Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

до виконання курсової роботи
з дисципліни «Захист інформації в комп`ютерних системах та мережах»
для студентів спеціальності 123 Комп'ютерна інженерія
освітньої програми 123.00.01 Комп'ютерна інженерія

Київ-2025

Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в комп`ютерних системах та мережах» для студентів спеціальності 123 Комп’ютерна інженерія, освітньої програми 123.00.01 Комп’ютерна інженерія / Укладачі: Костюк Ю.В., Складанний П.М., Рзаєва С.Л. Київ: КСУБГ, 2025. 82 с.

Методичні рекомендації містять загальні положення про організацію підготовки курсової роботи бакалавра спеціальності 123 Комп’ютерна інженерія, вимоги до її структурних елементів, виконання та оформлення. Описується порядок та процедура захисту. У додатках наведено зразки документів, що використовуються при підготовці курсової роботи бакалавра.

Рекомендовано Вченою радою Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка (протокол № 2 від 19 лютого 2025 р.)

ЗМІСТ

ВСТУП

Курсова робота є самостійною, науковою, теоретично-практичною, навчально-дослідною роботою студента, що завершує вивчення основних дисциплін, передбачених навчальним планом. В процесі її виконанні повинні бути використані і продемонстровані знання, вміння та навички, отримані за час вивчення дисциплін з циклу професійної підготовки.

Методичні рекомендації до виконання курсової роботи з дисципліни «Захист інформації в комп`ютерних системах та мережах» є нормативним документом Київського столичного університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка для здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 123 Комп'ютерна інженерія, освітньої програми 123.00.01 Комп'ютерна інженерія. Методичні рекомендації укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Курсова робота виконується з метою закріплення, поглиблення і узагальнення знань, одержаних студентами за час навчання, та їх застосування до комплексного вирішення конкретного фахового завдання. Виконання курсової роботи передбачає вироблення навичок самостійної роботи з джерелами й науковою літературою, допомагає здобувачу систематизувати отримані теоретичні знання та набути практичних вмінь, що дає можливість: виявити здатність здобувача самостійно осмислити проблему, творчо та критично її дослідити; вміння збирати, систематизувати і аналізувати джерела та літературу; застосовувати отримані знання при вирішенні практичних завдань; формулювати висновки, пропозиції й рекомендації з предмета дослідження.

Загальні вимоги до курсової роботи:

- чіткість побудови;
- логічна послідовність викладу матеріалу, переконлива аргументація;
- точність викладу, яка виключає можливість суб'єктивного та неоднозначного тлумачення;
- конкретність викладу результатів роботи;
- доведення висновків та обґрунтованість рекомендацій.

Захист курсових робіт відбувається згідно затвердженого графіку. Типова структура курсової роботи має бути такою: титульний аркуш, план-проспект, анотація, зміст, перелік умовних позначень (при необхідності), вступ, 4-5 розділів, що розкривають зміст проблеми та описують результати теоретичного дослідження і практичного завдання, висновки та пропозиції, список використаних джерел, додатки.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. МЕТА ТА ЗАВДАННЯ КУРСОВОЇ РОБОТИ

Відповідно до навчального плану спеціальності 123 Комп'ютерна інженерія, освітньої програми 123.00.01 Комп'ютерна інженерія, здобувачі освітнього рівня першого (бакалаврського) виконують курсову роботу (КР) з дисципліни «Захист інформації в комп`ютерних системах та мережах».

Курсова робота – складовий компонент освітнього процесу вивчення дисципліни. Виконання курсової роботи − перший самостійний крок майбутнього фахівця, коли право остаточного вибору інженерно-технічних рішень і відповідальність за їх прийняття цілком належить його автору. **Метою курсової** роботи є:

- закріплення, поглиблення й узагальнення знань, отриманих студентами за час вивчення дисципліни «Захист інформації в комп'ютерних системах та мережах», а також отримання практичних навичок моделювання та розрахунку параметрів комп'ютерних мереж (КМ), аналізу їх функціонування в сучасному середовищі з урахуванням вимог інформаційної безпеки;
- розвиток навичок самостійної роботи і використання сучасних інформаційних технологій для розв'язання задач, пов'язаних із захистом інформації в комп'ютерних системах та мережах;
- отримання навичок адміністрування, конфігурування КМ, організації доступу до мережі Internet, а також забезпечення захисту інформації в комп'ютерних системах та мережах.

Завдання до курсової роботи передбачає:

- розробку структурної схеми комп'ютерної мережі (КМ) з урахуванням вимог захисту інформації;
- вибір та вставлення топології мережі згідно з варіантом із забезпеченням її надійності та безпеки;
- встановлення IP-адрес для мережевих інтерфейсів із урахуванням заходів захисту від несанкціонованого доступу;
- налагодження серверів з акцентом на безпеку, зокрема конфігурування засобів захисту, таких як міжмережеві екрани, системи виявлення та запобігання вторгненням;
- вибір кабельної системи, що відповідає вимогам інформаційної безпеки, а також комунікаційного обладнання та комутаційних елементів (роз'єми, коннектори, кросові панелі, шафи, антено-фідерний тракт) з акцентом на захищеність фізичного середовища;
- формування висновків щодо працездатності та безпеки КМ з урахуванням реалізованих заходів захисту інформації.

Виконання курсової роботи з дисципліни «Захист інформації в комп'ютерних системах та мережах» та її захист є формою контролю рівня знань студентів за вивченням даної навчальної дисципліни.

На виконання роботи відводиться один семестр. Студент має виконати курсову роботу згідно з графіком та вчасно подати її на кафедру.

Курсова робота є самостійною роботою студента. Відповідальність за правильність аналітичних висновків, результатів розрахунків і моделювання, а також оформлення несе студент − автор КР.

1.2. Тематика курсової роботи

Спрямування КР повинне забезпечувати творчу роботу студента та самостійне розв'язання окремих технічних завдань. Вміст та структура курсової роботи (КР) повинні враховувати специфіки напряму та вимоги освітньої програми.

З урахуванням викладеного тематика курсової роботи повинна:

- бути актуальною і відповідати сучасному стану науки і техніки;
- відображати перспективи розвитку відповідних галузей техніки з урахуванням останніх наукових досліджень;
- стимулювати студентів на творчий пошук нових науково-технічних, проєктних та інших рішень;
- викликати у студентів необхідність опрацювання спеціальної науково-технічної літератури;
- передбачати вибір сприйнятого вирішення поставленого завдання на основі використання сучасних засобів комп'ютерної техніки;
- бути націленою на вирішення задач, які є актуальними для організацій, в яких проводиться курсова робота.

За трудомісткістю КР повинна відповідати терміну, який відведений на курсову роботу навчальним планом.

Виконання курсової роботи з однієї теми кількома студентами однієї групи не припустиме. Обрані студентами й узгоджені з науковими керівниками теми робіт затверджуються на засіданні кафедри. Курсові роботи виконанні студентами на теми, які не затверджені кафедрою не розглядаються.

1.3. Порядок виконання

Вибір теми студентом здійснюється на початку семестру. Студент обговорює тему курсової з викладачем, складає план роботи та список літератури з обраної теми. Вивчення літератури необхідно розпочати з нормативно-правових актів України та нормативних документів системи технічного захисту інформації (ТЗІ), а потім перейти до вивчення наявної експлуатаційно-технічної документації та більш спеціальних досліджень, наприклад наукових статей. У процесі виконання роботи студент підтримує зв'язок з викладачем, звертаючись до нього за консультацією по мірі виникнення питань або ускладнень.

Складання розширеного плану роботи студентом здійснюється протягом першої половини семестру. Роль викладача полягає в уточненні плану роботи та списку літератури за темою, обговоренні предмету, об'єкту,

мети та завдань дослідження, повноти та достатності викладення теми, сприянні творчим пошукам за темою роботи, а також у підготовці студента до захисту курсової роботи.

Оформлюючи роботу, студент спочатку складає її електронний (чорновий) варіант та представляє його викладачу. Після перевірки, враховуючи зауваження та вказівки, студент доопрацьовує роботу.

Студент подає роботу для перевірки, оформлює роботу у відповідності до вимог. Після цього робота друкується та пред'являється викладачу не пізніше ніж за тиждень до дати захисту.

На захист студент повинен підготувати доповідь та презентацію по результатам проведеної роботи. Студент розробляє презентацію роботи за допомогою засобів «Microsoft Office PowerPoint» тривалістю 3-5 хвилин. Захист курсової роботи здійснюється згідно графіку захисту курсових робіт перед членами комісії кафедри.

1.4. Приклади тем на курсову роботу

1. Моделювання та візуалізація бездротових сенсорних мереж з впровадженням методів захисту даних та контролю доступу.
2. Моделювання захищеної комп'ютерної мережі в середовищі Packet Tracer з акцентом на багаторівневий захист інформації.
3. Розробка захищеної безпровідної комп'ютерної мережі із використанням сучасних криптографічних методів для захисту конфіденційних даних.
4. Проєктування корпоративної комп'ютерної мережі з впровадженням засобів шифрування та захисту інформації на всіх рівнях OSI.
5. Розробка комп'ютерної мережі із захистом інформації з використанням технології Ethernet і протоколів безпеки на мережевому рівні.
6. Проєктування захищеної корпоративної мережі на основі 100Base-TX Full Duplex з інтеграцією криптографічних засобів захисту.
7. Побудова захищеної бездротової локальної мережі на базі Wi-Fi 6 (802.11ax) із впровадженням протоколів захисту від атак.
8. Проєктування бездротової локальної мережі підприємства з багаторівневим захистом даних і контролем доступу.
9. Проєктування локальної мережі з шифруванням даних для підприємств, розташованих на різних поверхах будівлі.
10. Проєктування захищеної локальної мережі для підприємства в одній будівлі з використанням технології Ethernet і багаторівневого захисту.
11. Проєктування мережі з інтеграцією засобів захисту даних для підприємства, розташованого в різних будівлях.
12. Проєктування локальної мережі підприємства на базі Gigabit Ethernet з впровадженням шифрування та захисту на рівні мережі.
13. Проєктування захищеної локальної мережі на основі технології Gigabit Ethernet для багаторівневого захисту даних.
14. Проєктування безпровідної локальної мережі з використанням технологій Gigabit Ethernet і бездротового захисту від атак.

15. Розробка захищеної локальної мережі на базі Gigabit Ethernet для малого підприємства з впровадженням багаторівневих політик безпеки.
16. Проєктування корпоративної мережі з інтеграцією технології Fast Ethernet та шифруванням трафіку.
17. Проєктування бездротової мережі на основі Fast Ethernet із захистом від атак на рівні Wi-Fi.
18. Розробка захищеної корпоративної мережі з використанням технології оптоволоконного кабелю та криптографії.
19. Проєктування мережі з оптоволоконним зв’язком та засобами захисту даних для багатоповерхових підприємств.
20. Розробка захищеної локальної мережі на основі технології Fast Ethernet з впровадженням політик безпеки і захисту трафіку.
21. Проєктування корпоративної мережі з використанням технології Gigabit Ethernet та засобів захисту інформації від несанкціонованого доступу.
22. Моделювання захищеної корпоративної мережі з підтримкою захисту на рівні трафіку і фізичної безпеки.
23. Побудова захищеної корпоративної мережі у програмному середовищі Packet Tracer з інтеграцією систем виявлення вторгнень (IDS).
24. Розробка VPN-захисту для віддаленого доступу до корпоративної мережі.
25. Проєктування локальної мережі з використанням Fast Ethernet і впровадженням протоколів для захисту від атак DoS/DDoS.
26. Побудова структурної схеми захищеної мережі в Packet Tracer із використанням сучасних методів шифрування трафіку.
27. Розробка захищеної комп’ютерної мережі з інтеграцією політики безпеки даних у середовищі корпоративної інфраструктури.
28. Оптимізація локальної мережі з використанням технологій Ethernet і впровадженням комплексних засобів безпеки.
29. Розробка корпоративної мережі з підтримкою технології Gigabit Ethernet і впровадженням сучасних криптографічних методів.
30. Проєктування локальної мережі на основі 10Base-T із застосуванням захисту на рівні каналу зв'язку.
31. Моделювання бездротової мережі з використанням технології Bluetooth Low Energy (BLE) та засобів шифрування для захисту інформації.
32. Розробка корпоративної мережі з впровадженням технології IPv6 та захистом даних на мережевому рівні.
33. Проєктування системи управління доступом до корпоративної мережі з багаторівневим захистом від несанкціонованого доступу.
34. Розробка політики інформаційної безпеки для корпоративної мережі із захистом від внутрішніх загроз.
35. Впровадження технології VLAN для сегментації мережі з підвищенням рівня захисту інформації.
36. Проєктування мережі для малого підприємства з використанням протоколів VPN для захисту віддаленого доступу.

37. Використання технології MPLS у корпоративній мережі з впровадженням політик безпеки на рівні маршрутизації.
38. Моделювання мережі із захистом від атак ARP-spoofing у середовищі корпоративної інфраструктури.
39. Проєктування комп'ютерної мережі з використанням технології SD-WAN та інтеграцією засобів захисту трафіку.
40. Розробка стратегії захисту інформації у хмарній корпоративній інфраструктурі з використанням сучасних методів шифрування.
41. Проєктування захищеної локальної мережі на основі технології Power over Ethernet (PoE) з інтеграцією засобів контролю доступу.
42. Моделювання гібридної хмарної інфраструктури з впровадженням захисту інформації на всіх рівнях передачі даних.
43. Інтеграція IDS та IPS систем у корпоративну мережу з використанням технології Ethernet для захисту від зовнішніх атак.
44. Проєктування мережі для банківської інфраструктури з впровадженням криптографічних методів для захисту фінансових операцій.
45. Розробка політики захисту даних для медичної інфраструктури з акцентом на захист конфіденційної інформації пацієнтів.
46. Впровадження технології двофакторної аутентифікації у корпоративну мережу для підвищення безпеки доступу до інформації.
47. Проєктування мережі з технологією IoT з акцентом на захист даних, що передаються через бездротові сенсори.
48. Використання технології NAT для захисту внутрішніх IP-адрес у корпоративній мережі від зовнішніх загроз.
49. Моделювання захищеної мережі для фінансової інституції з акцентом на захист даних, що передаються через платіжні системи.
50. Розробка багаторівневої стратегії захисту інформації для корпоративної мережі з використанням технології Zero Trust Network.
51. Інтеграція міжмережевих екранів наступного покоління (NGFW) у корпоративну мережу для запобігання загрозам.
52. Розробка стратегії захисту інформації у корпоративній мережі з використанням технології сегментації VLAN.
53. Проєктування захищеної мультисервісної мережі з інтеграцією систем шифрування та контролю доступу.
54. Проєктування захищеної бездротової мережі з використанням WPA3 і криптографічних протоколів для захисту трафіку.
55. Впровадження систем багатофакторної аутентифікації у захищеній корпоративній мережі.
56. Побудова багаторівневої стратегії захисту даних у корпоративній мережі з використанням DLP (Data Loss Prevention).

Таблиця 1. – Рекомендований календарний план

№ з/п	Назва етапу роботи	Гермін виконання (№ тижня)
1	Отримання завдання	1 тиждень
2	Аналіз технічного завдання	2 тиждень
3	Розробка структурної схеми захищеної комп'ютерної мережі на основі заданої мережної технології, яка повинна включати комплексний підхід до захисту інформації, що включає як превентивні заходи (Firewall, IDS/IPS), так і заходи для захисту даних (VPN, шифрування), а також управління доступом та сегментацію мережі для зменшення можливих загроз.	3 тиждень
4	Опис структури кабельної системи захищеної комп'ютерної мережі (вибір конкретних типів кабелів та заходів безпеки) повинен враховувати не лише вибір типів кабелів, але й забезпечення комплексної захищеності від перехоплення даних, фізичних атак та електромагнітних впливів. Використання STP та оптоволоконних рішень у поєднанні із додатковими захисними заходами забезпечує високий рівень безпеки передачі інформації в комп'ютерних мережах.	4 тиждень
5	Вибір і розміщення обладнання для захищеної мережі має базуватися на інтеграції сучасних засобів захисту інформації. Це включає використання мережних адаптерів з підтримкою шифрування, маршрутизаторів з функцією VPN, брандмауерів, повторювачів з можливістю моніторингу та надійного антивірусного програмного забезпечення, оскільки комплексний підхід до вибору обладнання гарантує високий рівень захисту інформації в комп'ютерних мережах.	5 тиждень
6	Опис конкретних типів обладнання для захищеної мережі (мережні адаптери, інтерфейси, повторювачі, концентратори та антенно-фідерні пристрої) **(**докладний опис обладнання з акцентом на його безпеку, наприклад, мережні адаптери з підтримкою апаратного шифрування).	6 тиждень
8	Підтвердження коректності побудови захищеної комп'ютерної мережі є критично важливим для забезпечення високого рівня захисту інформації, що включає оцінку надійності обладнання, ефективності шифрування, захисту від атак типу Man-in-the-Middle, а також регулярні перевірки та удосконалення захисних механізмів для мінімізації ризиків і підвищення	7 тиждень

	надійності мережевих рішень.	
9	Аналіз недоліків захищеної комп'ютерної мережі, побудованої на основі заданої модифікації мережної технології, та рекомендації щодо покращення захисту (включає виявлення слабких місць у системі захисту, таких як незахищені точки доступу, та розробку заходів для їх усунення).	7 тиждень
10	Оформлення пояснювальної записки	8 тиждень
11	Захист курсової роботи	8-9 тиждень

1.5. Складові частини

Організаційно процес курсового проєктування складається з наступних етапів:

- підготовчого, на якому студент отримує тему, узгоджує з керівником об’єкт проєктування, особливості технічного завдання (ознайомлення зі станом проблеми, збирання фактичних матеріалів, проведення необхідних спостережень, досліджень тощо);
- основного, який починається одразу після узгодження технічного завдання й завершується тривалістю семестру. На цьому етапі робота повинна бути повністю виконана та перевірена керівником;
- заключного, який включає підготовку до захисту КР.

Основним документом, що представляють КР є пояснювальна записка. Текст пояснювальної записки до курсової роботи повинен бути викладений лаконічно, у обґрунтованому стилі. Не дозволяється переписування літературних джерел та використання не опрацьованих студентом Інтернет-оглядів.

1.6. Захист курсових робіт

В терміни, зазначені документом, курсова робота здається керівникові на перевірку. КР перевіряється по суті.

Захист КР проводиться у формі співбесіди зі з'ясуванням всіх питань, що виникли у керівника під час перевірки курсової роботи та під час захисту.

Оцінка за курсову роботу виставляться за державною шкалою.

На оцінку за КР впливають:

- якість виконання КР;
- компетентність та загальна ерудиція студента на запитання під час захисту.

Захист курсових робіт відбувається на відкритому засіданні за затвердженим графіком у такому порядку:

- оголошується початок чергового відкритого захисту курсової роботи;
- зачитується прізвище студента, тема роботи;
- студент чітко, коротко, технічно правильно і лінгвістично грамотно доповідає про зміст виконаної роботи;
- відповідає на кожне запитання чітко та за суттю;

– оголошується закінчення захисту.

На доповідь дається 5 хвилин. За цей час необхідно продемонструвати результати виконаної роботи на комп’ютері в середовищі моделювання КМ, стисло викласти суть прийнятих рішень, довести працездатність мережі, обґрунтувати результати розрахунку PDV. Після закінчення доповіді викладач може задавати питання, призначення яких – уточнити рівень кваліфікації і ступень самостійності доповідача. На питання необхідно давати стислі прямі відповіді, при необхідності використовувати середовище моделювання КМ.

За результатами захисту визначається оцінка, яка потім оголошується студенту. У результаті захисту курсової роботи виставляється оцінка в балах: 90-100, 82-89, 75-81, 69-74, 60-68, 35-59, 1-34.

2. СТРУКТУРА КУРСОВОЇ РОБОТИ

2.1. Обсяг курсової роботи

Курсова робота як оригінальне теоретично-прикладне дослідження мусить мати певну логіку побудови, послідовність і завершеність. Для успішного виконання КР необхідно чітко дотримуватись основних вимог до теоретичного рівня роботи, її змісту, структури, обсягу, форми викладання матеріалу, оформлення і захисту.

Виконання курсової роботи з дисципліни «Захист інформації в комп'ютерних системах та мережах» розпочинається з оформлення титулки (Додаток А). Курсова робота виконується тільки за індивідуальними завданням.

Індивідуальне завдання на курсову роботу видається керівником. На бланку за формою, що наведена в Додатку Б обов'язково повинна бути вказана дата видачі завдання. Індивідуальне завдання засвідчується підписом керівника КР. Завдання не нумерується як розділ. Далі має бути правильно оформлена анотація (Додаток В), перелік умовних позначень, одиниць, символів, скорочень і термінів (Додаток Г), зміст роботи (Додаток Д), вступ (Додаток Ж).

Загальний обсяг пояснювальної записки – від 28 до 40 сторінок (не рекомендовано обсяг більший за 45 сторінок), причому технічна її частина, у якій викладаються конкретні дані про розробку конкретної КМ, має містити не менш ніж 20 – 25 сторінок тексту з рисунками. Рисунки можуть містити необхідні для пояснень і розрахунків фрагменти загальної моделі мережі.

До записки додаються додатки формату А4 (структурна схема мережі, функціональна схема мережі, тощо) того ж формату.

Бібліографічні описи в переліку посилань наводять відповідно до чинних стандартів з бібліотечної та видавничої справи відповідно ДСТУ ГОСТ 7.1:2006 "Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання". Приклад оформлення бібліографічного опису наведено у Додатку К.

Робота має бути виконана з урахуванням державних і галузевих стандартів (ДСТУ 3008−95. Документація. Звіти у сфері науки і техніки. Структура та правила оформлення).

Мова курсової роботи − державна, стиль − науковий, чіткий, без орфографічних і синтаксичних помилок.

