UNICHECK

Ім'я користувача:
приховано налаштуваннями конфіденційності

ID перевірки:
1015577078

Дата перевірки:
13.06.2023 09:28:53 EEST

Тип перевірки:
Doc vs Library

Дата звіту:
13.06.2023 09:30:44 EEST

ID користувача:
100011372

Назва документа: **Гр ЕЗ-41 Фенікс Віктор**

Кількість сторінок: **41** Кількість слів: **7258** Кількість символів: **55278** Розмір файлу: **1.93 MB** ID файлу: **1015227439**

8.32%
Схожість

Найбільша схожість: **2.99%** з джерелом з Бібліотеки (ID файлу: **1004215970**)

Пошук збігів з Інтернетом не проводився

8.32% Джерела з Бібліотеки | 35 ..... Сторінка 43

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 10

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Аналітичний огляд існуючих рішень

1.1.1 Інформаційні технології підвищення ефективності управління діяльністю підприємства

Зовнішні загрози – це, вірусні атаки, атаки типу «відмова в обслуговуванні» (у тому числі розподілені), несанкціонований доступ на сервери компанії, порушення конфіденційності інформації, що передається. Їх поява обумовлена взаємодією підприємства із зовнішніми інформаційними системами. Але замикатися на зовнішніх загрозах, недооцінюючи серйозність внутрішніх загроз, було б помилкою, оскільки значно більший збиток компанії може нанести некоректну поведінку співробітників, що порушують корпоративну політику безпеки.

Внутрішні атаки не відносяться до загальних типів атак. На відміну від зовнішніх зловмисників, внутрішній порушник – це авторизований користувач, що має офіційний доступ до ресурсів інтрамережі, у тому числі до тих, в яких циркулює конфіденційна інформація. В Україні в основному використовують служби інформаційної безпеки для захисту периметра інтрамережі, а захисту від внутрішніх загроз надається набагато менше увага. Насправді ж уявлення про те, що безпеку можна забезпечити захистом периметра мережі від зовнішніх атак, вже давно зжило себе. Необхідно виробляти комплексну стратегію, що забезпечує безпеку на всіх рівнях – на рівні шлюзу, серверу і клієнта.

У даний час левову частку вітчизняного ринку інформаційної безпеки складають міжмережні екрани, системи запобігання комп'ютерних атак (Intrusion Prevention Systems - IPS) і антивірусні системи.

Об'єднуючи ці дві технології і усуваючи таким чином їх взаємні недоліки, можна одержати засіб виявлення відомих і невідомих атак. У підходах ведучих виробників засобів інформаційної безпеки в даний час

домінує принцип ешелонованого захисту. Замість окремих міжмережних екранів, пристроїв організації віртуальних приватних мереж (VPN), антивірусних систем, систем виявлення і запобігання вторгнень на ринок поставляються комплексні рішення, у тому числі і на програмно-апаратній основі (security appliance), що інтегруються в інфраструктуру компанії для забезпечення інформаційного захисту на всіх рівнях. Перехід до об'єднання в одному продукті основних засобів інформаційного захисту не тільки дає можливість спростити мережну інфраструктуру, але і забезпечує багаторівневий захист з більш ефективним управлінням.

Інформаційну безпеку, цю, треба сказати, не маленьку статтю витрат, раніше могли дозволити собі тільки крупні компанії. Компаніям середнього і малого бізнесу високий рівень безпеки був не по кишені через високу вартість і складність розрізнених рішень. До тих пір, поки ці рішення не сталі об'єднувати в багатофункціональні апаратні і програмно-апаратні комплекси. Подібна інтеграція дозволила значно понизити загальну вартість володіння засобами захисту інформації, спростити процес установки і адміністрування і в теж час підвищити рівень безпеки інформаційних ресурсів, що захищаються. Фізичне об'єднання впливає, в першу чергу, на вартість системи, оскільки одна платформа дешевше декількох, а технічні ресурси в такій консолідованій системі використовуються ефективно. До того ж ці рішення легко інтегруються в корпоративне середовище.

Практично всі основні виробники засобів захисту пропонують свої рішення в цьому сегменті.

При установці програмно-апаратних засобів захисту в розрив мережі вимоги до надійності і відмовостійкості зростають у декілька разів, оскільки вихід з ладу пристрою спричинить за собою порушення функціонування мережі. Щоб уникнути цього, розробники передбачають механізми так званого апаратного шунтування, що забезпечує безперешкодний прохід мережного трафіку через пристрій у разі порушень в його роботі.

Прислухаючись до загальних тенденцій на ринку інформаційної безпеки, розробники об'єднують різні засоби захисту. Це робить подібні з'єднані пристрої більш гнучкими при упровадженні в інформаційні системи підприємств і набагато спрощує процес установки і експлуатації.

Тенденція заміни програмних рішень програмно-апаратними комплексами збережеться. Можна припустити, що ще більше зросте популярність програмно-апаратних рішень з єдиним центром управління як серед виробників, так і серед споживачів.

Оцінивши нинішній рівень розвитку технологій інформаційної безпеки, можна вивести формулу ефективного захисту: інтеграція апаратної платформи, міжмережного екрану і системи виявлення і запобігання вторгнень, що використовує сигнатурний і поведінковий аналіз.

В даній дипломній роботі пропонується побудова системи захисту локальної комп'ютерної мережі на основі апаратного пристрою – файєрвола.

Взагалі апаратні засоби захисту інформації – це різні технічні пристрої, системи і споруди, призначені для захисту інформації від розголошування, витоку і несанкціонованого доступу.

До апаратних засобів забезпечення інформаційної безпеки відносяться самі різні за принципом роботи, пристроєм і можливостями технічні засоби, що забезпечують припинення розголошування, захист від витоку і протидію несанкціонованому доступу до джерел конфіденційної інформації.

Використовування апаратних засобів захисту інформації дозволяє вирішувати наступні задачі:

– проведення спеціальних досліджень технічних засобів на наявність можливих каналів просочування інформації;

– виявлення каналів просочування інформації на різних об'єктах і в приміщеннях;

– локалізація каналів просочування інформації;

– пошук і виявлення засобів промислового шпигунства;

– протидія несанкціонованому доступу до джерел конфіденційної інформації і інших дій.

Сучасний ринок пристроїв захисту мережі містить велику кількість представників даного класу.

Основні конкуренти запропонованого в даній дипломній роботі центру безпеки – це такі програмно-апаратні комплекси: Imperva Web Application Firewall (рис.1.1), TippingPoint (рис.1.2), IBM Proventia Network Intrusion Prevention System (рисунок 1.3) та інші.

Рисунок 1.1 – Imperva Web Application Firewall

Рисунок 1.2 – TippingPoint

Рисунок 1.3 – IBM Proventia Network Intrusion Prevention System

Але, не дивлячись на безумовні гідності кожного з вище вказаних пристроїв, в дипломному проекті було зроблено вибір на користь між мережного екрану Juniper.

Шлюзи безпеки Secure Services Gateway 5 (SSG 5) і Secure Services Gateway 20 (SSG 20) – це спеціалізовані пристрої безпеки, які чудово поєднують в собі продуктивність, безпека і можливості по підключенню невеликих офісів до LAN/WAN (рис.1.4). Весь вхідний і витікаючий трафік офісу захищається від мережних черв'яків, шпигунського програмного забезпечення, Трої і іншого шкідливого ПЗ за допомогою фірмової технології Unified Threat Management (UMT), до складу якої входять міжмережевий екран з контролем полягання сесій, система запобігання вторгнень, антивірус, антиспам і веб-фільтр.

