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 ступеню бакалавра

студента Сенипостол Ілля Васильович
(П.І.Б.)
академічної групи 123-17ск-1
(шифр)
Спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)
на тему Комп'ютерна система обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі
(назва за наказом ректора)

Керівник	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинг.	інституційною	
кваліфікаційної роботи	ас. Бешта Д.О.			
розділів:				
апаратний розділ	доц. Ткаченко С.М.			
розрахунок мережі	ас. Панферова Я.В.			
економічний розділ	ст. викл. Яремчук І.О.			
охорона праці	доц. Яворська О.О.			
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних систем
та технологій
(повна назва)
_____ Гнатушенко
В.В.
(підпис) (прізвище, ініціали)

«_____»_____2020 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студенту Сенипостол І.В. **академічної групи** 123-17ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

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

на тему Комп'ютерна система обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі

затверджену наказом ректора НТУ «Дніпровська політехніка» від № -с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати завдання, конкретизувати предмет та мету роботи.	18.05.2020
Технічні вимоги до комп'ютерної системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи.	25.05.2020
Спеціальна частина	Розв'язати завдання з розробки комп'ютерної системи з опрацюванням побудови і захисту інформації та налаштуванням корпоративної мережі	01.06.2020
Економічна частина	Економічно обґрунтувати доцільність витрат на створення та дослідження системи	08.06.2020
Охорона праці	Розробити організаційно-технічні заходи, щодо реалізації правил безпеки при експлуатації системи	15.06.2020

Завдання видано _____ ас. Бешта Д.О.
(підпис п. керівника) (прізвище, ініціали)

Дата видачі 27.01.2020

Дата подання до екзаменаційної комісії 18.05.2020

Прийнято до виконання _____ Сенипостол І.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: _____ с., _____ рис., _____ табл., _____ додатки, _____ джерел.

Об’єкт розробки: Комп'ютерна система обліку електричної енергії для коксохімічного підприємства з дета-льним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета: створення Комп’ютерної системи обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

У роботі викладені результати обстеження об’єкту інформаційної діяльності коксохімічного підприємства, розроблена модель загроз витоку конфіденційної інформації.

Розроблена комп’ютерної системи з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову системи контролю роботи коксохімічного підприємства, а також для збору і підготовки статистичної інформації.

В спеціальній частині розроблені вимоги до кожної складової комплексу технічного захисту інформації, обґрунтований вибір технічних засобів та інженерних заходів. Розробка комп’ютерної мережі виконана відповідно до завдання на кваліфікаційну роботу бакалавра. Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці або додатках.

Практична значимість полягає в тому, що впровадження комплексу технічного захисту інформації підвищить рівень захисту конфіденційної інформації, що циркулює на об’єкті інформаційної діяльності коксохімічного підприємства, від витоку технічними каналами.

СИСТЕМА, КОМП’ЮТЕР, КОНТРОЛЬ, МЕРЕЖА, НАЛАШТУВАННЯ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АРМ − автоматизоване робоче місце;

АРМО − АРМ оператора;

АРМД − АРМ диспетчера;

АСУ − автоматизована система управління;

ПО − програмне забезпечення;

КС - комп’ютерна система;

ТЗ − технічне завдання;

ЕОМ − електронно-обчислювальна машина.

ВСТУП

Металургія України це сукупність підприємств та організацій гірничо-металургійного комплексу, який об’єднує підприємства чорної та кольорової металургії, а також гірничо-збагачувальні комбінати, феросплавні заводи, збагачувальні фабрики, коксохімічні заводи та підприємства, що випускають вироби з металів.

Одна з базових галузей економіки України, основними галузями металургійної промисловості є чорна металургія України та кольорова металургія України.

Коксохімічна промисловість це галузь чорної металургії, що займається переробкою кам'яного вугілля методом коксування.

Основна продукція коксохімічної промисловості:

кам'яновугільний кокс, коксовий газ, хімічні продукти (бензол, толуол, етилен, різні смоли, масла).

Кам’яновугільний кокс використовується в металургії як паливо в доменних та ливарних виробництвах. Коксовий газ та інші продукти коксування служать сировиною для хімічних виробництв. На їх основі випускають різні полімери, азотні добрива, синтетичні миючі засоби, пестициди, лікарські препарати та багато іншого.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика підприємства та умов застосування КС

Історія Дніпровського КХЗ – одного з перших підприємств вітчизняної коксохімії – почалася в 1931 р., з моменту видачі першого коксу. Вже до 1940 р. завод досягнув проектної потужності й став одним з найкращих серед коксохімічних підприємств країни. Підприємство виробляло якісний і найдешевший кокс в Україні, що неодноразово було відмічене винагородами уряду. У 1950 р. ДКХЗ виробляв десяту частину коксу, що виробляється в Україні. У 1996 р. Дніпродзержинський коксохімічний завод імені С. Орджонікідзе був перетворений у ВАТ «Дніпродзержинський КХЗ». ЄВРАЗ придбав 93,83% акцій ОАО «Дніпродзержинський КХЗ» наприкінці 2007 р. Станом на 30 квітня 2011 р., доля ЄВРАЗа в ДКХЗ склала 93,86%.

Історія одного з перших підприємств вітчизняної коксохімії розпочалася в серпні 1927 р. Не було урочистого мітингу, ніхто не виголошував промов, коли безіменний робітник викопав першу лопату ґрунту на місці майбутнього коксохімічного заводу на березі Дніпра в Кам'янському. Спочатку коксохім планувався як окремий цех Дніпровського металургійного заводу – легендарної Дзержинки. І лише потім він виділився в самостійне підприємство – Дніпродзержинський коксохімічний завод №24. На будівництві заводу вперше в країні був застосований спосіб глибинного водовідливу для пониження рівня ґрунтових вод на місці спорудження котлованів. Осушене в такий спосіб дно котловану покрили дорогою тришаровою ізоляцією зі свинцевих листів, зварених автогеном. І тільки потім на цю свинцеву підстилку був укладений гранітобетон. Інженерні вирішення об'єктів по будівництву коксохімічного заводу були дуже складними для того часу, тому багато потужностей заводу зводилися під керівництвом інженерів з Бельгії, Франції, Німеччини. На досвіді будівництва перших коксохімічних підприємств вчилися вітчизняні будівельники і проектувальники. Надалі коксохімічні заводи на території колишнього СРСР зводилися вже за вітчизняними проектами. Над

Дніпром виросли значних розмірів споруди – вугільна вежа, вуглемийка, коксові батареї.

27 листопада 1930 р. відбувся мітинг, учасники якого з підйомом зустріли пропозицію передовика Г.Карпова присвоїти коксохімічному заводу ім'я Серго Орджонікідзе. 8 лютого 1931 року був виданий перший кокс. Дата ця увійшла до історії вітчизняної коксохімії як День народження і перший робочий день Дніпродзержинського коксохімічного заводу. Вуглезбагачувальна фабрика, дві коксові батареї №1 і №2 системи "Дістікок" по 40 камер в кожній, проектною потужністю 415 тис. тонн металургійного коксу в рік, цехи уловлювання і переробки смоли були введені в експлуатацію 18 березня 1931 року в числі об'єктів, що входять в першу чергу заводу. Друга черга заводу – три коксові батареї по 45 камер в кожній, цехи уловлювання і ректифікації – вводилися в експлуатацію протягом 1932–1933 років. Причому, починаючи з другої батареї, будівництво і пуск основних агрегатів здійснювалися під керівництвом вітчизняних інженерно-технічних працівників, без участі іноземних фахівців. Вже до 1940 року завод досяг проектної потужності і став одним з найкращих серед коксохімічних підприємств країни. Підприємство виробляло якісний і найдешевший кокс в республіці, що і було відмічено винагородами уряду. Під час ВВВ в найкоротший строк найважливіші вузли, головним чином електродвигуни, коксові машини, інші апарати і агрегати, були демонтовані і вивезені на майданчик Орсько-халіловського металургійного комбінату, що будується. Прощаючись із заводом, коксохіміки сподівалися, що війна продовжиться недовго і після повернення їм удається швидко налагодити виробництво. Проте війна розпорядилася по-своєму. Ворог повністю зруйнував вуглезбагачувальний цех, висадив у повітря всі п'ять коксових батарей. Значні пошкодження були нанесені парокотельному, хімічним і допоміжним цехам.

З квітня 1946 року, відбудований заново, він тепер мало чим нагадував колишній, то хіба лише своїми зовнішніми контурами. На нім почали освоюватися перші вітчизняні коксові батареї типу ПВР-46, упроваджуватися пне-

вматичне обвалення шихти у вугільних баштах, принципово нові технологічні схеми тощо.

Відновлення всіх цехів заводу було завершене до 1950 року. Підприємство швидко нарощувало технологічну потужність. Десяту частину коксу, який вироблявся в Українській РСР, виробляли дніпродзержинські коксохіміки. Завдяки досягнутим високим виробничим показникам, зразковій трудовій дисципліні, високому технічному і культурному рівню трудового колективу в 1960 році Дніпродзержинський коксохімічний завод імені С. Орджонікідзе один з перших в Україні завоював почесне право називатися колективом Комуністичної праці. За успіхи по збільшенню випуску коксохімічної продукції, в удосконаленні технології і організації виробництва в 1976 році завод нагороджений орденом "Знак Пошани".

Ринок коксохімічної промисловості в Україні характеризується досить високою концентрацією, при цьому спостерігається значна нерівномірність у рівні забезпеченості власним коксом і коксівним вугіллям. Найбільш сильні позиції серед конкурентів мають підприємства Метінвест і Донецьксталь.

Для більшості підприємств коксохімічної галузі характерний досить високий рівень зносу основних фондів. Ураховуючи поточний стан основних засобів українських коксохімів, у середньостроковій перспективі очікується зростання потреби у здійсненні значних капітальних інвестицій для відновлення виробничих потужностей.

Дослідження діяльності коксохімічних підприємств свідчить про високий рівень зносу основних фондів. Так, цей показник склав у 2011 р: Харківський КЗ – 25,22%, Авдіївський КХЗ – 28,03 і Макіївкокс – 31,37%. Найбільш зношеними були основні засоби Донецькккоксу – 81,97% і підприємств групи Evraz – Дніпродзержинського КХЗ – 78,83% і Баглійкоксу – 75,37%.

Модернізація підприємств буде здійснена як за рахунок власних коштів груп компаній, так і за рахунок внутрішніх позик. Ураховуючи поточний стан основних виробників коксу та кон'юнктуру на світових ринках, вихід на зовнішній ринок капіталу для цих підприємств є недостатньо перспективним.

Лише при використанні нових технологій стає можливим істотне скорочення собівартості виробництва, що дозволить українському коксу зберегти конкурентоспроможність як на внутрішньому, так і на зовнішньому ринках. При цьому потрібно пам'ятати, що освоєння нових технологій з виробництва високоякісного коксу – досить витратний процес. У наступні роки варто очікувати підвищення тиску на фінансовий результат підприємств, зважаючи на необхідність освоєння значних капітальних інвестицій.

За результатами 2011 р. підприємства коксохімічної галузі переважно характеризувалися достатньою забезпеченістю оборотним капіталом. Проблеми з ліквідністю в останні роки відчували Макіївкокс і Харківський КЗ. Наявність досить великого оборотного капіталу говорить про можливість здійснення капітальних інвестицій для розширення діяльності.

При цьому частина підприємств останніми роками мала надлишкову ліквідність, що вказує на недостатньо ефективне використання наявних можливостей. Однак найбільші виробники успішно управляють ризиком ліквідності, використовуючи ресурси з досить високою ефективністю.

Частка переробної промисловості у структурі ВВП 2015 р. складає 66,45 %, а коксохімічних підприємств (КХП) – 3,02 %. Рівень інвестицій у промисловість у 2015 р. складав 32,09 %, тоді як у КХП – 0,12 %. Аналіз виробництва коксу за період 2001-2015 р.р. свідчить про нестабільність діяльності цих підприємств (рис.1.1).

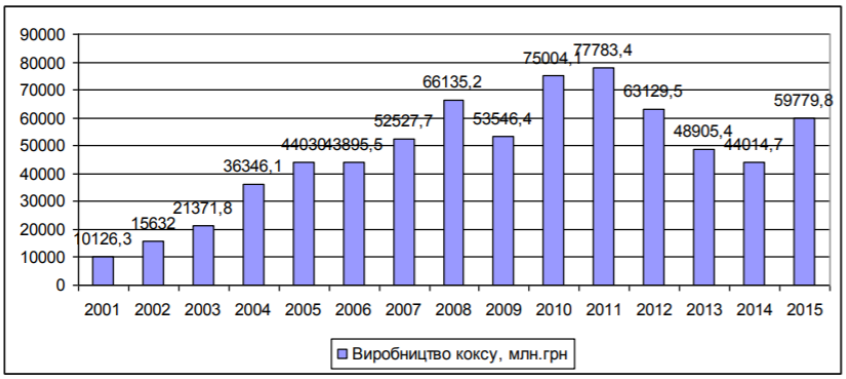


Рисунок 1.1 – Динаміка виробництва коксу у 2001-2015 рр.

1.2 Характеристика підприємства та умов застосування КС

Центральній офіс Приватне акціонерне товариство "Дніпровський коксохімічний завод" розташований за адресом, 51901, Дніпропетровська обл., місто Кам'янське, Південний район, вулиця Колеусівська, будинок 1.

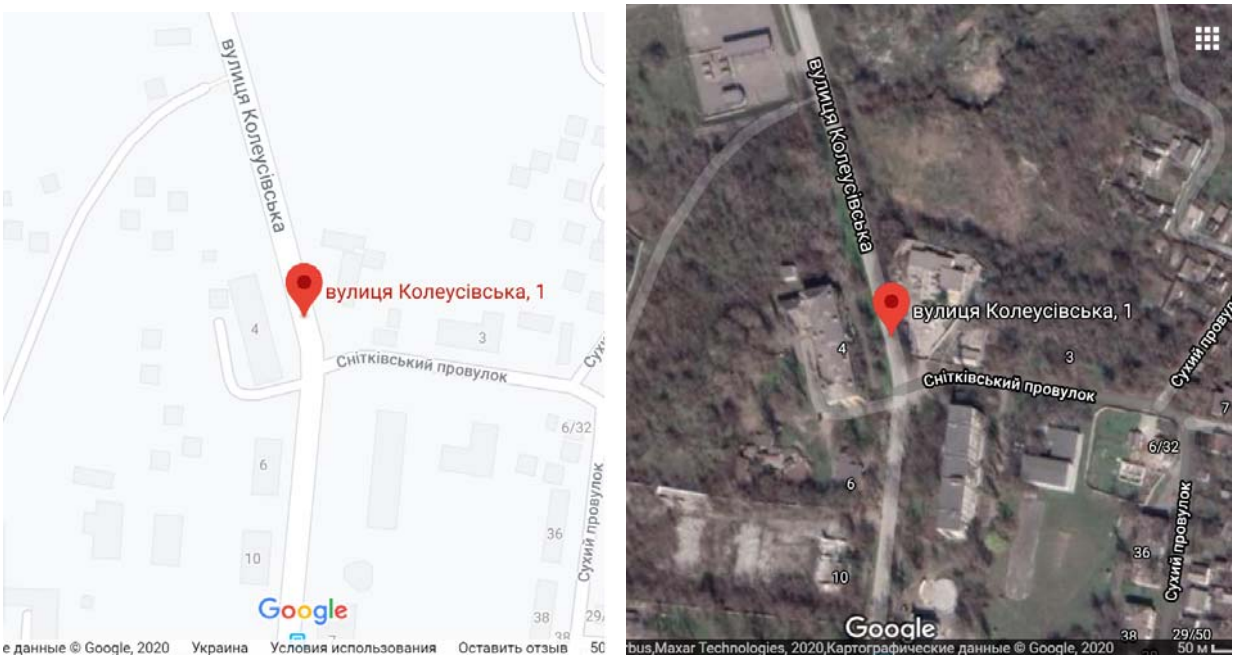


Рисунок 1.2 – Топологія ПАТ «Дніпропетровський коксохімічний завод»

Для створення і забезпечення роботи систем контролю і збору даних треба розглянути організаційну структура представлена на рис. 1.3.

Вищий рівень управління підприємством представлений генеральним директором, який приймає рішення загального стратегічного характеру, впроваджує і дотримується єдиної політики організації праці та інших функцій, зокрема експлуатації, збуту, дотримання норм і правил з охорони праці, підвищення кваліфікації кадрів, дотримання стандартів якості. Генеральний директор є представником підприємства при спілкуванні з усіма зацікавленими особами та організаціями. Він підписує договори, бухгалтерські документи та інші супутні папери.

У підпорядкуванні генерального директора перебувають комерційний директор, виконавчий директор та служба економічної безпеки.

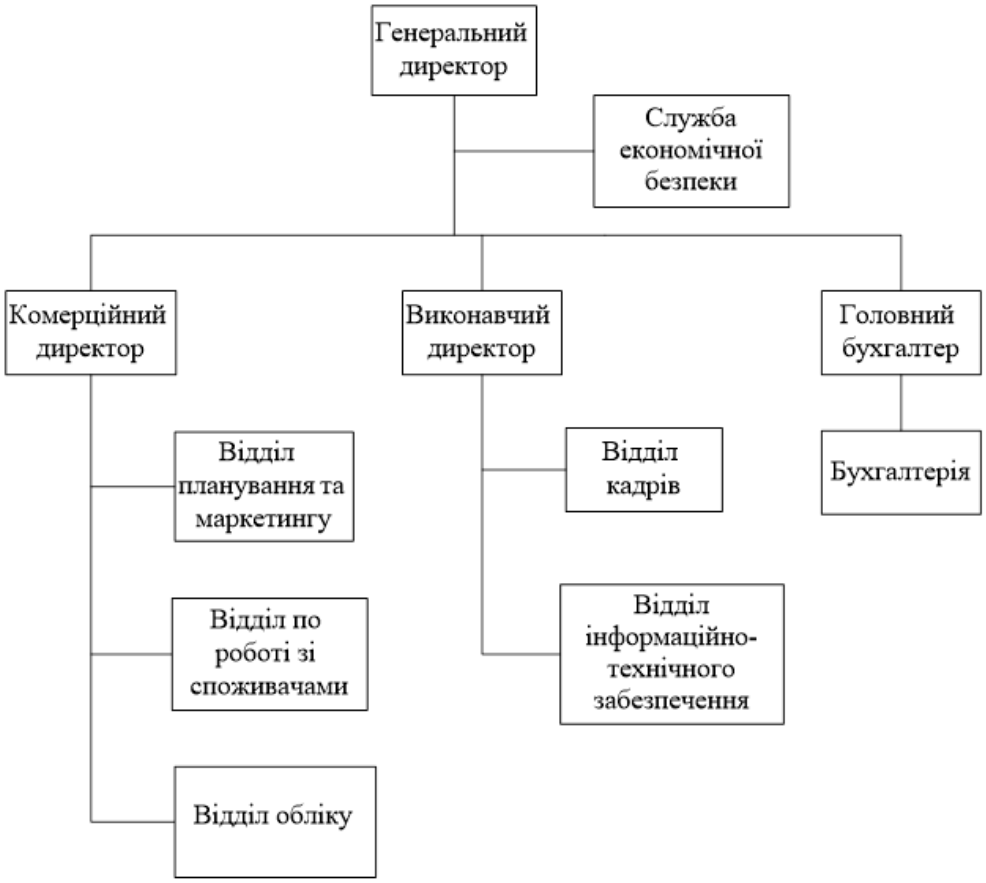


Рисунок 1.3 – Організаційна структура підприємства

Служба економічної безпеки – це підрозділ, основною функцією якого є розробка комплексу організаційно-управлінських, режимних, технічних, профілактично-пропагандистських заходів, спрямованих на захист економічних інтересів підприємства від внутрішніх та зовнішніх загроз. Вона забезпечує захист законних прав та інтересів підприємства та його співробітників, виявлення недобросовісної конкуренції з боку інших підприємств, фізична і технічна охорона майна підприємства, недопущення технічного проникнення на підприємство із злочинною метою, охорона інформації, що є комерційною таємницею підприємства і здобуття необхідної інформації для вироблення керівництвом обґрунтованих рішень, виявлення некредитоспроможних, ненадійних ділових партнерів і збір інформації для проведення ділових переговорів.

Комерційний директор координує розробку маркетингової стратегії та прогнозування споживчого попиту та здійснює керівництво щодо надання

послуг. Організує систему обліку усіх фінансових операцій, підготовку фінансової звітної документації. Керує розробкою заходів для ресурсозбереження, удосконалювання нормування запасів, поліпшення економічних показників, підвищення ефективності діяльності підприємства, зміцнення фінансової дисципліни.

Виконавчий директор займається забезпеченням необхідних ресурсів для підприємства (включаючи матеріали, обладнання, відповідний персонал), координує обслуговування обладнання на підприємстві і може вирішувати питання, що відносяться до виробничих послуг, інформаційних технологій, технічної підтримки, планування чисельності співробітників або планування витрат на персонал.

Головний бухгалтер забезпечує ведення бухгалтерського обліку, дотримуючись єдиних методологічних засад з урахуванням особливостей діяльності підприємства і технології оброблення облікових даних. Організовує роботу бухгалтерської служби, контроль за відображенням на рахунках бухгалтерського обліку всіх господарських операцій. Здійснює контроль за веденням касових операцій, раціональним та ефективним використанням матеріальних, трудових та фінансових ресурсів.

В свою чергу комерційний директор у своєму підпорядкуванні має відділ планування та маркетингу, відділ по роботі зі споживачами та відділ обліку водопостачання. Відділ планування та маркетингу працює над аналізом ринкових ситуацій, вивченням тенденцій розвитку ринку, прогнозуванням обсягів продажу, вивченням попиту, формуванням та реалізацією маркетингової політики, розробкою бюджету маркетингу, плануванням іміджу підприємства. Функціями відділу по роботі зі споживачами є організація, розробка, впровадження та вдосконалення систем і методів проведення розрахунків з побутовими споживачами за використану ними питну воду, постійна організація покращення форм обслуговування споживачів, а також контроль своєчасної оплати споживачами всіх видів нарахувань. Відділ обліку водопостачання займаються складанням звітів за місяць для подальшої бухгалтерсь-

кої обробки, облікової архівної документації, документів для аналізу маркетинговим відділом та обробкою інформації для надання її споживачам, що сплачують за надані послуги.

Виконавчий директор відповідає за роботу відділу кадрів та відділу інформаційно-технологічного забезпечення. Відділ кадрів на підприємстві організовує роботу із забезпечення підприємства працівниками потрібних професій, спеціальностей і кваліфікації згідно з цілями, стратегією та профілем підприємства. Бере участь у розробленні кадрової політики і кадрової стратегії підприємства, вирішує питання найму, звільнення, переведення працівників. Здійснює роботу з добору, відбирання і розставлення кадрів на основі оцінювання їх кваліфікації, особистих і ділових якостей, а також організовує своєчасне оформлення, приймання, переведення і звільнення працівників згідно з трудовим законодавством, положеннями та інструкціями. Відділ інформаційно-технічного забезпечення займається забезпеченням розвитку і впровадження сучасних інформаційних технологій, систем технічного захисту інформації, організацією та виконанням модернізації, обслуговування засобів і систем обчислювальної техніки, організацією роботи локальних мереж, інформаційних систем із забезпеченням розподіленого доступу до інформаційних ресурсів. Він відповідає за здійснення технічної підтримки та забезпечення обслуговування серверного й мережевого обладнання, програмно-апаратних комплексів, забезпечення функціонування офіційного вебсайту та надання доступу до мережі Інтернет.

Головний бухгалтер організовує роботу і керує бухгалтерією. Бухгалтерія підприємства забезпечує ведення обліку матеріально-технічних цінностей, розрахунків з оплати праці (нарахування заробітної плати, утримання із заробітної плати, відрахування на соціальне та медичне страхування, у пенсійний фонд і фонд зайнятості), фінансової діяльності, грошових операцій, а також складання бухгалтерської звітності.

Розглянемо технологічну структуру ПАТ «Дніпропетровський коксохімічний завод» (рис. 1.4).

За організаційною структурою коксохімічні підприємства існують як окремі коксохімічні та коксогазові заводи або як коксохімічні виробництва в складі металургійних заводів та комбінатів. У складі коксохімічних підприємств є основні (технологічні), допоміжні цехи (підрозділи) та заводоуправління.

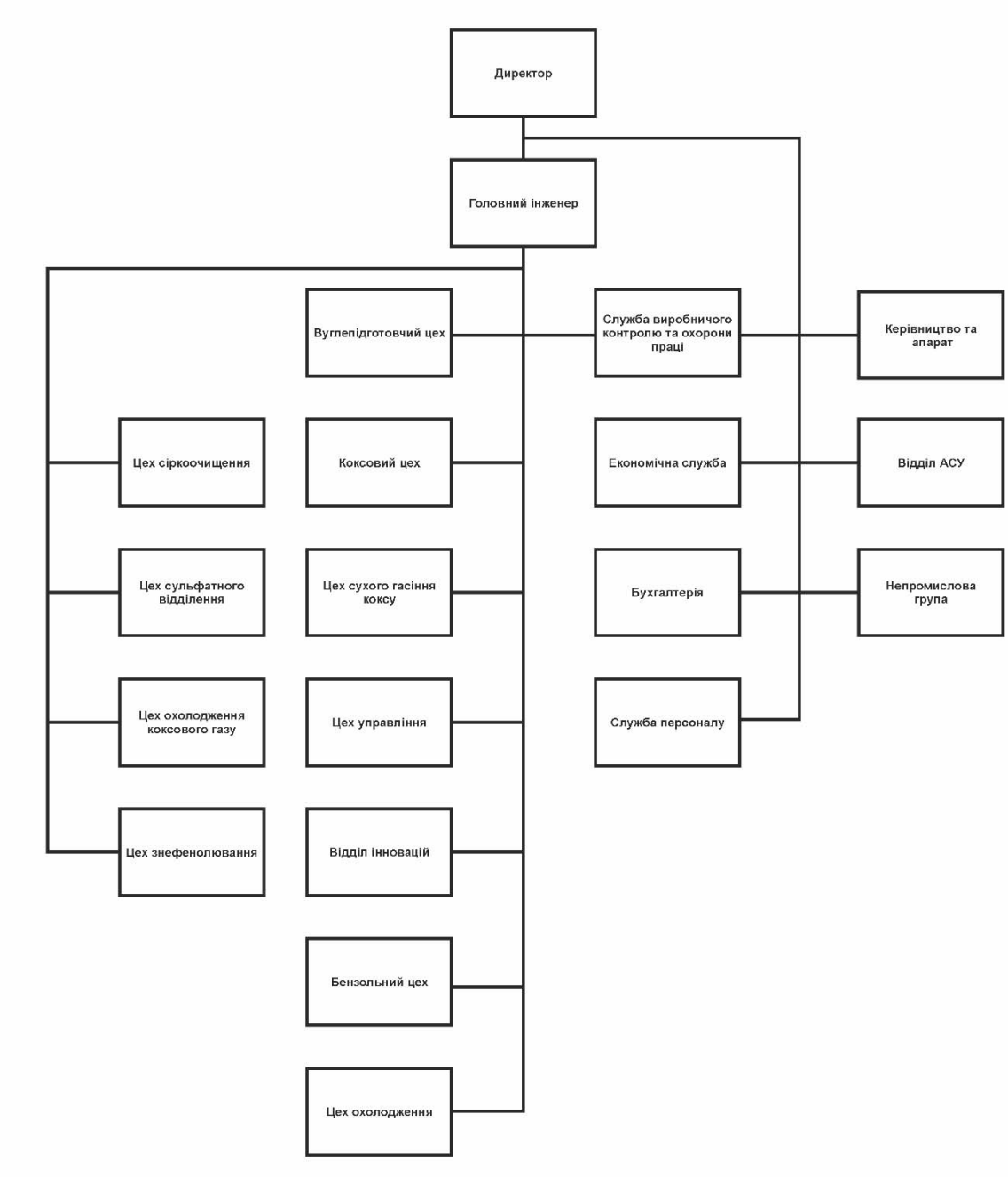


Рисунок 1.3 – Технологічна структура ПАТ «Дніпропетровський коксохімічний завод»

Цех є основним виробничим підрозділом підприємства. Ділянки та відділення можуть існувати як самостійні підрозділи і можуть бути в складі цехів.