Рекомендується така структура курсової роботи:

1. Титульний лист (Додаток А)
2. Індивідуальне завдання на курсовий проєкт за формою (Додаток Б)
3. Анотація (Додаток В)
4. Перелік умовних позначень, одиниць, символів, скорочень і термінів (Додаток Г)
4. Зміст роботи (Додаток Д)

ВСТУП (Додаток Ж)

ОСНОВНА ЧАСТИНА. Розробка структурної схеми захищеної комп'ютерної мережі на основі заданої мережної технології, що включає опис структури кабельної системи захищеної комп'ютерної мережі, вибір конкретних типів кабелів та заходів безпеки. Особлива увага приділяється вибору екранованих кабелів (STP), оптоволокна та впровадженню заходів для захисту від перехоплення інформації). Вибір і розміщення обладнання для захищеної мережі з урахуванням конкретних типів мережних адаптерів, інтерфейсів, повторювачів, концентраторів та засобів захисту (включає підбір мережного обладнання з інтегрованими засобами захисту, такими як брандмауери, маршрутизатори з функцією VPN та антивірусне ПЗ). Опис конкретних типів обладнання для захищеної мережі (мережні адаптери, інтерфейси, повторювачі, концентратори та антенно-фідерні пристрої) (докладний опис обладнання з акцентом на його безпеку, наприклад, мережні адаптери з підтримкою апаратного шифрування).

Розрахунки, що підтверджують коректність побудови захищеної комп'ютерної мережі (провідної та безпровідної), що включають оцінку надійності мережевих рішень та захисних механізмів, таких як шифрування трафіку та захист від атак типу «людина посередині» (Man-in-the-Middle) тощо.

Аналіз недоліків захищеної комп'ютерної мережі, побудованої на основі заданої модифікації мережної технології, та рекомендації щодо покращення захисту (включає виявлення слабких місць у системі захисту, таких як незахищені точки доступу, та розробку заходів для їх усунення).

Недоліки комп’ютерної мережі, побудованої на основі заданої модифікації мережної технології і рекомендації по їх усуненню.

Висновки та пропозиції;

Список використаних джерел (приклад у Додатку К);

Додатки.

Змістовне наповнення пояснювальної записки та графічної частини – це результат самостійної – творчої роботи студента з питань, сформульованих у завданні на курсову роботу.

2.2. Вимоги до змісту розділів, оформлення та обсягу

До *пояснювальної записки (ПЗ*) необхідно включати матеріал, який безпосередньо відноситься до конкретної комп'ютерної мережі, яка підлягає моделюванню, у відповідності до завдання, згідно варіанту. Не рекомендується робити великі реферативні огляди. При необхідності можна робити посилання на відповідну літературу. Основний зміст записки – це обґрунтування прийнятих рішень та модель комп'ютерної мережі, згідно затвердженої назви. При цьому треба мати на увазі, що записку складають тоді, коли розробку комп'ютерної мережі завершено, всі рішення прийнято, всі деталі є відомими, є кінцевий результат, і саме його необхідно привести у записці разом з аргументацією вибору рішень, необхідними розрахунками, таблицями, рисунками, діаграмами, графіками та іншими матеріалами, які обґрунтовують прийняті рішення.

Пояснювальна записка не повинна бути перевантаженою за рахунок малоінформативного оглядового матеріалу, для скорочення обсягу якого рекомендується робити посилання на використані джерела інформації та менше їх цитувати. Доцільно вживати однакову термінологію. При перекладі з іноземної на українську мову невідомих термінів доцільно використовувати відповідні словники.

Не допускається дослівне переписування матеріалів з будь-яких джерел.

При необхідності дозволяється коротке цитування використаного матеріалу та посилання на джерела інформації.

Приблизний рекомендований обсяг кожного розділу наведено нижче. Назви розділів у конкретній роботі можуть відрізнятись від наведених далі, послідовність розташування розділів може бути іншою, але в цілому у пояснювальній записці рекомендовано висвітлити всі питання.

1. Розробка структурної схеми захищеної комп'ютерної мережі на основі заданої мережної технології є важливим етапом створення ефективної системи захисту інформації. Процес розробки включає детальне планування мережної архітектури, де особлива увага приділяється впровадженню засобів захисту інформації. Зокрема, потрібно врахувати використання міжмережевих екранів (Firewall) для контролю вхідного та вихідного трафіку з метою запобігання несанкціонованому доступу.

Крім того, важливо інтегрувати системи виявлення та запобігання вторгнень (IDS/IPS) для постійного моніторингу мережевого трафіку і своєчасного виявлення загроз. IDS надає можливість аналізувати підозрілі дії в мережі, тоді як IPS допомагає не тільки виявити, але й автоматично заблокувати загрози в реальному часі. Це дозволяє значно підвищити рівень захисту мережі від зовнішніх атак.

Також, при розробці схеми необхідно врахувати використання шифрування на різних рівнях комунікацій для забезпечення конфіденційності та цілісності даних, що передаються. Наприклад, протоколи TLS/SSL можуть бути застосовані для захисту HTTP-трафіку, а шифрування на рівні VPN забезпечує безпеку віддаленого доступу до ресурсів корпоративної мережі.

Важливим аспектом є правильне розташування мережевих сегментів з відповідними засобами захисту, наприклад, розподіл на внутрішні та зовнішні зони доступу (DMZ). Це дозволяє ізолювати критичні ресурси від прямого контакту з незахищеними зонами.

Додатково, варто розглянути застосування систем багатофакторної аутентифікації (MFA) для контролю доступу до мережевих ресурсів та посилення безпеки ідентифікації користувачів.

Таким чином, розробка структурної схеми захищеної комп'ютерної мережі повинна включати комплексний підхід до захисту інформації, що включає як превентивні заходи (Firewall, IDS/IPS), так і заходи для захисту даних (VPN, шифрування), а також управління доступом та сегментацію мережі для зменшення можливих загроз.

2. Опис структури кабельної системи захищеної комп'ютерної мережі є важливим етапом створення безпечного інформаційного середовища. При побудові такої системи необхідно ретельно обирати типи кабелів і впроваджувати спеціальні заходи безпеки для захисту даних від перехоплення, зломів та інших загроз.

Основний акцент має бути зроблений на використанні екранованих витих пар (STP). Цей тип кабелю має додатковий шар захисту від електромагнітних перешкод, що допомагає знизити ризик перехоплення сигналу через зовнішні інтерференції. Використання STP кабелів мінімізує можливість витоків інформації через кабельний канал, особливо в умовах високої концентрації мережевого обладнання або в чутливих зонах.

Для мереж, що потребують ще вищого рівня безпеки, рекомендується застосування оптоволоконних кабелів, які є найбільш захищеними від несанкціонованого доступу. Оптоволокно не піддається електромагнітним інтерференціям і не передає радіочастотних сигналів, що робить його практично неможливим для перехоплення без фізичного втручання. Такий кабель особливо важливий для захисту конфіденційних даних на довгих дистанціях або між критичними вузлами мережі.

Додатково, для захисту кабельної інфраструктури від фізичних загроз варто впроваджувати спеціальні заходи безпеки, такі як прокладання кабелів у захищених коридорах або використання металевих труб для їх фізичної ізоляції. Це знижує ризики фізичного доступу до кабелів зловмисниками та перехоплення сигналу через несанкціоновані підключення або розриви.

Також необхідно передбачити використання кабелів із підвищеною стійкістю до вібрацій та зовнішніх впливів у критичних частинах мережі для забезпечення безперервної роботи мережевих систем навіть у випадках зовнішніх атак або аварійних ситуацій.

Таким чином, опис структури кабельної системи захищеної комп'ютерної мережі повинен враховувати не лише вибір типів кабелів, але й забезпечення комплексної захищеності від перехоплення даних, фізичних атак та електромагнітних впливів. Використання STP та оптоволоконних рішень у поєднанні із додатковими захисними заходами забезпечує високий рівень

безпеки передачі інформації в комп'ютерних мережах.

3. Вибір і розміщення обладнання для захищеної комп'ютерної мережі є критичним етапом побудови системи, що забезпечує надійний захист інформації в комп'ютерних системах та мережах. Під час цього процесу необхідно враховувати не лише технічні характеристики пристроїв, але й їхню здатність забезпечувати високий рівень інформаційної безпеки.

При виборі мережних адаптерів особливу увагу слід приділяти моделям, що підтримують апаратне шифрування даних. Це дозволяє захищати інформацію ще на етапі її передачі з комп'ютера до мережі, знижуючи ризик перехоплення даних. Додатково, адаптери з вбудованими засобами аутентифікації та контролю доступу забезпечують захист від несанкціонованого доступу до мережі.

Мережні інтерфейси, що підтримують технології захисту, такі як віртуальні локальні мережі (VLAN) і протоколи безпечної передачі даних (SSL/TLS), також є важливими елементами при побудові захищених мереж. Вибір таких інтерфейсів забезпечує сегментацію трафіку і захист переданої інформації від перехоплення або підміни.

Для безпечної передачі даних у великих мережах важливим є правильний вибір та розміщення повторювачів і концентраторів з можливістю моніторингу та блокування підозрілої активності. У сучасних захищених мережах варто використовувати пристрої з вбудованими функціями захисту, такими як фільтрація трафіку та захист від атак на мережевому рівні.

Ключову роль у захисті інформації грає вибір брандмауерів (міжмережних екранів), які дозволяють створити бар'єр між внутрішньою мережею та зовнішніми загрозами. Використання сучасних брандмауерів з підтримкою інтелектуального аналізу трафіку, виявлення атак і блокування шкідливих дій є обов'язковим для забезпечення безпеки.

Ще однією важливою складовою є маршрутизатори з функцією VPN, що дозволяють створити безпечні канали передачі даних через незахищені мережі, такі як Інтернет. VPN забезпечує шифрування трафіку, тим самим захищаючи інформацію від перехоплення або підміни на шляху від відправника до одержувача.

Крім того, вибір антивірусного ПЗ для мережевого обладнання є невід’ємною частиною захисту. Антивірусні програми повинні інтегруватися з мережевими пристроями для сканування вхідного та вихідного трафіку на наявність шкідливого ПЗ та попередження загроз, таких як віруси, трояни або шпигунське ПЗ.

Отже, вибір і розміщення обладнання для захищеної комп'ютерної мережі має базуватися на інтеграції сучасних засобів захисту інформації. Це включає використання мережних адаптерів з підтримкою шифрування, маршрутизаторів з функцією VPN, брандмауерів, повторювачів з можливістю моніторингу та надійного антивірусного програмного забезпечення. Лише комплексний підхід до вибору обладнання гарантує високий рівень захисту інформації в комп'ютерних мережах.

4. Підтвердження та висновки про коректність побудови захищеної комп'ютерної мережі (провідної та безпровідної) є критично важливими для забезпечення високого рівня захисту інформації в комп'ютерних системах та мережах. Ось ключові аспекти, що охоплюють оцінку надійності мережевих рішень і захисних механізмів:

Оцінка надійності мережевих рішень

Для підтвердження коректності побудови захищеної мережі проводиться всебічна оцінка надійності мережевих рішень. Це включає перевірку обладнання (маршрутизаторів, комутаторів, брандмауерів) на відповідність сучасним стандартам безпеки, а також надійність реалізації механізмів захисту:

- Визначення часу напрацювання на відмову (MTBF) та середнього часу відновлення після збою (MTTR), щоб гарантувати стабільну та безперебійну роботу мережі.
- Аналіз якості шифрування даних, включаючи перевірку криптографічних алгоритмів (AES, RSA) на відповідність актуальним вимогам безпеки і їх стійкість до можливих атак.
- Оцінка ефективності використання засобів захисту, таких як брандмауери і системи запобігання вторгненням (IPS), для забезпечення належного рівня захисту трафіку і системи в цілому.

Захист від атак типу Man-in-the-Middle

Одним з ключових аспектів є захист від атак типу «людина посередині» (Man-in-the-Middle). Для цього необхідно:

- Впроваджувати шифрування трафіку як основний механізм захисту даних від перехоплення і модифікації. Це включає використання TLS/SSL для захищених з'єднань та VPN для забезпечення конфіденційності комунікацій.
- Аналізувати та впроваджувати сертифікати та аутентифікаційні механізми, які знижують ризики несанкціонованого доступу і підробки даних.
- Перевіряти ефективність захисту за допомогою тестування на вразливості і симуляції атак, щоб виявити можливі слабкі місця у системі захисту.

Висновки та рекомендації

На основі проведених розрахунків та оцінок:

1. Підтвердження коректності мережевих рішень забезпечується через проведення комплексних тестувань та оцінки результатів з точки зору ефективності захисту і надійності.
2. Розрахунки підтверджують правильність вибору механізмів захисту: застосування шифрування, впровадження сучасних протоколів безпеки та надійних засобів захисту.
3. Оцінка результатів дозволяє зробити висновки про необхідність додаткових заходів або удосконалення існуючих рішень для підвищення загального рівня безпеки.

Рекомендації щодо покращення захисту включають:

- Регулярне оновлення програмного забезпечення та апаратних засобів для забезпечення їх відповідності актуальним стандартам безпеки.
- Впровадження додаткових механізмів захисту, таких як багатофакторна аутентифікація та системи виявлення аномальної поведінки.
- Проведення регулярних аудитів безпеки для виявлення і усунення потенційних слабких місць у мережевих рішеннях та системах захисту.

Така всебічна перевірка та підтвердження коректності побудови захищеної комп'ютерної мережі дозволяє забезпечити високий рівень захисту інформації, мінімізуючи ризики і підвищуючи надійність мережевих рішень.

В анотації у реферативному стилі наводиться інформація про зміст та результати, що отримані в курсової роботі. Як розділ анотація не нумерується.

Зміст курсової роботи може займати 1–1,5 сторінки. В ньому записуються назви всіх розділів і підрозділів (параграфів) із зазначенням початкових сторінок. Назви розділів і підрозділів мають бути стислими і зрозумілими, літературно грамотними, тісно пов'язаними з назвою роботи, але не повторювати її. Усі назви повинні бути записані так само як вони сформульовані в КР. Визначення сторінок обов'язкове. Зміст характеризує структуру КР. Як розділ зміст не нумерується.

У вступі студент повинен висвітлити стан питання, яке розглядається, обґрунтовувати необхідність і можливість його вирішення, описати зв'язок з виробничими задачами, а також обґрунтувати актуальність теми роботи та сформулювати основну мету. Вступ має бути коротким (1-2 сторінки) і чітким. Його не слід перевантажувати загальними фразами. Головне, щоб було зрозуміло, чому присвячена робота, які завдання автор поставив сам для себе. Вступ як розділ не нумерується.

В процесі розробки комп'ютерної мережі повинні бути:

- ❖ **Розробка структура (топологія) захищеної комп'ютерної мережі.**
  - ✓ Включає планування мережі з урахуванням захисту інформаційних потоків, таких як ізоляція критично важливих сегментів мережі, використання VLAN для підвищення безпеки, DMZ-зон, а також інтеграція міжмережних екранів і систем виявлення вторгнень (IDS) та інших методів для підвищення безпеки мережі.
- ❖ **Вибір кабельної системи з врахуванням захисту інформації.**
  - ✓ Включає вибір екранованих кабелів (STP), оптоволокна та забезпечення фізичної безпеки комунікаційних каналів для захисту від несанкціонованого перехоплення інформації та зниження впливу електромагнітних перешкод.
- ❖ **Вибір необхідного комунікаційного обладнання і комутаційних елементів. (роз'єми, коннектори, кросові панелі і шафи, антено-фідерний тракт) з врахуванням засобів захисту інформації.**
  - ✓ Включає підбір обладнання з вбудованими засобами захисту, такими як маршрутизатори з функціями шифрування, брандмауери, захищені коннектори, а також додаткові механізми фізичного захисту.

- **Розробка системи захисту інформації в комп'ютерній мережі.**
  - ✓ Включає впровадження політик безпеки, багаторівневої системи захисту, що передбачає використання міжмережних екранів, систем виявлення та запобігання вторгнень (IDS/IPS), шифрування даних на рівні канального та транспортного протоколів, а також засобів контролю доступу та аутентифікації користувачів, а також впровадження засобів моніторингу та управління доступом і регулярні аудити безпеки.

Курсова робота повинна містити графічну частину і записку пояснення.

Графічна частина

Схеми повинен відповідати структурі (топології) комп'ютерної мережі з планом поверхів будівлі з нанесеним на них маршрутом проходження кабелів комп'ютерної мережі по кожному поверху (вертикальне та горизонтальне з'єднання) та схеми антено-фідерних трактів.

На кожній приведеній схемі повинно бути показано розміщення комп'ютерів, комунікаційного і іншого необхідного обладнання вибраного студентом самостійно.

Кожна схема виконується на окремому листі формату А4.

У першому розділі (3-4 сторінки) ПЗ необхідно провести детальний огляд та аналіз предметної області, що охоплює сучасні мережеві технології та методи забезпечення безпеки комп'ютерних систем та мереж. Здобувач має описати існуючі загрози і вразливості, що можуть вплинути на захист інформації, і дослідити актуальні рішення для їх усунення. Важливо визначити основні завдання, які потрібно вирішити в курсовій роботі, з особливим акцентом на аспекти безпеки інформації в мережах. На основі проведеного аналізу слід сформулювати технічне завдання, яке включає цілі проєкту, вимоги до безпеки.

У другому розділі (4-5 сторінок) потрібно створити структурну схему комп'ютерної мережі, яка включає опис топології мережі та методи її сегментації, такі як використання VLAN, DMZ-зон і інших технік для підвищення безпеки. Здобувач повинен обґрунтувати вибір топології мережі, пояснюючи, як її елементи сприяють підвищенню рівня захисту. Важливо також спланувати топологію мережі, враховуючи кількість підключених робочих станцій, підмережі та інші елементи, що забезпечують ефективність і безпеку роботи мережі.

У третьому розділі здобувач має вказати вибрану кабельну систему, зокрема типи кабелів, такі як екрановані виті пари (STP) або оптоволокно, і їх характеристики. Важливо обґрунтувати вибір кабелів з точки зору захисту від перехоплення даних і фізичного захисту кабельних трас. Окрім того, слід описати вибране комунікаційне обладнання, включаючи маршрутизатори, комутатори, роз'єми, конектори і кросові панелі, з акцентом на їх захисні властивості. У розділі також наводяться відомості про робочі станції, сервери та фізичне середовище, яке використовується при моделюванні. Здобувач має

надати теоретичні відомості про мережеві протоколи і стандарти, що використовуються у мережі, описати їх особливості та вплив на безпеку.

У четвертому розділі необхідно розробити багаторівневу систему захисту інформації. Здобувач має впровадити міжмережні екрани (брандмауери), що контролюють вхідний і вихідний трафік, та налаштувати системи виявлення та запобігання вторгненням (IDS/IPS) для моніторингу і реагування на потенційні загрози. Окрім того, потрібно реалізувати шифрування даних на рівні канального та транспортного протоколів, описати методи і технології шифрування, а також розробити систему контролю доступу, що включає аутентифікацію користувачів і управління привілеями, включаючи багатофакторну аутентифікацію для підвищення безпеки. Здобувач також має налаштувати системи моніторингу і управління безпекою для забезпечення постійного нагляду за станом мережі і реагування на інциденти. Нарешті, слід підготувати документацію, що детально описує всі аспекти захисту інформації, включаючи процедури, конфігурації і політики безпеки, а також оформити звітність про впроваджені заходи безпеки, результати тестування і оцінки ефективності системи захисту.

У висновках (1-2 сторінки) формулюються основні результати, які отримані під час виконання курсової роботи. В реферативній формі повинні бути описані результати, отримані студентом на кожному з етапів виконання роботи, а також висновків щодо досягнення мети курсової роботи, перспективи розвитку даної галузі тощо. Як розділ не нумерується. Робота включала кілька ключових етапів, кожен з яких був спрямований на досягнення високого рівня захисту інформації в комп'ютерних системах та мережах.

По-перше, у розділі про розробку структури та топології мережі було проведено детальний аналіз і планування архітектури мережі з урахуванням захисту інформаційних потоків. Це включало реалізацію сегментації мережі через VLAN, створення DMZ-зон для забезпечення додаткового рівня безпеки, а також інтеграцію міжмережних екранів і систем виявлення вторгнень (IDS). В результаті, було створено надійну структуру, що забезпечує захист критично важливої інформації від несанкціонованого доступу та атака ззовні.

По-друге, у розділі вибору кабельної системи акцент було зроблено на використанні екранованих кабелів (STP) та оптоволокна, що забезпечує високий рівень фізичної безпеки комунікаційних каналів. Це дозволяє захистити інформацію від несанкціонованого перехоплення і зменшити вплив електромагнітних перешкод. Вибір та обґрунтування використовуваних матеріалів і технологій забезпечують фізичну стійкість мережі до різних загроз.

По-третє, у розділі про вибір комунікаційного обладнання та комутаційних елементів було підібрано обладнання з вбудованими засобами захисту, такими як маршрутизатори з функціями шифрування, брандмауери та захищені коннектори. Це забезпечує додатковий рівень захисту інформації,

гарантуючи безпеку даних на всіх рівнях комунікаційної інфраструктури. Забезпечення фізичного захисту також стало важливою частиною цієї роботи.

Нарешті, у розділі розробки системи захисту інформації було впроваджено політики безпеки, багаторівневу систему захисту, включаючи міжмережні екрани, системи виявлення та запобігання вторгнень (IDS/IPS), а також шифрування даних на рівні канального та транспортного протоколів. Впровадження засобів контролю доступу та аутентифікації користувачів, а також регулярний моніторинг і аудит безпеки, забезпечують цілісний захист інформаційної інфраструктури транспортного підприємства.