Рисунок 1.4 – Пристрої захиситу Junipe

Багатий функціонал дозволяє використовувати SSG 5 і SSG 20 як комплексний пристрій, що забезпечує безпеку мережі. Підтримка функцій маршрутизації дозволяє використовувати SSG 5 і SSG 20 як традиційний маршрутизатор або як пристрій, об'єднуючий функціонал маршрутизатора і пристрою захисту мережі. Таким чином, SSG дозволяє істотно понизити капітальні і операційні витрати на IT-інфраструктуру.

SSG 5 і SSG 20 надають клієнтам безліч переваг.

Розширювана модульна архітектура об'єднує фіксовані LAN-порти з можливістю додаткової установки модулів WAN-портів.

Технологія UTM, заснована на кращих в своєму класі рішеннях, дозволяє захистити мережу від всіх видів атак.

Спеціалізована, орієнтована на безпеку, апаратна платформа володіє достатньою продуктивністю, щоб забезпечувати захист як на високих швидкостях LAN, так і в WAN-каналах.

Вживані великими і маленькими компаніями, а також провайдерами, SSG 5 і SSG 20 ідеально підходять для установки і в інших місцях з набагато меншою кількістю персоналу, але по-прежнему вимагаючих захисту критичного трафіку, передаваного по WAN або LAN. Типові інсталяції включають підприємства малого бізнесу, філіали, точки роздрібної торгівлі і видалених співробітників, що працюють з будинку.

SSG 5 – це пристрій з фіксованою конфігурацією портів. Пропускна спроможність міжмережевого екрану складає 160 Мбіт/с. На борту SSG 5 розташовується сім вбудованих портів 1 0/100 і один WAN-порт (ISDN BRI S/T, V.92 або RS-232 Serial/Aux). Опциональная підтримка протоколів 802.1 1 a/b/g і широкий спектр можливостей по захисту бездротових мереж дозволяє використовувати SSG 5 одночасно як пристрій безпеки, маршрутизатора і точки бездротового доступу.

SSG 20 – це модульний пристрій. Пропускна спроможність міжмережевого екрану складає 160 Мбіт/с. SSG 20 оснащений п'ятьма вбудованими портами 10/100 і двома слотами для установки WAN-модулів (ADSL2+, E1, ISDN BRI S/T, V.92). Опциональная підтримка протоколів 802.11 a/b/g і широкий спектр можливостей по захисту бездротових мереж дозволяє використовувати SSG 20 одночасно як пристрій безпеки, маршрутизатора і точки бездротового доступу.

Міжмережуий екран з контролем полягання сесій з'єднаний з широким спектром функціональних модулів UTM, серед яких: запобігання атак (IPS, Deep Inspection), антивірус (включаючи протидію шпигунському ПЗ, Adware і фишингу), антиспам і веб-фільтрація. МСЕ надійно захищає локальний і

інтернет-трафік від мережних черв'яків, Трої і іншого шкідливого ПО, а також нових типів мережних атак.

Комбінація LAN/WAN інтерфейсів і підтримка різних мережних протоколів надає замовникам можливість установки SSG 5 і SSG 20 як традиційний LAN-файрвол-ла або як пристрій, об'єднуючий в собі функції маршрутизації і захисту, тим самим, зменшуючи сукупну вартість володіння (TCO).

SSG 5 і SSG 20 надає розширений набір опцій по сегментації мережі: зони безпеки (Security Zones), віртуальні маршрутизатори (Virtual Routers) і VLAN-ы. Це дозволяє адміністратору гнучко настроювати різні рівні захисту різним групам користувачів, розділяючи мережу на окремі захищені домени, кожний з своєю власною політикою безпеки.

В дипломній роботі пропонується використання в мережі саме моделі Juniper SSG 20.

1.1.2 Локальні комп'ютерні мережі

Мережа – група комп'ютерів, з'єднаних другу іншому за допомогою спеціального устаткування, що забезпечує обмін інформацією між ними. З'єднання між двома комп'ютерами може бути безпосереднім або з використанням додаткових вузлів зв'язку.

Надалі комп'ютер, що підключений до мережі, називається робочою станцією (Workstation). Як правило, із цим комп'ютером працює людина, у мережі присутні й такі комп'ютери, на яких ніхто не працює. Вони використовуються як керуючі центри в мережі і як накопичувачі інформації. Такі комп'ютери називають серверами.

Якщо комп'ютери розташовані порівняно недалеко друг від друга й з'єднані за допомогою високошвидкісних мережних адаптерів (швидкість передачі даних - 10-100 Мбіт/с), то такі мережі називаються локальними. При використанні локальної мережі комп'ютери, як правило, розташовані в межах однієї кімнати, будинку або в декількох близько розташованих будинках,

Для об'єднання комп'ютерів або цілих локальних мереж, які розташовані на значній відстані друг від друга, використовуються модеми, а також виділені чи супутникові канали зв'язку. Такі мережі звуться глобальних. Звичайно швидкість передачі даних у таких мережах значно нижче, ніж у локальні.

Існують два види архітектури мережі: однорангова (Peer-to-peer) та клієнт/ сервер (Client/Server). На даний момент архітектура клієнт/сервер практично витиснула однорангову.

Якщо використовується однорангова мережа, то всі комп'ютери, що входять у неї, мають однакові права. Відповідно, будь-який комп'ютер може виступати в ролі сервера, що надає доступ до своїх ресурсів, або клієнта, що використовує ресурси інших серверів,

У мережі, побудованої на архітектурі клієнт/сервер, існує кілька основних комп'ютерів - серверів. Інші комп'ютери, які входять у мережу, звуться клієнтів, або робітників станцій.

Сервер – це комп'ютер, що обслуговує інші комп'ютери в мережі. Існують різноманітні види серверів, що відрізняються друг від друга послугами, які вони надають: сервери баз даних, файлові сервери, принт сервери, поштові сервери, Web-сервери й т. д.

Однорангова архітектура одержала поширення в невеликих офісах або в домашніх локальних мережах. У більшості випадків, щоб створити таку мережу, вам знадобиться пара комп'ютерів, які постачені мережними картами, і кабель. В якості кабелю використовують, як правило, виту пару четвертої або п'ятої категорії.

Після того як мережа буде створена, а комп'ютери з'єднані між собою, потрібно настроїти всі необхідні параметри програмно. Насамперед встановити операційні системи з підтримкою роботи в мережі Linux, FreeBSD, Windows 7, Windows 10, Windows Server 2019.

У випадку використання архітектури мережі клієнт/сервер керування доступом здійснюється на рівні користувачів. В адміністратора з'являється можливість дозволити доступ до ресурсу тільки деяким користувачам.

Щоб одержати доступ до ресурсу в локальній мережі, побудованої на архітектурі клієнт/сервер, користувач зобов'язаний увести ім'я користувача (Login - логін) і пароль (Password). Слід зазначити, що ім'я користувача є відкритою інформацією (наприклад, обов'язково потрібно знати ім'я користувача, щоб відправити йому електронний лист), а пароль - конфіденційної.

Процес перевірки ім'я користувача називається ідентифікацією. Процес перевірки відповідності уведеного пароля ім'я користувача - аутентифікацією. Разом ідентифікація й аутентифікація становлять процес авторизації. Часто термін «аутентифікація» - використовується в широкому змісті: для позначення перевірки дійсності.

Із усього сказаного можна зробити висновок про те, що єдина перевага однорангової архітектури – це її простота й невисока вартість. Мережі клієнт/сервер забезпечують більше високий рівень швидкодії й захисту.

Важливим етапом реалізації проекту побудови мережі, є вибір орієнтації на мережні технології, які повинні забезпечувати необхідну продуктивність і

перспективність системи. Проте вибір мережної технології вимагає ретельного аналізу мережного трафіку, що генерується кожною робочою групою, окремими підрозділами підприємства. Локалізація цього трафіку, об'єднання його локальних потоків, розділення на сегменти широкомовних запитів допомагають визначити відповідну стратегію у виборі тієї або іншої мережної технології, на базі якої здійснюватиметься розвиток системи в цілому.