Організаційне оформлення процесів і обладнання (в цехах, ділянках і відділеннях) залежить від сировини, технологічної схеми та обсягів виробництва і може змінюватися як щодо об'єднання технологічних і допоміжних підрозділів, так і з розділення однотипних цехів. До основних цехах на більшості коксохімічних підприємств відносяться вуглепідготовчий, вуглезбагачувальний (вуглезбагачувальна), коксовий, уловлювання хімічних продуктів коксування (цех уловлювання) очищення коксового газу від сірководню. (Цех сіркоочищення), переробки сирого бензолу (цех ректифікації), смолопереробний, пекококсовий. На деяких підприємствах є основні цехи по глибокій переробці вугілля і продуктів коксування ФТА-лівого ангідриду, роданистих з'єднань, термоантрацітовий.

До складу деяких вуглепідготовчих цехів входять вуглезбагачувальні фабрики з відділеннями гравітаційного і флотаційного збагачення, зневоднення і дроблення концентратів, освітлення оборотної води, сушіння дрібного і флотаційного концентратів, усереднення концентратів, накопичення і навантаження породи, проміжного продукту і відходів флотації.

Охолоджений кокс надходить на коксосортіровкі, обладнані комплексом агрегатів для класифікації коксу по крупності, відбору проб для аналізів, навантаження в залізничні вагони або транспортування в доменні цехи.

До складу цеху уловлювання хімічних продуктів коксування зазвичай входять такі відділення конденсації, машинне, сульфатне, аміачне і бензольное. До складу відділення конденсації входять освітлювачі для відділення води і механічних домішок (фусов) від смоли, первинні газові холодильники для охолодження прямого коксового газу і виділення з нього смоли і води, електрофільтри для тонкої очистки газу від смоляного туману.

У машинному відділенні розташовуються газодувки-нагнітачі, що відсмоктують прямий коксовий газ з газосборніков коксових печей і здійсню-

ють подальше транспортування його через уловлює апаратуру і далі споживачам.

У сульфатному відділенні уловлюються аміак і піридіновиє підстави. У аміачних відділенні можна отримувати концентровану аміачну воду або безводний аміак або витягувати з надсмольної води аміак, що направляється на піридинове установку або в газопровід перед установкою, вирабативаюшей сульфат амонію.

На обесфенолівающій установці з надсмольної води витягуються феноли і у вигляді фенoляту натрію відправляються на централізовану переробку В бензольному відділенні з прямого коксового газу поглинальним маслом уловлюються бензольні вуглеводні (сирої бензол). Газ після виділення з поглинального масла направляється на подальшу переробку. У цьому відділенні проводиться також регенерація поглинального масла. Утилізаційна установка служить для переробки смолистих речовин, які утворюються в різних цехах - (кислої смолки сульфатного відділення і цеху ректифікації, фусов і ін.). З цих відходів на установці виходить водяна емульсія, яка повинна рівномірно подаватися на вугільну шихту.

У складі деяких коксохімічних заводів, що переробляють донецькі вугілля, є хімічні установки з вилучення рідкоземельних елементів з продуктів коксування.

Цехи з очищення аза від сірчистої сполуки є на заводах для переробки вугілля з високим вмістом сірки. При уловлюванні сірчистої сполуки отримують плавлення або колоїдну елементарну сірку або сірчану кислоту. Під час вилучення сірководню з коксового газу миш'яково-содовим способом утворюються баластні солі, що містять гипосульфит і роданистий натрій, які на деяких заводах виділяють як товарні продукти. На деяких заводах з газу окремо вловлюють ціаністий водень, який потім переробляється в роданистий натрій. На великих коксохімічних заводах є цехи переробки хімічних продуктів.

Цех ректіфікашш сирого бензолу служить для переробки надходить до цеху уловлювання або привезеного з інших коксохімічних виробництв сирого бензолу. Основними товарними продуктами є чисті бензол і його гомологи толуол, ксилоли. На деяких коксохімічних виробництвах і заводах виробляються инденкумаронові смоли, дициклопентадієн, чисті піридин, лутідін, коллідіни і інші продукти. У цеху є відділення дистиляції сирого бензолу, в складі деяких цехів відділення ректифікації легких піридинових підстав, кислотною мийки або гідроочищення, регенерації сірчаної кислоти.

1.3 Огляд існуючих інженерних рішень КС в галузі

Сучасне коксохімічне підприємство це великомасштабне комплексне виробництво, в якому утилізуються і переробляються всі компоненти Коксівність сировини. Існує два типи коксохімічних підприємств: заводи з повним циклом коксохімічного виробництва, що розміщуються окремо від металургійних підприємств та коксохімічні цехи (виробництва), що входять до складу металургійних комбінатів, і розміщуються на одному майданчику з ними.

Металургійний кокс становить найважливіший компонент сировини в доменному процесі і транспортування його економічно невигідна. Крім того, коксохімічні заводи часто кооперують з виробництвами аміаку і азотної кислоти, основного органічного синтезу, барвників, вибухових речовин і ракетних топ лив, пластичних мас, в яких в якості сировини використовуються продукти коксохімії.

Відповідно до призначення всі цехи коксохімічного заводу поділяються на основні та допоміжні. До основних виробничих цехів відносяться:

1) вуглепідготовчий цех, де здійснюється прийом, зберігання і підготовка вугілля до коксування. Готова продукція цеху - вугільна шихта.

2) Коксовий цех, в якому відбувається основний процес – переробка вугільної шихти з одержанням цільового продукту коксу і летючих хімічних продуктів – прямого коксового газу – коксування.

3) Цех уловлювання, в якому відбувається охолодження прямого коксового газу і виділення з нього хімічних продуктів: сирого бензолу, кам'яновугільної смоли і з'єднань аміаку.

4) Переробні цехи, в яких хімічні продукти, що надходять з цеху уловлювання, піддаються подальшій переробці. Готовою продукцією цих цехів є індивідуальні ароматичні вуглеводні, нафталін, фталевий ангідрид, феноли і пірідіновиє підстави, пек, пековий кокс і інші.

До допоміжних цехів відносяться: залізничний, ремонтний, енергетичний, господарський, ВТК, ЦЗЛ і інші. Технологічна схема виробництва ЗАТ «Дніпропетровский коксохімічний завод» наведена на рис. 1.5.

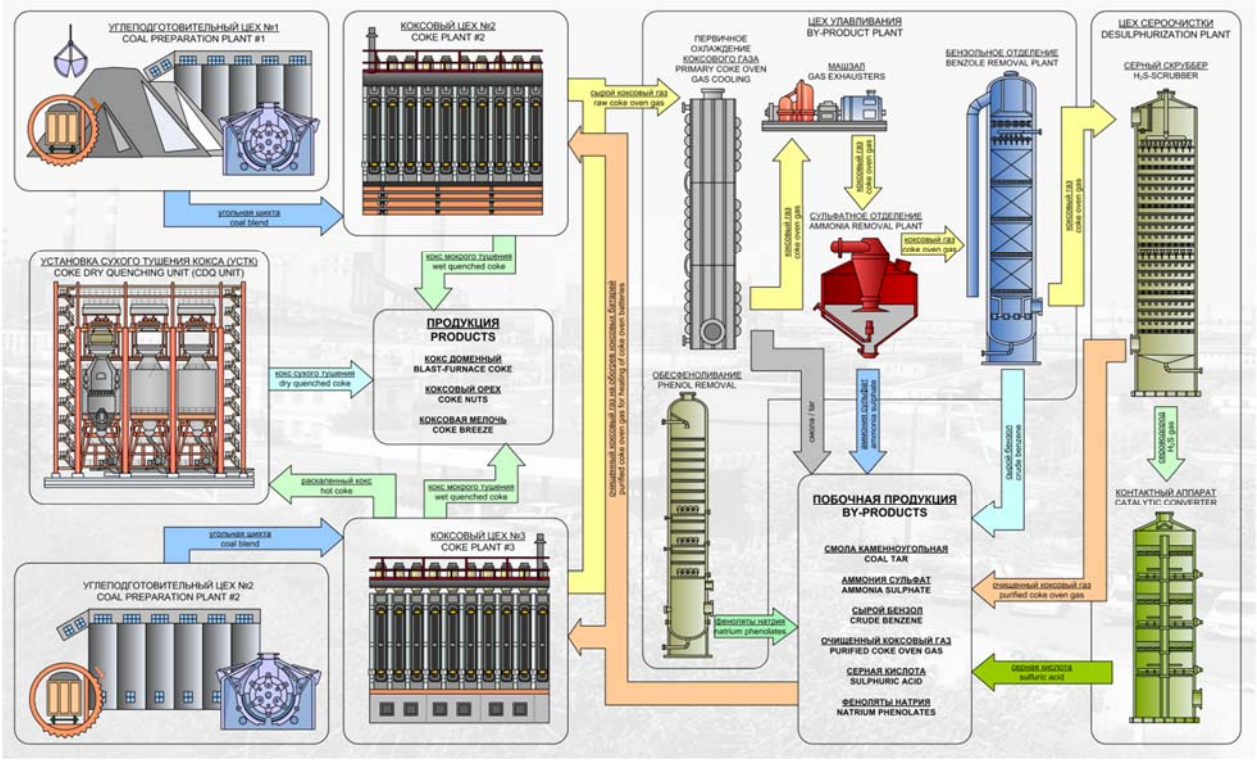


Рисунок 1.5 – Технологічна схема виробництва ЗАТ «Дніпропетровский коксохімічний завод»

Розрахунки за споживану електроенергію є однією з основоположних позицій договірних взаємовідносин між споживачем та енергопостачальною організацією, що враховують інтереси обох сторін.

Вимоги до розрахункових приладів обліку електроенергії є багатогранними та включають в себе достовірність і точність визначення витрати елек-

троенергії з урахуванням її втрат в електричних мережах, відкритості та доступності результатів вимірювань на всіх етапах виробництва, передачі, розподілу та споживання електроенергії.

Правила обліку електричної енергії визначають загальні вимоги до організації її обліку та взаємозв'язок між основними нормативно-технічними документами, чинними в цій галузі.

Допускається на підставі діючих правових і нормативно-технічних документів відомствами розробляти і затверджувати в установленому порядку в межах своєї компетенції відомчі нормативно-технічні документи в галузі обліку електроенергії, що не суперечать затверджених Правил обліку електричної енергії. Якщо ці документи містять вимоги міжвідомчого характеру.

Правила обліку електричної енергії є обов’язковими при: здійсненні виробництва, передачі, розподілу та споживання електричної енергії; виконанні проектних, монтажних, налагоджувальних та ремонтних робіт по організації обліку електричної енергії; забезпеченні експлуатації засобів обліку електричної енергії.

Основною метою обліку електроенергії є отримання достовірної інформації про її виробництві, передачу, розподіл та споживанні на оптовому і роздрібному ринках для вирішення наступних основних техніко-економічних завдань: фінансових розрахунків за електроенергію і потужність між енергопостачальними організаціями та споживачами електроенергії з урахуванням її якості; визначення та прогнозування техніко-економічних показників виробництва, передачі і розподілу електроенергії в енергетичних системах; визначення та прогнозування техніко-економічних показників споживання електроенергії на підприємствах промисловості, транспорту, сільського господарства, комунально-побутовим сектором; забезпечення енергозбереження та управління електроспоживанням.

Облік активної електроенергії повинен забезпечувати визначення кількості електроенергії (і в необхідних випадках середніх значень потужності): виробленої генераторами електростанцій; спожитої на виробничі потреби

енергосистеми; відпущеної споживачам по лініях, що відходять від шин електростанцій безпосередньо до споживачів; переданої в мережі інших власників або отриманої від них; відпущеної споживачам з електричної мережі; переданої на експорт і отриманої з імпорту.

Організація обліку активної електроенергії повинна забезпечувати можливість: визначення надходження електроенергії в електричні мережі різних класів напруги енергосистем; складання балансів електроенергії для госпрозрахункових підрозділів енергосистем і споживачів; контролю за дотриманням споживачами заданих їм режимів споживання і балансів.

1.4 Визначення можливих напрямків рішення поставлених завдань

Робота внутрішніх алгоритмів трифазних або однофазних конструкцій відбувається за одним і тим же законам, за винятком того, що в 3-х фазному, більш складному пристрої, йде геометричне підсумовування величин кожного з трьох складових каналів.

Повна величина потужності визначається складовими: активної та реактивної (суми індуктивної та ємнісної навантажень). Струм, що протікає по загальному ланцюжку однофазної мережі, однаковий на всіх ділянках, а падіння напруги на кожному її елементі залежить від виду опору і його величини. На активному опорі воно збігається з вектором струму, а на реактивному відхиляється в сторону. Причому на індуктивності воно випереджає струм за кутом, а на ємності відстає.

Електронні лічильники здатні враховувати і відображати повну потужність і її активну і реактивну величину. Для цього проводяться виміри векторів струму з напругою, підведених на його вхід. За значенням відхилення кута між цими вхідними величинами визначається і розраховується характер навантаження, надається інформація про всі її складових.

У різних конструкціях електронних лічильників набір функцій неоднаковий і може значно відрізнятися своїм призначенням. Цим вони кардинально відрізняються від своїх індукційних аналогів, які працюють на основі вза-

ємодії електромагнітних полів і сил індукції, що викликають обертання тонкого алюмінієвого диска. Конструктивно вони здатні заміряти тільки активну або реактивну потужність в однофазної або трифазної ланцюга, а значення повної - доводиться обчислювати окремо вручну.

Автоматизована система управління технологічним процесом представляє собою ієрархічну структуру, що включає в себе рівень операторського управління, рівень автоматичного управління та польовий рівень.

На польовому рівні знаходяться пристрої, що встановлюються безпосередньо на технологічних об’єктах та поблизу від них: датчики, виконавчі пристрої, спеціалізовані контролери, сервоперетворювачі, системи віддаленого вводу-виводу, частотні перетворювачі. Основними завданнями, які розв’язуються на даному рівні, є: вимірювання технологічних параметрів процесу та вироблення керуючих впливів.

На рівні автоматичного управління знаходяться пристрої управління та сигналізації, які розміщуються в шафах управління: програмовані логічні контролери, системи віддаленого вводу-виводу, пульти управління. Пульти управління можуть бути реалізовані за допомогою кнопок, перемикачів та світлосигнальної арматури; панелей операторів; комп’ютерів або терміналів зі спеціалізованим програмним забезпеченням, що реалізує людино-машинний інтерфейс. Основними завданнями, які розв’язуються на даному рівні, є: обробка даних, що надходять з польового рівня, формування значень керуючих впливів та передача їх на польовий рівень, сигналізація про вихід значень параметрів технологічного процесу за задані межі, блокування помилкових дій персоналу та управляючих пристроїв, реалізація протиаварійного захисту при виникненні нештатних ситуацій.

На рівні операторського управління знаходяться пристрої збору та зберігання інформації та пристрої візуалізації технологічних процесів: сервера SCADA систем, сервера баз даних, автоматизовані робочі місця. Основними завданнями, які розв’язуються на даному рівні, є: збір інформації, що надходить з рівня автоматичного управління, її обробка, зберігання та архівування,

формування звітів, передача інформації EMS системі, обчислення параметрів які не можуть бути вимірювані, діагностика та захист від збоїв, налаштування управляючих пристроїв.

SCADA (Supervisory Control And Data Acquision System – Диспетчерське управління та збір даних) система являє собою програмне забезпечення призначене для забезпечення роботи в реальному часі систем збору, обробки, відображення та архівування інформації про об’єкт контролю або процеси управління. Сервера SCADA системи вирішують завдання збору, резервування, архівування та надання інформації, а автоматизовані робочі місця операторів вирішують завдання візуалізації технологічного процесу за допомогою HMI (Human Machine Interface - Людино-машинного інтерфейсу), формування сигналів тривоги, запису інформації про нештатні ситуації, формування звітів, організації управління рецептами.

Як видно зі структури автоматизованої системи управління технологічним процесом програмовані логічні контролери знаходяться на рівні автоматичного управління. Вони отримують дані від датчиків, систем віддаленого вводу-виводу та спеціалізованих контролерів, на підставі отриманої інформації відповідно до алгоритму управління формуються значення керуючих впливів які передаються виконавчим пристроям, як безпосередньо, так і за допомогою спеціалізованих контролерів, систем віддаленого вводу-виводу, перетворювачів. Для контролю окремих ділянок технологічного процесу та зміни режимів роботи локальних систем управління використовуються пульти оператора, а для контролю за технологічним процесом та зміни налаштувань управляючих пристроїв використовуються автоматизовані робочі місця.

Таким чином сучасна система управління базується на використанні у якості пристроїв управління програмованих логічних контролерів. Які отримують інформацію від датчиків формують за заданим алгоритмам сигнали управління які за допомогою виконавчих пристроїв формують керуючі впливи. Зміна параметрів системи управління та візуалізація процесу виконується за допомогою SCADA систем які встановлюються на серверах та автомати-

зованих робочих місцях операторів. SCADA системи виконують збір, обробку візуалізацію та зберігання інформації отриманої від програмованих логічних контролерів та операторських пультів.

Розглянемо принцип побудови системи обліку. Збір первинної інформації та її обробка здійснюється на підстанціях виробництва – ДПП; ПС-1, РУ-0,4 кВ; ПС-1, РУ-6 кВ; ПС-2, ПС-6; ПС-7; ТП-9; ТП-17. Збір вторинної інформації: на всіх облікових фідерах для обліку споживання активної електроенергії встановлених існуючі лічильники електроенергії: СТК3; СТ-ЕА08; НІК 2301 з імпульсним виходом; на кожній з підстанцій (ДПП, ПС-1, РУ-0,4 кВ; ПС-1, РУ-6 кВ; ПС-2, ПС-6; ПС-7; ТП-9; ТП-17) встановлюється тарифікатор облік-Т20 на 20 імпульсних входів; імпульсні вихідні ланцюга лічильників електроенергії підключаються до входів тарифікатора типу Облік-Т20; в тарифікатор Облік-Т20 підсумовуються імпульси множаться на запрограмовані коефіцієнти, і отримуються результати в кВт/год по змінах, що відображається на дисплеях тарифікатора окремо.

Вся зареєстрована інформація зберігається в пам'яті тарифікатора (поденна протягом 3-х діб, місячна протягом 3-х місяців).

З кожного тарифікатора інформація може бути виведена: або на індикатор, встановлений на лицьовій панелі, що забезпечує можливість візуального зчитування показань, або по інтерфейсу RS485 на комп'ютер. передача інформації з тарифікатора Облік-Т20 на сервер обліку АСТУЕ відбувається по виділеній провідної лінії зв’язку з використанням інтерфейсу RS-485 за викликом оператора АСТУЕ через ПЕОМ. Вся отримана інформація обробляється і архівується в ПЕОМ.

На підстанції вся інформація про врахованої електроенергії зберігається в енергонезалежній пам'яті приладів Облік-Т20.

На сервері АСТУЕ створюється база даних, що дозволяє видавати звіти про споживання електроенергії та складати добові графіки електроспоживання за поточні і за минулі періоди обліку.

1.5 Висновок за розділом

В розділі стан питання і постановка задачі було проведене обстеження інформаційної діяльності коксохімічного підприємства, за результатами обстеження була розроблена стратегія розробки комп'ютерної системи обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі,. Опираючись на отримані результати була поставлена задача на проектування комплексу технічного захисту інформації.

Виходячи з існуючих підходів та вимог система повинна вирішувати наступні завдання:

- вимірювання активної потужності;
- вимірювання реактивної потужності;
- реєстрацію отриманої інформації;
- передачу інформації до серверу;
- візуалізацію отриманої інформації.

Мета роботи розробка комп'ютерної системи обліку електричної енергії ЧАО «Дніпровський коксохімічний завод» з опрацюванням побудови та налаштування комп'ютерної мережі.

2 ТЕХНІЧНІ ВИМОГИ ДО КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Вимоги до системи в цілому

Комп'ютерна система повинна включати обладнання необхідне для підключення до загальнопромислової мережі, пристрій управління, датчики, програмне забезпечення яке реалізує алгоритм управління, персональний комп'ютер з SCADA системою, сервер баз даних. Система повинна дозволяти здійснювати повний контроль технологічного процесу, відображення процесу його ходу та відповідних параметрів. Система повинна включати наступні підсистеми: передачі інформації, відображення, вводу та доступу до інформації, аналізу інформації, управління, збору інформації, аварійного захисту та інтеграції з АСУТП.

Функціонування системи має відповідати наступним критеріям: забезпечувати безперебійне функціонування системи; забезпечення мінімального часу на обслуговування; забезпечувати можливість роботи в різних режимах.

2.1.1 Вимоги до структури і функціонуванню системи

До складу комплексу ТЗІ повинні входити наступні інженерно-технічні засоби і заходи:

- організація виділеного приміщення для ведення переговорів і нарад, на яких озвучується інформація з обмеженим доступом;
- розробка системи контролю і управління доступом;
- розробка інженерно-технічних заходів для захисту інформації від витоку технічними каналами зазначених у моделі загроз;
- розробка захищеного приміщення серверної.

2.1.2 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему і режиму його роботи

Підготовка операторів, інженерів та фахівців з програмного забезпечення для систем контролю здійснюється на спеціалізованих курсах відпові-

дних фірм виробників продукції яке використовується при створенні системи, а також в політехнічних університетах.

До самостійної роботи допускаються тільки оператори, попередньо навчені, пройшли інструктаж і які засвоїли безпечні прийоми роботи.

Для забезпечення роботи системи потрібно 4 оператора, 2 інженера-системотехніка з налагодження та обслуговування обладнання.

Режим роботи персоналу – змінний.

2.1.3 Показники призначення

Підготовка операторів технологічного процесу, інженерів та фахівців з програмного забезпечення для систем контролю здійснюється на спеціалізованих курсах відповідних фірм виробників продукції яке використовується при створенні АСУ ТП, а також в політехнічних університетах.

До самостійної роботи допускаються тільки оператори, попередньо навчені, пройшли інструктаж і які засвоїли безпечні прийоми роботи.

Для забезпечення роботи системи потрібно 4 оператора, 2 інженера-системотехніка з налагодження та обслуговування обладнання.

Режим роботи персоналу – змінний.

Створюваний комплекс ТЗІ має відповідати вимогам чинного законодавства України і діючим нормативно-правовим актам, тому при створенні комплексу ТЗІ слід використовувати наступні документи:

- Закон України «Про інформацію»;
- Указ про положення про технічний захист інформації в Україні;
- ДСТУ 3396.2-97 «Захист інформації. Технічний захист інформації. Терміни та визначення»;
- НД ТЗІ 1.1-005-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення»;
- ТР ЕОТ - 95 «Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих систе-

мах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок»;

– НД ТЗІ 3.1-001-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи».

Витрати на створюваний комплекс ТЗІ не повинні перевищувати можливих збитків зазнаних від витоку інформації з обмеженим доступом.

Створюваний комплекс ТЗІ має відповідати наступним умовам:

– встановлення інженерних конструкцій і технічних засобів не повинно потребувати значних змін в конструкції будівлі;
– комплекс ТЗІ не повинен заважати технологічному процесу і ведення господарства, а також створювати
– незручності під час роботи працівників;
– монтаж конструкції має бути розрахований на можливе подальше удосконалення і модернізації, а також враховувати легкий демонтаж конструкцій і технічних засобів під час ремонту.

Основними критеріями при проектуванні комп’ютерної системи виробництва є критерії якості доступу до продуктивність, надійність, розширюваності та дотримання технологічних параметрів із заданою точністю.

Система повинна повністю забезпечувати режими роботи ручний та автоматичний. У разі зміни конфігурації обладнання система повинна мати можливість простого налаштування на нові умови роботи.

Під час першого налаштування обладнання повинна бути забезпечена можливість ручного режиму роботи. У тому випадку, якщо система починає працювати в штатному режим повинна бути реалізована можливість перемикання на автоматичний режим.

2.1.4 Вимоги до надійності

При аварійних ситуаціях - вихід з ладу окремого робочого місця не повинно приводити до втрати інформації. Перебої з електропостачанням на повинні впливати на працездатність обладнання. Необхідні резервні джерела енергії такої потужності, щоб забезпечити можливість впродовж 10 хвилин завершити роботу і зберегти дані.

Для технічних пристроїв використовуються такі показники надійності, як середній час наробітки на відмову, імовірність відмови, інтенсивність відмов.

Необхідно забезпечити збереження даних і захист їх від спотворень. Крім цього, повинна підтримуватися узгодженість (несуперечність) даних, наприклад, якщо для підвищення надійності на декількох файлових серверах зберігається декілька списків даних, то треба постійно забезпечувати їх ідентичність.

Надійність програмного забезпечення повинна забезпечуватися за рахунок використання ліцензійних програмних продуктів.

На етапі повного функціонування комп'ютерної системи підприємства, її обслуговування повинно забезпечуватися системним адміністратором. Ремонт системи має виконуватися спеціалістами підрядниками. Елементи системи, що вийшли з ладу повинні замінюватися новими.

2.1.5 Вимоги до захисту інформації від несанкціонованого доступу

Для захисту програмного забезпечення системи від несанкціонованого доступу забороняється допуск до налаштувань та обслуговування людей, які не мають на те відповідного дозволу керівництва.

Повинна бути забезпечена програмний та апаратний захист від некваліфікованих дій користувача та від спроб несанкціонованого доступу користувачів до внутрішньо системної інформації. Залежно від статусу користувача повинні бути передбачені різні рівні доступу до внутрішньо системної інформації.

Для захисту програмного забезпечення системи від несанкціонованого доступу забороняється допуск до налаштувань та обслуговування людей, які не мають на те відповідного дозволу керівництва.

Повинна бути забезпечена програмний та апаратний захист від некваліфікованих дій користувача та від спроб несанкціонованого доступу користувачів до внутрішньо системної інформації. Залежно від статусу користувача повинні бути передбачені різні рівні доступу до внутрішньо системної інформації.

Захисту підлягає інформація з обмеженим доступом. Вибір запропонованих приладів повинен бути доцільним та відповідати вимогам до захисту інформації з обмеженим доступом.

До відкритої інформації, що циркулює, належить:

- статутні документи підприємства;
- інформація про замовлення;
- прайси на продукцію підприємства;
- договори про надання клієнтам послуг;
- інформація про штат співробітників підприємства, наявність вільних місць;
- інформація про місце розташування офісу.

