Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»
Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних систем та технологій
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи бакалавра

Студенту Сіверцов Микола Григорович
(ПІБ)

Академічної групи 123-19-1
(шифр)

Спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

освітній рівень бакалавр
(назва освітнього рівня)

на тему: *" Компютерна система мережі автосервісів з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі "*

Виконавець: студент 4 курсу, групи 123-19-1 _____ Сіверцов М.Г.
(підпис) (прізвище та ініціали)

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинг.	інституційною	
Кваліфікаційної роботи	Доц. Шедловський І.А.			
Розділів:				
Загальна частина	Доц. Шедловський І.А.			
Розробка корпоративної мережі	Ас. Панферова Я.В.			
Розробка апаратної частини	Доц. Бешта Д.О.			
Рецензент				
Нормоконтролер	Проф.Цвіркун Л.І.			

Дніпро
2023

«ЗАТВЕРДЖУЮ»
Завідувач кафедри
Інформаційних систем та технологій
проф. Гнатушенко В.В.

_____
" " 2023 р.

ЗАВДАННЯ
на кваліфікаційну роботу
бакалавра
(назва освітньо-кваліфікаційного рівня)

студенту групи *123-19-1* Сіверцову Миколі Григоровичу
(група) (прізвище, ім'я та по батькові)

Тема кваліфікаційної роботи *"Комп'ютерна система мережі автосервісів з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"*

затверджена наказом ректора НТУ "Дніпровська політехніка"
від 16.05.2023р. № 350-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	*На основі матеріалів виробничих практик, інших науково-технічних джерел обгрунтувати необхідність модернізації комп'ютерної системи з детальною розробкою комп'ютерної мережі.*	*15.03.2023 р.*
Технічні вимоги до комп'ютерної мережі	*На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної мережі.*	*01.04.2023 р.*
Розробка корпоративної мережі	*Розв'язати завдання з розробки комп'ютерної мережі автоматизованої системи управління дорожнім рухом з опрацюванням побудови та налаштування.*	*15.05.2023 р.*
Графічна частина	*Графічні результати розробки системи подати у вигляді рисунків схем таблиць на 10 арк. формату А4.*	*25.05.2023 р.*

Завдання видав, кер. роботи Доц. Шедловський І.А.
(підпис)

Завдання прийняв до виконання Сіверцов М. Г.
(підпис)

Дата видачі завдання *01.03.2023 р.*
Термін подання дипломної роботи до ДЕК *05.06.2023 р.*

РЕФЕРАТ

Пояснювальна записка: 90 с., 14 рис., 5 табл., 1 додаток, 20 джерел.

Об’єктом розрбки в кваліфікаційній роботі є комп’ютерна система мережі автосервісів.

Мета: створення комп’ютерної мережі, яка повинна забезпечувати повноцінне функціонування комп’ютерної системи.

В складі комп’ютерної системи є функціональні елементи, що відповідають за документальний супровід робіт, що виконуються на підприємстві. База даних персоналу, база складського обліку, організація черг на обслуговування. Додаткові функції з забезпечення інформаційної безпеки, функціонування систем контролю доступу та відеоспостереження.

Розроблена комп’ютерна мережа спроектована таким чином, щоб підприємство могло без додаткових витрат нарощувати кількість філій та станцій техобслуговування. Технічна та програмна модернізація комп’ютерної системи може здійснюватися поелементно що вигідно з позиції мінімальних капіталовкладень в цей процес.

Розроблена адресація комп’ютерної мережі, відповідно до завдання.

Розроблена модель комп’ютерної мережі на симуляторі Cisco Packet Tracer та виконані відповідні налаштування. Розроблена модель дозволила підтвердити правильність налаштувань та адресації і надала можливість підтвердити працездатність спроектованої мережі.

Результати роботи у вигляді таблиць, графіків, рисунків описані і наводяться у пояснювальній записці та додатках.

СИСТЕМА, КОМПЮТЕРНА МЕРЕЖА, АДРЕСАЦІЯ, МОДЕЛЬ, НАЛАШТУВАННЯ

ЗМІСТ

ПЕРЕЛІК УМОВНХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

ОЗП–оперативний запомнюючий пристрій;

КЗ–контрольована зона;

АРМ–автоматизоване робоче місце;

КІСП – комп’ютерна інформаційна система підприємства;

ЛОМ – локальна обчислювальна мережа;

ЦП – цифровий підпис;

ВСТУП

Збалансований та динамічний розвиток регіонального господарства, забезпечення зручних та комфортних умов життя населення міста неможливо собі уявити без створення та нормального функціонування сфери послуг.

До найбільш загальних принципів розвитку сфери послуг можна віднести такі:

1. Облік соціально-економічної специфіки регіону, перспектив його економічного та демографічного потенціалу, оскільки це значною мірою визначає темпи зростання невиробничої сфери у регіоні.

2. Дослідження основних тенденцій зміни попиту аналізований вид послуг і виявлення основних чинників, які на нього впливають.

3. Дослідження наявної матеріально-виробничої бази задоволення попиту послуги та виявлення можливостей її розширення з допомогою інвестицій.

4. Пошук джерел фінансових ресурсів для реалізації наміченої стратегії розвитку; узгодження мети та наявних готівкових коштів.

5. Аналіз конкретних інвестиційних проектів зі створення, розширення та реконструкції об'єктів невиробничої сфери.

Першочерговим моментом розвитку автосервісної мережі є аналіз її економічного стану. Вирішення цих завдань може сприяти підвищенню ділової активності за рахунок пожвавлення торгово-транспортних шляхів, збільшення обсягів вантажів, що перевозяться, зростання чисельності діючого автопарку. Комплексний розвиток автосервісу може стати імпульсом, який надалі стане початком шляху для регіону, що виводить його з депресивного стану.

Таким чином, розвиток автосервісу має бути органічно пов'язаний із загальною комплексною програмою розвитку міста загалом. Досвід розробки таких програм свідчить про те, що їх центральним напрямом зазвичай є розвиток малого підприємництва та забезпечення працевлаштування населення.

Вирішення цих проблем значною мірою може вирішуватися шляхом створення мережі щодо невеликих автосервісних підприємств; при цьому стратегія формування автосервісного господарства має бути складовою підпрограм розвитку малого бізнесу та зайнятості населення. Таким чином, розвиток автосервісу може успішно виконувати важливі соціально-економічні функції, забезпечуючи у регіоні нові робочі місця та підвищення зайнятості населення.

Перспективи розвитку автосервісного господарства ґрунтуються на науково-обґрунтованій оцінці перспектив розвитку транспортної мережі, пов'язаних із загальноекономічними завданнями розвитку міста загалом.

В основі успішної діяльності підприємства є інформаційна складова. Використання сучасних інформаційних технологій надасть більшу гнучкість основному виробничому напряму, високу швидкість реагування на запити клієнтів можливість заздалегіть забезпечити відповідну філію необхідними запасними частинами та матеріалами.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Загальна характеристика сучасного забезпечення технічного обслуговування автотранспорту

Типи автосервісів за розміром та приладдям.

Автосервіси в залежності від потужності (розміру) поділяються на:

• малі (від 1 до 10 прийомних постів),

• середні (від 11 до 30 постів),

• великі (від 31 до 50 постів),

• великі станції (від 50 постів).

Усі вони можуть працювати за двома моделями:

• Мережа автосервісів

• Одна станція технічного обслуговування автомобілів.

За належністю виділяють дилерські, незалежні та гаражні послуги для авто.

Дилерські автосервіси

Зазвичай надають повний комплекс послуг та ремонтних робіт. Принципова відмінність у тому, що вони є офіційними партнерами автовиробників та обслуговують моделі лише певних марок. Тому використовують оригінальні запчастини, виконують звичайний та гарантійний ремонт за корпоративними стандартами.

Важливо пам'ятати, що гарантія поширюється на автомобілі та запчастини, придбані у дилера, анулюється після обслуговування в неофіційному автосервісі. Тому після покупки машини, доки діє гарантія, більшість водіїв звертаються саме до дилерських автосервісів. А після закінчення гарантійного терміну переходять до незалежних СТО, оскільки офіційні послуги обходяться набагато дорожче.

Незалежні СТО

Як і дилерські, незалежні СТО можуть виконувати всі види робіт, але є партнерами автовиробників. Ціни дешевші, ніж у офіційних автосервісів,

тому що їм не обов'язково використовувати оригінальні запчастини та немає націнки за відомий бренд та рівень кваліфікації персоналу.

Незалежні СТО, найчастіше офіційно зареєстровані, сплачують податки, встановлюють професійне обладнання та наймають добрих фахівців.

Гаражні автосервіси.

Свою назву отримали за те, що їхні власники не орендують великі приміщення, а ремонтують машини у звичайному гаражі. Рідко зареєстровані як підприємство та не дають жодної гарантії на свою роботу.

Найчастіше виконують лише кілька видів робіт. Невеликий простір гаража не дозволяє встановити професійне обладнання для виконання всіх типів ремонтних робіт.

У гаражних автосервісах ціни нижчі, ніж у звичайних СТО та дилерських центрах. Це і приваблює водіїв авто, навіть незважаючи на ризик отримати низький рівень обслуговування та відсутність гарантій. Але бувають винятки, коли в гаражах працюють такі висококваліфіковані майстри, яких не знайти в офіційних та незалежних автосервісах.

Якщо для авторинку в цілому 2020 став по-справжньому проблемним, то пов'язаний з ним ринок автосервісу впевнено пережив певне зростання. Експерти вважають його тимчасовим та не зовсім стійким, але не заперечують можливостей для нового розвитку. Основну тривогу пов'язують із зниженням платоспроможності населення. Під впливом ринку післяпродажного обслуговування значно зростає значення мереж автосервісу. Сервіси стають основним джерелом інформації, консультування та підтримки автовласників. Фахівці говорять про тренд на розвиток агрегаторів автосервісів, мобільних додатків та загальне посилення позиції мереж.

Автосервісний ринок тісно пов'язаний із продажами автозапчастин, адже гаражний парк вітчизняних споживачів містить високий відсоток автомобілів, старших за 3 роки. Виробники амортизаторів, свічок та інших

деталей тепер охоче продають запчастини автосервісам через посередників. Ще кілька років тому основними постачальниками були роздрібні та дрібнооптові магазини, сьогодні основним споживачем автокомпонентів стають саме СТО, для них це і супутній товар до послуги, і логічний додаток до продажу. Саме вони стають основним каналом збуту, що сприяє зростанню ринку автосервісів.

Франчайзинг автосервісів

Франчайзингові мережі автосервісів стали одним із найзручніших форматів розвитку галузі. Так як боротьба йде за довіру клієнтів, повторні відвідування та постійну клієнтуру, то імідж мережі, її досвід та доступність стають козирями франшиз. Крім цього, франчайзинг автосервісів знижує ризики і для підприємців, робота всередині великої системи дозволяє знижувати і регулювати ціни, впроваджувати нововведення та технології, навчатися, перепрофілюватися в залежності від нових потреб часу. Саме франшизи можуть наголошувати на якості, а не кількості послуг. Плюс вигідніші договори з постачальниками, офіційними дилерами та маркетинговими майданчиками.

Стандарти авторизованих дилерів вплинули і на незалежний сектор ринку, який розвиває незалежні мережі ремонтників, що конкурують з дилерами, з єдиними стандартами, щоб краще відповідати запитам споживачів на високоякісне, ефективне та надійне обслуговування.

Незалежні мережі ремонтників усіх типів можуть надавати своїм членам такі самі переваги, які мають члени авторизованих мереж автовиробників, зокрема інвестиції у бренд, доступ до навчання, технічної інформації, широку номенклатуру запчастин, ефективність витрат у логістиці запчастин тощо.

У минулому багато з цих мереж, наприклад, Speedy, Kwikfit, Pitstop, ATU, спеціалізувалися на вузькому асортименті часто необхідних робіт, таких, як вихлоп, шини або заміна амортизаторів. Тепер мережі ремонтників

пропонують ширшу палітру послуг, щоб обслуговувати клієнтів, які вважають за краще спілкуватися з однією майстернею.

Мережі ремонтників, що надають широкий спектр послуг, збільшують свою частку на ринку, одночасно має місце консолідація мереж, що показує тенденцію обмеження кількості великих мереж за рахунок поглинання традиційних незалежних ремонтників. Хоча мережі не представляють консолідацію у сенсі спільної власності, вони потенційно дуже важливі у розвиток конкурентоспроможності незалежної ринку.

Незалежні мережі ремонтників стали силою, з якою рахуються. Порівняння у Німеччині показали, що найкращі незалежні мережі конкурують на рівних із авторизованими ремонтниками. Асоціація дистриб'юторів запчастин "GVA" у Німеччині повідомляє про потік клієнтів від офіційних дилерів до незалежних мереж ремонтників. Розширення незалежних мереж ремонтників останніми роками частина пояснюється припливом компетентного персоналу від колишніх авторизованих ремонтників, і навіть зусиллями незалежних мереж навчання, у результаті члени мереж виграють як сервіс[1].

Сервісні мережі, включаючи мережі майстерень швидкого ремонту та автоцентрів, займають суттєві частки ринку у Великій Британії та у Франції [2].

Сервісні мережі здійснюють близько половини всіх роздрібних продажів запчастин. У Німеччині вже 2004р. у незалежних групах ремонтників було понад 7000 підприємств, що становить 33% від загальної кількості незалежних ремонтників.

Німецька група "1a", що надає повний комплекс послуг, мережа включає 1250 підприємств автосервісу в Німеччині та Австрії [3].

Група Norauto, 1000 підприємств якої розташовані у Франції, Іспанії, Бельгії, Італії, Австрії, Польщі та Португалії, збільшує кількість підприємств на 10% щорічно. Зростанню групи за останні роки допомогло безліч

придбань: мережа “Авто 5” у 2002р., мережа “Maxauto” у 2003р., та мережа “Midas” у 2004р.

Група “Feu Vert” має понад 300 підприємств у Франції, 68 в Іспанії, 8 у Польщі та 1 у Португалії. Придбання “Feu Vert” у 2003р. з 55 підприємств мережі Service Auto Carrefour — інший приклад зростання через консолідацію незалежних груп ремонтників.

Група “KwikFit”, яка управляє 566 “KwikFit” центрами та 106 іншими фірмовими центрами у Великій Британії, 173 “KwikFit” центру в Нідерландах та 326 центрів “PitStop” у Німеччині. Придбання французької мережі Speedy зіграло важливу роль у роботі групи. Фірмі “Speedy” належать понад 500 автосервісів

Бельгії, Голландії, Швейцарії, Туреччини, Угорщини.

Мережа Bosch Auto Service має близько 11000 сервісних підприємств.

1.2 Засоби забезпечення функціонування мережевих автосервісів

1.2.1 Можливості мережевого формату автосервісу

Основна причина приєднання до мережі незалежного автосервісу в Європі, де мережевий формат є єдиною перспективною формою бізнесу автосервісу, отримання конкурентних переваг. Що шукають в мережах одиночки, що приєднуються до них:

Брендову підтримку;

Доступ до каналів постачання запчастин;

Вирішення кадрової проблеми через навчання своїх співробітників у мережевому навчальному центрі;

Доступ до мережевої бази технічної інформації;

Зниження рекламних витрат з допомогою участі у общесетевой рекламної програмі.

Все разом це дозволяє за більш-менш осудну ціну отримати необхідний розвиток бізнесу комплект інформаційно-технічних інструментів. Весь цей інструментарій, починаючи від грамотної маркетингової політики,

розробленої професіоналами, та закінчуючи прописаними регламентами обслуговування автомобіля, потрібен щоб залучити первинного клієнта та дати йому достатньо аргументів для повернення знову і знову.

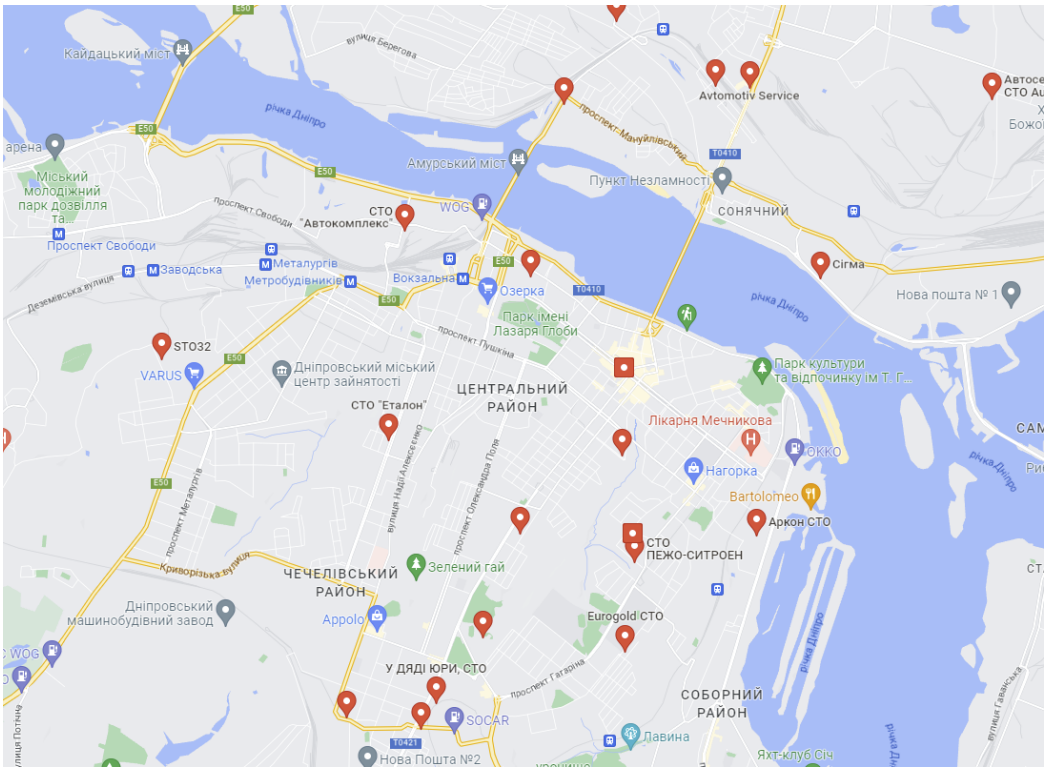

Рисунок 1.1 – Кількість станцій техобслуговування в невеликій частині міста.

Незалежний одинак, безумовно, може досягти таких самих результатів у благородній справі залучення клієнтів, як і учасник мережі, проте це й коштуватиме йому стільки ж, скільки витрачають мережі, діючи на бюджеті, сформованому в складчину. Проте деякі питання неможливо вирішити навіть за гроші. Власний навчальний центр – невиправдана розкіш для одинаки, а мережеві центри підготовки фахівців обслуговують лише учасників мережі.