В результаті проведеної роботи вдалося досягти поставлених цілей щодо розробки захищеної комп'ютерної мережі, що підвищує ефективність управлінських і логістичних процесів підприємства. Визначено ключові аспекти для покращення безпеки в умовах постійного розвитку кіберзагроз. Перспективи розвитку цієї галузі включають інтеграцію новітніх технологій захисту інформації, що дозволить забезпечити ще вищий рівень безпеки мережевих систем у майбутньому.

У Списку використаних джерел наводиться перелік джерел, на які були посилання в тексті. Список повинен формуватися в порядку посилань за текстом і вміщувати бібліографічні відомості офіційно виданих книжок, статей, патентів, депонованих рукописів тощо. Як розділ перелік літератури не нумерується. Формат опису літературних джерел повинен відповідати ГОСТ 7.1.−84.

У *додатки* включають логічні схеми, а також інші документи. Крім цього, в додатки помішуються таблиці, графіки та методики, які з якихось причин не увійшли до пояснювальної записки, але потрібні для пояснень. Як розділ додатки не нумеруються, але кожен з додатків нумерується великими літерами алфавіту згідно ДСТУ 3008-95, оскільки до додатків помішуються документи, що мають самостійну нумерацію сторінок, то різна нумерація (спільна для всієї пояснювальної записки) зберігається.

3. ЗАВДАННЯ НА КУРСОВУ РОБОТУ

3.1. Теоретичні відомості. Вибір розміру мережі і її структури

Будь-яке проєктування, як відомо, є сильно спрощеним моделюванням дійсності, що ще не настала. Саме тому передбачити усі можливі чинники, врахувати усі споживи, які можуть виникнути в майбутньому, практично неможливо.

Проте найзагальніші підходи до проєктування локальних комп'ютерних ятерів все-таки можуть бути сформульовані, деякі корисні принципи такого проєктування можуть бути запропоновані і з успіхом використані.

При створенні нової мережі для якого-небудь підприємства необхідно враховувати наступні чинники :

- необхідний розмір мережі (у найближчому майбутньому і за прогнозом на перспективу);
- необхідна структура, ієрархія і основні частини мережі (по підрозділах підприємства, а також по кімнатах, поверхах і будівлях підприємства);
- основні напрями і інтенсивність інформаційних потоків (у найближчому майбутньому і в далекій перспективі);
- технічні характеристики устаткування (комп'ютерів, адаптерів, кабелів, повторювачів, концентраторів, комутаторів) і його вартість;
- можливості прокладення кабельної системи в приміщеннях і між ними, а також заходь забезпечення цілісності кабелю;
- забезпечення обслуговування мережі і контролю за її безвідмовністю і безпекою;
- вимоги до програмних засобів за допустимим розміром мережі, швидкості, гнучкості, розмежуванням прав доступу, вартості, можливостям контролю за обміном інформацією, і т.п;
- необхідність підключення до глобальних ятерів або до інших локальних ятерів.

Цілком можливо, що після вивчення усіх перерахованих і не перерахованих чинників з'ясується, що цілком можна обійтися взагалі без мережі, уникнувши тим самим досить великих витрат на апаратуру і програмне забезпечення, на установку і експлуатацію мережі, на зарплату обслуговуючому персоналу, на підтримку і ремонт і т.п. Наприклад, якщо є всього декілька користувачів, які працюють на своїх комп'ютерах автономно і тільки іноді обмінюються файлами, то мережу цілком може замінити звичайний матеріальний носій (це і дешевше, і набагато менш проблематично).

Мережа породжує безліч додаткових проблем в порівнянні з автономними комп'ютерами: від простих механічних (комп'ютери, підключені до мережі, складніше переносити з місця на місце) до складних інформаційних (необхідність контролювати спільно використовувані ресурси, запобігати зараженню мережі вірусами). До того ж користувачі мережі вже не так незалежні, як користувачі автономних комп'ютерів, їм потрібно дотримуватися певних правил, підкорятися встановленим вимогам, яким їх необхідно навчити.

Нарешті, мережа гостро ставить питання про безпеку інформації, захисту від несанкціонованого доступу, адже з будь-якого комп'ютера мережі можна рахувати дані із загальних мережевих дисків. Захистити один комп'ютер або навіть декілька поодиноких комп'ютерів у будь-якому випадку набагато простіше, ніж цілу мережу. Тому приступати до установки мережі доцільно тільки тоді, коли без мережі робота стає просто неможливою, непродуктивною, коли відсутність зв'язку між комп'ютеррами гальмує роботу і стримує розвиток справи.

Першим етапом проєктування мережі повинен стати аналіз існуючої ситуації і завдань, які вирішуватиме мережа. Має бути визначений (хоч би приблизно) розмір мережі і її структура.

Під ***розміром мережі*** в даному випадку розуміється як кількість об'єднуваних в мережу комп'ютерів, так і відстані між ними. Потрібно чітко уявляти собі, скільки комп'ютерів (мінімально і максимально) потребує підключення до мережі. У будь-якому випадку потрібно залишати можливість для подальшого росту кількості комп'ютерів в мережі, хоч би відсотків на 20-50. До речі, зовсім не обов'язково раз і назавжди включати в мережу усі комп'ютери підприємства. Можливо, має сенс залишити деякі з них автономними, наприклад, з міркувань безпеки інформації на їх дисках. Кількість підключених до мережі комп'ютерів сильно впливає як на її продуктивність, так і на складність її обслуговування. Воно також визначає вартість необхідних програмних засобів. Тому помилки в даному випадку можуть мати досить серйозні наслідки.

Необхідна довжина ліній зв'язку мережі грає не меншу, а іноді і велику роль в проєктуванні мережі, чим кількість комп'ютерів. Наприклад, якщо відстані дуже великі, може знадобитися використання дуже дорогого або рідкісного устаткування. До того ж зі збільшенням відстані різко зростає значущість захисту ліній зв'язку від зовнішніх електромагнітних завад. Від відстані залежить і швидкість передачі інформації по мережі. Доцільно при виборі відстаней закладати невеликий запас (хоч би відсотків 10) для різних непередбачених обставин. До речі, здолати обмеження по довжині, іноді, можна шляхом вибору структури мережі, розбиття її на окремі частини.

Під ***структурою мережі*** розуміється спосіб розділення мережі на частини (сегменти), а також спосіб з'єднання цих сегментів між собою. Мережа підприємства може включати робочі групи комп'ютерів, мережі підрозділів, опорні мережі, засоби зв'язку з іншими мережами. Для об'єднання частин мережі можуть використовуватися повторювачі, концентратори, комутатори, мости і маршрутизатори. Причому у ряді випадків вартість цього об'єднувального устаткування може навіть перевищити вартість комп'ютерів, мережевих адаптерів і кабелю. Тому вибір структури мережі виключно важливий.

У ідеалі структура мережі повинна відповідати структурі будівлі або комплексу будівель підприємства. Робочі місця групи співробітників, що займаються одним завданням (наприклад, бухгалтерія, відділ продажів, інженерна група) повинні розташовуватися в одній кімнаті або в поруч розташованих кімнатах. Тоді можна усі комп'ютери цих співробітників об'єднати в один сегмент, в одну робочу групу і встановити поблизу їх кімнат сервер, з яким вони працюватимуть, а також концентратор або комутатор, що зв'язує їх комп'ютери. Так само робочі місця співробітників підрозділу, близьких завдань, що займаються комплексом, краще розташувати на одному поверсі будівлі, що істотно спростить їх об'єднання в єдиний сегмент і

подальше адміністрування цього сегменту. На цьому ж поверсі зручно розташувати комутатори, маршрутизатори і сервери, з якими працює цей підрозділ.

Як і в інших випадках, при виборі структури доцільно залишати можливості для подальшого розвитку мережі. Наприклад, краще придбавати комутатори або маршрутизатори з кількістю портів, дещо великою необхідного зараз (хоч би на 10-20 відсотків). Це дозволить при необхідності легко включити в мережу новий сегмент або декілька сегментів. Адже будь-яке підприємство завжди прагне до росту, і цей ріст не повинен призводити до необхідності проєктувати мережу підприємства наново.

Під ***захистом інформації в комп'ютерних системах та мережах*** розуміється комплекс заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності даних. Ці заходи включають використання апаратних і програмних засобів, організаційних політик та процедур, що мають на меті запобігання несанкціонованому доступу, знищенню, зміні або витоку інформації. Основними аспектами захисту є забезпечення фізичної безпеки обладнання, захист від вірусів і зловмисного програмного забезпечення, шифрування даних, управління доступом і автентифікація користувачів, а також впровадження систем виявлення і запобігання вторгненням. Важливими елементами є також моніторинг безпеки, аудит системи, навчання користувачів та розробка планів реагування на інциденти.

Апаратні засоби захисту інформації включають фізичні пристрої та обладнання, які сприяють забезпеченню безпеки інформаційних систем. До них відносяться:

- ✓ ***Мережеві екрани (файрволи*)** — пристрої, які контролюють вхідний і вихідний трафік у мережі на основі визначених правил безпеки, блокуючи несанкціоновані спроби доступу.
- ✓ ***Системи виявлення і запобігання вторгненням (IDS/IPS)*** — апаратні та програмні системи, що моніторять мережевий трафік і системні події, виявляючи та запобігаючи підозрілим або шкідливим активностям.
- ✓ ***Шифратори (апаратні криптографічні пристрої)*** — спеціалізовані пристрої для забезпечення криптографічного захисту даних на рівні апаратного забезпечення.
- ✓ ***Безпечні сервери та пристрої збереження даних*** — обладнання, яке забезпечує фізичний захист даних, таких як сервери з високим рівнем захисту, системи резервного копіювання з шифруванням даних.
- ✓ ***Біометричні системи доступу*** — пристрої, що використовують фізичні характеристики, такі як відбитки пальців або розпізнавання обличчя, для ідентифікації та автентифікації користувачів.

Програмні засоби захисту інформації включають програмне забезпечення, яке реалізує політики безпеки і забезпечує захист даних:

- ✓ ***Антивірусне програмне забезпечення*** — програми, які виявляють,

знешкоджують та видаляють віруси і шкідливе програмне забезпечення.

- ✓ ***Антишпигунське програмне забезпечення*** — програми, які захищають систему від шпигунських програм, що збирають особисті дані без відома користувача.
- ✓ ***Програми для шифрування даних*** — програмні рішення для забезпечення конфіденційності даних, які перетворюють інформацію в нечитабельний формат для неавторизованих осіб.
- ✓ ***Системи управління доступом (IAM)*** — програмне забезпечення для управління правами доступу та автентифікацією користувачів, включаючи багатофакторну автентифікацію (MFA).

Організаційні політики та процедури включають правила і практики, що визначають, як повинна бути забезпечена безпека інформації:

- ✓ ***Політика безпеки інформації*** — документ, що визначає загальні принципи та правила, які організація повинна дотримуватися для захисту інформації. Включає політики доступу, управління ризиками та відповідальності за безпеку.
- ✓ ***Процедури управління інцидентами*** — визначають, як організація повинна реагувати на інциденти безпеки, включаючи процеси виявлення, аналізу, реагування та відновлення після атак або порушень безпеки.
- ✓ ***Процедури резервного копіювання і відновлення даних*** — правила, що визначають, як часто потрібно створювати резервні копії даних, де їх зберігати та як відновлювати інформацію у разі її втрати або пошкодження.
- ✓ ***Навчання користувачів*** — програми навчання та підвищення обізнаності для співробітників про загрози безпеці, найкращі практики щодо захисту інформації та їх роль у забезпеченні безпеки організації.

Фізична безпека обладнання передбачає захист фізичних ресурсів інформаційної системи:

- ✓ ***Охорона приміщень*** — використання фізичних бар'єрів, таких як двері, замки, системи контролю доступу для обмеження фізичного доступу до серверних кімнат та інших критичних зон.
- ✓ ***Системи відеоспостереження*** — камери та монітори для моніторингу та запису активності у важливих зонах, що допомагає забезпечити фізичну безпеку обладнання.
- ✓ ***Антивандальні пристрої*** — захисні конструкції, такі як кейси для серверів, що забезпечують захист від фізичних атак або вандалізму.

Захист від вірусів і зловмисного програмного забезпечення включає впровадження технічних та організаційних заходів для захисту систем від атак:

- ✓ ***Регулярне оновлення антивірусного програмного забезпечення*** — забезпечення актуальності бази даних вірусів та патчів для запобігання новим загрозам.
- ✓ ***Впровадження політик безпечного використання мережі*** — включає

обмеження доступу до підозрілих веб-сайтів та небезпечних вкладок електронної пошти.

Шифрування даних забезпечує конфіденційність даних як під час їх зберігання, так і під час передачі:

- ✓ ***Шифрування на рівні файлів та дисків*** — перетворення даних на дисках у незрозумілий формат, що забезпечує захист даних при фізичному доступі до носіїв інформації.
- ✓ ***Шифрування передачі даних*** — використання протоколів, таких як TLS/SSL для захисту даних, що передаються по мережі.

Управління доступом і автентифікація користувачів включає технології та практики, що забезпечують контроль над доступом до інформаційних систем:

- ✓ ***Системи контролю доступу*** — механізми, які регулюють, які користувачі мають доступ до яких ресурсів у системі, включаючи права читання, запису і виконання.
- ✓ ***Багатофакторна автентифікація (MFA)*** — технології, які вимагають від користувачів надання більше одного підтвердження особи перед доступом до системи.

Впровадження систем виявлення і запобігання вторгненням (IDS/IPS) забезпечує моніторинг і захист мережевої інфраструктури:

- ✓ ***Системи виявлення вторгнень (IDS)*** — системи, які моніторять мережевий трафік і системні події для виявлення підозрілої або небезпечної активності.
- ✓ ***Системи запобігання вторгненням (IPS)*** — активні системи, які не лише виявляють, але і автоматично блокують або зменшують загрози у реальному часі.

3.2. Огляд і аналіз існуючих комп'ютерних мереж

На сьогоднішній день існує безліч мережевих технологій передачі даних. Сфери застосування цих технологій різні. Починаючи від малих локальних обчислювальних мереж закінчуючи загальноміськими і глобальними світовими мережами.

Існують наступні основні сучасні стандарти локальних мереж:

- **Ethernet;**
- **Fast Ethernet, Gigabit Ethernet, 100VG-AnyLAN;**
- **WI-FI (Wireless Fidetly);**
- **WIMAX (Worldwide Interoperability for Microwave Access).**

3.3. Технологія Ethernet

Ветераном мережевих технологій (архітектури) є **Ethernet** – ця специфікація була запропонована фірмами DEC, Intel і Xerox в 1980 році і дещо пізніше на її основі з'явився стандарт IEEE 802.3. По перших буквах назв їх фірм утворено скорочення DIX, що фігурує в описах цієї технології. Слово Ether (ефір) в назві технології позначає різноманіття можливих середовищ передачі.

Перші версії – Ethernet v1.0 і Ethernet v2.0 призначалися тільки для коаксіального кабелю, стандарт IEEE 802.3 розглядає і інші варіанти середовища передачі ─ виту пару і оптоволокно. Зараз під назвою Ethernet мають на увазі стандарт IEEE 802.3 (швидкість 10 Мбіт/с). В 1995 році був ухвалений стандарт IEEE 802.3u ─ Fast Ethernet із швидкістю 100 Мбіт/с, а в 1997 року IEEE 802.3z ─ Gigabit Ethernet (1000 Мбіт/с). Восени 1999 року ухвалений стандарт IEEE 802.3a/b ─ Gigabit Ethernet на витій парі категорії 5, пізніше була анонсований 10GBit Ethernet (10000 Мбіт/с). Популярні різновиди Ethernet позначаються як 100BaseTX і ін. Тут перший елемент позначає швидкість передачі, Мбіт/с.

Другий елемент: Base ─ пряма (не модульована) передача, Broad ─ використання широкосмугового кабелю з частотним ущільненням каналів.

Третій елемент: середовище передачі (T, TX, T2, T4 - виті пари, FX, FL, FB, SX і IX ─ оптоволокно).

Технологія Ethernet заснована на методі множинного доступу до середовища передачі з прослуховуванням несучій і виявленням колізій ─ CSMA/CD. Суть цього методу стосовно «класичної» версії Ethernet (10 Мбіт/с на коаксіальному кабелі).

3.4. Технологія Fast Ethernet 100 Мбіт/с

Варіанти Fast Ethernet із швидкістю передачі даних 100 Мбіт/с описуються стандартом IEEE 802.3u ─ додатковими розділами 802.3, ухваленими в 1995 року. Вони засновані на тому ж методі доступу CSMA/CD із збереженням форматів кадрів. При цьому всі співвідношення, зміряні в бітових інтервалах, зберігаються. Оскільки тривалість бітового інтервалу скоротилася в 10 раз, максимально допустимий час проходження між двома вузлами скоротився до 2,6 мкс, що навело до посилювання топологічних обмежень. Всі різновиди використовують зіркоподібну топологію з активним пристроєм в центрі, можливе і безпосереднє з'єднання пари станцій.

Стандарт 802.3u спирається на ті ж рівні MAC і LLC, які були визначені в початковому 802.3, зміни торкаються фізичного рівня. Фізичний рівень є тришаровим:

- *Reconciliation sublayer* ─ рівень узгодження з MAC-рівнем 802.3, орієнтованим на AUI-інтерфейс;
- *MII (Media Independent Interface*) ─ електричний інтерфейс, незалежний від середовища передачі. Представляє собою специфікацію сигналів TTL-рівня, використовує 40-контактний штирьовий роз'єм. По ідеї він нагадує інтерфейс AUI, але розташовується на іншому рівні. Довжина кабелю MII не повинна перевищувати 0,5 м. Наявність доступного інтерфейсу MII не є обов'язковим;
- *PHY (Physical layer device)* ─ пристрій фізичного рівня, прив'язаний до конкретного середовища передачі (100BaseTX, 100BaseFX або 100BaseT4).

Пристрій фізичного рівня виконує логічне кодування ─ перетворення 4B/5B або 6B/8T, фізичне кодування і приєднання до середовища передачі, і необов'язково ─ автоматичне узгодження режимів передачі. Фізичний рівень в 100BaseTX і 100BaseFX позичений з технології FDDI, в 100BaseT4 застосована оригінальна розробка.

100BaseTX ─ найпопулярніша версія Fast Ethernet, що використовує дві виті пари категорії 5. По використанню роз'ємів повністю відповідає 10BaseT. Можлива робота в напівдуплексному і повнодуплексному режимах. Логічне кодування проводиться по схемі 4B/5B ─ 4 біта початкової інформації перетворяться в 5-бітний символ. Надмірність використовується для підвищення достовірності і службових цілей. Метод фізичного кодування MLT-3 запозичений з TP-PMD ─ реалізації FDDI. В паузі між кадрами в лінію посилається послідовності символів Idle.

100BaseT4 ─ версія, що використовує 4 виті пари категорії не нижче 3. Окрім одно-направлених пар, використовуваних в 100BaseTX, тут дві додаткові пари є двонаправленими і служать для розпаралелювання передачі даних. Кадр передається по трьох лініях паралельно, що дозволяє понизити пропускну спроможність кожної пари до 33,3 Мбіт/с. Кожні 8 біт (двійкових розрядів ─ Binary), передаванні по конкретній парі, кодуються шістьма трійковими (Ternary) цифрами (кодування 8B/6T). В результаті при бітовій швидкості 33,3 Мбіт/с швидкість зміни сигналів в лінії складає 25 Мбод (33,3x6/8=25). Ці заходи дозволяють звузити необхідну смугу пропускання кабелю до вимог категорії 3 (16 МГЦ). Четверта пара використовується при передачі для прослуховування сигналу від протилежного передавача ─ по його появі визначається факт колізії. Для підключення кінцевих вузлів до портів активного устаткування використовується кабель, для безпосереднього з'єднання кінцевих вузлів або з'єднання двох комунікаційних пристроїв застосовують «перехресний» кабель.

Для наведених вище реалізацій передбачений протокол узгодження режимів (autonegotiation), по якому порт може вибрати найефективніший з режимів, доступних обом учасникам обміну. Узгодження здійснюється шляхом обміну посилками FLP (Fast Link Pulse), які є ознакою справної активної лінії (аналогічно NLP 10BaseT). На відміну від одиночних імпульсів NLP, імпульси FLP йдуть пачкою. Розрізняють синхронізуючі і сигнальні імпульси FLP. Сигнальні імпульси можуть вставлятися між синхронізуючими, йдуть пачкою по 17 штук. Місця між цими імпульсами відводяться під кодування 16-бітного слова: наявність сигнального відповідає одиничному біту, відсутність ─ нульовому. Перший вузол пропонує найефективніший режим, кодуючи його в посилці FLP. Приймач на цю посилку відповідає аналогічно. В якості робітника вибирається найприоритетніший з доступних обом вузлам. Пріоритети режимів в порядку убування: 100BaseTX повнодуплексний, 100BaseT4, 100BaseTX напівдуплексний, 10BaseT повнодуплексний, 10BaseT напівдуплексний. Якщо другий вузол має порт 10BaseT «не розуміючий» FLP і посилаючий NLP, буде ухвалений протокол

10BaseT. Протокол автоматичного узгодження може бути відключений (або не реалізований), в цьому випадку режим роботи задається примусово при конфігуруванні порту. Можливість перемикання режимів відображається в назвах портів (Fast Ethernet 10/100), підтримка режиму 100BaseT4 зустрічається нечасто.

100BaseT2 ─ мало поширена (і не стандартизована) версія з використанням двох пар категорії 3 і вище. Звуження смуги досягається за рахунок застосування кодування 5-рівня PAM-5. Підтримує напів- і повний дуплекс, в режимі повного дуплексу сигнали розповсюджуються по кожній парі в зустрічних напрямах (пропускна спроможність 100 Мбіт/с відноситься тільки до повного дуплексу, швидкість передачі в одну сторону ─ 50 Мбіт/с).

