod setenvif

11) Змінюємо права володіння:

- chown -R www-data:www-data /var/www/nextcloud/

12) Перезапускаємо веб-сервер:

- service apache2 restart

Для підключення в браузері вводимо ip-адресу сервера та потрапляємо на сторінку налаштування Nextcloud (рисунок 4.1). При першому підключенні до сховища створюємо обліковий запис адміністратора, вводимо ім'я адміністратора та пароль. Натискаємо «Finish setup» .

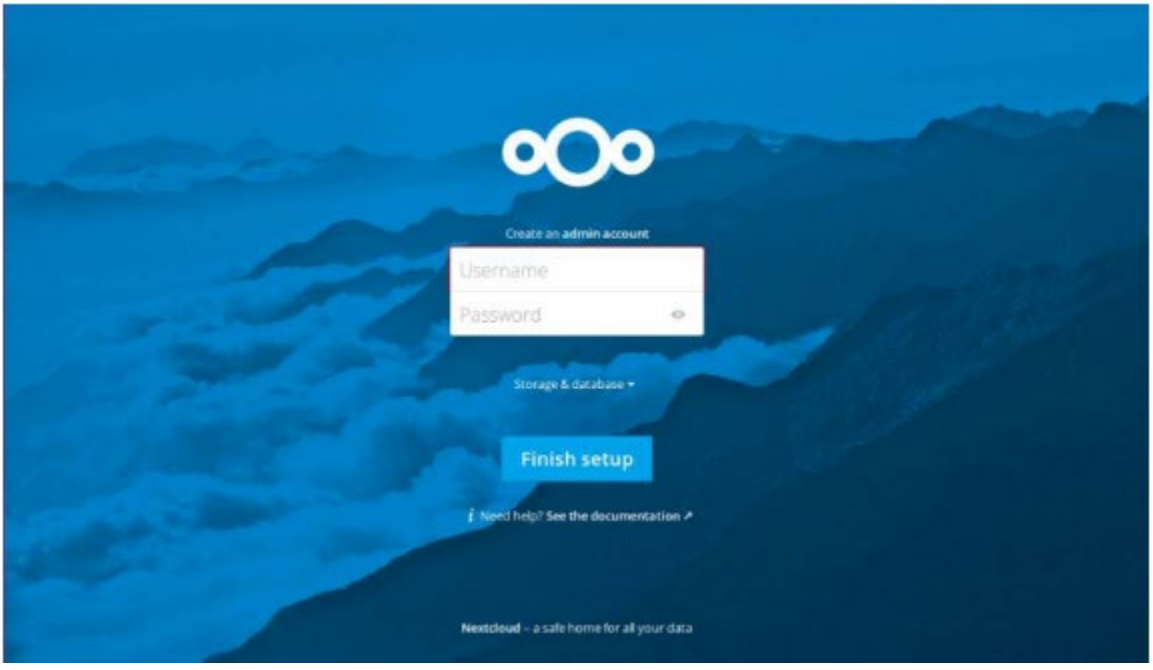


Рисунок 4.1 – Сторінка налаштування Nextcloud

Після завершення встановлення відкриється інтерфейс із файлами та каталогами, який вже можна використовувати для роботи (рисунок 4.2).

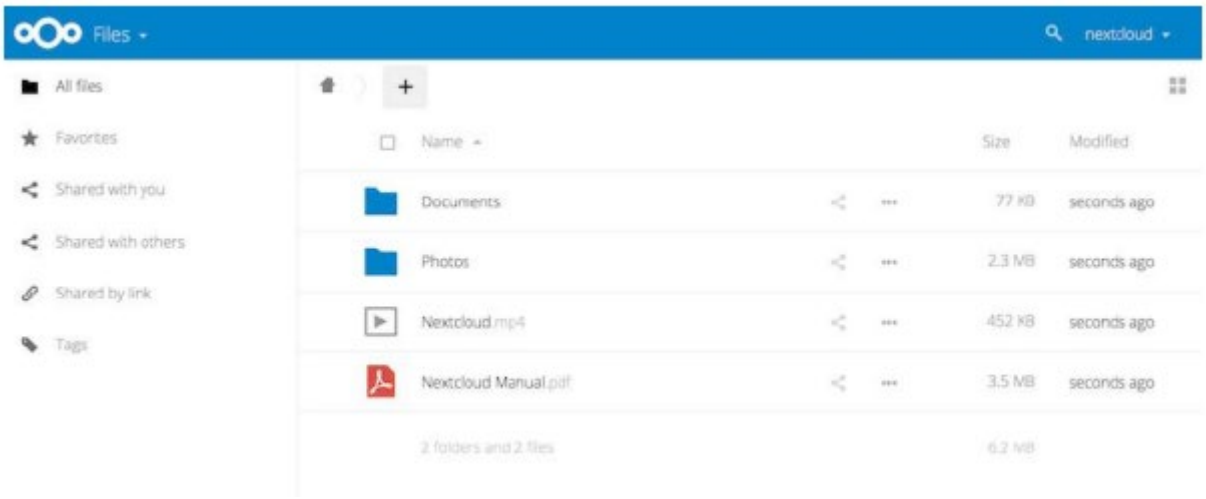


Рисунок 4.2 – Інтерфейс Nextcloud

Далі активуємо додатки, які будемо використовувати. Для цього переходимо «Files» вибираємо «Apps» після чого потрапляємо до менеджеру додатків. У правому меню вибираємо «Not enabled» (рисунок 4.3).

