МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет комп'ютерних наук та технологій
Кафедра «Комп'ютерні системи та мережі»

ШКОЛОВИЙ ВЛАДИСЛАВ ВЯЧЕСЛАВОВИЧ
Група КНТ-514м

СИСТЕМА ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ КОРПОРАТИВНИХ МЕРЕЖ ЗА ДОПОМОГОЮ ПРОТОКОЛІВ РЕЗЕРВУВАННЯ

АВТОРЕФЕРАТ

дипломної роботи на здобуття освітньо-кваліфікаційного рівня
«магістр» 123 Комп'ютерна інженерія
освітньої програми Комп'ютерні системи та мережі

2025 р.

Дипломна робота є рукопис.

Робота виконана в національному університеті «Запорізька політехніка», на кафедрі комп’ютерних систем та мереж

Керівник	кандидат технічних наук, доцент **Киричек Галина Григорівна,** Національний університет «Запорізька політехніка», доцент кафедри комп'ютерних систем та мереж
Офіційний рецензент:	**Романовський Олександр Володимирович,** генеральний директор ТОВ «Науково-виробниче підприємство «ХАРТРОН-ЮКОМ»

Захист відбудеться "25" грудня 2025 р.

Секретар екзаменаційної комісії, доцент кафедри комп’ютерних систем та мереж Т.В. Голуб

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Сучасні корпоративні мережі є критичною складовою інформаційної інфраструктури підприємств, забезпечуючи безперервний обмін даними, доступ до сервісів та підтримку бізнес-процесів. Будь-які простої мережі безпосередньо впливають на фінансові показники, репутацію компанії та безпеку даних. Зі зростанням вимог до доступності сервісів (24/7), появою хмарних технологій, віддаленої роботи та сервісів реального часу (VoIP, відеоконференції) питання відмовостійкості корпоративних мереж набуває особливої актуальності.

Одним із ключових напрямів підвищення надійності мережевої інфраструктури є використання протоколів резервування шлюзів першого переходу (FHRP), які забезпечують автоматичне перемикання трафіку у разі відмови основного маршрутизатора. Попри наявність значної кількості теоретичних описів, у практиці проєктування корпоративних мереж часто бракує кількісних рекомендацій щодо вибору та налаштування протоколів резервування з урахуванням їхніх часових характеристик, втрат пакетів та впливу на якість обслуговування. Це зумовлює необхідність комплексного аналізу FHRP та експериментального дослідження їх роботи на моделі корпоративної мережі.

Мета і завдання дослідження. Мета магістерської роботи полягає в розробленні та дослідженні системи забезпечення відмовостійкості корпоративної мережі на основі протоколів резервування, а також в оцінці ефективності їх застосування для підвищення надійності та безперервності функціонування сучасних інформаційних систем.

Для досягнення поставленої мети необхідно виконати такі основні завдання:

1. Проаналізувати архітектуру та особливості функціонування корпоративних мереж, фактори, що впливають на їхню надійність, а також показники MTBF, MTTR та параметри QoS;

2. Дослідити існуючі методи резервування мережевих ресурсів і протоколи резервування першого переходу (HSRP, VRRP, GLBP), визначити їх переваги, недоліки та області застосування;

3. Виконати порівняльний аналіз FHRP-протоколів за критеріями сумісності, часу перемикання, можливостей балансування навантаження та складності впровадження;

4. Розробити модель відмовостійкої корпоративної мережі на основі обладнання Cisco з використанням протоколу HSRP у середовищі Cisco Packet Tracer;

5. Реалізувати тестову схему мережі, налаштувати HSRP зі стандартними та оптимізованими таймерами та перевірити базову працездатність мережі;

6. Розробити методику експериментальних досліджень (сценарії відмов, серії вимірювань, показники оцінки) та провести експерименти для різних конфігурацій мережі;

7. Проаналізувати отримані результати, порівняти роботу мережі без резервування та з використанням HSRP, сформувати практичні рекомендації щодо побудови відмовостійких корпоративних мереж.

Об'єкт дослідження – корпоративна мережа як інфраструктура передавання та обробки даних.

Предмет дослідження – методи забезпечення відмовостійкості та протоколи резервування шлюзів (FHRP), зокрема їх часові характеристики, вплив на доступність сервісів і якість обслуговування.