Брендова підтримка

Цінність приналежності до якого-небудь бренду полягає в тому, що багато питань потенційного клієнта знімаються ще побачивши вивіску автосервісу і залишається тільки чесно виконати роботу і отримати належні

гроші. Брендовому автосервісу не витрачати час і доводити, що він «не верблюд». З питань ціноутворення також завжди можна апелювати до вбивчого аргументу «у нас у мережі такі правила». На думку не спадає торгуватися в супермаркеті, ціна сприймається як даність, особливо якщо вона обґрунтована антуражем і супутнім сервісом. Крім того, у приналежності до бренду є психологічна тонкість вже для власника бізнесу автосервісу та його співробітників - невловиме відчуття приналежності до чогось великого і світлого, що знімає занепокоєння і почуття захищеності. Вплив цієї ефірної складової важко переоцінити. Знаючи, що за складні питання відповідає хтось інший, людина концентрує свою увагу на конкретній справі та починає діяти ефективно.

Приєднання до бренду – це шлюб із розрахунку. Невипадково франчайзингові мережі показують кращі результати зростання протягом усього свого існування. Регулярна експрес-діагностика автомобіля клієнта становить суть програми і багато в чому відповідає процедурі «прямого приймання» дилерськими центрами, що практикується. Така діагностика дозволяє вчасно виявляти несправності та брати гроші з клієнта за їхнє усунення. Клієнту це теж вигідно, оскільки проблема, що народжується, вирішується ще до того, як розвиток хвороби завдасть відчутної шкоди автомобілю.

Канали постачання запчастин.

Доступ до каналів постачання запчастин за спеціальними цінами – одна із суттєвих можливостей, яка може і повинна бути надана мережами своїм учасникам. Економічна логіка підказує, що підсумовування обсягів споживання дає переваги при закупівлі і дозволяє отримувати запчастини за найбільш оптовими цінами. Створення та налаштування стійко працюючого механізму постачання учасників мережі витратними матеріалами та запчастинами – справа тонка і потребує часу. Однак у ньому є здорова економічна основа, і отже, такий механізм буде неминуче сформований будь-якою мережею.

Зародок такого механізму можна спостерігати на прикладі служби замовлення запчастин мережі - відштовхуючись від знижок учасників мережі, нарощуючи обсяг споживання за рахунок приєднання нових учасників, мережа виходить на рівень оптових цін, недоступних одинакам. Звичайно, для цього ще доведеться попрацювати, але справа видається однозначно вигідною. Підготовка та підвищення кваліфікації фахівців СТО.

Підготовка кадрів

Вирішення кадрової проблеми галузі авторемонту та технічного обслуговування автомобілів якимось чином має бути знайдено, інакше через 5 – 10 років ситуація з кадрами посилиться настільки, що обслуговувати величезний автопарк країни буде просто нікому, а ті нечисленні фахівці, яким пощастило пройти навчання у навчальних центрах автовиробників знову ставляться до рангу небожителів. Їм може й непогано, але якими будуть ціни на ремонт. Розраховувати на вирішення проблеми на державному рівні навряд чи варто. Все-таки автосервіс відноситься до малого бізнесу.

Великі компанії, безумовно, здатні організувати навчання персоналу на своїй базі, але це робитимуть тільки для себе. Мережі автосервісів виглядають найперспективнішою силою, здатною хоча б частково зняти напруженість у цьому питанні.

Доступ до актуальної технічної інформації

З доступом до новітньої технічної інформації на пострадянському просторі справа, щонайменше, дивна. По-перше, не всі автосервіси розуміють необхідність інформаційного ресурсу. Справді, навіщо комп'ютер та бази даних тому, хто бачить свою роботу у відкручуванні гайок. Їхня доля незавидна. Ті ж, хто розуміє цінність науково-технічної інформації, правдами та неправдами добувають старі дилерські бази, інвестуючи у них частину своїх доходів.

Варто зазначити, що ці інвестиції дуже вигідні – швидко окупаються та дозволяють бізнесу розвиватись. По-друге, про легальні канали отримання

свіжої інформації мультибрендовими сервісами ніхто не чув. Втім, це тільки до певного часу. Політика автовиробників з цього питання, що проводиться в Європі, дозволяє розраховувати на відкриття таких каналів відразу, як тільки кому їх відкриватиме. Одинак і навіть невеликі мережі незалежних автосервісів не дотягують до партнерського рівня з погляду світових автобрендів.

Франчайзингові мережі певному етапі свого розвитку мають практично гарантовану перспективу підключення до каналів поширення актуальної технічної інформації. І це полягає ще одна причина для автосервісів збиратися в мережі.

1.2.2 Системи автоматизованого обліку та локалізації виробничих послуг мережевого автосервісу

Автоматична обробка прайсів.

У каталогах понад 25 млн унікальних запчастин, 6 млн фотографій та 84 млн крос-пар та оригінальних номерів. Завжди зможете додати необхідні товари, фото, тексти та інші дані.

В системі працює інтеграція з понад 30 постачальниками з України та Польщі, весь їх асортимент правильно розпізнається системою та прив'язується до фотографій, оригінальних номерів для підбору по авто через ТекДок. Ви більше не налаштовуватимете прайси та склади постачальників. Коли йде пошук товару за артикулом чи назвою, система підкаже правильний варіант написання коду, видасть найкращу пропозицію за ціною та всі відомі аналоги.

У 2021 році додано окремий каталог для продуктових та господарських магазинів - у базі вже є сотні тисяч фото та штрих-кодів товарів продуктової групи, побутової хімії та будівельних матеріалів, а також безкоштовний програмний РРО.

Власний каталог товарів.

Каталог AutoSelling дозволяє налаштувати товарні категорії, прописати значення для фільтрів, зберегти описи та рейтинги товару в одній картці.

У товарів є рейтинг популярності, що генерується автоматично, а також гнучкі націнки, система бонусних рахунків, власні аналоги, генерація штрих-коду, коментар для товару (видимий буде в магазині) - все це можна задавати з вікна картки товару.

Автоматизація складського обліку.

Система складського обліку підтримує роботу з декількома складами та філіями компанії, є друк усіх необхідних документів та контроль переміщення товарів між віддаленими філіями.

Для всіх великих постачальників в Україні налагоджено імпорт файлів-накладних, тому прийом партій товару на склад займає лише кілька хвилин. Ми готові налаштувати Вам необхідний формат накладної, якщо постачальник може її надати. Якщо постачальник дає лише паперові накладні – не проблема, товар можна приймати за штрих-кодом, артикулом або ім'ям. Ця процедура зовсім не складна.

Система планування асортименту.

Наші клієнти мають великий досвід торгівлі та планування асортименту, але вони регулярно дивуються тому, наскільки об'єктивна статистика, показана в потрібний момент, допомагає приймати рішення. Замовляти проданий товар в асортимент чи ні, коли були останні продажі цього товару, який залишок, чи є його аналоги на складі - все це щоденна робота, відточена в системі реальним бізнесом, а не поглядами програмістів на торгівлю.

Можна вказувати мінімальні залишки на складі, є необхідні звіти для контролю товарів, які давно не продавалися чи, навпаки, мають більший потенціал. Також можна налаштувати експорт таких товарів або призначити дисконт.

Автоматизація бухгалтерських операцій та звітності.

Підхід: бухгалтерський облік для малого бізнесу має бути простим та зрозумілим. Так, всі борги враховуються на рахунках контрагентів, є оборотно-сальдові відомості, є всі необхідні бухгалтерські операції для управлінського обліку, І все це зроблено просто і зрозуміло, навіть для «не бухгалтера».

Автоматизація бухгалтерського обліку для малого бізнесу від AutoSelling – це легка та зрозуміла система, яка не потребує спеціальних знань чи виділеного співробітника. Навіть програмний касовий апарат у системі реалізований так, щоб робота з ним не була важкою та незвичною.

1.3 Галузь застосування комп'ютерної системи

Компютерна система мережі автосервісів повинна забезпечувати ефективну робота усіх підрозділів в досить насиченому інформаційному середовищі.

У якості універсального цифрового простору в якому працює підприємство використовують CRM системи.

CRM має зручний віджет онлайн-запису, електронний журнал, конструктор лендінгу та інші. Окремо доплачувати (як це часто буває у CRM) нізащо не потрібно. При першому налаштуванні система сама підкаже, що як і в якій послідовності заповнити. Але про всяк випадок, є документація та оператори, які готові прийти на допомогу. Жодних складних налаштувань, зайвих модулів, громіздких таблиць - все, що потрібно, вже під рукою. Одного разу налаштували і все працює.

Запис клієнтів на послуги. Можна настроїти онлайн-віджет запису та підключити його до сайту. Клієнти зможуть самостійно записатися на послугу у режимі 24/7 у зручній обстановці. Так ви не пропустите жодної заявки.

Важливо: якщо у віджеті немає вільного часу для запису, з'являється кнопка «Зателефонувати», і клієнт може записатись стандартним способом по телефону. А ви додати його в CRM вручну. Також є функція «Записатися

до» для обліку клієнтів, які надійшли на послугу без попереднього запису. Наприклад, йшли повз автосалон і вирішили зайти і записатися. Тобто у сервісі створені всі умови, щоб не втрачати клієнтів.

Запис автоматично потрапляє до електронного журналу CRM. Картка клієнта також заводиться автоматично на основі даних із віджету. Все, що потрібно - додати у віджет локацію автосервісу, майстрів, послуги та розклад, після чого встановити на сайт через HTML-код.

Якщо немає свого сайту, всього кілька кліків ви зможете безкоштовно його зробити. У нього вже вбудовано кнопку запису. Сайт заповнюється на основі налаштувань для віджету. У ньому відображається докладна інформація з автосервісу з переліком послуг, майстрами, фотогалереєю, відповідями на питання, що часто задаються. Посилання на лендинг можна розмістити у соцмережах та приймати заявки від клієнтів. Також до лендингу можна підключити інструменти просування та отримувати трафік із пошукових систем.

До аналітики додані UTM-мітки, тепер можна відстежувати джерело заявок та ефективність рекламних кампаній в особистому кабінеті.

Також можна встановлювати персональні знижки для клієнтів, що стане мотивацією продовжувати обслуговування у вашому автосервісі.

Повідомлення. Є кілька видів повідомлень для клієнтів та співробітників. Клієнтам вчасно нагадають запис, а співробітники зможуть планувати свій робочий день.

Для клієнтів: повідомлення по SMS та на електронну пошту.

Для співробітників: повідомлення по SMS, на електронну пошту, push-повідомлення в мобільному додатку та веб-версії. Також для майстрів передбачено окреме розсилання з денним розкладом.

Фінансова та складська звітність. У сервісі доступні найголовніші звіти, які покажуть прихід грошей, найбільш популярні послуги в автосервісі, а також клієнтів та майстрів, які приносять найбільше грошей бізнесу.

Контроль працівників. Для працівників передбачено окремі облікові записи, повідомлення про запис на послуги, мобільний додаток та автоматичний розрахунок зарплати. У сервісі видно, скільки годин відпрацював кожен майстер та які роботи виконав.

В цілому інформаційна система повинна бути забезпечена сучасними технічними пристроями, і головне комп'ютерною мережею з високими швидкостями обробки та передачі даних.

1.4 Характеристика і структура об'єкта впровадження

Підприємство складається з 27 окремих станцій технічного обслуговування. Головний офіс підприємства знаходиться в окремому приміщенні. Усі окремі станції в більшості випадків мають свою спеціалізацію. Винятком є віддалені СТО які розташовані у інших регіонах – вони універсальні (багатопрофільні).

Запас запасних частин є на кожному окремому підрозділі. Доступ до номенклатури запчастин – єдиний для усіх станцій обслуговування.

Структура управління підприємством в цілому – типова для для мережевої структури. Кожна окрема СТО має структуру управління яка показана на Рис.1.2.

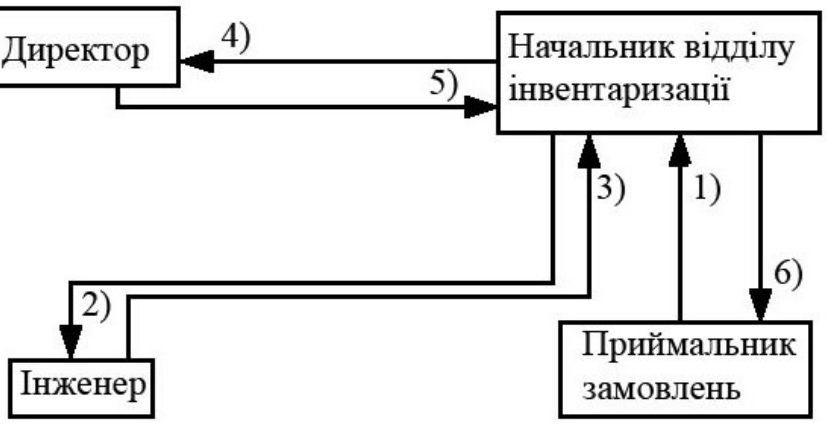

Рисунок 1.2 – Схема роботи відділів окремої СТО

1) Спочатку клієнт звертається до приймальника замовлень; 2) далі приймальник відправляє замовлення начальнику відділу з інвентаризації; 3) начальник відділу віддає замовлення інженерам, контролюючи процес виконання; 4) Після закінчення роботи начальник відділу з інвентаризації віддає на контроль виконане замовлення директору; 5) далі віддає замовлення приймальнику (на видачу).

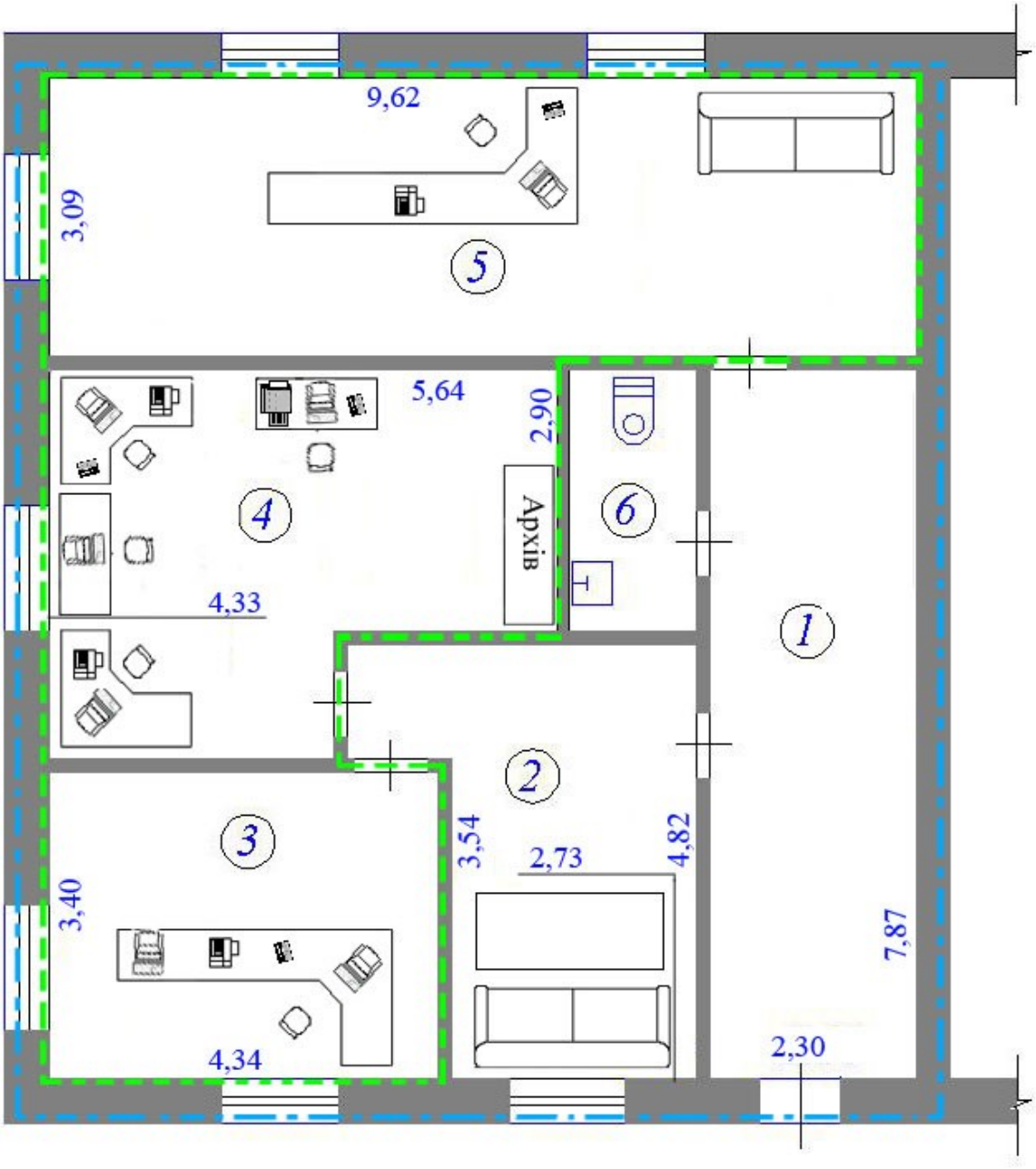

Рисунок 1.3 – План приміщення управління

1 Коридор;

2 Кімната очікування;

3 Кабінет директора;

4 Інженерно-технічний відділ, архів;

5 Зала прийому замовлень;

6 Санвузол.

Відповідно до потреб клієнта необхідні запасні частини переміщуються з одного підрозділу до іншого. Це проводиться або завчасно (за попереднім замовленням) або після звернення клієнта.

Висновки

Метою кваліфікаційної роботи є розробка комп'ютерної мережі, яка лежить в основі інформаційної системи мережевого автосервісу..

Технічне забезпечення комп'ютерної мережі повинно забезпечувати роботу сучасних систем автоматизації бізнес процесів, швидкий і зручний доступ до сервісів які надаються підприємством.

Для зв'язку локальних робочих станцій мережі з сервером доцільно використовувати Ethernet з гігабітними швидкостями передачі даних.

Виходячи з характеристик топології підприємства доцільно обєднати однією локальною мережею кілька станцій технічного обслуговування, які розташовані недалеко одна від другої.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМПЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до комп'ютерної системи

2.1.1 Вимоги до системи в цілому

2.1.1.1 Структура і функціонування системи

Виходячи із галузі використання – автоматизована інформаційна система повинна забезпечувати роботу підрозділів мережевої структури автомобільного сервісу.

Призначення системи- автоматизація бізне та виробничих процесів підприємства.

Ціль з якою проектується система .

Забезпечення функціонування CRM-системи для автосервісу.

Основні функції:

Запис клієнтів на послуги. На планове ТО, ремонт чи заміну запчастин, а також інші роботи. Система має враховувати джерела заявок. Виграють CRM, де є можливість самостійного онлайн-запису з боку клієнта.

Повідомлення. При виборі CRM уточніть, які типи оповіщень передбачені для клієнтів та співробітників: на електронну пошту, SMS, push-повідомлення в додатку або повідомлення для месенджера.

Фінансова та складська звітність. Контроль за замовчуванням фінансів є в будь-якій CRM незалежно від галузі. Вибирайте CRM, де будуть найважливіші фінансові звіти для вашого бізнесу. А також звіти по складу, щоб контролювати використання запчастин та розхідників під час ремонту.

