

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Запорізький національний технічний університет

МЕТОДИЧНІ ВКАЗІВКИ

до виконання курсового проекту з дисципліни

"Проектування комп'ютерних мереж"

для студентів спеціальності 8.05010203 "Спеціалізовані комп'ютерні системи" та 8.05010201 "Комп'ютерні системи та мережі", усіх форм навчання

Методичні вказівки до виконання курсового проекту з дисципліни "Проектування комп'ютерних мереж" для студентів спеціальності 8.05010203 "Спеціалізовані комп'ютерні системи" та 8.05010201 "Комп'ютерні системи та мережі", усіх форм навчання // Укл. Г.Г.Киричек. - Запоріжжя: ЗНТУ, 2015. - 54с.

Укладач:

Г.Г. Киричек, доцент, к.т.н.

Рецензент:

Р.К. Кудерметов, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ

Протокол № 3
від 05 жовтня 2015 року

ЗМІСТ

1 ЗАГАЛЬНІ ВІДОМОСТІ	4
1.1 Календарний план та отримання завдання	4
1.2 Вимоги до змісту розділів, оформлення та обсягу пояснювальної записки	6
1.3 Теми проектів	9
1.4 Порядок захисту курсового проекту	10
2 СТРУКТУРА КУРСОВОГО ПРОЕКТУ	11
2.1 Аналіз технічного завдання	12
2.2 Вибір технологій LAN\WAN сегментів та обладнання об'єднаної мережі підприємства	13
2.3 Планування структури кожної ЛОМ об'єднаної мережі	15
2.4 Підключення до Інтернету	18
2.5 Вибір маршрутизатору та постачальника послуг Інтернету	20
2.6 З'єднання через маршрутизатори окремих віддалених ЛОМ підприємства	21
2.7 Віддалений доступ до мережі	22
2.8 Вибір операційної системи та обладнання	23
2.9 Забезпечення мережевої безпеки	25
2.10 Забезпечення мережевої безпеки в бездротових ЛОМ	29
2.11 Призначення IP-адрес	31
2.12 Подання мережі головного офісу організації в Інтернеті	35
3 ЗАГАЛЬНІ ВИМОГИ ДО ОФОРМЛЕННЯ ПРОЕКТУ	37
3.1 Вимоги до оформлення пояснювальної записки	37
3.2 Вимоги до оформлення графічних документів	38
3.3 Схеми алгоритмів, програм, даних та систем	39
3.4 Вимоги до виконання електричних схем	41
РЕКОМЕНДОВАНА ЛІТЕРАТУРА	43
Додаток А	44
Додаток Б	45
Додаток В	46
Додаток Е	49

1 ЗАГАЛЬНІ ВІДОМОСТІ

Мета роботи – одержання практичних навичок розробки об'єднаних комп'ютерних мереж (КМ) та аналіз їх функціонування у сучасному середовищі. Вміння проектувати та адмініструвати, як локальні так і об'єднані мережі рівня масштабу підприємства. Отримання практичних знань з організації доступу до мережі Internet. А також: узагальнення, закріплення та поглиблення теоретичних та практичних знань зі спеціальності; використання цих знань для обґрунтованого прийняття проектних рішень та для вирішення конкретних задач; практичне закріплення навичок розробки комп'ютерних мереж рівня масштабу підприємства.

Завдання до курсового проекту передбачають розробку структурної схеми об'єднаної мережі підприємства (загальна кількість кінцевих вузлів не менше 250), планування топології кожної локальної обчислювальної мережі (ЛОМ) з яких складається об'єднана мережа, призначення IP-адрес, планування дозволу імен, з'єднання через маршрутизатори окремих ЛОМ підприємства, здійснення віддаленого доступу до мережі та забезпечення мережевої безпеки, як у дротових так і в бездротових ЛОМ.

На всіх етапах проектування необхідно проводити оцінку альтернативних варіантів побудови КМ та її окремих частин.

1.1 Календарний план та отримання завдання

Систематичне і своєчасне виконання роботи – запорука одержання якісного результату і високої оцінки.

Рекомендований графік роботи наведено в таблиці 1.1. Студент може корегувати графік в межах наведених дат, не змінюючи дати захисту.

Таблиця 1.1- Етапи виконання курсового проекту

№ п/п	Назва етапів курсового проекту	Термін виконання
1	Отримання технічного завдання	до 20.09
2	Аналіз технічного завдання	21.09 – 27.09
3	Робота з літературою	28.09 – 3.10
4	Розробка функціональної схеми мережі	04.10 – 09.10
5	Вибір технологій локальних і глобальних сегментів об'єднаної мережі	10.10 – 15.10
6	Розробка структурної схеми об'єднаної мережі підприємства	16.10 – 21.10
7	Вибір і налаштування маршрутизаторів, згідно політики безпеки об'єднаної мережі підприємства і ISP (постачальника послуг Інтернет), отримання пулу відкритих адрес	22.10 – 27.10
8	Організація віддаленого доступу до мережі	28.10 – 03.11
9	Вибір та налаштування роботи протоколів маршрутизації	04.11 – 10.11
10	Вибір та розміщення мережевого і клієнтського обладнання	11.11 – 15.11
11	Вибір та налаштування ОС	16.11 – 19.11
12	Забезпечення мережевої безпеки	20.11 – 22.11
13	Призначення IP-адрес та DNS-імен	23.11 – 25.11
14	Монтаж мережі. Об'єднання віддалених сегментів	26.11 – 29.11
15	Оформлення ПЗ та захист КІ	29.11 – 06.12

У відповідності до теми керівник видає технічне завдання на курсовий проект з вказівкою термінів виконання окремих етапів та всього проекту в цілому.

У завданні повинно бути чітко визначено такі данні: назва проекту, призначення комп'ютерної мережі, що розробляється, вихідні данні до

проектування та умови експлуатації, перелік загальних питань, які розглядаються та відображаються в проекті.

Календарний графік виконання курсового проекту, який складається студентом (за прикладом календарного плану) і затверджується керівником проекту, повинен відповідати етапам розробки, вивченню та аналізу загальних питань стосовно до всього об'єкту проектування в цілому.

1.2 Вимоги до змісту розділів, оформлення та обсягу пояснювальної записки

До пояснювальної записки необхідно включати матеріал, який безпосередньо відноситься до конкретної комп'ютерної мережі, що підлягає проектуванню, у відповідності до технічного завдання. Не рекомендується робити великі реферативні огляди. При необхідності можна робити посилання на відповідну літературу. Основний зміст записки – це обґрунтування прийнятих рішень та проект об'єднаної мережі, згідно затвердженої назви. При цьому треба мати на увазі, що записку складають тоді, коли розробку проекту 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, іншими матеріалами, які обґрунтовують прийняті рішення.

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.

У рефераті проектант вказує мету, задачі, технології, вид обладнання, протоколи та стандарти, які використані у розробленому

проекті. Наводить ключові слова та об'єм пояснювальної записки. Реферат рекомендовано оформити на заключному етапі (1 сторінка).

У вступі проєктант повинен висвітлити загальний стан питання, яке розглядається, обґрунтовувати необхідність і можливість його вирішення, описати зв'язок з виробничими задачами, а також обґрунтувати актуальність теми проєкту. 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.

У першому розділі (5-7 сторінок) ПЗ необхідно провести аналіз технічного завдання, розглянути структуру підприємства в цілому, визначити яке обладнання потребує заміни, а яке необхідно придбати додатково для підключення віддалених сегментів об'єднаної мережі. Студент повинен визначити коло задач, які необхідно вирішити в курсовому проєкті, а також сформулювати технічне завдання згідно діючих стандартів та оформити його окремим підрозділом.

У другому розділі (5-8 сторінок) на підставі проведеного аналізу розробляються функціональна та структурна схема об'єднаної мережі підприємства, виконується обґрунтування вибору та опис LAN\WAN-технологій окремих сегментів об'єднаної мережі. Кількість підключених робочих станцій не повинна бути меншою за 250 одиниць.

Третій розділ (5-8 сторінок) повинен містити опис апаратної та кабельної частини проєкту з урахуванням попереднього вибору та можливості з'єднання через маршрутизатори окремих ЛОМ підприємства, з метою здійснення віддаленого доступу. Цей розділ містить вибір конкретних елементів реалізації функціональної та принципових електричних схем, розрахунок окремих елементів, вузлів та підсистем.

У четвертому розділі (4-7 сторінок) розкриваються питання вибору операційних систем робочих станцій та серверів, які в подальшому підтримають функціонування загальних сегментів мережі та об'єднаної мережі в цілому.

У п'ятому розділі (4-6 сторінок) розглядається підключення розробленої мережі підприємства до Internet.

Питання забезпечення мережевої безпеки, як у дротових так і в бездротових ЛОМ треба розглянути в наступному розділі (4-7 сторінок) пояснювальної записки. Проектантом розкриваються питання забезпечення якості та надійності розробленої мережі, питання апаратного та програмного захисту інформації, а також захист від несанкціонованого доступу.

У сьомому (3-5 сторінок) розділі розглядається призначення IP-адрес та подання мережі головного офісу організації (підприємства) в Інтернеті.

У висновках (1-2 сторінки) формулюються основні результати, що отримані під час виконання курсового проекту.

Оформлення записки здійснюється у відповідності до діючих стандартів ДСТУ 3008-95 “Документація. Звіти в сфері науки і техніки”, Єдиної Системи Конструкторської Документації (ЄСКД), у тому числі, у відповідності до ГОСТ 19.701-90 (Схемы алгоритмов, программ, данных и систем), ГОСТ 19.401-78 (Текст програми), ГОСТ 19.402-78 (Опис програми). 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 А.

До записки додаються два креслення формату А4 (структурна та монтажна схеми) та 1 плакат (функціональна схема мережі) того ж формату. Креслення і плакати повинні відображати проходження кабелю на всіх ділянках мережі з роз'ясненням особливостей його прокладки. Ці плакати, як доповнення до основних, треба розробляти для мереж масштабу підприємства, району, області, регіону.

Загальний обсяг ПЗ – не менше 40 сторінок (не рекомендовано обсяг більший за 50 стор.), причому технічна її частина, має містити не менш ніж 30 сторінок тексту з рисунками. Рисунки можуть містити необхідні для пояснень і розрахунків фрагменти загального креслення мережі.

1.3 Теми проектів

Далі наведено приклади тем проектів.

1. Комп'ютерна мережа металургійного підприємства ВАТ „Запоріжсталь”.
2. Безпроводна мережа адміністративного сегменту ВАТ „Мотор-Січ”.
3. Корпоративна мережа супермаркетів „Сільпо”.
4. Комп'ютерна мережа підприємства «Дніпровська електроенергетична система» на основі технології NGN.
5. Корпоративна мережа державного підприємства „Екологія України”.
6. Комп'ютерна мережа фірми «Радіоком» міста Запоріжжя.
7. Кампусна комп'ютерна мережа для мешканців мікрорайону.
8. Корпоративна комп'ютерна мережа банку.
9. Оптиволоконна мережа ВАТ „Дніпроспецсталь”.
10. Корпоративна мережа агропромислового комплексу „Україна”.
11. Комп'ютерна мережа концерну „Теплові мережі України”.
12. Об'єднана комп'ютерна мережа торговельного підприємства „Центромеблі”.
13. Корпоративна мережа Запорізької філії ВАТ «Укртелеком».
14. Розподілена мережа підприємства на базі ADSL та VPN-технологій.
15. Комп'ютерна мережа комунального підприємства «Водоканал».
16. Комп'ютерна мережа ЗАТ «Запорізький залізорудний комбінат».
17. Розподілена комп'ютерна мережа підтримки проведення соціологічних досліджень.
18. Комп'ютерна мережа пенсійного фонду України.

19. Об'єднуюча магістраль енергетичного комплексу ВАТ „УкрЕнерго”.
20. Віртуальна приватна мережа.
21. Комп'ютерна мережа підприємства з використанням технологій Wi-Fi.
22. Комп'ютерна мережа фірми з підвищеною надійністю Internet з'єднання.
23. Цифрова кабельна мережа на базі DVB-C.
24. Корпоративна мережа регіональних лікарень України.