Нижче наведено коротку характеристику деяких сучасних технологій локальних мереж.

Ethernet, що виникла в 1973 році, є технологією з середовищем передачі, що розділяється, а на практиці має на увазі розділення максимальної пропускної здібності 10 Mbps серед всіх користувачів.

Проте із зростанням мережі все велике число користувачів експлуатують магістраль з фіксованою пропускною здібностю, що спричиняє за собою зниження продуктивності мережі з розрахунку на одного клієнта. Також, більш могутні комп'ютери і сучасні мережні додатки вимагають все більш високої продуктивності мережі.

Одним з варіантів підвищення смуги пропускання є зменшення кількості вузлів в мережі, що автоматично збільшує пропускну здібность з розрахунку на одного користувача. В ідеальному випадку вся пропускна здібность 10 Mbps надається одному користувачу. Такий підхід отримав назву сегментації і фактично полягає в розбитті мережі на невеликі сегменти. Для взаємодії користувачів цих сегментів застосовується комутатор, що виконує функції міжсегментної взаємодії.

Щоб подолати бар'єр смуги пропускання в 10 Mbps, слід звернутися до однієї з конкуруючих швидкісних технологій мережної передачі: ATM (асинхронний режим передачі), FDDI, 100VG-AnyLAN або Fast Ethernet, з яких Fast Ethernet дозволяє провести найплавніший перехід від найпопулярніших сьогодні мереж Ethernet, що працюють із швидкістю 10 Mbps, до високопродуктивних мереж з пропускною спроможністю 100 Mbs, і навіть 200 Mbs в режимі повного дуплексу.

Fast Ethernet базується на тому ж протоколі доступу до середовища CSMA/CD підрівня MAC канального рівня, який є ядром технології Ethernet. Це означає, що формат пакетів, їх довжина, методи виправлення помилок і управління визначені в Fast Ethernet точно так, як і в попередньому стандарті. Тому перехід на більш високопродуктивні устаткування не зажадає, як зміни існуючих мережних додатків і систем управління, так і перенавчання користувачів. До того ж зберігаються інвестиції вкладені в прокладку кабельних систем, оскільки Fast Ethernet підтримує виту пару, що стала сьогодні стандартом.

У міру збільшення продуктивності робочих станцій, додатки вимагають більшій пропускній здібності для доступу користувачів, що використовують

нові формати, такі як мультимедіа, відео, Intranet і Internet. Достатня пропускна здібность мережі стає центральною задачею для забезпечення зростаючих потреб користувачів.

Рішення достатньо прозоро: продуктивність мережної інфраструктури повинна бути еквівалентний можливостям робочих станцій, що ростуть. У зв'язку з цим повинні бути розроблені високошвидкісні з'єднання, щоб зменшити зростаючу напруженість трафіку, ліквідовувати вузькі місця і, таким чином підвищити продуктивність людей, які використовують обчислювальну мережу.

В той же час, нові рішення повинні бути сумісні з існуючими технологіями, щоб захистити інвестиції в мережну інфраструктуру. По цій і іншим причинам, Gigabit Ethernet з'явився як промисловий стандарт для локальних високошвидкісних обчислювальних мереж.

Gigabit Ethernet - розширення стандартів 10Mbps (10BASE-T) Ethernet та 100Mbps (100BASE-T) Fast Ethernet для обчислювальних мереж. Gigabit Ethernet повністю сумісний з Ethernet і Fast Ethernet. Початкова специфікація Ethernet була визначена як формат фрейма і підтримка протоколу CSMA/CD, повний дуплекс, управління потоком і управління об'єктами, як визначено стандартом IEEE 802.3. Gigabit Ethernet підтримує всі ці специфікації.

Gigabit Ethernet може служити як високошвидкісна магістраль і, потенційно, замінити інші типи магістральних технологій або виступати як високошвидкісне між`єднання декількох корпусів або будівель (при відстані між ними менше ніж домен колізій), між робочими групами або серверами.

На сьогоднішній день технологія Gigabit Ethernet може забезпечити передавання даних по мережі з пропускної здібністю до 1000 Мбіт/с, що з повним правом може представляти цю технологію як високо швидку.

Порядок розташування й підключення комп'ютерів і інших елементів у мережі називають мережною топологією. Топологію можна зрівняти з картою мережі, на якій відображені робочі станції, сервери та інше мережне встаткування. Обрана топологія впливає на загальні можливості мережі, протоколи й мережне

встаткування, які будуть застосовуватися, а також на можливість подальшого розширення мережі.

Фізична топологія – це опис того, яким образом будуть з'єднані фізичні елементи мережі. Логічна топологія визначає маршрути проходження пакетів даних усередині мережі.

Виділяють три види топології мережі:

– шина;

– кільце;

– зірка.

У випадку шинної топології всі комп'ютери підключаються до одного кабелю, що називається шиною даних. При цьому пакет буде прийматися всіма комп'ютерами, які підключені до даного сегмента мережі.

Швидкодія мережі багато в чому визначається числом підключених до загальної шини комп'ютерів. Чим більше таких комп'ютерів, тим повільніше працює мережа. Крім того, подібна топологія може стати причиною різноманітних колізій, які

виникають, коли кілька комп'ютерів одночасно намагаються передати інформацію в мережу. Імовірність появи колізії зростає зі збільшенням кількості підключених до шини комп'ютерів. Схема даної топології зображена на (рис.1.5.).

Рисунок 1.5 – Шинна топологія

На рисунку також зображені термінатори. Такі пристрої встановлюються на кінцях мережі й обмежують поширення сигналу, замикаючи сегмент мережі. Якщо десь відбудеться обрив кабелю або хоча б на одному кінці мережі не буде встановлений термінатор, сигнал почне відбиватися від місця обриву й відповідного кінця мережі, що приведе до порушення зв'язку.

Переваги використання мереж з топологією «загальна шина» наступні:

– значна економія кабелю;

– простота створення й керування.

Основні недоліки:

– імовірність появи колізій при збільшенні числа комп'ютерів у мережі;

– обрив кабелю приведе до відключення безлічі комп'ютерів;

– низький рівень захисту переданої інформації. Будь-який комп'ютер може одержати дані, які передаються по мережі.

У випадку використання кільцевої топології всі комп'ютери мережі підключаються до єдиного кільцевого кабелю. Пакети проходять по кільцю в одному напрямку через всі мережні плати підключених до мережі комп'ютерів. Кожний комп'ютер буде підсилювати сигнал і відправляти його далі по кільцю. Мережа з такою топологією зображена на (рис.1.6).

Рисунок 1.6 – Мережа з кільцевою топологією

У представленій топології передача пакетів по кільцю організована маркерним методом. Маркер являє собою певну послідовність двійкових розрядів, що містять керуючі дані. Якщо мережний пристрій має маркер, то в

нього з'являється право на відправлення інформації в мережу. Усередині кільця може передаватися всього один маркер. Комп'ютер, що збирається транспортувати дані, забирає маркер з мережі й відправляє запитану інформацію з кільця. Кожний наступний комп'ютер буде передавати дані далі, поки цей пакет не дійде до адресата. Після одержання адресат поверне підтвердження про одержання комп'ютеру-відправникові, а останній створить новий маркер і поверне його в мережу.

Переваги даної топології наступні:

– ефективніше, ніж у випадку із загальною шиною, обслуговуються більші обсяги даних;

– кожний комп'ютер є повторювачем: він підсилює сигнал перед відправленням наступній машині, що дозволяє значно збільшити розмір мережі;

– можливість задати різні пріоритети доступу до мережі; при цьому комп'ютер, що має більший пріоритет, зможе довше затримувати маркер і передавати більше інформації.