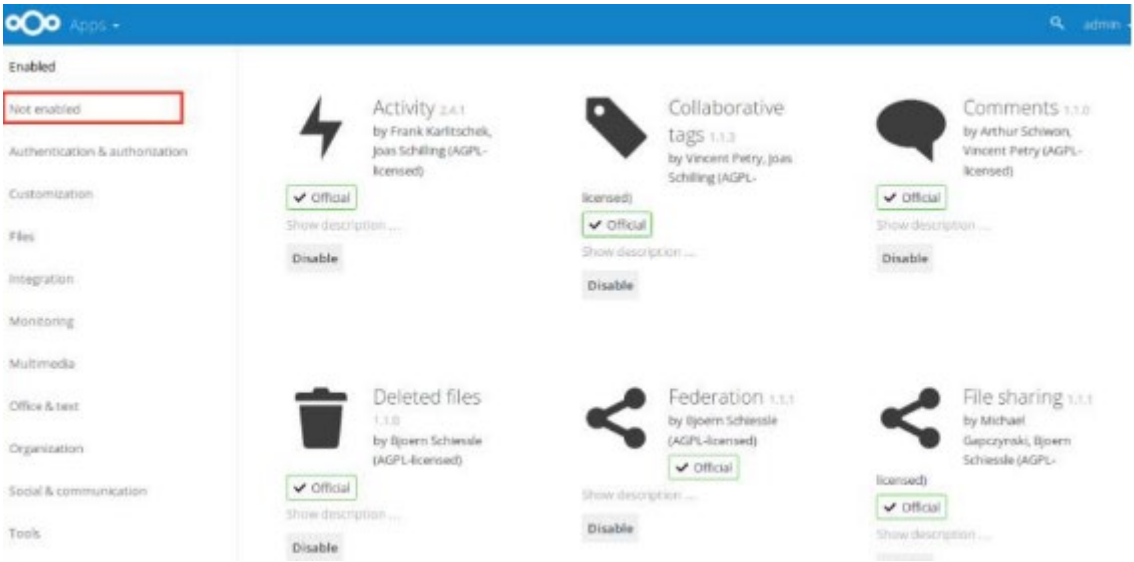


Рисунок 4.3 – Менеджер додатків

У менеджері додатків вибираємо додатки «LDAP user and group backend» та «Onlyoffice» і активуємо їх натискання кнопки « Enable». Далі переходимо до панелі адміністратора натиснувши «Admin» (рисунок 4.4).

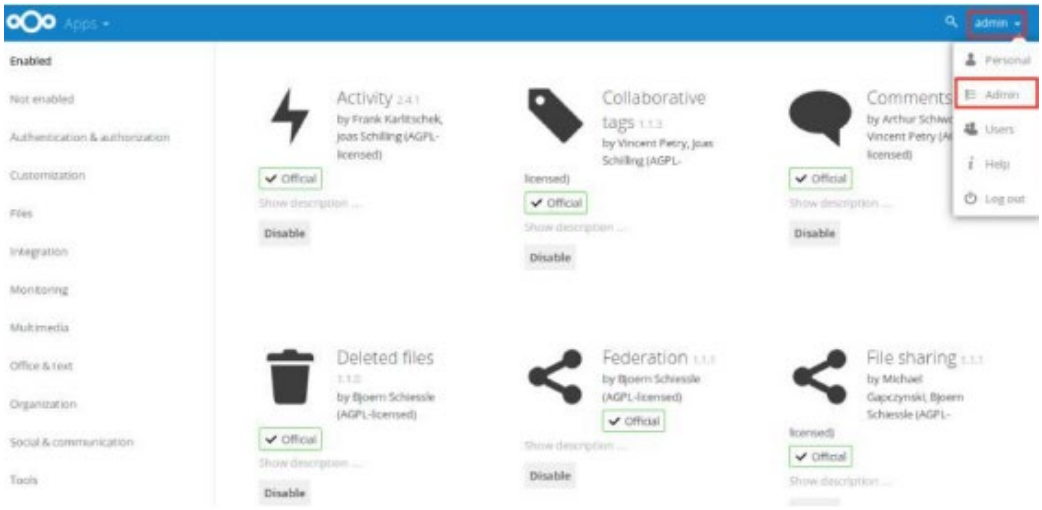


Рисунок 4.4 – Перехід до панелі адміністратора

В панелі адміністратора опускаємося до пункту Onlyoffice (рисунок 4.5).

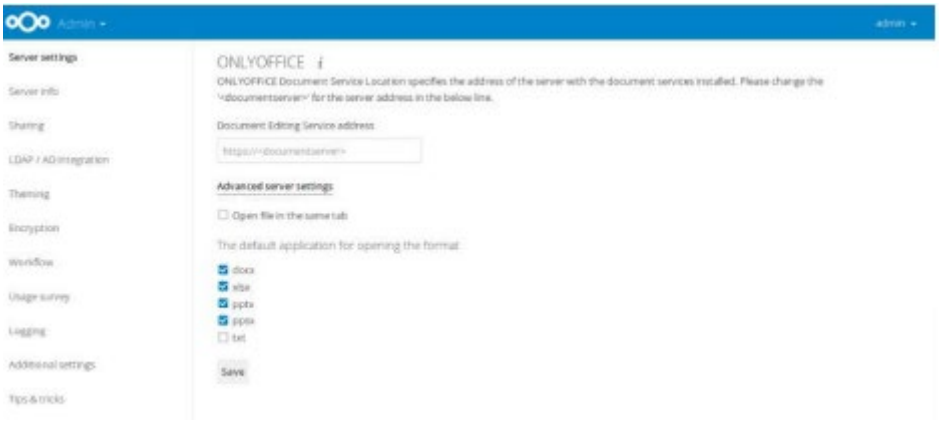


Рисунок 4.5 – Налаштування Onlyoffice

Функціональні можливості, які надає платформа Nextcloud при використанні її у навчальному процесі:

- створення папок та документів;
- завантажування файлів;
- видалення файлів та папок;
- перегляд файлів;
- редагування документів;
- розмежування прав доступу;
- створення посилань на матеріали.

Створення папок. Папку можна створити натиснувши на іконку «+» (рисунок 4.6).