100BaseFX ─ версія для оптоволокна з довжиною хвилі 1300 нм. Логічно близька до 100BaseTX ─ те ж логічне кодування 4B/5B, але фізичне ─ NRZI (як в FDDI). В напівдуплексі дальність 412 м ─ обмеження за часом подвійного обороту. В повному дуплексі дальність визначається властивістю волокна: по MM-волокну може досягати 2 км, по SM ─ 32 км.

100BaseSX ─ стандарт на дешевих короткохвильових (830 нм) світлодіодних передавачах і багатомодовому волокні. Дальність зв'язку обмежена волокном і менше, ніж у FX, ─ всього 300 м, зате підтримується сумісність з 10BaseFL і автоматичне узгодження швидкості передачі 10/100 Мбіт/с (802.3u). Версія розроблена як дешева альтернатива дорогій 100BaseFX у випадках, коли не вимагається подолання великих відстаней.

Центральним пристроєм в Fast Ethernet може бути повторювач або комутатор. Повторювачі діляться на два класи:

- *Повторювач класу I* є транслюючим, він підтримує різні схеми кодування, ухвалені в технологіях 100BaseTX/FX і 100BaseT4.
- *Повторювач класу II* є прозорим (transparent repeater), він підтримує тільки одну з схем кодування ─ технологію 100BaseTX/FX або 100BaseT4.

Завдяки надмірності кодування в порівнянні з Ethernet повторювачі Fast Ethernet працюють дещо складніше. У разі виявлення помилкового сигналу замість його прозорої трансляції в інші порти повторювач може посилати ознаку пошкодження кадру. Якщо повторювач підтримує дві схеми кодування, йому доводиться проводити декодування по схемі 4B/5B і подальше кодування в 6B/8T (або навпаки), що вносить додаткову затримку.

Топологічні обмеження Fast Ethernet жорсткіші ─ діаметр домена колізій для витої пари не повинен перевищувати 205 м, в одному домені колізій може бути не більше двох повторювачів класу II, повторювач класу I може бути тільки один. Якщо прийняти допустиму відстань від повторювача до станції рівним 100 м, то їх можна сполучати між собою кабелем довжиною не більше 5 м.

3.5. Технологія Gigabit Ethernet 1000 Мбіт/с

Технологія Gigabit Ethernet із швидкістю передачі даних 1000 Мбіт/с розроблена для прискорення передачі даних при використанні найпопулярнішої технології (Ethernet). Проте підвищення швидкості на порядок при збереженні всіх пропорцій попередніх технологій навело б до звуження діаметра домена колізій до неприйнятного розміру ─ 0,26 мкс затримки відповідає приблизно 50 м кабелю, а ще затримку вносить і повторювач. З цієї причини мінімально допустимий розмір кадру, визначаючий максимально допустиму затримку передачі, був збільшений до 512 байт (4096 bit). З урахуванням затримок в повторювачі і адаптерах діаметр домена колізій може досягати 200 м, тобто вписуватися в стандартну концепцію побудови. Обмеження, породжені методом CSMA/CD, актуальні тільки для напівдуплексного режиму роботи портів. Для Gigabit Ethernet більш характерний повнодуплексний режим, при якому допустима довжина лінії зв'язку обмежується загасанням сигналу і частотними властивостями лінії.

Додатково передбачається можливість пакетної передачі кадрів (frame bursting). Вузол, що отримав доступ до середовища, після передачі одного кадру замість паузи посилає спеціальну послідовність, після якої йде наступний кадр. Кадри пакету можуть адресуватися різним одержувачам. Значення пакетної передачі полягає в скороченні невигідних витрат на отримання доступу до середовища ─ між кадрами пакету середовище для інших вузлів виглядає зайнятий.

Gigabit Ethernet описується двома стандартами ─ IEEE 802.3z (1000BaseSX, 1000BaseLX і 1000BaseCX), ухваленим в 1998 року, і IEEE 802.3ab (1000BaseT), ухваленим восени 1999 р.

Стандарт 802.3z ґрунтується на напрацюваннях технології Fiber Channel. Тут використовується надмірне кодування 8B/10B, а схеми фізичного рівня розігнані з швидкості 800 Мбіт/с до 1 Гбіт/с (тактова частота ─1,25 ГГЦ). Стандарт пропонує наступні версії:

1000BaseSX (Short wavelength) ─ оптичний інтерфейс з короткохвильовими (850 нм) лазерними передавачами для зв'язку по MM-волокну на невеликі відстані. Для кабелю з невисокою смугою пропускання допустима довжина з'єднання виявляється менше, ніж обмеження на довжину магістрального кабелю 500 м, встановлене стандартами СКС.

1000BaseLX (Long wavelength) ─ інтерфейс з довгохвильовими (1310 м) лазерними передавачами для зв'язку по SM і MM-волокну на великі відстані.

1000BaseLH ─ інтерфейс з лазерними передавачами 1310 нм для зв'язку по SM і MM-волокну на надвеликі відстані, поки в стандарт IEEE не входить.

1000BaseCX ─ електричний інтерфейс для зв'язку на короткій дистанції (25 м), призначений для зв'язку устаткування в межах апаратної кімнати або телекомунікаційного приміщення. Використовує двохосьовий (twinaxial) кабель або скручені четвірки дротів (quad cable) з частотними характеристиками, перевершуючими STP типів 1 і 2. Як коннекторів поки пропонується DB-9 (використовуваний для STP в Token Ring), розробляється новий тип коннектора HSSDC (HIGH-SPEED Serial Data Connector).

1000BaseT ─ електричний інтерфейс на витій парі (4 пар дротів) категорії 5е (і навіть 5) при обмеженні на довжину лінії в 100 м. Фізичне кодування ─ 5-рівень. Сигнал передається одночасно по чотирьох парах дротів, причому для повного дуплексу передача ведеться по кожній парі відразу в обох напрямах. Кінцеві ланцюги виділяють з суміші сигнал протилежного передавача. Рішення цієї задачі на надвисоких частотах стало можливим завдяки застосуванню сучасних сигнальних процесорів. Для задоволення вимогам до середовища передачі рекомендується застосування в кабельній системі компонентів категорії 5е (розетки, шнури, 4-парні кабелі стаціонарної проводки). Кількість з'єднань в каналі повинна бути мінімальною. В телекомунікаційних приміщеннях рекомендується схема безпосереднього підключення, без крос-панелі. В горизонтальній кабельній системі виключається з'єднання двох шматків кабелів в одній лінії в точці переходу.

3.6. Технологія 100VG-AnyLAN

100VG-AnyLAN ─ технологія із швидкістю передачі 100 Мбіт/с по 4-парному кабелю категорії 3. VG означає VOICE-GRADE TP ─ вита пара для голосової телефонії, закінчення «Any LAN» означає можливість роботи з «любими ЛОМ» (Ethernet і Token Ring). Розроблена фірмами HEWLETT-PACKARD і AT&T Microelectronics як розвиток Ethernet, описується стандартом IEEE 802.12. Фізична і логічна топологія ─ дерево, побудована на хабах. Метод доступу ─ Demand Priority (пріоритет запитів), управління доступом до середовища передачі реалізовується апаратурою хабів. Цим 100VG принципово відрізняється від інших технологій, в яких функції управління доступом розподілені по вузлах мережі.

Використовувати кабель з гарантованою смугою частот 16 МГЦ дозволяє одночасна передача сигналів в одну сторону по всіх чотирьох парах (quartet signaling), внаслідок чого кожна пара пропускає усього 25 Мбіт/с. Проте при цьому повний дуплекс неможливий. Інформація логічно кодується по схемі 5B/6B, після чого фізично ─ по NRZ («1» ─ високий рівень «0» ─ низький). Бітова швидкість в кожній парі дротів ─ 30 Мбіт/с.

Центральним елементом в управлінні доступом є хаб. Кожний хаб має один порт для каскадування (uplink або cascade port) і декілька регулярних (звичайних) портів, до яких підключаються кінцеві вузли або проміжні хаби (каскадними портами). Без хабів побудова мережі неможлива навіть для з'єднання двох вузлів. Мережа може містити безліч хабів, побудованих в деревовидній структурі. В мережі є один кореневий хаб (root hub), він може бути і єдиним. Під ним можуть знаходитися проміжні хаби (до яких підключаються хаби наступних рівнів)до яких підключаються тільки кінцеві вузли. Припускається ієрархічне каскадування до п'яти рівнів хабів.

Топологічні обмеження прості: довжина будь-якої лінії (між хабом і вузлом або між двома хабами) не більше 100 м (для кабелю категорії 5 - 200 м), кількість рівнів хабів ─не більше п'яти. Максимальна відстань між вузлами (діаметр мережі) може досягати 2000 м (застосування оптоволоконних

з'єднань не дає можливості долати цей бар'єр, оскільки обмежена максимальна затримка проходження сигналу). Максимальна кількість вузлів мережі ─ до 1024 (рекомендовано ─ до 250).

3.7. Технологія WiFi

WiFi – скорочення від англійського словосполучення Wireless Fidelity, що означає стандарт безпровідного (радіо) зв'язку, який об'єднує декілька протоколів та має офіційне найменування IEEE 802.11 (Institute of Electrical and Electronic Engineers – міжнародної організації, що займається розробкою стандартів у сфері електронних технологій). Найбільш відомим та поширеним на сьогоднішній день є протокол IEEE 802.11g, що визначає функціонування бездротових мереж.

Максимальна дальність передачі сигналу у такій мережі складає 100 метрів, однак на відкритій місцевості вона може досягати й більших відстаней (до 300-400 м).

Ядром безпровідної мережі WiFi є так звана точка доступу (Access Point), яка підключається до якоїсь наземної мережевої інфраструктури (каналам Інтернет-провайдера) та забезпечує передачу радіосигналу. Зазвичай, точка доступу складається із приймача, передавача, інтерфейсу для підключення до дротової мережі та програмного забезпечення для обробки даних. Навколо точки доступу формується територія радіусом 50-100 метрів (її називають хот-спотом або зоною WiFi), на якій можна користуватися бездротовою мережею.

Для того щоб підключитися до точки доступу та відчути всі переваги безпровідної мережі, власник ноутбуку або мобільного пристрою, із WiFi адаптером, необхідно просто потрапити в радіус її дії. Усі дії із визначення пристрою та налаштування мережі більшість операційних систем комп'ютерів та мобільних пристроїв проводять автоматично. Якщо користувач одночасно потрапляє в декілька WiFi зон, то підключення здійснюється до точки доступу, що забезпечує самий сильний сигнал.

3.8. Технологія WIMAX

Ціль технології WIMAX полягає в тому, щоб надати універсальний бездротовий доступ для широкого спектру пристроїв (робочих станцій, портативних пристроїв і мобільних телефонів) і їхнього логічного об'єднання ─ локальних мереж. Треба відзначити, що дана технологія має ряд переваг:

В порівнянні з дротяними (xDSL або широкосмуговим), безпровідними або системами супутників мережі WIMAX повинні дозволити операторам і сервіс-провайдерам економічно ефективно охопити не тільки нових потенційних користувачів, але і розширити спектр інформаційних і комунікаційних технологій для користувачів, що вже мають фіксований (стаціонарний) доступ.

Стандарт об'єднує технології рівня оператора зв'язку (для об'єднання декількох підмереж і надання їм доступу до Internet), а також технології "останньої милі" (кінцевого відрізка від точки входу в мережу провайдера до комп'ютера користувача), що створює універсальність і, як наслідок, підвищує надійність системи.

Безпровідні технології більш гнучкі і, як наслідок, простіші в розгортанні, оскільки у міру необхідності можуть масштабуватися.

Простота установки як чинник зменшення витрат на розгортання мереж в країнах, що розвиваються, малонаселених або віддалених районах.

Дальність обхвату є істотним показником системи радіозв'язку. На даний момент більшість безпровідних технологій широкосмугової передачі даних вимагають наявності прямої видимості між об'єктами мережі. WIMAX завдяки використанню технології OFDM створює зони покриття в умовах відсутності прямої видимості від клієнтського устаткування до базової станції, при цьому відстані обчислюються кілометрами.

Технологія WIMAX містить протокол IP, що дозволяє легко і прозоро інтегрувати її в локальні мережі.

Система WIMAX складається з двох основних частин:

- ***Базова станція WIMAX***, може розміщуватися на висотному об'єкті - будівлі або вежі.
- ***Приймач WIMAX***: антена з приймачем.

З'єднання між базовою станцією і клієнтським приймачем проводиться в СВЧ діапазоні 2-11 ГГЦ. Дане з'єднання в ідеальних умовах дозволяє передавати дані із швидкістю до 20 Мбіт/с і не вимагає, щоб станція знаходилася на відстані прямої видимості від користувача. Цей режим роботи базової станції WIMAX близький широко використовуваному стандарту 802.11 (WI-FI).

WIMAX застосовується як на "останній милі" - кінцевій ділянці між провайдером і користувачем, - так і для надання доступу регіональним мережам: офісним, районним.

Між сусідніми базовими станціями встановлюється постійне з'єднання з використанням надвисокої частоти 10-66 ГГЦ радіозв’язку прямої видимості. Дане з'єднання в ідеальних умовах дозволяє передавати дані із швидкістю до 120 Мбіт/с. Обмеження по умові прямої видимості, зрозуміло, не є перевагою, проте воно накладається тільки на базові станції, що беруть участь в покритті району, що цілком можливо реалізувати при розміщенні устаткування.

Як мінімум одна з базових станцій може бути постійно пов'язана з мережею провайдера через широкосмугове швидкісне з'єднання. Фактично, чим більше станцій мають доступ до мережі провайдера, тим вище швидкість і надійність передачі даних. На базі стільникового принципу розробляються також шляхи побудови оптимальної мережі, що огинає великі об'єкти (наприклад, гірські масиви), коли серія послідовних станцій передає дані за естафетним принципом.

По структурі мережі стандарту IEEE 802.16 дуже схожий на традиційні мережі мобільного зв'язку: тут також є базові станції, які діють в радіусі до 50 км, при цьому їх також необов'язково встановлювати на вежах. Для них цілком підходять дахи будинків, потрібне лише дотримання умови прямої видимості між станціями. Для з'єднання базової станції з користувачем необхідна наявність абонентського устаткування. Далі сигнал може потрапляти по стандартному Ethernet-кабелю, як безпосередньо на конкретний комп'ютер, так і на точку доступу стандарту 802.11 WI-FI або в локальну дротяну мережу стандарту Ethernet.

Це дозволяє зберегти існуючу інфраструктуру районних або офісних локальних мереж під час переходу з дротового доступу на WIMAX. Крім того, це дає можливість максимально спростити розгортання мереж, використовуючи знайомі технології для підключення комп’ютерів.

3.9. Побудова мереж Ethernet та Fast Ethernet

Кабельна структура визначає час життя мережі ─ всі інші компоненти залежать від неї. Для нових і існуючих мереж кабельна структура (кабельна ділянка) є основою для з'єднання локальної мережі з глобальною. В 1970 — 80-х роках в локальних мережах для горизонтальної розводки по робочих місцях широко використовувався тонкий коаксіальний кабель, а товстий коаксіальний кабель застосовувався як вертикальний висхідний кабель (riser cable), прокладений між поверхами будівлі. На рис. 1 зображена стара, традиційна шинна топологія, в якій для розширення мережі спочатку використовуються багатопортові повторювачі, а потім ─ мости.

Традиційні кабельні структури з використанням тонкого і товстого коаксіальних кабелів мають істотні обмеження. По-перше, їх смуга пропускання не відповідає високим вимогам трафіку, створюваного сучасними програмами. По-друге, ці мережі (де застосовується негнучкий коаксіальний кабельний кабель, що не витримує багатократні перегини) дуже дорогі при експлуатації і ремонті.

BNC-конектори для коаксіальний кабельних кабелів коштують більше, ніж конектори RJ-45, що використовуються для витої пари. Їх складніше встановлювати, вони менш надійні після декількох підключень/відключень. Крім того, несправний трансивер для тонкого коаксіального кабелю складніше знайти у разі відмови мережі, оскільки для реалізації мережного підключення використовуються декілька різних компонентів з BNC-роз'ємами.

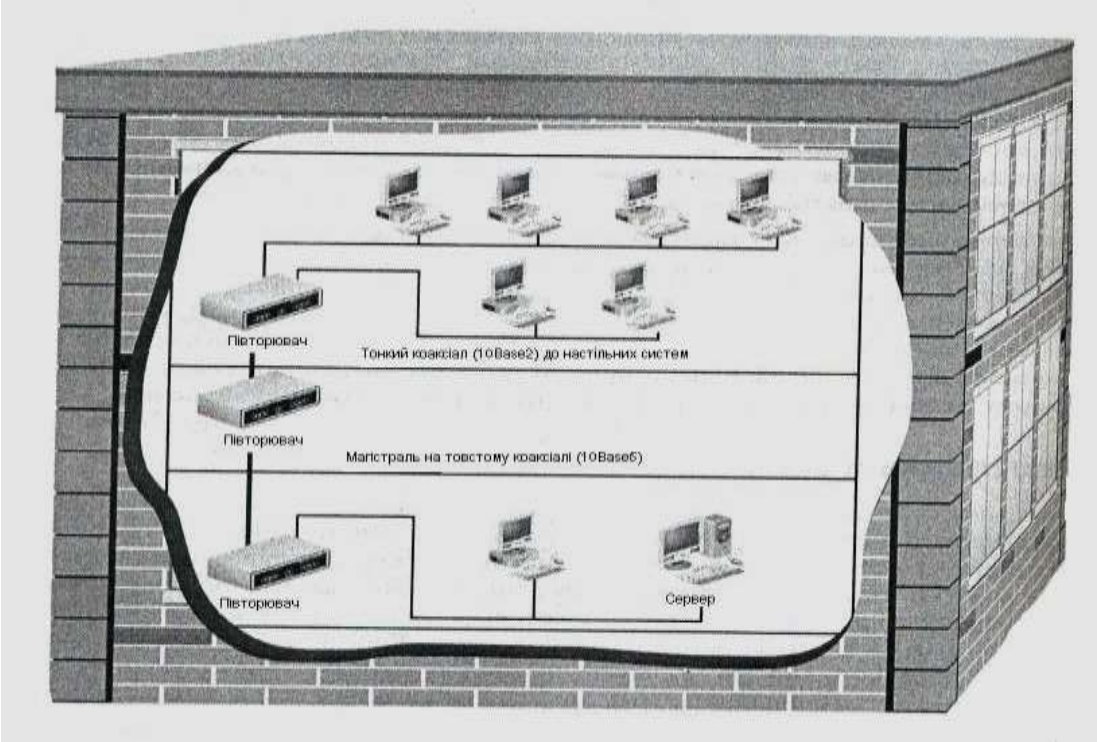

Рис. 1. Традиційна кабельна ділянка мережі на базі тонкого і товстого коаксіального кабелю

Ще одна проблема полягає в тому, що цілий сегмент мережі легко вивести з ладу, якщо з нього (випадково або навмисне) зняти термінатор або якщо в ньому з'явиться всього лише один несправний пристрій (або відмовить компонент кабельної розводки). Невдало вибрана топологія мережі може зробити практично неможливим її розширення. Крім того, може виникнути необхідність заміни вже існуючої мережі на нову, більш досконалу.
При цьому необхідно враховувати наступні чинники:

- можливість заміни застарілого кабелю (наприклад, тонкого і товстого коаксіального кабелю, а також кабелю Категорії 3);
- вартість кабелю і конекторів;
- монтажні витрати;
- умови середовища (наприклад, наявність коробів і джерел радіо- і електромагнітних перешкод);
- додаткові вимоги до кабелю;
- створення і перебудова приміщень для монтажних шаф.

В будівлі, замість товстого магістрального коаксіального кабелю, прокладіть багатомодовий оптоволоконний кабель, а повторювачі замініть на комутатори. Замініть тонкий коаксіальний кабель або кабель Категорії 3, що йде до робочих станцій, на кабель Категорії 5 (або кращий), проте майте на увазі, що вам буде потрібно також замінити встановлені мережні адаптери під тонкий коаксіальний кабель на адаптери, що забезпечують підключення витої пари. Для прокладених між будівлями сегментів регіональної мережі замініть

товстий коаксіальний кабель або кабель Категорії 3 на одно- або багатомодовий (залежно від відстані) оптоволоконний кабель.

У багатьох випадках вартість сучасного кабелю і конекторів буде нижчою, ніж витрати на старий кабель через існуючий масовий попит. Визначаючи витрати на заміну старого кабелю порівняєте їх з тими сумами, які будуть заощаджені при експлуатації і супроводі. Прокладка нового кабелю може виявитися дорогою з погляду трудовитрат (залежно від ступеня складності робіт по видаленню старого кабелю і наявності ускладнюючих моментів, наприклад, якщо при цьому потрібно прибрати або нейтралізувати небезпечні будівельні матеріали). Вартість кабелю може збільшитися, якщо через будівельні нормативи і/або умови середовища необхідно придбати спеціальний кабель для прокладки у вентиляційній зоні або екранований кабель, захищений від радіо- і електромагнітних перешкод). Крім того, у всіх випадках має сенс залишати запас кабелю від 20% до 50% для спрощення і здешевлення підключення нових робочих станцій, оскільки витрати на оплату праці по прокладці кабелю більше вартості самого кабелю. Завжди дешевше встановити кабель "з нуля", ніж прокладати додаткові відрізки кабелю. Організації розширюються, і в приміщенні, де сьогодні сидить п'ять чоловік, завтра може виявитися вісім. Ще однією причиною для прокладки додаткового кабелю є необхідність створення надмірних комунікаційних магістралей.

3.10. Рекомендації по прокладці кабелів

Для будь-якої ситуації – чи замінюєте ви існуючий кабель або прокладаєте новий – є безліч перевірених рекомендацій. Якщо ви йтимете за вказаними рекомендаціям, то реалізована кабельна структура з більшою вірогідністю справиться з очікуваним мережним трафіком і зможе бути модернізована в майбутньому. Ніхто не хоче прокладати кабель так, щоб він із самого початку працював неправильно. Проте помилки трапляються, і для їх виправлення потрібні дорогі переробки або повна заміна розведеного кабелю, внаслідок чого марно витрачається час і виникають невиправдані витрати.