1.4 Порядок захисту курсового проекту

Призначення захисту – оцінити складність розробленого проекту, кваліфікацію проектанта і ступінь самостійності його праці.

Захист відбувається за графіком у присутності комісії з двох викладачів, один з яких є керівником курсового проекту. На доповідь дається 4-5 хвилин. За цей час необхідно стисло викласти зміст поставленої задачі (одна хвилина), доповісти про власну роботу щодо розробки комп'ютерної мережі підприємства (2-3 хвилини) і зробити висновки (одна хвилина).

Необхідно розповідати про свою власну роботу, пояснювати, чому прийнято саме такі рішення при проектуванні мережі, на основі яких міркувань було обрано те або інше апаратне та програмне забезпечення, сформовано ті або інші ЛОМ об'єднаної мережі підприємства.

Після закінчення доповіді учасники комісії можуть задавати питання, призначення яких – уточнити рівень кваліфікації і ступінь самостійності доповідача. На питання необхідно давати стислі прямі відповіді, при необхідності ілюструючи їх відповідними кресленнями.

2 СТРУКТУРА КУРСОВОГО ПРОЕКТУ

В процесі проектування мережі рівня підприємства студенту рекомендовано розглянути наведені нижче питання, тримаючись загального плану проекту.

Основні етапи проектування можуть включати.

1. Аналіз технічного завдання:

- аналіз структури підприємства (з описом основних підрозділів і філій, з урахуванням їх віддаленості один від одного);
- аналіз інформаційних потоків (типи переданих даних);
- аналіз (для модернізації) наявних апаратних і мережевих пристроїв;
- постановку завдань, пов'язаних з проектуванням та шляхи їх вирішення.

2. Вибір технологій, апаратних і мережевих пристроїв:

- короткий аналіз, наявних LAN і WAN технологій і вибір технологій (певних специфікацій) для конкретних ліній зв'язку між сегментами та мережами вашої організації, з урахуванням підключення філій;
- вибір мережевих пристроїв з визначенням технічних характеристик для кожного конкретного пристрою або групи ідентичних пристроїв, опис їх призначення та особливості застосування;
- вибір апаратних пристроїв (сервери, ПК, ноутбуки, термінали, планшети, IP-телефони та ін.) З описом технічних характеристик для кожного пристрою або групи пристроїв, опис призначення та особливості застосування.

3. Монтаж мережі:

- визначення основних LAN і WAN сегментів;
- проектування структурної схеми мережі;
- побудова монтажної схеми (розміщення мережевих і апаратних пристроїв (в будівлях, на поверхах, в кімнатах));
- розрахунок кабелю і потужності антен;
- підключення (об'єднання мережевих і апаратних пристроїв єдиною мережу).

4. Адміністрування мережі.

- вибір і опис операційних систем серверів та ПК;
- вибір принципу адресації для LAN і WAN сегментів (мереж);
- вибір принципів маршрутизації (опис особливостей роботи обраних протоколів маршрутизації);
- програмна настройка всього мережевого обладнання (з урахуванням адресації і маршрутизації);
- опис настроювання віддаленого доступу до філіям;
- підключення до Інтернет;
- забезпечення мережевої безпеки (налаштування обладнання, протоколів).

Кількість і назви розділів у проекті можуть відрізнятися від наведених далі, послідовність розташування розділів може бути іншою але це не повинно впливати на загальну мету проектування.

2.1 Аналіз технічного завдання

У цьому розділі пропонується провести детальний аналіз та огляд предметної області, визначити мету роботи та провести аналіз технічного завдання (ТЗ), окреслити задачі, які вирішуються при розробці об'єднаної комп'ютерної мережі, а також вказати, які особливості ТЗ визначили вибір тих чи інших рішень. Проектант повинен проаналізувати структуру підприємства, визначити типи даних, що передаються та наявність апаратних і мережевих пристроїв. Визначитись із шляхами вирішення завдань, які поставлені в процесі формування технічного завдання на проектування об'єднаної мережі підприємства.

2.2 Вибір технологій LAN\WAN сегментів та обладнання об'єднаної мережі підприємства

Зараз ви плануєте мережу, ви - головний, і вам ніхто не заважає. Дуже важливо продумати всі нюанси, пов'язані з побудовою мережі. Адже корпоративна мережа - це дуже складна система, яка складається з тисяч різних компонентів.

У корпоративній (об'єднаній) мережі завжди використовується 3-4 технології, як каналного рівня так і ті, які накладені поверх каналного рівня, тому можуть використовуватись і найрізноманітніші пристрої. Дуже важливо орієнтуватися у цьому устаткуванні. Модель маршрутизатора, яка була популярна торік, уже давно не є такою - на її місце прийшла більш нова, з кращими функціями та показниками, які дозволяють ефективніше використовувати всю систему в цілому.

Серверне приміщення - найважливіше приміщення корпоративної мережі. Хости та сервери можна розташовувати в мережі централізовано або в різних точках мережі. Групу серверів звичайно розташовують в машинній залі з контрольованим середовищем. Вона має спеціальне устаткування для фільтрації коливань силової напруги та підтримки температури в заданому діапазоні. Крім того, у ньому встановлюють системи архівації.

Поки мережа не стане настільки ж важливою, як робочі станції користувачів, вона повинна мати надлишкові маршрути та відповідати вимогам надійності для підтримки поетапної реалізації її плану. Тоді додаткові сегменти можуть додаватися в різних місцях, їх можна підключати до маршрутизатора при розширенні мережі в різних випадках.

Завдання ІТ-співробітників і сфери їхньої відповідальності повинні бути чітко розподілені. Звичайно ієрархія того або іншого підрозділу зображується у вигляді організаційної або пірамідальної діаграми.

Магістраль - один із самих головних і, отже, найдорожчих компонентів мережі. Через магістраль проходить більша частина трафіку мережі, тому вона впливає на роботу всієї мережі в цілому. Рішення про вибір магістралі є одним з найважливіших при плануванні мережі. Все частіше виникає необхідність у підвищенні пропускну здатності каналів між клієнтами мережі та серверами. Потужні комп'ютери дозволяють ефективно працювати з мультимедіа та передавати мультимедіа інформацію по мережі та Інтернету.

Вибір технології магістралі - це завжди компроміс між швидкістю та вартістю. Можна вибрати все швидкодіюче і дороге, але в деяких випадках застосування такого устаткування не виправдає себе. Канали, що зв'язують сервери та мережеве устаткування, повинні бути високошвидкісними, і їх варто ізолювати від тих сегментів, у яких розташовуються робочі станції.

Мережеве керування тісно пов'язане з моделлю, технологіями і топологією мережі, оскільки одними топологіями простіше управляти, чим іншими. У багатьох випадках зіркоподібна топологія забезпечує більш швидке виявлення проблем. Крім того, мережева структура, у якій використані комутатори та маршрутизатори, простіше для моніторингу та діагностики.

В Інтернеті можна скачати різні програми для планування вашої мережі. З їхньою допомогою ви накидаєте схему мережі, що допоможе потім при розгортанні мережі. Одна з таких програм: LanFlow (рис. 2.1). Скачати ознайомлювальну версію програми можна на сайті www.pacestar.com/lanflow.

Також ви можете скористатися програмою Visio, що є в пакеті офісних програм Microsoft або вже відомим з лабораторних робіт програмним забезпеченням Cisco Packet Tracer, яке дозволяє імітувати роботу різних мережевих пристроїв: маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп'ютерів, мережевих принтерів, IP-телефонів і т.д.

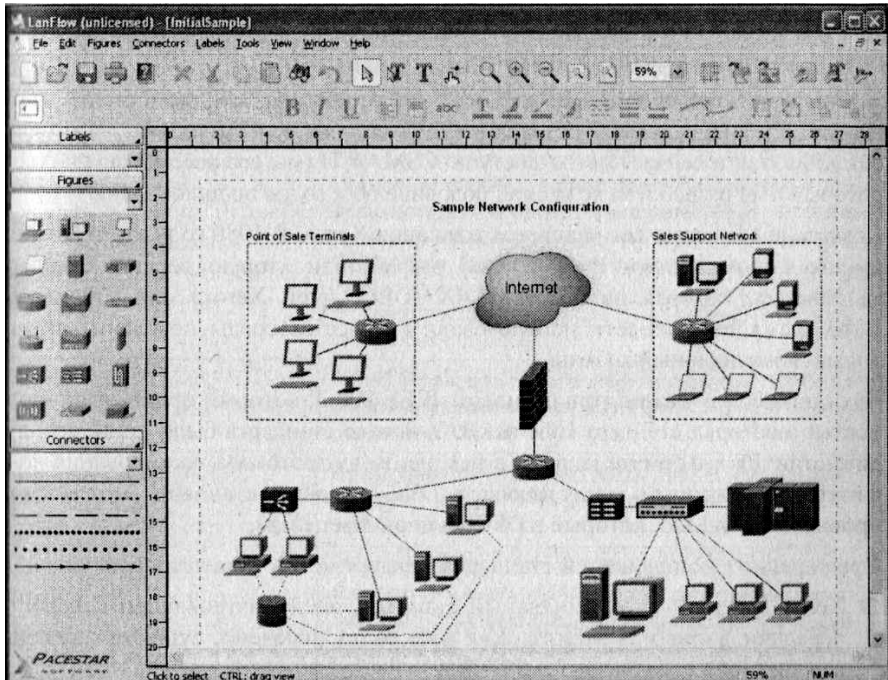


Рисунок 2.1 - Програма LanFlow

Загальні питання для розгляду [4,5].

1. Визначення кількості ЛОМ (як дротових так і бездротових), з яких складатиметься об'єднана мережа та вибір їх технологій.
2. Складання плану об'єднаної мережі з розбивкою на внутрішню (локальну) і зовнішню (демілітаризовану зону, периметр) частини.

2.3 Планування структури кожної ЛОМ об'єднаної мережі

Створення плану мережевої інфраструктури - найважливіша частина проектування мережі. Як правило, не всі елементи

інфраструктури мережі доводиться проектувати "з нуля", деякі з них успадковуються від інших елементів.

Планування інфраструктури набагато складніше інших етапів побудови мережі, оскільки припускає створення плану, що буде використаний для монтажу мережі і підтримки її надалі. На плані повинно бути зазначене розміщення основних компонентів мережі: кабельних ліній, комутаторів і інших комунікаційних пристроїв, а також комп'ютерів і периферії.

Знаючи, які протоколи обрані для мережі, можна приступати до планування розміщення мережевих ресурсів, тому що від протоколу залежить максимальна довжина кабелю і число комутаторів у мережі.

Вибір протоколу каналного рівня в основному зводиться до вибору типу несучого середовища: неекранованої витोї пари, оптоволоконного кабелю і частоти для бездротових каналів. Кожний тип має свої переваги та недоліки, які потрібно врахувати при виборі середовища передачі. Швидкість передачі - важливий критерій вибору протоколу каналного рівня.

Кабель UTP відносно дешевий і простий в установці, але чутливий до електромагнітних перешкод і має обмежену максимальну довжину. Оптоволоконні кабелі менш чутливі до електромагнітних перешкод і ослаблення сигналу в порівнянні з мідними кабелями, але дорожче і складніше в установці та обслуговуванні. Перш ніж включати бездротову технологію в інфраструктуру мережі, настійно рекомендується її ретельно протестувати на ділянці, де передбачається її використання. Самі різні фактори навколишнього середовища, товщина і матеріал стін будинку, близькість устаткування, електроприладів і навіть погодні умови створюють перешкоди для передачі даних у бездротовій мережі. Залежно від цих умов ефективний радіус дії бездротового пристрою може змінюватися ледве не щохвилино.

Схема кабельних з'єднань - важлива частина плану мережі, оскільки після монтажу мережі всі кабелі, швидше за все, будуть захищені. Крім самого кабелю, на плані необхідно вказати перешкоди,

які кабель огинає, а також розташування розеток і розподілених панелей.

TCP/IP - це пакет протоколів мережевого та транспортного рівнів, що став промисловим стандартом, підходить для більшості мереж.