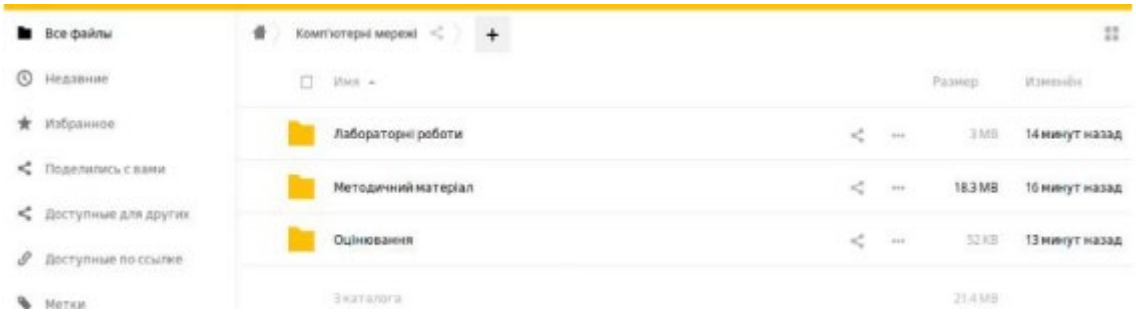


Рисунок 4.6 – Створення папки

Завантаження файлів. Файли можна завантажувати через кнопку «+» або перетаскуванням у область веб-сторінки. При однократному натисканні на файл зліва з’являється вікно з мініатюрою вмісту файлу та інформація про нього (рисунок 4.7).

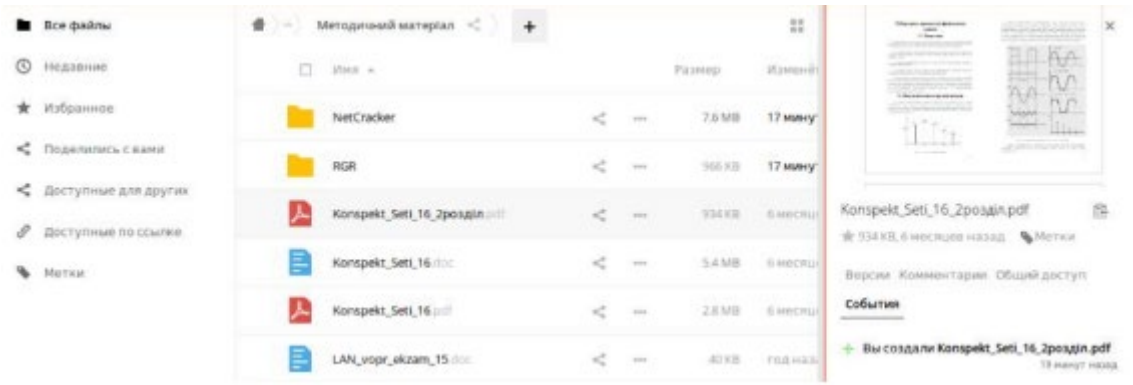


Рисунок 4.7 – Вікно з інформацією про файл

Відкриття PDF документів (рисунок 4.8). Файли pdf відкриваються у стандартному перегляді.

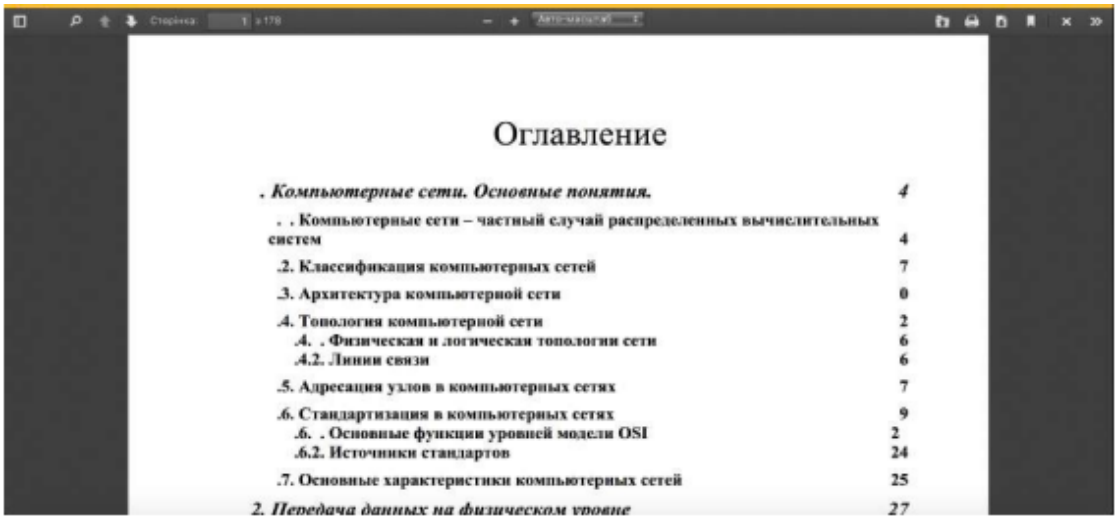


Рисунок 4.8 – Вікно перегляду PDF файлу

Створення документів. Новий документ створюється натисканням кнопки «+» та введенням назви створюваного документа. Наприклад, після створення презентацій з’явиться вікно яке показано на рисунку 4.9.