Контроль працівників. У системі повинні бути інструменти контролю за роботою майстрів (кілька годин відпрацювали, з яких послуг) та інших співробітників (наприклад, відділу продажу). Буде плюсом наявність опції автоматичного розподілу послуг між вільними майстрами та розрахунок зарплат усередині CRM.

2.1.1.2 Чисельність і кваліфікація персоналу, що обслуговує систему і режим роботи

Компютерна система повинна забезпечувати повноцінне функціонування підприємства.

Проектна команда повинна включати кваліфікованих співробітників та досвідом не менше 3-х років, у т.ч.

- не менше 1 (одного) керівника проекту;

- не менше 1 (одного) бізнесаналітика (аналітика процесів);

- не менше 1 (одного) архітектора ІТ-рішень;

- щонайменше 1 (одного) інженерів-програмістів, мають навички розробки доп. функціоналу для системи;

- не менше 1 (одного) спеціаліста з тестування програмного забезпечення

Загальна кількість робочих місць – не менше 270.

Режим роботи комп'ютерної системи – цілодобово.

Система має забезпечувати ефективну роботу пыдроздылыв ы структурно складатися з 5 локальних комп'ютерних мереж.

LAN1 – 41 LAN2 – 57 LAN3 – 65 LAN4 – 92 LAN5 - 13

Інтенсивність трафіку $\mu = 139$ (кадрів/с).

Блокадрес - 10.23.IPn.0/22; для виділення підмереж IPn = 128.

Зовнішня адреса HTTP-сервера: 209.165.201.5/28

Середня довжина вихідного повідомлення в найбільшій мережі – 600 байт.

Затримка передачі пакету в найбільшій мережі $-\leq 5$ мс.

2.1.1.3 Вимоги до надійності

На основі реальної інформації перевіряється якість конкретних проектних рішень, інструктивних матеріалів, підготовленість кадрів до роботи у нових умовах. Перевіряється можливість виконання комплексу

організаційно-правових рішень проекту, зокрема щодо використання інформації, її захисту, достовірності, повноти, дотримання встановлених строків надходження даних та видачі результатів розрахунку. Досвідчена експлуатація проводиться на основі спеціальної програми. За результатами експлуатації, що оцінюються спеціальною комісією, здійснюється аналіз впровадження поданих технічного завдання та робочого проекту. За позитивних результатів складається двосторонній акт про приймання окремих завдань та їх комплексів у промислову експлуатацію. Після завершення приймання всіх завдань замовником відбувається приймання комісією системи загалом. Дата підписання акта приймання системи є датою введення АІС у промислову експлуатацію. З цього моменту відповідальність за функціонування АІС несе замовник.

2.1.1.4 Вимоги безпеки

Організаційні та технічні заходи щодо забезпечення безпеки включають:

– навчання, інструктаж та допуск до роботи з електроустановками осіб, які пройшли медичний огляд;

– виконання ряду технічних заходів при проведенні робіт з відключенням напруги в діючих електроустановках або поблизу них, а саме: замикання приводів, зняття запобіжників, від'єднання кінців живильних ліній;

– дотримання особливих вимог при роботах на струмовідних частинах, що знаходяться під напругою або поблизу них, а саме: виконання робіт за нарядом не менше ніж двома особами, організація нагляду за проведенням робіт, застосування електрозахисних засобів.

На підприємстві існують наступні небезпечні і шкідливі фактори:

– підвищений рівень шуму;

– знижена в холодний період року температура повітря робочої зони;

– підвищений рівень природного освітлення;

– підвищений рівень статичної електрики;

– підвищений рівень електромагнітного випромінювання;

– підвищений рівень ультрафіолетового випромінювання;

– розумове перенапруження;

– перенапруження зорового аналізатора;

– монотонність праці.

2.1.1.5 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів системи

Введення в експлуатацію проводиться силами замовника за участю розробника та здійснюється поетапно:

• підготовка об'єкта до впровадження АІС

• дослідна експлуатація окремих завдань чи їх комплексів

• здавання системи у промислову експлуатацію.

Технічне обслуговування системи проводиться персоналом підприємства. У разі виникнення потреби провести більш глибоке технічне обслуговування запрошується фірма розробник.

Ремонт компонентів системи власними силами не передбачено. Технічні компоненти замінюються. У разі потреби гарантійне обслуговування виконує виробник.

Збереження компонентів системи забезпечується відповідними до технічних умов умовами експлуатації.

2.1.1.6 Вимоги до захисту інформації від несанкціонованого доступу

Засоби захисту повинні бути прості для технічного обслуговування і «прозорі» для користувачів. Кожен користувач повинен мати мінімальний набір привілеїв, необхідних для роботи. Незалежність системи захисту від суб’єктів захисту.

Для виконання визначених вимог у складі ІС повинні бути розроблені та впроваджені:

– організаційні заходи щодо забезпечення захисту інформації в ІС;

– комплекс засобів захисту інформації АС від несанкціонованого доступу та від комп'ютерних вірусів;

– заходи контролю забезпечення безпеки інформації в ІС.

Захист від загроз несанкціонованих дій, (зокрема, несанкціонованого доступу (НСД)) в ІС здійснюється комплексом засобів захисту (КЗЗ), який має забезпечувати ідентифікацію та автентифікацію користувачів, персоналу і ресурсів ІС, розмежування доступу користувачів до інформації, цілісність інформації та конфігурації ІС, реєстрацію та облік дій користувачів, відмови у запит на спроби несанкціонованих дій.

Доступ до в ІС надається тільки ідентифікованим та автентифікованим користувачам.

У системі здійснюється обов'язкова реєстрація:

– результатів ідентифікації та автентифікації користувачів;

– результатів виконання користувачем операцій з обробки інформації;

– спроб несанкціонованих дій з інформацією;

– результатів перевірки цілісності засобів захисту інформації.

Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають адміністративних повноважень.

У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації. Контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

2.1.1.7 Вимоги до патентної чистоти

В комп'ютерній системі повинні використовуватися елементи та

пристрої, програмне забезпечення ліцензовані та сертифіковані для використання на території України.

2.1.1.8 Вимоги до стандартизації й уніфікації

Інформаційна система підприємства повинна відповідати стандартам групи IEEE 802підгрупи 802.3. Дані в системі повинні відповідати міжнародним стандартам ONVIF (OpenNetworkVideoInterfaceForum), PSIA (PhysicalSecurityInteroperabilityAlliance) CAP (CommonAlertingProtocol).

Проектні рішення повинні відповідати вимогам, що висуваються державними контролюючими органами для забезпечення функціонування розрахункового та касового обслуговування клієнтів.

Використане обладнання повинно відповідати сучасним стандартам і повинно мати характеристики по входу та виходу що дозволяють використовувати також інші зразки обладнання без переформатування системи.

2.1.2 Вимоги до видів забезпечення

2.1.2.1 Інформаційне забезпечення системи

Опис бізнес-процесів продажів за моделлю «Як треба» (список процесів продажів, що моделюються, блок-схема(-и) із застосуванням об'єктів системи ERP).

Побудова архітектури нормативно-довідкової інформації (номенклатури, характеристик, специфікацій, у тому числі параметричних, додаткових властивостей), опис призначення об'єктів, що використовуються в підсистемі продажів ERP.

Розробка механізму планової собівартості із включенням накладних витрат.

Ціноутворення продукції

Формування плану продажу в ERP

Опис бізнес-процесів забезпечення матеріалів за моделлю «Як треба» (список процесів, що моделюються, блок-схема із застосуванням об'єктів системи ERP).

Формування плану закупівель та резервування матеріалів

Опис бізнес-процесів планування виробництва та відображення випуску за моделлю «Як треба» (список процесів, що моделюються, блок-схема із застосуванням об'єктів системи ERP) у виконанні:

виробництво без замовлень,

виробництво за етапами (одноетапне/багатоетапне),

пооперaційне планування,

пооперaційне планування MES.

Опис виробничих потужностей – видів робочих центрів (ВРЦ) та робочих центрів (РЦ).

Формування плану виробництва з ВРЦ і РЦ за різними виробничими моделями (точно вчасно, рівномірно, мінімальна кількість переналагодок) в ERP.

Опис структури цехової автоматизації. Вивчення питання розробки автоматизованих робочих місць (АРМ) у цеху.

Облік трудовитрат випуску продукції ERP

Розрахунок фактичної собівартості в ERP

План-фактний аналіз собівартості в ERP

2.1.2.2 Технічне забезпечення системи

Технічні засоби для використання в системі;

Основними технічними засобом у приміщеннях є персональні комп’ютери. До складу технічних засобів, що призначені для обробки входять: ПЕОМ (іноземного виробництва).

Оргтехніка, що використовується в системі повинна відповідати сучасним вимогам і забезпечувати як віддалений так і мережевий доступ. Техніка повинна бути сертифікована для використання на Україні.

Сервер та мережеві пристрої також повинні відповідати вимогам законодавства.

Програмні продукти, що використовуються в системі повинні мати ліцензію та бути сертифіковані до використання в країні.

2.1.2.3 Вимоги до організаційного забезпечення

Адміністратор інформаційної системи несе відповідальність за:

За неналежне виконання або невиконання своїх посадових обов'язків, передбачених цією посадовою інструкцією.

За правопорушення, скоєні в процесі здійснення своєї діяльності, – в межах, визначених чинним адміністративним, кримінальним та цивільним законодавством.

За завдання матеріальної шкоди – в межах, визначених чинним цивільним законодавством.

Недостовірну інформацію про стан виконання отриманих завдань і доручень, порушення термінів їх виконання.

Порушення правил внутрішнього трудового розпорядку, правил протипожежної безпеки і техніки безпеки.

2.1.2.4 Вимоги до складу нормативно-технічної документації системи

Опис бізнес-процесів продажів за моделлю «Як треба» (список процесів продажів, що моделюються, блок-схема(-и) із застосуванням об'єктів системи ERP).

Побудова архітектури нормативно-довідкової інформації (номенклатури, характеристик, специфікацій, у тому числі параметричних, додаткових властивостей), опис призначення об'єктів, що використовуються в підсистемі продажів ERP.

Розробка механізму планової собівартості із включенням накладних витрат.

Ціноутворення продукції

Формування плану продажу в ERP

Опис бізнес-процесів забезпечення матеріалів за моделлю «Як треба» (список процесів, що моделюються, блок-схема із застосуванням об'єктів системи ERP).

Формування плану закупівель та резервування матеріалів

Опис бізнес-процесів планування виробництва та відображення випуску за моделлю «Як треба» (список процесів, що моделюються, блок-схема із застосуванням об'єктів системи ERP) у виконанні:

До складу технічних інструкцій, які, як правило, є типовими, входять інструкції щодо: збору, реєстрації, контролю та передачі інформації; перенесення її на машинні носії, ведення архіву носіїв документів; порядок передачі вихідної, результатної інформації. Посадові інструкції визначають правничий та обов'язки виробничого і управлінського персоналу під час експлуатації АІС, регламентують їх дії нових умовах виробництва.

1. Керівництво програміста, що містить описи використовуваних засобів програмування, безпосередньо програм та їх функціонування, алгоритмів обробки даних, способів та засобів діагностики та ін.

2. Керівництво оператора, у складі якого можна виділити опис його дій при запитах програми, правила організації програм на зовнішніх носіях, тестування.

3. Експлуатаційні програми, якщо використовується ППП або тексти програм.

4. Контрольний приклад, кіт. включає опис функцій і параметрів, складу необхідних технічних засобів, вхідної інформації та результатів апробування.

2.2 Вибір апаратної частини комп’ютерної системи

2.2.1 Організаційна структура інформаційної мережі

Організаційна структура визначається функціональними підрозділами які є на підприємстві і зв’язками між ними.

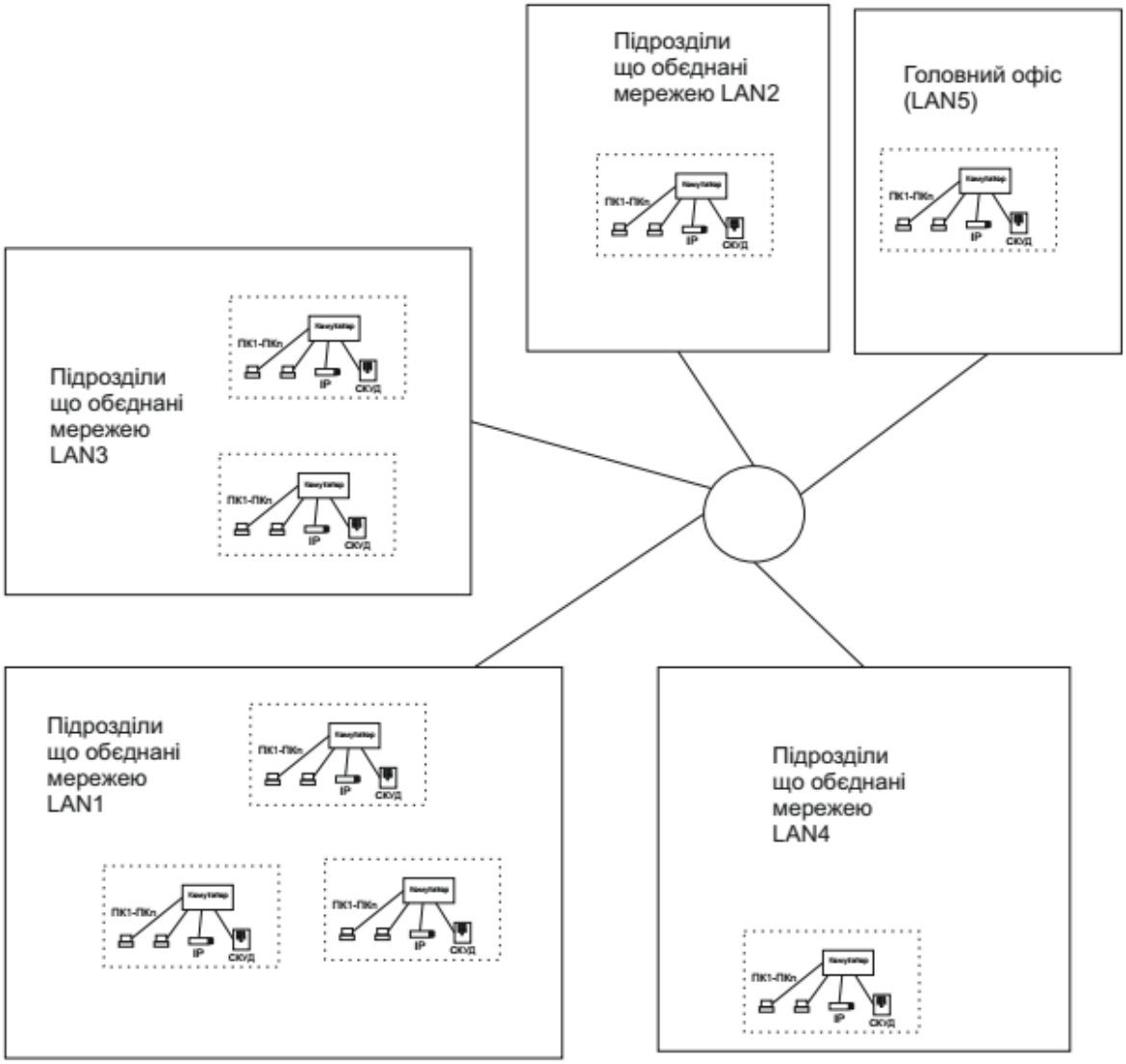

Рисунок 2.1 – Структура інформаційної системи підприємства

Робота інформаційної системи підприємства забезпечується комп'ютерною мережею. Мережеве обладнання є незамінним для

функціонування комп'ютерної мережі. Прикладами таких пристроїв є повторювачі, концентратори, мультиплексори та ін. Мережеві пристрої бувають двох видів: пасивні та активні.

До пасивних відносяться пристрої, які не мають «інтелектуальних» особливостей. Як приклад можна назвати телекомунікаційні шафи, монтажні стійки та шафи, кабельну систему.

Основна відмінність активних мережевих пристроїв – наявність певних інтелектуальних особливостей. Такі пристрої, як комутатор чи маршрутизатор, вважаються активними.

Концентратори (Hub) – це центральні мережеві пристрої. Вони застосовуються в мережах, побудованих за топологією "зірка", або кабельних системах. Hub Після того, як пакет приходить на один з портів, пристрій перенаправляє його на інші порти. Внаслідок цього відбувається формування мережі, загальна шина якої має логічну структуру. Дане обладнання буває пасивним та активним. Пасивні пристрої здатні лише пропустити сигнал без його посилення та відновлення, тоді як активні можуть здійснювати передачу сигналів, попередньо їх посилюючи.

Повторювачі (Repeater) – обладнання, що підсилює та повторно формує сигнал аналогового типу з подальшою передачею в інший сегмент. Вони здатні збільшити відстань мережного з'єднання. Їхня дія здійснюється на електричному рівні і допомагає з'єднати мережні сегменти. Подібне обладнання не здатне розпізнавати адреси в мережі. З цієї причини вони не використовуються для зниження трафіку.

Комутатори (Switch) – пристрої, що з'єднують мережні вузли та керуються відповідним ПЗ. Їх використовують для скорочення трафіку в мережі. Це досягається шляхом аналізу вхідного пакета з метою встановлення адреси одержувача. В результаті пакет приходить лише йому. Застосування комутаторів обумовлено їх високою продуктивністю, незважаючи на те, що це дороге обладнання. Також це досить складні пристрої, які одночасно обслуговують наскільки запитів. При зайнятості

певного порту пакет переноситься в буфер пам'яті. Мережа, яка побудована з використанням комутаторів, складається із сотень комп'ютерів. Протяжність таких мереж сягає кількох кілометрів.

Маршрутизатори (Router) – мережні пристрої стандартного типу, що дозволяють пересилати пакети між мережними сегментами, здійснюючи якісну фільтрацію повідомлень широкого мовлення.

2.2.2 Структура комп’ютерної мережі

Структура комп’ютерної мережі визначається як організаційною структурою підприємства та функціональними особливостями підрозділів, так і топологічними особливостями розташування підрозділів мережевої станції технічного обслуговування.

На структурній схемі (Рис. 3.2) зображено компютерну мережу яка складається з 5 локальних мереж.

LAN1 – локальна мережа, яка об’єднує техніку у кількості 41 одиницьі.

LAN2 – локальна мережа, яка об’єднує 57 підключених до мережі пристроїв.

LAN3 – локальна мережа, яка об’єднує 65 користувачів.

LAN4 – локальна мережа яка об’єднує 92 користувача.

LAN5 – об’єднує 13 терміналів центрального офісу.