Недоліки:

– обрив мережного кабелю приводить до непрацездатності всієї мережі;

– будь-який комп'ютер може одержати дані, які передаються по мережі.

При використанні зіркоподібної топології кожний кабельний сегмент, що йде від будь-якого комп'ютера мережі, буде підключатися до центрального комутатора. Всі пакети будуть транспортуватися від одного комп'ютера до іншого через цей пристрій. У випадку розриву з'єднання між комп'ютером і комутатором інша мережа продовжує працювати. Якщо ж комутатор вийде з ладу, то мережа працювати перестане. За допомогою зіркоподібної структури можна підключати друг до друга навіть локальні мережі. Мережа з такою топологією зображена на (рис.1.7).

Рисунок 1.7 – Мережа з топологією «зірка»

Використання даної топології зручно при пошуку ушкоджених елементів: кабелю, мережних адаптерів. «Зірка» набагато зручніше «загальної шини» та «кільця» і у випадку додавання нових пристроїв. Варто врахувати й те, що мережі зі швидкістю передачі 100 і 1000 Мбіт/с побудовані по топології «зірка».

Переваги «зірки»:

– простота створення й керування;

– високий рівень надійності мережі;

– висока захищеність інформації, що передається усередині мережі (якщо в центрі зірки розташований комутатор).

Основний недолік - поломка комутатора приводить до припинення роботи всієї мережі.

1.1.3 Пристрої мережі і засоби комутації

При створені комп'ютерної мережі головну роль грає вибір пристроїв, які забезпечують передачу інформації між комп'ютерами. Далі представлена характеристика основних пристроїв, необхідних для побудови мережі.

Мережні інтерфейсні плати (NIC, Network Interface Card) встановлюються на настільних і портативних комп'ютерах (рис.1.8). Вони служать для взаємодії з іншими пристроями в локальній мережі. Існує цілий спектр мережних плат для різних комп'ютерів, що мають певні вимоги

вимогам до продуктивності. Характеризуються за швидкістю передачі даних і способах підключення до мережі

Рисунок 1.8 – Мережнаінтерфейсна плата

Сучасні мережеві плати відіграють активну роль в підвищенні продуктивності, призначенні пріоритетів для відповідального трафіку (передаючої/приймаючої інформації) і моніторингу трафіку в мережі. Крім того, вони підтримують такі функції, як видалена активізація з центральної робочої станції або видалена зміна конфігурації, що значно економить час і сили адміністраторів мереж, що постійно ростуть.

У структурованій кабельній конфігурації всі комп'ютери, що входять в мережу, взаємодіють з комутатором.

Комутатор (Switch) – багатопортовий пристрій, що забезпечує високошвидкісну комутацію пакетів між портами (рис.1.9).

Рисунок 1.9 - Комутатор (Switch)

Комутатор надає кожному пристрою, або комп'ютеру, підключеному до одного з його портів, всю смугу пропускання мережі. Це підвищує продуктивність і зменшує час відгуку мережі за рахунок скорочення числа користувачів на сегмент. Комутатори часто конструюються для підтримки 10, 100, 1000 Мбіт/с, залежно від максимальної швидкості пристрою, що підключається. Якщо вони оснащуються засобами автоматичного пізнання швидкості передачі, то можуть самі настроюватися на оптимальну швидкість – змінювати конфігурацію в ручну не потрібно.

Маршрутизатори (Router) використовують для підключення локальних мереж (LAN) до територіально-розподілених мереж (WAN) та з'єднання декількох локальних мереж (рис.1.10).

Рисунок 1.10 – Маршрутизатор (Router)

Маршрутизатори залежать від використовуваного протоколу (наприклад, TCP/IP, IPX, AppleTalk) і, на відміну від мостів і комутаторів, що функціонують на другому рівні, працюють на третьому або сьомому рівні моделі OSI. Продуктивність маршрутизатора в плані об'єму передаваних даних в секунду звичай но пропорційна його вартості. Оскільки маршрутизатор працює на основі протоколу, він може ухвалювати рішення про якнайкращий маршрут доставки даних, керуючись такими чинниками як вартість, швидкість доставки і т. д. Крім того, маршрутизатори дозволяють ефективно управляти трафіком широкомовної розсилки, забезпечуючи передачу даних тільки в потрібні порти.

Модеми (рис.1.11) дозволяють користувачам комп'ютерів обмінюватися інформацією і підключатися до Internet по звичайних телефонних лініях.

Назва «модем» обумовлена функцією пристрою і означає «модулятор/демодулятор».

Модем модулює цифрові сигнали, що надходять від комп'ютера, в аналогові сигнали, передавані по телефонній мережі загального користування, а інший модем демодулює ці сигнали на приймальному кінці, знову перетворюючи їх в цифрову форму.

Рисунок 1.11 – Модем

На відміну від маршрутизаторів, що забезпечують загальний зовнішній доступ користувачів, модем підтримує в кожен момент тільки одне з'єднання. При цьому передбачається така ж оплата, як за телефон, включаючи вартість послуг міжміського зв'язку. Інсталяція модемів на центральному мережевому сервері може забезпечити їх сумісне використання. Для комп’ютерів застосовуються вбудовані і зовнішні модеми, а для портативних комп'ютерів звичайно використовуються модеми формату PC Card.

Далі будуть розглянуті основні засоби комутації мереж, а саме кабельні. Нижче наведено опис існуючих видів кабелю, що використовуються для передавання даних в комп`ютерних мережах.

Коаксіальний кабель (рис.1.12). Він має середню ціну, добре завадозахищений і застосовується для зв'язку на великі відстані (декілька кілометрів).

Рисунок 1.12 – Коаксіальний кабель

Швидкість передачі інформації від 1 до 10 Мбіт/с, а в деяких випадках може досягати 50 Мбіт/с. Коаксіальний кабель використовується для основної і широкосмугової передачі інформації.

На сьогоднішній день коаксіальний кабель як середовище передавання даних можна зустріти тільки в застарілих мережах. В сучасних використовуються інші два види кабелю, описані нижче.

Перший і найпоширеніший тип кабелю, що використовується в сучасних комп`ютерних мережах - вита пара (рис.1.13).

Кабель типу "вита пара" (TP, Twisted Pair) буває двох видів: екранована вита пара (STP, Shielded Twisted Pair) і неекранована вита пара (UTP, Unshielded Twisted Pair). Обидва типу кабелю складаються з пари скручених мідних проводів.

Рисунок 1.13 – Вита пара

Кабель типу "неекранована вита пара" став найбільш популярним завдяки своїй низькій вартості, гнучкості і простоті інсталяції. Єдиним недоліком такого кабелю є уразливість до електричних перешкод і "шумів" в лінії. Цей кабель дозволяє передавати інформацію із швидкістю до 100 Мбіт/с. Кабелі "вита пара" бувають різній категорії (3, 4 або 5). Чим вищий номер категорії, тим більшу швидкість передачі підтримує кабель.

Інший популярний вид кабелю – оптоволоконний кабель (рис.1.14) підтримує швидкість передачі даних 1000 Мбіт/с. Дані передаються за допомогою світлових імпульсів, що проходять по оптичному волокну.

Рисунок 1.14 – Оптоволокно

Хоча цей кабель набагато дорожче і складніше в інсталяції, він часто застосовується в центральних магістральних мережах, оскільки забезпечує повний захист від електричних перешкод і дозволяє передавати інформацію на дуже великі відстані. Крім того, завдяки вдосконаленню оптоволоконної технології даний кабель стає все більш прийнятним за ціною.