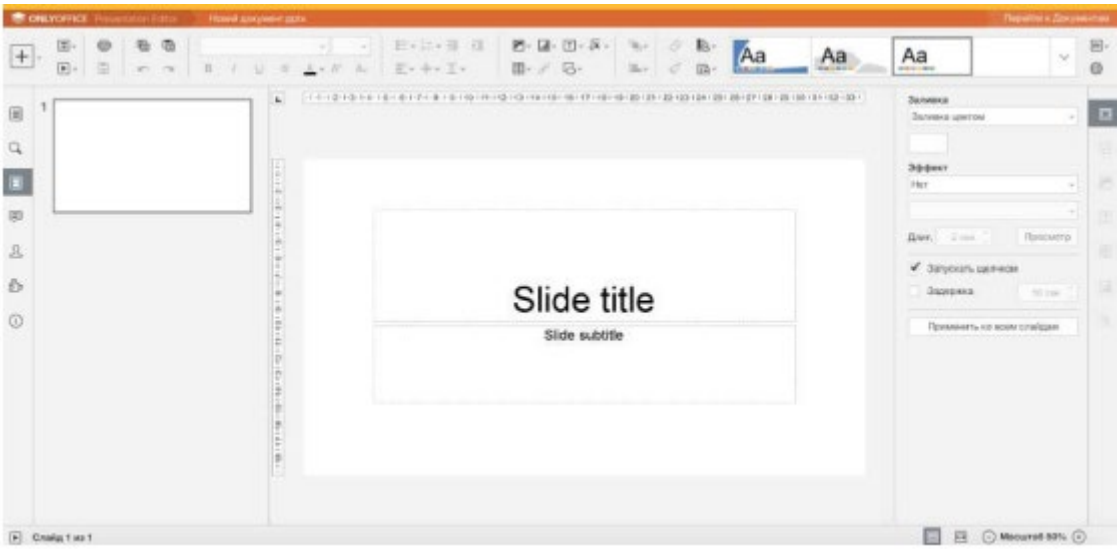


Рисунок 4.9 – Вікно створення презентації

Розмежування прав доступу до файлів (рисунок 4.10). У вікні інформації про файл за допомогою пункту «Общий доступ» можливо налаштовувати права доступу до файлу користувачам або групам користувачів.

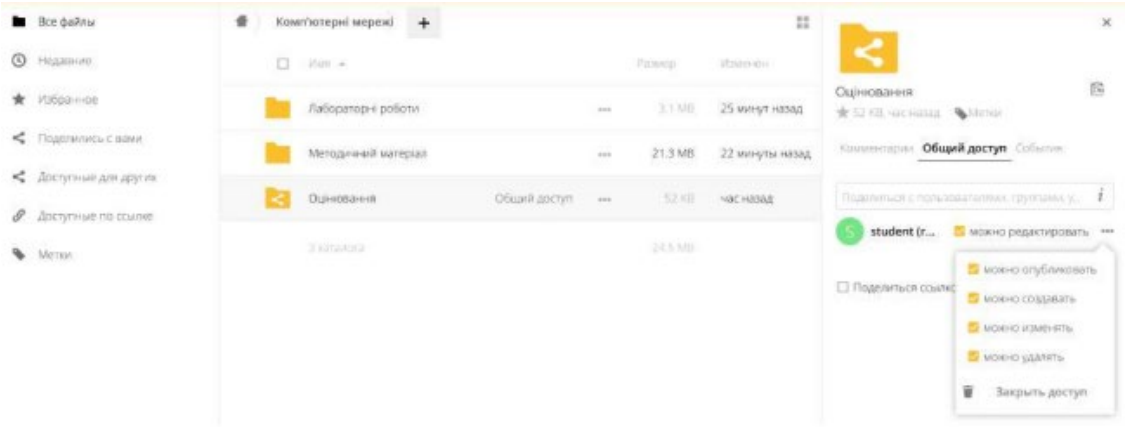


Рисунок 4.10 – Можливі права доступу

Створення посилань на матеріали (рисунок 4.11). Посилання файл створюється у пункті «Общий доступ» вікна інформації про файл або папки. Також є можливість захисти посилання паролем або встановити дату, до якого воно буде дійсним.

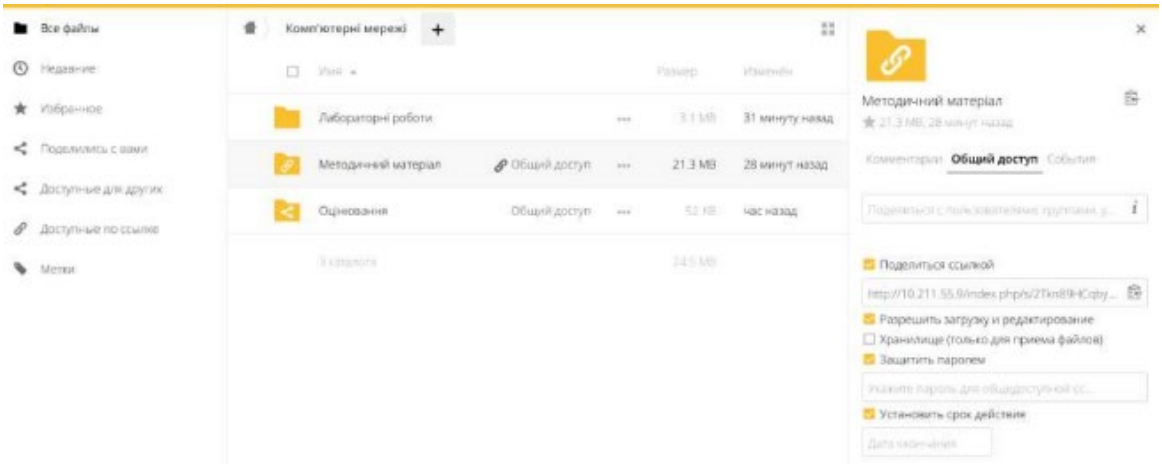


Рисунок 4.11 – Вікно налаштування посилання

## 4.3 Висновки за розділом

В даному розділі надано обґрунтування та вибір платформи для організації хмарного сховища у локальній мережі кафедри.

Наведено покроковий процес встановлення та налаштування платформи Nextcloud. Результатом встановлення отримано робоче хмарне сховище даних, яке можна використовувати у навчальному процесі.

Надано опис функціоналу та можливостей платформи Nextcloud.