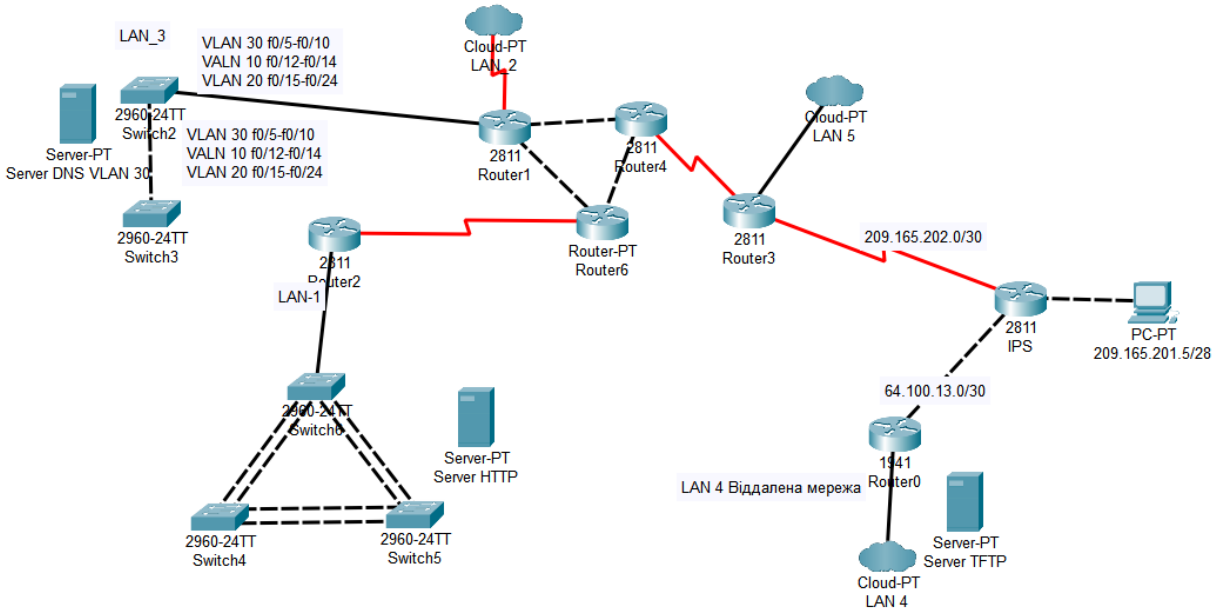

Рисунок 2.2 – Структура комп’ютерної мережі

Що до особливостей обладнання, яке підключене до комутаторів кожного з підрозділів можем виділити комп’ютерні системи технічної діагностики автомобілів, системи управління та контролю доступу, IP камери відеоспостереження, а також звичайні персональні комп’ютери.

2.2.3 Характеристики обраних апаратних засобів комп’ютерної мережі

Комутатор TFortis PSW-2G+Box

Промисловий комутатор PSW-2G+Box - це керований гігабітний вуличний комутатор, призначений для підключення до 4-х IP-камер або інших IP-пристроїв з живленням PoE/PoE+ (до 60 Вт на будь-якому з портів), і організації передачі даних по волоконно-оптичної лінії.

Рисунок 2.3 – Коммутатор TFortis PSW-2G+Box

Особливості.

всепогодне виконання зі ступенем захисту від пилу та вологи IP66;

не схильний до корозії корпус з максимальним індексом удароміцності IK10;

робота за температури від -60 до +50°З допомогою використання індустріальної елементної бази;

підтримка подвійного PoE+ (до 60 Вт) всіх портах комутатора;

два оптичні порти дозволяють підключати комутатори ланцюжком або кільцем;

вбудований оптичний крос для зручного підключення оптичного кабелю;

датчик розтину контролю несанкціонованого доступу;

вбудоване реле контролю напруги захисту устаткування при аварійних ситуаціях на мережах електроживлення;

вбудований грозозахист по портах Ethernet та живлення ~230 В для захисту від імпульсних перешкод;

зручний вузол підключення живлення з автоматичним вимикачем та клемними затискачами.

Склад комутатора.

плата комутатора; Блок живлення; Оптичний крос; Автоматичний вимикач; Прохідні клеми; Корпус IP66.

Порти для IP-камер

10/100Base-Tx із роз'ємом RJ-45: 4 шт;

кількість портів із PoE: 4 шт;

стандарт PoE: 802.3af/802.3at;

підтримка Passive PoE;

потужність на порт: до 60 Вт;

бюджет потужності PoE для IP-камер: 160 Вт;

відстань передачі даних та PoE: до 100 м.

Uplink порти

1000Base-X з роз'ємом SFP: 2 шт.

Продуктивність

комутаційна матриця: 4,8 Гбіт/с;

швидкість комутації: 9,83 Mpps;

таблиця MAC-адрес: 8К;

буфер пакетів: 1 Мбіт;

MTU: 1522 байти.

Управління

Web-інтерфейс (IPv4); Telnet; SNTP; SNMP v1, v3; SNMP Trap; DHCP Client; TFTP Client; Syslog; системний журнал.

Функції рівня L2

Flow Control (802.3x); IGMP Snooping v2; LLDP; Дзеркало портів; STP (802.1d)/RSTP(802.1w).

VLAN

802.1Q Tagged VLAN; Port Based VLAN; VLAN Trunking; максимальний VLAN ID: 4096; максимальна кількість активних VLAN: 100.

QoS

802.1p Quality of Service; CoS; ToS.

Додаткові функції

автоматичне перезавантаження відеокамер:

- за відсутності з'єднання з камерою (Link);

- за відсутності відповіді на службові запити (Ping);

- при зниженні швидкості потоку (Speed);

- За розкладом (Time).

кабельний тестер.

Входи/виходи

датчик розтину;

вхід "сухий контакт": 1 шт.

Вбудований грозозахист

відповідає 4 класу ГОСТ Р 51317.4.5;

максимальний імпульс лінії живлення: 4 кВ;

максимальний імпульс по лінії Ethernet: 2 кВ;

час імпульсу: 1/50 мкс.

живлення

напруга живлення: ~ 230В (від 187В до 253В);

максимальна споживана потужність: не більше 280Вт;

споживана потужність (без PoE навантаження): не більше 10 Вт.

Вбудований оптичний крос

планка під адаптери: 8 місць; SC (duplex LC);

кількість місць у сплайс-касеті: 32 КДЗС;

Розмір гільз для сплайс-касети: 40 або 60 мм.

Увага! Аксесуари для зварювання оптичного кабелю (гільзи, пігтейли, адаптери та патч-корди) до комплекту не входять.

Автоматичний вимикач

кількість: 1 шт;

номінальний струм: 6А;

кількість полюсів: 1;

характеристика розчіплювача: З.

Прохідні клеми

кількість: 6 шт;

тип затискачів: пружинний;

перетин дроту: 0,5 – 4 кв. мм.

номінальний струм: 32А.

Корпус

матеріал: армований полікарбонат;

ступінь захисту від зовнішніх впливів: IP66;

клас ударостійкості: IK10;

кабельні вводи:

- PG9 – 8 прим. діаметр кабелю 4-8 мм;

- PG13,5 – 5 шт. діаметр кабелю, що обтискається, 6-12 мм.

Фізичні параметри

маса: 7 кг;

розміри (без урахування кабельних вводів): 300 х 400 х 210 мм.

Умови експлуатації

робоча температура: від -60 до +50 ° С;

напрацювання на відмову: не менше ніж 75 000 годин (8,6 років).

Керований комутатор 28 портів D-Link DGS-1210-28/ME (24x1Гбіт/с, 4xSFP) 2 рівня

Рисунок 2.4 – Коммутатор D-Link DGS-1210-28/ ME

PoE-бюджет:

Гарантія: 12 міс

Кількість комбо-портів RJ45/SFP: 1

Кількість портів 1 Гбіт/с: 24

Кількість портів SFP: 4

Загальна кількість портів: 28 портів

Рівень пристрою: 2 рівні.

DSA-2006 Сервісний маршрутизатор з 6 портами, що настроюються.

Рисунок 2.5 – Маршрутизатор DSA-2006

Маршрутизатор DSA-2006 призначений для застосування у малому та середньому бізнесі для захисту мережевої інфраструктури від зовнішніх загроз та організації безпечного VPN-підключення. Маршрутизатор підтримує одночасне підключення великої кількості користувачів.

Розширені функції безпеки підтримують поділ мережі на зони, налаштування політик для взаємодії зон та правил фільтрації трафіку з широким вибором параметрів.

Маршрутизатор підтримує безліч типів тунелів для організації безпечного підключення VPN: IPsec (IKEv1/IKEv2), L2TP over IPsec, PPTP/L2TP, GRE, IPIP, EoGRE, а також некеровані L2TPv3-тунелі.

Крім того, підтримка протоколу SSH підвищує безпеку при віддаленому налаштуванні маршрутизатора та керуванні ним за рахунок шифрування всього трафіку, що передається, включаючи паролі.

Маршрутизатор підтримує роботу з сервісом контентної фільтрації SkyDNS, який пропонує більше налаштувань та можливостей для організації безпечної роботи в Інтернеті як для домашніх користувачів усіх вікових категорій, так і професійної діяльності співробітників офісів та підприємств.

Також у пристрої реалізована функція розкладу для застосування правил та налаштувань міжмережевого екрану, перезавантаження маршрутизатора у вказаний час або через задані інтервали часу та автоматичного збереження резервної копії конфігурації пристрою на підключений USB-накопичувач.

Нова функція блокування реклами допоможе ефективно блокувати рекламні оголошення, що виникають під час перегляду веб-сторінок.

Перетворення LAN/WAN, резервне WAN-з'єднання

Ви можете використовувати будь-який Ethernet-порт маршрутизатора як LAN- або WAN-порт. ПЗ підтримує можливість призначення декількох WAN-портів, наприклад, для налаштування основного та резервного WAN з'єднання від різних провайдерів. Крім того, можливе резервування доступу до Інтернету за допомогою 3G/4G-модему.

USB-порти

Маршрутизатор оснащений двома USB-портами для підключення USB-модему, USB-накопичувача або принтера. Ви зможете оперативно підключатися до мережі Інтернет за допомогою USB-модему та використовувати USB-накопичувач як мережний диск.

Для ефективного використання багатофункціональних USB-портів реалізовано можливість одночасної роботи з кількома USB-пристроями. Наприклад, Ви можете отримувати доступ до мультимедійного контенту з підключеного HDD-накопичувача і одночасно використовувати USB-принтер.

DCS-3511 1 Мп мережна HD-камера с PoE, варіофокальним об'єктивом та слотом microSD.

Мережева HD-камера DCS-3511 оснащена 1-мегапіксельним CMOS-сенсором з технологією прогресивного сканування та варіофокальним об'єктивом з фокусною відстанню 2,8-12 мм. Камера забезпечує захоплення HD-відео з роздільною здатністю до 1280x800 зі швидкістю до 30 кадрів за секунду. Можна зберегти снапшоти та відео на мережному диску або на карті microSD, підключеній до камери.

Відеоспостереження високої роздільної здатності

Вбудований мегапіксельний сенсор дозволяє отримувати снапшоти та відео високої якості з роздільною здатністю до 720p, забезпечуючи зображення високої чіткості із захопленням усіх деталей. DCS-3511 підтримує функцію ePTZ для деталізації об'єктів, що цікавлять зйомки в будь-якій точці огляду камери. Підтримка технології Power over Ethernet (PoE) забезпечує підключення DCS-3511 до мережі та подачу живлення по одному кабелю Ethernet, що спрощує встановлення і дозволяє розміщувати камеру в місцях, де відсутні розетки живлення.

Підтримка кількох відео потоків

Для збільшення ефективності використання смуги пропускання та збільшення якості зображення DCS-3511 використовує одночасну потокову передачу відео у форматах MJPEG, MPEG-4 і H.264. Крім того, камера може організовувати багатоадресні потоки даних та надавати доступ до відео на вимогу.

Комплексне рішення для ведення відеоспостереження

Камера DCS-3511 є комплексним рішенням для ведення спостереження, що забезпечує запис снапшотів та відео на microSD-карту, за винятком необхідності використовувати комп'ютер або мережевий пристрій зберігання даних. Для розширення можливостей відеоспостереження в комплект поставки включено безкоштовне програмне забезпечення D-

ViewCam, призначене для керування 32 камерами з широким набором функцій, таких як перегляд зображень одночасно з кількох камер та надсилання на e-mail повідомлень про підозрілі події або виникнення нештатних ситуацій.

Сервер на платформу Supermicro SYS-4029GP-TRT3, 4U

Рисунок 2.6 – Серверна платформа Supermicro SYS-4029GP-TRT3, 4U

Бренд SUPERMICRO

Модель SYS-4029GP-TRT3

Тип корпусу Rack

Монтаж у стійку 4U

PartNumber/Артикул Виробника

SYS-4029GP-TRT3

Процесори

Для процесорів Intel Xeon

Максимально процесорів 2

Пам'ять

Тип пам'яті DDR4

Кількість слотів пам'яті 24

Максимальний об'єм пам'яті 6144 ГБ

ОЗП, частота 2933 ГГц

Жорсткі диски HDD SATA HDD, розмірність 2.5"

Гаряча заміна HDD Так

Підтримка RAID 0 є

Підтримка RAID 1 є

Підтримка RAID 5 є

Підтримка RAID 10 є

Мережа

Мережевий інтерфейс 10G 2P

Блок живлення

БП, тип Titanium

Встановлено БП 2

Максимальна кількість БП 4

Потужність одного встановленого БП 2000 Вт

Гаряча заміна БП Да

Обрано сучасні мережеві пристрої що будуть актуальні досить довгий термін і забезпечують ефективну роботу інформаційної системи.

2.2.4 Захист інформації в комп’ютерній системі

2.2.4.1 Основні загрози інформаційної безпеки

Зовнішні хакери

Це одна з найбільш очевидних і легко усувних загроз. Якщо ми не говоримо про безпеку веб-сайту або іншого ресурсу, відкритого в Інтернеті, захист внутрішньої мережі не становить серйозних проблем. Достатньо мати грамотно налаштований роутер, досить строгу політику при підключенні

ззовні, відсутність небезпечних сервісів та надійний антивірусний захист, і ймовірність злому Вашої мережі різко знижується до мінімальних значень.

Віруси, трояни та використання їх для доступу до корпоративної мережі

Вирішення цієї проблеми залежить від того, чи випадкова вірусна атака. Якщо випадкова, тобто вірус написаний не безпосередньо під злом Вашої мережі, то, швидше за все, хороший антивірус його визначити та блокує. Якщо вірус хтось спеціально підготував для Вас, то шанси на успішний захист знижуються: якщо хтось серйозно працював над вірусом, то його виявлення може виявитися не по зубах антивірусній системі. Це пов'язано з тим, що антивірусні системи мають два механізми визначення вірусу – порівняння з відомими вірусними сигнатурами (унікальними шматками коду) та визначення за характерною поведінкою. Антивірус може не знати про новий вірус і визначати лише за поведінкою, зверненням до дисків або програм.

Однак, щоб вірус спрацював, необхідно його якось доставити у вашу мережу і запустити. І тут на шляху проблеми мають стати інструкції з роботи в мережі, обмеження прав доступу до ресурсів, політики безпеки мережі.

Власні співробітники

За статистикою, частку зламів та отримання доступу до даних через зовнішні мережі чи Інтернет припадає близько 20%. Інші 80% відносяться до внутрішніх зламів, витоків та розкрадань інформації. Ми рідко чуємо, що хтось зламав сервер, але часто - що співробітник, що йде, потер усі дані після того, як "злив" базу клієнтів.

Атаки зсередини часто не є атаками в прямому розумінні - людина просто бере доступну інформацію або використовує програмні засоби для отримання доступу до закритих областей. Відбити таку атаку набагато складніше, але можна значно знизити доступність інформації та ускладнити роботу зловмиснику. [13].

2.2.4.2 Особливості забезпечення інформаційної безпеки в комп’ютерній мережі

Приріст обсягу даних у середній компанії, що не зайнята графікою, обчислюється десятками гігабайт. За три-чотири роки це може зрости до сотень гігабайт, чи одиниць терабайт. Для розуміння - копіювання 1 Терабайта по локальній ста мегабітної мережі займе приблизно півтори доби. Тобто навіть резервне копіювання таких обсягів потребує серйозного підходу, а зливати щоночі кудись в інтернет, щоб мати актуальну копію, практично неможливо.

Звідси слід простий висновок потрібно відокремити від гігабайт мотлоху дійсно важливу, цінну інформацію. І ніхто не зможе це зробити за вас.

Ключ ЕП – унікальна послідовність символів, призначена для створення електронного підпису. Ключ ЕП зберігається користувачем системи у таємниці. В інфраструктурі відкритих ключів відповідає закритому ключу ЕЦП.

Ключ перевірки ЕП - унікальна послідовність символів, однозначно пов'язана з ключем електронного підпису та призначена для автентифікації електронного підпису.

Ключ перевірки ЕП відомий всім користувачам системи та дозволяє визначити автора підпису та достовірність електронного документа, але не дозволяє обчислити ключ електронного підпису. Ключ перевірки ЕП вважається таким, що належить користувачеві, якщо він був йому виданий встановленим порядком. В інфраструктурі відкритих ключів відповідає відкритому ключу ЕЦП.

Сертифікат ключа перевірки ЕП - електронний документ або документ на паперовому носії, видані посвідчувальним центром або довіреною особою центру, що засвідчує, і що підтверджують належність ключа перевірки електронного підпису власнику сертифіката ключа перевірки електронного підпису.

Посвідчувальний центр - юридична особа або індивідуальний підприємець, які виконують функції щодо створення та видачі сертифікатів ключів перевірки електронних підписів, а також інші функції, передбачені законодавством.

Власник сертифіката ключа перевірки ЕП - особа, якій у встановленому порядку видано сертифікат ключа перевірки електронного підпису.

Засоби ЕП – шифрувальні (криптографічні) засоби, що використовуються для реалізації хоча б однієї з таких функцій – створення електронного підпису, перевірка електронного підпису, створення ключа електронного підпису та ключа перевірки електронного підпису.

Сертифікат відповідності – документ, виданий за правилами системи сертифікації для підтвердження відповідності сертифікованої продукції встановленим вимогам.

Підтвердження автентичності електронного підпису в електронному документі – позитивний результат перевірки відповідним засобом ЕП приналежності електронного підпису в електронному документі власнику сертифіката ключа перевірки підпису та відсутності спотворень у підписаному електронним підписом електронному документі.

Компрометація ключа – втрата довіри до того, що використовувані ключі забезпечують безпеку інформації. До подій, пов'язаних із компрометацією ключів, відносяться, включаючи, але не обмежуючись, такі:

Втрата ключових носіїв.

Втрата ключових носіїв зі своїми подальшим виявленням.

Звільнення працівників, які мали доступ до ключової інформації.

Порушення правил зберігання та знищення (після закінчення терміну дії) закритого ключа.

Виникнення підозр на витік інформації чи її спотворення у системі конфіденційного зв'язку.

Порушення друку на сейфі із ключовими носіями.

Випадки, коли не можна достовірно встановити, що сталося з ключовими носіями (у тому числі випадки, коли ключовий носій вийшов з ладу та доказово не спростовано можливість того, що цей факт стався внаслідок несанкціонованих дій зловмисника).