1.1.4 Мережні операційні системи для локальних мереж

Мережні операційні системи (ОС) – комплекс програм, що забезпечує обробку, передачу і збереження даних у мережі. Мережна ОС надає користувачам різні види мережних служб (керування файлами, електронна пошта, процеси керування мережею й ін.), підтримує роботу в абонентських системах.

Мережні операційні системи використовують архітектуру клієнт-сервер або однорангову архітектуру. Найбільш популярні ОС в світі на сьогоднішній день ОС сімейства Windows NT, що було оцінено з комплексу критеріїв: продуктивність, розмаїтість можливостей зв'язку користувачів, можливості адміністрування та інші. Тому далі буде описані саме ці ОС компанії Microsoft.

Операційна система Windows NT є багатофункціональною, призначена для архітектури клієнт-сервер і використання різних протоколів

транспортного рівня мережної ОС, має 32-розрядну та 64-разрядну архітектуру і забезпечує функції локальної мережі:

– можливість кожної абонентської системи в мережі бути сервером або клієнтом;

– спільну роботу групи користувачів; адресацію оперативної і зовнішньої пам'яті великого розміру;

– багатофункціональність обробки даних; підтримку мультипроцесорної обробки й інші.

Останніми версіями цих ОС являються Windows Server 2019 R2 – для серверів, та Windows 10 – для клієнтських ПК. Тому в даній бакалаврські роботі пропонується використання саме цих ОС. Нижче наведено їх основні характеристики.

Покращений робочий стіл. Windows 10 дає змогу переміщуватись елементами комп’ютера швидше, ніж будь-коли. Кнопки панелі завдань збільшено, і з’явилася можливість попереднього перегляду в повному розмірі. Окрім цього, тепер можна закріпити програму за однією з цих кнопок для швидкого запуску. Списки переходів містять ярлики на файли, папки та веб-сайти. А завдяки таким функціям, як Snap, Peek та Shake є можливість просто переходити між усіма відкритими вікнами.

Зручніший пошук. Введіть потрібний елемент у поле пошуку, розташованому в меню "Пуск",– і результати відобразяться миттєво та будуть згруповані за категоріями (документи, зображення, музика, електронна пошта та програми). Здійснюючи пошук у папці або бібліотеці, можно настроїти його, наприклад, застосувавши фільтр дати чи типу файлу. Коли пошук буде завершено, за допомогою панелі попереднього перегляду швидко ознайомтеся з результатами.

Швидкість понад усе. У Windows 10 підвищено продуктивність за основними показниками. Тепер операційна система використовує менше пам’яті та запускає фонові служби лише за потреби. Розробники цієї операційної системи працювали над тим, щоб прискорити такі операції, як

запуск програм, перехід комп'ютера до режиму сну та відновлення його роботи, а також повторне встановлення підключення до безпроводових мереж. Завдяки підтримці 64-розрядних версій можна скористатися всіма перевагами сучасних потужних комп'ютерів, оснащених 64-розрядним процесором.

Сьогодні можна переглядати веб-сайти, гортати фотографії, відкривати файли та папки на комп'ютері із сенсорним екраном одним дотиком пальця, адже відтепер Windows оснащено справжньою технологією мультидотику – Windows Touch. Масштабування, обертання зображень і навіть вибір правою кнопкою миші виконується спеціальними рухами – усе це формує зовсім інший підхід до роботи на ПК.

Ефективне відтворення із пристроїв. Device Stage – це нова функція у Windows 10, що працює як домашня сторінка для портативних музичних програвачів, смартфонів і принтерів. Після підключення будь-якого сумісного пристрою до ПК на екрані відобразиться меню з інформацією та популярними завданнями, зокрема заряд акумулятора, кількість готових до завантаження фотографій, а також параметри друку.

Завдяки новим можливостям у медіапрогравачі Windows 12 є можливість насолоджуватися файлами з медіатеки, незалежно від того, у якому куточку будинку або навіть міста ви знаходитесь. Відтворити за допомогою дає змогу виконувати потокове передавання музики, відео та фотографій із комп'ютера на стереосистему або телевізор (для цього може знадобитися додаткове обладнання). З функцією Віддалене потокове передавання медіаданих можна передавати потоком медіадані через Інтернет з одного комп'ютера під керуванням Windows 10 на інші, розташовані за тисячі кілометрів.

Центр підтримки – це нова функція у Windows 10, яка дає змогу стежити за повідомленнями стосовно настройок безпеки й обслуговування. Повідомлення можна вмикати та вимикати для таких об'єктів, як технологія Windows Defender або Служба захисту користувачів. Якщо Windows потребує

уваги, праворуч на панелі завдань відобразиться відповідне сповіщення. Його треба натиснути, щоб переглянути рекомендовані способи вирішення будь-яких проблем.

1.2 Розробка структурної схеми мережі

Структурна схема включає топологію мережі та кількісний склад апаратного забезпечення – робочих станцій, периферійних пристроїв, серверів та мережного устаткування.

Для ПП «Telnet» були обрані наступні параметри мережі.

В якості технології була вибрана Fast Ethernet, яка забезпечує швидкість передачі даних до 100 Мбіт/с.

Оптимальним типом топології на сьогоднішній день є «зірка».

В якості кабелю, використовуваного при прокладці локальної мережі фірми була вибрана «вита пара», що зумовлено параметрами ціна-якість.

Апаратний склад мережі наступний:

– 1 сервер;

– 21 робоча станція;

– 6 принтерів;

– 2 комутатори;

– 1 сканер;

– 1 модем;

– 1 джерело безперебійного живлення;

– 1 платформа безпеки Juniper SSG 20.

Рисунок 1.15 – Структурна схема мережі

1.3 Апаратна частина мережі

Для побудови локальної мережі ПП «Telnet» використовувалося устаткування з наступною конфігурацією:

Сервер – HP ProLiant ML330 G6 E5603 з процесором Intel Xeon Quad-Core E5603 .

HP ProLiant ML330 G6 – це сервер в корпусі tower на базі процесорів Intel Xeon з технологією QPI, призначений для створення унікальної системної архітектури. Ця архітектура дозволяє підприємствам в міру необхідності розширювати інфраструктуру, оптимізуючи витрати на IT. Завдяки системі Integrated Lights-Out 2 (iLO 2) сервер HP ProLiant ML330 G6 пропонує наймогутніші в галузі вбудовані можливості видаленого управління.

Унікальна архітектура для підвищення продуктивності і доступності.

Системна архітектура Intel підтримує 2 процесори Xeon (можливість додавання другого) з унікальною архітектурою, що масштабується.

Передовий RAID-контроллер Smart Array забезпечує додатковий захист даних.

Технологія DDR3 забезпечує максимальний об'єм системної пам'яті і скорочення енергоспоживання.

Робочі станції – Intel Core i3-2100 (3.1 ГГц) / RAM 4 ГБ / HDD 500 ГБ / nVidia GeForce GT440, 1 ГБ / DVD±RW / кард-ридер / LAN (мережна карта ASUS NX1101)

Для серверу та робочих станцій використовуються монітори Samsung SyncMaster S19A10N.

Комутатори – ASUS FX-D1162 (switch), 16 портов Ethernet 10/100 Мбіт/сек;

Сканер – HP ScanJet G4010 photo.

Принтери – HP LaserJet P1102w+ USB cable Модем - Zyxel P660HN Lite

Джерело безперебійного живлення - Powercom BNT-1000AP.

В якості передавального середовища використовується кабель UTP 5e.

Також в мережі використовується пристрій захисту – Juniper SSG 20 (рисунок 1.16).

Рисунок 1.16 – Juniper SSG 20

Міжмережеві екрани Juniper SSG 20 - це спеціалізовані модульні пристрої безпеки, які чудово поєднують в собі продуктивність, безпека і можливості по підключенню невеликих офісів до LAN/WAN.