# 5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

## 5.1 Вимоги безпеки при виконанні робіт на робочому місці

Охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

Працівник - особа, яка працює на підприємстві, в організації, установі та виконує обов'язки або функції згідно з трудовим договором (контрактом).[13]

Перед початком роботи працівник повинен:

- оглянути і привести в порядок робоче місце;

- відрегулювати освітленість на робочому місці, переконатись у її достатності, відсутності відблисків на екрані, відсутності зустрічного світла;

- перевірити правильність включення обладнання в електромережу;

- переконатись у наявності захисного заземлення (занулення) і підключення екранного проводу до корпусу процесора;

- протерти спеціальною салфеткою поверхню екрана і захисного фільтра;

- переконатись у відсутності дискет у дисководах процесора;

- перевірити правильність встановлення стола, стільця, підставки для ніг, пюпітра, положення обладнання, кута нахилу екрану, положення клавіатури і, за необхідності, провести регулювання положення робочого стола, стільця, розташування елементів ПЕОМ;

- перевірити дотримання вимог гігієнічних норм розміщення обладнання (при однорядному розташуванні відстань до стінок повинна бути не менше 1 м.; при розташуванні робочих місць одне за одним відстань між ними – не менше 1,5 м.; норма площі приміщення - 6 квадратних метрів на одне робоче місце).

При включенні ПЕОМ необхідно дотримуватись наступної послідовності дій:

- включити блок живлення;

- включити периферійні пристрої (принтер, монітор, сканер тощо);

- включити системний блок (процесор).

Усі кабелі, що з'єднують системний блок (процесор) з іншими пристроями, слід вмикати тільки при вимкненому комп'ютері. Відрегулювати яскравість свічення екрана відеотерміналу (далі - ВДТ), мінімальний розмір світної точки, фокусування, контрастність. Не слід робити зображення занадто яскравим, щоб не втомлювати очей.

У разі виявлення несправності обладнання, пристрою, засобів захисту тощо повідомити про це керівника робіт.

Працівник під час роботи зобов'язаний:

- виконувати тільки ту роботу, яка була йому доручена, і щодо якої він був проінструктований;

- на протязі всього робочого дня підтримувати порядок і чистоту на робочому місці;

- тримати відкритими всі вентиляційні отвори обладнання;

- зовнішній пристрій "миша" застосовувати тільки за наявності спеціального килимка;

- за необхідності припинення роботи на деякий час коректно закрити всі активні завдання;

- вимикати живлення тільки в тому випадку, коли працівник під час перерви в роботі на ПЕОМ змушений перебувати у безпосередній близькості від відеотерміналу (менше 2 м); якщо це не так, дозволяється живлення не вимикати;

- додержуватись відстані від очей до екрану в межах 60 - 80 см;

- дотримуватись вимог санітарних норм режиму праці та відпочинку, регламентованих перерв у роботі, виконувати під час цих перерв рекомендовані вправи для очей, шиї, рук, тулуба, ніг.

Регламентовані перерви у роботі: для розробників програм тривалістю 15 хвилин через кожну годину роботи за ВДТ.

Є неприпустимими такі дії при роботі на ПЕОМ:

- виконання ремонту та налагодження ПЕОМ безпосередньо на робочому місці;

- відключення захисних пристроїв, самочинні зміни у конструкції та складі ПЕОМ;

- одночасне доторкання до екрану монітора і клавіатури;

- доторкання до задньої панелі процесора при включеному живленні;

- перемикання кабелів периферійних пристроїв при включеному живленні;

- вимикання живлення під час виконання активного завдання;

- часті перемикання живлення, допущення попадання вологи на поверхню процесора, монітора, клавіатури, дисководів, принтерів та інших пристроїв;

- включення в мережу обладнання щойно принесеного знадвору в холодну пору року.

## 5.2 Шкідливі виробничі фактори на робочому місці

При роботі на ПЕОМ необхідно враховувати, що при не виконанні вимог охорони праці, обумовлених Вимогами щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями, затвердженими наказом Міністерства соціальної політики України від 14.02.2018 №207, на працівників можуть діяти такі небезпечні і шкідливі виробничі фактори:

фізичні:

- електромагнітне випромінювання, при наближенні до екрану чи задньої частини ВДТ ближче 0,6 - 0,7 м.;

- м'яке рентгенівське випромінювання, при наближенні до ВДТ ближче 0,05 м.;

- ультрафіолетове і інфрачервоне випромінювання;

- електростатичне поле між екраном і працівником;

- можлива наявність шуму та вібрації при роботі принтерів застарілої модифікації;

- нерівномірність розподілу яскравості у полі зору;

- підвищена яскравість світлового зображення;

- висока напруга у електричній мережі, замикання якої може відбутись крізь тіло людини при порушенні вимог електробезпеки,

хімічні:

- можлива наявність озону, оксидів азоту й аероіонізації; психофізіологічні:

- напруження зору;

- напруження уваги;

- інтелектуальні навантаження;

- емоційні навантаження;

- тривалі статичні навантаження;

- монотонність праці;

- необхідність обробки великого обсягу інформації у одиницю часу;

- нераціональна організація робочого місця.

До роботи оператора, програміста, інженера і техніка, користувача ПЕОМ допускаються:

- особи, не молодші 18 років, які не мають медичних протипоказань і пройшли обов'язкові медичні огляди - попередній під час оформлення на роботу та періодичні на протязі трудової діяльності - в порядку, передбаченому "Положенням про медичний огляд працівників певних категорій", затвердженим наказом Міністерства охорони здоров'я України від 31.03.94 №45, зареєстрованим в Міністерстві юстиції України 21.06.94 за №136/345;

- особи, що пройшли в установленому порядку інструктаж з охорони праці та пожежної безпеки;

Мікроклімат. Мікроклімат приміщень — комплекс фізичних факторів, що здійснюють вплив на теплообмін людини з оточуючим середовищем, обумовлюють самопочуття, працездатність, стан здоров'я і якість праці співробітників.