При плануванні розміщення мережевих компонентів необхідно врахувати кілька критеріїв. Перший і головний - можливість доступу до устаткування, яке необхідне для виконання посадових обов'язків персоналу, тобто доступу до робочих станцій і периферійних пристроїв, таким як принтери та сканери.

Не у всіх офісах у кожного є свій стіл з комп'ютером. Іноді робочі станції перебувають у загальному доступі для різних співробітників. Для таких комп'ютерів необхідно вибрати та указати на плані зручне розміщення.

Розміщення серверів повинне бути зручним для тих, хто буде їх підтримувати та обслуговувати. У кожному разі захист серверів повинен бути надійним. Їх необхідно захищати не тільки від фізичного доступу, але також від стрибків напруги та перебоїв струму. Розміщення сервера повинне враховувати розташування робочих місць користувачів, характер трафіку і бути зручним для обслуговуючого персоналу.

Загальні питання для розгляду [2,4].

1. Вибір протоколу канального рівня.
 2. Вибір типу несучого середовища: неекранована вита пара, екранована вита пара, оптоволоконний кабель, бездротові канали.
 3. Вибір швидкості передачі.
 4. Вибір протоколів мережевого і транспортного рівнів.
- Складання структурних і монтажних схем для всіх ЛОМ об'єднаної мережі: критерії розміщення компонентів мережі, розміщення робочих станцій, розміщення периферійних пристроїв, прокладка кабелю, розміщення комунікаційних пристроїв, розміщення серверів.

2.4 Підключення до Інтернету

Плануючи стратегію підключення доступу в Інтернет, вибираючи розміщення маршрутизаторів та устаткування, треба оцінити не тільки пропускну здатність каналу зв'язку, але й розташування комп'ютерів, яким потрібен доступ до Інтернету. Якщо доступ до Інтернету потрібен усім користувачам корпоративної мережі, то маршрутизатор найкраще підключити до магістральної мережі або до іншого центрального каналу. Якщо всі комп'ютери, яким потрібен доступ до Інтернету, наприклад група Web-серверів, розміщені окремо, то для уникнення перевантаження інших ділянок мережі Інтернет - канал варто підключати тут же.

Мінімальний набір устаткування для підключення до мережі Інтернету складатиметься з маршрутизатора та каналу глобальної обчислювальної мережі (ГОМ).

Підключення через модем можна настроїти так, що воно буде доступно всім користувачам мережі. Однак одне модемне з'єднання через телефонну лінію забезпечує швидкість не більше 56 Кбит/с. Цього вистачить лише для декількох користувачів, та й то за умови, що вони не працюють із додатками, що вимагають високої пропускну здатності та продуктивності.

Цифрова мережа комплексних послуг (Integrated Services Digital Network, ISDN) - працює через телефонні лінії. Вона вимагає підтримки з боку телефонної компанії та спеціального устаткування. Складається із двох служб: базового інтерфейсу абонента (Basic Rate Interface, BRI або 2B+D), що забезпечує швидкість до 128 Кбит/с і первинного інтерфейсу обміну (Primary Rate Interface, PRI) зі швидкістю до 1,544 Мбит/с (як у лінії T-1). ISDN-канал цілком придатний для роботи з електронною поштою Інтернету для користувачів середньої мережі.

Рішення для доступу в Інтернет на основі мережі кабельного телебачення (КТВ) і абонентських цифрових ліній (Digital Subscriber Line, DSL) орієнтовані, у першу чергу, на домашнього користувача,

але можуть застосовуватися й у корпоративних мережах. Багато постачальників послуг КТВ мають мережі на оптоволоконному кабелі з досить щільним покриттям території. DSL - це служба високошвидкісної передачі цифрових даних по стандартних телефонних лініях. DSL являє собою виділений канал з постійною швидкістю передачі. Існує кілька типів DSL-технологій з різними назвами, включаючи ADSL і HDSL, тому DSL часто називають узагальненим ім'ям - xDSL.

Виділена лінія являє собою постійний, як правило, цифровий канал (звичайно використовує телефонні лінії) з постійною пропускнуою здатністю. Найчастіше для підключення більших і середніх мереж до Інтернету застосовують канал T-1 (швидкість - 1,544 Мбит/с). Наступна градація - канал T-3, еквівалентний 672 каналам по 64 Кбит/с кожний або 28 каналам T-1, що забезпечує швидкість 44,736 Мбит/с. В Інтернеті канали T-3 використовуються для магістральних з'єднань.

Ретрансляція кадрів (frame relay) - ГОМ- технологія передачі даних зі змінною швидкістю. Дозволяє оплачувати використання каналу залежно від реальної швидкості передачі даних. Для установки ГОМ- з'єднання необхідно провести виділену лінію між абонентом і постачальником послуг доступу, має назву хмара (cloud) і з'єднує дві виділені лінії.

Загальні питання для розгляду [2,6].

1. Визначення вимог до каналу зв'язку з Інтернетом для вашої мережі:

- оцінка необхідної пропускнуої здатності каналу зв'язку;
- призначення часу доступу в Інтернет;
- розміщення користувачів.

2. Вибір каналу для підключення до Інтернету:

- модемне з'єднання через телефонну лінію;
- PPPoE; DSL;
- VPN;
- мережі кабельного телебачення;
- виділені лінії;

- підключення з ретрансляцією кадрів;
- Wi-Fi;
- 3G-UMTS/CDMA;
- 4G-WiMAX/LTE.

2.5 Вибір маршрутизатору та постачальника послуг Інтернету

Модуль служби маршрутизації та віддаленого доступу (RRAS) можна настроїти для маршрутизації трафіку між ЛОМ і будь-яким ГОМ-каналом, підключеним до комп'ютера, на якому працює RRAS. Крім того, RRAS підтримує NAT і здатна забезпечити доступ в Інтернет комп'ютерам ЛОМ із незареєстрованими IP-адресами. Перетворення мережевих адрес (Network address translation, NAT) реалізовано програмою, вбудованою в маршрутизатор.

Маршрутизатор може бути виконаний у вигляді окремого пристрою. Більшість маршрутизаторів з нижнього сегмента цінового діапазону - це комбіновані пристрої, які на додаток до стандартних функцій маршрутизації підтримують NAT і DHCP. Такі маршрутизатори, підключені безпосередньо до ГОМ, забезпечують загальний доступ в Інтернет через стандартний модем, ISDN, мережа KTV або DSL. Оскільки загальний доступ надається з використанням NAT, мережа пов'язана з ISP через єдиний канал, отже, такі пристрої не підходять для великих мереж, а також мереж, де зареєстровані IP-адреси, які потрібні декільком комп'ютерам. Більшість ГОМ-технологій, вимагають також спеціального устаткування: для з'єднання через телефонну лінію - модему, для виділеної лінії - пристроїв CSU/DSU.

Вибір постачальника послуг Інтернету (ISP) - важливий аспект планування стратегії доступу в Інтернет для великої та середньої мережі. Основна функція ISP - надання доступу в Інтернет. ISP підтримує власну мережу, з'єднану з Інтернетом, до якої абоненти

підключаються за допомогою самих різних ГОМ- технологій. Різні ISP займають різні рівні володіння мережами. Одні підключені безпосередньо до магістралей Інтернету, а інші є лише посередниками. Одні ISP орієнтовані на домашніх користувачів, а інші - на корпоративних.

Загальні питання для розгляду [2,6].

1. Вибір типу маршрутизатора.
2. Вибір постачальника послуг Інтернету та визначення, які служби (Web, DNS, електронна пошта) будуть підтримуватися в мережі, а які – буде отримано у постачальника послуг Інтернету.
3. Захист і керування доступом в Інтернет:
 - визначення вимог до захисту доступу в Інтернет;
 - вибір методу доступу до Інтернет (за допомогою маршрутизатора NAT або проксі-серверу).

2.6 З'єднання через маршрутизатори окремих віддалених ЛОМ підприємства

ГОМ-топологія - структура з'єднань між віддаленими сегментами або ЛОМ підприємства. Вибирати ГОМ- топологію треба з урахуванням особливостей наміченої для використання ГОМ-технології. Обрану ГОМ-топологію можна реалізувати на основі постійних підключень або підключень за запитом.

Постійні підключення забезпечують постійну швидкість передачі даних, звичайно за фіксовану щомісячну плату. Підключення за запитом дозволяють оплачувати тільки ресурси каналу зв'язку, які реально використані.

Служби доступу через лінії, що підключенні з ретрансляцією кадрів і VPN дозволяють реалізувати мережі з топологією без попарного з'єднання вузлів виділеними ГОМ- каналами.

Статична маршрутизація вимагає створювати маршрути вручну, тому вона не підходить для великих мереж із інфраструктурою, яка часто змінюється.

Динамічна маршрутизація використовує протокол, що дозволяє маршрутизаторам автоматично адаптуватися до змін у мережі та обмінюватися повідомленнями з даними про мережі, у яких вони розміщені.

RIP - протокол маршрутизації оптимальний для мереж, всі ділянки яких працюють на однаковій швидкості. OSPF - протокол маршрутизації на основі стану каналу. Завдяки масштабованості він придатний для мереж практично будь-якого розміру, але вимагає більше ретельного планування, налаштування та підтримки, чим RIP.

Загальні питання для розгляду [2].

1. Вибір ГОМ- топології (на основі постійних підключень і/або на основі підключень за запитом).
2. Вибір ГОМ- технології:
 - виділені лінії;
 - підключення за запитом;
 - з'єднання з ретрансляцією кадрів;
 - віртуальна приватна мережа.
3. Вибір маршрутизаторів.
4. Вибір протоколу маршрутизації.

2.7 Віддалений доступ до мережі

Для того, щоб сформулювати вимоги безпеки до серверу віддаленого доступу, визначите, які користувачі мають потребу у віддаленому доступі до мережі, який тип доступу їм потрібно, а також чи необхідно вводити різні рівні доступу.

RRAS підтримує кілька протоколів перевірки дійсності: EAP, MS-CHAP (версій 1 і 2), CHAP, SPAP і PAP.

Політики віддаленого доступу є наборами умов, яким повинні задовольняти клієнти, які намагаються підключитися до серверу віддаленого доступу. Політики управляють віддаленим доступом залежно від членства користувачів у групах.

RRAS звіряє параметри всіх вхідних підключень зі списком політик віддаленого доступу, які створені на сервері, і дозволяє доступ тільки підключенням, що задовольняють всім умовам хоча б однієї з політик.

Профілі віддаленого доступу являють собою набори атрибутів, які RRAS застосовує до підключень, що пройшли аутентифікацію та авторизацію. Профілі дозволяють задавати час, коли підключення дозволене, установлювати типи дозволеного IP-трафіку, а також обов'язкові до використання протоколи перевірки та алгоритми шифрування.

Невірне налаштування протоколу маршрутизації порушує обмін повідомленнями між маршрутизаторами мережі та веде до передачі пакетів невірними маршрутами.

Загальні питання для розгляду [2].

1. Визначення вимог до безпеки:

- визначення користувачів, яким потрібен віддалений доступ до мережі;
- визначення типу доступу для кожного користувача, якому він потрібен.

2. Керування доступом через властивості облікових записів.

3. Планування перевірки дійсності (аутентифікації).

4. Застосування політик віддаленого доступу.

2.8 Вибір операційної системи та обладнання

Сервери здатні виконувати в мережі організації безліч ролей: контролер домену, Web-сервер, сервер БД, поштовий сервер, сервер

інфраструктури, сервери файлів та друку, сервер резервного копіювання.

Конфігурація серверів звичайно створюється розраховуючи на вимоги конкретного програмного середовища, а робочі станції проектуються для вирішення широкого кола завдань.

Створюючи специфікацію устаткування сервера, варто передбачити можливість нарощування числа процесорів і пам'яті, а також об'єму дискової підсистеми.

Сімейство ОС Windows для робочих станцій включає дві лінії, засновані, відповідно, на технологіях DOS і Windows NT, для використання в мережах віддають перевагу останній.

У якості серверної ОС варто вибирати платформу, що максимально підходить для даної серверної ролі, пріоритетом при виборі ОС для робочих станцій є стандартизація. Для робочих станцій варто вибрати ОС, що підійде для максимально можливого числа користувачів.