Весь вхідний і витікаючий трафік офісу захищається від мережних черв'яків, шпигунського програмного забезпечення, Трої і іншого шкідливого ПЗ за допомогою технології Unified Threat Management (UTM), до складу якої входять міжмережевий екран з контролем полягання сесій, система запобігання вторгнень, антивірус, антиспам і веб-фільтр (підтримується на SSG-20-SH і SSG-20-SH-W-E, потрібна покупка ліцензій).

Багатий функціонал дозволяє використовувати SSG 20 як комплексний пристрій, що забезпечує безпеку мережі. Підтримка функцій маршрутизації дозволяє використовувати SSG 20 як традиційний маршрутизатор або як пристрій, об'єднуючий функціонал маршрутизатора і пристрою захисту мережі, а модульний конструктив забезпечує підтримку широкого набору WAN інтерфейсів.

Таким чином, SSG 20 дозволяє істотно понизити капітальні і операційні витрати на IT-інфраструктуру. Міжмережевий екран Juniper SSG20-SH-W-E має 5 портів 10/100Base-T, 2 слоти розширення для установки модулів Mini-PIM (модулі з підтримкою ADSL2+, E1, Gigabit Ethernet), вбудовану точку доступу WiFi 802.1a/b/g і 256 Мб оперативної пам'яті.

Максимальна продуктивність:

– Продуктивність MCE (великі пакети) – 160 Мбіт/с.

– Продуктивність MCE (змішані пакети) – 90 Мбіт/с.

– Продуктивність MCE (короткі 64Б пакети) - 30.000 пакетів/с.

– Одночасних сесій – 4000.

– Нових сесій в секунду – 2800.

– Політик безпеки – 200.

– Користувачів – необмежено.

Міжмережевий екран:

– захист від мережних атак;

– захист від DoS і DDoS;

– збірка/розбирання TCP-сегментів для перевірки;

– захист від неправильно сформованих пакетів.

Unified Threat Management (UTM):

– захист від атак рівня додатків Deep Inspection;

– розпізнавання аномалій протоколів;

– сигнатури з урахуванням полягання сесій (Stateful signatures);

– антивірус;

– база даних сигнатур - більше 100 тис.

– скановані протоколи – POP3, SMTP, HTTP, IMAP, FTP.

Протидія фішингу:

– шпигунському ПЗ;

– рекламному ПЗ;

– антиспам;

– вбудований URL-фільтр;

– зовнішня веб-фільтрація.

Опції UTM Security (IPS/Deep Inspection, Antivirus, Anti-Spam і Web filtering) оформляються як річні підписки. Річна підписка забезпечує оновлення сигнатур і відповідну техпідтримку.

Автентифікація:

– Вбудована база даних - до 100 користувачів.

– Зовнішня автентифікація RADIUS, RSA, 802.1x.

– Веб-автентифікація.

Трансляція мережних адрес:

– Трансляція мережних адрес (NAT).

– Трансляція портів (PAT).

– NAT на основі політик

– Трансляція адрес 1:1 (mapped IP).

– Віртуальний IP.

– IP і маршрутизація.

– Статичний IP, DHCP, PPPoE клієнт.

2 РОЗРАХУНКОВИЙ РОЗДІЛ

2.1 Розробка схеми розташування мережі

Схема розташування локальної комп`ютерної мережі проектується з урахуванням таких факторів, як: площа приміщення (будівлі), а також кількість та площа кімнат, де буде розташована обчислювальна техніка; апаратний склад мережі (кількість активного та пасивного обладнання), а також його взаємозв`язок (тобто структурна схема мережі).

При розробці схеми розташування необхідно враховувати всі вимоги по техніці безпеки щодо використання обчислювальної техніці.

Площа приміщення, де розташована локальна мережа складає 260м^2.

При використанні кабелю в якості комунікаційного середовища мережі, необхідною вимогою при проектуванні схеми розташування є розрахунок його довжини (кількості метрів кабелю). В даному випадку довжина кабелю складає 270м.

Рисунок 2.1 – Схема розташування обладнання

2.2 Розрахунок параметрів мережі

2.2.1 Розрахунок пропускної здатності мережі

Пропускна здібність – максимально можлива швидкість обробки трафіку, визначена стандартом технології, на якій побудована мережа. Пропускна здібність відображає максимально можливий об'єм даних, що передається мережею або її частиною в одиницю часу. Пропускна здібність вимірюється або у бітах в секунду, або в пакетах в секунду.

Пропускна здібність мережі залежить як від характеристик фізичного середовища передачі (мідний кабель, оптичне волокно) так і від прийнятого способу передачі даних (технологія Ethernet, FastEthernet, ATM).

Пропускна здібність часто використовується як характеристика не стільки мережі, скільки власне технології, на якій побудована мережа. Важливість цієї характеристики для мережної технології показує, зокрема, і те, що її значення іноді стає частиною назви, наприклад, 10 Мбіт/с Ethernet, 100 Мбіт/с Fast Ethernet,1000 Мбіт/с Gigabit Ethernet.

На відміну від часу реакції або швидкості передачі трафіку пропускна здібність не залежить від завантаженості мережі і має постійне значення, визначуване використовуваними в мережі технологіями. На різних ділянках мережі, де використовується декілька різних технологій, пропускна здібність може бути різною. Для аналізу і настройки мережі дуже корисно знати дані про пропускну здібність окремих її елементів.

Для підвищення пропускної здібності складеного шляху необхідно в першу чергу звернути увагу на найповільніші елементи. Іноді корисно оперувати загальною пропускною здібністю мережі, яка визначається як середня кількість інформації, переданої між всіма вузлами мережі за одиницю часу. Цей показник характеризує якість мережі в цілому, не диференціюючи його по окремих сегментах або пристроях.

Інтенсивність потоку заявок розраховується по формулі:

$$r_0 = \lambda \cdot t, \text{ Мбіт.} \quad (2.1)$$

де λ – інтенсивність потоку даних, біт/с, Кбіт/с, Мбіт/с;

t – час протягом якого відбувається передача даних, с.

Імовірність вільного стану всіх каналів розраховується по формулі:

$$P_0 = \frac{1}{1 + \sum_{k=1}^{n} \frac{\exp\{k \cdot \ln r_0\}}{k!}}, \quad (2.2)$$

де n – кількість каналів, од.

В результаті обчислень значення P_0 має бути більше 0.

Імовірність зайнятості кожного каналу:

$$P_k = \frac{\exp\{k \cdot \ln r_0\}}{k!} \cdot P_0 \quad (2.3)$$

В результаті обчислень значення $P_т$ має бути більше 0.

Відносна пропускна здібність обчислюється за формулою:

$$q = 1 - P_n \quad (2.4)$$

Абсолютна пропускна здібність обчислюється за формулою:

$$A = \lambda \cdot q \quad (2.5)$$

Для розрахунку відносною і абсолютною пропускних здібностей даної мережі необхідні початкові дані:

n – число каналів (24)

λ – інтенсивність потоку даних (100 Мбіт/с)

t – час протягом якого відбувається передача даних (10800 с)

Після розрахунків за вище вказанимиі формулами, отримуємо:

Відносна пропускна здібність:

$q=2,407 \cdot 10^{-5}$

Абсолютна пропускна здібність:

$A=2,407 \cdot 10^{-3}$

2.3 Розрахунок надійності

Надійністю називається властивість об’єкту (в даному випадку мережі) виконувати задані функції, зберігаючи свої характеристики у встановлених межах протягом певного часу при заданих режимах і умовах експлуатації, технічного обслуговування, умовах збереження і транспортування.