Санітарні норми ДСН 3.3.3-042-99 «Державні санітрані норми мікроклімату виробничих приміщень» [14] встановлюють гігієнічні вимоги до параметрів мікроклімату робочих місць з урахуванням інтенсивності енергозатрат

працюючих, часу виконання робіт, природних умов і вміщують вимоги до методів вимірів і контролю мікрокліматичних умов.

До параметрів мікроклімату належать:

- температура повітря і його відносна вологість;

- швидкість руху повітря;

- інтенсивність теплового випромінювання приладів та устаткування, що знаходяться у приміщенні.

Оптимальні мікрокліматичні умови характеризуються такими параметрами, які при їх спільній дії на людину протягом робочого дня забезпечують оптимальний функціональний стан людини. У таких умовах напруга терморегуляції мінімальна, дискомфортні тепловідчуття відсутні, що дозволяє зберегти здоров'я працюючих і забезпечити якість праці.

Порушення параметрів мікроклімату на робочих місцях сприяє створенню шкідливих і небезпечних мікрокліматичних умов, які при спільній дії на людину викликають значні зміни теплового стану, що може призвести до порушення стану здоров'я працівників.

Вимоги до освітлення. Приміщення, обладнані ПК з ВДТ повинні мати природне і штучне освітлення. Оскільки при недостатньому освітленні різко знижується продуктивність праці користувачів ПК, спостерігається швидка їх стомлюваність, а також можливе виникнення короткозорості.

Вимоги до природного та штучного освітлення приміщень, обладнаних ПК з ВДТ, визначаються згідно ДБН В.2.5-28-2018«Природне і штучне освітлення» [15].

Природне освітлення має здійснюватися через світлові прорізи, орієнтовані переважно на північ або північний схід і забезпечувати коефіцієнт природної освітленості (КПО) не нижче 1,5%.

Для захисту від прямих сонячних променів, які створюють прямі та відбиті відблиски на поверхнях дисплеїв і клавіатури, повинні бути передбачені сонцезахисні пристрої на вікнах (жалюзі або штори).

Задовільне природне освітлення легше забезпечити в невеликих приміщеннях на 5-8 робочих місць.

Штучне освітлення в приміщеннях з ПК повинно здійснюватися системою загального рівномірного освітлення.

У виробничих та адміністративно-громадських приміщеннях, у разі переважної роботи з документами, допускається застосування системи комбінованого освітлення. Тобто крім системи загального освітлення додатково встановлюються світильники місцевого освітлення.

Значення освітленості на поверхнях робочих столів, в зоні розміщення документів, має становити 300-500 лк.

Вимоги, що забезпечують захист від шуму і вібрації. Джерелами шуму при роботі з ПК є:

- жорсткий диск;
- вентилятор блока живлення ПК;
- вентилятор, розташований на процесорі (кулер);
- швидкісні CD-ROM та DVD-ROM;
- механічні сканери;
- пересувні механічні частини принтера.

При роботі матричних голчастих принтерів шум виникає при переміщенні головки принтера і в процесі удару голок головки по паперу. При роботі вентиляційної системи ПК, яка забезпечує оптимальний температурний режим електронних блоків, створюється аеродинамічний шум. Крім того, діють й інші зовнішні джерела шуму, не пов’язані з роботою ПК.

Шум, що створюється працюючими ПК, є широкосмужним, постійним з аперіодичним посиленням при роботі принтерів. Тому шум повинен оцінюватися загальним рівнем звукового тиску по частотному коригуванню «А» та вимірюватися в дБА.

Рівні звукового тиску в октавних смугах частот, рівні звуку та еквівалентні рівні звуку на робочих місцях, обладнаних ПК, мають відповідати вимогам ДСанПіН 3.3.2.007-98 «Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» [16] та ДСН 3.3.6-037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку»[17].

Зниження рівня шуму в приміщеннях, обладнаних ПК,

здійснюють наступними способами:

- використанням блоків живлення ПК з вентиляторами на гумових підвісках;

- використанням ПК, в яких термодавачі вмонтовані в блоці живлення та в критичних точках материнської плати (процесор, мікросхеми чипсету), які дозволяють програмним шляхом регулювати як моменти ввімкнення вентиляторів, так і їх швидкість обертання;

- переведення жорсткого диска в режим сплячки (Standby), якщо комп'ютер не працює протягом визначеного часу;

- використовуються ПК з малошумною системою охолодження процесорів (BOX-процесор з малошумним кулером);

- застосуванням материнських плат (наприклад, формату ATX та ATX – корпусів), що дозволяють регулювати автономну швидкість та моменти часу відмикання вентилятора блока живлення від електромережі;

Оцінка вібраційної безпеки проводитися в процесі трудової діяльності безпосередньо на робочих місцях обладнаних ПК.

Середні квадратичні значення віброшвидкості (V) і віброприскорення (а) або їх логарифмічні рівні в дБ для приміщень обладнаних ПК і на робочих місцях, при дії постійної локальної та загальної вібрації, нормуються в певних діапазонах октавних смуг згідно вимог ДСанПіН 3.3.2.007-98 «Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електроннообчислювальних машин» [16], ДСН 3.3.6-039-99 «Державні санітарні норми виробничої загальної та локальної вібрації» [18].

Розрахунок освітленості робочого місця. Для штучного освітлення у приміщенні використовуються люмінесцентні лампи.

Розрахунок штучного освітлення проведемо для кімнати площею 20 м2, ширина якої складає 5м, довжина – 4м, висота – 3м.