2.2.4.3 Система заходів із захисту даних

Існують такі засоби захисту:

Від вірусних атак;

Від несанкціонованого внутрішнього чи зовнішнього доступу;

Електронний цифровий підпис;

Захист у комп'ютерних мережах;

Криптографічний захист.

Антивірусний захист

1. Поділ прав доступу. Людина повинна мати доступ лише туди, куди потрібно виконання своїх обов'язків.

2. Наявність та чітке дотримання політики паролів. Паролі повинні бути досить довгими, складними, і зазнавати регулярної зміни.

3. Правильне адміністрування мережі. Адміністратор повинен уважно ставитися до своєї роботи, регулярно проводити аудит безпеки, видаляти або відключати облікові записи, що не використовуються.

4. Використання засобів криптозахисту для захисту файлів та електронної пошти.

5. Використання централізованої системи автентифікації та автентифікації. У windows-мережах це зазвичай Active Directory.

6. Використання надійного антивірусного забезпечення.

7. Правильне налаштування всіх апаратних та програмних точок контакту із зовнішньою мережею – роутери, сервери, використання VPN при підключенні ззовні та між офісами.

8. Поділ прав доступу до документів та ресурсів. Впровадження практики контролю над отриманням доступу, коли отримання нового доступу можливе лише з санкції керівництва компанії.

9. Використання політик паролів – визначення вимог до паролів та їх регулярної зміни, реалізованої на програмному рівні.

10. Регламентація роботи користувачів у мережі. Опис дозволених та заборонених дій, політик паролів, правил доступу до тих чи інших ресурсів.

Всі ці заходи разом дозволяють серйозно підвищити рівень безпеки в компанії і сильно знизити ймовірність витоку дачах [19].

3 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРАХУНОК ЇЇ НАЛАШТУВАНЬ

3.1 Розрахунок адресації комп'ютерної мережі та схеми адресації пристроїв

Відповідно до структури комп'ютерної мережі необхідно розробити адресацію мережі, виконати налаштування пристроїв мережі та перевірити її працездатність. Для цього необхідно використати спеціалізований пакет програм PacketTracer.

Адресний простір заданий: 10.23.128.0/22

Кількість вузлів приведена в таблиці 3.1. Налаштування паролів базової конфігурації пристроїв приведене у таблиці 3.2.

Таблиця 3.1 – Кількість вузлів у підмережах

LAN1	LAN2	LAN3	LAN4	LAN5
41	57	65	92	13

LAN1, LAN2, LAN3, LAN4 – Мережі користувачів (філії, обладнання майстерень, системи контролю доступу, відеоспостереження).

LAN5 – Мережа центрального офісу.

Таблиця 3.2 – Налаштування паролів базової конфігурації пристроїв

Паролі		
консолі і vty	привілейованого режиму	користувача
cisco12319	*class12319*	*Sivertcov*

На рисунку 3.2 приведено структуру комп'ютерної мережі, яка повинна бути розроблена у роботі. На основі цієї структури була розроблена модель комп'ютерної мережі. Схема моделі приведена на рисунку 3.1.

Організації виділено блок IP-адрес 10.23.128.0/22, який треба розбити на 5 різних за розмірами під мереж.

Необхідно врахувати необхідність адресації зєднань між маршрутизаторами. Для цього достатньо використовувати префікс підмережі /30. В нашій мережі необхідно забезпечити адресами 8 зєднань.

Для адресації мережі використовуватимемо метод VLSM (Variable Length Subnet Masks, RFC 950). Цей метод дозволяє за рахунок кількох ітерацій більш оптимально розподілити адресний простір [9,10].

Виділено блок IP-адрес 10.23.128.0/22 – що дає можливість адресувати 1022 пристрої.

Для мережі LAN1 на 41 вузол:
Маска 255.255.255.192 (або префікс /26).
Діапазон 10.23.129.65 - 10.23.129.126.
Широкомовлення 10.23.129.127.
Для адресації 41 пристрою 10.23.129.67 - 10.23.129.108.

Мережа LAN2 на 57 вузлів
Маска 255.255.255.192 (або префікс /26).
Діапазон адрес 10.23.129.1 - 10.23.129.62.
Широкомовлення 10.23.129.63.
Для адресації 57 пристроїв 10.23.129.3 - 10.23.129.60.

Для мережі LAN3 на 65 вузлів:
Маска 255.255.255.128 (або префікс /25).
Діапазон 10.23.128.129 - 10.23.128.254.
Широкомовлення 10.23.128.255.
Для адресації 65 пристроїв 10.23.128.131 - 10.23.128.196.

Для мережі LAN4 на 92 вузли:

Маска 255.255.255.128 (або префікс /25).

Діапазон 10.23.128.1 - 10.23.128.126.

Широкомовлення 10.23.128.127.

Для адресації 92 пристроїв 10.23.128.3 - 10.23.128.95.

Для мережі LAN5 на 13 вузлів:

Маска 255.255.255.240 (або префікс /28).

Діапазон 10.23.129.129 - 10.23.129.142.

Широкомовлення 10.23.129.143.

Для адресації 41 пристрою 10.23.129.131 - 10.23.129.44.

Для зєднань між маршрутизаторами розраховуєм 8 мереж WAN (Табл.3.3).

Таблица 3.3 – Схема адресування мережі

Ім’я мережі	Кількість вузлів	Адреса мережі	Маска мережі	Початкове значення діапазону	Кінцеве значення діапазону
LAN1	41	10.23.129.64	255.255.255.192	10.23.129.65	10.23.129.126
LAN2	57	10.23.129.0	255.255.255.192	10.23.129.1	10.23.129.62
LAN3	65	10.23.128.128	255.255.255.128	10.23.128.129	10.23.128.254
LAN4	92	10.23.128.0	255.255.255.128	10.23.128.1	10.23.128.126
LAN5	13	10.23.129.128	255.255.255.240	10.23.129.129	10.23.129.142
WAN1	2	10.0.2.0	255.255.255.252	10.0.2.1	10.0.2.2
WAN2	2	10.0.2.4	255.255.255.252	10.0.2.5	10.0.2.6
WAN3	2	10.0.2.8	255.255.255.252	10.0.2.9	10.0.2.10
WAN4	2	10.0.2.12	255.255.255.252	10.0.2.13	10.0.2.14
WAN5	2	10.0.2.16	255.255.255.252	10.0.2.17	10.0.2.18
WAN6	2	10.0.2.20	255.255.255.252	10.0.2.21	10.0.2.22
WAN7	2	10.0.2.24	255.255.255.252	10.0.2.25	10.0.2.26
WAN8	2	10.0.2.28	255.255.255.252	10.0.2.29	10.0.2.30

В таблиці 3.4 перелічені адреси всіх пристроїв у мережі.

Таблиця 3.4 – Адреси всіх пристроїв у мережі

Им’я пристрою	Інтерфей	IP адреса	Маска	Шлюз	VLAN	Для ПК інтерфейс підключеного пристрою
(LAN 1)						
Sivertcov _ Rout2	G0\0	10.23.129.65	/26			Sw1_1_Fa0
	G0\1	10.0.2.1	/30			R6_G0/0
Sivertcov _ Sw1_1	Vlan1	10.23.129.66	/26	10.23.129.65		-
PC1_1 - PC1_41	NIC	10.23.129.68-10.23.129.109	/26	10.23.129.65		-
Server HTTP	Fa0	10.23.129.67	/26	10.23.129.65		-
(LAN 2)						
Sivertcov _ Rout1	G0\0	10.23.129.1	/26			Sw2_1_Fa0
	G0\1	10.0.2.5	/30			R4_G0/0
	G0\2	10.0.2.9	/30			R6_G0/1
	G0/3	10.23.128.129	/25			Sw3_1_Fa0
Sivertcov _ Sw2_1	Vlan1	10.23.129.2	/26	10.23.129.1		-
PC2_1-PC2_57	NIC	10.23.129.3 - 10.23.129.60	/26	10.23.129.1		-
(LAN 3)						
Sivertcov _ Rout1	G0/3	10.23.128.129	/25			Sw3_1-Fa0
	G0/0/10	10.23.128.131	/25	10.23.128.129	10	-
	G0/0/20	10.23.128.141	/25	10.23.128.129	20	-
	G0/0/30	10.23.128.151	/25	10.23.128.129	30	-
	G0/0/99	10.23.128.161	/25	10.23.128.129	99	-
	G0/1	10.0.2.5	/30			R4_G0/0
	G0/2	10.0.2.9	/30			R6_G0/1
	G0/0	10.23.129.1	/26			Sw2_1-Fa0
Sivertcov _ Sw3_1	Vlan99	10.23.128.130	/25	10.23.128.129	99	-
Server DNS	Fa0	10.23.128.200	/25	10.23.128.129		-
PC10_1 – PC10_9	NIC	10.23.128.132-10.23.128.140	/25	10.23.128.131	10	-
PC20_1 – PC20_9	NIC	10.23.128.142-10.23.128.150	/25	10.23.128.141	20	-

PC30_1 – PC30_47	NIC	10.23.128.152-10.23.128.199	/25	10.23.128.151	30	-
(LAN 4)						
Sivertcov _ Rout0	G0\0	10.23.128.1	/25			Sw4_Fa0
	G0\1	10.0.2.25	/30			IPS_G0/2
Sivertcov _ Sw4_1	Vlan1	10.23.128.2	/25	10.23.128.1		-
PC4_1-PC4_92	NIC	10.23.128.3-10.23.128.95	/25	10.23.128.1		-
Server TFTP	Fa0	10.23.128.100	/25	10.23.128.1		-
(LAN 5)						
Sivertcov _ Rout3	G0\0	10.23.129.129	/28			Sw5_Fa0
	G0\1	10.0.2.21	/30			ISP_G0/0
	G0\2	10.0.2.17	/30			R4_G0/1
Sivertcov _ Sw5_1	Vlan1	10.23.129.130	/28	10.23.129.129		R3_G0/0
PC5_1-PC5_13	NIC	10.23.129.131-10.23.129.144	/28	10.23.129.129		-
Sivertcov _ Rout4	G0\0	10.0.2.6	/30			R1_G0/1
	G0\1	10.0.2.18	/30			R3_G0/2
	G0\2	10.0.2.13	/30			R6_G0/2
Sivertcov _ Rout6	G0\0	10.0.2.2	/30			R2_G0/1
	G0\1	10.0.2.10	/30			R1_G0/2
	G0\2	10.0.2.14	/30			R4_G0/2
ISP	G0\0	10.0.2.22	/30			R3_G0/1
	G0\1	209.165.201.5	/30			PC00_Fa0
	G0\2	10.0.2.26	/30			R0_G0/1
PC00	Fa0	209.165.201.6	/30	209.165.201.5		ISP_G0/1

VLAN має ті самі атрибути, як і фізична локальна мережа, але дозволяє кінцевим станціям бути згрупованими разом, навіть якщо вони не перебувають на одному мережевому комутаторі. Реконфігурація мережі може бути зроблена за допомогою програмного забезпечення замість фізичного переміщення пристроїв. Щоб фізично копіювати функції VLAN,

необхідно встановити окремий, паралельний збір мережевих кабелів і перемикачів, які зберігаються окремо від первинної мережі. Однак на відміну від фізичної відділеної мережі, VLAN ділить пропускну здатність; дві окремих одно-гігабітних віртуальних мережі які використовують одно-гігабітний зв'язок мають знижену пропускну здатність. Це віртуалізує поведінку VLAN (настроювання портів комутатора, позначки кадрів при вході в мережу VLAN, пошук MAC таблиці, щоб перейти до магістральних зв'язків і видалення тегів при виході з VLAN).

```
Switch8(config)#int g0/1
Switch8(config-if)# switchport mode trunk
Switch8(config-if)# switchport trunk native vlan 100
Switch8(config-if)# switchport trunk allowed vlan 10,20,30,99
Switch8(config-if)#int range f0/1-2
Switch8(config-if-range)# switchport mode trunk
Switch8(config-if-range)# switchport trunk native vlan 100
Switch8(config-if-range)# switchport trunk allowed vlan 10,20,30,99
Switch8(config-if-range)# int range f0/0-5
Switch8(config-if-range)# switchport mode access
Switch8(config-if-range)# switchport access vlan 30
Switch8(config-if-range)# int range f0/6-10
Switch8(config-if-range)# switchport mode access
Switch8(config-if-range)# switchport access vlan 20
Switch8(config-if-range)# int range f0/10-15
Switch8(config-if-range)# switchport mode access
Switch8(config-if-range)# switchport access vlan 10
Central (config)# int g0/1.16
Central (config-if)# encapsulation dot1Q 21
Central (config-if)# ip address 121.100.9.20 255.255.240.0
Central (config-if)# int g0/1.26
```

```
Central (config-if)# encapsulation dot1Q 26
Central (config-if)# ip address 121.100.9.75 255.255.240.0
Central (config-if)# int g0/1.36
Central (config-if)# encapsulation dot1Q 36
Central (config-if)# ip address 121.100.9.150 255.255.240.0
```

3.2 Розробка моделі та перевірка роботи комп’ютерної системи

Програмне рішення Cisco Packet Tracer дозволяє імітувати роботу різних мережевих пристроїв. Імітаційне моделювання - це метод, що дозволяє створювати і реалізовувати математичні моделі, що відображають процеси, що відбуваються в системі, у часі. При імітаційному моделюванні логіко-математична модель досліджуваної системи є алгоритм її функціонування, програмно-реалізований на комп'ютері. Відмінною рисою методу є відтворення процесу функціонування системи у часі та просторі, тобто. у режимі роботи реального об'єкта. Імітаційна модель відображає функціонування реальної системи та складових її елементів із збереженням логічної структури системи та динаміки взаємодії її елементів. Так як імітаційна модель відображає процес функціонування складної системи з певною похибкою, метод імітаційного моделювання є експериментальним методом дослідження реальної системи за її імітаційною моделлю. Найбільш об'єктивне уявлення про роботу реальної системи можна отримати на основі серії експериментів (прогонів) моделі, оскільки результат кожного прогону має випадковий характер. На основі серії прогонів формується вибіркова сукупність характеристик Формально модельована система може бути представлена як система масового обслуговування (СМО) з відповідними їй об'єктами (черга, обслуговуючий пристрій, вхідний та вихідний потік транзактів на обслуговування). Подання динамічного об'єкта як мережі СМО

і розрахунок основних характеристик роботи мережі дозволяє виявити у ній «вузькі місця».

Вузьким місцем є перевантаженість вузлів мережі (і отже, наявність великої черги транзактів на обслуговування) або його недовантаженість (тоді підприємство недоотримуватиме дохід, матиме високу собівартість продукції внаслідок високих питомих витрат на амортизацію обладнання. Це дозволяє виробити адекватні управлінські рішення щодо раціоналізації її роботи). до яких, наприклад, може бути віднесена заміна обладнання на більш продуктивне або введення додаткових каналів обслуговування) Усі можливі стратегії можуть бути оцінені за допомогою розробленої імітаційної моделі.

Модель розроблюваної мережі показана на рисунку 3.1.

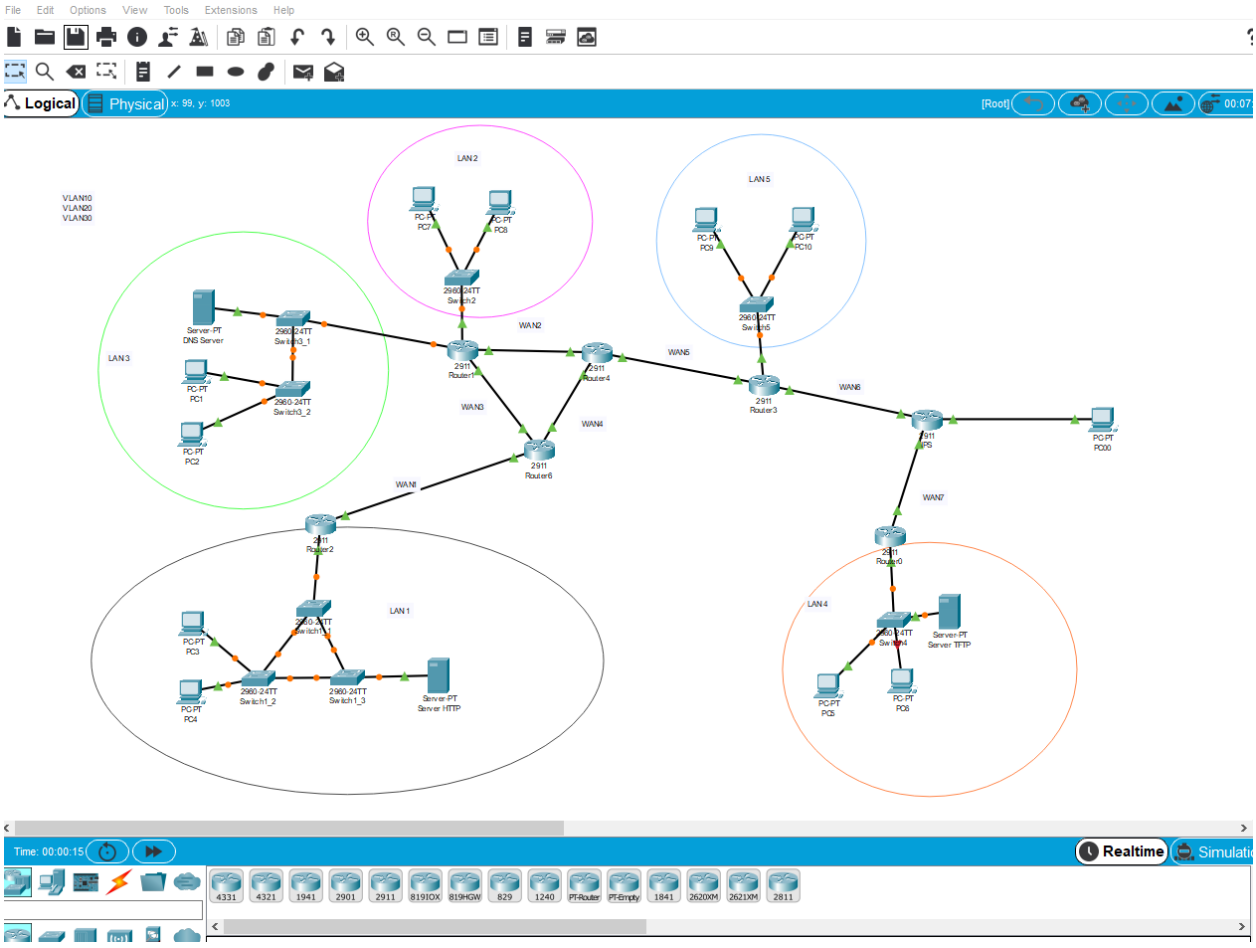

Рисунок 3.1 – Схема моделі мережі

Необхідно вказати на відмінності моделі від проекту, який був розроблений в розділі 2. Наведені відмінності не вплинули на можливості дослідження створеного проекту мережі.