До конфіденційної інформації, що циркулює в мережі належить:

- організаційно-розпорядча інформація;
- внутрішні документи (накази, службові записки і т. д.);
- персональні дані про співробітників;
- інформація про паролі системи;
- трудові договори співробітників;
- інформація з сервера БД;
- база даних клієнтів підприємства;
- дані про особисті рахунки замовників;
- інформація служби охорони.

У тому числі до інформації, що становить комерційну таємницю підприємства, належить:

- відомості про фінанси підприємства;
- відомості про плани підприємства (плани закупівлі, продажу тощо);
- відомості про постачальників;
- відомості про способи придбання і реалізації продукції підприємства;
- зміст договорів і контрактів, однією зі сторін яких виступає підприємство.

2.2 Вимоги до функцій, які виконує КС

Система повинна забезпечувати виконання таких функцій:

- автоматизований збір і первинну обробку технологічної інформації;
- автоматичний контроль стану технологічного процесу, попереджувальну сигналізацію при виході технологічних показників за встановлені межі;
- керування технологічним процесом в реальному масштабі часу;
- подання інформації в зручному для сприйняття та аналізу вигляді на кольорових графічних операторських станціях у вигляді графіків, мнемосхем, гістограм, таблиць.
- автоматичну обробку, реєстрацію та зберігання виробничої інформації, обчислення усереднених, інтегральних та питомих показників;
- автоматичне формування звітів та робочих листів за затвердженою формою за певний період часу, і вивід їх на друк за розкладом та на вимогу;
- отримання інформації від системи протиаварійного захисту, сигналізацію та спрацювання системи;

- контроль над працездатним станом засобів мережі, включаючи вхідні та вихідні ланцюги польового обладнання;
- підготовку вихідних даних для розрахунку матеріальних та енергетичних балансів по виробництву, розрахунків витратних норм по сировині, енергетиці;
- автоматизовану передачу даних в єдину мережу підприємства;
- захист баз даних та програмного забезпечення від несанкціонованого доступу;
- діагностику та видачу повідомлень по відмовах всіх елементів комплексу технічних засобів з точністю до модуля.

Система повинна забезпечувати відновлення працездатності не більше ніж за 120 хвилин після виходу з ладу. При припинення подачі електроенергії не більше ніж за 30 хвилин після її відновлення.

В якості комплектуючих одиниць та деталей повинні застосовуватися серійно випускаються вироби. Елементи пристроїв захисту, панелей, кріплення та вузли повинні бути уніфікованими.

2.3 Вимоги до видів забезпечення КС

2.3.1 Вимоги до інформаційного забезпечення

Математичні методи та алгоритми, які використовуються для шифрування та дешифрування даних, а також програмне забезпечення, що реалізує їх, повинні бути сертифіковані уповноваженими організаціями для використання в державних органах.

Структура та способи організації даних в системі повинні бути обґрунтовані на етапі технічного проектування.

Технічні засоби, що забезпечують зберігання інформації, повинні використовувати сучасні технології, що дозволяють забезпечити підвищену надійність зберігання даних та оперативну заміну обладнання.

При проектуванні та розгортанні системи необхідно розглянути можливість використання накопиченої інформації з уже функціонуючих інформаційних систем.

Математичні методи та алгоритми, які використовуються для шифрування та дешифрування даних, а також програмне забезпечення, що реалізує їх, повинні бути сертифіковані уповноваженими організаціями для використання в державних органах.

2.3.2 Вимоги до програмного забезпечення

Прикладне програмне забезпечення системи для організації взаємодії з користувачем повинно використовувати українську мову.

Для реалізації функцій АСУ ТП повинні використовуватися сучасні засоби конфігурації та візуального програмування, орієнтовані на фахівців-розробників. Такі рішення дозволяють істотно мінімізувати час розробки, та надають виняткову наочність алгоритмам керування та обробки інформації.

Зважаючи на відсутність вітчизняних нормативних документів, як їх прототип необхідно використовувати МЕК 61131-3, який регламентує мови програмування які можуть використовуватися для розробки прикладного програмного забезпечення систем.

Для реалізації завдань комп’ютерної системи повинно використовуватися спеціалізоване програмне забезпечення, яке повинно функціонувати на програмованому логічному контролері.

Характеристики програмного забезпечення повинні задовольняти вимогам щодо виконання функцій, зазначених у попередніх розділах.

Мережеві програмні засоби, що забезпечують об’єднання підсистем, операторських станцій та засобів архівування даних в єдину систему, повинні реалізовувати завантаження та керування запуском завдань, забезпечувати обмін між завданнями та базами даних, і надавати доступ до периферійних пристроїв.

Комп’ютерна система повинна мати можливість оперативного конфігурування прикладного програмного забезпечення в процесі функціонування системи.

Всі помилкові ситуації, що виникають при роботі програм, повинні діагностуватися, супроводжуватися повідомленнями, та не повинні викликати порушень в роботі системи.

Технічне забезпечення системи повинно максимально та найбільш ефективним чином використовувати існуючі технічні засоби.

Комплекс технічних засобів комп’ютерної системи повинен бути достатній для реалізації визначених функцій, та будуватися на базі наступних спеціалізованих програмно-технічних комплексів:

Засоби вимірювання, що входять в систему контролю, керування повинні мати сертифікат про затвердження типу, опис типу, методику повірки. У специфікацію обладнання системи повинні бути включені спеціальні технічні та програмні засоби для калібрування вимірювальних каналів.

Метрологічне обслуговування комп’ютерної системи має забезпечувати можливість як поелементної, так і комплексної повірки або калібрування вимірювальних каналів.

Для технічних засобів, що беруть участь в процесі вимірювання контрольованих параметрів повинні бути забезпечені відповідні умови експлуатації та їх контроль.

Організаційне забезпечення системи повинно бути достатнім для ефективного виконання персоналом покладених на нього обов’язків при здійсненні автоматизованих та пов’язаних з ними неавтоматизованих функцій системи.

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1 Розробка схеми організаційної структури підприємства

3.1.1 Розробка функціональної схеми автоматизації

Відповідно до завдання розроблено функціональна схему комп'ютерної системи, яка наведена на рис. 3.1.

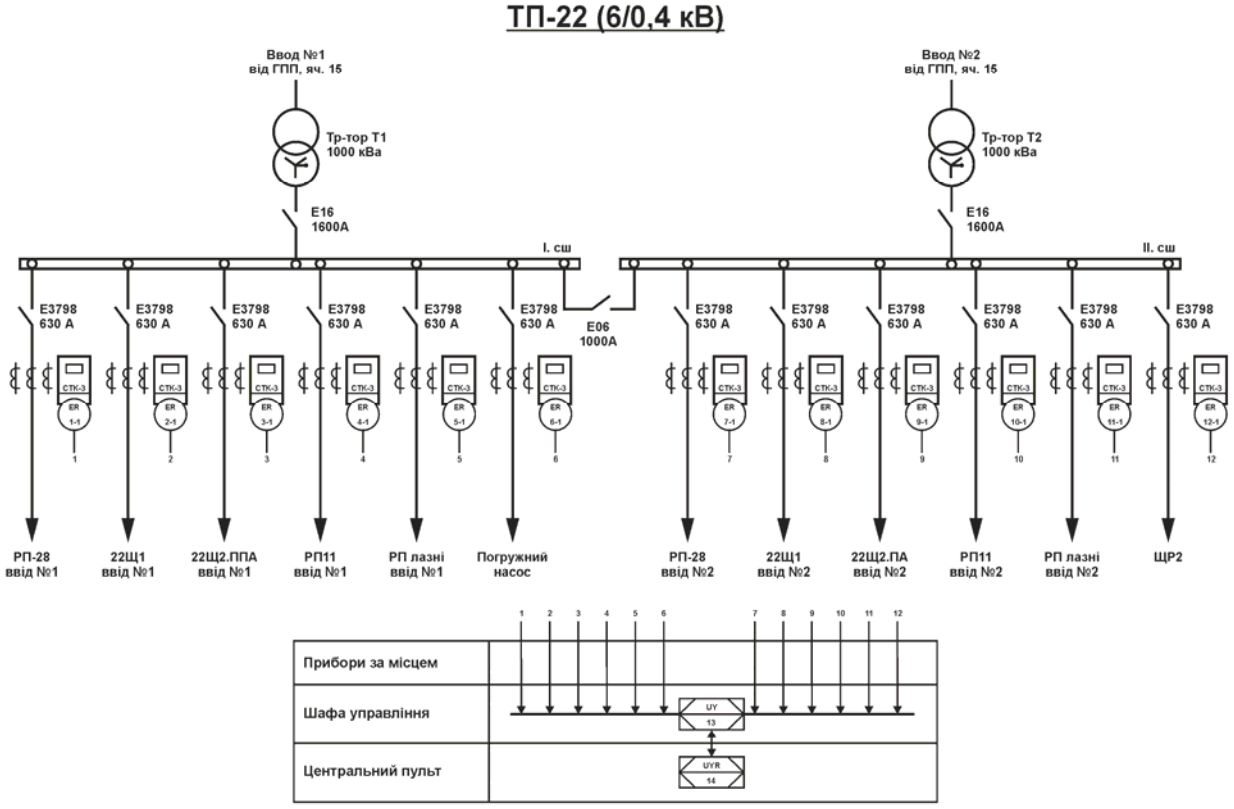


Рисунок 3.1 – Функціональна схему комп'ютерної системи

Система включає трифазні лічильники які позначенні як EE 1-1 – EE 12-1. Кожен лічильник вимірює споживану потужність свого споживача, та видає його на імпульсному виході. Усі лічильники підключаються до пристрою контролю UY13 який обчислення значення споживаної потужності та зберігає його. По запиту від пульта оператора UYR14 пристрій контролю передає значення споживаної потужності.

3.1.2 Розробка схеми функціональної структури

Структури схема системи наведена на рис. 3.2. Система складається з двох великих елементів автоматизованого робочого місця оператора та пристрою контролю. Система виконує наступні функції:

1) протоколювання технологічного процесу;

2) обробку інформації про стан об’єкту управління;

3) зберігання отриманої інформації;

4) формування звітів;

5) зв’язок з іншими системами підприємства.

Рисунок 3.2 – Схема функціональної структури комп’ютерної системи

Відповідно до функцій система складається з наступних підсистем: передачі інформації, відображення, вводу та доступу до інформації, аналізу інформації, розрахунку, збору інформації.

3.1.3 Розробка переліку вхідних та вихідних сигналів і даних

З метою визначення входів і виходів необхідно провести аналіз та класифікацію входів і виходів датчиків та виконавчих пристроїв технологічного обладнання.

В результаті аналізу отримано перелік вхідних та вихідних сигналів який наведено в табл. 3.1.

Таблиця 3.1 – Перелік вхідних та вихідних сигналів

№ п/п.	Найменування інформації (сигнали, дані)	Ідентифікатор	Напр. вх./вих.	Функція	Вид	Джерело/ Отримувач	Форма подання (розрядність, точність)		Період вв./вив., сек
							Зовніш-ня	Внутріш-ня	
1	СП РП-28-1	ЕЕ1	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1
2	СП 22Щ1-1	ЕЕ2	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1
3	СП 22Щ2.ПА-1	ЕЕ3	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1
4	СП РП11-1	ЕЕ4	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1
5	СП РП бані-1	ЕЕ5	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1
6	СП погружной насос	ЕЕ6	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1
7	СП РП-28-2	ЕЕ7	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1
8	СП 22Щ1-2	ЕЕ8	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1
9	СП 22Щ2.ПА-2	ЕЕ9	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1
10	СП РП11-2	ЕЕ10	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1
11	СП РП бані-2	ЕЕ11	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1
12	СП ЩР2	ЕЕ12	Вхід	Контроль	Імп.	СТК-3	4/20 мА	4 байта	0,1

3.1.4 Вибір пристрою керування

У якості пристрою контролю обрано тарифікатор ОБЛІК-Т20. Який має 20 імпульсних входів, дозволяє зберігати поточну інформацію о споживаній потужності, інформацію за останні три доби та інформацію за останні три місяці.

Тарифікатор ОБЛІК-Т20 має інтерфейс RS-485 та працює відповідно до протоколу Modbus RTU з сервером обліку АСТУЕ. На одній лінії RS-485 може знаходитися до 32 тарифікаторів.

Тарифікатор дозволяє працювати двох тарифному режимі при цьому перерахунок імпульсів для кожного тарифного часу виконується за своїм коефіцієнтом. Коефіцієнти перерахунку задаються з сервера АСТУЕ.

3.1.5 Розробка схеми електричної принципової

На підставі обраної елементної бази та переліку вхідних та вихідних сигналів розроблено схема електрична принципова яка наведена на рис. 3.2.

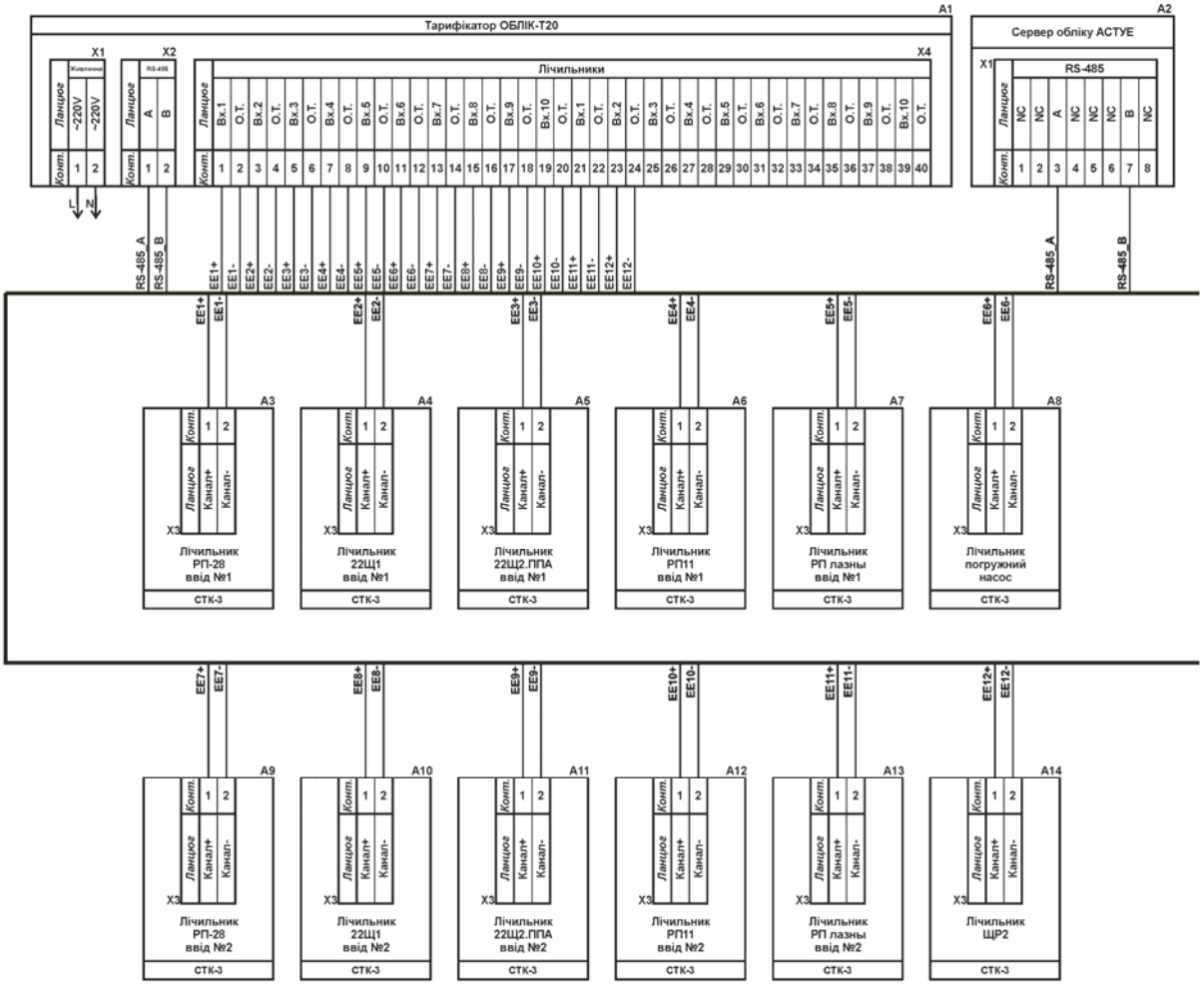


Рисунок 3.3 – Схема електрична принципова

3.1.6 Вибір технічних засобів реалізації системи

Значення споживаної потужності по споживачам вимірюється трифазними лічильниками СТК-3:

- клас точності 1,0;
- номінальна наруга ~380 В;
- номінальний струм 10 А;
- максимальний струм 100 А;
- частота мережі 50 Гц;

- повна потужність споживана послідовним ланцюгом 0,1 ВА;
- повна потужність споживана паралельним ланцюгом 4,0 ВА;
- чутливість 12,5 мА.

3.1.7 Обґрунтування системного програмного забезпечення

У якості програмного забезпечення верхнього рівня обрано сервер обліку АСТУЕ який дозволяє працювати з тарифікатором ОБЛІК-Т20.

Для дослідження, моделювання та налагодження мережі підприємства використано PacketTracer V7. Спостереження за трафіком мережі виконувалося за допомогою пакету Wireshark V2.

Віддалений доступ для відлагождення програмного забезпечення системи виконувався за допомогою програмного забезпечення TeamViewer V13.

В якості платформи для означеного переліку програмного забезпечення обрано операційну систему Microsoft Windows 7 Service Pack 1, оскільки підприємство має відповідну корпоративну ліцензію.

Для захисту персонального комп'ютера автоматизованого робочого місця від несанкціонованого доступу та шкідливого програмного забезпечення використано ESET NOD32 V11 з корпоративною ліцензією.

3.2 Розробка апаратних засобів комп'ютерної системи

Відповідно до вимог структури в системі повинен бути шлюз. Шлюз LoRa – пристрій, який приймає дані через радіоканал від кінцевих пристроїв і передає їх в транзитну мережу в якості якої може виступати Ethernet, Wi-Fi, стільникові мережі та будь-які інші телекомунікаційні канали.

З урахуванням вимог до функцій та з точки зору мінімізації вартості був обраний пристрій Multi-Tech MultiConnect Conduit MTCDT-210, що зображений на рис. 3.4.

Рисунок 3.4 – Шлюз Multi-Tech MultiConnect Conduit MTCDT-210

Multi-Tech MultiConnect Conduit MTCDT-210 – шлюз з інтерфейсом Ethernet для побудови мереж LoRaWAN в частотному діапазоні 868 МГц. Наявність двох слотів для змінних модулів забезпечує гнучке налаштування шлюзу. В якості змінних модулів можуть використовуватися як LoRaWAN, так і модулі з послідовним інтерфейсом або GPIO. Шлюз також може виконувати роль сервера LoRaWAN.

Шлюз LoRaWAN має два варіантами внутрішнього ПО: AEP і mLinux. Варіант AEP (Application Enablement) передбачає просте та інтуїтивно зрозуміле конфігурування/ програмування шлюзу в графічному середовищі Node-RED. Варіант mLinux надає повний контроль над шлюзом, дозволяє створювати практично будь-які додатки. В стандартний дистрибутив mLinux (Linux 3.12 Kernel, Yocto 1.6) включена підтримка Java, Python, C/C ++, C #, JavaScript.

Технічні характеристики шлюзу Multi-Tech MultiConnect Conduit MTCDT-210:

− Процесор – ARM9, 400 МГц.

− Об’єм оперативної пам’яті – 2 Гбайт ;

− Об’єм flash-пам’яті – 256 Мбайт;

− Вхідна напруга (В) – 9-32 В.

− USB Host (Type A), USB Device (Micro B) – 1.

− USB роз’єм типу B для налаштування типу – 1 (за табличкою).

− Порт Ethernet RJ-45 – 1.

− Wi-Fi / Bluetooth роз’єм – 1.

− Роз’єм для GPS антени – 1.

− Роз’єм для карти пам’яті Micro SD.

− Розміри, см – 16,1 х 10,7 х 4,3.

− Вага – 442,25 г.

− Температура робочого середовища від -30 до +70 С.

Серед можливих змінних модулів було обрано модуль LORA MTAC-LoRa та модуль Ethernet MTAC-ETH.

Модуль LORA MTAC-LoRa використовується для прийому радіосигналів від кінцевих пристроїв розташованих на дальніх відстанях з забезпеченням технології LoRa від компанії Semtech. Його зовнішній вигляг зображний на рис. 3.5.

Рисунок 3.5 – Модуль LORA MTAC-LoRa

Модуль Ethernet MTAC-ETH забезпечує Ethernet-з’єднання за допомогою роз’єму RJ-45. Цей модуль використовується для підключення до мережі Інтернет. Він представлений на рис. 3.6.

Рисунок 3.6 – Модуль Ethernet MTAC-ETH

Для підрахунку імпульсів та їх передачі на шлюз необхідний спеціальний кінцевий пристрій. Серед можливих варіантів був обраний пристрій Вега

СІ-11 оскільки це закінчений пристрій, що має не високу вартість і забезпечує виконання вимог до функцій підсистеми на нижньому рівні, а також враховуючи, що всі кінцеві пристрої побудовані з використанням трансиверу LoRa від компанії Semtech.

Вега СІ-11призначений для виконання підрахунку імпульсів, що приходять на 4 незалежні входи, з подальшим накопиченням і передачею цієї інформації в мережу LoRaWAN. Передача здійснюється за допомогою технології LoRa розробленої компанією Semtech та трансиверу Semtech SX1272.

Два з чотирьох входів можуть бути налаштовані на використання в якості охоронних. Лічильник імпульсів може бути використаний на приладах обліку комунальних ресурсів та промисловому обладнанні з імпульсним виходом, таких як водоміри, електролічильники, теплолічильники. Елементом живлення для лічильника служить батарея ємністю 3400 мАг, розрахована на термін служби до 10 років при передачі даних один раз на добу. Пристрій Вега СІ-11 зображений на рис. 3.7.

Рисунок 3.7 – Кінцевий пристрій ВЕГА СІ-11

Технічні характеристики пристрою ВЕГА СІ-11:

− Процесор – ARM Cortex-M3.

− Входи імпульсні – 4.

− Максимальна частота імпульсного сигналу – 200 Гц.

− USB-порт – так.

− Діапазон робочих температур – від -40 до + 85 °С.

− Протокол передачі даних: LoRaWan.

− Клас пристрою LoRaWAN – А.

− Кількість каналів LoRaWAN – 16.

− Діапазон частот: 868 МГц (можливість налаштування будь-якого частотного плану в діапазоні 860-1000МГц)

− Спосіб активації в мережі LoRaWAN – АВР або ОТАА.

− Період виходу на зв’язок – 1, 6, 12 або 24 години.

− Тип антени LoRaWAN – внутрішня.

− Дальність радіозв’язку в сільській місцевості – до 15 км.

− Дальність радіозв’язку в щільній міській забудові – до 5 км.

− Ємність вбудованої батареї – 3400 мАг.

− Час безперервної роботи від батареї – до 10 років.

− Розміри корпусу, мм – 95 х 50 х 45.

− Ступінь захисту корпусу – IP65.

− Кріплення стяжками до опори, на DIN-рейку, настінне.

Контакти для підключення лічильника до пристрою ВЕГА СІ-11 зображені на рис. 3.8.

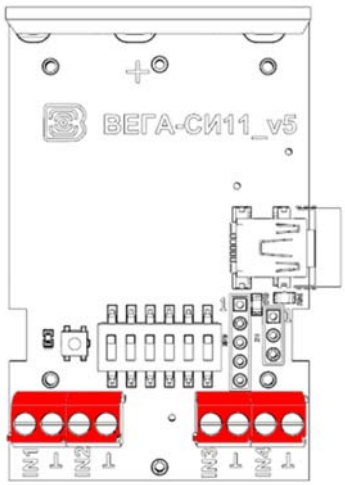


Рисунок 3.8 – Контакти для підключення

Лічильник імпульсів має 4 пари контактів і дозволяє підключати ланцюги з замикаючих контактів типу геркон. Входи № 3 і 4 можуть бути налаштовані для використання в режимі “Охорона” за допомогою перемикачів на платі. В такому випадку пристрій не провадить підрахунок імпульсів на вході “Охорона”, а тільки стежить за його замиканням. У разі замикання входу“Охорона”, пристрій активується і відправляє в мережу повідомлення з сигналом тривоги.

Для збору, обробки і архівування даних використані сервера Cisco UCS C240 M5. Зовнішній вигляд сервера Cisco UCS C240 M5 представлений на рис. 3.9.

Рисунок 3.9 – Сервер Cisco UCS C240 M5

Технічні характеристики сервера Cisco UCS C240 M5:

− Тип чіпсета – Intel C621.
− Тип процесора – Intel Xeon.
− Модель процесора – Xeon Platinum 8158.
− Частота – 3.00 ГГц.
− Кількість ядер – 12.
− Встановлено процесорів – 1. Максимально процесорів – 2.
− Об’єм оперативної пам’яті – 32 Гбайт.
− Стандарт оперативної пам’яті – DDR4-2666.
− Тип слотів – DIMM.
− Кількість слотів – 24.
− Максимальний об’єм оперативної пам’яті – 768 Гбайт.
− Внутрішня пам’ять – 6 Тбайт.
− Інтерфейс – SAS, SATA.

− Потужність блока живлення – 1600 Вт.

− Встановлено блоків живлення – 2.

− Максимально блоків живлення – 2.

− Зовнішні порти – 2x USB 3.0, 2x USB 2.0, VGA, KVM.

− Кількість PCI-Express 3.0 слотів – 6.

− Мережевий адаптер – 4x Gigabit Ethernet.

− Тип корпуса монтаж в стійку.

− Розміри, см – 44,8 x 73,8 x 8,7.

− Додатково – LGA3647 Socket, SD Card.

Задля виконання вимог до збереження інформації при аваріях і збоях в системі для серверів були використані джерела безперебійного живлення FSP Galleon 2000VA, що забезпечують захист серверів від збоїв електропостачання та перепадів напруги, а також створюють умови для збереження цілісності баз даних і захисту інформації під час прийому, обробки, збереження та передачі даних. Зовнішній вигляд джерела безперебійного живлення FSP Galleon 2000VA представлений на рис. 3.10.

Рисунок 3.10 – Джерело безперебійного живлення FSP Galleon 2000VA

Технічні характеристики пристрою FSP Galleon 2000VA:

− Тип – подвійне перетворення (on-line).

− Вихідна потужність – 2000 ВА (1600 Вт).

− Час роботи від батарей при 100%/50% навантаженні – 6,5/17 хвилин.

− Вхід – 150-300 В.

− Вихід – 2 розетки Schuko.

− Інтерфейс – RS-232, USB, SNMP-адаптер.

− Тип і кількість вбудованих батарей – 6 шт. х 12 В, 7Ач.

− Час перезарядки батарей – 4 години до ємності 90%.

− Розміри, см – 48х 43,8х 8,8.

− Вага, кг – 20,6.

Для захисту базової станції Multi-Tech MultiConnect Conduit MTCDT-210 від втручання в роботу пристрою використовується бокс монтажний навісний БМ-20 (IP54) з частковим захистом від проникнення пилу від компанії Bilmax. Можливе, часткове потрапляння пилу на пристрій не порушить його роботу. Бокс монтажний навісний БМ-20 зображений на рис. 3.11.