Вибір ОС для серверів ширше, для кожного сервера він здійснюється відповідно до вимог програмного середовища, яке буде працювати на цьому сервері. Але більш бажаною для використання у ГОМ вважають сімейство ОС Unix та Linux.

Установка ОС у базовій конфігурації забезпечує мінімальний рівень безпеки, необхідний організації. Для комп'ютерів з особливими вимогами до захисту базову конфігурацію можна змінити шляхом налаштування її параметрів і установки додаткового захисного ПЗ і устаткування.

Загальні питання для розгляду [2].

1. Установка сервера (серверів) з необхідною роллю:

- сервер резервного копіювання;
- сервер баз даних;
- контролер домену;
- поштовий сервер;
- сервер файлів та друку;
- сервер інфраструктури;

- Web-сервер.
- 2. Визначення вимог до обладнання серверів.
- 3. Визначення вимог до обладнання робочих станцій.
- 4. Вибір операційної системи:
 - для робочих станцій;
 - для серверів.

2.9 Забезпечення мережевої безпеки

Інформаційна система перебуває в стані захищеності, якщо забезпечені її конфіденційність, доступність і цілісність. Безпека забезпечується технічними засобами - системами шифрування, аутентифікації, авторизації, аудита, антивірусного захисту, мережевими екранами та ін., а також юридичними і морально-етичними нормами, просвітньою роботою та адміністративними мірами.

Існує два класи алгоритмів шифрування - симетричні (наприклад, DES) і асиметричні (наприклад, AFS). Дайджест - результат односторонньої функції шифрування. Знання дайджесту не дозволяє й навіть не припускає відновлення вихідних даних. Дайджест використовується для контролю цілісності й автентичності документа (цифровий підпис).

Аутентифікація користувача - процедура доказу того, що він є той, за кого себе видає. Це багаторазові та одноразові паролі, володіння якимось унікальним предметом (фізичним ключем, документом, сертифікатом), біохарактеристики (малюнок райдужної оболонки ока).

Авторизація - це процедура контролю доступу легальних користувачів до ресурсів системи та надання кожному з них саме тих прав, які визначені йому адміністратором.

Антивірусний захист служить для профілактики та діагностики вірусного зараження, а також для відновлення працездатності уражених вірусами інформаційних систем.

Мережевий екран здійснює інформаційний захист однієї частини комп'ютерної мережі від інших шляхом аналізу трафіку.

Мережеві екрани діляться на: екрани з фільтрацією пакетів на основі IP-адрес; екрани сеансового рівня, здатні фільтрувати пакети з урахуванням контексту; найбільш інтелектуальні мережеві екрани прикладного рівня.

Проксі- сервер - виконує функції посередника між клієнтськими та серверними частинами розподілених мережевих частин, причому клієнти належать внутрішній мережі, а сервери – зовнішній (потенційно небезпечній) мережі.

Технологія захищеного каналу забезпечує захист трафіку між двома підключеннями у відкритій транспортній мережі, наприклад в Інтернеті. Захищений канал має на увазі виконання трьох основних функцій: взаємна аутентифікація абонентів при встановленні з'єднання; шифрування переданих повідомлень; підтвердження цілісності повідомлень. До числа найбільш популярних протоколів захищеного каналу відносять IPSec і SSL.

Більш масштабним засобом захисту трафіку, в порівнянні із захищеними каналами, є віртуальні приватні мережі (VPN). VPN на основі шифрування гарантують конфіденційність корпоративних даних при передачі через відкриту мережу, аутентифікацію взаємодіючих систем на обох кінцях VPN і тунелювання, що дозволяє передавати зашифровані пакети по відкритій публічній мережі.

VPN забезпечують той же рівень безпеки, що і виділені канали.

Конфіденційність (Privacy) - відсутність у третьої особи можливості скопіювати або переглянути дані, які передаються по мережі Інтернет. **Аутентифікація** (Authentication) - перевірка, чи дійсно відправник пакетів VPN - істинне пристрій, а не використовується зломисником. **Цілісність даних** (Data integrity) - перевірка, чи не піддавався змінам пакет при передачі через Інтернет. **Пересилання недостовірної інформації** (Antireplay) - відсутність у третьої особи можливості копіювати пакети даних, відіслані істинним

відправником, а потім пересилати ці пакети, видаючи себе за істинного відправника.

Для вирішення цих завдань двома пристроями створюється VPN (тунель VPN). Вони додають ще один заголовок до оригінального пакету. У заголовок включаються поля, які дозволяють VPN-пристроєм виконувати функції безпеки. Пристрої відповідають за шифрування оригінальних пакетів IP. Інформація передається в зашифрованому вигляді. Прочитати дані, можна лише володіючи ключем до шифру. Управління доступом, автентифікація і шифрування - важливі елементи захищеного з'єднання.

IPSec VPN - класичний приклад VPN, побудованої за так званою накладеної моделі (Overlay) - обладнання сервіс-провайдера чи не задіюється в процесі маршрутизації клієнтського трафіку, а його мережа надає лише «прозоре» з'єднання між майданчиками підприємства - модель дозволяє забезпечити високу безпеку мережі без додаткових коштів і витрат з боку адміністративно-технічного персоналу оператора. IPSec - архітектура або набір концепцій, які використовуються для захисту мереж IP (скорочена версія найменування в RFC (RFC +4301; архітектура безпеки Інтернет-протоколу - Security Architecture for the Internet Protocol), для якої вживається назва "IPSecurity" або скорочена версія - "IPSec").

Визначає методи ідентифікації при ініціалізації тунелю, методи шифрування для кінцевих точок тунелю і механізми обміну та управління ключами шифрування між ними. Недолік - протокол орієнтований на IP. При шифруванні в IPSec використовується декілька алгоритмів, фактично - математичні формули, які вибираються так, щоб одна використовувалася для шифрування даних, а інша - дата розшифрування і щоб неавторизована особа не змогло дешифрувати пакет даних або текст. Є важлива вимога: навіть якщо вдалося дешифрувати пакет, це ні як не повинно сприяти дешифруванню подальших пакетів даних.

Загальні питання для розгляду [1,2].

1. Вибір «технічного» методу (методів) забезпечення інформаційної безпеки (забезпечення конфіденційності, доступності, цілісності при передачі інформації):

– аутентифікація;

- авторизація;
- шифрування (симетричне, асиметричне, шифрування за допомогою односторонньої функції);
- антивірусні засоби, мережевий екран (мережевий екран мережевого рівня, мережевий екран сеансового рівня, мережевий екран прикладного рівня);
- проксі-сервер (проксі-сервер прикладного рівня, проксі-сервер рівня з'єднань);
- фільтруючий маршрутизатор;
- захищений канал, (захищений канал на базі протоколу S/MIME, захищений канал на базі протоколу SSL, захищений канал на базі протоколу PPTP, захищений канал на базі протоколу IPSec (у транспортному режимі, в тунельному режимі));
- віртуальна приватна мережа (віртуальна приватна мережа на основі розмежування трафіку, віртуальна приватна мережа на основі шифрування).

2. Вибір «нетехнічних» засобів захисту:

- у сфері законодавства;
- морально-етичні норми, просвітня робота;
- адміністративні заходи;

3. Вибір фізичних засобів захисту:

- замки;
- камери спостереження;
- охоронні системи.

4. Резервне копіювання даних:

- вибір устаткування для архівації;
- вибір програми для архівації;
- складання плану резервного копіювання:

- 1) вибір даних, що архівуємо;
- 2) типи архівації;
- 3) повна;
- 4) додаткова;
- 5) різницева (диференціальна);

- планування архівації;
- повна (щотижня) + додаткова або різницева (щодня).

2.10 Забезпечення мережевої безпеки в бездротових ЛОМ

Паролі адміністратора та ідентифікатори SSID у більшості випадків вільно доступні в Інтернеті для більшості моделей бездротового устаткування. Потрібно обов'язково змінити стандартні пароль адміністратора та ідентифікатор SSID, що задає ім'я мережі. А це означає, що зловмисникові досить з'ясувати модель вашої бездротової точки доступу, щоб одержати до неї доступ, попередньо довідавшись стандартні SSID і пароль адміністратора. Також треба змінити IP-адрес. Багато точок доступу за замовчуванням транслюють усім свій SSID. Тому до вашої може підключитися будь-який небажаний гість, навіть ненавмисно, - людина просто запустить пошук мережі і знайде вашу точку доступу.

Протоколи WPA (Wi-Fi Protected Access), WPA2 і WEP (Wired Equivalent Privacy) забезпечують захист і шифрування даних, переданих бездротовою точкою доступу та бездротовим клієнтом. Переважніше використовувати WPA2. Алгоритм WPA2 є модифікацією алгоритму WPA. WPA2 - найбільш захищений алгоритм шифрування даних, що робить його просто незамінним для організації роботи бездротової локальної мережі. WPA2 використовується при шифруванні за допомогою алгоритму AES з 128-бітним ключем.

Ви можете вказати список MAC-адрес адаптерів комп'ютерів, які зможуть одержати доступ до вашої мережі. Потрібно відзначити, що фільтрація MAC-адрес не забезпечує надійного захисту, а служить просто додатковим бар'єром.

Іноді за допомогою відновлення прошивки вдається додати підтримку WPA. У новій версії прошивки можуть бути усунуті помилки, наявні в її поточній версії, а також додані нові методи

шифрування. Інструкції з перепрошивки точки доступу та її нову версію можна скачати із сайту виробника.

На допомогу адміністраторові також приходять методи аутентифікації: WPA-PSK і WPA2-PSK. RADiUS - сервер буде корисний у досить великих мережах, де потрібно аутентифікувати не тільки бездротових, але й інших клієнтів мережі, - наприклад, клієнтів, які підключаються за VPN.

Деякі точки доступу дають можливість понизити потужність передачі, що дозволяє знизити число як навмисних, так і випадкових, несанкціонованих підключень до точки доступу. Понизивши потужність передачі, можна домогтися того, що точка доступу буде доступна тільки в межах офісу вашої компанії.

Вимикайте точку доступу, коли ви не працюєте - так ви на 100% будете впевнені, що ніхто не проникне у вашу мережу.

Інтерфейси керування бездротовими мережами не повинні бути доступні по бездротовій мережі - все керування бездротовою мережею повинне здійснюватися тільки по внутрішній (кабельній) мережі. Також доступ до портів керування варто дозволити тільки одним-двом конкретним станціям.

Антивіруси та брандмауери ніхто не скасовував і у випадку з бездротовим зв'язком. Бажано встановити не один загальний брандмауер/ антивірус - на сервері, але й установити клієнтські брандмауери та антивіруси для захисту кожного комп'ютера мережі окремо .

Загальні питання для розгляду [5].

1. Зміна параметрів за замовчуванням.
2. Відключення широкомовлення SSID.
3. Використання протоколу WPA2.
4. Фільтрація MAC- адрес.
5. Відновлення прошивки устаткування.
6. Використання аутентифікації.
7. Зниження потужності передачі.
8. Відключення точки доступу, коли ви не працюєте.

9. Захист портів керування.
10. Захист від зовнішніх погроз (брандмауер і антивірус на кожному комп'ютері мережі).

2.11 Призначення IP-адрес

У кожного комп'ютера мережі TCP/IP повинен бути унікальний IP-адрес. З метою безпеки, комп'ютери із зареєстрованими IP-адресами розміщують в окремій мережі. Будь-яку мережу можна розбити на частини, виділивши трохи бітів ідентифікатора хосту під ідентифікатор підмережі. Щоб розрахувати маску підмережі та IP-адреси, представте адреси у двійковому вигляді, збільшіть їх та переведіть результат назад у десятковий вид.

Настроювати TCP/IP на клієнтських комп'ютерах можна вручну або автоматично за допомогою DHCP-серверів, що призначають комп'ютерам IP-адреси та інші параметри конфігурації.

Більшість неполадок DHCP, якщо тільки вони не викликані збоями устаткування, виникають через невірне налаштування DHCP-клієнтів, DHCP-серверів і агентів DHCP-ретрансляції.