Щоб мережа працювала нормально, при монтажі кабельної ділянки користуйтеся наступними рекомендаціями:

- використовуйте принципи побудови структурованих кабельних систем і структурованих мереж (буде описаний пізніше);
- встановлюйте кабельну систему, смуга пропускання якої відповідає або перевершує смугу, необхідну в конкретній зоні (з урахуванням передбачуваних прикладних програм, комп'ютерів і мережних ресурсів, що використовуються);
- для горизонтальної розводки (для підключення настільних систем) використовуйте виту пару (UTP) Категорії 5 (або вище);
- для висхідного кабелю між поверхами застосовуйте багатомодове оптоволокно;

- перевірте, чи відповідають по довжині всі відрізки кабелю специфікаціям IEEE для вибраного комунікаційного середовища;
- на великих відстанях (наприклад, між будівлями) використовуйте одномодовий оптоволоконний кабель;
- встановлюйте бездротові мережі стандарту 802.11 в тих випадках, коли прокладка кабелю обходиться дуже дорого або для цього є дуже багато перешкод. При виборі такого рішення переконаєтеся в тому, що дотримані всі стандарти, і що ви ретельно вибрали обладнання, відповідне наявним або тим стандартам, що розробляються;
- прокладайте зіркоподібні кабельні ділянки;
- використовуйте тільки високоякісний кабель;
- слідуйте всім будівельним нормативам (наприклад, на прокладку спеціального кабелю для монтажу у вентиляційній зоні);
- уникайте великих зусиль при прокладці кабелів на основі витої пари;
- точно дотримуйте вимоги до радіусу вигину кабелю (щоб не пошкодити кабель монтажними кліщами або багатократними перегинами);
- в кінцевих точках залишайте достатній запас кабелю, що забезпечить гнучкість при подальших змінах, переробках або переміщеннях комп'ютерів;
- якщо для проведення робіт вибраний підрядчик, перевірте у нього наявність необхідних сертифікатів і ліцензій, а також переконаєтеся в тому, що він надав на кабельну ділянку документацію і результати тестування;
- переконайтеся, що кабель і монтаж сертифікований на відповідність специфікаціям IEEE;
- промаркіруйте всі кабелі відповідно до стандарту EIA/TIA-606 (наприклад, помітьте всі виходи і термінатори);
- правильно заземліть всі кабельні ділянки відповідно до стандарту EIA/TIA-607.

Сертифікація кабелю проходить в два етапи. Спочатку виробник кабелю сертифікує його на відповідність стандартам EIA/TIA, IEEE і UL. Потім за допомогою спеціального обладнання тестуються всі змонтовані сегменти кабелю і перевіряється їх відповідність стандартам EIA/TIA і IEEE.

Як загальне правило слід запам'ятати, що мінімальний радіус вигину для кабелю на основі чотирьох витих пар приблизно в чотири рази більше довжини кола кабелю, а якщо число пар більше чотирьох - то в 10 разів.

Структурована кабельна система

В даний час багато мереж створюються з використанням ідеології структурованих кабельних систем (структурована розводка, structured wiring). Це поняття може по-різному потрактувати тими, хто прокладає кабель, і проєктувальниками мереж. Ми так називатимемо спосіб прокладки кабелю, при якому він (сходиться по горизонталі у вигляді зірки, в центрі якої знаходиться один або декілька стійкових концентраторів або комутаторів,

розташованих в телекомунікаційних кімнатах або монтажних шафах (телекомунікаційні кімнати, telecommunication rooms, описані в стандарті EIA/TIA-569-A). Часто стійкові концентратори або комутатори знаходяться на одному поверсі і розміщуються в монтажній шафі, як показано на мал. 2.

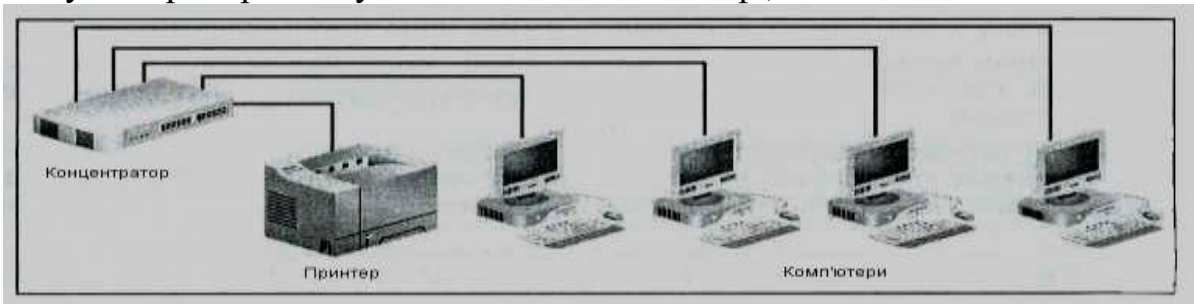

Рис. 2. Структурована кабельна система

Для реалізації структурованої кабельної системи необхідні наступні компоненти і умови:

- гнучкий кабель (наприклад, на основі витої пари);
- розводка у вигляді фізичної зірки;
- відповідність стандартам EIA/TIA-568-A і EIA/TIA-568-B на горизонтальну розводку;
- централізоване підключення кабельної ділянки до стійкових концентраторів або комутаторів;
- наявність "інтелектуальних здібностей" у концентраторів і комутаторів для виявлення несправностей у вузлах;
- можливість ізолювання хостів і серверів в своєму кабельному сегменті;
- наявність високошвидкісних каналів до хостів і серверів, а також до інших мережних пристроїв.

Звичайно горизонтальна розводка охоплює окремий поверх будівлі, яка віялоподібно розходиться по різних кімнатах і зонах офісу. Якщо в будівлі декілька поверхів, то існує декілька рівнів горизонтальної розводки, сполучених вертикальними кабелями, що в сукупності утворює структуровану мережу. Однією з переваг принципу горизонтальної розводки є те, що вона спрощує проєктування, розділяючи кабельну структуру на окремі модулі (подібно тому, як програміст створює в програмі підпрограми і зв'язує їх в цілий функціональний модуль). В будівлі кожний поверх є самостійною одиницею кабельної ділянки.

3.11. Вертикальна розводка і структуровані мережі

З'єднайте структуровану проводку кожного поверху в багатоповерховій будівлі, використовуючи ретельно продуману схему вертикальних кабелів, і ви отримаєте структуровану мережу. Компоненти вертикальної розводки такої мережі включають кабелі і мережне обладнання, що використовується між поверхами будівлі і часто фізично зв'язуючи телекомунікаційні кімнати суміжних поверхів. Вертикальна розводка використовується як логічна магістраль, до якої підключаються горизонтальні кабелі всіх поверхів будівлі.

При реалізації вертикальної розводки мережі потрібно керуватися наступними принципами:

- для зв'язку пристроїв використовуйте розширену зіркоподібну топологію (монтажні шафи, розташовані на поверхах, іноді можна сполучати в ланцюжок);
- застосовуйте високошвидкісний кабель, краще всього багатомодове оптоволокно, щоб зменшити вірогідність перевантаження магістралі і для захисту від радіо- і електромагнітних перешкод;
- дотримуйте стандарти EIA/TIA-568-A і EIA/TIA-568-B на вертикальну і магістральну розводку;
- використовуйте сертифікований висхідний кабель (кабель, придатний для прокладки між поверхами) для сегментів, що проходять по кабельних каналах і вертикальних шахтах; цей кабель повинен відповідати стандартам Underwriters Laboratories, Inc. (UL) і National Electric Code (NEC) на вогнестійкість;
- застосовуйте вогнестійкі матеріали для захисту відрізків кабелю між поверхами (якщо є більше двох поверхів або відповідно до стандартів UL і NEC, а також з урахуванням місцевих будівельних нормативів).

Для двох перших пунктів приведеного списку необхідні додаткові коментарі. ***По-перше,*** застосування розширеної зіркоподібної топології між поверхами відповідає специфікаціям EIA/TIA-568-A і EIA/TIA-568-B. Перевага такого підходу полягає в тому, що він спрощує управління з'єднаннями з використанням повторювачів, через які сигнал повинен передаватися. Недоліком є те, що центральний стійкових концентратор або комутатор може стати єдиною точкою відмови. Цю проблему можна розв'язати, придбавши пристрої з надмірністю (наприклад, з резервними задніми панелями і джерелами живлення). Крім того, такі пристрої можна підключити до джерела безперебійного живлення (uninterruptible power supply, UPS), що є системою резервного батарейного живлення, що включається при порушенні енергопостачання, а також у разі сплесків або падінь напруги.

По-друге, застосування оптоволокна для вертикальної розводки не тільки дозволить вам підвищити швидкість магістралі для реалізації високошвидкісних комунікацій, але і захистить магістраль від радіо- і електромагнітних перешкод. Це означає, що ви можете прокласти кабель біля ліній силової напруги, електричних кабелів, джерел світла і ліфтів, Крім того, на оптоволоконний кабель не розповсюджуються вимоги заземлення, чого не скажеш про мідний кабель.

Об'єднуючи структуровану кабельну систему з надійною вертикальною розводкою, ви одержуєте структуровану мережу (structured network), концепціям якої в книзі надається особлива увага. Елементи такої мережі зосереджені в стратегічних точках. Наприклад, комутатори поміщаються в монтажних шафах, які підключаються за допомогою високошвидкісних каналів до головного стійкових комутатора, розташованого в машинному залі або в деякій вузловій точці кабельної структури будівлі. Нерідко сервери

безпосередньо з'єднуються з головним або центральним комутатором по швидкісному каналу (наприклад, по 1-гігабітному каналу, як показано на рис. 3).

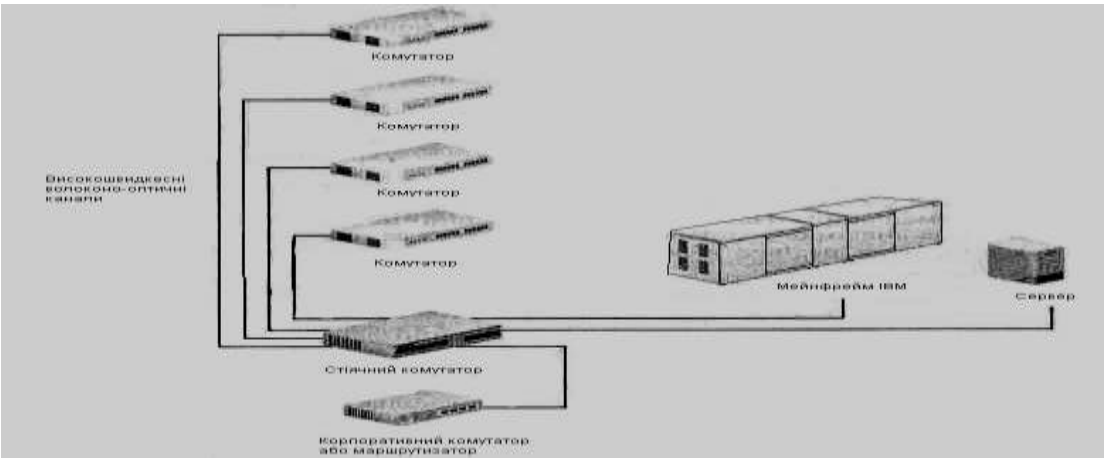

Рис. 3. Структурована мережа для централізованого управління

Для реалізації структурованої мережі в головних точках встановлюються стійкові комутатори або концентратори, які можуть централізувати кабельну структуру, а також модулі мостів, маршрутизаторів і комутаторів.

Структуровані мережі дозволяють мережному адміністратору вирішувати наступні задачі:

- централізувати або розподіляти управління мережею;
- об'єднувати вертикальні і горизонтальні мережні структури за допомогою високошвидкісної магістралі;
- перебудовувати фізичну і логічну топологію мережі;
- сегментувати мережу, використовуючи модель груп і віртуальні локальні мережі (VLAN);
- забезпечувати надмірність;
- швидко розширювати мережу і створювати нові високошвидкісні канали;
- здійснювати профілактичний моніторинг мережі, а також швидко знаходити і усувати виникаючі проблеми.

Крім того що в структурованій мережі головні мережні пристрої розташовані централізовано, іншою перевагою такої мережі є можливість централізованого мережного управління. Для цього вибираються базові точки в яких реалізуються важливі мережні функції. Наприклад, мережний моніторинг може здійснюватися на станції управління мережею з використанням протоколу SNMP і підключень до інтелектуального стійкового комутатора або концентратора. SNMP-сумісні комутатори (мережні агенти по збору інформації) розміщуються на кожному поверсі і забезпечують станцію управління безперервними даними про всі елементи мережі. При централізованому управлінні мережею багато операцій по конфігуруванню

мережі можна виконувати з однієї точки. Це особливо важливо для великих мереж.

При централізованому управлінні мережею також спрощуються такі операції, як моніторинг серверів і хостів, які можуть розміщуватися в таких зонах, де їх легко обслуговувати (наприклад, поряд з головними стійковими комутаторами). В цьому випадку резервування інформації і оновлення програмних засобів можна проводити на одному майданчику, а не на декількох, що нерідко дозволяє понизити трафік.

Сервери і хости можуть бути підключені до одного джерела безперебійного живлення і до джерела фільтрованого живлення (conditioned power source), заміна яких обходиться дешевше, ніж при їх розміщенні по різних приміщеннях. Джерело фільтрованого живлення є пристроєм, іноді вбудовуваним в джерела безперебійного живлення (UPS), який згладжує як невеликі, так і помітні зміни потужності силової напруги, одержуваної від енергетичних компаній, і забезпечує деякий заданий діапазон потужностей. Завдяки такому пристрою коливання потужності силової напруги згладжуються і не можуть пошкодити пристрою або створити перешкоди в компонентах.

Один з виробників джерел фільтрованого живлення ─ компанія Powercom ─ називає фільтрованою таку потужність, яка містить не більше 10% шуму, а злагодженою "землею" ─ лінію, коливання напруги в якій не перевищують 0,5 В. Для комп'ютерного обладнання, розташованого централізовано, необхідно також дотримувати вимог до температури, вологості і кількості пилу в приміщенні. Деякі організації не звертають достатньої уваги на зовнішні умови в приміщеннях, де встановлені комп'ютери, до тих пір, поки не почнуться проблеми. Це стосується і якості силової проводки.

Також існує ряд вимого до побудови безпровідних каналів зв’язку. Найбільш важливим є знання дальності його роботи.

3.12. Розрахунок безпровідного каналу зв'язку

Приведемо формулу розрахунку дальності. Вона береться з інженерної формули розрахунку втрат у вільному просторі:

$$FSL = 33 + 20(\lg F + \lg D)$$

FSL (Free Space Loss) – втрати у вільному просторі (дБ);
F – центральна частота каналу, на якому працює система зв'язку (Мгц);
D – відстань між двома точками (км).

FSL визначається сумарним посиленням системи. Воно вважається таким чином:

$$Y_{\text{дБ}} = P_{t,\text{дБмВт}} + G_{t,\text{дБи}} + G_{r,\text{дБи}} - P_{\min,\text{дБмВт}} - L_{t,\text{дБ}} - L_{r,\text{дБ}},$$

де $P_{t,\text{дБмВт}}$ – потужність передавача;

$G_{t,\text{дБи}}$ – коефіцієнт посилення передавальної антени;

$G_{r,\text{дБи}}$ – коефіцієнт посилення приймальної антени;

$P_{\min,\text{дБмВт}}$ – чутливість приймача на цій швидкості;

$L_{т,дБ}$ – втрати сигналу в коаксіальному кабелі і роз'ємах передавального тракту;

$L_{т,дБ}$ – втрати сигналу в коаксіальному кабелі і роз'ємах приймального тракту.

Таблиця 2. Залежність чутливості від швидкості передачі даних

Швидкість	Чутливість
54 Мбіт/с	- 66 дБмВт
48 Мбіт/с	- 71 дБмВт
36 Мбіт/с	- 76 дБмВт
24 Мбіт/с	- 80 дБмВт
18 Мбіт/с	- 83 дБмВт
12 Мбіт/с	- 85 дБмВт
9 Мбіт/с	- 86 дБмВт
6 Мбіт/с	- 87 дБмВт

Для кожної швидкості приймач має певну чутливість. Для невеликих швидкостей (наприклад, 1-2 Мбіт) чутливість найменша : від – 90 дБмВт до – 94 дБмВт. Для високих швидкостей чутливість набагато вища. Як приклад в таблиці 1 приведені декілька характеристик звичайних точок доступу 802.11a, b, g.

Залежно від марки радіомодулів максимальна чутливість може трохи варіюватися. Ясно, що для різних швидкостей максимальна дальність буде різною.

FSL обчислюється за формулою:

$$FSL = Y_{дБ} - SOM$$

де SOM (System Operating Margin) – запас в енергетиці радіозв'язку (дБ). Враховує можливі чинники, що негативно впливають на дальність зв'язку, такі як:

- температурний дрейф чутливості приймача і вихідної потужності передавача;
- всілякі атмосферні явища: туман, сніг, дощ;
- розузгодження антени, приймача, передавача з трактом антенного фідера.

Параметр SOM зазвичай береться рівним 10 дБ. Вважається, що 10-децибельный запас по посиленню достатній для інженерного розрахунку.

Центральна частота каналу F береться з таблиці 2.

Таблиця 3. Обчислення центральної частоти

Канал	**Центральна частота (Мгц)**
1	2412
2	2417
3	2422
4	2427
5	2432

6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

У результаті отримаємо формулу дальності зв'язку :

$$D = 10^{\left(\frac{FSL}{20} - \frac{33}{20} - \lg F\right)}.$$

3.13. Розрахунок зони Френеля

Радіохвиля в процесі поширення в просторі займає об'єм у вигляді еліпсоїда обертання з максимальним радіусом в середині прольоту, який називають зоною Френеля (рис. 4). Природні (земля, пагорби, дерева) і штучні (будівлі, стовпи) перешкоди, що потрапляють в цей простір, послабляють сигнал.

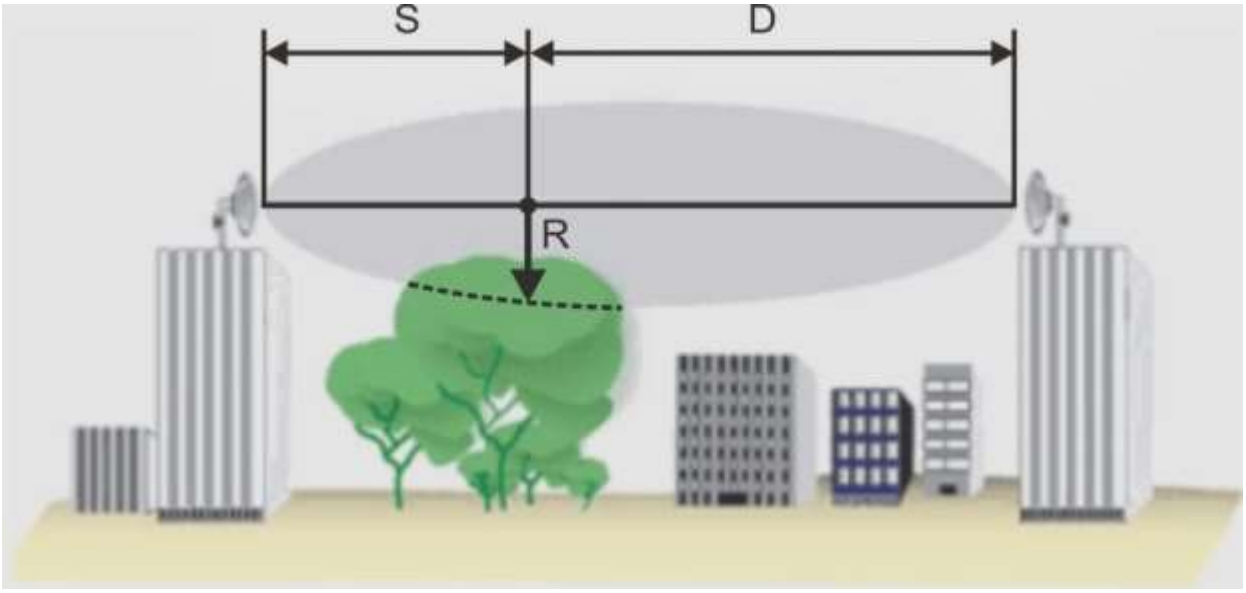

Рис. 4. Зона Френеля.

Радіус першої зони Френеля над передбачуваною перешкодою може бути розрахований за допомогою формули:

$$R = 17,3\sqrt{\frac{1}{f}\frac{SD}{S+D}},$$

де R – радіус зони Френеля (м);

S, D – відстань від антен до самої вищої точки передбачуваної перешкоди (км);
f – частота (ГГц).

Зауваження:

- Звичайне блокування 20% зони Френеля вносить незначне загасання в канал. При блокуванні понад 40% загасання сигналу буде вже значним, слід уникати попадання перешкод на шляху поширення.
- Цей розрахунок зроблений в припущенні, що земля плоска. Він не враховує кривизну земної поверхні. Для протяжних каналів слід проводити сукупний розрахунок, що враховує рельєф місцевості і природні перешкоди на шляху поширення. У разі великих відстаней між антенами слід намагатися збільшувати висоту підвісу антен, зважаючи на кривизну земної поверхні.

3.14. Побудова трактів антенних фідерів і радіосистем із зовнішніми антенами

Завдання по підключенню до безпровідного устаткування додаткових антен, посилення потужності передавача, включенню в систему додаткових фільтрів досить часто зустрічаються в практиці побудови безпровідних мереж. І, як правило, на цю тему виникає багато питань, найпоширенішими з яких є питання про відповідність роз'ємів на використовуваному устаткуванні і додаткових кабелях, а також питання за розрахунком отриманих систем.