Рисунок 3.11 – Бокс монтажний навісний БМ-20

Характеристики боксу:

− Серія – БМ.

− Ступінь захисту – IP54.

− Розміри боксу, мм – 200х200х100.

− Товщина металу, мм – 0,5.

− Тип монтажу – навісний.

За повноцінний захист від потрапляння пилу і від попадання води на модуль ВЕГА СІ-11, а також захист від втручання в роботу відповідає бокс монтажний навісний BW-2,5.2,5.1,5 (IP65) від компанії Bilmax. Бокс монтажний навісний BW-2,5.2,5.1,5 зображений на рис.3.11.

Рисунок 3.11 – Бокс монтажний навісний BW-2,5.2,5.1,5

Характеристики боксу:

- Серія – BW.
- Ступінь захисту – IP65.
- Розміри боксу, мм – 250x250x150.
- Товщина металу, мм – 1,5.
- Тип монтажу – навісний.

3.3 Розробка топологічної схеми розміщення структурних підрозділів підприємства

Структурна схема комплексу технічних засобів системи складається з трьох рівнів:

– рівень ядра;

– рівень комутаторів розподілення;

– рівень комутаторів доступу.

Рівень ядра складається з п’яти поєднаних один з одним маршрутизаторів через канали WAN. Основна мета цього рівня в тому, щоб максимально швидко передавати пакети між підмережами. Підключення до віддаленої мережі здійснюється через мережу Internet за допомогою технології VPN.

Рівень комутаторів розподілення складається з комутаторів які розташовані у підрозділах ВНЗ 1 рівня. Ці комутатори зв’язують рівень доступу і

рівень ядра. Комутатори рівня розподілу покликані зняти навантаження з ядра мережі розподіляючи трафік між комутаторами доступу.

Рівень комутаторів доступу складається з комутаторів, які розташовані у підрозділах ВНЗ 1 рівня та та НТУ «ДП». Завданням цих комутаторів є безпосереднє підключення кінцевих вузлів мережі, таких як сервери, персональні комп'ютери, та принтери.

Структурна схема корпоративної мережі підрозділів заводу зображена на рис. 3.12.

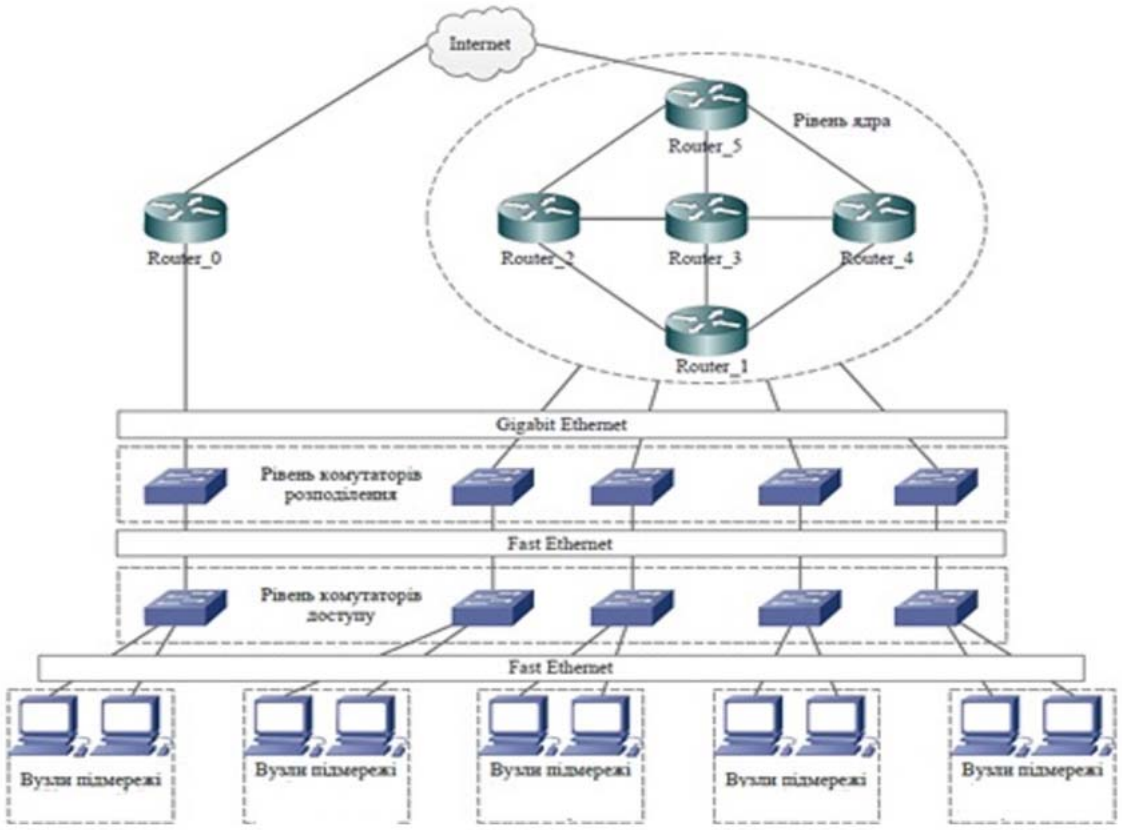
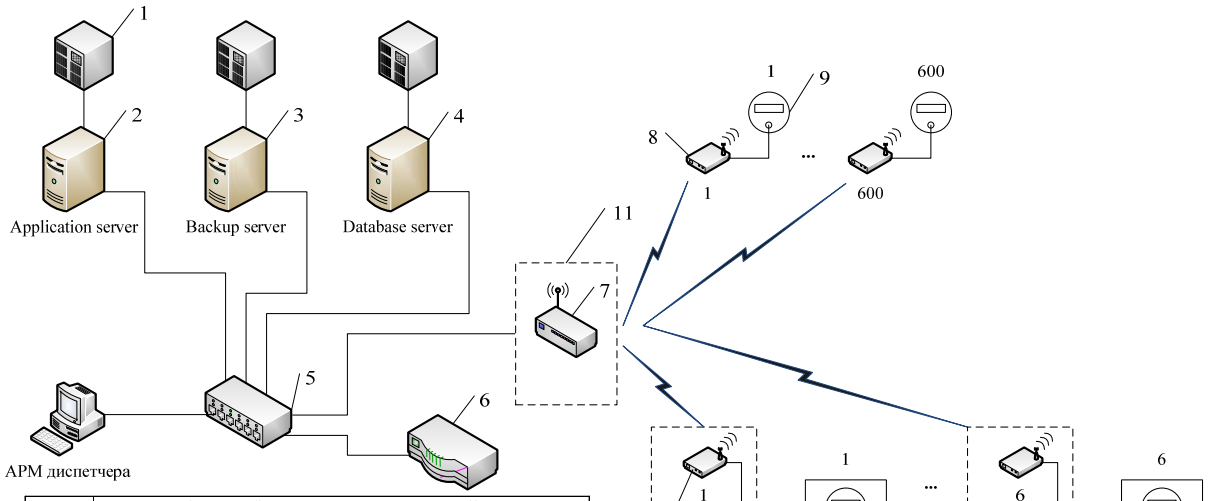


Рисунок 3.12 – Структурна схема корпоративної мережі підрозділів заводу

3.4 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

Відповідно до перспективної структурної схеми комп'ютерної системи та обраного обладнання для реалізації системи контролю обліку була побудована структурна схема комплексу технічних засобів. Структурна схема комплексу технічних засобів зображена на рис. 3.13.



1	Джерело безперебійного живлення FSP Galleon 2000VA
2, 3, 4	Сервер Cisco UCS C240 M5
5	Комутатор
6	Маршрутизатор
7	Шлюз Multi-Tech MultiConnect Conduit MTCDT-210
8	Модуль LoRa ВЕГА CI-11
9	Лічильник Apator Powogaz JS-1,5 NK
10	Лічильник Apator Powogaz MWN-65 NK
11	Бокс монтажний навісний БМ-20
12	Бокс монтажний навісний BW-2,5.2,5.1,5

Рисунок 3.13 – Структурна схема комплексу технічних засобів

До устаткування системи входить:

- джерела безперебійного живлення FSP Galleon 2000VA для постійного захисту серверів від неякісного електропостачання;
- сервери Cisco UCS C240 M5 (задля виконання вимог до збереження інформації при аваріях і збоях в системі, а також для зменшення навантаження та повноцінного розподілу обов’язків між серверами кількість серверів збільшено до трьох);
- комутатор, що об’єднує між собою пристрої підмережі контролю об’єкту;
- маршрутизатор який відокремлює підмережу контролю об’єкту від інших підмереж підприємства і забезпечує маршрутизацію мережевого трафіку;
- шлюз MultiConnect Conduit MTCDT-210 від компанії Multi-Tech;

– модуль LoRa ВЕГА CI-11;
– лічильник Apator Powogaz JS-1,5 NK;
– лічильник Apator Powogaz MWN-65;
– АРМ диспетчера;
– бокс монтажний навісний БМ-20;
– бокс монтажний навісний BW-2,5.2,5.1,5.

3.5 Розрахунок основних характеристик для вихідного трафіку

Для забезпечення коректної роботи мережі та відсутності перевантажень на обладнанні, що використане при побудові мережі, необхідно розрахувати основні характеристик для вихідного трафіку в найбільшому сегменті мережі підприємства за умови, що послугами одночасно користуються 100% користувачів. Характеристики такі як: коефіцієнт зайнятості обладнання, завантаження каналу передачі даних, середню затримку кадру, середню довжину черги, середній час перебування пакета в черзі, пропускну здатність каналу.

Для розрахунку приймається модель ділянки мережі як модель системи масового обслуговування M/M/1. Результати розрахунків порівнюються із заданими параметрами комп'ютерної системи.

Дано:

– кількість вузлів в найбільшій мережі: 120;
– середня інтенсивність трафіку: $\mu = 205$ (кадрів/с);
– середня довжина повідомлення: $l = 900$ байт;
– вимоги до затримки передачі пакету – ≤ 5 мс.

Для підключення 120 вузлів в найбільшій підмережі обрано комутатори Cisco 2960-24TT-L 24 10/100 (5 шт), що використовувались при розробці моделі комп'ютерної системи. Комутатори працюють на рівні розподілу і на рівні доступу. Вихідний трафік пересилається на маршрутизатор в лінію з пропускною здатністю 1Гбіт/с.

Для того, щоб комутатори рівня розподілу не були перенавантжений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Середня інтенсивність трафіку μ = 205 (кадрів/с), а середня довжина повідомлення – 900 байт.

Розрахунок пропускної здатності мережі на рівні доступу допускаючи, що послугами одночасно користуються 100% користувачів:

$P_{р.д}$ = μ * l * n * 8 = 205 * 900 * 24 * 8 = 35,4 Мбіт/с, де

n – кількість портів в комутаторі рівня доступу.

Пропускна здатність мережі на рівні розподілу розраховується наступним чином:

$P_{р.р}$ = μ * l * N * 8 = 205 * 900 * 120 * 8 = 177,1 Мбіт/с, де

N – кількість вузлів в найбільшій мережі.

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

Основний комутатор рівня розподілу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1Гбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

$\mu_{вих}$ = 1 000 000 000 / (900 * 8) = 138889 пакетів/с

Оскільки кожне джерело формує в середньому 205 пакетів/с, то до комутатора рівня розподілу можна приєднати максимум:

N = 138889 / 105 = 678 джерел.

Що задовольняє мережу на 120 ПК.

Кожен з 120 ПК посилає потік заявок з інтенсивністю 205 кадрів/с. Інтенсивність вихідного трафіку від всіх користувачів:

$\lambda = N * \mu$ = 120 * 205 = 24600 пакетів/с

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

$$\rho = \frac{\lambda}{\mu_{вих}} = \frac{24600}{138889} = 0{,}18$$

Коефіцієнт зайнятості комутатора рівня розподілу:

$$r = \frac{\rho}{1-\rho} = \frac{0{,}18}{1-0{,}18} = 0{,}22$$

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

$$T = \frac{1}{(\mu - \lambda)} = \frac{1}{138889 - 24600} = 8{,}7 \text{ мкс}$$

Середня довжина черги:

$$\mathcal{L}_{чер} = \frac{\rho^2}{1-\rho} = \frac{0{,}18^2}{1-0{,}18} = 0{,}04$$

Ця цифра може бути корисною при налаштуванні черг на обладнанні – в пристроях можна вказувати максимальний розмір черги пакетів. В даному випадку в системі на обслуговуванні менше 1 пакету, а це свідчить про те, що система працює з великим запасом по продуктивності.

Середній час перебування пакета в черзі:

$$T_{оч} = \frac{\mathcal{L}_{чер}}{\lambda} = \frac{0{,}04}{24600} = 1{,}63 \text{ мкс}$$

Це значення менше необхідного значення ≤5 мс, що задовольняє вимогам. Пропускна здатність каналу:

$$\lambda = \frac{\text{пропускна здатність}}{\text{довжина кадру}} = \frac{b}{l}$$

$$b = \lambda * l = 24600 * 900 * 8 = 177100000 \ \frac{\text{біт}}{\text{с}} = 177{,}1 \text{ Мбіт/с}$$

Що задовольняє пропускній здатності вихідного каналу в 1Гбіт/с.

3.6 Висновок за розділом

В спеціальній частині розроблені вимоги до кожної складової комплексу технічного захисту інформації, обґрунтований вибір технічних засобів та інженерних заходів.

У розділі проведена розробка комп'ютерної системи обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Система вирішує наступні завдання:

- вимірювання активної потужності;

- вимірювання реактивної потужності;
- реєстрацію отриманої інформації;
- передачу інформації до серверу;
- візуалізацію отриманої інформації.

Розроблена комп’ютерної системи з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову системи контролю роботи коксохімічного підприємства, а також для збору і підготовки статистичної інформації.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота.

4 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

4.1 Розрахунок схеми адресації корпоративної мережі

Розрахунок адресації комп'ютерної мережі проводився за допомогою CIDR та VLSM. CIDR (безкласова маршрутизація) – метод IP-адресації, що дозволяє гнучка управляти простором IP-адрес, не використовуючи жорсткі рамки класової адресації. CIDR використовує VLSM (маски підмереж змінної довжини), щоб виділяти IP-адреси підмережам згідно з потребами, а не за класами. При використанні VLSM мережа спочатку розділяється на підмережі, а потім вони, в свою чергу, також розбиваються на менші підмережі. Цей процес можна повторювати багаторазово для створення підмереж різних розмірів.

Для побудови мережі організації використаний адресний простір 192.168.40.0/21. Послідовні канали між маршрутизаторами використовують адреси з діапазону 10.0.6.0/24.

Розрахунок схеми IP-адресації методом VLSM дозволив поділити адресний простір на невеликі підмережі, які максимально наближені до вимог необхідної кількості вузлів (табл. 3.2). VLSM дав можливість більш ефективно використовувати IP-адреси, ніж звичайний поділ на підмережі з використанням класової адресації.

Таблиця 4.1 – Кількість вузлів в підмережах

LAN_1	LAN_2	LAN_3	LAN_4	LAN_5
55	65	80	70	120

Розрахунок схеми IP-адресації методом VLSM був розглянутий на прикладі найбільшої підмережі LAN_5, що ділиться на VLAN та WAN_A для адрес між маршрутизаторами:

− LAN_5. Необхідний розмір підмережі становить 120 вузлів. Для адресації достатньо виділити 7 біт з вузлової частини. Виділений розмір підмережі дорівнює 128 ($N = 2^7 – 2 = 126$). Адреса мережі: 192.168.40.0. IP-адреса мережі 192.168.00101|000.0|0000000 та маска 255.255.11111|000. 0|0000000 у десятково-двійковій формі з урахуванням виділених 7 біт з вузлової частини. Десятковий формат визначеної маски: 255.255.255.128. Префікс: /25. Діапазон допустимих IP-адрес вузлів в десятково-двійковій формі: 192.168.00101000.0|0000001 – 192.168.00101000.0|1111111 (в десятковій формі: 192.168.40.1 – 192.168.40.126). Широкомовна адреса: 192.168.40.127. LAN_5 розділена на чотири VLAN. Три з яких розподілені між відділами і одна для віддаленого доступу для налаштування пристроїв.

− VLAN_16. Необхідний розмір підмережі становить 30 вузлів. Для адресації достатньо виділити 5 біт з вузлової частини. Виділений розмір підмережі дорівнює 32 ($N = 2^5 – 2 = 30$). Адреса мережі: 192.168.40.0. IP-адреса мережі 192.168.00101000.0|00|00000 та маска 255.255.11111000. 0|00|00000 у десятково-двійковій формі з урахуванням виділених 5 біт з вузлової частини. Десятковий формат визначеної маски: 255.255.255.224. Префікс: /27. Діапазон допустимих IP-адрес вузлів в десятково-двійковій формі: 192.168.00101000.000|00001 – 192.168.00101000.000|11111 (в десятковій формі: 192.168.40.1 – 192.168.40.30). Широкомовна адреса: 192.168.40.31.

− VLAN_26. Необхідний розмір під мережі становить 30 вузлів. Для адресації достатньо виділити 5 біт з вузлової частини. Виділений розмір підмережі дорівнює 32 ($N = 2^5 – 2 = 30$). Адреса мережі: 192.168.40.32. IP-адреса мережі 192.168.00101000.001|00000 та маска 255.255.11111000. 001|00000 у десятково-двійковій формі з урахуванням виділених 5 біт з вузлової частини. Десятковий формат визначеної маски: 255.255.255.224. Префікс: /27. Діапазон допустимих IP-адрес вузлів в десятково-двійковій формі: 192.168. 00101000.001|00001 – 192.168.00101000.001|11111 (в десятковій формі: 192.168.40.33 – 192.168.40.62). Широкомовна адреса: 192.168.40.63.

− VLAN_36. Необхідний розмір підмережі становить 30 вузлів. Для адресації достатньо виділити 5 біт з вузлової частини. Виділений розмір підмережі дорівнює 32 ($N = 2^5 – 2 = 30$). Адреса мережі: 192.168.40.64. IP-адреса мережі 192.168.00101000.010|00000 та маска 255.255.11111000. 010|00000 у десятково-двійковій формі з урахуванням виділених 5 біт з вузлової частини. Десятковий формат визначеної маски: 255.255.255.224. Префікс: /27. Діапазон допустимих IP-адрес вузлів в десятково-двійковій формі: 192.168. 00101000.010|00001 – 192.168.00101000.010|11111 (в десятковій формі: 192.168.40.65 – 192.168.40.94). Широкомовна адреса: 192.168.40.95.

− VLAN_99. Необхідний розмір підмережі становить 30 вузлів. Для адресації достатньо виділити 5 біт з вузлової частини. Виділений розмір підмережі дорівнює 32 ($N = 2^5 – 2 = 30$). Адреса мережі: 192.168.40.96. IP-адреса мережі 192.168.00101000.011|00000 та маска 255.255.11111000. 011|00000 у десятково-двійковій формі з урахуванням виділених 5 біт з вузлової частини. Десятковий формат визначеної маски: 255.255.255.224. Префікс: /27. Діапазон допустимих IP-адрес вузлів в десятково-двійковій формі: 192.168. 00101000.011|00001 – 192.168.00101000.011|11111 (в десятковій формі: 192.168.40.97 – 192.168.40.126). Широкомовна адреса: 192.168.40.127.

− WAN_A. Необхідний розмір під мережі становить 2 вузла. Для адресації достатньо виділити 2 біта з вузлової частини. Виділений розмір підмережі дорівнює 2 ($N = 2^2 – 2 = 2$). Адреса мережі 10.0.6.0. IP-адреса мережі 10.0.6.|000000|00 та маска 255.255.255.|000000|00 у десятково-двійковій формі з урахуванням виділених 2 біт з вузлової частини. Десятковий формат визначеної маски: 255.255.255.252. Префікс: /30. Діапазон допустимих IP-адрес вузлів в десятковій формі: 10.0.6.1 – 10.0.0.2. Широкомовна адреса: 10.0.6.3.

В табл. 4.2 представлена розроблена схема IP-адресації мережі організації методом VLSM.

Таблиця 4.2 – Адресація підмереж

Назва мережі	Кількість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону	Кінцеве значення діапазону
LAN_5	120	192.168.40.0	255.255.255.128	192.168.40.1	192.168.40.126
VLAN 16	30	192.168.40.0	255.255.255.224	192.168.40.1	192.168.40.30
VLAN 26	30	192.168.40.32	255.255.255.224	192.168.40.33	192.168.40.62
VLAN 36	30	192.168.40.64	255.255.255.224	192.168.40.65	192.168.40.94
VLAN 99	30	192.168.40.96	255.255.255.224	192.168.40.97	192.168.40.126
LAN_3	80	192.168.40.128	255.255.255.128	192.168.40.129	192.168.40.254
LAN_4	70	192.168.41.0	255.255.255.128	192.168.41.1	192.168.41.126
LAN_2	65	192.168.41.128	255.255.255.128	192.168.41.129	192.168.41.254
LAN_1	55	192.168.42.0	255.255.255.192	192.168.42.1	192.168.42.62
A	2	10.0.6.0	255.255.255.252	10.0.6.1	10.0.6.2
B	2	10.0.6.4	255.255.255.252	10.0.6.5	10.0.6.6
C	2	10.0.6.8	255.255.255.252	10.0.6.9	10.0.6.10

4.2 Розробка топологічної схеми корпоративної мережі

Під час розрахунку схеми адресації пристроїв було виконано деякі наступні настанови для більш зручної взаємодії з пристроями в побудованій мережі та спрощення конфігурування кінцевих пристроїв:

− перші можливі для використання IP-адреси призначені інтерфейсам і підінтерфейсам маршрутизаторів у LAN;

− другі з можливих IP-адрес призначені комутаторам у LAN;

− серверам привласнено IP-адреса за правилом: IP-адрес дорівнює першому можливому адресу у мережі+9+6;

− останні з використовуваних IP-адрес відведені вузлам;

− в мережах VLAN адресація кінцевих пристроїв організована за допомогою протоколу DHCP.

Розрахунок схеми адресації пристроїв представлений у вигляді табл. 4.3 був проведений з урахуванням розробленої схема IP-адресації мережі представленої в табл. 4.4 та топології спроектованої мережі зображеної на рис. 4.1.

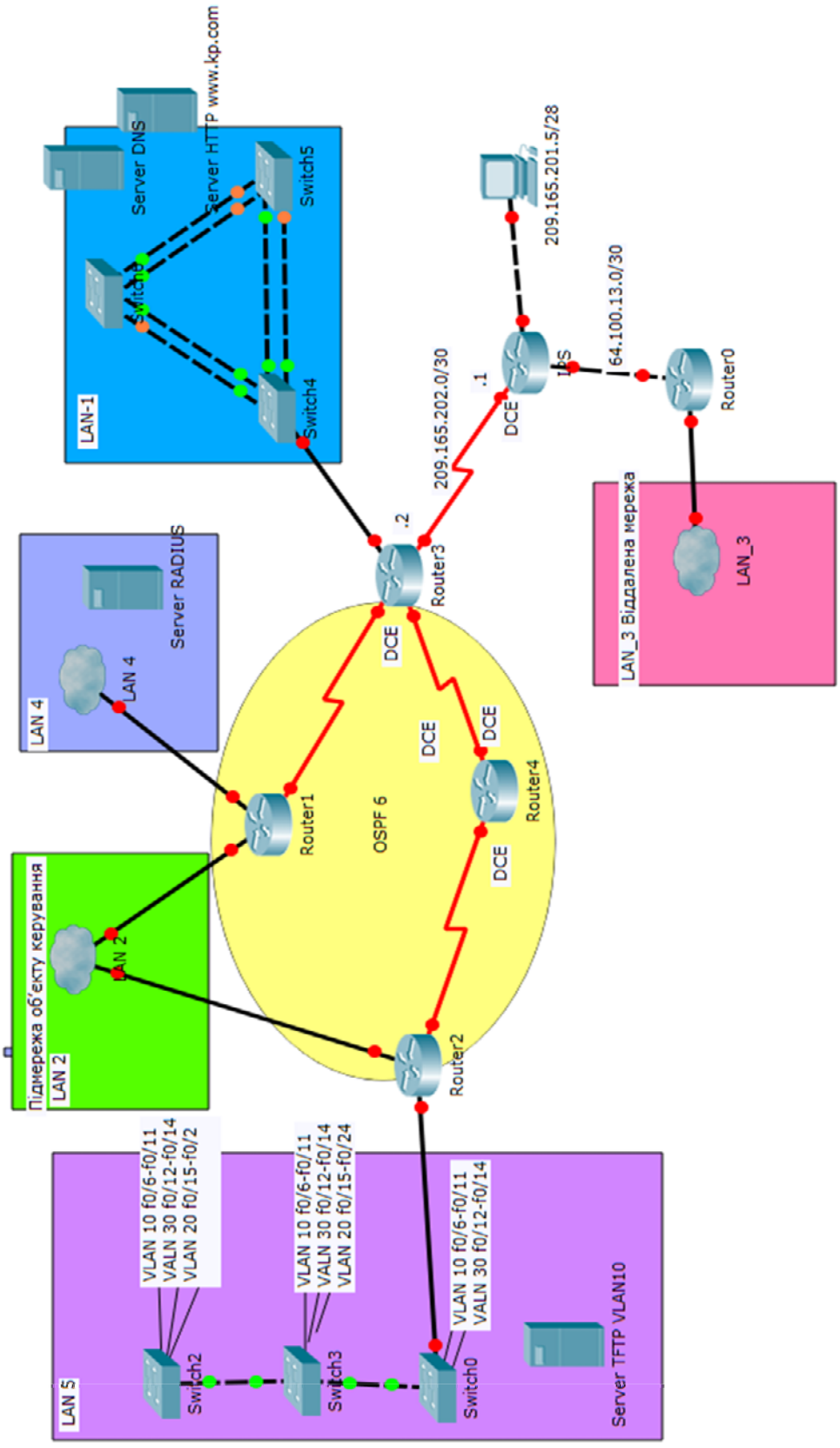


Рисунок 4.1 – Топологія спроектованої мережі

Таблиця 4.4 – Схема адресації пристроїв

Пристрій	Інтер-фейс	IP-адреса	Маска	Шлюз	VLAN	Для ПК інтер-фейс підклю-ченого при-строю
Sinepostol_Router_0	G0/0	64.100.13.2	255.255.255.252	-	-	-
	G0/1	192.168.40.129	255.255.255.128	-	-	-
Sinepostol_Router_1	S0/0/0	10.0.6.1	255.255.255.252	-	-	-
	G0/0	192.168.41.130	255.255.255.128	-	-	-
	G0/1	192.168.41.1	255.255.255.128	-	-	-
Sinepostol_Router_2	S0/0/0	10.0.6.6	255.255.255.252	-	-	-
	G0/0.16	192.168.40.1	255.255.255.224	-	17	-
	G0/0.26	192.168.40.33		-	27	-
	G0/0.36	192.168.40.65		-	37	-
	G0/0.99	192.168.40.97		-	99	-
	G0/1	192.168.41.131	255.255.255.128	-	-	-
Sinepostol_Router_3	S0/0/0	10.0.6.9	255.255.255.252	-	-	-
	S0/0/1	10.0.6.2		-	-	-
	S0/1/0	209.165.202.1		-	-	-
	G0/0	192.168.42.1	255.255.255.192	-	-	-
Sinepostol_Router_4	S0/0/0	10.0.6.5	255.255.255.252	-	-	-
	S0/0/1	10.0.6.10		-	-	-
Sinepostol_Router_IPS	S0/0/0	209.165.202.2		-	-	-
	G0/0	64.100.13.1		-	-	-
	G0/1	209.165.201.6	255.255.255.240			
LAN_1						
Sinepostol_Switch_3	Vlan1	192.168.42.4	255.255.255.192	192.168.42.1	1	-
Sinepostol_Switch_4		192.168.42.3				-
Sinepostol_Switch_5		192.168.42.2				-
PC_1_LAN_1	F0/0	192.168.42.5			-	f0/6
PC_2_LAN_1		192.168.42.6			-	f0/5
PC_3_LAN_1		192.168.42.7			-	f0/5
PC_4_LAN_1		192.168.42.8			-	f0/6
PC_5_LAN_1		192.168.42.9			-	f0/5
PC_6_LAN_1		192.168.42.10			-	f0/6
Server HTTP		192.168.42.17			-	f0/7
Server DNS		192.168.42.16			-	f0/7
LAN_2						
Sinepostol_Switch_6	Vlan1	192.168.41.132	255.255.255.128	192.168.41.129	1	-
PC_1_LAN_2	F0/0	192.168.41.133			-	f0/1
PC_2_LAN_2		192.168.41.134			-	f0/2
PC_3_LAN_2		192.168.41.135			-	f0/3
PC_4_LAN_2		192.168.41.136			-	f0/4
LAN_3						
Sinepostol_Switch_8	Vlan1	192.168.41.130	255.255.255.128	192.168.41.129	1	-
PC_1_LAN_3	F0/0	192.168.41.131			-	f0/1
PC_2_LAN_3		192.168.41.132			-	f0/2
PC_3_LAN_3		192.168.41.133			-	f0/3
PC_4_LAN_3		192.168.41.134			-	f0/4

Продовження таблиці 4.4

LAN_4						
Sinepostol_Switch_7	Vlan1	192.168.41.2	255.255.255.128	192.168.41.1	1	-
Server RADIUS	F0/0	192.168.41.16			-	f0/4
PC_1_LAN_4		192.168.41.3			-	f0/1
PC_2_LAN_4		192.168.41.4			-	f0/2
PC_3_LAN_4		192.168.41.5			-	f0/3
LAN_5						
Sinepostol_Switch_0	Vlan99	192.168.40.98	255.255.255.224	192.168.40.97	99	-
Sinepostol_Switch_1		192.168.40.99			99	-
Sinepostol_Switch_2		192.168.40.100			99	-
PC_1_VLAN_16	F0/0	192.168.40.11		192.168.40.1	16	f0/6
PC_2_VLAN_16		192.168.40.13			16	f0/6
PC_3_VLAN_16		192.168.40.12			16	f0/7
Server TFTP VLAN16		192.168.40.16			16	f0/6
PC_1_VLAN_26		192.168.40.43		192.168.40.33	26	f0/15
PC_2_VLAN_26		192.168.40.44			26	f0/15
PC_1_VLAN_36		192.168.40.75		192.168.40.65	36	f0/12
PC_2_VLAN_36		192.168.40.77			36	f0/12
PC_3_VLAN_36		192.168.40.76			36	f0/12

4.3 Розрахунок налаштувань маршрутизації корпоративної мережі

Розроблену схему мережі та розраховану адресацію реалізовано у вигляді моделі комп'ютерної системи за допомогою інтерфейсу програми Cisco Packet Tracer. Для цього розроблену схему комп'ютерної мережі і представлену адресацію підмереж у табл. 4.2 введено у програму Cisco Packet Tracer. Розраховану схему адресації пристроїв, що представлена у табл. 4.4, перенесено до моделі. Розроблену схему моделі комп'ютерної системи представлено на рис. 4.2.