Надійність мережі складається з надійності окремих пристроїв, що складають мережу. Надійність є комплексною величиною і характеризується цілим рядом параметрів, основними з яких являються безвідмовність і ремонтоздатність. Поняття надійності тісно пов'язано з теорією імовірності. Закони розподілу випадкових величин (інтервалів між відмовленнями і збоями, часом відновлення і т.ін.) подають вичерпну інформацію про потоки відмов, збоїв і відмов. Усі ці величини є випадковими, але вони дозволяють прогнозувати себе. Цей прогноз ґрунтується на практичному використанні електронних пристроїв.

Надійність комп'ютерних мереж залежить і від надійності програмного забезпечення мережі.

При розрахунку надійності апаратної частини комп'ютерної мережі розраховуються такі основні показники надійності:

– загальна інтенсивність відмов мережі;

– середній час напрацювання на відмову;

– імовірність безвідмовної роботи.

Загальна інтенсивність відмов мережі складається з загальної суми інтенсивності відмов окремих пристроїв (елементів), що входять до складу мережі і обчислюється за формулою:

$$\lambda_{заг} = \sum_{i=1}^{n} N_i \lambda_i \text{, 1/год.} \qquad (2.6)$$

де $\lambda_{заг}$ – загальна інтенсивність відмов пристрою складових мережі, 1/год;

n – кількість типів пристроїв, од.;

N_i – кількість пристроїв даного типу, од.;

λ_i – інтенсивність відмов пристроїв даного типу, 1/год.

Результати розрахунку загальної інтенсивності відмови мережі зведено в таблицю 2.1. До неї також занесено всі пристрої (елементи) комп'ютерної мережі, їх кількість і інтенсивність їх відмов.

Таблиця 2.1 –Результати розрахунку загальної інтенсивності відмови даної мережі

Найменування пристроїв	Інтенсивність відмов пристроїв, $\times 10^{-6}$ (1/год.)	Кількість пристроїв, од.	Інтенсивність відмов всіх пристроїв, $\times 10^{-6}$ (1/год.)
Мережна плата	0,5	21	10,5
Системна плата	0,8	21	16,8
Вінчестер	0,6	21	12,6
Процесор	0,5	21	10,5
Пам`ять ОЗП	0,4	21	8,4
Монітор	0,8	22	17,6
Роз`єм RJ45	0,3	69	20,7
Розетки RJ45	0,3	21	6,3
Комутатор	0,9	2	1,8
Джерело безперебійного живлення	0,7	1	0,7
Сервер	0,5	1	0,5
Принтер	0,7	6	4,2
Сканер	0,4	1	0,4
Модем	0,5	1	0,5
Платформа захисту	0,9	1	0,9
$\lambda_{заг}$			120,5

Середній час напрацювання на відмову обчислюється за формулою:

$$T_в = 1/\lambda_{заг}, \text{ год.} \quad (2.7)$$

де $\lambda_{заг}$ – загальна інтенсивність відмов, 1/год.

Тв=1/120,5 · 10-6=8299 (год.)

Імовірність безвідмовної роботи визначається для окремих інтервалів часу по формулі:

$$P = e^{(-1/T_в)t}, \quad (2.8)$$

де t – інтервал часу, год.

Результати розрахунку імовірності безвідмовної роботи мережі для окремих проміжків часу надано в таблиці 2.2. В загальному випадку інтервали часу для визначення вірогідності безвідмовної роботи визначаються у межах розрахованого середнього часу напрацювання на відмову ($T_в$).Останнє значення інтервалу часу взято не менше за розрахований середній час напрацювання на відмову.

Таблиця 2.2 – Результати розрахунку імовірності безвідмовної роботи мереж

Інтервал часу, год.	Імовірність безвідмовної роботи
500	0,94
1000	0,89
2000	0,79
3000	0,70
4000	0,62
5000	0,56
6000	0,49
7000	0,43
8000	0,38
8500	0,36

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Мережне програмне забезпечення проектованої мережі

В якості серверної ОС в мережі підприємства ПП «Telnet» була вибрана Windows Server 2019 Standard Edition, на робочих станціях встановлено ОС Windows 10 (рис.3.1).

Рисунок 3.1 – ОС локальної мережі

В якості ПЗ моніторингу мережі використовується набір утиліт Essential NetTools (рис.3.2).

Рисунок 3.2 – Essential NetTools 4.3 Build 261

Essential NetTools – це набір мережних утиліт для діагностики мереж і моніторингу мережних з'єднань комп'ютера. Це незамінний інструмент з набором могутніх мережних інструментів для щоденного використовування.

Essential NetTools включає:

– NetStat: показує список вхідних і хостів мережних підключень, відкриті порти.

– ProcMon: відображає список активних процесів з повною інформацією про знаходження програми, виробника, ідентифікатор процесу, завантажені модулі.

– TraceRoute і Ping: утиліти, які забезпечені множиною функцій і наочним представленням результатів, дозволяють досліджувати Інтернет і виявляти проблеми з'єднань.

– PortScan: сканер TCP-портів з розширеними можливостями, що дозволяє сканувати мережу на предмет активних портів.

– NSLookup: дозволяє переводити адреси IP в імена хостів і навпаки, одержувати аліаси і виконувати розширені DNS-запити, такі як MX або CNAME.

– NBScan: могутній сканер NetBIOS.

– RawSocket: дає можливість встановлювати низькорівневі з'єднання TCP для виявлення проблем з різними мережними службами.

– Shares: відображає ресурси комп'ютера, відкритих для загального доступу, показує користувачів, підключених по мережі до ресурсів ПК.

– NetAudit (NetBIOS Auditing Tool): дозволяє проводити різні перевірки безпеки мережі та/або окремих комп'ютерів, на яких запущена служба доступу до ресурсів, що розділяються, по NetBIOS.

– SNMPAudit: просунутий сканер SNMP-пристроїв.

– SysFiles: зручний редактор для п'яти важливих системних файлів: services, protocol, networks, hosts і lmhosts.

– RawTCP: дозволяє встановлювати низькорівневі TCP підключення.

3.2 програмне забезпечення для користувача

Основний пакет програм, що використовуються на підприємстві – Microsoft Office 2019 (рисунок 3.3). Додатки Word, Excel і PowerPoint, що входять до складу системи Office 2019 забезпечують максимальний ефект при роботі з документацією та інформацією.

Рисунок 3.3 – Microsoft Office 2019

В якості програмного забезпечення обліку діяльності використовується «1С: Управління невеликою фірмою 8» (рис.3.4).

Рисунок 3.4 – «1С: Управління невеликою фірмою 8»

У програмі "1С: Управління невеликою фірмою 8" реєструються як вже досконалі, так і плановані господарські операції і події. Наприклад,

зобов'язання перед клієнтами, замовлення покупців, полягання замовлень, завдання співробітників, плановане завантаження ресурсів підприємства, плани-графіки виконання робіт, виробництва, плани продажів і багато інше.

У єдиній інформаційній базі:

– база клієнтів;

– банківські і касові операції, клієнт-банк, платіжний календар;

– розрахунки з контрагентами, персоналом;

– облік матеріалів, товарів, продукції;

– замовлення клієнтів, замовлення-наряди;

– планування і облік виконання робіт і надання послуг;

– планування і облік виробничих операцій;

– планування завантаження ресурсів підприємства;

– торгові операції, у тому числі роздрібні продажі;

– облік персоналу, розрахунок управлінської заробітної платні;

– облік витрат і розрахунок собівартості;

– майно, капітал;

– доходи, витрати, прибутки і збитки;

– фінансове планування (бюджетування) і т. д.

У програмі передбачено оформлення практично всіх первинних документів торгового, складського і виробничого обліку, а також документів руху грошових коштів.

Широкий спектр звітів забезпечує власникам, керівникам і співробітникам можливість швидко одержувати інформацію в зручній для роботи і ухвалення рішень формі, з необхідною оперативністю і деталізацією.