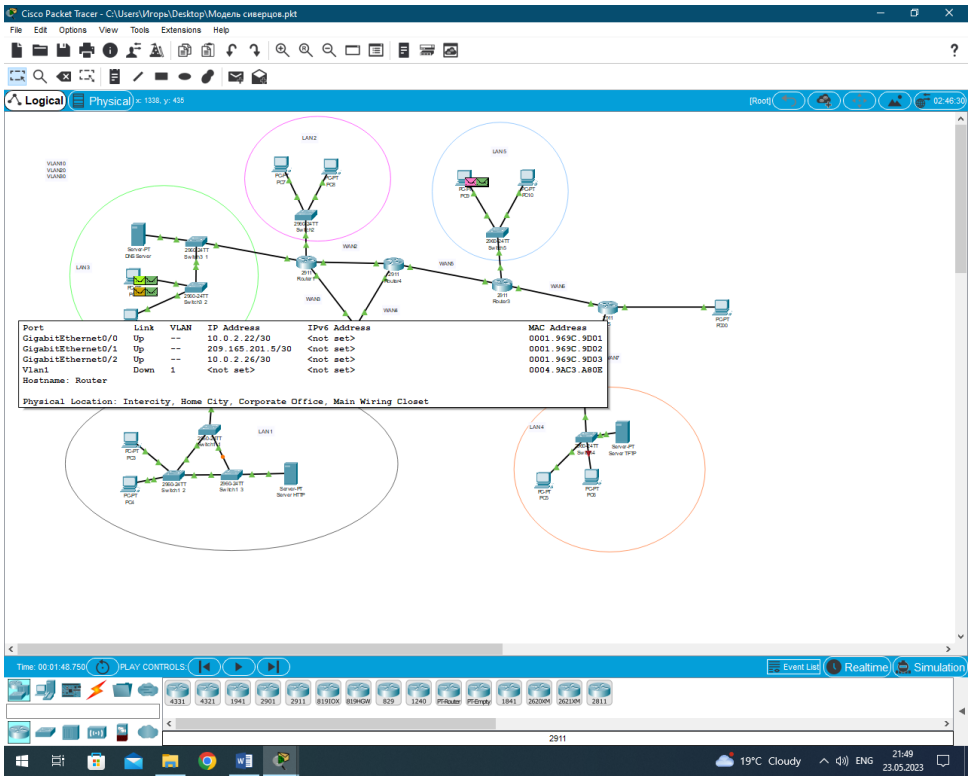

Рисунок 3.2 – Статус портів складових моделі

Налаштування маршрутизації проводиться статичним методом. Компанія в найближчому часі не буде поширюватися. Для налаштування маршрутизації потрібно прописати шляхи пакетів. Налаштувати маршрут за замовченням. Після налаштування всі вузли в віддалених мережах досяжні між собою і мають шлях в Internet.

Налаштування виконувалося як за допомогою графічного інтерфейсу, так і за допомогою IOS command line interface.

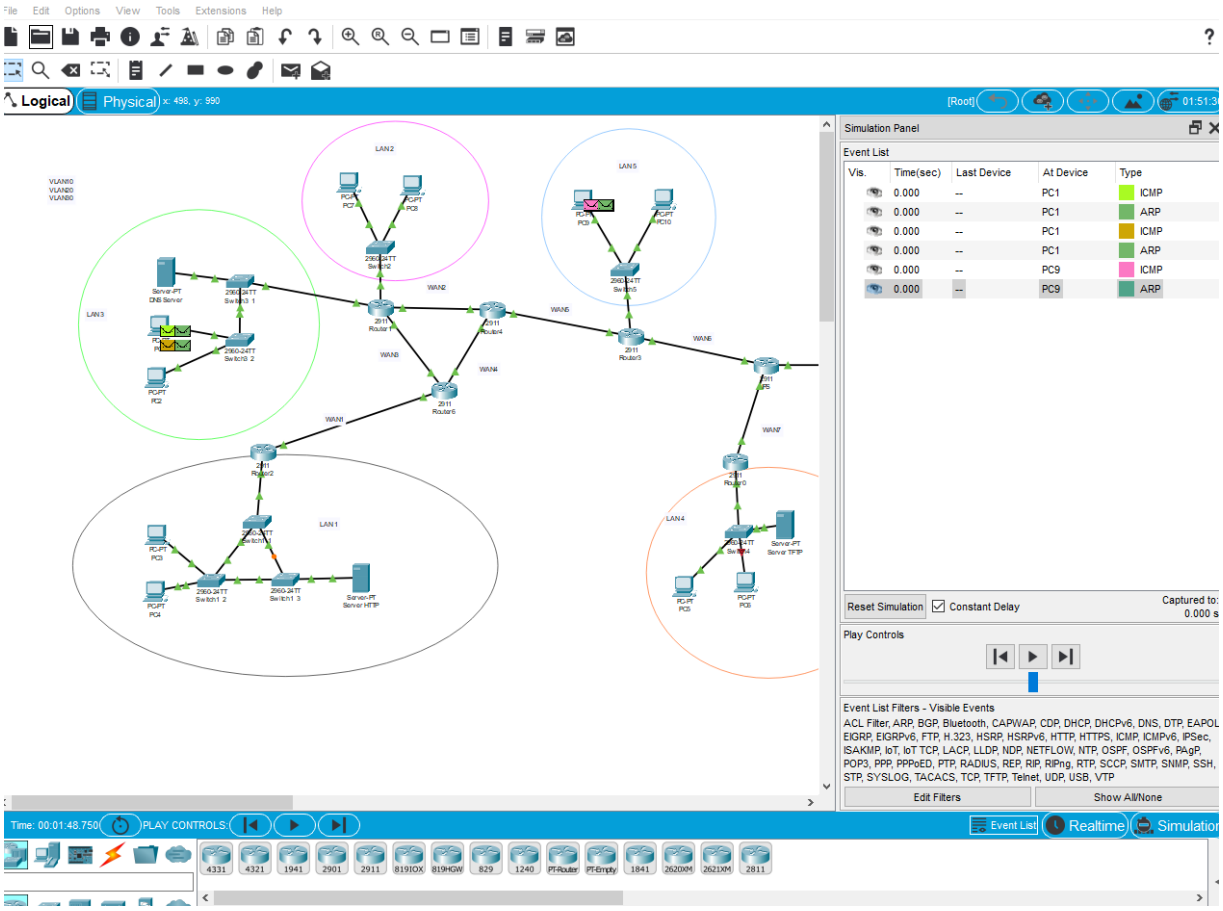

Рисунок 3.3 – Перевірка проходження пакетів між елементами моделі

Розроблена та налаштована модель комп’ютерної мережі у програмі Cisco Packet Tracer. Ця модель відповідає мережі підприємства і працює відповідно вимог. Тому результати моделювання мережі і конфігураційні файли віртуального мережевого устаткування можуть бути використані на реальному обладнанні підприємства з урахуванням того, що в проекті використали пристрої різних виробників.

3.2.1 Базове налаштування конфігурації пристроїв

Коммутатор D-Link DGS-1210-28/ ME

Комутатору повинна бути призначена власна IP-адреса, яка використовується для зв'язку з SNMP-менеджером або іншим додатком TCP/IP (наприклад, BOOTP, TFTP). IP-адреса комутатора за замовчуванням -

10.90.90.90. Його можна змінити відповідно до вимог мережі користувача. Комутатору також призначено унікальну заводську MAC-адресу. Ця MAC-адреса не може бути змінена. Його можна переглянути, ввівши команду CLI show switch.

MAC-адресу комутатора також можна знайти у Web-інтерфейсі у вікні System Information розділу Configuration. IP-адреса комутатора повинна бути призначена до того, як керування пристроєм зможе здійснюватися через Web-інтерфейс. IP-адреса комутатора може бути автоматично встановлена за допомогою протоколів BOOTP або DHCP, при цьому актуальна адреса, призначена комутатору, повинна бути відома. IP-адреса може бути встановлена за допомогою CLI. Для цього введіть команду config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy, де x - IP-адреса, призначена інтерфейсу з ім'ям System, y - відповідна маска підмережі. Як альтернативний варіант, можна ввести config ipif System ipaddress xxx.xxx.xxx.xxx/z, де x — IP-адреса, призначена інтерфейсу з ім'ям System, z — відповідне число підмереж при безкласовій адресації (CIDR).

Кожному комутатору повинна бути призначена власна IP-адреса, яка використовується для зв'язку з SNMP-менеджером. SNMP (Simple Network Management Protocol) є протоколом рівня 7 моделі OSI, розробленим спеціально для керування мережевими пристроями. SNMP дозволяє мережним станціям управління зчитувати та змінювати налаштування шлюзів, маршрутизаторів, комутаторів та інших мережних пристроїв.

DSA-2006 Сервісний маршрутизатор

Налаштування авторизації та доступу до SSH

! включаємо шифрування паролів

service password-encryption

! використовуємо нову модель AAA та локальну базу користувачів

aaa new-model

aaa authentication login default local

! заводимо користувача з максимальними правами

```
username admin privilege 15 secret PASSWORD
! даємо ім'я роутеру
hostname <...>
ip domain-name router.domain
! генеруємо ключик для SSH
crypto key generate rsa modulus 1024
! тюнінгуємо SSH
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh version 2
! і дозволяємо його на віддаленій консолі
line vty 0 4
  transport input telnet ssh
  privilege level 15
```

Налаштування роутингу

```
! включаємо прискорену комутацію пакетів
ip cef
```

Архівування конфігів

```
! включаємо архівування всіх змін конфіга, приховуючи паролі в логах
archive
  log config
   logging enable
   hidekeys
! історію зміни конфігу можна переглянути командою
show archive log config all
```

Налаштування DNS

```
! увімкнути дозвіл імен
ip domain-lookup
! включаємо внутрішній DNS сервер
ip dns server
```

```
! прописуємо DNS провайдера
ip name-server XXX.XXX.XXX.XXX
! про всяк випадок додаємо кілька публічних серверів DNS
ip name-server 4.2.2.2
ip name-server 208.67.222.222
ip name-server 208.67.220.220
```

Налаштування локальної мережі

```
! зазвичай порти внутрішнього світчу на роутері об'єднані в Vlan1
interface Vlan1
  description === LAN ===
  ip address 192.168.???.1
```

! включаємо на інтерфейсі підрахунок пакетів, що передаються клієнтам — зручно переглядати хто з'їдає трафік

```
  ip accounting output-packets
! подивитися статистику можна командою
show ip accounting
! очистити
clear ip accounting
```

Налаштування сервера DHCP

```
! виключаємо деякі адреси з пулу
ip dhcp excluded-address 192.168.???.1 192.168.???.99
! і налаштовуємо пул адрес
ip dhcp pool LAN
   network 192.168.???.0 255.255.255.0
   default-router 192.168.???.1
   dns-server 192.168.???.1
```

Налаштування Internet та Firewall

! налаштовуємо фільтр вхідного трафіку (за замовчуванням все заборонено)

```
ip access-list extended FIREWALL
```

```
 permit tcp any any eq 22
! включаємо інспектування трафіку між локальною мережею та Інтернетом
ip inspect name INSPECT_OUT dns
ip inspect name INSPECT_OUT icmp
ip inspect name INSPECT_OUT ntp
ip inspect name INSPECT_OUT tcp router-traffic
ip inspect name INSPECT_OUT udp router-traffic
ip inspect name INSPECT_OUT icmp router-traffic
! налаштовуємо порт в Інтернет і вішаємо на нього певний захист
interface FastEthernet0/0
 description === Internet ===
 ip address ???.???.???.??? 255.255.255.???
 ip virtual-reassembly
 ip verify unicast reverse-path
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 no cdp enable
 ip inspect INSPECT_OUT out
 ip access-group FIREWALL in
! ну і насамкінець шлюз за замовчуванням
ip route 0.0.0.0 0.0.0.0 ???.???.???.???
Налаштування NAT
! на Інтернет інтерфейсі
interface FastEthernet0/0
 ip nat outside
! на локальному інтерфейсі
interface Vlan1
 ip nat inside
```

```
! створюємо список IP, які мають доступ до NAT
ip access-list extended NAT
  permit ip host 192.168.???.??? any
! включаємо NAT на зовнішньому інтерфейсі
ip nat всередині source list NAT interface FastEthernet0/0 overload
! додаємо інспекцію популярних протоколів
ip inspect name INSPECT_OUT http
ip inspect name INSPECT_OUT https
ip inspect name INSPECT_OUT ftp
Вимкнення непотрібних сервісів
no service tcp-small-servers
no service udp-small-servers
no service finger
no service config
no service pad
no ip finger
no ip source-route
no ip http server
no ip http secure-server
no ip bootp server
```

3.3 Налаштування роботи Інтернет

Для того, щоб локальна мережа була повноцінно підключена до Інтернету, повинні дотримуватися три умови:

- кожна машина в локальній мережі повинна мати "реальні", інтернетівські IP-адреси;
- ці адреси повинні бути не будь-якими, а виділеними провайдером для локальної мережі (швидше за все, це буде підмережа класу C);

- на комп'ютері-шлюзі, підключеному до двох мереж - локальної мережі та мережі провайдера, повинна бути організована IP-маршрутизація, тобто передача пакетів з однієї мережі в іншу.

В цьому випадку локальна мережа стає частиною Інтернету. Власне, це той спосіб підключення, де підключені до Інтернету самі Інтернет-провайдери та хостинг-провайдери [17].

На відміну від звичайного підключення, розрахованого на один комп'ютер, при такому підключенні "під клієнта" виділяється не одна IP-адреса, а кілька, так звана "IP-підмережа". У такій підмережі перші три байта IP-адреси ідентифікують саму підмережу, а останнє число - комп'ютер в даній (Вашої) підмережі.

При такому способі підключення можна організувати в своїй мережі сервіси, доступні з Інтернету - адже при даному підключенні не тільки Інтернет повністю доступний з локальної мережі, але і локальна мережа - з Інтернету, тому що є його частиною.

Однак така "прозорість" мережі різко знижує її захищеність - адже будь-які сервіси в локальній мережі, навіть призначені для "внутрішнього" використання, стануть доступними через Інтернет, але доступ в локальну мережу з інтернету можна обмежити програмою-firewall.

Технологія Network Address Translation (NAT) - "трансляція мережевих адрес" дозволяє декільком машинам локальної мережі мати доступ до Інтернет через одне підключення і один реальний зовнішній IP-адреса.[17]

Для того, щоб комп'ютера локальної мережі могли встановлювати з'єднання з серверами мережі Інтернет, потрібно, щоб:

- IP-пакети, адресовані сервера в Інтернет, змогли його досягти;
- відповідні IP-пакети, що йдуть від сервера Інтернет на машину в локальній мережі, також змогли її досягти.

Працює це в такий спосіб - на комп'ютері-шлюзі встановлена програма NAT-сервера. Комп'ютер-шлюз прописаний на машинах локальної

мережі як "основний шлюз", і на нього відправляються усі пакети, що йдуть в Інтернет (не до самої локальної мережі). Перед передачею цих IP-пакетів в Інтернет NAT-сервер замінює в них IP-адреса відправника на свій, одночасно запам'ятовуючи у себе, з якої машини локальної мережі прийшов цей IP-пакет. Коли приходить відповідь пакет (на адресу шлюзу), NAT визначає, на яку машину локальної мережі його треба направити. Потім в отриманому пакеті змінюється адреса одержувача на адресу потрібної машини, і пакет доставляється цій машині через локальну мережу.

Робота NAT-сервера прозора для машин локальної мережі. Єдиним принциповим обмеженням цього методу є неможливість встановити вхідні TCP-з'єднання з Інтернет на машину локальної мережі. Однак для "клієнтських" мереж цей недолік перетворюється на гідність, різко збільшуючи їх захищеність і безпеку.

3.4 Розрахунок основних характеристик для вихідного трафіку мережі підприємства

Необхідно розрахувати трафік в мережі, який генерується найбільшою локальною мережею за умови що усі користувачі генерують запити у мережу.

У результаті розрахунку ми отримуємо наступні характеристики:

коефіцієнт зайнятості;

завантаження каналу;середня затримка кадру;

середня довжина черги;

середній час перебування пакета в черзі;

пропускна здатність каналу.

Для розрахунку приймається модель ділянки мережі як модель СМО M/M/1.

Характеристики системи:

кількість вузлів в мережі: 92

середня інтенсивність трафіку: μ=80 (кадрів/с)

середня довжина повідомлення: l=600 байт;

вимоги до затримки передачі пакету – ≤5 мс.

Розрахунок характеристик.

Рр.д= μ·l·n·8=80·600·92·8= 35,3 (Мбіт/с), де

n- кількість користувачів.

Отримані при розрахунку результати не перевищують задані параметри мережі. Отже, перевантажень на обраному обладнанні не буде.

Комутатор рівня розподілу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1000Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

μвих=1000 000 000/(600*8)=208334 пакетів/с

Оскільки кожне джерело виробляє в середньому 80 пакетів/с, то ми обмежені приєднанням до комутатора рівня розподілу максимум:

N=208334/80=2604 джерела.

Що задовольняє нашу мережу на 92 ПК.

Кожен з 92 ПК посилає потік заявок з інтенсивністю 80 кадрів/с. Максимальна інтенсивність вихідного трафіку від всіх користувачів:

λ=N·μ= 92*80=7360 (пакетів/с)

Коефіцієнт затримки на рівні розподілу, тобто показник завантаженості вихідного каналу зв'язку, який впливає на час стояння в черзі:

ρ=λ/μ_вих =7362/208334=0,035

Коефіцієнт зайнятості комутатора рівня розподілу:

r=ρ/(1-ρ)=0,035/(1-0,035)=0,036

Середня затримка кадру, пов’язана з чергою M/M/1, дорівнює:

$T=1/((\mu-\lambda))=1/(208334-7360)=4.9\cdot10^{-6}$ с

Середня довжина черги:

L_чер=ρ^2/(1-ρ)= 〖0,035^2/(1-0,035)=0,0012

У результаті розрахунків ми бачимо, що завантаження мережі досить не значне у порівнянні з можливостями маршрутизаторів та каналів передачі даних.

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Функціональне призначення парольного захисту

За функціональним призначенням парольний вхід, як правило, використовується для контролю завантаження системи, контролю функціонування та з метою блокування (рис. 4.1).

Для вирішення задачі контролю функціонування обчислювальної системи виділяються:

• контроль користувача під час доступу до системи. Реалізується зокрема штатними засобами ОС.

• контроль під час запуску процесу. Встановлення парольного захисту для запуску деяких програм.

• контроль доступу до локальних ресурсів. Встановлення пароля на конкретну машину з'єднану ЛОМ.

• контроль доступу до мережевих ресурсів.

Як реакцію несанкціонований вхід системою захисту може встановлюватися блокування деяких функцій: завантаження системи, доступом у систему, запуск певних додатків тощо.

4.2 Реалізація механізмів парольного захисту.

Реалізація залежить від способу введення пароля та від розташування еталонних даних.

Способи введення пароля:

• З клавіатури (консольне введення)

• З зовнішнього носія

• З використанням біометричних характеристик користувача.

• Комбінований.