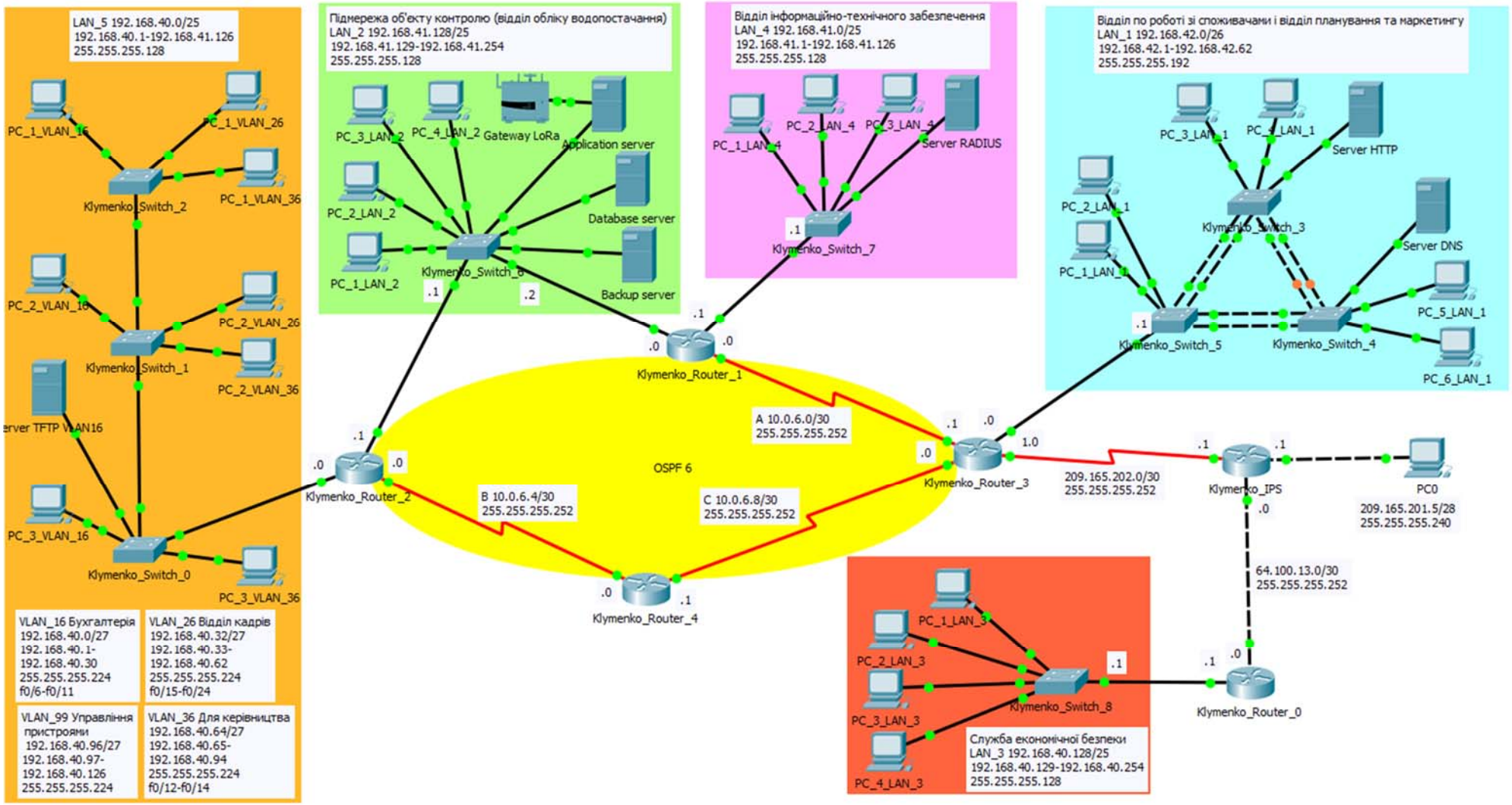


Рисунок 4.2 – Схема моделі комп’ютерної системи

Після проведення всіх операцій з реалізації моделі комп'ютерної системи за допомогою інтерфейсу програми Cisco Packet Tracer було проведено базове налаштування конфігурації пристроїв.

Для пристроїв в мережі була розроблена базова конфігурація відповідно до якої:

− Пристрої отримали назву за певним правилом, що спрощує подальшу роботу з обладнанням та орієнтування в мережі навіть при її збільшенні до доволі великих розмірів.

− На всіх пристроях задано пароль до консолі, vty, а також – пароль до привілейованого режиму, що задовольняє найпростіші вимоги інформаційної безпеки та інформаційний банер, що з'являється перед входом до консолі. Після чого всі паролі були зашифровані.

− На лініях vty налаштовано використання протоколу ssh і локальних облікових записів. SSH – мережевий протокол, який дозволяє забезпечувати віддалене управління операційною системою на мережевих пристроях. За своєю функціональністю схожий з протоколами Telnet і rlogin, але SSH шифрує трафік і паролі, які передаються і саме тому був використаний при конфігуруванні. Для шифрування даних створено ключ RSA завдовжки 1024 біт.

− На портах маршрутизаторів до яких під'єднані підмережі і на serial портах встановлені IP-адреси згідно табл. 4.3.

В додатку наведене програмне забезпечення програмування базового налаштування конфігурації пристроїв, а в додатку Б – програмне забезпечення налаштування мережевих пристроїв системи контролю, що включає в себе базове налаштування конфігурації пристроїв.

4.4 Налаштування та перевірка роботи комп'ютерної системи

4.4.1 Налаштування маршрутизаторів на підтримку служби AAA

Щоб забезпечити більший рівень захисту мережі, окрім використання паролів для доступу до пристроїв, було налаштовано підтримку служби AAA на всіх маршрутизаторах. AAA – система аутентифікації, авторизації і обліку

подій, вбудована в операційну систему Cisco IOS, що служить для надання безпечного доступу до мережного обладнання Cisco. Вона пропонує різні методи ідентифікації користувача, авторизації, а також збору і відправки інформації на сервер.

Для перевірки підключень до VTY ліній на маршрутизаторі вирішено використовувати локальну базу даних користувачів, а для доступу до консолі – аутентифікацію на основі протоколу RADIUS і якщо немає − локальну базу даних. Протокол RADIUS є однією зі складових системи захисту AAA. Він призначений для реалізації аутентифікації, авторизації та збору відомостей про використані ресурсах, використовується для передачі даних між сервером і обладнанням. В мережі налаштований RADIUS-сервер з базою користувачів і ввімкнена аудит і відправку повідомлень про початок і завершення процесу exec.

В додатку А наведений приклад програмного забезпечення програмування налаштування маршрутизаторів на підтримку служби AAA, а в додатку Б – програмне забезпечення налаштування мережевих пристроїв системи контролю, що включає в себе налаштування маршрутизаторів на підтримку служби AAA.

4.4.2 Налаштування об’єднання фізичних портів

З метою збільшення пропускної здатності і надійності каналів в мережі LAN_1для відділу по роботі зі споживачами і відділу планування та маркетингу на комутаторах виконано об’єднання фізичних портів. Дану можливість надає технологія EtherChannel, яка дозволяє об’єднувати декілька фізичних портів на комутаторах в один логічний. Головна перевага такого каналу збільшення швидкості передачі даних. У плані надійності EtherChannel відрізняється від використання протоколу Spanning Tree тим, що якщо в STP пропадає якийсь лінк, то починається перерахунок топології, що займає якийсь час, після чого, резервний канал вводиться в дію, у випадку EtherChannel, топологія не змінюється, просто дещо зменшується швидкість каналу. Іншими словами,

EtherChannel не рятує від необхідності використовувати Spanning Tree, але в разі, якщо лінк пропадає саме на агрегованій ділянці, позбавляє від необхідності перерахунку топології.

В додатку А наведена реалізація програмного забезпечення програмування налаштування об’єднання фізичних портів, а в додатку Б – програмне забезпечення налаштування мережевих пристроїв системи контролю, що включає в себе налаштування об’єднання фізичних портів.

4.4.3 Налаштування мереж VLAN, параметрів безпеки комутаторів та адресації ПК в мережах VLAN

VLAN (Virtual Local Area Network, віртуальна локальна мережа) – це функція в роутерах і комутаторах, що дозволяє на одному фізичному мережевому інтерфейсі (Ethernet, Wi-Fi інтерфейсі) створити кілька віртуальних локальних мереж. VLAN використовується для створення логічної топології мережі, яка ніяк не залежить від фізичної топології.

Переваги використання VLAN:

- Гнучкий поділ пристроїв на групи – одному VLAN відповідає одна підмережа. Комп’ютери, що знаходяться в різних VLAN ізольовані один від одного. Також можна об’єднати в одну віртуальну мережу комп'ютери, підключені до різних комутаторів.
- Зменшення широкомовного трафіка в мережі – кожен VLAN представляє окремий широкомовний домен. Широкомовний трафік не буде транслюватися між різними VLAN. Якщо на різних комутаторах налаштувати один і той же VLAN, то порти різних комутаторів будуть утворювати один широкомовний домен.
- Збільшення безпеки і керованості мережі – у мережі, розбитою на віртуальні підмережі, зручно застосовувати політики та правила безпеки для кожного VLAN. Політика застосовується до цілої підмережі, а не до окремого пристрою.

– Зменшення кількості обладнання та мережевого кабелю – для створення нової віртуальної локальної мережі не потрібно купувати комутатор і прокладати мережевий кабель. Однак в такому випадку потрібно використовувати більш дорогі комутатори з підтримкою VLAN.

Найбільшу підмережу LAN_5 було вирішено розділити на VLAN і розмістити в них бухгалтерію, відділ кадрів, керівництво. Дане рішення було прийнято оскільки ці групи володіють важливими даними і повинні бути відокремлені від решти пристроїв мережі при взаємодії один з одним, завдяки чому знизиться ймовірність витоку конфіденційної інформації. Дані про мережі VLAN внесені до табл. 4.3.

Використовуючи табл. 4.3 в LAN_5 були створені мережі VLAN і присвоєне кожній з них ім’я.

Таблиця 4.5 – Мережі VLAN

Номер VLAN	Ім’я VLAN	Примітка
1	default	Не використовується
16	Accounting	Для бухгалтерії
26	Resources Department	Для відділу кадрів
36	Guest	Для керівництва
99	Management	Для управління пристроями
100	Native	Власна

В даній підмережі для маршрутизації даних між VLAN налаштований маршрутизатор Sinepostol_Router_2 router on a stick за допомогою sub-interface на порті gig0/0, який виступає в якості транкового порта 802.1Q. Транковий порт – це канал через який передається трафік всіх VLAN. Він не належить до жодної VLAN і передає тегований трафік. Транкові канали створені між комутаторами, а також між комутатором і маршрутизатором.

Для адресації ПК в мережах VLAN використовується маршрутизатор Sinepostol_Router_2, що виступає в якості DHCP-серверу. Цей підхід спрощує процес конфігурування пристроїв в доволі великій підмережі.

DHCP – це протокол, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі. Протокол DHCP працює за схемою клієнт-сервер. Під час запуску системи комп'ютер, який є DHCP-клієнтом, відправляє в мережу запит на отримання IP-адреси. DHCP-сервер відповідає і відправляє повідомлення-відповідь, яка містить IP-адресу і деякі інші конфігураційні параметри.

Для кожної VLAN створені пули з яких комп'ютери будуть отримувати адреси. Для пулу вказана адреса DNS-сервера і шлюз за замовчуванням, які будуть роздаватися з адресами як додаткові конфігураційні параметри .

Додатковий захист інформації на серверах в усіх підмережах надає функція безпеки портів на комутаторах під назвою port security. Суть цієї функції полягає у тому, що тим чи іншим способом, для кожного порту обмежується список (або кількість) MAC-адрес, які на ньому можуть з'являтися, якщо на порту помічено занадто багато адрес, то порт може відреагувати вимкненням або відкидування пакетів, що приходять на порт.

Серед можливих варіантів захисту були обрані:

- тільки двом унікальним пристроям дозволений доступ до порту;
- MAC-адреса пристрою розпізнається динамічна і додається в поточну конфігурацію;
- під час порушення системи безпеки з'являється повідомлення, а порт залишається включеним.

Функція безпеки портів була використана на Sinepostol_Switch_0, Sinepostol_Switch_3, Sinepostol_Switch_4 і Sinepostol_Switch_7, а саме на портах до яких приєднані сервери.

В додатку А представлено програмне забезпечення програмування налаштування мереж VLAN, параметрів безпеки комутаторів та адресації ПК в мережах VLAN, а в додатку Б – програмне забезпечення налаштування мережевих пристроїв системи контролю, що включає в себе налаштування мереж VLAN, параметрів безпеки комутаторів та адресації ПК в мережах VLAN.

4.4.4 Включення протоколу маршрутизації

Для маршрутизації трафіку в проекті була реалізована динамічна маршрутизація представлена протоколом OSPF.

OSPF – протокол динамічної маршрутизації, заснований на технології відстеження стану каналу (link-state technology), що використовує для знаходження найкоротшого шляху алгоритм Дейкстри.

Опис роботи протоколу:

- маршрутизатори обмінюються hello-пакетами через всі інтерфейси, на яких активований OSPF. Маршрутизатори, що розділяють загальний канал передачі даних, стають сусідами, коли вони приходять до домовленості при певних параметрах, зазначених в їх hello-пакетах;
- на наступному етапі роботи протоколу маршрутизатори намагаються перейти в стан суміжності зі своїми сусідами. Перехід у стан суміжності визначається типом маршрутизаторів, які обмінюються hello-пакетами, і типом мережі, по якій передаються hello-пакети. OSPF визначає кілька типів мереж і кілька типів маршрутизаторів. Пара маршрутизаторів, що знаходяться в стані суміжності, синхронізують між собою бази даних стану каналів;
- кожен маршрутизатор посилає оголошення про стан каналу маршрутизаторам, з якими він знаходиться в стані суміжності;
- кожен маршрутизатор, який отримав оголошення від суміжного маршрутизатора, записує передану в ньому інформацію в базу даних стану каналів маршрутизатора і розсилає копію оголошення всім іншим суміжним з ним маршрутизаторам;
- розсилаючи оголошення всередині однієї OSPF-зони, всі маршрутизатори будують ідентичну базу даних стану каналів маршрутизатора;
- коли база даних побудована, кожен маршрутизатор використовує алгоритм “найкоротший шлях першим” для обчислення графа без

петель, який буде описувати найкоротший шлях до кожного відомого пункту призначення із собою як кореня. Цей граф – дерево найкоротших шляхів;

– кожен маршрутизатор будує таблицю маршрутизації зі свого дерева найкоротших шляхів.

При налаштуванні протоколу на кожному маршрутизаторі оголошені тільки безпосередньо підключені мережі та відключено поширення оновлень маршрутизації на інтерфейси в локальні мережі, тому що відправка повідомлень OSPF в мережу LAN має наступні наслідки для мережі:

– Неефективне використання пропускної здатності – доступна пропускна здатність використовується для передачі непотрібних повідомлень.
– Неефективне використання ресурсів – всі пристрої в мережі LAN повинні обробити повідомлення і згодом видалити його.
– Підвищений ризик для інформаційної безпеки – оголошення оновлень широкомовної розсилки є загрозою інформаційної безпеки мережі. OSPF-повідомлення можуть бути перехоплені програмами для аналізу мережевих протоколів. Оновлення маршрутизації можна змінити і відправити їх на маршрутизатор, що дозволить пошкодити таблиці маршрутизації через наявність невірних метрик за допомогою яких трафік може бути направлений в будь-якому напрямку.

На маршрутизаторі Sinepostol_Router_3 з прямим підключенням до інтернет-провайдера налаштований маршрут за умовчанням і розповсюджений через оновлення маршрутизації. Даний статичний маршрут призначений для отримання доступу до інтернету (якщо адресі призначення з пакету на маршрутизаторі не буде відповідати жоден маршрут в таблиці маршрутизації, то пакет буде відправлений по даному статичному маршруту останньої надії).

Для зменшення таблиць маршрутизації і відповідно навантаження на процесор, пам’ять маршрутизуючого обладнання і смуги пропускання, якими користується OSPF, було проведене підсумовування маршрутів. Дані зміни

досягнуті за рахунок того, що без підсумовування кожне оновлення маршрутизації в одній зоні передається в зону 0, а при підсумовуванні тільки сумарні маршрути потрапляють в зону 0. Також це дає можливість масштабувати мережу до дуже великих розмірів.

Розрахований сумарний маршрут для мережі загалом представлений в табл. 4.6, а сумарний маршрут для VLAN – в табл. 4.7.

Таблиця 4.6 – Підсумовування адрес мережі

Назва підмережі	Адреса підмереж у двійковому форматі	Адреса підмереж у десятковому форматі	Префікс
LAN_5	192.168.00101000.00000000	192.168.40.0	/25
VLAN 16	192.168.00101000.00000000	192.168.40.0	/27
VLAN 26	192.168.00101000.00100000	192.168.40.32	/27
VLAN 36	192.168.00101000.01000000	192.168.40.64	/27
VLAN 99	192.168.00101000.01100000	192.168.40.96	/27
LAN_3	192.168.00101000.10000000	192.168.40.128	/25
LAN_4	192.168.00101001.00000000	192.168.41.0	/25
LAN_2	192.168.00101001.10000000	192.168.41.128	/25
LAN_1	192.168.00101010.00000000	192.168.42.0	/26
Сумарний маршрут	192.168.001010|00.00000000	192.168.40.0	/22

Таблиця 3.7 – Підсумовування адрес VLAN

Назва підмережі	Адреса підмереж у двійковому форматі	Адреса підмереж у десятковому форматі	Префікс
VLAN 16	192.168.00101000.00000000	192.168.40.0	/27
VLAN 26	192.168.00101000.00100000	192.168.40.32	/27
VLAN 36	192.168.00101000.01000000	192.168.40.64	/27
VLAN 99	192.168.00101000.01100000	192.168.40.96	/27
Сумарний маршрут	192.168.00101000.0|0000000	192.168.40.0	/25

Підмережа об’єкту керування забезпечена основною і резервною лінією для передачі даних і відповідно двома маршрутизаторами Sinepostol_Router_1 і Sinepostol_Router_2. Для коректного вибору шлюзу за умовчанням при передачі даних на пристроях був налаштований протокол HSRP. Даний протокол вибирає з групи маршрутизаторів один active і один standby маршрутизатори. Якщо є інші маршрутизатори, то вони виступають як члени групи.

Активний маршрутизатор відповідає за пересилку пакетів. Standby-маршрутизатор займе місце активного маршрутизатора в разі відмови останнього. Маршрутизатор з найбільшим пріоритетом, з решти членів групи, в цьому випадку, буде обраний в якості standby. Вибори проводяться на підставі пріоритету маршрутизатора, який може змінюватися в межах від 1 до 255 (значення за замовчуванням рівне 100).

Якщо жодному з маршрутизаторів в групі не був призначений пріоритет, то пріоритети всіх маршрутизаторів співпадуть і активним в цьому випадку стане маршрутизатор з найбільшою IP-адресою інтерфейсу на якому налаштований HSRP. В процесі роботи active і standby маршрутизатори обмінюються hello-повідомленнями. Якщо протягом 10 секунд (три тривалості hello-) немає жодного hello-повідомлення від активного маршрутизатора, резервний маршрутизатор бере на себе роль активного маршрутизатора.

При підключенні нового маршрутизатора до вже існуючої групи він буде обраний в якості active при наявності більшого пріоритету, оскільки налаштована опція preempt.

В додатках наведене програмне забезпечення програмування включення протоколу маршрутизації, та програмне забезпечення налаштування мережевих пристроїв системи контролю, що включає в себе включення протоколу маршрутизації.

Таблиці маршрутизації всіх маршрутизаторів наведені в також в додатках.

4.4.5 Налаштування роботи Інтернет

Для того, щоб всі робочі станції організації мали вихід в Інтернет на прикордонному маршрутизаторі Sinepostol_Router_3 був використаний NAT з урахуванням виділеного пулу зовнішніх адрес, які починаються з 209.165.200.5 по 209.165.200.30 та адреси 209.165.200.4 для серверу HTTP.

NAT – це механізм зміни мережевої адреси в заголовках IP датаграм, поки вони проходять через маршрутизуючий пристрій з метою відображення

одного адресного простору в інший. Завдяки NAT можна, використовуючи одну або кілька зовнішніх IP-адрес, виданих провайдером, підключити до мережі практично будь-яку кількість комп'ютерів.

Принцип роботи даного механізму:

- користувач мережі відправляє запит в Інтернет, який надходить на внутрішній інтерфейс маршрутизатора (пристрій NAT);
- пристрій NAT отримує пакет і робить запис в таблиці відстеження з'єднань, яка управляє перетворенням адрес;
- потім підміняє адресу джерела пакету зовнішньою загальнодоступним IP-адресом і посилає пакет за місцем призначення в Інтернет;
- вузол призначення отримує пакет і передає відповідь назад пристрою NAT;
- пристрій NAT, в свою чергу, отримавши цей пакет, відшукує відправника вихідного пакета в таблиці відстеження з'єднань, замінює IP-адресу призначення на відповідну приватну IP-адресу і передає пакет на вихідний комп'ютер.

У випадку з сервером був використаний статичний NAT. Він виконує трансляцію однієї локальної IP-адреси в одну глобальну IP-адресу. Використовується для того, щоб до серверу був постійний доступ з зовнішньої мережі.

Незахищена передача даних між підмережею відділу обліку водопостачання і віддаленою мережею служби економічної безпеки може спричинити витік важливої внутрішньої інформації, що призведе до непередбачуваних наслідків, серед яких втрата конкурентоспроможності і серйозні фінансові втрати. У зв'язку з цим виникає необхідність забезпечення безпечної передачі інформації між Sinepostol_Router_3 і Sinepostol_Router_0, що досягається шляхом налаштування VPN з використанням технології IPSec.

VPN (Віртуальна приватна мережа, англ. Virtual Private Network) – сімейство технологій, що дозволяють будувати логічну мережу, створену поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі

може реалізуватися за допомогою шифрування, в наслідок чого створюється закритий для сторонніх канал обміну інформацією.

Для організації шифрованого VPN-каналу використовується технологія IPSec (IP Security). IP Security – це комплект протоколів, що стосуються питань шифрування, аутентифікації і забезпечення захисту при транспортуванні IP-пакетів.

Щоб створити захищене з'єднання в IPSec учасникам треба домовиться, які механізми захисту вони будуть використовувати для свого захищеного з'єднання. За реалізацію процесу відповідає протокол IKE. IKE (Internet Key Exchange protocol – протокол обміну ключами) використовується для формування IPSec SA (Security Association – узгодження роботи учасників захищеного з'єднання).

Процес складається з двох фаз. В першій фазі учасники аутентифікують один одного і домовляються про параметри встановлення спеціального з'єднання (теж захищеного), призначеного лише для обміну інформацією про бажані алгоритми шифрування і інші деталі майбутнього IPSec-тунеля. Параметри цього міні-тунелю (ISAKMP Tunnel) визначаються політикою ISAKMP. При формуванні політики пропонуються наступні параметри для узгодження:

- Метод аутентифікації (з використанням електронного підпису або визначених ключів).
- Алгоритм шифрування повідомлень, що використовується в рамках протоколу IKE.
- Хеш-алгоритм, який використовується в рамках протоколу IKE.
- Алгоритм, який буде використовуватися для забезпечення безпечного обміну ключами, які використовуються для шифрування даних.