Методи дослідження у роботі охоплюють аналіз наукових публікацій і технічної документації з питань надійності мереж, високої доступності та FHRP-протоколів, моделювання мережевої інфраструктури в середовищі Cisco Packet Tracer, а також імітацію аварійних ситуацій (відмова активного шлюзу, відновлення маршрутизатора, зміна таймерів) із використанням режиму Simulation Mode. У ході експериментів здійснювалося вимірювання часу автоматичного перемикання (failover), часу відновлення активної ролі маршрутизатора (preemption), кількості втрачених ICMP-пакетів, після чого проводився порівняльний та статистичний аналіз отриманих результатів для різних конфігурацій мережі.

Наукова новизна отриманих результатів полягає в систематизації вимог до відмовостійкої корпоративної мережі з позицій показників надійності (MTBF, MTTR) та параметрів QoS і формуванні узагальненої моделі впливу відмов на якість

обслуговування. Узагальнено та структуровано підходи до застосування протоколів резервування першого переходу (HSRP, VRRP, GLBP) у корпоративних мережах, орієнтованих на обладнання Cisco. Запропоновано й реалізовано методику експериментального дослідження параметрів HSRP у тестовій моделі мережі з варіацією таймерів hello/hold та аналізом часових характеристик перемикання, а також отримано кількісні оцінки впливу стандартних (3/10) та оптимізованих (1/3) значень таймерів HSRP на час failover, час відновлення активної ролі та втрати пакетів у типовій корпоративній мережі.

Практичне значення отриманих результатів:

Розроблена тестова модель корпоративної мережі з використанням HSRP може бути безпосередньо застосована як шаблон під час проєктування та модернізації реальних мережевих інфраструктур на базі обладнання Cisco. Отримані експериментальні результати та сформульовані рекомендації щодо налаштування таймерів HSRP дають змогу зменшити час простою, мінімізувати втрати пакетів і підвищити доступність сервісів у корпоративних мережах. Матеріали роботи можуть використовуватися в навчальному процесі при викладанні дисциплін з комп'ютерних мереж, адміністрування та мережевої безпеки, а також слугувати основою для подальших досліджень у сфері відмовостійкості та високої доступності.

Апробація результатів дипломної роботи. Основні положення магістерської роботи та результати досліджень представлено на науково-практичній конференції «Теорія та практика актуальних наукових досліджень» 26–27 вересня 2025 року, м. Полтава, Україна та опубліковано у збірці тез конференції.

Структура та обсяг роботи. Дипломна робота складається зі вступу, чотирьох розділів, висновків, переліку джерел посилання, додатку. Основна частина містить 86 сторінок, 36 рисунків і 14 таблиць, переліку джерел посилання зі 21 найменування.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У першому розділі проведено аналіз корпоративних мереж як основи сучасної IT-інфраструктури, розглянуто їхню структуру, основні компоненти, класифікацію за масштабом (LAN, MAN, WAN) та модульні підходи до побудови. Окремо проаналізовано переваги використання корпоративних мереж (масштабованість, централізоване управління, підтримка різних типів трафіку) та виклики, пов'язані зі зростанням складності, вимогами до безпеки і забезпеченням безперервності сервісів. Розглянуто проблеми надійності та вплив відмов на якість обслуговування, введено показники MTBF, MTTR, параметри QoS та показано їх взаємозв'язок з доступністю мережевих сервісів. На основі проведеного огляду сформульовано мету роботи, об'єкт і предмет дослідження, а також перелік основних задач, пов'язаних з розробленням і дослідженням системи забезпечення відмовостійкості корпоративної мережі.

У другому розділі розглянуто технології забезпечення відмовостійкості корпоративних мереж, зосереджено увагу на понятті високої доступності (High Availability), резервуванні та відмовостійкості, а також їх ролі у побудові надійної мережевої інфраструктури. Проаналізовано основні підходи до підвищення доступності: балансування навантаження, усунення єдиних точок відмови, моніторинг, резервування фізичної інфраструктури, каналів зв'язку, сервісів і даних, а також організація аварійного відновлення. Також були розглянуті методи захисту інформації як складові надійності, що доповнюють механізми резервування та формують комплексний підхід до забезпечення безперервної роботи корпоративних мереж. Окрему увагу приділено протоколам резервування першого переходу (FHRP): HSRP, VRRP, GLBP, їх архітектурі, механізмам вибору активного та резервного шлюзів, принципам функціонування в умовах відмов. Узагальнений порівняльний аналіз представлено на рисунку 1 у вигляді радарного графіку, який наочно відображає відмінності між протоколами за основними критеріями.