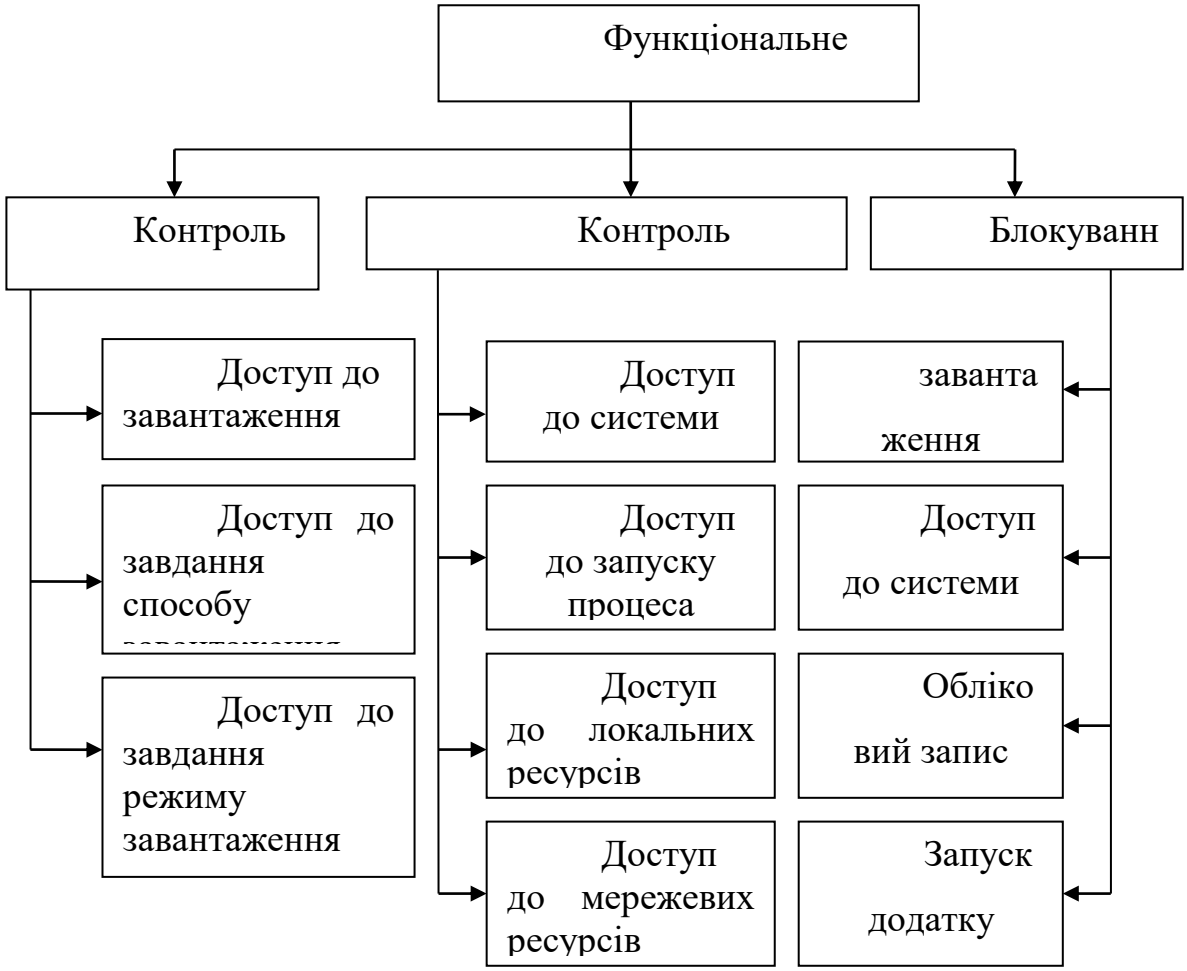

Рисунок 4.1 – Функціональне призначення парольного захисту

Консольне введення найпоширеніше. Є у всіх ОС. Все дуже просто: користувач вводить пароль, який запитує система, з клавіатури. Недолік цього способу візуальний знімання пароля зловмисником. Введення пароля із зовнішнього носія - під ними можемо розуміти: дискету, пристрої, що спеціально підключаються для введення пароля.

Суть у тому, що на носіях записується пароль, який зчитується системою під час автентифікації користувача. Що відрізняє цей спосіб від попереднього це те, що довжина пароля може бути досить довгою, цим ми запобігаємо візуальному зніманню. Недоліком є те, що носій може бути вкрадений зловмисником.

Комбінований. Здійснюється двома механізмами, один з яких є основним, а інший – додатковим. тобто. для входу потрібно ввести пароль за допомогою двох, перерахованих вище способів: спочатку пароль вводимо за допомогою зовнішнього носія (основний), а далі вводимо з клавіатури (додатковий).

Біометричні характеристики користувача Так як кожна людина індивідуальна і має свої особливості. Чим унікальний цей спосіб, що кожна людина має свій пароль, який не можна підробити або передати.

4.3 Зберігання та хешування паролів

Безпечне зберігання паролів є добре дослідженим завданням у науці про безпеку, яка свідчить, що найкращий спосіб зберегти пароль – це зберігати його зовсім, а зберегти хеш-пароль – результат застосування односторонньої хеш-функції до вихідного паролю. Одностороння хеш-функція чудова тим, що знаючи значення аргументу, обчислити її значення дуже легко, але за значенням функції знайти відповідний аргумент за розумний час практично неможливо. Таким чином, якщо ми маємо пароль P, то замість того, щоб зберігати значення P у явному вигляді, ми зберігаємо значення H(P), де H – відповідна хеш-функція. Навіть якщо зловмисникам вдасться заволодіти збереженими хешами, їм теоретично знадобляться сотні років, щоб знайти вихідні паролі, яким відповідають ці значення. Коли настає час перевірити пароль P', введений користувачем, ми обчислюємо H(P') і порівнюємо його зі збереженим значенням H(P). Якщо значення хеш-функції збігаються, це з дуже високим ступенем ймовірності говорить про те, що її аргументи збігаються, тобто введений користувачем пароль збігається з тим паролем, який був заданий на самому початку. Описана вище схема має, однак, істотну ваду [3]. Справа в тому, що користувачі досить передбачувані у виборі паролів, що уможливлює так звану атаку за словником. Суть атаки в тому, що зловмисникам достатньо перебрати відносно невеликий набір паролів, що складається з широковживаних слів, імен, назв міст і т.д. Хакери

можуть піти ще далі та заздалегідь обчислити значення хеш-функції для всіх слів зі словника. У такому разі, заволодівши нашою базою паролів, їм залишиться лише порівняти значення з нашої бази із заздалегідь обчисленими значеннями хеш-функції, щоб знайти усі паролі зі словника. Інший недолік запропонованого методу полягає в тому, що якщо два користувача виберуть один і той же пароль, то значення в базі даних паролів збігатимуться. Таким чином, "зламавши" пароль одного користувача, зловмисники автоматично дізнаються пароль іншого. Щоб уникнути цих недоліків і максимально утруднити завдання зловмисникам, використовується схема хешування із синхропосилкою. У цій схемі спочатку генерується невелике випадкове число - синхропосилання (в англомовній літературі це число називають словом salt [сіль]) - яка хешується разом з вихідним паролем. Синхропосилання не є секретним, але є унікальним для кожного збереженого пароля і зберігається разом з отриманим хеш. Коли потрібно перевірити пароль, синхропосилання та хеш вилучаються з бази даних, введений пароль хешується разом із синхропосилкою, і результат порівнюється зі значенням хешу, витягнутим з бази даних. Якщо вони збігаються, це свідчить, що введений пароль збігається з вихідним паролем. Тепер, навіть якщо два користувача виберуть однаковий пароль, збережений хеш буде різним, оскільки синхропосилання унікальне для кожного збереженого пароля. Більше того, тепер зловмисники не можуть наперед обчислити значення хеш-функції для словникової атаки. Їм доведеться хешувати кожне слово окремо з кожним синхропосиланням, що значно уповільнює процес підбору пароля (але, втім, не робить його неможливим, тому постарайтеся, щоб ваш пароль не був словом зі словника). Межа запам'ятовуваності паролів лежить на межі 8-12 символів, і, отже, якщо змушувати користувача оперувати саме ключем, цим практично змусимо його до запису ключа на якомусь аркуші паперу чи електронному носії, наприклад, у текстовому файлі. Це, звісно, різко знижує захищеність системи. Для вирішення цієї проблеми були розроблені методи, що

перетворюють свідомий, осмислений рядок довільної довжини - пароль, в зазначений ключ заздалегідь заданої довжини. У переважній більшості випадків цієї операції використовуються звані хеш-функции (від англ. hashing – дрібна нарізка і перемішування). Хеш-функцією називається таке математичне чи алгоритмічне перетворення заданого блоку даних, яке має такі властивості:

1. хеш-функція має нескінченну область визначення,

2. хеш-функція має кінцеву область значень,

3. вона незворотня,

4. зміна вхідного потоку інформації однією біт змінює близько половини всіх біт вихідного потоку, тобто результату хеш-функции.

Ці властивості дозволяють подавати на вхід хеш-функції паролі, тобто текстові рядки довільної довжини будь-якою національною мовою і, обмеживши область значень функції діапазоном 0..2N-1, де N – довжина ключа в бітах, отримувати на виході досить рівномірно розподілені області значення блоки інформації – ключі.

Вимоги, подібні до 3 і 4 пунктів вимог до хеш-функції, виконують блокові шифри. Це вказує на один із можливих шляхів реалізації стійких хеш-функцій – проведення блокових криптоперетворень над матеріалом рядка-паролю. Цей метод і використовується у різних варіаціях практично у всіх сучасних криптосистемах. Матеріал рядка-пароля багаторазово послідовно використовується як ключ для шифрування деякого заздалегідь відомого блоку даних - на виході виходить зашифрований блок інформації, що однозначно залежить тільки від пароля і при цьому має досить хороші статистичні характеристики. Такий блок або декілька таких блоків і використовуються як ключ для подальших криптоперетворень. Характер застосування блокового шифру для хешування визначається ставленням розміру блоку використовуваного криптоалгоритму і розрядності необхідного хеш-результату. Якщо вищевказані величини збігаються, то використовується схема одноцепочного блочного шифрування. Початкове

значення хеш-результату H0 встановлюється рівним 0, весь рядок-пароль розбивається на блоки байт, рівні по довжині ключа використовуваного для хешування блочного шифру, потім проводять перетворення за реккурентною формулою:

Hj = Hj-1 XOR EnCrypt (Hj-1, PSWj),

де EnCrypt (X, Key) - використовується блоковий шифр (рис.4.2).

Останнє значення Hk використовується як шуканий результат

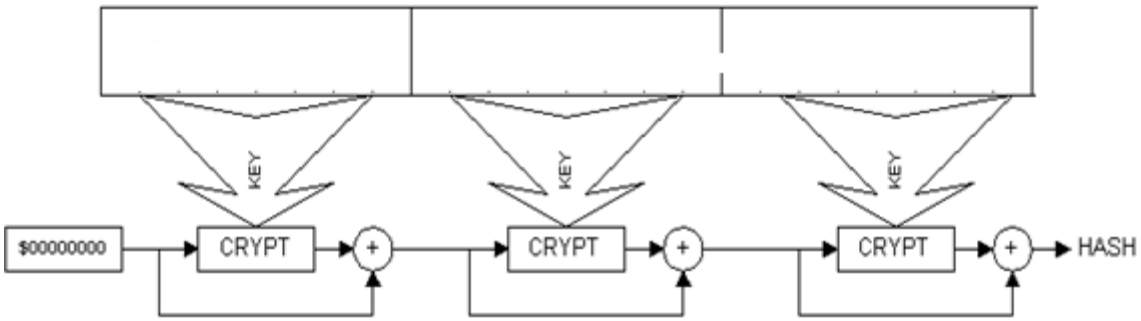

Рисунок 4.2 - Схема хешування блочного шифру

У тому випадку, коли довжина ключа рівно в два рази перевищує довжину блоку, а подібна залежність досить часто зустрічається в блокових шифрах. Для проведення лише одного перетворення, наприклад, блоковим шифром з ключем довжиною 128 біт Для отримання та володіння паролем, а відповідно інформацією деякі зловмисники вигадують різні способи, але в основному все можна світити до ряду стандартних:

• Візуальний знімок пароля.

• Викрадення носія, інформаційного ключа.

• Вгадування або підбір пароля.

• Скидання пароля

• Розгадування хешу

• Використання розрахункових таблиць

• Аналіз паролів.

• Технічне знімання пароля під час введення.

• Вимкнення механізму захисту авторизації.

• Модифікація облікових даних на захищеному об'єкті.

Якщо перші два зрозуміло як реалізуються, то розглянь інші

Вгадування або підбір пароля

Найпоширеніший тип атаки – вгадування пароля. Зломщики можуть вгадувати паролі локально чи дистанційно, вручну та із застосуванням автоматичних методів. Іноді вгадати пароль простіше, ніж здається здавалося б. У налаштуваннях більшості мереж не потрібні довгі і складні паролі, і хакеру достатньо знайти лише один слабкий пароль, щоб отримати доступ до мережі. Не всі протоколи використовується 16 байт рядка-паролю, а сама довжина пароля рідко перевищує 32 символи. Отже, при обчисленні хеш-функції над паролем буде зроблено максимум 2 "повноцінні" криптоперетворення.

Вирішення цієї проблеми можна досягати двома шляхами:

1) попередньо "розмножити" рядок-пароль, наприклад, записавши його багаторазово послідовно до досягнення довжини, скажімо, в 256 символів;

2) модифікують схему використання криптоалгоритму так, щоб матеріал рядка-паролю "повільніше" витрачався при обчисленні ключа.

Автентифікації однаково ефективні проти спроб вгадування паролів. Наприклад, процедура аутентифікації LAN Manager нечутлива до регістру символів, тому під час відгадування пароля не доводиться враховувати регістр літер. Багато інструментів злому автоматизують процес, вводячи пароль за паролем.

Деякі поширені інструменти відгадування:

• Hydra - для відгадування будь-яких паролів, у тому числі HTTP, Telnet та Windows;

• TSGrinder – для атак методом «перебору» проти з'єднань Terminal Services та RDP;

• SQLRecon -для атаки методом «перебору» проти процедури автентифікації SQL.

В автоматизованих програмах вгадування та злому пароля використовується кілька підходів. Метод «перебору» забирає найбільше часу і є найефективнішим. При цьому перебираються всі можливі комбінації символів для пароля при заданому наборі символів (наприклад, abcda | ABCDa | 1234a | !@#$) та максимальна довжина пароля.

Атака за словником

Це метод, за допомогою якого можна розкрити осмислений пароль. Метод заснований на тому, що користувач для легшого запам'ятовування вибирає існуюче деякою мовою (словникове) слово. Якщо врахувати, що у будь-якій мові трохи більше 100.000 слів, очевидно, що перебір словникових слів відбудеться протягом невеликого проміжку часу. Словникові атаки проводяться у припущенні, більшість паролів складається з цілих слів, дат і чисел, взятих зі словника. Для інструментів з урахуванням словникових атак потрібен вхідний словниковий список. З Internet можна завантажити різні безкоштовні та комерційні бази даних із спеціалізованими словниками (наприклад, англійський словник, спорт і навіть лексика «Зоряних війн»). При гібридному методі вгадування паролів передбачається, що адміністратори мережі вимагають від користувачів, щоб пароль хоча б трохи відрізнявся від терміна зі словника. Правила гібридного вгадування відрізняються в різних інструментах, але в більшості поєднуються символи нижнього і верхнього регістрів, додаються цифри в кінці пароля, слова вводяться в зворотному порядку або з граматичними помилками, використовуються такі символи, як @! #. Гібридний режим реалізований у програмах John the Ripper та Cain & Abel [4]. Наприклад, в результаті

проведеного аналізу встановлено максимальний час злому паролів програмою PwlTool методом "перебору". Швидкість перебору паролів 106 000 паролів.

У таблиці 4.1 показані відносні інтервали часу, які підбираються паролі різної довжини з різних словників.

Таблиця 4.1 - Відносні інтервали часу підбору паролів

Довжина пароля	Довжина - 26 (тільки букви)	36 (букви і цифри)	70 (всі печатаемі символи)	Кирилиця
4	Відразу	Відразу	3 хвилини	Відразу
5	1 хвилина 48 секунд	9 хвилин	3 год.	5 хвилин
6	50 хвилин	5 год. 48 хвилин	10 днів 17 год.	2 год. 53 хвилини
7	22 год.	8 днів 17 год.	2 роки 3 дня	26 год.
8	24 дні	314 днів 17 год.	138 років	123 дні 12 год.
9	1 год 248 днів	30 років	9363 років	10 років

Скидання пароля – ефективний підхід, коли потрібний лише доступ до блокованого комп'ютера, але спроби скидання пароля привертають небажану увагу. Зазвичай зломщики вважають за краще впізнавати паролі, не скидаючи їх. Зламування пароля полягає в перетворенні захопленого хеша пароля (або іншої секретної форми текстового пароля або пакетів «запит-відповідь») у чисто текстовий оригінал. Щоб розкрити пароль, зломщику необхідні такі інструменти, як екстрактори для розгадування хеша, розрахункові таблиці для пошуку текстових паролів та аналізатори паролів для вилучення даних про аутентифікацію.

Розгадування хеша. Деякі інструменти злому паролів забезпечують як вилучення, так і злом хеша пароля, але більшості необхідний хеш LM, щоб розпочати процес злому. Деякі інструменти придатні для хешів NT.

Найпоширеніший екстрактор хеша паролів Windows - сімейство програм Pwdump. За кілька років випустили багато версій Pwdump, поточна версія — Pwdump4.

Багато інструментів злому паролів приймають хеші у форматі Pwdump. У таких інструментах процес злому зазвичай починається з генерації ряду можливих паролів, які потім хешуються, і хеші порівнюються з вилученим хеш. Типові програми злому паролів - John the Ripper та Cain & Abel. Випускаються версії John the Ripper для UNIX та Windows. Це дуже швидкий інструмент, який працює з командного рядка, який постачається з модулем розширення для розподілених обчислень. Cain & Abel забезпечує злом понад 20 типів хешів паролів, у тому числі LM, NT, Cisco та RDP.

Розрахункові таблиці. Сучасні програми злому паролів генерують всі можливі паролі та його хеші у цій системі і вводять результати таблицю перетворення, іменовану розрахункової. Виймаючи хеш з цільової системи, зломщик може легко звернутися до розрахункової таблиці і знайти суто текстовий пароль. Деякі програми (і Web-вузли) за пару секунд зламують будь-які хеші LM із використанням розрахункової таблиці. Можна придбати дуже великі таблиці, розміри яких становлять від сотень мегабайтів до сотень гігабайтів, або генерувати власну з використанням Rainbow Crack. Метод захисту від розрахункових таблиць - відключити хеші LM і використовувати довгі, складні паролі.

Аналіз паролів.

Деякі програми зламування паролів аналізують трафік автентифікації між клієнтом і сервером і витягують хеші паролів, або достатню інформацію для початку процедури зламування. Cain & Abel аналізує трафік автентифікації та зламує вилучені хеші. Інші програми аналізу та злому паролів - ScoopLM і KerbCrack, які працюють з трафіком автентифікації Kerberos.