Якщо сторони дійшли згоди, встановлюється ISAKMP тунель за яким вже проходить друга фаза IKE. Коли учасники вже довіряють один одному, то вони домовляються про те, як будувати основний тунель для даних. Вони по черзі пропонують один одному варіанти, зазначені в сформованому наборі пе-

ретворень і якщо приходять до згоди, то формується основний тунель. Після його встановлення, допоміжний ISAKMP тунель нікуди не пропадає – він використовується для поновлення SA основного.

Весь процес створення тунелю відбувається з урахування правил, які знаходяться в криптографічній карті. При створенні криптографічної карти використовуються наступні параметри:

- Прив’язка списку доступу до запису криптографічної карти.
- Адреса партнера з яким буде встановлюватися тунель.
- Встановлення опції PFS. Використання даної опції дозволяє підвищити рівень захищеності трафіку – при створенні кожного IPSec SA відбуватиметься регулярна подача нових сесійних ключів.
- Ім’я раніше створеного набору перетворень.

В додатку наведено групу команд для налаштування доступу в Інтернет та віртуальної приватної мережі.

В додатку наведене програмне забезпечення програмування налаштування доступу в Інтернет та віртуальної приватної мережі, також – програмне забезпечення налаштування мережевих пристроїв системи контролю, що включає в себе налаштування доступу в Інтернет та віртуальної приватної мережі.

4.4.6 Перевірка роботи комп’ютерної системи

На рис 4.15 зображена таблиця маршрутизації на Sinepostol_Router_3 в якій містяться мережі з типом “O” і це означає, що протокол OSPF працює коректна і отримав інформацію про мережі від кожного маршрутизатора.

Type	Network	Port	Next Hop IP	Metric
S	0.0.0.0/0	---	209.165.202.2	1/0
O	10.0.6.4/30	Serial0/0/0	10.0.6.10	110/15000
O	192.168.40.0/27	Serial0/0/0	10.0.6.10	110/15001
O	192.168.40.32/27	Serial0/0/0	10.0.6.10	110/15001
O	192.168.40.64/27	Serial0/0/0	10.0.6.10	110/15001
O	192.168.40.96/27	Serial0/0/0	10.0.6.10	110/15001
O	192.168.41.0/25	Serial0/0/1	10.0.6.1	110/7501
O	192.168.41.128/25	Serial0/0/1	10.0.6.1	110/7501

Рисунок 4.15 – Таблиця маршрутизації на Sinepostol_Router_3

Коротка інформація про групу реалізовану протоколом HSRP на рис. 4.16 і 4.17 свідчить про те, що шлюзи на маршрутизаторах знаходяться в першій групі в активному стані і в режимі очікування відповідно та мають інформацію один про одного і однакову віртуальну адресу, що гарантує правильність роботи протоколу HSRP.

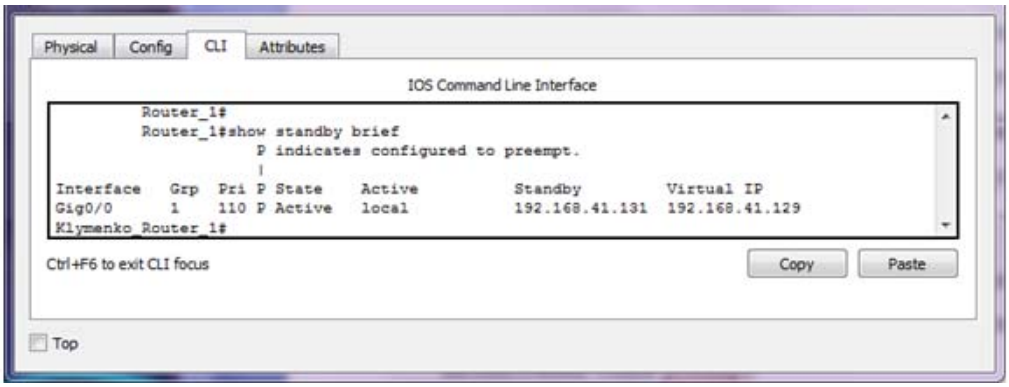


Рисунок 4.16 – Інформація про активний шлюз першої групи HSRP на Sinepostol_Router_1

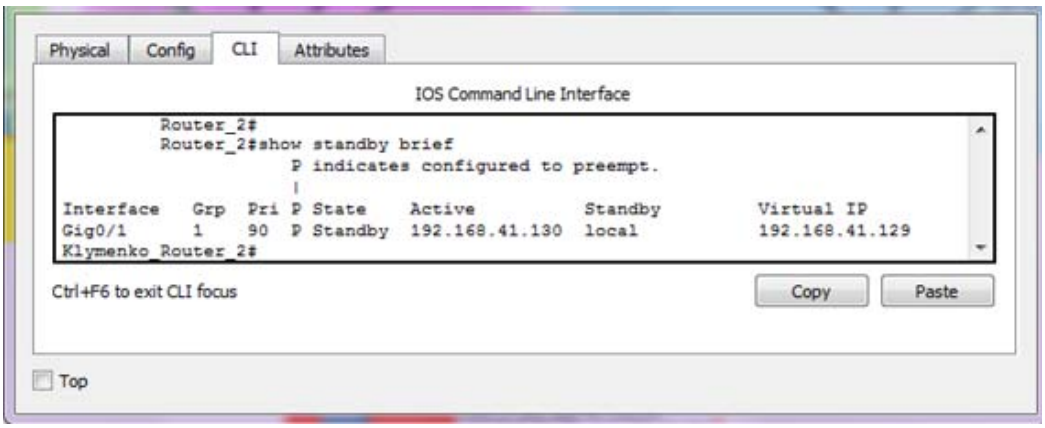


Рисунок 4.17 – Інформація про шлюз в режимі очікування першої групи HSRP на Sinepostol_Router_2

На рис. 4.18 зображений пакет з запитом на дозвіл доступу відправлений на RADIUS сервер.

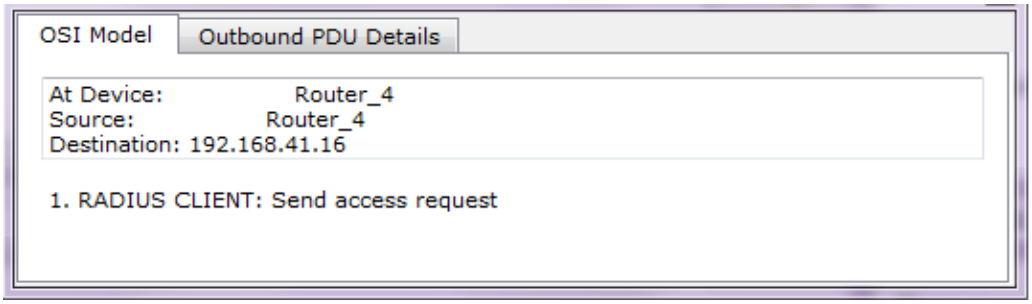


Рисунок 4.18 – Пакет з інформацією для проходження аутентифікації від Sinepostol_Router_4

Оскільки аутентифікація була пройдена, то RADIUS сервер відповів пакетом зі згодою на рис. 4.19. За можливість взаємодії маршрутизаторів з RADIUS сервером та реалізацію аутентифікації відповідає протокол AAA.

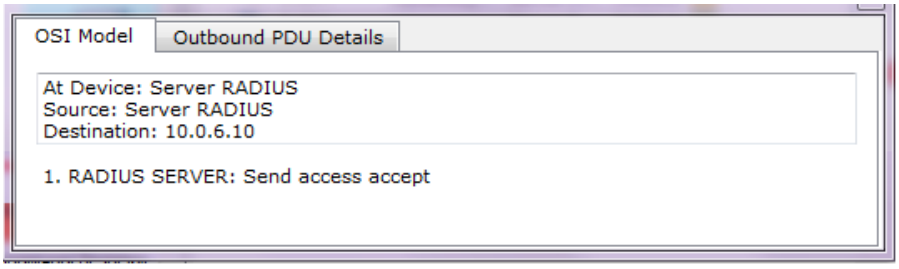


Рисунок 4.19 – Пакет зі згодою на доступ до пристрою від RADIUS сервера

Рис. 4.20 вказує на те, що відбулось об’єднання фізичних портів, по двоє в одну групу, технологією EtherChannel відповідно до використаних налаштувань.

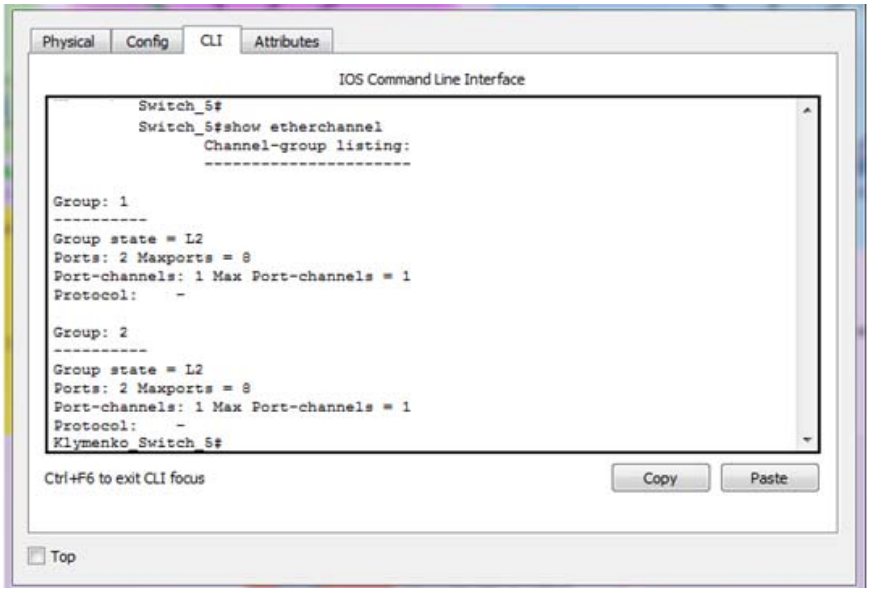


Рисунок 4.20 – Група 1 та 2 на Sinepostol_Switch_5

На прикладі Sinepostol_Switch_0 підтверджено створення VLAN та розподіл портів між ними, що зображено на рис. 4.21, а також створення транкових портів для обміну даними між VLAN – на рис. 4.22.

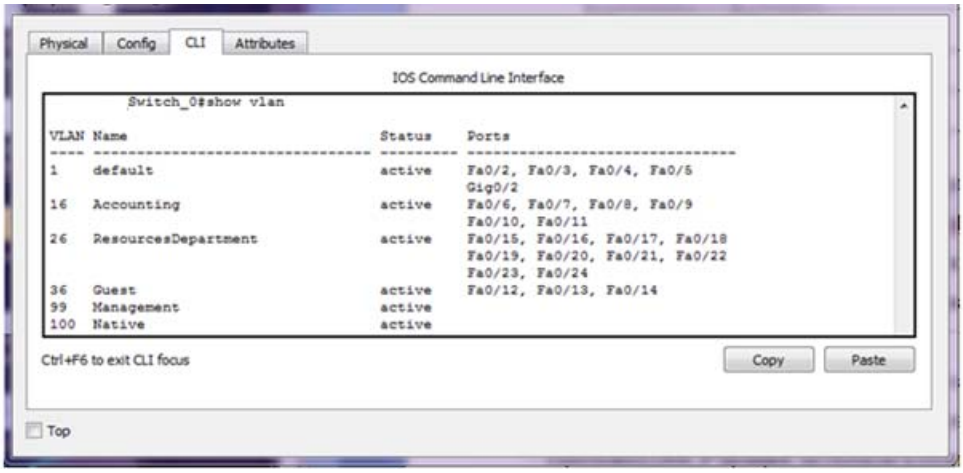


Рисунок 4.21 – Створені VLAN і розподіл портів між ними на Sinepostol_Switch_0

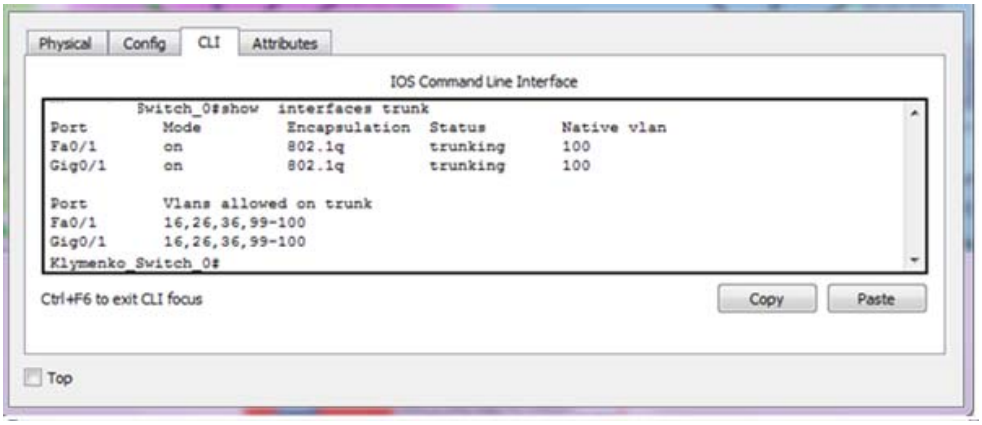


Рисунок 4.22 – Транкові порти на Sinepostol_Switch_0

На Sinepostol_Router_2 відбувся розподіл інтерфейсу GigabitEthernet0/0 на підінтерфейси і кожен має назначену IP-адресу, що гарантує маршрутизацію між VLAN. Ці дані вказані на рис. 4.23.

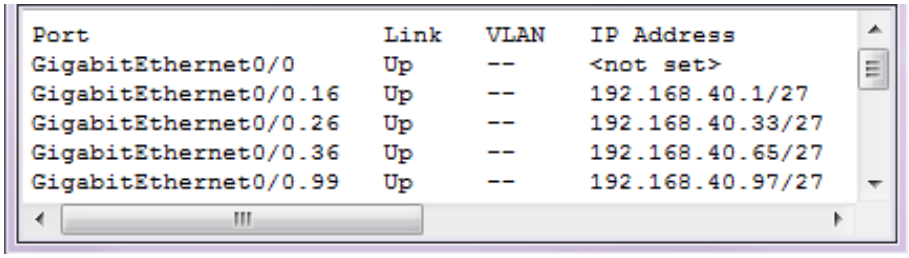


Рисунок 4.23 – Порти для маршрутизації між VLAN на Sinepostol_Router_2

Комп’ютер PC_3_VLAN_36 відправив запит на DHCP сервер для отримання даних IP конфігурації, що вказано на рисунку 3.24. Після чого він отримав пакет відповідь з необхідними даними виданими відповідно до виділеного пулу адрес, що свідчить про коректність використаних налаштувань. Отримана IP конфігурація – на рис. 4.25.

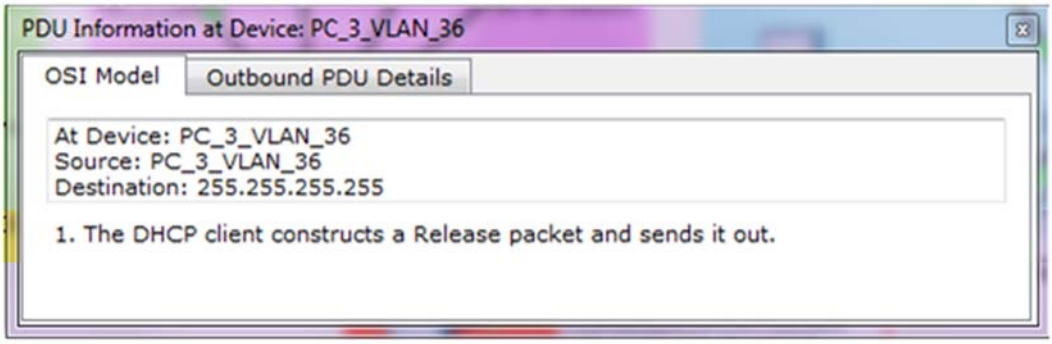


Рис. 4.24 – Пакет від PC_3_VLAN_36 з запитом на отримання IP-адреси від DHCP сервера

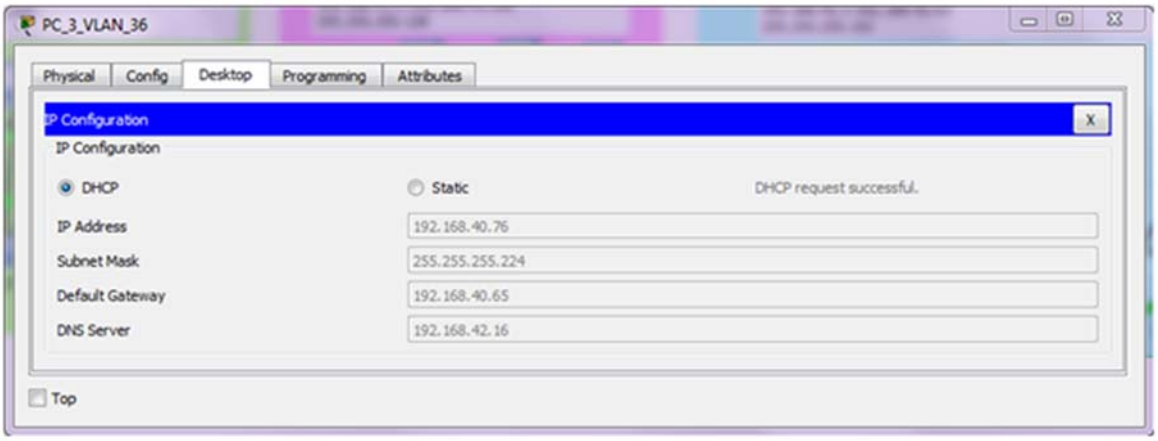


Рисунок 4.25 – IP конфігурація отримана від DHCP сервера

На рис. 4.26 відображена таблиця NAT на Sinepostol_Router_3 в якій вказані підміни адрес при проходженні через маршрутизатор для доступу до Інтернету та статичний NAT для серверу. Дана інформація в таблиці говорить про те, що пакети отримують глобальні адреси і дані про підімну зберігаються і це вказує на правильну роботу NAT.

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.200.5:1032	192.168.40.77:1	192.168.40.133:1	192.168.40.133:1032
icmp	209.165.200.5:1	192.168.41.4:1	192.168.40.133:1	192.168.40.133:1
icmp	209.165.200.5:1029	192.168.41.5:1	192.168.40.131:1	192.168.40.131:1029
icmp	209.165.200.5:1033	192.168.41.5:2	64.100.13.2:2	64.100.13.2:1033
icmp	209.165.200.5:1025	192.168.42.7:1	192.168.40.134:1	192.168.40.134:1025
icmp	209.165.200.5:2	192.168.42.7:2	64.100.13.2:2	64.100.13.2:2
icmp	209.165.200.5:1030	192.168.42.8:1	209.165.201.7:1	209.165.201.7:1030
icmp	209.165.200.5:1026	192.168.42.9:1	209.165.201.7:1	209.165.201.7:1026
---	209.165.200.4	192.168.42.17	---	---

Рисунок 4.26 – Таблиця NAT на Sinepostol_Router_3

Інформація на рис. 4.27 та 4.28 вказує на те, що між двома вузлами був створений захищений VPN тунель.

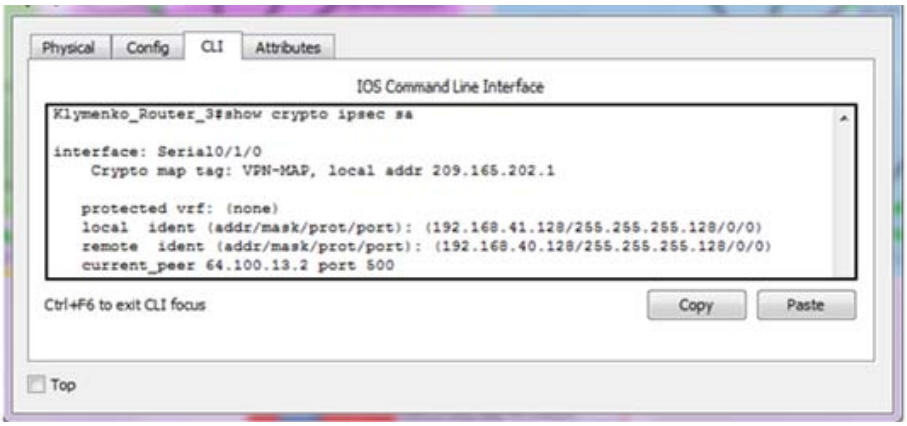


Рисунок 4.27 – Інформація про IPSec VPN тунель на Sinepostol_Router_3

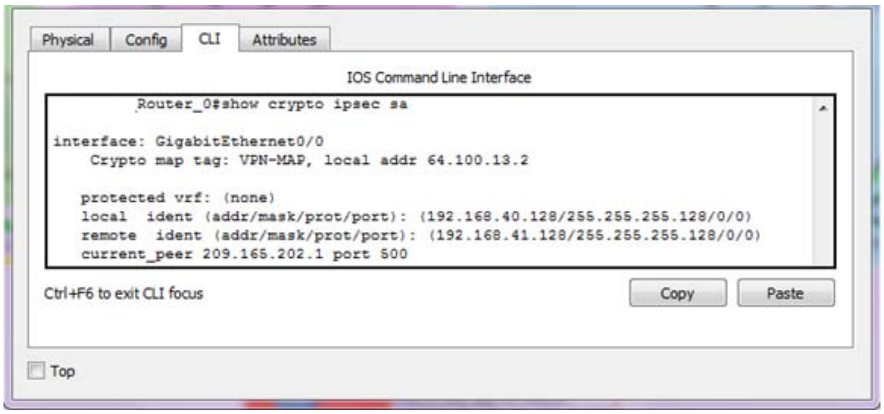


Рисунок 4.28 – Інформація про IPSec VPN тунель на Sinepostol_Router_0

Пакет на рис. 4.29 має два заголовки протоколу IP, а це означає, що пакет потрапляє до VPN тунелю, що в свою чергу говорить про правильність налаштування VPN та його коректну роботу.

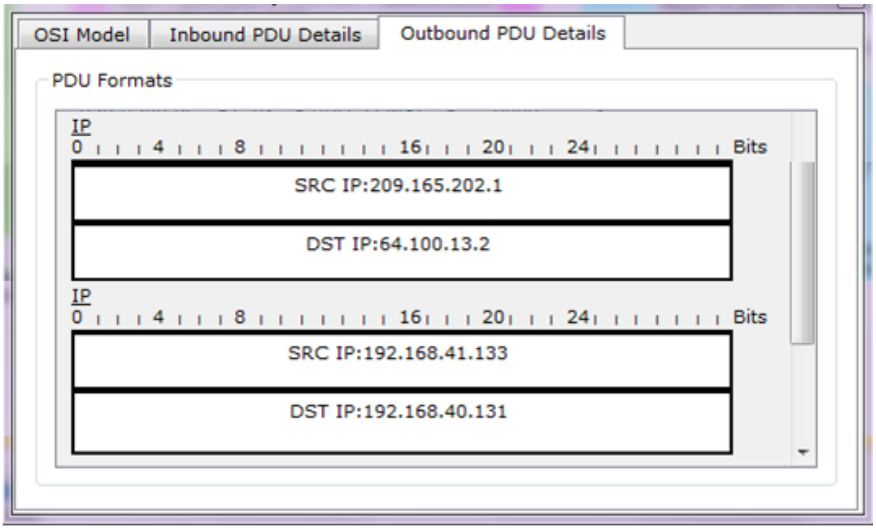


Рисунок 4.29 – Пакет з двома заголовками протоколу IP

4.5 Висновок за розділом

Розроблена комп’ютерної системи з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову системи контролю роботи коксохімічного підприємства, а також для збору і підготовки статистичної інформації.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота.

5 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

5.1 Розробка методів для захисту інформації в комп'ютерній системі підрозділів ВНЗ

Для захисту інформації в комп'ютерній системі підрозділів заводу використовуються наступні методи:

- налаштування мереж VLAN і маршрутизації між ними;
- На портах комутаторів, підключених до серверів, налаштувати функцію безпеки портів.

5.2 Налаштування мереж VLAN

Оскільки підприємстві працює багато відділів, виникла необхідність розділити користувачів в мережі LAN_3 на три групи по виконуваних ними функціями, незалежно від їх фізичного розташування. Таким чином потрібно сегментувати мережу LAN_3 на три підмережі для наступних груп користувачів: Дирекція, Відділ адміністрування обчислювальних систем (ВАОС), Рядові співробітники. Організація не погоджується на придбання додаткового обладнання, тому було прийнято рішення реалізувати поставлену задачу за допомогою віртуальних локальних мереж (VLAN) на існуючих комутаторах. Таблиця VLAN і призначень портів представлена в табл. 5.1.

Таблиця 5.1 – Мережі VLAN и призначень портів

Номер VLAN	Ім'я VLAN	Порт	Примітка
1	Default	-	Не використовується
28	Rectorat	Sinepostol_Switch_0 – fa0/1-2 Sinepostol_Switch_1 – fa0/1-2 Sinepostol_Switch_16 – fa0/1-2	Для «Ректорату»
38	Admins	Sinepostol_Switch_1 – fa0/3-5 Sinepostol_Switch_16 – fa0/3-5	Для «ІКК»

Продовження таблиці 5.1

Номер VLAN	Ім’я VLAN	Порт	Примітка
48	Ordinary_empoyees	Sinepostol_Switch_0 – fa0/6-18 Sinepostol_Switch_1 – fa0/6-18 Sinepostol_Switch_16 – fa0/6-18	Для «Рядові співробітники»
99	Management	SVI	Для управління пристроями
100	Native	Sinepostol_Switch_0 – Gig0/1-2 Sinepostol_Switch_1 – Gig0/1-2 Sinepostol_Switch_16 – Gig0/1	Транковый канал 802.1Q

Таблиця схеми адресації підмереж VLAN представлена в табл. 5.2

Таблиця 5.2 – схеми адресації підмереж VLAN

Назва підмережі	Необхідний Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес
Rectorat	6	6	192.168.144.112	255.255.255.248	192.168.144.113 - 192.168.144.118
Admins	5	6	192.168.144.120	255.255.255.248	192.168.144.121 - 192.168.144.126
Ordinary_empoyees	29	30	192.168.144.64	255.255.255.224	192.168.144.65 - 192.168.144.94
Management	4	6	192.168.144.96	255.255.255.248	192.168.144.97 - 192.168.144.102
Native	4	6	192.168.144.104	255.255.255.248	192.168.144.105 - 192.168.144.110

В табл. 5.3 продемонстровані використані команди для налаштування VLAN 28 на прикладі комутатора Sinepostol_Switch_1. Аналогічне налаштування виконується для інших мереж VLAN на відповідних портах.