Для приватних адрес із загального діапазону адрес 0.0.0.0 - 255.255.255.255 виділено та зарезервоване три діапазони:

- 10.0.0.0 - 10.255.255.255 (мережа класу А, маска 255.0.0.0, кількість припустимих адрес $2^{24}=16777216$);
- 172.16.0.0 - 172.31.255.255 (16 мереж класу В, маска 255.255.0.0, кількість припустимих адрес $2^{16}=65536$);
- 192.168.0.0 - 192.168.255.255 (256 мереж класу С, маска 255.255.255.0, кількість припустимих адрес $2^8=256$).

Адреси із цих трьох діапазонів не видаються для використання в глобальній мережі (Інтернет). Область застосування - тільки локальні мережі. На їхній основі можна побудувати мережі трьох розмірів:

- маленька - на 256 адрес, діапазон 192.168.0.0 - 192.168.255.255;
- середня - на 65 536 адрес, діапазон 172.16.0.0 - 172.31.255.255;

– велика - на 16 777 216 адрес, діапазон 10.0.0.0 - 10.255.255.255.

Може існувати скільки завгодно багато локальних мереж, у яких буде використовуватися той самий діапазон IP-адресов, наприклад, 192.168.0.0 - 192.168.255.255. Природно, що в цьому випадку комп'ютери з різних локальних мереж будуть мати однакову IP-адресу, що неприпустимо. Для запобігання такої ситуації локальні мережі робляться закритими - жоден з комп'ютерів такої мережі не має прямого доступу в глобальну мережу (Інтернет).

Один з комп'ютерів такої локальної мережі робиться трохи відособленим - перетворюється в шлюз ("ворота"). Такий шлюз має дві мережні карти - одна підключена до локальної мережі, інша ж - підключена безпосередньо до Інтернету (має прямий доступ). Мережній карті, підключеній до локальної мережі, привласнюється одна з адрес приватного діапазону (найчастіше, це адреса 192.168.0.1). Мережевій карті, підключеній до Інтернет, привласнюється IP-адрес, який надається для глобального використання. Така адреса унікальна і тільки один комп'ютер в Інтернеті (а точніше - мережева карта цього комп'ютера) може мати його.

IP-адрес орендується в організації, що займається видачею та контролем використання всіх IP-адрес Інтернету - повноважний комітет з нагляду за присвоєнням номерів Internet (IANA). Дублювання точно такої ж адреси іншим комп'ютером неприпустимо.

Для простоти запису маски, після ір адреси самого пристрою використовують запис в скороченій формі - число. Це число - кількість біт у масці, які дорівнюють 1. Наприклад, якщо ір адреса 192.168.58.4, а маска 255.255.255.0:

192.168.58.4 = 11000000.10101000.00111010.00000100

255.255.255.0 = 11111111.11111111.11111111.00000000

кількість біт = 1 у масці, дорівнює 24, то ір адресу можна записати в такий спосіб 192.168.58.4/24.

Перетворення мережевих адрес (Network address translation, NAT) реалізовано програмою, вбудованої в маршрутизатор. Ця програма відіграє роль посередника між приватною мережею та Інтернет - серверами із зареєстрованими адресами. Навіть клієнтські

комп'ютери із незареєстрованими адресами можуть відправляти запити серверам Інтернету та одержувати від них відповідь за допомогою NAT. Звичайні маршрутизатори змінюють дейтаграми не частіше, ніж працівники пошти звичайні конверти. На відміну від них маршрутизатор NAT заміняє вміст поля з адресою відправника у всіх дейтаграм, отриманих від комп'ютерів з незареєстрованим IP-адресом. Маршрутизатор NAT також підтримує таблицю незареєстрованих адрес приватної мережі - вона необхідна для відстеження оброблених їм дейтаграм.

Маршрутизатори, що працюють по протоколу IPv6, не виконують фрагментацію, як в IPv4, зменшуючи службову інформацію в заголовку IP-паketу. Замість фрагментації вони визначають MTU (maximum transmission unit, доступний максимальний розмір пакета) для кінцевого вузла в рамках конкретної сесії.

На початку передачі IPv6 пристрій відправляє пакет розміром, який вказаний одним з верхніх рівнів (транспортним або прикладним). При отриманні у відповідь ICMP-повідомлення - пакет занадто великий - виконується відправка пакету MTU-discover меншого розміру до тих пір, поки розмір буде задовольняти всім проміжним пристроям - нове MTU встановлюється для всієї сесії. У ICMP-повідомленні - пакет занадто великий - може міститися пропонування розмір MTU. Для кожної сесії визначається своє значення MTU.

Структура IPv6 адрес описана в RFC 3513 і 4291. Описують 3 типи адрес.

Unicast адреси - призначені для ідентифікації конкретного пристрою в мережі. Пакет відправлений на Unicast адрес доставляється на ідентифікований за допомогою адреси інтерфейс. Існує 2 типу Unicast адрес:

- Link-local unicast address (локальна Unicast адреса) - може використовуватися тільки в рамках локальної мережі (аналог автономних адрес IPv4);
- Global unicast address (глобальна Unicast адреса) - може використовуватися в мережах будь-якого розміру (аналог реальних адрес IPv4).

Кожен інтерфейс повинен мати мінімум 1 локальну Unicast адресу. Однак інтерфейс може мати одночасно декілька адрес всіх трьох типів.

Multicast адреси - в IPv6 не використовуються широкомовні адреси, замість них застосовуються Multicast адреси. Вони дозволяють відправляти пакети з даними одночасно кільком мережних інтерфейсів. Для цього використовуються Multicast групи, що дозволяють відправляти дані обмеженій групі вузлів. Кількість Multicast адрес IPv6 значно перевищує кількість Multicast адрес IPv4.

Anycast адреси - Anycast адреса може посилатися одночасно на декілька інтерфейсів одного вузла. Пакет відправлений на Anycast адресу буде доставлений на найближчий інтерфейс вузла визначений за допомогою протоколу маршрутизації. Anycast адреса не може використовуватися в якості адреси відправника.

У протоколі IPv6 зарезервовано декілька спеціальних IP-адрес:

:: / 128 - може використовуватися тільки при розробці програмного забезпечення;

:: 1/128 - локальна адреса кільцевого інтерфейсу. Використовується для звернення до самого себе (Аналог 127.0.0.1 в IPv4);

2001: db8 :: / 32 - скрізь, де наводяться приклади IPv6-адрес, слід використовувати адреси цього діапазону;

fe80 :: / 10 - локальний префікс, вказує, що адреса є дійсною тільки всередині місцевої фізичної мережі. Це аналог IP адреси 169.254.0.0/16 в IPv4;

ff00 :: / 8 - багатоадресний префікс використовується для Multicast розсилки.

Загальні питання для розгляду [2,4].

Загальні (зареєстровані) IPv4-адреси, їх призначення. Приватні (незареєстровані) IPv4-адреси, їх призначення: три діапазони адрес для використання в приватних мережах:

- 10.0.0.0/8 - 10.255.255.255/8;
- 172.16.0.0/16 - 172.31.255.255/16;
- 192.168.0.0/24 - 192.168.255.255/24.

Доступ в Інтернет з приватної мережі: підключення до Інтернету через маршрутизатор NAT, підключення до Інтернету через проксі-сервер, вибір варіанта доступу.

Обчислення IPv4-адрес для комп'ютерів.

Вибір способу настройки TCP / IP на клієнтських комп'ютерах: вручну, за допомогою сервера DHCP, вибір варіанта настройки.

Вибір типу адресації IPv6. Використання Anycast адрес.

2.12 Подання мережі головного офісу організації в Інтернеті

Компанія **Fabrikam, Inc.** (назва надана як приклад для використання, кожен повинен зробити вибір за назвою своєї компанії) зареєструвала для своєї нової мережі домен `fabrikam.com`. Вам доручено створити простір імен DNS для нової мережі. З урахуванням наведених нижче відомостей, запишіть для кожного з розміщених на рисунку комп'ютерів повне доменне ім'я.

1. `Fabrikam.com` - єдиний доступний компанії домен 2-го рівня.
2. Внутрішня і зовнішня мережі компанії повинні бути в різних доменах.

3. Компанія складається з 3 відділів: відділу збуту (Sales), відділу кадрів (Human Resources) і виробничого відділу (Production). Комп'ютери кожного відділу повинні бути в окремому домені. У кожному відділі є різні сервери і до 250 робочих станцій (на діаграмі (рис.2.2) показані лише деякі з них). Імена комп'ютерів повинні відображати їх функції.

4. Три сервера, розташовані у зовнішній мережі (периметрі), підтримують служби Інтернету: Web, FTP і електронну пошту. Ці сервери повинні бути в домені `fabrikam.com`.

Примітка. У вас, звичайно, своє ім'я компанії; ім'я зареєстрованого домену; кількість відділів; назви відділів; кількість робочих станцій в кожному відділі; кількість серверів, розташованих у зовнішній мережі (периметрі); а тому і свій вигляд таблиці.

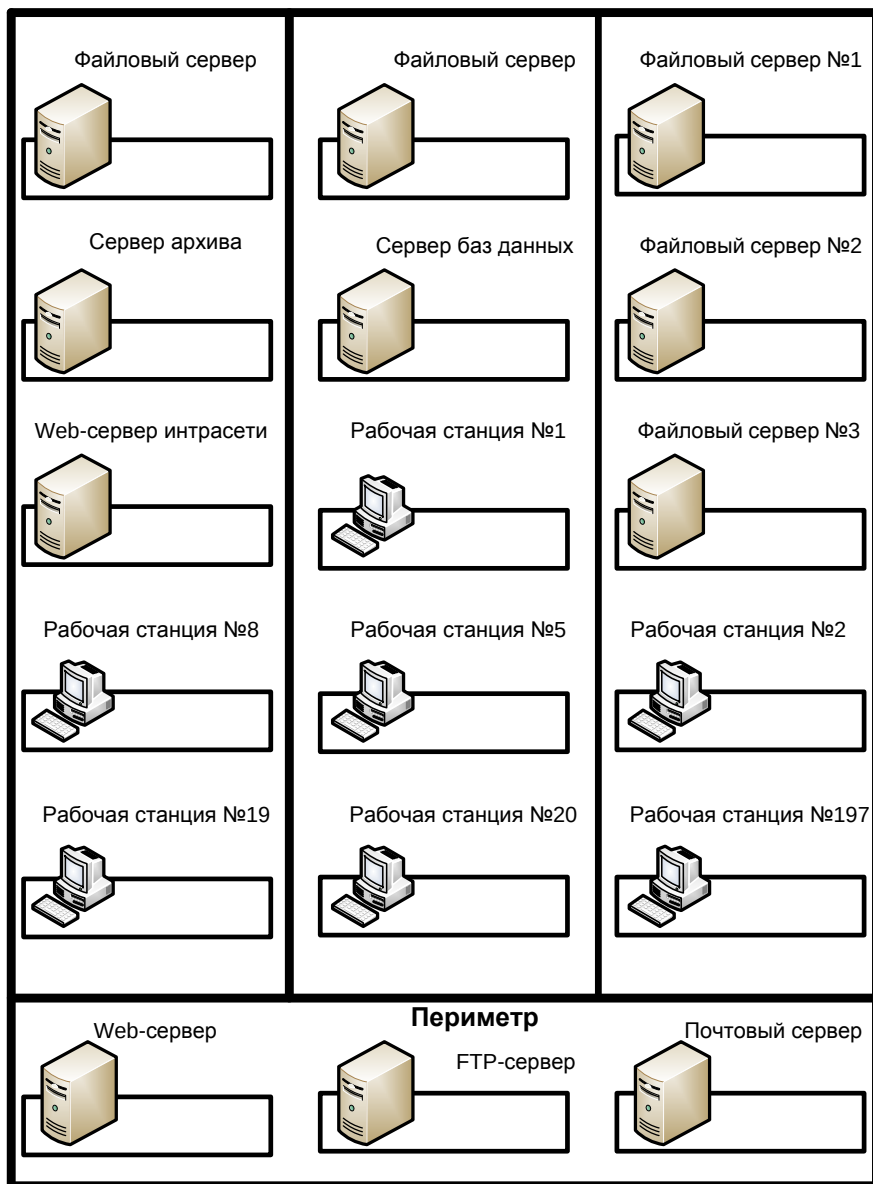


Рисунок 2.2 – Мережа головного офісу організації.