Технічне знімання (захоплення) пароля

Існують програми, які можуть перехопити надходить інформацію на об'єкт, що захищається. Прикладом таких програм можуть бути реєстратори натискань клавіш (кейлоггери), сніфери клавіатури і каналів связи[4]. Сніфери клавіатури запам'ятовують всі послідовності паролів, що вводяться, а кейлоггери (клавіатурні шпигуни) — програмне забезпечення, основним призначенням якого є прихований моніторинг натискань клавіш і ведення журналу цих натискань. Перехоплення натискань клавіш може використовуватися звичайними програмами і часто використовується для виклику функцій програми з іншої програми за допомогою «гарячих клавіш» або, наприклад, перемикання неправильної розкладки клавіатури. Існує маса легального ПЗ, яке використовується адміністраторами для спостереження за тим, що робить працівник протягом дня, або для спостереження за активністю сторонніх людей на своєму комп'ютері. Те ж «легальне» ПЗ найчастіше використовується і з метою навмисного викрадення секретних даних користувача, наприклад паролів. Багато хакерів захоплюють паролі, просто встановлюючи для реєстрації натискань на клавіші «троянських коней» або один з багатьох фізичних пристроїв контролю над клавіатурою. Компанія Symantec повідомляє, що 82% шкідливих програм, що найбільш широко використовуються, крадуть конфіденційну інформацію. Більшість краде паролі. За 99 дол. будь-хто може купити клавіатурний реєстратор, який записує більше 2 млн. натискань на клавіші. Фізичний пристрій довжиною менше 2,5 см легко вставити між шнуром клавіатури та портом комп'ютера. Крім того, не важко перехоплювати паролі з бездротових клавіатур навіть на відстані кварталу. Відключення механізму захисту авторизації, якщо механізм парольного захисту є певний процес, виконання цього процесу можна зупинити засобами системного моніторингу та інших. методами. Модифікація облікових даних захищеному об'єкті. Суть полягає в модифікації облікових записів на об'єкті, що захищається. Це здійснюється шляхом заміни або шляхом скидання у вихідний стан налаштувань механізмів захисту.

4.4 Стратегії вибору пароля

У нормативних документах та Інтернеті можна знайти величезну кількість рекомендацій щодо парольного захисту. Ці рекомендації можна звести до трьох груп:

• рекомендації щодо складання правильних (сильних) паролів;

• рекомендації щодо введення пароля

• заходи організаційного характеру

Рекомендації щодо складання паролів та типова інструкція щодо організації парольного захисту наведені в додатках А та Б

4.5 Парольний аудит.

Парольний захист не задовольняє сучасні уявлення про інформаційну безпеку. Причина цього - дуже сильна залежність цього виду аутентифікації від так званого людського фактора. Тобто. надійність парольної автентифікації повністю залежить від цього, яке ключове слово вибрав собі користувач і як і його зберігає.

В ідеалі ключове слово має бути абсолютно випадковим набором з літер, цифр та спеціальних символів та мати довжину не менше 8-10 знаків залежно від конкретного завдання. Тим більше що більшість користувачів намагаються полегшити собі життя, навіщо під час виборів пароля використовують або осмислені висловлювання, або персональну інформацію (прізвище, ім'я дитини, ім'я тварини, елементи адреси, телефону, номери документів тощо.). Інші люди йдуть шляхом скорочення ключового слова, залишаючи в ньому 4-5, а то й взагалі 2-3 символи. Є ще третій варіант спрощення використання пароля. Людина вигадує дійсно надійне ключове слово, яке відповідає всім вимогам інформаційної безпеки, запам'ятовує його, а потім застосовує скрізь, тобто у всіх сервісах з парольним захистом.

Все це робить паролі вразливими до різних атак зловмисників. Застосування усюди єдиного ключового слова дозволяє зловмисникам

проникати у добре захищені інформаційні системи шляхом злому "слабких" у плані безпеки сервісів.

Тому контролю якості паролів може використовуватися лише їх аудит.

Взагалі, в галузі інформаційної безпеки найбільшого поширення набув експертний аудит. При його проведенні спеціаліст або група фахівців досконально досліджують систему захисту або будь-яку її частину, після чого виносять рішення про її надійність або, навпаки, ненадійність, а також видають замовнику перелік потенційно небезпечних місць з рекомендаціями щодо їх усунення. У разі парольного аудиту експертний аудит не підходить.

По-перше, "експертом", швидше за все, виступатиме системний адміністратор, який відповідає у компанії за працездатність інформаційної системи. І далеко не факт, що він настільки добре розуміється на захисті комп'ютерних даних, щоб самостійно оцінити надійність пароля.

По-друге, у цьому випадку всім без винятку користувачам доведеться показати свої паролі одній людині. Це повністю "розв'язує руки" останньому, дозволяючи йому заходити від імені будь-якого співробітника та отримувати доступ до будь-якої корпоративної інформації.

Таким чином, повний контроль якості паролів може здійснюватися тільки за допомогою активного аудиту. При його проведенні відповідальний співробітник повторює всі можливі дії зловмисника зі злому парольного захисту, в ході яких з'ясовується, наскільки ключові слова користувачів можуть протистояти хакеру.

Для проведення активного аудиту якості паролів потрібне спеціальне програмне забезпечення. Причому бажано, щоб воно могло повністю взяти на себе все тестування, надаючи адміністратору лише його результати. Прикладом такої утиліти може бути продукт Proactive Password Auditor, розроблений фахівцями компанії "ЕлкомСофт". Приклад проведення активного аудиту.

• Перший крок у будь-якій атаці на систему – отримання хешів паролів.

Отримавши хеші, зловмисники можуть з допомогою різних атак спробувати відновити їх початкову інформацію, тобто паролі. Зробити це можна кількома способами за допомогою різних утиліт. Тому для запобігання можливим діям хакера бажано, щоб у програмі, що використовується для аудиту, були реалізовані всі.

• Відразу після отримання хешів аудитор має провести «швидку» атаку, яка допоможе знайти всі паролі, створені з грубим порушенням правил. Так, наприклад, у програмі Proactive Password Auditor в першу чергу запускається перебір за вбудованим словником (він невеликий, але містить найчастіше використовуються слова), потім слідує атака зі спеціально підібраними параметрами, спроба вилучення ключових слів з пам'яті і т.д.

• Наступним етапом аудиту є проведення різних атак.

Тут можливі чотири варіанти. Починати найкраще з атаки за словником. За її реалізації пароль підбирається за допомогою зазначених користувачем списків осмислених слів. Природно, що більше словник, то ймовірніший успіх атаки. Список слів можна знайти в Інтернеті або купити на компакт-диску.

Якщо підбір за словником не дав жодних результатів, необхідно перейти до методів, що потребують більшого часу. Першим із них є повний перебір. При виборі користувачеві необхідно вказати інтервал можливих довжин паролів та набори символів, які можуть використовуватися для їх створення (латинські літери, цифри, спецсимволи, введений людиною набір). Також при необхідності адміністратор може включити перевірку не всіх можливих варіантів, а лише кількох вказаних діапазонів. Цей метод підбору паролів може використовуватись для перевірки їхньої довжини. Виставивши значення на один символ менше мінімально достатнього значення (залежить від конкретного завдання, зазвичай коливається від 8 до 10 символів), адміністратор зможе перевірити всі можливі ключові слова, які не відповідають вимогам безпеки. Інший варіант – підбір пароля по масці. Тут адміністратор вказує не просто можливу довжину ключового слова, а може

ввести деякі відомі йому символи. В іншому ж ця атака нічим не відрізняється від повного перебору всіх можливих варіантів.

Останній крок аудиту – це складання звіту. Зазвичай звітів потрібно щонайменше два. Перший з них для системного адміністратора або співробітника, який відповідає за інформаційну безпеку, другий – для керівництва. У першому звіті відображаються користувачі, паролі яких були виявлені програмою. Ну а другий є наочним графіком, на якому відображається, скільки досліджених паролів за який час можуть підібрати зловмисники. Він чудово підходить для ілюстрації актуальності проблеми безпеки керівництва компанії.

Вирішення цього завдання досягається за рахунок

• Навчання користувачів.

• Генерування паролів комп'ютером.

• Реактивна перевірка пароля.

• Запобіжна перевірка пароля.

Користувачам можна роз'яснити важливість використання паролів, які важко вгадувати, і видати рекомендації щодо правильного вибору таких паролів. Стратегія навчання користувачів у більшості випадків виявляється малоефективною, особливо якщо число користувачів велике або є постійний приплив і відтік користувачів. Одні користувачі просто ігноруватимуть рекомендації, інші просто не зможуть оцінити, наскільки надійними є вибрані ними паролі.

Генерування паролів за допомогою комп'ютера також призводить до проблем. Якщо генерувати паролі у вигляді випадкових наборів букв та цифр, користувачі не зможуть їх запам'ятати. Навіть якщо паролі є більш менш вимовними словами, користувачі однаково, відчуваючи труднощі із запам'ятовуванням таких слів, прагнутимуть записати їх. Генерування паролів за допомогою комп'ютера має сумний досвід з погляду зручності користувача. Його алгоритм генерує вимовні слова за допомогою комбінації

вимовних буквосполучень. Потік символів, що формується з буквосполучення та слова, забезпечується генератором випадкових чисел.

Стратегія реактивної перевірки паролів полягає в тому, що система періодично запускає власну програму підбору паролів, що виявляє паролі, що легко вгадуються. Система скасовує всі розгадані паролі та сповіщає про це відповідних користувачів. Цей підхід має ряд недоліків. По-перше, виконання такої перевірки в повному обсязі вимагає від системи великої витрати ресурсів. Зважаючи на те, що потенційний противник, який зможе отримати копію файлу паролів, може дозволити собі кинути на вирішення завдання всі ресурси свого комп'ютера протягом багатьох годин або навіть днів, ефективна програма реактивної перевірки паролів знаходиться явно в більш програшному положенні. Крім того, всі наявні паролі залишаються вразливими до тих пір, поки програма реактивної перевірки паролів не закінчить роботу і паролі, що легко вгадуються, не будуть виявлені.

Найбільш перспективним з погляду поліпшення захисту паролів є стратегія попереджувальної перевірки паролей. У разі попереджувальної перевірки паролів користувачеві дозволяється вибирати пароль на свій розсуд, але в процесі вибору система перевіряє пароль на відповідність встановленим вимогам і, якщо необхідно, відкидає його. Такий підхід заснований на переконанні, що під керівництвом системи з досить широкого простору допустимих паролів користувач вибере пароль, який він зможе легко запам'ятати, але який практично неможливо вгадати за допомогою перебору значень зі словника.

Проблема попереджувальної перевірки паролів полягає у необхідності досягнення балансу між стійкістю пароля та прийнятністю пароля для користувача.

• Якщо система відкидає надто багато паролів, користувачі скаржаться, що вибрати відповідний пароль надто важко.

• Якщо система використовує для перевірки придатності паролів занадто простий алгоритм, це лише дає зломщику можливість удосконалити свою програму підбору паролей.

Існує кілька методів запобіжної перевірки паролів.

Перший метод полягає у створенні простої системи контролю над дотриманням певних правил. Наприклад, можна вимагати, щоб дотримувалися наступних правил.

• Усі паролі повинні містити не менше восьми символів.

• Серед перших восьми символів повинні бути принаймні одна мала літера, одна велика літера, одна цифра та один знак пунктуації.

Ці правила повинні супроводжуватись відповідними інструкціями користувачеві. Хоча цей підхід краще простого навчання користувачів, він не завжди може зупинити зломщика паролів. Така схема дає порушнику інформацію про те, які паролі не слід перевіряти, але зрештою не виключає можливості успішного проведення відповідної атаки.

Іншим способом попереджувальної перевірки паролів є просте створення великого словника потенційно " поганих " паролів. При виборі користувача пароля система перевіряє, чи не потрапляє вибраний пароль до "чорного списку". Цей підхід має два недоліки.

1. Щоб описаний вище підхід був досить ефективним, словник має бути досить великим.

2. Час пошуку у великому словнику також може бути занадто великим. Крім того, для перевірки можливих модифікацій слів необхідно або включити ці модифікації до словника, що зробить його взагалі величезним, або витрачати додатковий час для перевірки модифікацій слів з допомогою спеціальних алгоритмів.

ВИСНОВКИ

Віповідно до завдань в кваліфікаційній роботі спроектована комп’ютерна мережа підприємства.

Виконаний аналіз організаційної структури підприємства зроблені висновки що до відповідності попередньої моделі мережі вимогам підприємства.

Розроблений проект технічних вимог до розроблюваної мережі.

Вибрані мережеві технічні засоби, що характеризуються сучасними характеристиками які забезпечують високі експлуатаційні властивості мережі.

Розроблена адресація пристроїв комп’ютерної мережі.

Виконані базові налаштування роутерів і комутаторів мережевого обладнання.

Розроблені заходи що до інформаційної безпеки в комп’ютерній системі підприємства.

Розроблена та досліджена імітаційна модель комп’ютерної мережі у пакеті Cisco Packet Tracer.

Дослідження показали що проект мережі працездатний і комп’ютерна мережа відповідає поставленому завданню.

Як компонент системи розроблена методика генерування і зберігання паролів, які забезпечують надійність при доступі до функцій комп’ютерної системи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Журавська І. М. Проектування та монтаж локальних комп'ютерних мереж :[навчальний посібник] / І. М. Журавська. – Миколаїв : Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.
2. Жуков, І. А. Комп'ютерні мережі та технології : навч. посіб./І. А. Жуков, В. О. Гуменюк, І. Є. Альтман. – К. : НАУ, 2004. – 276 с.
3. Аналоговые и цифровые системы видеонаблюдения (Електрон. ресурс)/Спосіб доступу:URL:http://elites-montage.com.ua/svanalog.php. - Загол. з екрана.
4. Система відеоспостереження (Електрон. ресурс) / Спосіб доступу: URL: http://fidgur.livejournal.com/29944.html – Загол. з екрана.
5. Формати відеоспостереження (Електрон. ресурс) / Спосіб доступу: URL: http://spec.prom.ua/a37913-klassifikatsiya-formatov-razresheniya.html – Загол. з екрана.
6. Закон України "Про електронний цифровий підпис", 2003 – 10 с.
7. IP Калькулятор [Электронний ресурс] – Режим доступа : URL : http://ip-calculator.ru/. – Загол. з екрана.
8. VLSM Calculator – калькулятор подсетей с маской переменной длины [Электронный ресурс]. – Режим доступа:URL:http://www.vlsm-calc.net/. – Загол. з екрана.
9. Воробьёва Н.И., Корнейчук В.И., Савчук Е.В. Надёжность компьютерных систем. – К.: «Корнійчук», 2002. – 144 с.
10. Мережеве обладнання [Электронный ресурс] – Режим доступа : URL : https://elmir.ua/routers/router_zyxel_sbg5500-a.html. – Загол. з екрану.
11. Правила з технічного захисту інформації для приміщень банків, у яких обробляються електронні банківські документи (Електрон.

ресурс) / Спосіб доступу: URL: http://www.txnet.com/ekranuvanna-servernih-primisen – Загол. з екрана.

12. Кулаков Ю.А., Луцкий Г.М. Локальные сети. – К.: Юниор, 1998. – 336 с.
13. Кулаков Ю.А., Омелянский С.В. Компьютерные сети. Выбор, установка, использование и администрирование. – К: Юниор, 1999. – 544 с.
14. Баня Е.Н. Компьютерные сети. – К.: Світ, 1999. – 112 с.
15. Джеймс Челлис Основы построения сетей: Учебное пособие для специалистов MCSE 1.0. – СПб.: Питер, 1997. – 326 с.
16. Microsoft Corporation. Принципы проектирования и разработки программного обеспечения. Учебный курс MSCD/ Пер. с англ. – М.:, 2002. – 736 с.
17. Розробка програмного забезпечення комп'ютерних систем. Програмування [Текст]: навч. посібник / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова. – 2-ге вид., випр. – Д.: Національний гірничий університет, 2011. – 222 с.
18. Цвіркун Л.І. Глобальні комп'ютерні мережі. Програмування мовою PHP: навч. посібник / Л.І. Цвіркун, Р.В. Липовий, під заг. ред. Л.І. Цвіркуна. – Д.: Національний гірничий університет, 2013. – 239 с.
19. Комп'ютерні мережі. Методичні вказівки до виконання лабораторних робіт студентами напряму підготовки 6.050102 Комп'ютерна інженерія /Я.В. Панферова, І.В. Кмітіна, Л.І. Цвіркун. – Д.: Національний гірничий університет, 2012. – 31 с.
20. В.І. Голінько,В.Ю. Фрундін, Я.Я. Лебедєв, В.Є. Колесник Методичні вказівки з виконання розрахункової частини розділу „Охорона праці"в дипломних проектах студентів інституту електроенергетики. Частина 1 – Дн.: Редакційно-видавничий комплекс, 2004 - 37 стр.

ДОДАТОК А

Текст програми налаштування мережі комп’ютерної системи

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.23012-01 12 01

Листів 9

Дніпро

2023

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду програмування та налаштування компонентів мережі комп’ютерної системи.

Програма призначена для забезпечення налаштування, протоколу маршрутизації NAT комп’ютерної системи.

ЗМІСТ

1. Скрипт налаштування ISP

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX15249K7P-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.0.2.22 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 209.165.201.5 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.2.26 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
end
```

2. Скрипт налаштування Router0

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX15247C04-
spanning-tree mode pvst
```

```
interface GigabitEthernet0/0
 ip address 10.23.128.1 255.255.255.128
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.2.25 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
end
```

3. Скрипт налаштування Router1

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
no ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX15243EP6-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.23.129.1 255.255.255.192
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.2.5 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.2.9 255.255.255.252
```

```
 duplex auto
 speed auto
interface FastEthernet0/3/0
 switchport mode trunk
interface FastEthernet0/3/1
 switchport mode access
 switchport nonegotiate
interface FastEthernet0/3/2
 switchport mode access
 switchport nonegotiate
interface FastEthernet0/3/3
 switchport mode access
 switchport nonegotiate
interface Vlan1
 no ip address
 shutdown
router rip
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
end
```

4. Скрипт налаштування Router2

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX1524LEP0-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.23.129.65 255.255.255.192
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.2.1 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
```

```
 no ip address
 duplex auto
 speed auto
 shutdown
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
end
```

5. Скрипт налаштування Router3

```
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX1524F08Z-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.23.129.129 255.255.255.240
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.2.21 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.2.17 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
end
```

6. Скрипт налаштування Router4

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX152485D1-
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.0.2.6 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.2.18 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.2.13 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
end
```

7. Скрипт налаштування Router6

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname Router
ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX15242XGF-
```

```
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.0.2.2 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/1
 ip address 10.0.2.10 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/2
 ip address 10.0.2.14 255.255.255.252
 duplex auto
 speed auto
interface Vlan1
 no ip address
 shutdown
ip classless
ip flow-export version 9
line con 0
line aux 0
line vty 0 4
 login
end
```