Таблиця 5.3 – команди для базового налаштування пристроїв

Команда	Функції команди
Sinepostol_Switch_1(config)#vlan 28	Створення мережі VLAN 28
Sinepostol_Switch_1(config-vlan)# name Directorate	Надання імені мережі VLAN 28
Sinepostol_Switch_1(config)# interface range FastEthernet0/1-2	Вибір інтерфейсів для налаштувань
Sinepostol_Switch_1(config-if)# switchport mode access	Налаштування портів в якості портів доступу
Sinepostol_Switch_1(config-if)# switchport access vlan 28	призначте портам мережі VLAN
Sinepostol_Switch_1 (config)#vlan 100 *Sinepostol_Switch_1 (config-vlan)#name Native*	Налаштування мережі VLAN 100 як native VLAN
Sinepostol_Switch_1 (config)#interface range Gig0/1-2 *Sinepostol_Switch_1 (config-if)#switchport mode trunk* *Sinepostol_Switch_1 (config-if)#switchport trunk native vlan 100* *Sinepostol_Switch_1 (config-if)#switchport trunk allowed vlan 28,38,48,100*	Налаштування інтерфейсів між комутаторами для створення транкових каналів

5.3 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

Для налаштування маршрутизації у мережах VLAN було прийняте рішення використати протокол динамічного налаштування вузлів DHCP. Таке рішення було прийняте у зв’язку з можливим розширенням ВНЗ у майбутньому. Для використання даного протоколу, налаштуємо маршрутизатор Sinepostol_ Router _3 у якості DHCP-сервера. В табл. 5.4 продемонстровані використані команди для налаштування маршрутизації VLAN 38. Аналогічне налаштування виконується для інших мереж VLAN.

Таблиця 5.4 – команди для налаштування маршрутизації у мережах VLAN

Команда	Функції команди
Sinepostol_Router_3(config)#ip dhcp pool pollvlan38	Створення пулу DHCP
Sinepostol_Router_3(dhcp-config)#network 192.168.144.120 255.255.255.248	Вказання пулу адрес для використання
Sinepostol_Router_3(dhcp-config)#default-router 192.168.144.121	Налаштування шлюзу за замовчуванням
Sinepostol_Router_3(dhcp-config)#dns-server 192.168.144.92	Налаштування адреси DNS-серверу
Sinepostol_Router_3(config)#ip dhcp excluded-address 192.168.144.121 *Sinepostol_Router_3(config)#ip dhcp excluded-address 192.168.144.122* *Sinepostol_Router_3(config)#ip dhcp excluded-address 192.168.144.123* *Sinepostol_Router_3(config)#ip dhcp excluded-address 192.168.144.124*	Виключення адрес з пулу

На портах комутаторів, підключених до серверів, необхідно налаштувати функцію безпеки портів. В табл. 5.5 наведені відповідні команди.

Таблиця 5.5 – команди для налаштування функції безпеки портів

Команда	Функції команди
Sinepostol_Switch_1(config-if)#switchport mode access	Переведення порту в режим доступу
Sinepostol_Switch_1(config-if)#switchport port-security	Увімкнення port security на інтерфейсі
Sinepostol_Switch_1(config-if)#switchport port-security max 2	Дозвіл доступу до порту тільки двом унікальним пристроям
Sinepostol_Switch_1(config-if)#sw port mac-address sticky	Розпізнавання MAC-адреси пристрою динамічно і додавання в поточну конфігурацію
Sinepostol_Switch_1(config-if)#sw port violation restrict	Поява повідомлення під час порушенні системи безпеки та залишання порту включеним

6 ЕКОНОМІЧНА ЧАСТИНА

Нині на підприємстві знаходиться в експлуатації система управління технологічним процесом на базі контролерів і модулів розширення виробництва компанії «Siemens» (далі - базовий варіант). Контролери компанії «Siemens» мають високу вартість, тому в роботі запропоновано використати устаткування фірми «VIPA» (далі - проектний варіант).

6.1 Розрахунок капітальних витрат

Розрахуємо капітальні витрати, пов'язані з виготовленням і установкою системи управління система автоматичного управління.

Визначення проектних капітальних витрат робиться по наступній формулі:

$$К_{пр} = С_{об} + Д_{тр} + М_{мн} + К_{по} \quad (6.1)$$

де Соб - витрати на комплектуючі вироби;

Дтр - витрати на транспортно-заготівельні витрати;

Ммн - витрати на монтаж і наладку системи;

Кпо - витрати на програмне забезпечення.

Вартість комплектуючих деталей приведена в табл. 6.1.

Таблиця 6.1 - Вартість комплектуючих деталей

№ з/п	Найменування виробів згідно проектних розробок	Од. вим.	Кількість	Гуртова ціна за од., грн.	Сума, грн.
1	Термоперетворювач дТС065-РТ100.В3.200	шт.	2	142,80	285,60
2	Датчик-реле тиску А6 - 253221	шт.	2	29,50	59,00
3	Датчик індуктивний IA05BSF10NOP	шт.	4	38,00	152,00
4	Електромагнітні клапани загального призначення ТМ25	шт.	4	4,16	16,64
5	Модульний контролер VIPA System 115-6BL22 100V	шт.	1	490,00	490,00
6	Електромагнітний пускач ПМ12-010100 3з+2р 40В УХЛ4В	шт.	1	95,61	95,61
Разом					1 098,85

Витрати на транспортно-заготівельні і складські витрати визначаються по усіх розділах залежно від вартості устаткування матеріалів, виробів, конструкцій, беруться 8 % від загальної вартості.

$$Д_{тр} = С_{об} \cdot 0,08, \quad (6.2)$$

де Соб - вартість комплектуючих, грн.

Таким чином витрати на транспортно-заготівельні і складські роботи складають:

Дтр = 1098,85*0,08 = 87,91 грн.

Вартість монтажна-налагоджувальних робіт приймаємо на рівні 7 % від вартості устаткування.

$$М_{мн} = С_{об} \cdot 0,07 \quad (6.3)$$

Витрати на монтажно-налагоджувальні роботи складуть

Ммн = 1 098,85*0,07 = 76,92 грн.

Капітальні витрати за проектом складуть:

Кпр = 1 098,85 + 87,91 + 76,92 = 1 263,68 грн.

Нині на заводі в експлуатації знаходиться система управління на базі контролерів «Siemens». Капітальні витрати на систему управління що знаходиться в експлуатації складає 34 000 грн. Використовувана система в розрахунках прийнята за базовий варіант.

6.1.1 Розрахунок капітальних витрат на програмне забезпечення

Розрахунок часу на розробку програмного забезпечення. Трудомісткість розробки програмного забезпечення :

$$t = t_o + t_u + t_a + t_n + t_{от} + t_g \, , \quad (6.4)$$

де to - витрати праці на підготовку і опис поставленого завдання;

t_u – равитрати праці на дослідження алгоритму рішення завдання;

t_a – витрати праці на обробку блок-схеми алгоритму;

t_n – равитрати праці на програмування по готовій блок-схемі;

$t_{от}$ – расходы труда на настройку програм на ПОЕМ;

$t_д$ – витрати праці на підготовку документації за завданням.

Складові частини витрат праці визначаються на підставі умовної кількості оброблюваних операторів в програмному забезпеченні. До них відносять ті оператори, яких необхідно написати в процесі роботи над програмою з урахуванням можливих уточнень в постановці завдання і удосконалення алгоритму.

Умовна кількість операторів в програмі:

$$Q = q \cdot c \cdot (1+p), \quad (6.5)$$

де q - кількість операторів, використовуваних в програмі, для ПЗ на мовах FBD і LAD q = 90;

c - коефіцієнт складності програми;

p - коефіцієнт корекції програми в процесі її обробки.

Коефіцієнт складності «c» програми визначає відносну складність програми по відношенню до типового завдання, складність якого відповідає 1. Приймаю c = 1,25.

Коефіцієнт корекції програми «P» визначає збільшення об'єму робіт за рахунок внесення змін до алгоритму або програми в результаті уточнення постановки завдання. Приймаю p = 0,1, це відповідає внесенню 3,5 корекцій, що тягнуть за собою переробку 5…10 % готової програми.

Таким чином, для програми, описаної в роботі:

Q = 90*1,25*(1+0,1) = 124.

Оцінка витрат праці на підготовку і опис завдання в цьому роботі складають $t0$=40 чол.-годин.

Витрати праці на вивчення опису завдання визначаються з урахуванням уточнення опису і кваліфікації програміста по формулі:

$$t_и = \frac{Q \cdot B}{(75...85) \cdot k}, \text{ чол.-годин} \quad (6.6)$$

де B - коефіцієнт збільшення витрат праці, B=1,4;

k - коефіцієнт кваліфікації програміста, які визначається залежно від стажу роботи за фахом. У нашому випадку коефіцієнт кваліфікації програміста складає k = 1,2.

Для програмного забезпечення, що розробляється:

$t_и = \frac{124 \cdot 1,4}{80 \cdot 1,2} = 1,81$ чол.-годин.

Витрати на розробку алгоритму рішення завдання :

$$t_a = \frac{Q}{(20...25) \cdot k}, \text{ чол.-годин} \quad (6.7)$$

Для програмного забезпечення, що розробляється :

$t_a = \frac{124}{20 \cdot 1,2} = 5,17$ чол.-годин.

Витрати праці на складання програми по готовій блок-схемі алгоритму:

$$t_n = \frac{Q}{(20...25) \cdot k}, \text{ чол.-годин} \quad (6.8)$$

Для програмного продукту, що розробляється:

$t_n = \frac{124}{20 \cdot 1,2} = 5,17$ чол.-годин.

Витрати праці на наладку програми на ЕОМ розраховуються по формулі:

$$t_{отл} = \frac{Q}{(4...5) \cdot k}, \text{ чол.-годин} \quad (6.9)$$

Для конкретного програмного продукту:

$t_{отл} = \frac{124}{5 \cdot 1,2} = 20,67$ чол.-годин.

Витрати праці на підготовку документації за завданням визначаються по формулі:

$$t_Д = t_{ДР} + t_{ДО,} \text{ чел.-час}, \quad (6.10)$$

де $t_{ДР}$ - трудомісткість підготовки матеріалів до написання;

$t_{ДО}$ - трудомісткість редагування, друку і оформлення документації.

$$t_{ДР} = Q/(15…20) \cdot k, \quad (6.11)$$

$t_{ДР} = 124/18 \cdot 1,2 = 5,74$ чол.-годин;

$$t_{ДО} = 0,75 \cdot t_{ДР}, \quad (6.12)$$

$t_{ДО} = 0,75 \cdot 5,74 = 4,31$ чол.-годин.

Для програмного забезпечення витрати праці, що розробляється, на підготовку документації за завданням складатимуть:

$t_Д = 5,74 + 4,31 = 10,05$ чол.-час.

Трудомісткість розробки програмного забезпечення складатиме:

$t = 40 + 1,81 + 5,17 + 5,17 + 20,67 + 10,05 = 82,87$ чол.-годин.

Розрахунок витрат на розробку програмного продукту. Витрати на розробку програмного продукту Кпз включають витрати на заробітну плату розробника програми Ззп і вартість машинного часу, необхідного для налаштування програми на ЕОМ Змі.

$$К_{пз} = З_{зп} + З_{ми}, \text{ грн.} \quad (6.13)$$

Заробітна плата розробника програмного забезпечення:

$$З_{зп} = t \cdot С_{пр}, \text{ грн.} \quad (6.14)$$

де t - загальна трудомісткість обробки програмного забезпечення;

Спр - середня годинна тарифна ставка програміста (Спр = 50 грн./годину).

Заробітна плата за розробку програмного забезпечення складає:

Ззп = 82,87·50 = 4 143,5 грн.

Вартість машинного часу, необхідного для налаштування програми на ЕОМ:

$$З_{мв} = t_{отл} \cdot С_{мч}, \text{ грн.} \quad (6.15)$$

де tотл - трудомісткість відладки програми на ЕОМ, чол.-годин;

Смч - вартість машино-години ЕОМ, грн./годину, Смч = 5 грн./годину.

Змв = 20,67·5 = 103,35 грн.

Витрати на розробку програмного забезпечення підсистеми управління складатимуть:

Кпз = 4143,5 + 103,35 = 4246,85 грн.

Визначені, таким чином, витрати на створення програмного забезпечення є частиною одноразових капітальних витрат на створення підсистеми управління.

Очікувана тривалість розробки програмного забезпечення :

$$T = \frac{t}{B_k \cdot F_p}, \text{ міс.} \qquad (6.16)$$

де Вк - кількість розробників, оскільки програма в роботі розроблялася однією людиною, то Вк = 1;

Fр - місячний фонд робочого часу (Fр = 176 годин).

Визначимо тривалість розробки ПЗ:

$$T = \frac{82{,}87}{1 \cdot 176} = 0{,}47 \text{ ммміс.}$$

Визначивши усі показники, використовуємо формулу 6.1 і розраховуємо капітальні витрати:

Кпр = 1 098,85 + 87,91 + 76,92 + 4246,85 = 5 510,53 грн.

6.2 Розрахунок експлуатаційних витрат

Річні експлуатаційні витрати розраховуються по формулі:

$$Сэ = Са + Сз + Сс + Ст + Сээ + Спр \qquad (6.17)$$

де *Сэ* - річні поточні витрати, пов'язані із застосуванням підсистеми управління виробництвом;

Са - амортизація основних фондів;

Сз - заробітна плата обслуговуючого персоналу;

Сс - відрахування на соціальні заходи;

Ст - витрати на технічне обслуговування і поточний ремонт устаткування;

Сээ - вартість електроенергії;

Спр - інші витрати.

Визначимо експлуатаційні витрати при впровадженні підсистеми управління виробництвом.

Амортизація основних фондів. Устаткування, розробленої в роботі підсистеми управління виробництвом, відноситься до 4 групи по нормах нарахування амортизації основних фондів. Передбачуваний термін експлуатації системи складає 5 років.

Норма амортизації визначається по формулі:

$$C_a = \frac{Ф_{ост} * Н_a}{100\%} \quad (6.19)$$

де Т - термін корисного використання об'єкту;

На - норма амортизації;

При цьому річна сума амортизації визначається як твір залишкової вартості об'єкту на початок звітного року або первинної вартості на дату початку нарахування амортизації і річної норми амортизації, що обчислюється згідно з терміном корисного використання об'єкту.

$$C_a = \frac{Ф_{ост} * Н_a}{100\%} \quad (6.20)$$

де Са - амортизація основних фондів(річна);

Фост - залишкова вартість, рівна:

П - первинна вартість системи управління, що розробляється;

Л - ліквідаційна вартість системи управління. Для систем програмованих контролерів ліквідаційна вартість складає близько 20 % від первинної вартості.

$$Ф_{ост}=П – Л \quad (6.21)$$

Фост.пр= 5510,53 - 0,2*5510,53 = 4 408,42 грн.

Фост.баз= 34000 - 0,2*34000 = 27 200 грн.

Норма амортизації для проектованої системи управління складе:

$$На = \frac{2}{5} * 100\% = 40\% \quad (6.22)$$

Сума амортизації для проектованої і базової системи складе:

Са.пр = 0,4 * 4 408,42 = 1 763,37 грн.

Са.баз = 0,4 * 27 200 = 10 880 грн.

Розрахунок фонду заробітної плати. Номінальний річний фонд робочого часу одного працівника визначається відповідно до норм робочого часу на рік:

$$T_{ном}^{год} = (T_к - T_{вых,пр} - T_{отп}) * T_{см}, \text{ годин} \quad (6.23)$$

де $T_к$ - календарний фонд робочого часу, 365 днів;

$Твых_{, пр}$ - вихідні + святкові дні, 114 дні;

$T_{опт}$ – відпустка, 21 день.

Таким чином, річний фонд робочого часу працівника складе:

$T_{ном}^{год}$ = (365 – 114 – 21)*8 = 1 840 годин.

Розрахунок річного фонду заробітної плати виробничих робітників здійснюється відповідно до форми, приведеної в табл. 6.2.

Таблиця 6.2 - Розрахунок заробітної плати персоналу

№ з/п	Найменування професії робітників	Число працюючих, чел		Годинна тарифна ставка, грн/ч.	Номінальний річний фонд робочого часу (година)	Пряма заробітна плата, грн	Додаткова заробітна плата(10%), грн	Доплати (7%), грн	Всього заробітна плата, грн
		яв.	**сп.**						
1	Оператор процесу	2	2	25	1840	92000	9200	6440	107640
2	Технолог	1	1	24	1840	88320	8832	6182,4	103334,4
3	Налагоджувальник електроустаткування	1	1	24	1840	44160	4416	3091,2	51667,2
	Разом								**262641,6**

Після впровадження проектованої системи управління штат персоналу не зміниться і, отже, заробітна плата і відрахування на соціальні заходи будуть однакові.

$Сз._{пр} = Сз._{баз}$ = 26 2641,6 грн.

Відрахування на соціальні заходи. До складу відрахувань на соціальні заходи входять збори на обов'язкове державне пенсійне страхування, на обов'-язкове соціальне страхування, на обов'язкове соціальне страхування на випадок безробіття і тому подібне.

Відрахування на соціальні заходи визначаються по формулі:

$$Сс = 0,22 * Сз, \quad (6.24)$$

$Сс._{пр} = Сс._{баз}$ = 0,22 * 262 641,6 = 94 550,98 грн.

Витрати на технічне обслуговування і поточний ремонт устаткування і мережі приймаємо на рівні 5 % від величини капітальних витрат:

$$С_{то.тр} = 0,05 \cdot К_{пр} \quad (6.25),$$

Сто.тр.пр = 0,05 * 5 510,53 = 275,53 грн.

Сто.тр.баз = 0,05 * 34 000 = 1 700 грн.

Розрахуємо вартість електроенергії, споживаної системою управління, розробленою в проекті :

$$С_{ээ} = К_э \cdot К_{дг} \cdot ds \cdot Т, \quad (6.26)$$

де Кэ - кількість електроенергії, споживана проектованою системою управління у місці за годину, 400 Вт*ч;

$К_{дг}$Додг - кількість робочих днів в році (Кдг = 365 – 114 = 251 день);

ds - тривалість зміни, 8 год.;

Т - тариф на електроенергію для підприємств (для підприємств споживачів електроенергії 2 класу тариф складає 0,64272 грн. кВт/ч. з ПДВ.

Сээ.пр = 0,4 * 251 * 8 * 0,64272 = 101 677,09 грн.

Кількість електроенергії, споживана системою управління, що знаходиться в експлуатації, - 500 Вт*ч.

Сээ.баз = 0,5 * 251 * 8 * 0,64272 = 127 096,36 грн.

Інші витрати по експлуатації об'єкту проектування включають витрати по охороні праці, на спецодяг і ін. згідно з практикою, ці витрати визначають-

ся у розмірі 4 % від річного фонду заробітної плати обслуговуючого персоналу:

$$С_{пр} = С_з \cdot 0,04 \text{ грн.} \quad (4.27)$$

Спр.$_{пр}$= Спр.баз. = 262 641,6 * 0,04 = 10 505,64 грн.

Експлуатаційні витрати по проектному і базовому варіантам зведені в табл. 4.3.

По формулі 6.17 розраховуємо річні експлуатаційні витрати для проектного і базового варіантів:

Спр= 1 763,37 + 26 2641,6 + 94 550,98 + 275,53 + 101 677,09 + 10 505,64 = 471 414,21 грн.

Сбаз= 10880 + 262 641,6 + 94 550,98 + 1 700 + 127 096,36 + 10 505,64 = 507 374,58 грн.

Таблиця 6.3 - Експлуатаційні витрати по варіантах

Найменування показника	Базовий варіант	Проектний варіант
Амортизація	10 880,00	1763,37
Фонд заробітної плати	262 641,60	262 641,60
Відрахування на соц. виплати	94 550,98	94 550,98
Ремонт і тих. обслуговування	1 700,00	275,53
Електроенергія	127 096,36	101 677,09
Інші	10 505,64	10 505,64
Разом	507 374,58	471 414,21

Таким чином, економія експлуатаційних витрат, при впровадженні підсистеми управління виробництвом складатиме

ΔЗ = 507 374,58 – 471 414,21 = 35960,37 грн.

6.3 Визначення додаткового прибутку від впровадження системи управління

Середньодобового збільшення виходу готової продукції при впровадженні розробленої підсистеми управління складе 5%, за рахунок зниження простоїв устаткування.

Визначимо додатковий прибуток від впровадження проектованої системи управління:

$$\Delta П = (Ц_{пр.} - S_{пр.}) * Q_{пр} - (Ц_{баз.} - S_{баз.}) * Q_{баз.}, \quad (6.28)$$

де Sпр., Sбаз - собівартість тони продукції по проектному і базовому варіантам, грн/т. (кам'яного вугілля1 800 грн./т);

Цпр., Цбаз - ціна за одиницю продукції, грн, з урахуванням торгової надбавки 20 % складе 2 160 грн./т.;

Qпр., Qбаз - обсяг виробництва продукції, кг, зараз продуктивність лінії складає 15 000 кг/годину.

При 8 год. зміні і 251 робочій день об'єм вироблюваної продукції складе:

Qбаз. = 15000 * 8 * 251 = 30 120 000 кг/рік.

При впровадженні системи управління:

Qпр. = 1,05 * 15000 * 8 * 251 = 31 626 000 кг/рік

Додатковий прибуток від впровадження підсистеми управління

ΔП= (2 160 – 1 800) * 31 626 000 – (2 160 – 1 800) * 30 120 000 = 542 160 000 грн.

6.4 Оцінка економічної ефективності проекту

Визначимо показники економічної ефективності проектованої підсистеми управління виробництвом вафельного тіста :

- річний економічний ефект:

$$E = \Delta П + \Delta С - \Delta К * E_п > 0 \quad (6.29)$$

- і термін окупності розробки :

$$Т_{ок} = К_п / E < Т_{ож} \quad (6.30)$$

$$E_п = (N_{кр} - N_{инф}) / 100 \quad (6.31)$$

де Nкр - річна процентна ставка %;

Nинф - річний рівень інфляції, %.

В якості нормативного значення приймемо величину банківської кредитної ставки Nкр (37.38%) з урахуванням інфляції Nинф (16 %), тобто:

$E_п = (37{,}38 - 16) / 100 = 0{,}214$

Е = 542 160 000 + 35 960,37 – 0,214 *5 510,53 = 542 194 781,12 грн.

$Т_{ок}$ = 5510,53 / 542194781,12 = 0,1 року.

Коефіцієнт ефективності (доходності) капітальних витрат Ер показує, скільки гривен додаткового прибутку (економії) приносить одна гривна капітальних витрат:

$$Э = Е/К_{п} \quad (6.32)$$

Коефіцієнт ефективності складає:

Э = 542 194 781,12 /5 510,53 = 98 392,49.

Отже, при впровадженні підсистеми управління 1 грн капітальних витрат приносить 98 392,49 грн. прибутку.

Економічні показники, що характеризують ефективність створення і використання розробленого проекту відображені в табл. 6.4.

Таблиця 6.4 - Показники використання системи управління

Найменування показників	**Од. виміри**	**Показники базового варіанту системи**	**Показники проектного варіанту системи**
Капітальні витрати	грн.	34 000,00	5 510,53
Експлуатаційні витрати, всього	грн.	507 374,58	471 414,21
у тому числі: - амортизація	грн.	10 880,00	1 763,37
- заробітна плата обслуговуючого персоналу		262 641,60	262 641,60
- відрахування на соціальні заходи		94 550,98	94 550,98
- технічне обслуговування і поточний ремонт системи управління		1 700,00	275,53
- вартість споживаної електроенергії		127 096,36	101 677,09
- інші витрати		10 505,64	10 505,64
Додатковий прибуток	грн.	-	542 160 000,00
Річний економічний ефект	грн.	-	542 194 781,12
Коефіцієнт ефективності			98 392,49
Розрахунковий термін окупності капітальних вкладень	років	-	0,10

6.5 Висновок за розділом

При впровадженні проектованої системи капітальні витрати 5 510,53 грн. Річні експлуатаційні витрати, пов'язані з впровадженням системи 471 414,21 грн. Аналіз економічних показників при впровадженні підсистеми показав, що річний економічний ефект від впровадження системи управління дорівнює 542 194 781,12 грн. Термін окупності проектних капітальних вкладень за рахунок скорочення експлуатаційних витрат і збільшення продуктивності системи 0,1 року. Коефіцієнт ефективності капітальних витрат 98 392,49 грн. Виходячи з отриманих результатів, можна зробити висновок, що впровадження проектованої підсистеми економічно вигідне.

7 ОХОРОНА ПРАЦІ

7.1 Аналіз небезпечних і шкідливих виробничих факторів

В розділі аналізуються рівень небезпеки процесів роботи і обслуговування технологічного обладнання.

На досліджуваному підприємстві активно використовуються інструменти позитивної мотивації співробітників. Згідно з Положенням про мотивацію за підсумками року виробляється оцінка роботи цехів в області охорони праці і промислової безпеки. Навчання працівників заводу безпечним методам праці проводиться в сучасному учбовому центрі підприємства з використанням методів передового світового досвіду.

Введені в дію корпоративні стандарти, направлені на підвищення безпеки праці: «Аудити безпеки», «Визначення корінних причин випадків». В процесі впровадження знаходяться зараз на підприємстві наступні стандарти: «Блокування/Маркування/Перевірка», «Управління безпекою підрядних організацій», «Вимоги до спецодягу, спецвзуття та інших СІЗ для працівників підприємств/

Небезпечними й шкідливими виробничими факторами відділення є:

- аміак – має неприємний запах, подразнює слизуваті оболонки й дихальні шляхи, гранично допустима концентрація (ГДК) у повітрі робочої зони 20 мг/м^3;
- сірчана кислота - маслянистa, у чистому виді прозора або слабо забарвлена рідина.

Пари сірчаної кислоти викликають роздратування верхніх дихальних шляхів, кашель, утруднене подих, спазми голосової щілини, почуття печіння в очах.

Головну ж небезпеку представляє влучення сірчаної кислоти на шкіру. У цьому випадку виходять важкі хімічні опіки, аж до обвуглювання шкірних покривів.

Особливо небезпечне влучення сірчаної кислоти в очі.

Гранично допустима концентрація сірчаної кислоти в повітрі виробничих приміщень - 1 мг/м^3.

При влученні на шкіру сірчаної кислоти необхідно рясно промивати водою, чим швидше й сильніше місце опіку буде промито водою, тим менше буде ступінь опіку. Найпоширенішими небезпечними ситуаціями відповідно частоти їх виникнення при експлуатації таких агрегатів виявились наступні (рис. 7.1.) - витік шкідливих речовин, пожежа, вибух, а також опіки в результаті контакту з парою або водою.

Таблиця 7.1. Перелік основних небезпечних і шкідливих виробничих чинників, які зустрічаються на робочому місці:

Найменування чинників	Джерела виникнення	Характер дії на організм	Нормований параметр
Недостатня освітленість місця проведення робіт	Робоча зона	Вплив на функціювання зорового апарату, на психіку людини, його емоційний стан, викликає втому нервової системи	П.4 НПАОП 23.1-1.01-08 «Правила безпеки в коксохімічному виробництві».
Підвищена температура поверхонь обладнання і матеріалів	На трубопроводі пари частково відсутня та ушкоджена ізоляція Не прикріплені металеві таблички з даними	Опіки незахищених ділянок тіла	П.3 Р. IV. НАПОП 0.00-1.81.18 «Правила охорони праці під час експлуатації обладнання, що працює під тиском» П.1 НПАОП 23.1-1.01-08 «Правила безпеки в коксохімічному виробництві».
Підвищена запиленість	Внесення частинок пилу разом з повітрям, застосування в цеху сипучих і легко роздрібнюваних матеріалів	Кисневе голодування, прискорене дихання, ушкодження слизових оболонок	П.1 НПАОП 23.1-1.01-08 «Правила безпеки в коксохімічному виробництві». ГОСТ 12.1.005-88 п. 6 НПАОП 0.00-7.14-17 «Вимоги безпеки та захисту здоров’я під час використання виробничого обладнання працівниками»

7.2 Інженерно-технічні заходи з охорони праці

Вміст шкідливих речовин у повітрі робочої зони не повинне перевищувати значень гранично допустимих концентрацій (ГДК) (табл. 5.1).