3 ЗАГАЛЬНІ ВИМОГИ ДО ОФОРМЛЕННЯ КУРСОВОГО ПРОЕКТУ

3.1 Вимоги до оформлення пояснювальної записки

Пояснювальна записка курсового проекту оформлюється відповідно до діючих стандартів на оформлення програмної, текстової та графічної документації: ДСТУ 3008-95 «Документація. Звіти в сфері науки та техніки».

Кожна сторінка тексту пояснювальної записки оформлюється в основній рамці (відступ зліва на 20 мм, з інших сторін на 5 мм) та з надписом (рис. 3.1), в якому визначається десятильний номер курсового проекту та номер листа (сторінки) пояснювальної записки, написаний арабськими цифрами.

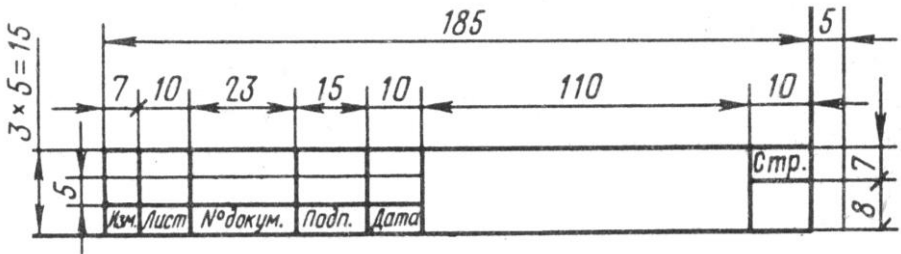


Рисунок 3.1 – Форма надпису в пояснювальній записці

Децимальний номер курсового проекту має структуру:

XX.XXXXXXXX.XXXXXX XX, де:

1 2 3 4

- 1 – шифр держави (для України – 13);
- 2 – шифр вищого навчального закладу (для ЗНТУ – 02070849);
- 3 – порядковий номер студента в журналі групи;
- 4 – літерно-цифровий шифр документа.

Наприклад, для пояснювальної записки курсового проекту студента з порядковим номером в журналі групи – 12, десятильний номер – 13.02070849.00012 ПЗ.

Перша сторінка пояснювальної записки (титульний лист) не нумерується.

Зразок оформлення титульного листа наведено в додатку Б.

Друга та третя сторінки пояснювальної записки – технічне завдання, виконується з обох сторін аркуша. Зразок оформлення технічного завдання наведено в додатку В.

Четверта сторінка – реферат, який оформлюється в основній рамці з повним надписом (рис. 3.2), в якому наводиться визначання десятичного номеру пояснювальної записки, підписи студента, керівника, назва курсового проекту, номер листа (4) та кількість листів в пояснювальній записці. Зразок оформлення реферату наводиться в додатку Д.

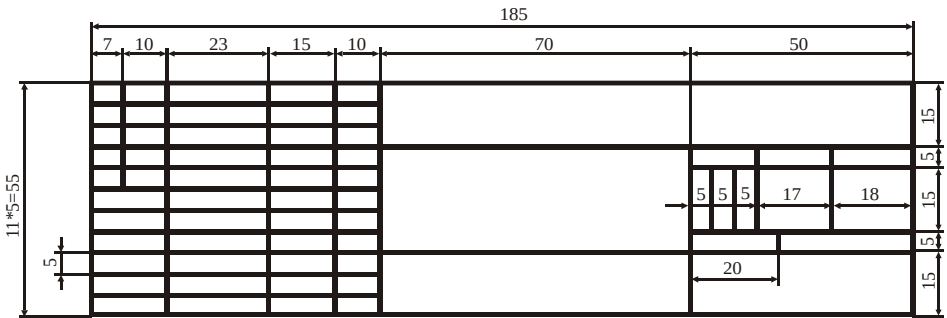


Рисунок 3.2 – Форма рамки для реферату курсового проекту

3.2 Вимоги до оформлення графічних документів

Графічні документи курсового проекту пропонується виконувати на папері для креслення з нанесенням зовнішньої рамки зліва на 20 мм, з інших сторін на 5 мм. В правому нижньому куті виконують основний надпис (рис. 3.2). Графічні матеріали виконуються на папері формату А4 (210x290) та розміщуються в додатках.

Кількість листів та вигляд графічних документів узгоджується студентом з керівником курсового проекту з урахуванням особливостей теми проекту. Рекомендована кількість графічних документів – 3-5 листів.

Графічні документи складаються з плакатів, що мають ілюстраційний характер, та креслень, які виконуються згідно стандартів. Графічна частина курсового проекту обов'язково повинна містити в собі два або одне креслення.

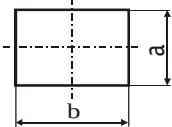
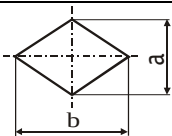
3.3 Схеми алгоритмів, програм, даних та систем

Схеми алгоритмів, програм, даних та систем виконуються згідно ГОСТ 19.701-90, ГОСТ 19.002-80, ГОСТ 19.003-80 [6-8].

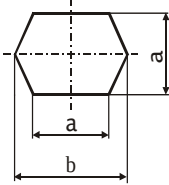
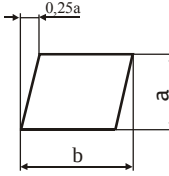
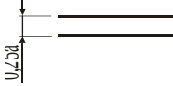
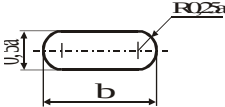
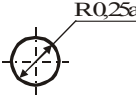
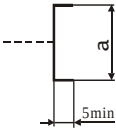
Схеми алгоритмів, програм, даних та систем (далі схеми) складаються з наявних значень символів, стислого пояснювального тексту та з'єднувальних ліній.

Нижче надані символи для використання в документації даних і наведені їх умовні зазначення (табл. 3.1) для використання їх в схемах алгоритмів, даних, програм, системи, взаємодії програм та тощо.

Таблиця 3.1 - Символи

Найменування	Позначення й розміри, мм	Функція
Процес		Виконання операції або групи операцій, в результаті яких змінюється значення, форма подання або розташування даних
Рішення		Вибір напрямлення виконання алгоритму або програми в залежності від деяких змінних умов

Продовження таблиці 3.1

Назва	Позначення та розміри, мм	Функція
Модифікація		Виконання операцій, які мають команди або групу команд, що змінюють програму
Введення – виведення		Перетворення даних в схему, яку можна використовувати для обробки (введення) або відображення результатів обробки (виведення)
Лінія потоку		Визначення послідовності зв'язків між символами
Паралельні дії		Початок або кінець двох або більше одночасно виконаних операцій
Пуск, зупинка		Початок, переривання, кінець обробки даних або виконання програм
З'єднувач		Визначення зв'язку між перериваннями ліній потоку, які зв'язують символи
Коментар		Зв'язок між елементом схеми та поясненням

Розмір **a** повинен вибиратись з ряду 10, 15, 20 мм. Розмір **a** дозволяється збільшувати на число кратне 5. Розмір **b** дорівнює $1,5a$.

Усі символи в схемі повинні бути пронумеровані. Порядковий номер проставляють зліва в верхній частині символу у розриві контуру (рис. 3.3).

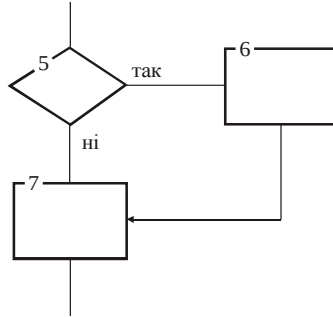


Рисунок 3.3 – Приклад частини алгоритму програми

В схемах, якщо направлення лінії потоку зліва направо або зверху вниз то стрілка не ставиться, в інших випадках стрілка ставиться. В випадках, коли відображаються варіанти рішення (наприклад, так, ні), вони ставляться над лінією потоку або справа від неї.

3.4 Вимоги до виконання електричних схем

В графічній частині курсового проекту пропонується виконувати креслення або плакати на 3-5 листах формату А4. В склад графічної частини включають:

- структурні схеми мережі, яка проектується;
- специфікації компонентів мережі;
- функціональні схеми мережі;
- схеми зв'язків;
- монтажні схеми розташування апаратних засобів.

З урахуванням особливостей конкретної теми курсового проекту склад графічних документів може бути змінено.

Схема – це графічний конструкторський документ, на якому відображені у вигляді умовних зображень або позначень складові частини виробу та зв'язки між ними. Схеми використовуються під час вивчення принципу дії механізмів, машин, пристроїв, апаратів, при їх налагодженні та ремонті, монтажі трубопроводів та електричних мереж, для пояснення зв'язку між окремими складових частин виробів без уточнення особливостей їх конструкцій.

Схеми в залежності від елементів й зв'язків між ними розділяються на такі види:

- структурна схема Е1 (визначає основні функціональні частини виробів, їх значення та взаємозв'язки);
- функціональна схема Е2 (служить для роз'яснення процесів, які протікають в окремих функціональних колах виробу або у виробі в цілому);
- принципова (повна) схема Е3 (визначає повний склад елементів та зв'язків між ними та дає детальне уявлення про принципи роботи виробу);
- схема з'єднань (монтажна) Е4 (показує з'єднання складових частин виробів та визначає проводи, джгути, кабелі або трубопроводи, за допомогою яких виконуються ці з'єднання, а також місця їх з'єднань та виведення);
- схема підключення Е5 (показує зовнішні підключення виробів);
- загальна схема Е6 (визначає складові частини комплексу й з'єднання їх між собою на місці експлуатації);
- схема розміщення (визначає розміщення складових частин виробу, при необхідності також джгутів, проводів, кабелю, трубопроводів);
- об'єднана схема (схема, коли на одному конструктивному документі виконуються схеми двох або кількох типів, випущених на один виріб).

Зразки схем наведено в додатку Е.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: / В. Г. Олифер, Н. А.Олифер. // Учебник для вузов. — 4-е изд. — СПб.: Питер, 2010. — 944с.: ил.

2. Закер Крэйг. Планирование и поддержка сетевой инфраструктуры Microsoft Windows Server 2003. Учебный курс MCSE / Закер Крэйг. // Пер. с англ.— М.: Издательско-торговый дом «Русская Редакция», 2005. — 544с. : ил.

3. Нортроп Т. Проектирование сетевой инфраструктуры Windows Server 2008. Учебный курс Microsoft / Т. Нортроп, Дж. К. Макин // Пер. с англ. — М. : Издательство «Русская Редакция», 2009. — 592с. : ил.

4. Палмер М. Проектирование и внедрение компьютерных сетей / М. Палмер, Р. Синклер. — СПб.:БХВ-Петербург, 2004. — 752с.; ил.

5. Колисниченко Д.Н. Беспроводная сеть дома и в офисе / Д.Н. Колисниченко. — СПб.: БХВ-Петербург, 2009. — 480с.; ил.

6. Демидов М. Невидимая паутина. Обзор технологий беспроводного подключения к Интернету / М. Демидов // HARD'n'SOFT. — 2010. — №8. — С.54-57.

ДОДАТОК А

Приклади оформлення бібліографічного опису

1. Биков В. Ю. Моделі організаційних систем відкритої освіти = Models of the Education Organizational Systems: [монографія] / В. Ю. Биков. – Київ : Атіка, 2009.- 682 с.
2. 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.
3. Нортроп Т. Проектирование сетевой инфраструктуры Windows Server 2008. Учебный курс Microsoft / Т. Нортроп, Дж. К. Макин // Пер. с англ. — М. : Издательство «Русская Редакция», 2009. — 592с. : ил.
4. Мосіяшенко В.А. Мережі [Текст] : навч. посіб. / В. А. Мосіяшенко. — Суми : Унів. кн., 2005. — 174 с.—ISBN 966-680-198-1.
5. Лепа Є.В. Системи підтримки прийняття рішень. Частина 1 / Є.В. Лепа, Є.К. Міхеєв, В.В. Крініцин. // Навчальний посібник. – Херсон, 2006. – 324 с.
6. Бібліографічний запис. Бібліографічний опис. Загальні вимоги та правила складання [Текст] : (ГОСТ 7.1—2003, ІДТ) : 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).
7. Perez K. Radiation therapy for cancer of the cervix / K. Perez // Oncology. – 1993. – Vol. 7, №2. – P. 89–96.
8. Камишин В. В. Система оцінки науково-технічних програм та напрямків за допомогою експертного опитування методом “ДЕЛЬФІ” / В. В. Камишин, А. М. Рибак, І. М. Петрінко [та ін.] // VIII Междунар. науч.-практ. конфер. ”Система научно-технической информации: проблемы развития и функционирования” : тезисы док. и сообщ., 30–31 мая 2001 г. – К. : УкрИНТЭИ, 2001. – С. 71–76.