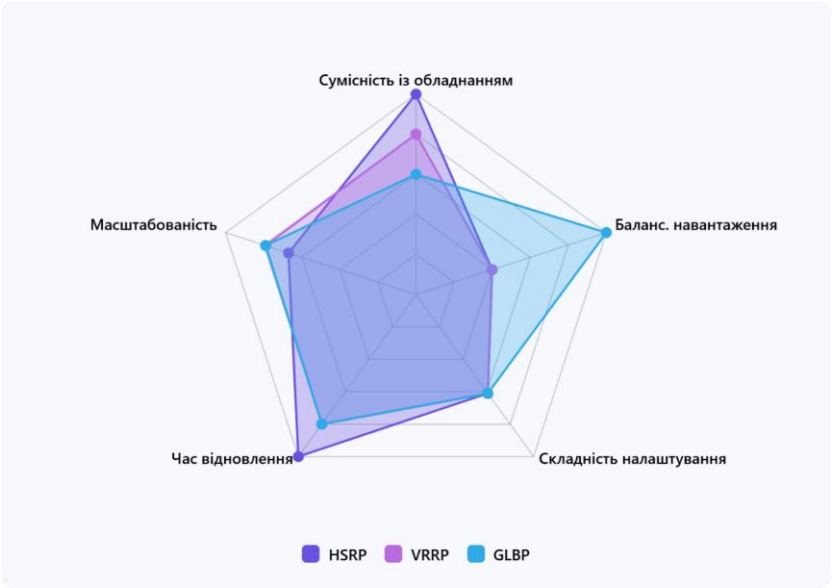

Рисунок 1 - Графік порівняння протоколів резервування

На основі отриманих результатів обґрунтовано вибір протоколу HSRP як основного засобу реалізації відмовостійкості шлюзу в подальших розділах роботи, тоді як VRRP та GLBP розглядаються як альтернативні рішення на теоретичному рівні.

У третьому розділі виконано проєктування та реалізацію відмовостійкої тестової корпоративної мережі в середовищі Cisco Packet Tracer. Наведено логічну схему мережі (рис.2) з двома шлюзами, комутаторами доступу, користувацькими ПК та VLAN-сегментацією, яка відображає типовий фрагмент корпоративної інфраструктури з резервуванням шлюзів. У вигляді лістингів 1-2 представлено ключові фрагменти налаштувань HSRP на маршрутизаторах, включно з налаштуванням пріоритетів та активацією механізму preempt.

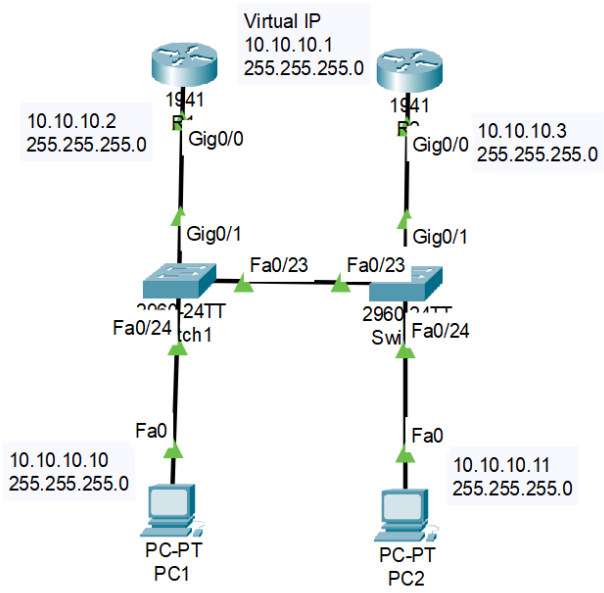

Рисунок 2 - Логічна схема мережі

Лістинг 1 - Налаштування R1

```
R1(config)# interface g0/0
R1(config-if)#ip address 10.10.10.2
255.255.255.0
R1(config-if)# no shutdown
R1(config-if)#standby 10 ip 10.10.10.1
R1(config-if)#standby 10 priority 120
R1(config-if)#standby 10 preempt
```