Відразу необхідно відмітити, що винесення антени – справа невдячна, оскільки негативні чинники, що виникають при цьому, такі як загасання сигналу на кабельних складках і збільшення рівня паразитних шумів, значно погіршують характеристики початкової радіосистеми. В той же час підключені антени (особливо з великими коефіцієнтами посилення) багато в чому компенсують усі ці негативні чинники, але, незважаючи на це, при проєктуванні, все ж, намагаються максимально скоротити відстань від порту активного устаткування точок доступу до винесеної антени і по можливості підключити антену безпосередньо до точки доступу.

Дуже часто бувають випадки, коли необхідно збільшити зону охоплення усередині приміщень, для цього використовують антени у внутрішньому (indoor) виконанні. Для зв'язку між будинками або районами використовують дорожче устаткування в зовнішньому (outdoor) виконанні.

3.15. Тракт антенного фідера з підсилювачем

На рис. 5 показана безпровідна система з трактом антенного фідера, в який включена безліч елементів. Їх може бути значно більше, але тут показані найчастіше використовувані. Далі пояснимо, для чого використовується той або інший елемент, як він називається, і які нюанси необхідно врахувати при його використанні.

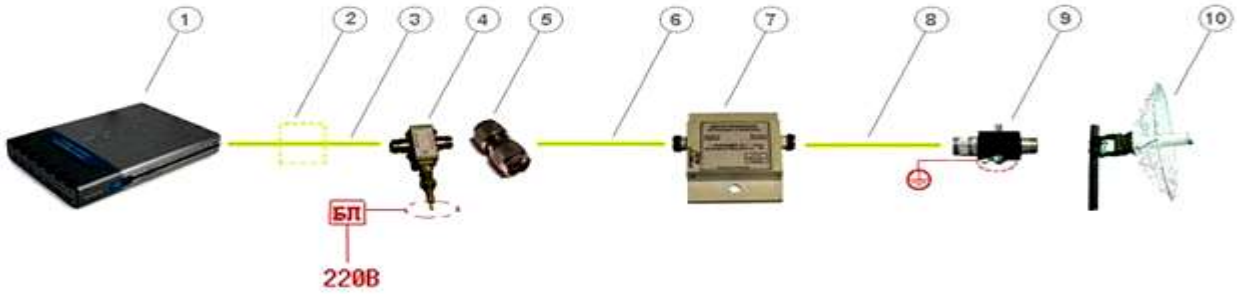

Рис. 5. Тракт антенного фідера з підсилювачем

1.Точка доступу зі знімною антеною

Майже усе безпровідне устаткування D-Link комплектується знімними штатними антенами 2-5 дБи (наприклад, DAP-1353 802.11n, DAP-1360U, DWL - 8200AP, DWL - 2700AP, DWL - 7700AP, DWL - G520 і т. д.) ─ це означає, що штатну антену можна легко зняти і підключити замість неї потужнішу антену з необхідним коефіцієнтом посилення і діаграмою спрямованості. У технічних характеристиках безпровідного устаткування завжди сказано, яким типом антен воно комплектується за умовчанням.

Окрім підтримуваних технологій і швидкісних характеристик точка доступу має декілька важливих фізичних характеристик, які є початковими даними для розрахунку тракту антенного фідера і енергетичних характеристик системи. До таких характеристик відносяться:

- потужність передавача, яка вимірюється або в міліватах (мВт) або в децибел-міліватах (дБмВт).
- чутливість приймача для певної швидкості – чим вона вища, тим вище швидкість.

2. Смуговий фільтр

Він показаний пунктиром, оскільки його досить рідко включають в систему, але, проте, він є присутнім в системах професійного рівня. Прийнято думати, що кабель вносить тільки втрати, пов'язані з довжиною кабелю, і досить вибрати кабель з малим загасанням або поставити підсилювач, і усі проблеми будуть вирішені. Проте це не зовсім так. В першу чергу, довгий кабель збирає перешкоди в усьому діапазоні частот, тому роботі заважатимуть усі радіопристрої, здатні створити на вході приймача карти досить сильну перешкоду. Тому часто трапляється, що в міському середовищі, в якому достатньо великий рівень завад, зв'язок між точками доступу в системах з винесеною на велику відстань антеною украй нестабільний, і тому в кабель необхідно включати додатковий смуговий фільтр безпосередньо перед вхідним роз'ємом точки доступу, який внесе ще втрати не менше 1,5 дБ.

Смугові фільтри бувають такими, що настроюються і з фіксованою центральною частотою, яка настроюється в процесі виробництва, наприклад як у фільтрів серії NCS F24XXX, тому бажано заздалегідь визначитися з вимогами по налаштуванню і вказати їх при замовленні. Фільтри розрізняються шириною смуги пропускання, що визначає діапазон частот, які не ослабляються.

3. Кабельна зборка SMA - RP - plug ↔ N - type - male

Часто її ще називають pigtale – це невеликий перехідник з антенного виведення indoor точки доступу, який називається SMA, – RP (реверс SMA), на широко використовуваний в устаткуванні антенного фідера високочастотний роз'єм N - type (рис. 6).

Рис. 6. Кабельна зборка pigtale

Pigtale – кабель входить в комплект постачання усіх зовнішніх (outdoor) антен D-Link, антени для внутрішнього використання також комплектуються необхідними кабелями. Вносить додаткове загасання близько 0,5 дБ.

1. Інжектор живлення

Включається в тракт між активним устаткуванням і вхідним портом підсилювача (вносить загасання не більше 0,5 дБ) і підключається до блоку живлення, який підключається до розетки 220В. Інжектор має 2 порти ─ обоє N - type - female. Інжектор живлення і блок живлення входять в комплект постачання підсилювачів.

2. Перехідник TLK - N - type - MM

Перехідник N-Type Male-Male (рис. 7) служить для зміни конфігурації порту з female на male, тут ми його використовуємо, щоб підключити до інжектора кабельну зборку (стандартні кабельні складки зазвичай мають роз'єми N - type - male ↔ N - type - female), що йде за ним.

Рис. 7. Перехідник TLK - N - type - MM

Загальноприйнятим є, що коаксіальний роз'єм, що встановлюється стаціонарно, наприклад входи або виходи підсилювачів, фільтрів, генераторів сигналів, роз'єми для підключення, що встановлюються на антенах, мають конфігурацію "гніздо" (female), а роз'єми на кабелях, що підключаються до них, мають конфігурацію "штекер" (male). Проте це правило не завжди дотримується, тому іноді виникають проблеми при зборці тракту на елементах

від різних виробників. Розв'язати цю проблему дозволяє використання перехідника N - type - male ↔ N - type - male.

6. Кабельна зборка (наприклад, HQNf - Nm15)

Це 15-метрова кабельна зборка N - type (female) ↔ N - type(рис. 8).

Рис. 8. Кабельна зборка N - type (female) ↔ N - type (male).

Можна також використати кабельні складки великої довжини, наприклад, послідовно об'єднавши дві 15-метрові зборки (чи інші довжини), важливо тільки щоб:

- рівень сигналу на вхідному порту підсилювача потрапляв в допустимий діапазон, який вказаний в характеристиках підсилювача;
- рівень сигналу, прийнятого від видаленої точки доступу і посиленого в підсилювачі, мав достатню інтенсивність для сприйняття приймачем точки після проходження кабельної зборки.

7. Підсилювач 2,4 ГГц (наприклад, NCS24XX)

Двонаправлений магістральний підсилювач (рис. 9) призначений для збільшення потужності сигналу, що передається і підвищення чутливості каналу прийому у безпровідних мережах передачі даних, а також компенсації втрат в каналі між радіомодемом і антеною.

Рис. 9. Підсилювач 2,4 ГГц

Підсилювач має зовнішнє виконання і може бути встановлений безпосередньо на антенному посту. Використання підсилювача дозволяє організувати зв'язок навіть за самих несприятливих умов з'єднання. При включенні підсилювача в радіосистему значною мірою збільшується зона її покриття.

При використанні підсилювачів необхідно враховувати наступні моменти: якщо потужність передавача точки доступу занадто велика і не потрапляє в діапазон допустимої інтенсивності сигналу на вхідному порту підсилювача, то використати її з підсилювачем все-таки можна, але вимагається включити в тракт між підсилювачем і точкою доступу кабельну зборку або який-небудь спеціальний елемент, загасання на якому забезпечить необхідне послаблення сигналу, з тим щоб його інтенсивність потрапила в допустимий діапазон. Послабляючи переданий сигнал, слід також пам'ятати, що одночасно ослабляється і прийнятий сигнал, тому не варто захоплюватися.

У таблиці зведені усі величини загасання від середовища поширення сигналу.

Таблиця 4. Загасання від середовища поширення сигналу

Найменування	**Од. вим.**	**Значення**
Вікно в цегляній стіні	дБ	2
Стекло в металевій рамі	дБ	6
Офісна стіна	дБ	6
Залізні двері в офісній стіні	дБ	7
Залізні двері в цегляній стіні	дБ	12,4
Скловолокно	дБ	0,5-1
Стекло	дБ	3-20
Дощ і туман	дБ/км	0,02-0,05
Дерева	дБ/м	0,35
Кабельна зборка pigtale	дБ	0,5
Смуговий фільтр NCS F24XXX	дБ	1,5
Коаксіальний кабель	дБ/м	0,3
Роз'їм N - type	дБ	0,75
Інжектор живлення	дБ	0,5

8. Кабельна зборка (наприклад, HQNf - Nml, 5)

HQNf - Nml, 5 - кабель (перехідник) N - type(female) ↔ N - type(male) довгою 1,5 м.

9. Модуль грозового захисту

У устаткуванні D - Link йде з усіма зовнішніми антенами. Має роз'єми N - type(female) ↔ N - type(male).

10.Зовнішня спрямована (наприклад, ANT24 - 2100)

Антена з коефіцієнтом посилення 21 дБі. Антени мають роз'єм N - type - female.

4. ЗАВДАННЯ НА КУРСОВУ РОБОТУ

Курсова робота полягає в ***розробці захищеної комп'ютерної мережі підприємства***. Вона повинна бути побудована на основі заданої модифікації мережних технологій Ethernet та об'єднання будівель за допомогою

безпроводового зв’язку. Структура комп'ютерної мережі, вживані кабелі, комунікаційне і інше обладнання і всі параметри, яких не вистачає, вибираються самим студентом.

Початковими даними є:

1. Поверховість і розміри будівель, в яких повинні бути розміщений складові частини комп'ютерної мережі;
2. Відстань між будівлями показано (мал. 10);
3. Кількість комп'ютерів в кожній будівлі (при цьому комп'ютери повинні бути встановлений на всіх поверхах будівель, кількість комп'ютерів на кожному поверсі вибирається відповідно до завдання.
4. Локальні мережі будівель об’єднуються за допомогою безпроводового зв’язку.

В процесі розробки захищеної комп'ютерної мережі повинні бути:

1. Розроблена структура (топологія) захищеної комп'ютерної мережі;
2. Вибрана кабельної системи з врахуванням захисту інформації;
3. Вибрано необхідне комунікаційне обладнання і комутаційні елементи з врахуванням засобів захисту інформації.
4. Розроблена системи захисту інформації в комп'ютерній мережі.

Ось що потрібно виконати чи розробити в кожному розділі курсової роботи, з особливим акцентом на захист інформації в комп'ютерних системах та мережах:

Розділ 1. Розробка структури (топології) захищеної комп'ютерної мережі

Завдання:

Огляд та аналіз предметної області:

- Провести огляд існуючих топологій мережі та визначити найкращі практики для забезпечення безпеки.
- Визначити вимоги до мережі на основі потреб організації та специфікацій безпеки.

Формулювання технічного завдання:

- Розробити технічне завдання, яке включає опис цілей проекту, вимоги до захисту інформації, бюджетні обмеження і технічні специфікації.
- Включити стандартні вимоги до захисту, такі як сегментація мережі, контролю доступу та захист від зовнішніх загроз.

Визначення сегментації мережі:

- VLAN (Virtual LAN): Розробити плани для використання VLAN для сегментації мережі і забезпечення безпеки, розділення трафіку і зменшення можливостей атаки.
- DMZ (Demilitarized Zone): Розробити і реалізувати DMZ-зони для відокремлення внутрішньої мережі від зовнішніх мереж і забезпечення публічного доступу до ресурсів без шкоди для основної мережі.

- Мережеві сегменти: Визначити мережеві сегменти для різних типів трафіку та систем, таких як сервіси, бази даних, і робочі станції, з метою зменшення ризику і збільшення контролю.

Аналіз уразливостей і ризиків:

- Провести оцінку потенційних уразливостей в запроектованій топології мережі.
- Розробити стратегії для мінімізації ризиків, включаючи резервні шляхи, забезпечення високої доступності і відновлення після збоїв.

Розділ 2. Вибір кабельної системи з врахуванням захисту інформації

Завдання:

Огляд кабельних систем:

- Розглянути різні типи кабелів, які можуть бути використані (екрановані виті пари STP, оптоволокно, коаксіальні кабелі) і їх відповідність вимогам до безпеки.
- Провести порівняння кабельних систем на основі їх характеристик, таких як захист від електромагнітних завад і перехоплення.

Вибір і обґрунтування кабелів:

- Вибрати кабелі, що відповідають вимогам до безпеки, наприклад, STP кабелі для захисту від перехоплення або оптоволокно для критичних з'єднань.
- Обґрунтувати вибір кабелів, описати їх характеристики та переваги для конкретної мережі.

Фізичний захист кабельних трас:

- Розробити план фізичного захисту кабельних трас, включаючи захищені канали, стійки, оболонки та інші засоби для запобігання фізичним пошкодженням і несанкціонованому доступу.
- Запровадити засоби для моніторингу і виявлення порушень кабельних трас.

Шифрування даних на рівні кабелів:

- Впровадити шифрування даних на рівні фізичного рівня передачі, де це необхідно, для підвищення рівня захисту інформації.

Розділ 3. Вибір необхідного комунікаційного обладнання і комутаційних елементів з врахуванням засобів захисту інформації

Завдання:

Вибір комунікаційного обладнання:

- Вибрати маршрутизатори, комутатори та інше мережеве обладнання, яке підтримує сучасні функції захисту, такі як VPN, IDS/IPS, брандмауери.
- Описати обладнання і його характеристики, які забезпечують захист мережі, наприклад, брандмауери з високою продуктивністю, маршрутизатори з підтримкою шифрування.

Вибір комутаційних елементів:

- Підібрати і описати комутаційні елементи, такі як роз'єми, конектори, кросові панелі і шафи, що мають захисні властивості.
- Включити інформацію про антивандальні конструкції і захист від несанкціонованого доступу до обладнання.

Забезпечення доступу і контроль:

- Розробити і впровадити рішення для контролю доступу до обладнання, включаючи фізичний доступ до мережевого обладнання і програмні засоби для моніторингу доступу.

Теоретичні відомості про мережеві протоколи/стандарти:

- Описати мережеві протоколи і стандарти, що використовуються в вашій мережі, їх особливості і вплив на безпеку, такі як IEEE 802.1X для аутентифікації і шифрування трафіку.

Розділ 4. Розробка системи захисту інформації в комп'ютерній мережі

Завдання:

Впровадження багаторівневої системи захисту:

- Міжмережні екрани (Firewall): Розробити і налаштувати міжмережні екрани для контролю вхідного і вихідного трафіку.
- Системи виявлення та запобігання вторгненням (IDS/IPS): Встановити і налаштувати IDS/IPS системи для моніторингу і блокування підозрілого трафіку.
- Шифрування даних: Впровадити шифрування даних на рівні канального та транспортного протоколів, забезпечуючи захист даних як при передачі, так і в спокої.

Засоби контролю доступу і аутентифікації:

- Розробити і реалізувати систему контролю доступу, яка включає аутентифікацію користувачів, авторизацію і управління привілеями.
- Впровадити багатофакторну аутентифікацію для підвищення безпеки доступу до критичних систем і даних.

Моніторинг і управління безпекою:

- Налаштувати системи моніторингу і управління безпекою для забезпечення постійного нагляду, виявлення і реагування на інциденти.
- Розробити процедури для регулярних перевірок безпеки, оновлень систем і управління вразливостями.
- Сформувати документацію, яка детально описує всі аспекти захисту інформації, включаючи процедури, конфігурації і політики безпеки.

- **4.1. ВИХІДНІ ДАНІ**

Рис. 10. Схема розташування об'єктів.

Таблиця 2. Залежність чутливості від швидкості передачі даних

Швидкість	Чутливість
54 Мбіт/с	- 66 дБмВт
48 Мбіт/с	- 71 дБмВт
36 Мбіт/с	- 76 дБмВт
24 Мбіт/с	- 80 дБмВт
18 Мбіт/с	- 83 дБмВт
12 Мбіт/с	- 85 дБмВт
9 Мбіт/с	- 86 дБмВт
6 Мбіт/с	- 87 дБмВт

Таблиця 3. Обчислення центральної частоти

Канал	**Центральна частота (Мгц)**
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

Таблиця 5

Номер будівлі	Розміри будівлі	Етажність
1	80x64м.	10
2	45x91м.	4
3	24x18м.	2
4	62x47м.	6
5	80x64м.	10
Висота поверху 3м.		

Таблиця 4. Загасання від середовища поширення сигналу

Найменування	**Од. вим.**	**Значення**
Вікно в цегляній стіні	дБ	2
Стекло в металевій рамі	дБ	6
Офісна стіна	дБ	6
Залізні двері в офісній стіні	дБ	7
Залізні двері в цегляній стіні	дБ	12,4
Скловолокно	дБ	0,5-1
Стекло	дБ	3-20
Дощ і туман	дБ/км	0,02-0,05
Дерева	дБ/м	0,35
Кабельна зборка pigtale	дБ	0,5
Смуговий фільтр NCS F24XXX	дБ	1,5
Коаксіальний кабель	дБ/м	0,3
Роз'їм N - type	дБ	0,75
Інжектор живлення	дБ	0,5

ПЕРЕЛІК ВАРІАНТІВ ЗАВДАНЬ

Варіант 1

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 3.

Задана модифікація (стандарт) мережної технології – 100Base-T4.

На 4 та 5 поверсі будівлі 1 по 10 хостів.

На кожному поверсі будівлі 3 по 15 хостів.

Швидкість передачі даних у бездротовій мережі – 18 Мбіт/с.

Канал передачі даних у бездротовій мережі – 4.

Варіант 2

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 5.

Задана модифікація (стандарт) мережної технології – 1000BASE-LH.

На 1 та 2 поверсі будівлі 1 по 9 хостів.

На 3 та 4 поверсі будівлі 5 по 7 хостів.

На 6 поверсі будівлі 5 по 10 хостів

Швидкість передачі даних у бездротовій мережі – 54 Мбіт/с.

Канал передачі даних у бездротовій мережі – 1.

Варіант 3

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 2 та 4.

Задана модифікація (стандарт) мережної технології – 10 Base-T.

На 2 поверсі будівлі 2 по 15 хостів.

На 2 та 3 поверсі будівлі 4 по 10 хостів.
Швидкість передачі даних у бездротовій мережі – 28 Мбіт/с.
Канал передачі даних у бездротовій мережі – 2.

Варіант 4

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 2 та 5.
Задана модифікація (стандарт) мережної технології – 1000Base-T.
На 1 та 2 поверсі будівлі 2 по 12 хостів.
На 5 та 6 поверсі будівлі 5 по 10 хостів.
На 10 поверсі будівлі 5 по 5 хостів.
Швидкість передачі даних у бездротовій мережі – 56 Мбіт/с.
Канал передачі даних у бездротовій мережі – 8.

Варіант 5

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 3 та 5.
Задана модифікація (стандарт) мережної технології – 100 Base-T4.
На кожному поверсі будівлі 3 по 16 хостів.
На 6 та 7 поверсі будівлі 5 по 10 хостів.
Швидкість передачі даних у бездротовій мережі – 24 Мбіт/с.
Канал передачі даних у бездротовій мережі – 5.

Варіант 6

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 3.
Задана модифікація (стандарт) мережної технології – 100 Base-TX Full Duplex.
На 3 та 4 поверсі будівлі 1 по 10 хостів.
На 1 та 2 поверсі будівлі 3 по 15 хостів.
Швидкість передачі даних у бездротовій мережі – 28 Мбіт/с.
Канал передачі даних у бездротовій мережі – 6.

Варіант 7

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 3 та 5.
Задана модифікація (стандарт) мережної технології – 100 Base-TX Full Duplex.
На кожному поверсі будівлі 3 по 12 хостів.
На 8 поверсі будівлі 5 - 15 хостів.
Швидкість передачі даних у бездротовій мережі – 38 Мбіт/с.
Канал передачі даних у бездротовій мережі – 9.

Варіант 8

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 4.

Задана модифікація (стандарт) мережної технології – 100 Base-TX Full Duplex.

На 4 та 9 поверсі будівлі 1 по 17 хоста.

На 5 та 6 поверсі будівлі 4 по 8 хостів.

Швидкість передачі даних у бездротовій мережі – 36 Мбіт/с.

Канал передачі даних у бездротовій мережі – 13.

Варіант 9

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 5.

Задана модифікація (стандарт) мережної технології – 1000BASE-LX.

На 3 та 4 поверсі будівлі 1 по 20 хостів.

На 5 та 7 поверсі будівлі 5 по 16 хостів.

Швидкість передачі даних у бездротовій мережі – 24 Мбіт/с.

Канал передачі даних у бездротовій мережі – 10.

Варіант 10

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 2 та 4.

Задана модифікація (стандарт) мережної технології – 100 Base-TX Full Duplex.

На 3 та 4 поверсі будівлі 2 по 18 хоста.

На 1 та 2 поверсі 4 будівлі по 16 хостів.