Додаток Б

Форма № 17

Комп'ютерних систем та мереж

(повна назва кафедри)

**КУРСОВИЙ ПРОЕКТ
(РОБОТА)**з Проектування комп'ютерних мереж
(назва дисципліни)на тему: _____
_____Студента (ки) _____ курсу _____ групи
напряму підготовки _____
спеціальності _____

(прізвище та ініціали)

Керівник _____

(посада, вчене звання, наук. ступінь, прізвище та ініціали)

Національна шкала _____

Кількість балів: _____ Оцінка: ECTS _____

Члени комісії _____
(підпис) (прізвище та ініціали)_____
(підпис) (прізвище та ініціали)_____
(підпис) (прізвище та ініціали)

м.Запоріжжя

20__ рік

ДОДАТОК В**Форма №24****Запорізький національний технічний університет****(повне найменування вищого навчального закладу)**

Інститут, факультет _____

Кафедра _____

Рівень вищої освіти (освітньо-кваліфікаційний рівень) _____

Напрямок підготовки _____

(код і назва)

Спеціальність _____

(код і назва)

ЗАВДАННЯ**на курсовий проект студенту**

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) _____

керівник проекту (роботи) _____

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від

“ ____ ” ____ 20 ____ року № ____

2. Строк подання студентом проекту (роботи) _____

3. Вихідні дані до проекту (роботи) _____

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) _____

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів курсового проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка

Студент

(підпис)

(прізвище та ініціали)

Керівник проекту

(підпис)

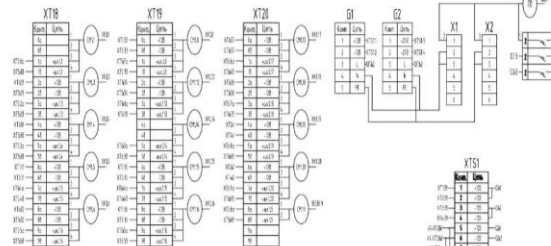
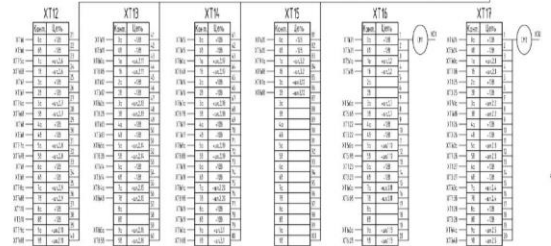
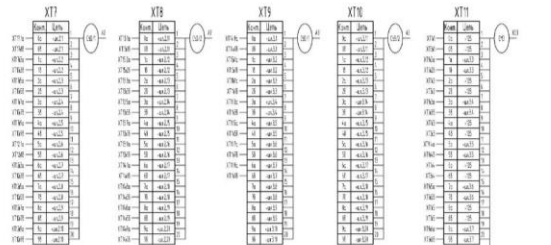
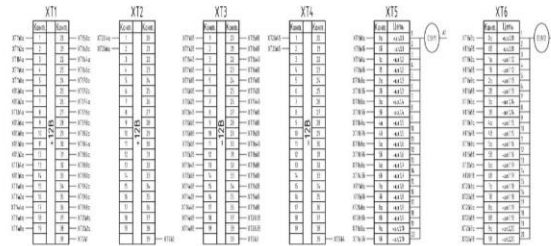
(прізвище та ініціали)

РАДІОРЕЛЕЙНІ ЛІНІЇ, СЕРВЕР, БЕЗДРОВОТІ ТЕХНОЛОГІЇ,
АНТЕНА, ВНУТРІШНІЙ МОДУЛЬ, РАДІОМОДУЛЬ,
КОМУТАТОР, МАРШРУТИЗАТОР, ОПЕРАЦІЙНА СИСТЕМА,
МЕРЕЖА.

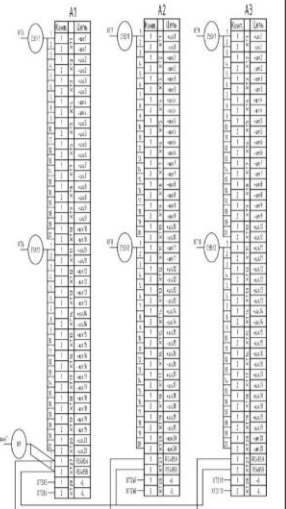
[illegible]

ДОДАТОК Е

Схема соединений ШП1



Поз. обозначение	Наименование	Кол.	Примечание
20	ШК-интер	2	
21	ШК-интер	2	
22	ШК-интер	2	
23	ШК-интер	2	
24	ШК-интер	2	
25	ШК-интер	2	
26	ШК-интер	2	
27	ШК-интер	2	
28	ШК-интер	2	
29	ШК-интер	2	
30	ШК-интер	2	
31	ШК-интер	2	
32	ШК-интер	2	
33	ШК-интер	2	
34	ШК-интер	2	
35	ШК-интер	2	
36	ШК-интер	2	
37	ШК-интер	2	
38	ШК-интер	2	
39	ШК-интер	2	
40	ШК-интер	2	
41	ШК-интер	2	
42	ШК-интер	2	
43	ШК-интер	2	
44	ШК-интер	2	
45	ШК-интер	2	
46	ШК-интер	2	
47	ШК-интер	2	
48	ШК-интер	2	
49	ШК-интер	2	
50	ШК-интер	2	
51	ШК-интер	2	
52	ШК-интер	2	
53	ШК-интер	2	
54	ШК-интер	2	
55	ШК-интер	2	
56	ШК-интер	2	
57	ШК-интер	2	
58	ШК-интер	2	
59	ШК-интер	2	
60	ШК-интер	2	
61	ШК-интер	2	
62	ШК-интер	2	
63	ШК-интер	2	
64	ШК-интер	2	
65	ШК-интер	2	
66	ШК-интер	2	
67	ШК-интер	2	
68	ШК-интер	2	
69	ШК-интер	2	
70	ШК-интер	2	
71	ШК-интер	2	
72	ШК-интер	2	
73	ШК-интер	2	
74	ШК-интер	2	
75	ШК-интер	2	
76	ШК-интер	2	
77	ШК-интер	2	
78	ШК-интер	2	
79	ШК-интер	2	
80	ШК-интер	2	
81	ШК-интер	2	
82	ШК-интер	2	
83	ШК-интер	2	
84	ШК-интер	2	
85	ШК-интер	2	
86	ШК-интер	2	
87	ШК-интер	2	
88	ШК-интер	2	
89	ШК-интер	2	
90	ШК-интер	2	
91	ШК-интер	2	
92	ШК-интер	2	
93	ШК-интер	2	
94	ШК-интер	2	
95	ШК-интер	2	
96	ШК-интер	2	
97	ШК-интер	2	
98	ШК-интер	2	
99	ШК-интер	2	
100	ШК-интер	2	



1. Обозначения компонентов элементов XT1-4, XT5, XT1-2, G1-2 приведены в приложении	
159753-12-0034.4	
Генеральный инженер-проектировщик	
Административно-хозяйственный отдел	
Система автоматизации	
Схема соединений ШП1	
340	
Инженер-проектировщик	

Лестничными клетками, санузлами и им подобными помещениями условно пренебрегаем.

1. Перечень оборудования приведен на схеме общей.
2. Марки и длины кабелей приведены в кабельном журнале.
3. Кабели проложить за подвесным потолком в кабель-каналах, выполнить в кабель-каналах Legrand 20х12,5.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

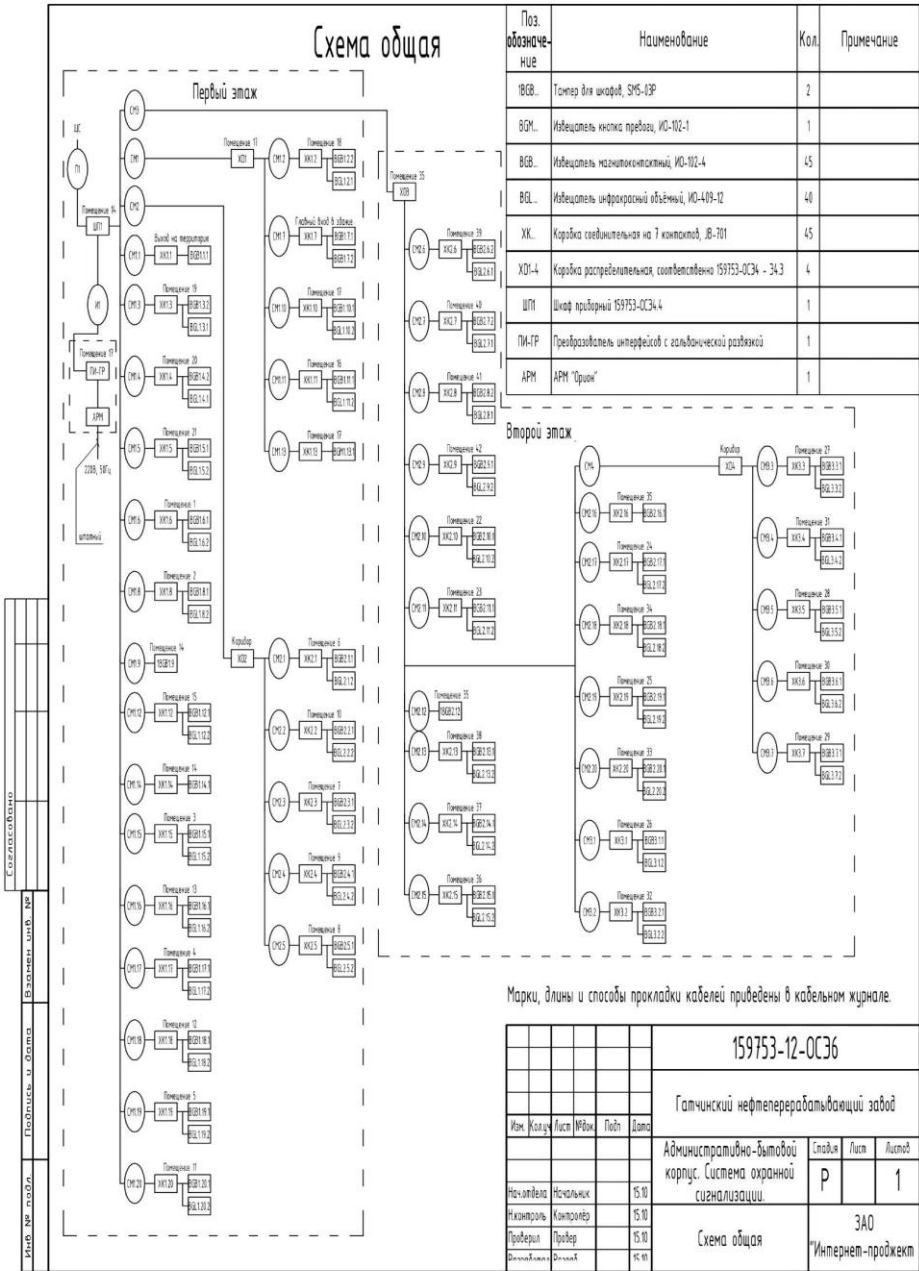
159753-12-0СЗ

Лестничными клетками, санузлами и им подобными помещениями условно пренебрегаем.

1. Перечень оборудования приведен на схеме общей.
2. Марки и длины кабелей приведены в кабельном журнале.
3. Кабели проложить за подвесным потолком в кабель-каналах. Спуски к ТСО выполнить в кабель-каналах Legrand 20x12,5.