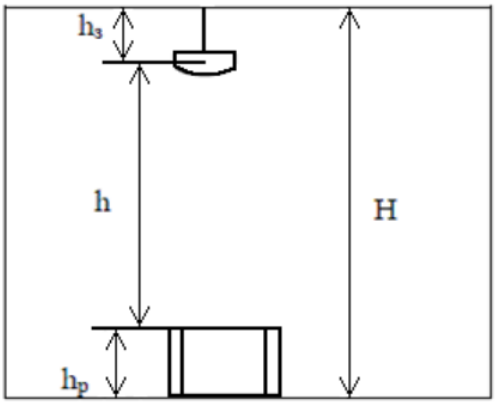


Рисунок 5.1 – Схема розміщення світильників над робочою поверхнею (Н – висота приміщення - 3м; hз – висота звисання світильника від стелі – 0.2м; h – висота підвісу світильника над робочою поверхнею - 2м; hр – висота робочої поверхні – 0.8м.)

Скористаємося методом використання світлового потоку. Для визначення потрібної кількості світильників, які повинні забезпечити нормований рівень освітленості, визначимо світловий потік, що падає на робочу поверхню за формулою:

$$F = \frac{E*K*S*Z}{n}$$, де

F – світловий потік, що розраховується, Лм;

E – нормована мінімальна освітленість, Лк; E = 300 Лк;

S – площа освітлюваного приміщення (у нашому випадку S=20м2 );

Z – відношення середньої освітленості до мінімальної (зазвичай приймається рівним 1,1... 1,2, в нашому випадку Z =1,1);

K – коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників в процесі експлуатації (його значення залежить від типу приміщення і характеру робіт, що проводяться в ньому, в нашому випадку К = 1,5);

n – коефіцієнт використання світлового потоку, (виражається відношенням світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп, і обчислюється в долях одиниці; залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами

відбиття від стін (ρст.) і стелі (ρстелі)), значення коефіцієнтів дорівнюють ρст = 40% і ρстелі=60%.

Обчислимо індекс приміщення за формулою:

$$I = \frac{S}{h(A+B)}, \text{ де}$$

S – площа приміщення, S = 20м2;

h – розрахункова висота підвісу, h = 2,9 м;

A – ширина приміщення, A = 4 м;

B – довжина приміщення, B = 5 м.

Підставивши значення отримаємо:

$$I = \frac{20}{2.9 * (4 + 5)} = 0.77$$

Знаючи індекс приміщення I, за таблицею знаходимо n =0,22.

Підставимо всі значення у формулу для визначення світлового потоку F :

$$F = \frac{300 + 1{,}5 * 20 * 1{,}1}{0{,}22} = 45000 \text{ Лм}$$

Для освітлення використані люмінесцентні лампи типу ЛБ 40-1, світловий потік яких F = 4320 Лм. Розрахуємо необхідну кількість ламп у світильниках за формулою:

$$N = \frac{F}{F_л}, \text{ де}$$

N – кількість ламп, що визначається;

F - світловий потік, F = 45000 Лм;

Fл- світловий потік лампи, Fл = 4320 Лм

$$N = \frac{45000}{4320} = 11$$

В приміщенні використовуються світильники типу ОД. Кожен світильник комплектується двома лампами. Тобто необхідно використовувати 6 світильників із 12 працюючими лампами в них.

## 5.3 Дій працівників в аварійних ситуаціях

Дії працівників у випадку електротравми. При ураженні електричним струмом необхідно якомога швидше звільнити потерпілого від струмопровідних частин обладнання. Дотик до струмопровідних частин (мережі під напругою) у більшості випадків призводить до судом м'язів, тобто людина самостійно не в змозі відірватися від провідника. Тому необхідно швидко відключити ту частину електрообладнання, до якої доторкається людина. Будь-яке зволікання при наданні допомоги, а також невміння того, хто допомагає, надати кваліфіковану допомогу, призводить до загибелі людини, яка знаходиться під дією струму.

При звільненні потерпілих від струмопровідних частин або проводу в електроустановках напругою до 1000 В відключають струм, використовуючи сухий одяг, палицю, дошку, шапку, сухі рукавиці, рукав одягу, діелектричні рукавиці. Провідники перерізають інструментом з ізольованими ручками, перерубують сокирою з дерев'яним сухим топорищем.

Потерпілого можна також відтягнути від струмопровідних частин за одяг, уникаючи дотику до навколишніх металевих предметів та до відкритих частин тіла потерпілого. Відтягуючи потерпілого за ноги, не можна торкатися його взуття, оскільки воно може бути сирим і стає провідником електричного струму. Той, хто надає допомогу, повинен одягнути діелектричні рукавиці або обмотати їх шарфом, натягнути на них рукав піджака або пальта. Можна також ізолювати себе, ставши на гумовий килимок, суху дошку тощо.

Після звільнення потерпілого від дії струму потрібно відразу ж надати йому необхідну медичну допомогу. Виділяють три стани людського організму внаслідок дії електроструму:

– I стан – потерпілий при свідомості. Слід забезпечити повний спокій, 2-3 годинне спостереження, виклик лікаря.

– II стан – потерпілий непритомний, але дихає. Людину покласти горизонтально, розстебнути комір і пасок, дати нюхати нашатирний спирт, викликати лікаря.

– III стан – потерпілий не дихає або дихає з перервами, уривчасто. Роблять штучне дихання і непрямий масаж серця.

Якщо потерпілий після звільнення від дії електричного струму і надання медичної допомоги прийшов до тями, його не слід одного відправляти додому або допускати до роботи. Такого потерпілого слід доставити в лікувальний заклад, де за ним буде встановлено спостереження, так як наслідки від впливу електричного струму можуть проявитися через кілька годин і привести до більш важких наслідків.

Дії працівників у випадку пожежі. Після закінчення робочого дня працівники повинні навести порядок на робочому місці, зачинити вікна та вимкнути електроживлення приладів і обладнання, яким вони користувалися (настільні лампи, друкарські та лічильні машинки, вентилятори, побутові кондиціонери, комп'ютери, радіоприймачі і таке інше).

Відповідальний за пожежну безпеку у приміщенні після закінчення роботи повинен оглянути його, переконатися у відсутності порушень, що можуть привести до пожежі, перевірити відключення електроприладів, обладнання, освітлення.