Швидкість передачі даних у бездротовій мережі – 48 Мбіт/с.

Канал передачі даних у бездротовій мережі – 7.

Варіант 11

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 3.

Задана модифікація (стандарт) мережної технології – 100Base-T4.

На 9 та 10 поверсі 1 будівлі по 15 хостів.

На кожному поверсі 3 будівлі по 10 хостів.

Швидкість передачі даних у бездротовій мережі – 18 Мбіт/с.

Канал передачі даних у бездротовій мережі – 9.

Варіант 12

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 4.

Задана модифікація (стандарт) мережної технології – 100Base-TX Full Duplex.

На 1 та 8 поверсі будівлі 1 по 18 хостів.

На 5 поверсі будівлі 4 по 14 хостів.

Швидкість передачі даних у бездротовій мережі – 24 Мбіт/с.

Канал передачі даних у бездротовій мережі – 2.

Варіант 13

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 3 та 5.

Задана модифікація (стандарт) мережної технології – 100Base-TX .

На кожному поверсі 3 будівлі по 16 хостів.

На 1 та 3 поверсі 5 будівлі по 12 хостів.

Швидкість передачі даних у бездротовій мережі – 48 Мбіт/с.

Канал передачі даних у бездротовій мережі – 2.

Варіант 14

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 2 та 5.

Задана модифікація (стандарт) мережної технології – 1000Base-T.

На 1 та 2 поверсі 2 будівлі по 9 хостів

На 7 та 8 поверсі 5 будівлі по 20 хостів.

Швидкість передачі даних у бездротовій мережі – 36 Мбіт/с.

Канал передачі даних у бездротовій мережі – 8.

Варіант 15

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 5.

Задана модифікація (стандарт) мережної технології – 100 Base-T4.

На 1 та 3 поверсі будівлі 1 по 15 хостів.

На 6 та 8 поверсі будівлі 5 по 7 хостів.

Швидкість передачі даних у бездротовій мережі – 24 Мбіт/с.

Канал передачі даних у бездротовій мережі – 12.

Варіант 16

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 4.

Задана модифікація (стандарт) мережної технології – 100 Base-TX Full Duplex.

На 10 поверсі будівлі 1 - 8 хостів.

На 1 та 4 поверсі будівлі 4 по 10 хостів.

Швидкість передачі даних у бездротовій мережі – 12 Мбіт/с.

Канал передачі даних у бездротовій мережі – 7.

Варіант 17

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 2 та 5.

Задана модифікація (стандарт) мережної технології – 1000BASE-SX.

На 1 та 2 поверсі будівлі 2 по 10 хостів.
На 3 та 4 поверсі будівлі 5 по 5 хостів.
На 9 поверсі будівлі 5 - 18 хостів.
Швидкість передачі даних у бездротовій мережі – 54 Мбіт/с.
Канал передачі даних у бездротовій мережі – 10.

Варіант 18

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 4.
Задана модифікація (стандарт) мережної технології – 100 Base-TX Full Duplex.
На 2 та 9 поверсі будівлі 1 по 9 хостів.
На 10 поверсі будівлі 1 - 6 хостів.
На 6 поверсі будівлі 4 - 10 хостів.
Швидкість передачі даних у бездротовій мережі – 36 Мбіт/с.
Канал передачі даних у бездротовій мережі – 13.

Варіант 19

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 5.
Задана модифікація (стандарт) мережної технології – 100 Base-TX Full Duplex.
На 1 та 2 поверсі будівлі 1 по 9 хостів.
На 5 та 7 поверсі будівлі 5 по 10 хостів.
Швидкість передачі даних у бездротовій мережі – 24 Мбіт/с.
Канал передачі даних у бездротовій мережі – 9.

Варіант 20

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 2 та 4.
Задана модифікація (стандарт) мережної технології – 100BASE-TX.
На 3 та 4 поверсі будівлі 2 по 18 хостів.
На 1 та 6 поверсі будівлі 4 по 10 хостів.
Швидкість передачі даних у бездротовій мережі – 48 Мбіт/с.
Канал передачі даних у бездротовій мережі – 7.

Варіант 21

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 3.
Задана модифікація (стандарт) мережної технології – 100Base-T4.
На 4 та 5 поверсі будівлі 1 по 14 хостів.
На кожному поверсі будівлі 3 по 10 хостів.
Швидкість передачі даних у бездротовій мережі – 32 Мбіт/с.
Канал передачі даних у бездротовій мережі – 4.

Варіант 22

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 5.

Задана модифікація (стандарт) мережної технології –10BASE5 .

На 10 поверсі будівлі 1 по 8 хостів.

На 4 та 9 поверсі будівлі 5 по 10 хостів.

Швидкість передачі даних у бездротовій мережі – 24 Мбіт/с.

Канал передачі даних у бездротовій мережі – 2.

Варіант 23

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 2 та 4.

Задана модифікація (стандарт) мережної технології – 10 Base-T.

На 3 та 4 поверсі будівлі 2 по 9 хостів.

На 1 та 2 поверсі будівлі 4 по 8 хостів.

Швидкість передачі даних у бездротовій мережі – 24 Мбіт/с.

Канал передачі даних у бездротовій мережі – 14.

Варіант 24

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 2 та 5.

Задана модифікація (стандарт) мережної технології – 1000BASE-LH.

На 1 та 2 поверсі будівлі 2 по 10 хостів.

На 5 та 6 поверсі будівлі 5 по 15 хостів.

Швидкість передачі даних у бездротовій мережі – 56 Мбіт/с.

Канал передачі даних у бездротовій мережі – 9.

Варіант 25

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 3 та 5.

Задана модифікація (стандарт) мережної технології – 100 Base-T4.

На кожному поверсі 3 будівлі по 8 хостів.

На 9 поверсі будівлі 5 - 10 хостів.

Швидкість передачі даних у бездротовій мережі – 24 Мбіт/с.

Канал передачі даних у бездротовій мережі – 7.

Варіант 26

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 4.

Задана модифікація (стандарт) мережної технології – 100Base-TX.

На 5 та 6 поверсі будівлі 1 по 5 хостів.

На 1 та 2 поверсі будівлі 4 по 9 хостів.

Швидкість передачі даних у бездротовій мережі – 12 Мбіт/с.

Канал передачі даних у бездротовій мережі – 6.

Варіант 27

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 3 та 5.

Задана модифікація (стандарт) мережної технології – 1000BASE-T.

На 1 та 2 поверсі будівлі 3 по 10 хоста.

На 7 та 8 поверсі будівлі 5 по 15 хостів.

На 9 поверсі будівлі 5 - 7 хостів.

Швидкість передачі даних у бездротовій мережі – 54 Мбіт/с.

Канал передачі даних у бездротовій мережі – 3.

Варіант 28

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 4.

Задана модифікація (стандарт) мережної технології – 100 Base-TX Full Duplex.

На 4 та 9 поверсі будівлі 1 по 13 хоста.

На 5 та 6 поверсі 4 будівлі по 10 хостів.

Швидкість передачі даних у бездротовій мережі – 36 Мбіт/с.

Канал передачі даних у бездротовій мережі – 13.

Варіант 29

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 5.

Задана модифікація (стандарт) мережної технології – 1000BASE-SX.

На 1 та 2 поверсі будівлі 1 по 20 хоста.

На 7 та 8 поверсі будівлі 5 по 16 хостів.

Швидкість передачі даних у бездротовій мережі – 52 Мбіт/с.

Канал передачі даних у бездротовій мережі – 10.

Варіант 30

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 4.

Задана модифікація (стандарт) мережної технології – 100 Base-TX Full Duplex.

На 1 та 2 поверсі будівлі 1 по 12 хостів.

На 3 та 6 поверсі будівлі 4 по 20 хостів.

Швидкість передачі даних у бездротовій мережі – 48 Мбіт/с.

Канал передачі даних у бездротовій мережі – 7.

Варіант 31

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 3.

Задана модифікація (стандарт) мережної технології – 100Base-T4.
На 9 та 10 поверсі будівлі 1 по 7 хостів.
На кожному поверсі 3 будівлі по 9 хостів.
Швидкість передачі даних у бездротовій мережі – 18 Мбіт/с.
Канал передачі даних у бездротовій мережі – 14.

Варіант 32

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 4.
Задана модифікація (стандарт) мережної технології – 100Base-TX Full Duplex.
На 1 та 2 поверсі будівлі 1 по 5 хостів.
На 1 та 2 поверсі будівлі 5 по 10 хостів.
Швидкість передачі даних у бездротовій мережі – 24 Мбіт/с.
Канал передачі даних у бездротовій мережі – 12.

Варіант 33

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 2 та 4.
Задана модифікація (стандарт) мережної технології – 10 Base-T.
На 1 та 2 поверсі будівлі 2 по 16 хостів.
На 3 та 4 поверсі будівлі 4 по 10 хостів.
Швидкість передачі даних у бездротовій мережі – 48 Мбіт/с.
Канал передачі даних у бездротовій мережі – 2.

Варіант 34

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 2 та 5.
Задана модифікація (стандарт) мережної технології – 1000Base-T.
На 1 та 2 поверсі будівлі 2 по 12 хостів.
На 4 поверсі будівлі 2 по 5 хостів
На 5 та 6 поверсі будівлі 5 по 9 хостів.
Швидкість передачі даних у бездротовій мережі – 36 Мбіт/с.
Канал передачі даних у бездротовій мережі – 7.

Варіант 35

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 2 та 5.
Задана модифікація (стандарт) мережної технології – 100 Base-T4.
На 1 та 4 поверсі будівлі 2 по 8 хостів.
На 1 та 7 поверсі 5 будівлі по 10 хостів.
Швидкість передачі даних у бездротовій мережі – 24 Мбіт/с.
Канал передачі даних у бездротовій мережі – 7.

Варіант 36

Локальна комп'ютерна мережа повинна об'єднати комп'ютери, встановлені в будівлях 1 та 4.

Задана модифікація (стандарт) мережної технології – 100 Base-TX Full Duplex.

На 1 та 9 поверсі 1 будівлі по 8 хостів.

На 1 та 2 поверсі 4 будівлі по 9 хостів.

Швидкість передачі даних у бездротовій мережі – 12 Мбіт/с.

Канал передачі даних у бездротовій мережі – 2.

5. ВИМОГИ ДО ОФОРМЛЕННЯ ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

5.1. Загальні вимоги

Курсова робота повинна містити графічну частину і записку пояснення.

Курсова робота має бути виконана й оформлена з додержанням усіх технічних вимог до наукових робіт. Текст роботи має бути набраний на комп'ютері в текстовому редакторі *MS Word* на одному боці аркуша білого паперу формату А4. Шрифт Times New Roman, 14 пт, через 1,5 інтервалу, текст вирівнюється по ширині аркуша. Можна також подати таблиці та ілюстрації на аркушах формату А3.

Текст розміщується на сторінці, яка обмежується полями: лівим − 30 мм, правим − 10 мм, верхнім − 20 мм, нижнім − 20 мм. Відстань між заголовком і текстом має бути в межах 15 мм.

Текст ПЗ пишеться літературною державною мовою. У тексті ПЗ не дозволяється: вживати звороти розмовної мови; вживати застарілі та жаргонні терміни і вислови; вживати скорочені слова, крім встановлених стандартами скорочень. У тексті ПЗ, за винятком формул, таблиць і рисунків, не допускається: вживати математичний знак мінус (-) перед від'ємними величинами (треба писати слово "мінус"); вживати без числових значень знаки >, <, =, :, %, №.

У ПЗ треба використовувати одиниці СІ. Якщо значення приведено в інших одиницях, переведення їх в одиниці СІ обов'язкове лише за умови викладення найважливіших положень ПЗ. Якщо в тексті ПЗ наводиться ряд числових значень в однакових одиницях, то позначення одиниці виміру зазначають тільки після останнього числового значення, наприклад: 1, 2, 3 м; або від 5 до 10 мм. Одиниці вимірювання від числових величин відокремлюють нерозривним пробілом (Ctrl+Shift+Space).

Числові значення величин треба відокремлювати від десяткової частини комою, наприклад: 7,5; 8,75; 10,00. Помилки та графічні неточності допускається виправляти підчищенням або зафарбовуванням білою фарбою і нанесенням на тому ж місці або між рядками виправленого зображення машинним способом або від руки. Виправлене повинно бути чорного кольору.

Прізвища, назви установ, організацій, фірм та інші власні назви у ПЗ наводять мовою оригіналу. Допускається транслітерувати власні назви і наводити назви організацій у перекладі на мову звіту, додаючи (при першій згадці) оригінальну назву. Структурні елементи «РЕФЕРАТ», «ЗМІСТ», «ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ», «ВСТУП», «ВИСНОВКИ ТА ПРОПОЗИЦІЇ», «СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ» не нумерують, а їх назви використовують за заголовки структурних елементів. Заголовки структурних елементів ПЗ слід розташовувати посередині рядка і друкувати великими літерами без крапки в кінці, не підкреслюючи

Список позначень і прийнятих скорочень обов'язково має бути окремим підрозділом роботи, якщо при її написанні застосовується спеціальні скорочення, символи та терміни. Цей розділ має передувати викладенню основної частини курсової роботи.

Скорочення, символи та терміни розміщуються стовпчиком, у якому зліва розташовані символи та спеціалізовані терміни, а праворуч – їх розшифрування.

Текст основної частини ПЗ поділяють на розділи відповідно до завдання і структури КР. Розділи і підрозділи повинні мати заголовки. Пункти і підпункти можуть мати заголовки.

Якщо заголовок складається з двох і більше речень, їх розділяють крапкою. Перенесення слів у заголовку розділу не допускається. Відстань між заголовком і подальшим чи попереднім текстом має бути не менше, ніж один порожній рядок. Не допускається розміщувати назву підрозділу, а також пункту й підпункту в нижній частині аркуша, якщо після неї розміщено тільки один рядок тексту.

Аркуші ПЗ слід нумерувати арабськими цифрами, додержуючись наскрізної нумерації впродовж усього тексту. Номер аркушу проставляють у відповідному полі основного напису.

Титульний аркуш та завдання на курсову роботу включають до загальної нумерації аркушів ПЗ. Номер на титульному аркуші та завданні не проставляють. Аркуш, розміщений після завдання на курсову роботу, нумерується цифрою 4.

Ілюстрації й таблиці, розміщені на окремих аркушах, включають до загальної нумерації аркушів ПЗ.

Кожен структурний елемент ПЗ починають з нового аркушу. Оформлення аркушу структурного елементу ПЗ проводиться відповідно до таких вимог.

5.2. Заголовки

Розділи, підрозділи мусять мати заголовки, що чітко й коротко відображають їхній зміст.

Заголовки розділів, підрозділів і пунктів слід друкувати з абзацним відступом з великої літери без крапки в кінці та без підкреслень.

Якщо заголовок складається з двох речень, їх відокремлюють крапкою. Перенесення слів у заголовку розділу не допускається. У разі використання набірних друкарських форм заголовки розділів і підрозділів слід виділяти шрифтом.

5.3. Переліки

У тексті пунктів або підпунктів можуть бути переліки. Перед кожною позицією переліку слід ставити дефіс або (за необхідності послатися в тексті на один із переліків) малу літеру, після якої ставлять дужку. Для подальшої деталізації переліку необхідно використовувати арабські цифри, після яких ставлять дужку.

Перелік першого рівня деталізації друкують малими літерами з абзацного відступу, другого рівня − з відступом відносно місця розташування переліків першого рівня.

Приклад:

а)_____

б)_____

1)_____

2)_____

в)_____

5.4. Графічний матеріал

Графічний матеріал – рисунки (схеми, діаграми тощо) розміщують у КР для встановлення властивостей або характеристик об'єкта, а також для ліпшого розуміння тексту роботи. На графічний матеріал мають бути посилання в тексті курсової роботи.

Графічний матеріал розміщують безпосередньо після тексту, в якому про нього згадується вперше, або на наступній сторінці, а за необхідності – у додатку.

Таблиці, що доповнюють графічний матеріал, подають після графічного матеріалу.

Графічний матеріал може мати тематичну назву, яку розміщують під ним. За необхідності під графічним матеріалом наводять пояснювальні дані. Слово «рисунок» і назву подають після пояснювальних даних. Графічний матеріал (за винятком графічного матеріалу додатків) слід нумерувати арабськими цифрами порядковою нумерацією в межах розділу. Якщо рисунок один, його позначають “Рис. 1”. Номер рисунка складається з номерів розділу та порядкового номера рисунка, відокремлених крапкою (Рис. 1.1).

Графічний матеріал кожного додатка позначають окремою нумерацією арабськими цифрами з додаванням перед цифрою позначення додатка (Рис. В.3).

Схеми повинен відповідати структурі (топології) комп'ютерної мережі з планом поверхів будівлі з нанесеним на них маршрутом проходження кабелів

комп'ютерної мережі по кожному поверху (вертикальне та горизонтальне з'єднання) та схеми антено-фідерних трактів.

На кожній приведеній схемі повинно бути показано розміщення комп'ютерів, комунікаційного і іншого необхідного обладнання вибраного студентом самостійно.

Кожна схема виконується на окремому листі формату А4.

5.5. Формули

Формули мають нумеруватися арабськими цифрами порядковою нумерацією в межах розділу, які друкують на рівні формули праворуч у круглих дужках.

Номер формули складається з номера розділу і порядкового номера формули, відокремлених крапкою.

Приклад:
(3.1), (3.3).

Посилання в тексті на порядкові номери формули дають у дужках.

Приклад:
... у формулі (1.1).

Формули в додатках нумерують окремо арабськими цифрами в межах кожного додатка з додаванням перед цифрою позначення додатка.

Приклад:
... у формулі (В. 1).

У формулі як символи фізичних величин слід застосовувати позначення, встановлені відповідними стандартами або іншими документами.

Пояснення символів і числових коефіцієнтів, що входять до формули, якщо вони не пояснювалися в тексті, мають бути наведені безпосередньо під формулою. Пояснення кожного символу слід давати з нового рядка в тій послідовності, в якій символи наведено у формулі. Перший рядок пояснення має починатися словом "де" без двокрапки.

Формули, що подаються одна за одною і не розділені текстом, відокремлюють комою.

5.6. Додатки

Матеріал, що доповнює положення курсової роботи, допускається розміщувати в додатках. Додатками можуть бути: графічний матеріал, таблиці великого формату, розрахунки, опис алгоритмів і програм задач, що розв'язуються на ПК тощо.

Додатки можуть бути обов'язковими та інформаційними. Інформаційні додатки можуть мати рекомендований або довідковий характер.

Додатки позначають великими літерами української абетки, починаючи з А, за винятком літер Ґ, Є, З, І, Ї, Й, О, Ч, Ь. Після слова "Додаток" друкують літеру, що позначає його послідовність.

Допускається позначення додатків літерами латинської абетки за винятком літер I та O.

У разі повного використання літер української та латинської абеток допускається позначення додатків арабськими цифрами.

Якщо у КР один додаток, то він позначається “Додаток А”.

Кожний додаток слід починати з нової сторінки із зазначенням угорі в середині сторінки слова “Додаток” і його позначенням, а під ним у дужках для обов'язкового додатка друкують слово “обов'язковий”, а для інформаційного – “рекомендований” чи “довідковий”. Додаток мусить мати заголовок, який друкують симетрично відносно тексту з великої літери окремим рядком.

Текст кожного додатка за необхідності може бути поділений на розділи, підрозділи, пункти, підпункти.

Запозичена з літературних чи статистичних джерел інформація (формули, таблиці, схеми, графіки, висновки тощо) потребує обов'язкових посилань (у квадратних дужках) на порядковий номер джерела у списку використаних джерел та номери сторінок, з яких узято інформацію.

5.7. ІЛЮСТРАЦІЇ

Усі ілюстрації у записці у вигляді креслень, ескізів, схем, графіків, діаграм, фотографій та ін. називаються рисунками. Ілюстрації можуть бути розташовані на окремих аркушах або безпосередньо в тексті записки.

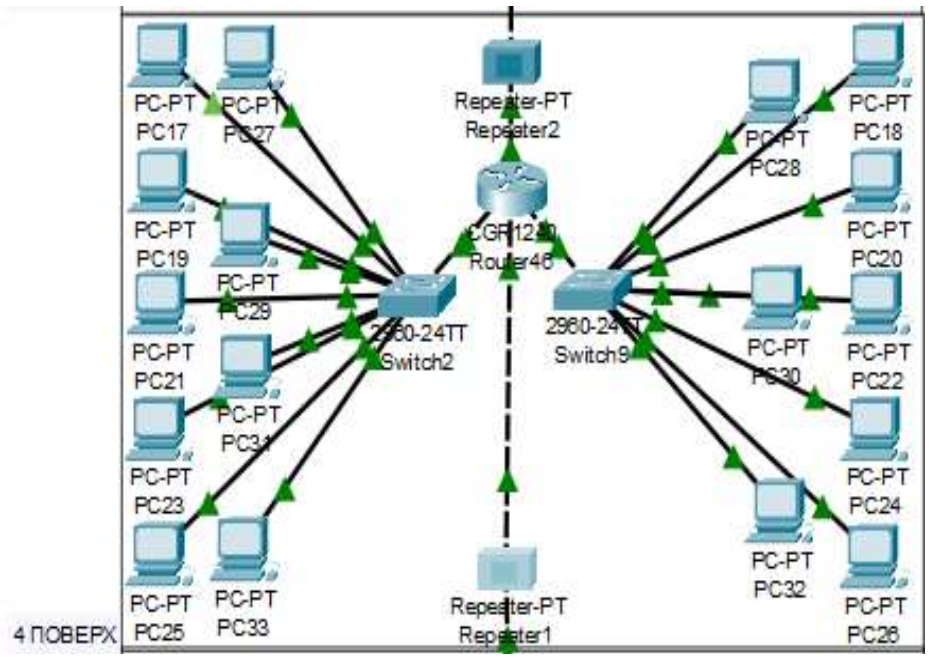

Рис. 2.16. Архітектура сегмента комп’ютерної мережі, побудованої для 5-поверху будівлі №4

Ілюстрації слід розміщувати у ПЗ безпосередньо після тексту, де вони згадуються вперше, або на наступній сторінці. На усі ілюстрації повинні бути посилання в тексті ПЗ, наприклад: «наведено на рис. 4.1». За необхідності під ілюстрацією розміщують пояснювальні дані. Ілюстрація позначається словом «Рисунок», яке разом з назвою ілюстрації розміщують після пояснювальних даних, наприклад, «Рис. 2.16. Архітектура сегмента комп’ютерної мережі,

побудованої для 5-поверху будівлі №4». Ілюстрації слід нумерувати арабськими цифрами порядковою нумерацією в межах розділу, за винятком ілюстрацій, наведених у додатках. Номер ілюстрації складається з номера розділу і порядкового номера ілюстрації, відокремлених крапкою, наприклад, рисунок 2.16 − шістнадцятий рисунок другого розділу (приклад наведено).