Лістинг 2 - Налаштування R2

```
R2(config)# interface g0/0
R2(config-if)#ip address 10.10.10.3
255.255.255.0
R2(config-if)# no shutdown
R2(config-if)#standby 10 ip 10.10.10.1
R2(config-if)#standby 10 priority 100
R2(config-if)#standby 10 preempt
```

На окремих рисунках (рис. 3-4) продемонстровано результати первинного тестування: статуси Active/Standby для маршрутизаторів, що підтверджує працездатність побудованої відмовостійкої схеми.

```
R1#show standby
GigabitEthernet0/0 - Group 10
  State is Active
    5 state changes, last state change 00:00:27
  Virtual IP address is 10.10.10.1
  Active virtual MAC address is 0000.0C07.AC0A
    Local virtual MAC address is 0000.0C07.AC0A (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.389 secs
  Preemption enabled
  Active router is local
  Standby router is 10.10.10.3
  Priority 120 (configured 120)
  Group name is hsrp-Gig0/0-10 (default)
R1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      10   120 P Active   local           10.10.10.3      10.10.10.1
R1#
```

Рисунок 3 - Перевірка HSRP на R1

```
R2#show standby
GigabitEthernet0/0 - Group 10
  State is Standby
    6 state changes, last state change 00:00:39
  Virtual IP address is 10.10.10.1
  Active virtual MAC address is 0000.0C07.AC0A
    Local virtual MAC address is 0000.0C07.AC0A (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.846 secs
  Preemption enabled
  Active router is 10.10.10.2
  Standby router is local
  Priority 100 (default 100)
  Group name is hsrp-Gig0/0-10 (default)
R2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gig0/0      10   100 P Standby  10.10.10.2      local           10.10.10.1
R2#
```

Рисунок 4 - Перевірка HSRP на R2

Четвертий розділ присвячено експериментальному дослідженню параметрів відмовостійкості корпоративної мережі в різних режимах функціонування. Спочатку розглянуто базову

конфігурацію без протоколів резервування, у якій відмова єдиного маршрутизатора-шлюзу призводить до повної втрати доступу до ресурсів. Експериментальні вимірювання показали, що тривалість простою мережі в такому випадку становить близько 60 с, при цьому втрачається значна кількість ICMP-пакетів і відновлення зв'язку можливе лише після ручного втручання адміністратора.

Далі досліджено роботу мережі з протоколом HSRP зі стандартними таймерами (standby 10 timers 3 10). Для цієї конфігурації виміряно час автоматичного перемикання (failover) при відмові активного маршрутизатора, час відновлення активної ролі (preemption) після повернення маршрутизатора в мережу та кількість втрачених ICMP-пакетів.

За результатами серії прогонів установлено, що середній час failover становить приблизно 12 с, а час повернення активної ролі - близько 7-8 с, при цьому втрати пакетів залишаються на прийнятному рівні (1-2 пакети на подію), а процес перемикання є повністю автоматизованим.

На завершальному етапі досліджено конфігурацію з оптимізованими таймерами HSRP (standby 10 timers 1 3). Повторено серію експериментів за тим самим сценарієм відмов і відновлення, виконано порівняльний аналіз отриманих часових характеристик.

Показано, що зменшення інтервалів hello/hold дозволяє скоротити середній час failover до ≈3 с, а час відновлення активної ролі - до ≈2 с, зберігаючи при цьому низький рівень втрат ICMP-пакетів (0-1 пакет за подію).

На рисунках 5-7 наочно порівнюються результати експерементів для базової мережі, HSRP зі стандартними таймерами та HSRP з оптимізованими параметрами, що дає змогу зробити висновки що впровадження протоколів резервування першого переходу є необхідною умовою для забезпечення високої доступності корпоративних мереж.