Програма не призначена для ведення бухгалтерського і податкового обліку для цих цілей можна використовувати "1С:Бухгалтерію 8", в яку автоматично передається необхідна інформація з УНФ.

Програму можна використовувати для декількох компаній або приватних підприємців як незалежних, так і працюючих в рамках одного

бізнесу. При зміні масштабів і структури бізнесу, підходів до управління або організації робіт програма може перенастроювати без великих витрат часу і грошей.

3.3 Обґрунтовування вибраного варіанту

В якості параметрів технології та топології розроблюваної локальної мережі було обрано Fast Ethernet та «зірку» відповідно, оскільки саме ці параметри для сучасних мереж є оптимальними на сьогоднішній день.

Різні критерії, такі як швидкість передачі даних і вартість, допомагають визначити найбільш відповідне середовище передачі даних. Виходячи з цього для з`єднання апаратного забезпечення в мережі використовувалася кабель вита пара (UTP) категорії 5е.

Конфігурація апаратного та програмного забезпечення підібрана згідно потреб в сучасних інформаційних технологіях та рівню захисту інформації, в тому числі пристрій захисту.

В даній дипломній роботі пропонується використання сучасного пристрою захисту мереж – мережного екрану Juniper SSG 20.

Цей пристрій містить об'єднання функцій міжмережного екрану, VPN-концентратора і маршрутизатора в одному.

Juniper SSG 20 має все необхідне для безпечної роботи користувачів в інтернеті, включаючи трансляцію адрес, IPSec VPN і вбудований захист контента: антивірус, антиспам, URL-фільтрацію, захист від атак. Більш детальний опис переваг було наведено вище в пояснювальній записці.

3.4 Технічне обслуговування мережі

Для пошуку несправностей будь-якої мережі звичайно користуються власним графіком пошуку несправностей, але звичайно всі вони схожі між

собою. Так, наприклад, для пошуку несправностей для даної мережі необхідно скористатися наступною картосхемою.

Апаратне тестування має на увазі собою детальну перевірку всього вхідного до складу мережі мережного й системного встаткування. Першим образом тестуються комп'ютери, ще не підключені в мережу. Спочатку вони тестуються шляхом простого включення, якщо ж один з комп'ютерів непрацеспроможний, то продовжують тестувати наступні, а після виявлення повної кількості непрацездатних комп'ютерів роблять докладний огляд кожного з них.

Після огляду працездатності комп'ютерів роблять тестування активного мережного забезпечення. Тестування виробляється шляхом перевірки кожного з їхніх портів. Перевірка може виконуватися шляхом ручного підключення одного тестуємого комп'ютера або ж автоматичних пристроїв.

Тестування кабелю виробляється на декількох етапах. Перший етап – це тестування всього мотка кабелю. Звичайно таке тестування роблять ще в магазині, при покупці кабелю. Якщо ж не виявлена не одна помилка в мережі або всіх помилках усунуті, то після підключення мережі приступають до програмного тестування, що являє собою настроювання користувальницьких систем обміну даними. Виробляється воно в такому порядку. Спочатку настроюються серверні станції. Звичайно в таких системах установлюють різноманітні

мережні сервіси й служби. Якщо ж виявлені деякі помилки в роботі мережних станцій то виробляється детальне тестування серверного програмного забезпечення.

Тестування користувальницьких станцій зробити набагато простіше. В основному вся робота пов'язана з настроюванням мережних інтерфейсів для кожної з машин. Комплексне тестування надається в руки користувача і являє собою роботу відділу в режимі тестування. У дійсності це вже нормальна робота підприємства, але фірма, що надає встановлення й настроювання мережі протягом місяця приймає й усуває скарги по працездатності мережі.

У мережі з топології зірка, і з централізованим керуванням, досить таки легко виявити несправність. Якщо клієнт не бачить мережу необхідно перевірити чи світитися індикатор, на комутаторі, над портом у який приєднаний клієнт. Якщо індикатор світитися, значить із устаткуванням усе в порядку, і несправність викликана програмним збоєм. Для усунення несправності, необхідно перевірити мережні настроювання клієнта. По-перше, необхідно перевірити, чи правильно уведена IP-Адреса клієнта й чи уведений він взагалі.

Якщо IP-Адреса клієнта уведена правильно, необхідно перевірити IP-Адресу DNS сервера. Якщо все уведено правильно виходить, необхідно ввести маску під мережі й IP-Адреса шлюзу.

Якщо ж індикатор на комутаторі не світитися, значить необхідно перевірити роботу комутатора, можливо вийшов з ладу порт, несправність усувається перепідключенням патч-корду у вільний порт. Якщо неполадка не зникла виходить, проблеми з мережною картою, і її необхідно замінити.

Після огляду працездатності комп'ютерів роблять тестування активного мережного забезпечення. Тестування виробляється шляхом перевірки кожного з їхніх портів. Перевірка може виконуватися шляхом ручного підключення одного тестуємого комп'ютера або ж автоматичних пристроїв.

Якщо ж не виявлена не одна помилка в мережі або всіх помилках усунуті, то після підключення мережі приступають до програмного тестування, що являє собою настроювання користувальницьких систем обміну даними. Спочатку настроюються серверні станції. Звичайно в таких системах установлюють різноманітні мережні сервіси й служби. Якщо ж виявлені деякі помилки в роботі мережних станцій, то виробляється детальне тестування серверного програмного забезпечення.

Якщо при підключенні мережі до Інтернет відбувається збій, тоді в першу чергу необхідно перевірити працездатність модему. Якщо ж причину відсутності Інтернет не вдається визначити самостійно, необхідно звернутися в технічний відділ провайдеру.

Схожість

Джерела з Бібліотеки 35

1	Студентська робота	ID файлу: 1004215970	Навчальний заклад: Lviv Polytechnic National University		2.99%
2	Студентська робота	ID файлу: 1013099555	Навчальний заклад: Yuriy Fedkovych Chernivtsi National	2 Джерело	1.61%
3	Студентська робота	ID файлу: 8320994	Навчальний заклад: National Technical University of Ukraine	2 Джерело	0.84%
4	Студентська робота	ID файлу: 1006774580	Навчальний заклад: National Aviation University		0.65%
5	Студентська робота	ID файлу: 1009016129	Навчальний заклад: National University of Life and Envir	6 Джерело	0.62%
6	Студентська робота	ID файлу: 1004182227	Навчальний заклад: National Aviation University		0.62%
7	Студентська робота	ID файлу: 9175049	Навчальний заклад: Kharkiv National Air Force University na	7 Джерело	0.54%
8	Студентська робота	ID файлу: 1005729069	Навчальний заклад: National Aviation University	4 Джерело	0.34%
9	Студентська робота	ID файлу: 1008155597	Навчальний заклад: Cherkasy State Technological University		0.32%
10	Студентська робота	ID файлу: 1015088276	Навчальний заклад: Lutsk National Technical University		0.3%
11	Студентська робота	ID файлу: 1001194368	Навчальний заклад: National Aviation University		0.17%
12	Студентська робота	ID файлу: 1000365040	Навчальний заклад: National University of Life and Environmenta...		0.14%
13	Студентська робота	ID файлу: 1007948541	Навчальний заклад: State University Kyiv National Economic Univ...		0.12%
14	Студентська робота	ID файлу: 3459064	Навчальний заклад: Lviv Polytechnic National University		0.12%
15	Студентська робота	ID файлу: 1013724065	Навчальний заклад: National Aviation University	2 Джерело	0.11%
16	Студентська робота	ID файлу: 1008109122	Навчальний заклад: Izmail State University of Humanities	2 Джерело	0.11%
17	Студентська робота	ID файлу: 1015217049	Навчальний заклад: National Technical University of Ukraine "Kyi...		0.11%