Ілюстрації і назва ілюстрації (рисунка) розміщуються по центру сторінки. Від основного тексту зверху і знизу відділяються пустим рядком.

Якщо ілюстрація велика, то її дозволяється розміщувати на аркуші А4 в альбомній орієнтації, при цьому найменування розміщують під рисунком, а рамка основного напису залишається в стандартному положенні (вздовж короткої сторони аркуша А4). Не прийнято завершувати розділ рисунком.

5.8. Таблиці

Таблицю слід розташовувати безпосередньо після тексту, у якому вона згадується вперше, або на наступній сторінці.

Таблиці слід нумерувати арабськими цифрами порядковою нумерацією в межах розділу, за винятком таблиць, що наводяться у додатках.

Номер таблиці складається з номера розділу і порядкового номера таблиці відокремлених крапкою, наприклад, таблиця 3.1 − перша таблиця третього розділу. Номер таблиці від назви виділяють тире. Приклад оформлення таблиці наведено нижче на рисунку.

Таблиця 2.4. Загасання від середовища поширення сигналу

Найменування	**Од. вим.**	**Значення**
1	**2**	**3**
Вікно в цегляній стіні	дБ	2
Стекло в металевій рамі	дБ	6
Офісна стіна	дБ	6
Залізні двері в офісній стіні	дБ	7
Залізні двері в цегляній стіні	дБ	12,4
Скловолокно	дБ	0,5-1
Стекло	дБ	3-20
Дощ і туман	дБ/км	0,02-0,05
Дерева	дБ/м	0,35
Кабельна зборка pigtale	дБ	0,5
Смуговий фільтр NCS F24XXX	дБ	1,5
Коаксіальний кабель	дБ/м	0,3
Роз'їм N - type	дБ	0,75
Інжектор живлення	дБ	0,5

Таблиці кожного додатка позначають окремою нумерацією арабськими цифрами з додаванням перед цифрою позначення додатка.

На всі таблиці мають бути посилання в тексті, які складаються зі слова

“таблиця” із зазначенням її номера.

Заголовки стовпців і рядків таблиці слід друкувати з великої літери, підзаголовки стовпців з малої, якщо вони е продовженням заголовка, або з великої, якщо вони мають самостійне значення. У кінці заголовків і підзаголовків таблиць крапки не ставлять, заголовки і підзаголовки стовпців друкують в однині.

Таблиці ліворуч, праворуч і знизу, як правило, обмежують лініями.

Розділення заголовків і підзаголовків боковика і стовпців діагональними лініями не допускається.

Горизонтальні та вертикальні лінії, що розмежовують рядки таблиці, можна не креслити, якщо відсутність таких не ускладнює користування таблицею.

Заголовки стовпців, як правило, друкують паралельно рядкам таблиці. За необхідності допускається перпендикулярне розміщення заголовків стовпців.

Допускається розміщення таблиці вздовж довгого боку аркуша.

Якщо рядки або стовпці таблиці виходять за формат сторінки, то таблицю ділять на частини, які розміщують одна під одною або поряд, при цьому в кожній частині таблиці повторюють її головку й боковик.

Якщо в кінці сторінки таблиця переривається і її продовження буде на наступній сторінці, то в першій частині таблиці нижню горизонтальну лінію, що обмежує таблицю, не креслять.

6. КРИТЕРІЇ ОЦІНЮВАННЯ КУРСОВОЇ РОБОТИ

Оцінка за курсову роботу складається із суми балів, які виставляються комісією на основі розгляду змісту ПЗ і графічного матеріалу та за підсумком усного захисту перед комісією основних положень, які розглянуті в курсовій роботі. Підсумкова оцінка знань, умінь та навичок студента, набутих при проєктуванні КР, встановлюється за 100-бальною шкалою із подальшим переведенням її у наступну шкалу оцінок:

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	Значення оцінки
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов’язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов’язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	Значення оцінки
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного виконання курсової роботи

7. ПІДГОТОВКА ДО ЗАХИСТУ КУРСОВОЇ РОБОТИ

Після завершення написання курсової роботи студент подає та реєструє роботу на кафедрі із зазначенням строку здачі у спеціальному журналі (під розпис студента).

Якщо робота допущена до захисту студент повинен ознайомитись із відзивом і підготуватись до захисту. При цьому він повинен підготувати відповіді на питання згадані у відгуку й показати усунені недоліки.

Захист курсової роботи проводиться перед початком екзаменаційної сесії. Процедура захисту передбачає стислий виклад студентом головних проблем дослідження роботи та їх рішення упродовж 10-15 хвилин, відповіді на запитання.

При оцінці курсової роботи береться до уваги:

- ✓ зміст і складність роботи;
- ✓ якість виконання;
- ✓ відповідність роботи щодо її оформлення;
- ✓ набуті студентом навички пов'язувати теоретичні знання з питаннями їх практичного застосування;
- ✓ повнота та точність відповідей на поставлені запитання.

Оцінка виконання КР виставляється у заліковій книжці студента, реєструється на спеціальному бланку та на титульному листі.

8. ДОТРИМАННЯ ПРИНЦИПІВ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

При виконанні курсової роботи студенти повинні дотримуватись принципів академічної доброчесності. Курсову роботу студент має виконувати самостійно. Необхідно дотримуватись етики цитування, давати посилання на використані джерела, подавати достовірну інформацію про виконану роботу та її результати. У разі виявлення порушення студентом академічної доброчесності, зокрема академічного плагіату, фабрикації, фальсифікації,

кваліфікаційна робота не допускається до захисту, а якщо такі факти були виявлені під час захисту, робота оцінюється на «незадовільно».

Студент зобов’язаний у терміни, визначені графіком освітнього процесу та розкладом екзаменів, допрацювати роботу та ліквідувати академічну заборгованість у визначеному порядку.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

2. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах: навч. посіб. – Кропивницький: Видавець Лисенко В. Ф., 2020. – 295 с.

3. Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Балюнов О.О. Захист інформації в комп'ютерних системах: підручник. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. – 236 с.

4. Вишняков В.М. Захист інформації в комп'ютерних системах: навч. посіб. / В.М. Вишняков. – Київ: КНУБА, 2022. – 120 с.

5. Пашорін В.І., Костюк Ю.В. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ : Держ. торг.-екон. ун-т, 2023. – 376 с.

Додатковий

5. Г.М. Гулак, О.Б. Жильцов, П.М. Складанний, Р.В. Киричок, Н.В. Коршун. Інформаційна та кібернетична безпека підприємства / Навчальний підручник. КУБГ. – К. 2022. 451с.

6. Технології захисту інформації / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці: Чернівецький національний університет, 2013. – 471 с.

7. Безпека інформації: конспект лекцій / укладач О. С. Кушнерьов. – Суми: Сумський державний університет, 2021. – 99 с.

8. Лемешко А.В. Проєктування безпроводових комп'ютерних мереж: навч. посібник / А.В. Лемешко, Л.А. Кирпач, Д.В. Сорокін, І.А. Бученко, М.М. Шрам. – К.: ДУТ, 2021. — 147 с.

9. Основи інформаційної безпеки [Текст]: навч. пос. / Дудикевич В. Б., Хорошко В.О., Яремчук Ю.Є. – Вінниця: ВНТУ, 2018. – 316 с.

10. О.Д. Азаров. Комп'ютерні мережі: підручник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.]. − Вінниця: ВНТУ, 2020. − 378 с

Інтернет-ресурси

10. Курси Cisco Packet Tracer. https://www.netacad.com/ua/courses/packet-tracer

ДОДАТКИ

ДОДАТОК А

Київський столичний університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

КУРСОВА РОБОТА
З ДИСЦИПЛІНИ
«ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ»
НА ТЕМУ:
РОЗРОБКА ЗАХИЩЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ …….

Студента (ки) _____ курсу ___ _____ ___ групи
освітньої програми 123.00.01 Комп'ютерна інженерія
спеціальності 123 Комп'ютерна інженерія
_____
(ПІБ)
Науковий керівник: _____
_____
(посада, вчене звання, науковий ступінь, ПІБ)

Національна шкала _____

Кількість балів: _____ Оцінка: ECTS_____

_____ _____
(підпис) (ім'я, прізвище)

Київ 20___

ДОДАТОК Б

Київський столичний університет імені Бориса Грінченка

Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Дисципліна Захист інформації в комп`ютерних системах та мережах

Курс _____ Група _____Семестр____

Затверджую
Завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
к.т.н., доц. Складанний П.М.
«___ » _____

ЗАВДАННЯ
на курсову роботу студента

_____
(прізвище, ім'я, по батькові)

1. Тема курсової роботи_____
_____
_____
2. План курсової роботи_____
_____
_____
_____
_____
_____
3. Перелік графічного матеріалу _____
_____
4. Термін подання студентом завершеної курсової роботи на кафедру _____
5. Термін захисту курсової роботи _____
6. Дата видачі завдання _____

Студент_____
(підпис) (ім'я, прізвище)
Науковий керівник _____ _____
(підпис) (ім'я, прізвище)

Завідувач кафедри ___ _____ _____
(підпис) (ім'я, прізвище)

ДОДАТОК В

Київський столичний університет імені Бориса Грінченка

Рецензія на курсову роботу і результат захисту

Студента _____
(прізвище, ім'я та по батькові)

III курсу ____ групи факультету інформаційних технологій та математики

Курсова робота з з дисципліни «Захист інформації в комп`ютерних системах та мережах»

Тема _____

Реєстраційний № _____, дата одержання «____» __ _____ 20___ р.

Науковий керівник _____
(вчене звання, прізвище, ініціали)

Зміст рецензії

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
_____
_____
_____

Допущено до захисту «___»_____ 20____ р.

Захист планується «_____»_____20____ р.

_____
(підпис наукового керівника)

Курсова робота захищена «_____» _____20____р.

з оцінкою _____
(за національною шкалою та шкалою ЄКТС)

_____ PhD, Юлія КОСТЮК
(підпис) (ім'я, прізвище)

Приклад анотації

АНОТАЦІЯ

Курсова робота виконана студентом Івановим Іваном Івановичем на тему «Розробка захищеної корпоративної комп’ютерної мережі підприємства» присвячена розробці захищеної корпоративної комп’ютерної мережі підприємства, з акцентом на забезпеченні конфіденційності, цілісності та доступності інформації.

В роботі розглядаються сучасні підходи до захисту комп’ютерних систем і мереж, включаючи апаратні та програмні засоби, шифрування даних, управління доступом та автентифікацію користувачів, а також впровадження систем виявлення і запобігання вторгненням. Оскільки зростання кількості загроз і кібернападів створює серйозні виклики для безпеки таких мереж, тому вимагає впровадження надійних заходів для захисту інформації.

Забезпечення конфіденційності, цілісності та доступності даних стає першочерговим завданням для підприємств, що прагнуть зберегти свою конкурентоспроможність і уникнути можливих збитків від витоку інформації.

Окрема увага приділяється розробці політик і процедур безпеки, спрямованих на мінімізацію ризиків та забезпечення стійкості корпоративної мережі до сучасних кіберзагроз. Результати дослідження сприятимуть підвищенню рівня захисту інформації на підприємствах та забезпеченню безперебійної роботи їхніх інформаційних систем.

Робота складається зі вступу, чотирьох розділів, висновків та пропозицій, списку використаних джерел, який складається з 17 найменувань, 8 додатків. Робота містить 5 рисунків і 8 таблиць. Загальний обсяг роботи становить 38 сторінок

Метою курсової роботи є розробка захищеної корпоративної комп'ютерної мережі підприємства, яка забезпечить надійний захист інформації від несанкціонованого доступу, кібератак та інших загроз, а також гарантуватиме безперебійну роботу і безпечний доступ до критично важливих даних. Модель, розроблена в прикладному пакеті PacketTracer, може використовуватись для побудови справжньої мережі на підприємстві.

Об’єктом дослідження є орпоративна комп'ютерна мережа підприємства, її структура, технологічні рішення та засоби забезпечення інформаційної безпеки.

Ключові слова: захищена комп'ютерна мережа, інформаційна безпека, корпоративна мережа, кіберзагрози, шифрування даних, управління доступом, автентифікація, системи виявлення і запобігання вторгненням.

ДОДАТОК Г

Приклад оформлення

Перелік умовних позначень, символів, одиниць, скорочень і термінів

КМ – комп’ютерна мережа
ОС – операційна система
ПП – патч-панель
СКС – структурована кабельна система
ТЗ – технічне завдання
ТР – комунікаційний роз'єм
ПК – персональний комп’ютер
ПЗ – програмне забезпечення
DMZ (Demilitarized Zone) – технологія забезпечення захисту інформаційного периметра, при якій сервери, що відповідають на запити з зовнішньої мережі, перебувають в особливому сегменті мережі і обмежені в доступі до основних сегментів мережі за допомогою брандмауера
ICMP (Internet Control Message Protocol) – мережевий протокол, що використовується для передачі повідомлень про помилки й інші виняткові ситуації, що виникли при передачі даних
SNMP (Simple Network Management Protocol) – це протокол керування мережами зв'язку на основі архітектури TCP/IP
STP (Spanning Tree Protocol) – мережевий протокол, основним завданням STP є приведення мережі Ethernet з множинними зв'язками до деревоподібної топології, що виключає цикли пакетів
VLAN (Virtual Local Area Network) – це логічні підгрупи мережі, створені програмним шляхом.

Шаблон для формування змісту

ЗМІСТ

ДОДАТОК Ж

Структура вступу до курсової роботи:

1. **Вступна частина** (не більше 1-го абзацу або 2-3 пропозиції) – описується загальний стан розглянутої теми.

2. **Актуальність теми дослідження** – тут слід написати про важливість вивчення даної теми в даний час. Тобто пояснити, чому ви вибрали саме це тему і що дозволить зробити її вивчення.

3. **Мета курсової роботи**. Це може бути: вивчення, опис, визначення, встановлення, дослідження, розгляд, розробка, розкриття, освітлення, виявлення, аналіз, узагальнення чого-небудь.

4. **Завдання дослідження** – вони пишуться для того, щоб за допомогою їх вирішення можна було досягти мети, яку ми ставимо в роботі. Тобто для досягнення мети роботи слід вивчити, описати, показати, визначити, встановити, досліджувати, розглянути, розробити, розкрити, висвітлити, виявити, проаналізувати, довести, узагальнити що-небудь.

5. **Об'єкт і предмет дослідження**. Об'єкт включає в себе предмет, а не навпаки. Адже предмет говорить про більш вузький сектор дослідження і змушує нас конкретизувати область дослідження.

6. **Огляд літератури.** У цій частині введення слід вписати тих авторів, праці яких використовувалися при написанні курсової, і коротко описати, що вони вивчали. При цьому важливо вказати також і тих авторів, які були рекомендовані науковим керівником.

7. **Опис структури курсової роботи.** Тут варто вказати всі розділи, які містить курсова робота і що в них розглянуто.

Приклад вступу до курсової роботи подано нижче.

ВСТУП

Електронна пошта, в даний час, є одним з найважливіших інформаційних ресурсів мережі Internet – засобом електронних комунікацій, основним призначенням якої є можливість спілкуватися користувачам один з одним.

Фактично появу електронної пошти можна віднести до 1965 року, коли співробітники Массачусетського технологічного інституту (MIT) Ноель Моррiс і Том Ван Вабив написали програму MAIL для операційної системи CTSS (Compatible Time-Sharing System), яка була встановлена на комп'ютері IBM 7090/7094.

Потім, протягом багатьох років створювалися нові поштові програми, які постійно вдосконалювалися.

Наприклад, в 1971 році Рей Томлінсон, співробітник компанії "Bolt Beranek and Newman, Inc." (BBN), розробив поштову програму для пересилки

повідомлень по розподіленої мережі. А в 1972 році, він же модернізував її, адаптувавши для використання в мережі ARPANET, яка була попередницею нинішньої мережі Інтернет. Саме в цей час в адресах електронної пошти став використовуватися символ «@».

Перша ж програма, яка дозволяла створювати і сортувати списки листів, зберігати повідомлення в файлі, а також пересилати електронні листи на іншу адресу або автоматично відповідати на отримане послання, була розроблена вже Ларрі Робертсом.

Поступово налаштовувалася електронний поштовий зв'язок між різними країнами і континентами, дозволяючи людям обмінюватися електронними листами на величезних відстанях.

У міру зростання популярності електронної пошти стали з'являтися також різні шкідливі об'єкти, які роблять пошту вразливою, такі як віруси і спам, поширювані через мережу.

Перший спам був розісланий в 1994 році, будучи тоді першої розсилкою рекламних оголошень, які мають зараз своє поширена назва і статус – розсилки "засмічують" поштові скриньки користувачів непотрібною інформацією.

Таким чином, електронний спосіб відправлення та отримання листів не здає своїх позицій і, на сьогоднішній день, мільйони людей використовують електронну пошту як спосіб зв'язку.

Актуальність. У сучасних умовах життя, коли необхідно швидко реагувати на події, що відбуваються в світі, використання електронної пошти незамінне. Особливо це стосується ділової сфери. Електронна пошта може застосовуватися в різних цілях. Наприклад, для інформаційної підтримки споживачів або рекламування товарів і послуг.

У зв'язку з цим використання електронної пошти є актуальним. Вона повинна забезпечувати користувачеві виконання всіх основних функцій:

– Доставку листів;

– Відправлення повідомлень.

З використанням електронної пошти, з'явилася необхідність вивчення основних її характеристик і принципів роботи, а також способів захисту від шкідливих об'єктів.

Мета курсової роботи – охарактеризувати поняття «електронна пошта» і вивчити принципи її роботи.

Завдання курсової роботи:

– Розкрити поняття «електронна пошта»

– Показати основні переваги використання електронної пошти;

– Виявити недоліки електронної пошти;

– Виявити необхідність в захисті електронної пошти від вірусів і спаму;

– Визначити основні шляхи вирішення проблеми захисту поштової скриньки.

– Вивчити, на підставі, яких протоколів функціонує сервіс електронної пошти.

Об’єктом дослідження процес забезпечення безпеки електронної поштаи в цілому.

Предмет дослідження – підходи, методи та інструменти забезпечення безпеки роботи електронної пошти, її програмних і апаратних компонентів.

Огляд літератури. В ході написання курсової роботи були використані літературні джерела наступних авторів: Гаєвський, А., Жуков А.С., Попов В.Б., Саврасенко А.А., Романенко В.В.

ДОДАТОК К

ЗРАЗКИ ОФОРМЛЕННЯ БІБЛІОГРАФІЧНИХ ОПИСІВ У СПИСКУ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мінухін С. В. Кавун С. В. Знахур С.В Комп’ютерні мережі. Навчальний посібник Харків, ХНЕУ, 2008. – 210с.

2. О.Д Азаров, С.М. Захарченко, О.В. Кадук, М.М. Орлова, В.П. Тарасенко Комп'ютерні мережі. - Підручник -Вінниця, ВНТУ, 2020.−378с.

3. Вершина А.И. Модель отримання знань / А.И. Вершина, Г.Г. Киричек // Тиждень науки: наук.-техн. конф., 19-23 квіт. 2010 р.: тези доп. – Запоріжжя: ЗНТУ, 2010. – Т. 2. – С.115–116.

4. Біленчук П.Д. Комп’ютерна злочинність / П.Д. Біленчук, Б.В. Романюк, В.С. Цимбалюк та ін. – К. : Атіка, 2002. – 240 с.

5. Мосіяшенко В.А. Мережі [Текст] : навч. посіб. / В. А. Мосіяшенко. — Суми : Унів. кн., 2005. — 174 с.—ISBN 966-680-198-1.

6. Лєпа Є.В. Системи підтримки прийняття рішень. Частина 1 / Є.В. Лєпа, Є.К. Міхеєв, В.В. Крініцин. // Навчальний пособник.– Херсон, 2006. – 324 с.

7. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання [Текст] : (ГОСТ 7.1—2003, IDT) : ДСТУ ГОСТ 7.1:2006. — Чинний з 2007—07—01. — К. : Держспоживстандарт України, 2007. — 47 с. ; 29 см. — (Система стандартів з інформації, бібліотечної та видавничої справи) (Національний стандарт України).

ДОДАТОК Л

ПРИКЛАД ЗАЯВИ НА ЗАТВЕРДЖЕННЯ ТЕМИ КУРСОВОЇ РОБОТИ

Завідувачу кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
к.т.н., доц. Складанному П.М.
студента групи_______
спеціальності 123 «Комп'ютерна інженерія»
Іанова Івана Івановича

ЗАЯВА

Прошу затвердити тему курсової роботи «Розробка захищеної комп'ютерної мережі з використанням технології Ethernet» з дисципліни «Захист інформації в комп`ютерних системах та мережах» та призначити керівником курсової роботи Костюк Ю.В.

«_____»_____ _____