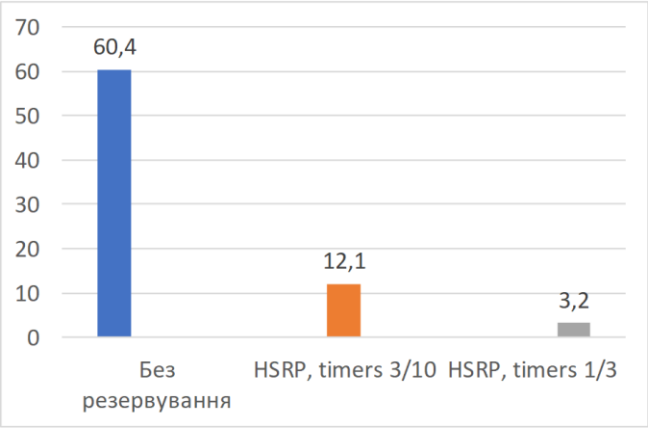

Рисунок 5 - Середній час простою мережі при відмові шлюзу

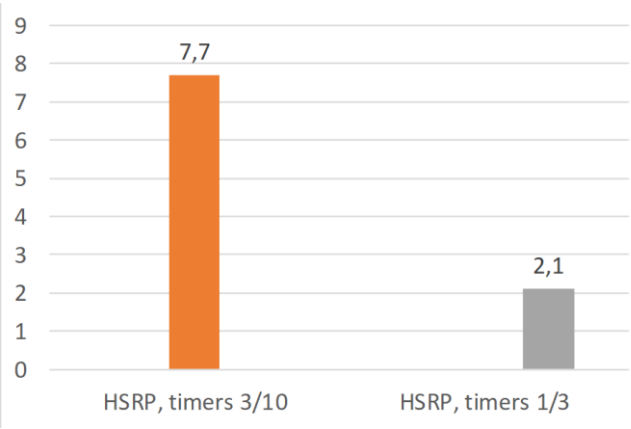

Рисунок 6 - Час відновлення активної ролі маршрутизатора R1 (preemption)

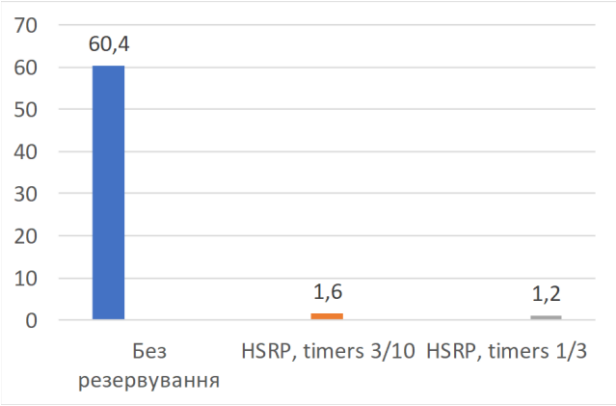

Рисунок 7 - Втрати ICMP-пакетів при відмові шлюзу для різних конфігурацій

Вибір конкретних значень таймерів HSRP повинен здійснюватися з урахуванням компромісу між швидкістю реагування на відмови та додатковим службовим навантаженням на мережу, однак результати експериментів показують, що навіть помірне зменшення таймерів дає суттєвий виграш у відмовостійкості без помітного погіршення інших характеристик.

ВИСНОВКИ

Результати, отримані в дипломній роботі, становлять практичне рішення задачі підвищення відмовостійкості корпоративних мереж на основі протоколів резервування першого переходу.

Отримано такі основні теоретичні й практичні результати:

1. Проведено комплексний аналіз архітектури корпоративних мереж, факторів, що впливають на їхню надійність, та показників доступності;

2. Досліджено методи забезпечення відмовостійкості і протоколи резервування першого переходу (HSRP, VRRP, GLBP), виконано їх порівняльний аналіз за ключовими критеріями;

3. Розроблено та реалізовано в середовищі Cisco Packet Tracer тестову модель відмовостійкої корпоративної мережі з використанням HSRP;

4. Проведено експериментальні дослідження роботи мережі в трьох конфігураціях: без резервування, з HSRP зі стандартними таймерами (3/10) та з оптимізованими таймерами (1/3). Встановлено, що впровадження HSRP дозволяє скоротити час простою з десятків секунд до ≈12 с, а оптимізація таймерів зменшує час failover до ≈3,2 с і час відновлення активної ролі до ≈2,1 с при мінімальних втратах пакетів.

Таким чином, усі поставлені в роботі завдання виконано, а поставлена мета досягнута.