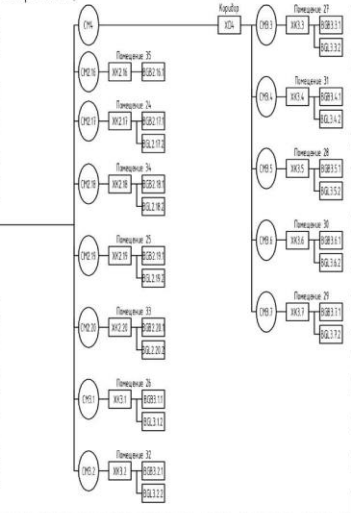
					159753-12-ОС37		
					Гатчинский нефтеперерабатывающий завод		
Имя	Класс	Адрес	Имя	Пол	Дата	Административно-бытовой корпус. Система охранной сигнализации.	
Начальник	Начальник				15.10	Столбы	Лист
Начальник	Контролер				15.10	P	1
Проверил	Провер				15.10	3АО	
Одобрено	Одобр				15.10	"Интернет-проект"	

Схема общая



Поз. обозначение	Наименование	Кол.	Примечание
1ВВВ.	Тензор для шкафов, 5М5-13Р	2	
ВВМ.	Индикатор кнопки тревоги, ИВ-102-1	1	
ВВВ.	Индикатор магнитоконтактный, ИВ-102-4	45	
ВВЛ.	Индикатор инфракрасный объёмный, ИВ-109-12	40	
ХК.	Коробка соединительная на 7 контактов, КВ-701	45	
ХВ1.4	Коробка распределительная, соответствует 159753-ОС34 - 34.3	4	
ШП.	Шкаф приборный 159753-ОС34.4	1	
ПМ-ГР	Предохранитель интерфейса с асимметрической развязкой	1	
АРМ	АРМ "Орион"	1	

Второй этаж



Марки, длины и способы прокладки кабелей приведены в кабельном журнале.

159753-12-ОС36					
Гатчинский нефтеперерабатывающий завод					
Административно-бытовой корпус. Система охранной сигнализации.					
Изм.	Кол.	Лист	Мф	Лист	Лист
Исполн.	Исполн.	15.10	Исполн.	15.10	15.10
Исполн.	Исполн.	15.10	Исполн.	15.10	15.10
Исполн.	Исполн.	15.10	Исполн.	15.10	15.10
Схема общая				340	
				Интернет-проект	

Позиция	Наименование и техническая характеристика	Тип, марка, обозначение документа, опросного листа	Код оборудования, изделия, материала	Завод-изготовитель	Единица измерения	Количество	Масса единицы, кг	Примечания
	<u>1.Оборудование</u>							
1.	Извещатель магнитоконтактный ИО-102-4	ИО-102-4			шт	50		8 пом числе 5 шт в ЗИП
2.	Тонер для шкода	SMS-33P			шт	2		
3.	Извещатель ИК объемный "Фотон-10"	ИО4-05-12			шт	44		8 пом числе 4 шт в ЗИП
4.	Кнопка тревожной сигнализации	ИО-102-1			шт	1		
5.	БРП 24-01, +12В/3А/7А+	БРП 24-01			шт	3		8 пом числе 1 шт в ЗИП
6.	Процор привода-контрольный охранно-пожарный, 20 шлейфов	Сенска-20			шт	4		8 пом числе 1 шт в ЗИП
7.	Электронно-вычислительная система для АРМ "Орион" в составе:				комп	1		
8.	Программное обеспечение АРМ "Орион"	АРМ "Орион"			комп	1		
9.	Преобразователь интерфейсов RS 232 - RS 485	ПМ-ТР			шт	1		
	<u>2.Кабели и провод</u>							
1.	Кабель оптический	КСГВ 4x0,5			м	670		
2.	Кабель силовой ВВГ 3x1,5	ВВГ 3x1,5			м	15		
3.	Провод кроссовый ГКСВ 2x0,5	ГКСВ 2x0,5			м	70		
4.	Кабель телефонный 10 пар	ТППан 10x2x0,5			м	75		
5.	Кабель телефонный 50 пар	ТППан 50x2x0,5			м	15		
6.	Кабель компьютерный 6/н 4x2x0,5	ВТР 3/45			м	15		
	<u>3.Электроника и установка продукция</u>							
1.	Блок замков на 10 контактов, зазор 0,35-4мм	БЗ 24-4x25-8/093-10			шт	1		
2.	Плмт светодиодный 2/10 с размыкаемыми контактами, 0,9	LSA-PLUS 6089 1 102-06			шт	24		
3.	Плмт светодиодный 2/38	LSA-PLUS 6089 2 017-00			шт	4		
4.	Хвостик монтажный 2/10 на 10 модулей, глубина 50мм	6050 3 150-10			шт	2		
5.	Коробка светодиодная на 7 контактов	JB 701			шт	45		

Согласовано

Взам. инв. №

Подп. и дата

Инв. № подл.

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Обозначение провода, кабеля	Откуда идет		Куда поступает		Марка	Длина, м	Назначение	Примечание
	Обозначение прибора	Место размещения прибора	Обозначение прибора	Место размещения прибора				
1	2	3	4	5	6	7	8	9
СМ1.1	ШП1	Первый этаж. Помещение 14	ХК1.1	Первый этаж. Выход на территорию	КСТВ 4x0,5	15	Сигнал, питание ±12В	6С, Б2
СМ1.2	ХД1	Первый этаж. Помещение 17	ХК1.2	Первый этаж. Помещение 18	КСТВ 4x0,5	10	Сигнал, питание ±12В	6С, Б2
СМ1.3	ШП1	Первый этаж. Помещение 14	ХК1.3	Первый этаж. Помещение 19	КСТВ 4x0,5	15	Сигнал, питание ±12В	6С, Б2
СМ1.4	ШП1	Первый этаж. Помещение 14	ХК1.4	Первый этаж. Помещение 20	КСТВ 4x0,5	10	Сигнал, питание ±12В	6С, Б2
СМ1.5	ШП1	Первый этаж. Помещение 14	ХК1.5	Первый этаж. Помещение 21	КСТВ 4x0,5	10	Сигнал, питание ±12В	6С, Б2
СМ1.6	ШП1	Первый этаж. Помещение 14	ХК1.6	Первый этаж. Помещение 1	КСТВ 4x0,5	15	Сигнал, питание ±12В	6С, Б2
СМ1.7	ХД1	Первый этаж. Помещение 17	ХК1.7	Первый этаж. Главный вход в здание	КСТВ 4x0,5	5	Сигнал	6С, Б2
СМ1.8	ШП1	Первый этаж. Помещение 14	ХК1.8	Первый этаж. Помещение 2	КСТВ 4x0,5	10	Сигнал, питание ±12В	6С, Б2
СМ1.9	ШП1	Первый этаж. Помещение 14	ВГВ1.9	Первый этаж. Помещение 14	КСТВ 4x0,5	0	Сигнал	
СМ1.10	ХД1	Первый этаж. Помещение 17	ХК1.10	Первый этаж. Помещение 17	КСТВ 4x0,5	5	Сигнал, питание ±12В	6С, Б2
СМ1.11	ХД1	Первый этаж. Помещение 17	ХК1.11	Первый этаж. Помещение 16	КСТВ 4x0,5	5	Сигнал, питание ±12В	6С, Б2
СМ1.12	ШП1	Первый этаж. Помещение 14	ХК1.12	Первый этаж. Помещение 15	КСТВ 4x0,5	5	Сигнал, питание ±12В	6С, Б2
СМ1.13	ХД1	Первый этаж. Помещение 17	ХК1.13	Первый этаж. Помещение 17	КСТВ 4x0,5	5	Сигнал	6С, Б2
СМ1.14	ШП1	Первый этаж. Помещение 14	ХК1.14	Первый этаж. Помещение 14	КСТВ 4x0,5	5	Сигнал, питание ±12В	6С, Б2
СМ1.15	ШП1	Первый этаж. Помещение 14	ХК1.15	Первый этаж. Помещение 3	КСТВ 4x0,5	15	Сигнал, питание ±12В	6С, Б2
СМ1.16	ШП1	Первый этаж. Помещение 14	ХК1.16	Первый этаж. Помещение 13	КСТВ 4x0,5	15	Сигнал, питание ±12В	6С, Б2
СМ1.17	ШП1	Первый этаж. Помещение 14	ХК1.17	Первый этаж. Помещение 4	КСТВ 4x0,5	20	Сигнал, питание ±12В	6С, Б2
СМ1.18	ШП1	Первый этаж. Помещение 14	ХК1.18	Первый этаж. Помещение 12	КСТВ 4x0,5	20	Сигнал, питание ±12В	6С, Б2
СМ1.19	ШП1	Первый этаж. Помещение 14	ХК1.19	Первый этаж. Помещение 5	КСТВ 4x0,5	20	Сигнал, питание ±12В	6С, Б2
СМ1.20	ШП1	Первый этаж. Помещение 14	ХК1.20	Первый этаж. Помещение 11	КСТВ 4x0,5	25	Сигнал, питание ±12В	6С, Б2
СМ2.1	ХД2	Первый этаж. Коридор	ХК2.1	Первый этаж. Помещение 6	КСТВ 4x0,5	5	Сигнал, питание ±12В	6С, Б2
СМ2.2	ХД2	Первый этаж. Коридор	ХК2.2	Первый этаж. Помещение 10	КСТВ 4x0,5	5	Сигнал, питание ±12В	6С, Б2
СМ2.3	ХД2	Первый этаж. Коридор	ХК2.3	Первый этаж. Помещение 7	КСТВ 4x0,5	5	Сигнал, питание ±12В	6С, Б2
СМ2.4	ХД2	Первый этаж. Коридор	ХК2.4	Первый этаж. Помещение 9	КСТВ 4x0,5	10	Сигнал, питание ±12В	6С, Б2
СМ2.5	ХД2	Первый этаж. Коридор	ХК2.5	Первый этаж. Помещение 8	КСТВ 4x0,5	10	Сигнал, питание ±12В	6С, Б2
СМ2.6	ХД3	Второй этаж. Помещение 35	ХК2.6	Второй этаж. Помещение 39	КСТВ 4x0,5	20	Сигнал, питание ±12В	6С, Б2
СМ2.7	ХД3	Второй этаж. Помещение 35	ХК2.7	Второй этаж. Помещение 40	КСТВ 4x0,5	15	Сигнал, питание ±12В	6С, Б2
СМ2.8	ХД3	Второй этаж. Помещение 35	ХК2.8	Второй этаж. Помещение 41	КСТВ 4x0,5	10	Сигнал, питание ±12В	6С, Б2
Инв. № подл.								Лист
					159753-12-ОСТБ			2

Иск.	Коп. зап.	Лист	ВРЗск	Подп.	Дата

В графе «Примечание» таблицы указан вид прокладки кабелей и проводов в соответствии с таблицей обозначений:

Таблица обозначений

Обозначение	Вид прокладки
1	В металлорукаве.
2	В ПВХ трубе.
3	В стальной трубе.
4	В асбоцементной трубе.
5	В существующих стояках и трубной разводке.
6	В коробе, лотке.
7	Открыто.
8	Скрыто, в штробе.
9	На тросовом подвесе.
Н	Наружная (по ограждению, стене сооружения).
С	Внутренняя (по стене сооружения).
З	Подземная.
Э	По эстакаде.
Д	В полу.
В	За подвесным потолком.
П	По основному полу.

1. Допускается замена марок указанных кабелей на марки кабелей, аналогичные по техническим характеристикам.
2. Способы прокладки кабелей уточнить при монтаже по результатам завершения строительных работ.

Инв. № подл.	Подп. и дата	Взам.инв. №	159753-12-ОСТБ					
			Гатчинский нефтеперерабатывающий завод					
			Изм.	Кол.уч.	Лист	№ док.	Подпись	Дата
			Административно-бытовой корпус.					
			Система охранной сигнализации.					
						Стадия	Лист	Листов
						Р	1	3
						Кабельный журнал		
						ЗАО «Интернет-проджект»		