У разі виявлення ознак пожежі працівник, який їх помітив, повинен:

- негайно повідомити про це державну пожежну охорону (номер телефону для виклику пожежної охорони 101), вказати при цьому адресу, кількість поверхів, місце виникнення пожежі, наявність людей, а також своє прізвище;

- повідомити про пожежу керівника (власника);

- вжити заходів щодо евакуації людей та матеріальних цінностей, гасіння пожежі з використанням наявних вогнегасників та інших засобів пожежогасіння.

Керівник (власник) , якому повідомлено про виникнення пожежі, повинен:

- перевірити, чи викликано державну пожежну охорону;

- перевірити здійснення оповіщення людей про пожежу;

- вимкнути у разі необхідності струмоприймачі та вентиляцію;

- у разі загрози життю людей негайно організувати їх рятування (евакуацію), вивести за межі небезпечної зони всіх працівників, які не беруть участь у ліквідації пожежі;

- забезпечити дотримання техніки безпеки працівниками, які беруть участь у гасінні пожежі;

- організувати зустріч підрозділів державної пожежної охорони, надати їм допомогу у її локалізації та ліквідації.

Після прибуття на пожежу пожежних підрозділів повинен бути забезпечений безперешкодний доступ їх до місця, де виникла пожежа.

# ВИСНОВКИ

В дипломній роботі було досліджено використання сучасних технологій при проектуванні чи модернізації локальної обчислювальної мережі на прикладі існуючої на кафедрі ЕОМ.

Інновації у сфері комп'ютерних мереж продовжують впроваджуватись швидкими темпами. Просування мережевих технологій нині відбувається усіма фронтами, зокрема у розгортанні високопродуктивних маршрутизаторів і збільшенні швидкостей передачі, як у магістральних мережах, так і у мережах доступу.

Мережі Wi-Fi є перспективними для їх застосування при проектуванні локальних мереж. Проаналізовано стандарти механізмів захисту, які використовуються в мережах Wi–Fi на різних етапах роботи, їх вразливості та наявні методики атак.

Надано рекомендації щодо вдосконалення архітектури існуючої мережі. Проведено налаштування встановленого нового мережевого обладнання.

Надано обґрунтування та вибір платформи, а також описано її налаштування для організації хмарного сховища у локальній мережі кафедри. Хмарні сховища даних дозволяють забезпечити більш зручний учбовий процес за рахунок доступності даних з будь-якого місця, резервного копіювання, спільного доступу.

Реалізація запропонованих рекомендацій у існуючій локально-обчислювальній мережі кафедри дозволить:

- збільшити ефективність використання;
- підвищити рівень безпеки;
- надати більш зручні інструменти адміністрування;
- скоротити час на обробку інформації;
- знизити обсяг мережевого трафіку;
- скоротити обсяг паперового документообігу;
- уникнути втрати критично важливої інформації.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Олифер, Н.А. Компьютерные сети. Принципы, технологии, протоколы: учб. для вузов. 3-е издание [ Текст] / В.Г. Олифер // СПб.: Питер, 2006. – 958с.

2. Жуковицький І.В. Аналіз безпеки бездротових мереж wi-fi в автоматизованих системах залізничного транспорту / І. В. Жуковицький, І. О. Педенко // Наука та прогрес транспорту. – 2020. – № 4 (88). – С. 7-21.

3. Баранова Е.А., Зарешин С.В. Анализ защищенности беспроводных клиентов. Современные информационные технологии и ИТ-образование. 2018. Т.14, No 4.С. 938–946.

4. «Облачные сервисы» - что это такое [Електронний ресурс]: - Режим доступу: http://sdcompany.su/article/cloud/service

5. Колосков С., Абашев А., Мельник Р. Риски и тенденции в сфере обеспечения Информационной безопасности. – М.: «Информационная безопасность». – № 1. – 2013. – С. 8.

6. Частное облако [Електронний ресурс]: - Режим доступу: https://ru.bmstu.wiki/%D0%A7%D0%B0%D1%81%D1%82%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%BB%D0%B0%D0%BA%D0%BE

7. Виды облачных технологий [Електронний ресурс]: - Режим доступу: https://sites.google.com/site/rabotaoblacnyetehnologii/home/oblacnye-tehnologii/vidy-oblacnyh-tehnologij

8. Что такое PaaS? [Електронний ресурс]: - Режим доступу: https://azure.microsoft.com/ruru/overview/what-is-paas/

9. SaaS - что это такое? Software as a Service — программное обеспечение как услуга [Електронний ресурс]: - Режим доступу: http://fb.ru/article/187934/saas---chto-eto-takoesoftware-as-a-service-programmnoe-obespechenie-kak-usluga

10. . Cloud Computing: What is Infrastructure as a Service [Електронний ресурс]: - Режим доступу: https://technet.microsoft.com/en-us/library/hh509051.aspx

11. OneDrive [Електронний ресурс]: - Режим доступу: https://uk.wikipedia.org/wiki/OneDrive

12. Облачные технологии. Плюсы и минусы облачных технологий. [Електронний ресурс]: - Режим доступу: https://sites.google.com/site/rabotaoblacnyetehnologii/home/oblacnye-tehnologii/plusy-i-minusy-oblacnyh-tehnologij

13. Про охорону праці Закон України від 14.10.1992 № 2694-XII

14. ДСН 3.3.3-042-99. Державні санітрані норми мікроклімату виробничих приміщень [Текст]: Постанова Головного державного санітарного лікаря України від 01.12.1999 №42

15. ДБН В.2.5-28-2018«Природне і штучне освітлення»

16. ДСанПіН 3.3.2.007-98 «Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин»

17. ДСН 3.3.6-037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку»

18. ДСН 3.3.6-039-99 «Державні санітарні норми виробничої загальної та локальної вібрації»