Таблиця 7.2 − Гранично допустимі концентрації шкідливих речовин у повітрі робочої зони

№№	Найменування	Велич. ГДК, мг/м3	Клас небезп.	Особл. дії на організм
1.	Ціаністий водень	0,3	I	Г
2.	Сірководень +	10	II	Г
3.	Фенол¬ +	0,3	II	–
4.	Бензол +	15/5	II	К
5.	Аміак	20	IV	–
6.	Нафталін	20	IV	–
7.	Сірчистий ангідрид +	10	III	–
8.	Оксид вуглецю	20	IV	Г
9.	Піридин	5	II	–
10.	Пил сульфату амонію –	–		–
11.	Оксиди марганцю	0,2	III	–
12.	Фтористий водень	0,5	I	Г

Умовні позначки:

Г − речовини з гостроспрямованим механізмом дії, що вимагають автоматичного контролю за їхнім змістом у повітрі;

К − канцерогени;

+ − вимагають спеціального захисту очей і шкіри.

Вміст шкідливих речовин у повітрі робочої зони підлягає систематичному контролю.

При надходженні в повітря робочої зони шкідливих речовин з гостроспрямованим механізмом дії повинен бути забезпечений безперервний контроль речовин із сигналізацією про перевищення ГДК.

Періодичність контролю шкідливих речовин у повітрі робочої зони (за винятком речовин з гостроспрямованим механізмом дії) здійснюється залежно від класу небезпеки шкідливої речовини (табл. 7.2).

Таблиця 7.3 − Періодичність контролю шкідливих речовин

Клас небезпеки	**Періодичність контролю**
I	не рідше 1 разу в 10 днів
II	не рідше 1 разу на місяць
III	не рідше 1 разу в квартал
IV	не рідше 1 разу в квартал

Контроль за вмістом шкідливих речовин у повітрі робочої зони здійснюється по методичних вказівках, затвердженим зам. головного державного санітарного лікаря.

Приміщення, де мають місце виділення парів, газів, аерозолів, повинні обладнатися загально-обмінною механічною приточно-витяжною вентиляцією.

Фіксовані місця виділення шкідливих речовин, повинні бути обладнані місцевою витяжною вентиляцією.

Працюючі й службовці повинні проходити попередній при надходженні на роботу й періодичний медичні огляди, одержувати безкоштовно молоко й забезпечуватися засобами індивідуального захисту.

При здійсненні технологічних процесів робітники піддаються впливу шуму, вібрації, інфрачервоного випромінювання, підвищених і знижених температур, вологості.

Припустимі рівні звуку й еквівалентні рівні звуку на робочих місцях для широкосмугового постійного й непостійного (крім імпульсного) шуму не повинні перевищувати значень, зазначених у відповідних санітарних правилах та нормах і повинні становити не більше 80 дБА.

Рівні вібрації на робочих місцях, порушувані роботою устаткування (електродвигунів, вентиляторів, дробарок, машин і т. д.) не повинні перевищувати значень, зазначених у відповідних вимогах безпеки, з урахуванням категорій вібрації.

Періодичність контролю рівнів шуму, вібрації на робочих місцях становить не рідше 1 разу на рік.

У літній період робітники піддаються впливу підвищених температур, а в зимовий період знижених температур.

Показники мікроклімату (температури повітря, відносної вологості, швидкості руху повітря) на різних робочих місцях різних категорій ваги робіт у холодний і теплий періоди року не повинні перевищувати значень, зазначених у загальних санітарно-гігієнічних вимогах до повітря робочої зони.

Інтенсивність теплового опромінення працюючих від нагрітих поверхонь технологічного устаткування, ізоляції на постійному й непостійному робочому місцях не повинна перевищувати 35 Вт/м^2 при опроміненні 50 % тіла й більше, 70 Вт/м^2 − при величині опромінюється поверхня, що, від 25 до 50 % і 100 Вт/м^2 − при опроміненні не більше 25 % поверхні тіла.

Інтенсивність теплового опромінення працюючих від відкритих джерел (нагрітий метал, "відкрите" полум’я й ін.) не повинна перевищувати 140 Вт/м^2 при опроміненні не більше 25 % поверхні тіла з обов’язковим використанням засобів індивідуального захисту , у т. ч. засобів захисту особи.

Контроль (вимір) показників мікроклімату проводиться на початку, середині й кінці холодного й теплого періоду року − не менш 3 разів у зміну (на початку, середині й кінці).

Все технологічне устаткування, електричний, вентиляційний і металевий трубопроводи повинні бути заземлені шляхом сполуки струмопровідними перемичками на всьому протязі даної системи в безперервне електричне коло й приєднані не менш, ніж у двох місцях до контурів заземлення електроустаткування й блискавкозахисту з дотриманням вимог правил експлуатації. Застосування безпечної напруги (12 В) при чищенні апаратури.

7.2.1 Освітлення

Для усунення недостатньої освітленості приміщення, а також забезпечення раціонального освітлення (що відповідає технічним і санітарно-гігієнічним нормам) підібрані світильники в поєднанні з природним світлом. Також проводиться підтримання чистоти віконного скла та поверхонь світи-

льників. В котельні передбачено робоче, ремонтне, аварійне та евакуаційне електроосвітлення. Напруга робочого освітлення становить 220 В, ремонтного – 12 В.

Робоче освітлення цеху живиться від двох автоматів, встановлених в силовому щиті. Освітленість приміщення залу методичної печі, приймається 150 лк.

Для робочого освітлення встановлені світильники з люмінесцентними лампами. Для забезпечення безпеки в цеху для робочого освітлення в складі вибухобезпечні світильники типу ВЗГ-200АМС, які включаються вимикачами, встановленими зовні біля вхідних дверей.

Рисунок 7.1 – Світильник ВЗГ-200АМС

Для аварійного освітлення використовуються переносні акумуляторні ліхтарі. Для евакуаційного освітлення встановлені два світильника з піктограмою «Вихід». Для ремонтного освітлення встановлено скриньку з знижувальних трансформатором 220 / 12 В і штепсельною розеткою.

7.2.2 Підвищена температура поверхонь

Для уникнення безпосереднього контакту з нагрітими поверхнями проведено технологічного обладнання необхідної гарнітури для безпеки: лази в обмурівці для огляду камери згоряння і газоходів, ізоляція окремих елементів методичної печі агрегату схильних до інтенсивного теплового впливу.

Для робітника, безпосередньо контактуючого з обладнанням, передбачені спеціальні рукавички які забезпечують захист від опіку при короткочас-

ному контакті з розпеченої поверхнею. Виготовляються з шкіряного спилка товщиною 1,1-1,3 мм, всередині - м'яка х / б підкладка, шви прошиті міцною негорючої ниткою.

7.2.3 Запиленість

Зниження запиленості повітря робочої зони досягається герметизацією формувального і паливо-заготовчого обладнання, а також пристроєм загально-обмінної і місцевої витяжної вентиляції в місцях подачі вугільного пилу

Повітря, що відсмоктується з цеху перед випуском в атмосферу очищається пилоочисними пристроями.

Виконано запобігання проникнення шкідливих речовин в повітря робочої зони за рахунок герметизації обладнання, ущільнення з'єднань, люків та отворів.

Передбачено використання системи пило-пригнічення, що змочує дрібні частинки, які потрапляють в повітря. Це дозволяє виключити пил з повітря шляхом розпилення дрібних крапель води в хмарі пилу.

Рисунок 7.2 - Водяна гармата для систем пилопригнічення

7.2.4 Монотонність праці

Для мінімізації монотонності роботи, вводиться чимала кількість автоматизованих систем, що зводить до мінімуму участь людини в роботі методичної печі, знижуючи тим сам одноманітність і тривалість робіт з присутністю людини. У нашому випадку, ми вводимо систему автоматичного управління, що дозволяє людині працювати у вільному ритмі і темпі, дозволяючи знизити монотонність процесу праці.

7.3 Пожежна профілактика

Категорії приміщень по вибуха-пожежній і пожежній небезпеці визначені відповідно до вимог загальносоюзних норм технологічного проектування. Класи зон приміщень − за правилами експлуатації. Згідно цих документів устаткування сульфатного відділення є невибуха- і непожежноопасною зоною. Їх класифікація наведена в табл. 7.4

Таблиця 7.4 – Класифікація приміщень сульфатного відділення

Найменування відділень, установок	Категорія виробництв по вибуха- та пожежонебезпечності,	Ступінь вогнестійкості будинків	Клас приміщень і зовнішніх установок по ПУЕ для застосування електроустаткування
Установки сульфатного відділення, розташовані в окремому будинку.			
- склад сульфату амонію	Д	III	Невибуха- та пожежонебезпечна
- сушіння сульфату амонію (без спалювання коксового газу)	Д	III	Невибуха- та пожежонебезпечна
- установка центрифуг	Д	III	Невибуха- та пожежонебезпечна
- насосна сульфатного відділення	Д	III	Невибухо- та пожежонебезпечна
Зовнішні установки сульфатного відділення (поза будинком).			
- збірники маткового розчину	В	-	П- III
- переробка надлишкової надсмольної води	Д1	-	Невибуха- та пожежонебезпечна

В усіх випадках виникнення пожежі на підприємстві чи появи гару й інших ознак горіння обслуговуючий персонал цеху чи установки зобов'язаний вжити заходів для ліквідації вогню, використовуючи наявні в наявності засобу пожежогасіння, і по встановленому зв'язку викликати пожежну охорону. Пожежний зв'язок поділяють на зв'язок оповіщення, ціль якого – своєчасний виклик на пожежу, диспетчерську – для керування силами і засобами пожежогасіння і зв'язок на пожежі – для керівництва пожежними підрозділами при гасінні пожежі. Ці види зв'язку забезпечують телефонами, радіопередавачами і пожежною сигналізацією.

Вогнегасні засоби можуть бути рідкими (вода, розчин солей), газоподібними (водяники пари, газоподібна вуглекислота), пінотипними, твердими (суха земля, пісок, тверда вуглекислота). Найбільш розповсюдженим способом боротьби з вогнем є вода, що застосовують для гасіння більшості пожеж.

Для посилення вогнегасних властивостей води в неї додають кислотно-лужний порошок. У цьому випадку утвориться хімічна піна, при введенні якої в зону вогню виникає хмара інертного газу, що перешкоджає доступу повітря в сферу вогню. Хімічну піну використовують для гасіння всіх нафтопродуктів (з температурою спалаху до 45°С) і твердих пальних речовин.

Кожен працівник повинен дотримувати наступні правила пожежної безпеки:

- проведення тимчасових вогневих робіт на території й у приміщенні цеху, розведення багать і інших випадків застосування відкритого вогню дозволяється тільки після оформлення плану проведення вогневих робіт і твердження його головним інженером заводу.
- постійні вогневі роботи проводити у встановлених наказом директора місцях і виробництвах.
- при роботах у пожеже і вибухонебезпечних місцях користуватися інструментом не дає іскріння.
- не курити на території й у приміщеннях цеху. Курити дозволяється тільки в спеціально відведених місцях.

- первинні засоби пожежогасіння на робочих місцях повинні бути в наявності і міститися в чистоті і справності, передаватися по зміні.
- забороняється застосовувати бензол, бензин, розчинники й інші легкозаймисті рідини для миття рук, підлог, стін, вікон і чищення спецодягу в приміщеннях цеху.
- систематично стежити за герметичністю устаткування, апаратів і комунікацій, не допускаючи витоку пар, рідин.
- стежити за справністю електропроводки й електроустаткування, заземлення, не допускати їхні іскріння й оголення. Не допускати улучення води й інших хімічних продуктів на електроустаткування.
- збереження газу, бензину, мастильних матеріалів, карбіду кальцію дозволяється тільки в спеціально відведених місцях.
- балони з газом установлювати удалині від джерел тепла.
- категорично забороняється працювати з кисневими балонами в промаслених рукавицях і спецодязі, чи забрудненими олією руками.
- категорично забороняється гасити електроустаткування водою, піною, пінними вогнегасниками.
- при загорянні усередині приміщення негайно зупинити виробництво, відключати вентиляційні системи від електропостачання.
- використання пожежного устаткування й інвентарю для виробничих, господарських і інших нестатків, не зв’язаних з пожежогасінням, забороняється.
- для внутрішнього висвітлення апаратів, цистерн, ємкостей під час їхнього огляду, чищення і ремонту повинні застосовуватися тільки вибухозахищені акумуляторні переносні лампи напругою не вище 12 В з захисними ковпаками і сітками.

7.4 Висновок за розділом

У розділі охорони праці виконаний аналіз небезпечних і шкідливих виробничих факторів, та розроблені інженерно-технічні заходи з охорони праці.

ВИСНОВКИ

У роботі була проведена розробка комп'ютерної система обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Розроблено структурну схему системи контролю на підставі котрої з урахуванням вимог технологічного процесу обрані датчики та виконавчі пристрої системи керування. За результатами аналізу вимог до функціонування системи керування, датчиків та виконавчих пристроїв обрано пристрій контролю. На підставі обраного апаратного забезпечення розроблено функціональну схему автоматизації системи керування та схему електричну принципову системи контролю.

Розроблена система автоматизації збільшить інформативність про хід виконання технологічного процесу, це досягається за рахунок застосування сучасної елементної бази і досконалого програмного забезпечення.

Розроблена комп’ютерна мережа реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота. Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці, або додатках.

В економічному розділі був зроблений розрахунок капітальних витрат на проектування та впровадження системи контролю та річних експлуатаційних витрат на функціонування цього комплексу, термін окупності капітальних інвестицій, коефіцієнті повернення інвестицій ROSI - ці показники доказують, що впровадження

У розділі охорони праці виконаний аналіз небезпечних і шкідливих виробничих факторів, та розроблені інженерно-технічні заходи з охорони праці.

ПЕРЕЛІК ПОСИЛАНЬ

1. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2020. – 69 с.
2. Методичні вказівки з виконання заходів щодо охорони праці та розрахункової частини розділу «Охорона праці та безпека в надзвичайних ситуаціях» в дипломних проектах студентів всіх спеціальностей /Уклад. В.І. Голінько, В. Ю. Фрундін, Ю.І. Чеберячко, М.Ю. Іконніков - Дніпропетровськ: - Дніпропетровськ: Національний гірничий університет, 2013. – 12 с.
3. Методичні вказівки з виконання економічного розділу в дипломних проектах студентів спеціальності "Комп'ютерні системи " / Уклад. О.Г. Вагонова, О.Б. Нікітіна Н.М. Романюк – Дніпропетровськ: Національний гірничий університет. – 2013. – 11 с.
4. https://netacad.com – Комп'ютерна академія Cisco.
5. Э. Таненбаум., Д.Уэзеролл. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.: ил.
6. В.Г. Олифер., Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2010. — 944 с.: ил.
7.
8.
9.
10. Указ про положення про технічний захист інформації в Україні
11. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення

12. НД ТЗІ 3.1-001-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.
13. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегрудов Д.А., Хорошко В.А., Под ред. В.А. Хорошко. – К.; Арий, 2008. – Том I. Несанкционированное получение информации. – 464 с.
14. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегрудов Д.А., Хорошко В.А., Под ред. В.А. Хорошко. – К.; Арий, 2008. – Том II. Информационная безопасность. – 344 с.
15. Инженерно-техническая защита информации / Торокин А.А. – М.: Гелиос АРВ, 2005. – 960 с.
16. Защита от утечки информации по техническим каналам: учебное пособие / Бузов Г.А., Калинов С.В., Кондратьев А.В. – М.: Горячая линия – Телеком, 2005. – 416 с.
17. Хорев А.А. Способы и средства защиты информации (Електрон. Ресурс) / Спосіб доступу: URL: http://www.analitika.info/zaschita.php - Заголовок з екрану
18. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации (Електрон. ресурс) / Спосіб доступу: URL:http://www.analitika.info/kanalutechki.php - Заголовок з екрану
19. Буров Є. В. Комп’ютерні мережі. – Львів: БАК, 1999. – 468 с.
20. Иванов А.С. Внедрение автоматизированных систем учета энергоресурсов в жилищно-коммунальном хозяйстве // Вестник поморского университета. Серия “Естественные и точные науки”. Архангельск: ПГУ им. Ломоносова, 2006. – 182 с.
21. Казачков В. С. Автоматизированная система поквартирного и домового учета потребления энергоресурсов. Материалы Форума Международных научно-практических конференций. СПб.: Политехника, 1999, – 25 с.
22. Коуров Л.В. Информационные технологии. Минск, “Амалфея”, 2000, – 192 с.

23. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. – М.: Горячая линия-Телеком. 2010. – 272 с.
24. Волковицкий В.Д., Волхонский В.В. Системы контроля и управления доступом. – СПб.: Экополис и культура, 2003. – 164 с.
25. Олифер В. Г., Олифер Н. А. – Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 2-е изд. СПБ.: Питер 2003. – 822 с.
26. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф.Шаньгина. М.: Радио и связь, 1999. – 328 с.
27. В.В. Ткачов, С.М. Ткаченко, Я.В. Панферова, Д.В. Славінський. Дипломування. Методичні рекомендації для бакалаврів галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія – Д.: НТУ "Дніпровська політехніка", 2018. – 66 с.
28. Иванов А.С., Тарасенков М.А., Лукичев А.Ю., Серов И.В., Грудин Д.В. Построение системы АСКУЭ на базе автоматизированной системы диспетчеризации АСУД-248 // Информатизация и системы управления в промышленности. М., 2006. – 213 с.
29. Автоматизированные системы учёта воды [Електронний ресурс] – Режим доступу: https://www.gkh.ru/article/101891-askuv – Назва з екрану.
30. Сообщество LoRaWAN [Електронний ресурс] – Режим доступу: http://lorawan.lace.io – Назва з екрану.

ДОДАТОК А – ТЕКСТ ПРОГРАМИ НАЛАШТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

Текст програми
програмування протоколів та служб
на мережевих пристроях системи контролю

НТУ “Придніпровська політехніка”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПРОГРАМУВАННЯ ПРОТОКОЛІВ ТА СЛУЖБ НА МЕРЕЖЕВИХ ПРИСТРОЯХ СИСТЕМИ КОНТРОЛЮ

Текст програм

804.02070743.00006-01 12 01

Листів 10

2020

АНОТАЦІЯ

Представлені набори використаних команд відображають процес програмування протоколів і служб на мережевих пристроях комп’ютерної мережі.

Дані приклади програмування повністю розкривають процес реалізації окремих протоколів і служб, що були обрані під час розробки комп’ютерної мережі та прийнятих рішень відносно вибору найкращих налаштувань серед можливих варіантів.

Програмування базового налаштування конфігурації пристроїв на прикладі Sinepostol_Router_1

```
Router>enable // перехід в привілейований режим
Router#configure terminal // перехід в режим глобальної конфігурації
Router(config)#hostname Sinepostol_Router_1 // задати ім’я пристрою
Sinepostol_Router_1(config)#line vty 0 15 // налаштування віртуальних ліній
Sinepostol_Router_1(config-line)#password cisco // пароль на лінії vty
Sinepostol_Router_1(config-line)#login local  // вимагає ввод імені користувача і паролю з перевіркою наявності в локальній базі
Sinepostol_Router_1(config-line)#transport input ssh // дозвіл для підключення по ssh
Sinepostol_Router_1(config-line)#exit // вихід з режиму
Sinepostol_Router_1(config)#line con 0 // налаштування консолі
Sinepostol_Router_1(config-line)#password cisco // пароль для консолі
Sinepostol_Router_1(config-line)#login // вимагає ввод паролю при вході до консолі
Sinepostol_Router_1(config-line)#exit // вихід з режиму
Sinepostol_Router_1(config)#enable password class // пароль на привілейований режим
Sinepostol_Router_1(config)#service password-encryption // шифрування всіх паролів
Sinepostol_Router_1(config)#banner motd #warning# // інформаційний банер
Sinepostol_Router_1(config)#ip domain-name Sinepostol_Router_1 // ім’я домену
Sinepostol_Router_1(config)#crypto key generate rsa // генерація пари ключів RSA
Sinepostol_Router_1(config)#username KIITS151_Sinepostol password admincisco // ім’я користувача і пароль для підключенна по ssh
Sinepostol_Router_1(config)# interface GigabitEthernet0/0 // налаштування  інтерфейсу
Sinepostol_Router_1(config-if)#ip address 192.168.41.130 255.255.255.128 // задає IP–адресу на порті
Sinepostol_Router_1(config-if)#no shutdown // ввімкнення порта
Sinepostol_Router_1(config-if)#exit
Sinepostol_Router_1(config)#int gig0/1
Sinepostol_Router_1(config-if)#ip address 192.168.41.1 255.255.255.128
Sinepostol_Router_1(config-if)#no shutdown
Sinepostol_Router_1(config-if)#exit
Sinepostol_Router_1(config)#int serial0/0/0
Sinepostol_Router_1(config-if)#ip address 10.0.6.1 255.255.255.252
Sinepostol_Router_1(config-if)#clock rate 128000 // тактова частота на інтерфейсі
Sinepostol_Router_1(config-if)#no shutdown
Sinepostol_Router_1(config-if)#exit
Sinepostol_Router_1(config)#exit
Sinepostol_Router_1#copy running-config startup-config // збереження поточної конфігурації в стартову
```

Програмування протоколу OSPF на маршрутизаторах

```
Sinepostol_Router_2
Sinepostol_Router_2(config)#router ospf 6 // ввімкнення протоколу маршрутизації ospf  з process-id 3
Sinepostol_Router_2(config-router)#router-id 2.2.2.2 // ідентифікатор маршрутизатора
// налаштування пасивних інтерфейсів (через пасивні інтерфейси не відбувається відправка пакетів протоколу ospf)
Sinepostol_Router_2(config-router)#passive-interface g0/0
Sinepostol_Router_2(config-router)#passive-interface g0/0.16
Sinepostol_Router_2(config-router)#passive-interface g0/0.26
Sinepostol_Router_2(config-router)#passive-interface g0/0.36
Sinepostol_Router_2(config-router)#passive-interface g0/0.99
```

Sinepostol_Router_2(config-router)#passive-interface g0/1
Sinepostol_Router_2(config-router)#network 192.168.40.0 0.0.0.31 area 0
Sinepostol_Router_2(config-router)#network 192.168.40.32 0.0.0.31 area 0
Sinepostol_Router_2(config-router)#network 192.168.40.64 0.0.0.31 area 0
Sinepostol_Router_2(config-router)#network 192.168.40.96 0.0.0.31 area 0
Sinepostol_Router_2(config-router)#network 192.168.41.128 0.0.0.127 area 0
Sinepostol_Router_2(config-router)#network 10.0.6.4 0.0.0.3 area 0
Sinepostol_Router_2(config-router)#auto-cost reference-bandwidth 1000 // зміна пропускної спроможності для обчислення вартості інтерфейсів Gigabit на значення 1000
Sinepostol_Router_2(config-router)#area 0 range 192.168.40.0 255.255.255.128 // задання сумарного маршруту
Sinepostol_Router_2(config-router)#exit
Sinepostol_Router_2(config)#interface s0/0/0
Sinepostol_Router_2(config-if)# bandwidth 128 // зміна пропускної спроможності на serial-інтерфейсі
Sinepostol_Router_2(config-if)#ip ospf cost 7500 // зміна вартості метрики
Sinepostol_Router_3
Sinepostol_Router_3(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.2 // статичний маршрут для отримання доступу до інтернету (якщо адресі призначення з пакету на маршрутизаторі не буде відповідати жоден маршрут в таблиці маршрутизації, то пакет буде відправлений по даному статичному маршруту останньої надії)
Sinepostol_Router_3(config)#router ospf 6
Sinepostol_Router_3(config-router)#router-id 3.3.3.3
Sinepostol_Router_3(config-router)#passive-interface g0/0
Sinepostol_Router_3(config-router)#network 10.0.6.0 0.0.0.3 area 0
Sinepostol_Router_3(config-router)#network 10.0.6.8 0.0.0.3 area 0
Sinepostol_Router_3(config-router)#network 192.168.42.1 0.0.0.63 area 0
Sinepostol_Router_3(config-router)#default-information originate // розповсюдження інформації про статичні маршрути на інші маршрутизатори
Sinepostol_Router_3(config-router)#auto-cost reference-bandwidth 1000
Sinepostol_Router_3(config-router)#area 0 range 192.168.40.0 255.255.252.0
Sinepostol_Router_3(config-router)#exit
Sinepostol_Router_3(config)#interface s0/0/0
Sinepostol_Router_3(config-if)#bandwidth 128
Sinepostol_Router_3(config-if)#ip ospf cost 7500
Sinepostol_Router_3(config-if)#interface s0/0/1
Sinepostol_Router_3(config-if)#bandwidth 128
Sinepostol_Router_3(config-if)#ip ospf cost 7500

Програмування статичних маршрутів для можливості відправки даних з зовнішньої мережі (з інтернету) у внутрішню і навпаки
Sinepostol_IPS(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1
Sinepostol_IPS(config)#ip route 192.168.40.128 255.255.255.128 64.100.13.2
Sinepostol_Router_0(config)#ip route 0.0.0.0 0.0.0.0 64.100.13.1

Програмування протоколу HSRP на маршрутизаторах
Sinepostol_Router_1
Sinepostol_Router_1(config)#interface gigabitEthernet 0/0
Sinepostol_Router_1(config-if)#standby 1 ip 192.168.41.129 // віртуальна IP адреса, яка буде виступати шлюзом
Sinepostol_Router_1(config-if)#standby 1 priority 110 // установка пріоритету маршрутизатора

Sinepostol_Router_1(config-if)#standby 1 preempt // дозволяє маршрутизатору с більш високим пріоритетот перехоплювати роль активного маршрутизатора
Sinepostol_Router_2
Sinepostol_Router_2(config)#interface gigabitEthernet 0/1
Sinepostol_Router_2(config-if)#standby 1 ip 192.168.41.129
Sinepostol_Router_2(config-if)#standby 1 priority 90
Sinepostol_Router_2(config-if)#standby 1 preempt

Програмування служби AAA на прикладі Sinepostol_Router_1
Sinepostol_Router_1(config)#aaa new-model // ввімкнення aaa
Sinepostol_Router_1(config)#aaa authentication login default local // створення конфігураціїї аутентифікайії з використанням локальної бази
Sinepostol_Router_1(config)#aaa authentication login LOGRAD group radius local // створення конфігураціїї аутентифікайії з використанням спочатку сервера radius, а потім локальної бази
Sinepostol_Router_1(config)#line console 0
Sinepostol_Router_1(config-line)#login authentication LOGRAD // застосування конфігураціїї аутентифікайії на лінії
Sinepostol_Router_1(config-line)#exit
Sinepostol_Router_1(config)#line vty 0 15
Sinepostol_Router_1(config-line)#login authentication default
Sinepostol_Router_1(config-line)#exit
Sinepostol_Router_1(config)#radius-server host 192.168.41.16 auth-port 1645 // адреса та порт radius сервера
Sinepostol_Router_1(config)#radius-server key radiuskiit // ключ
Sinepostol_Router_1(config)#aaa accounting exec default start-stop group radius // аудит і відправку повідомлень про початок і завершення процесу exec

Програмування об’єднання фізичних портів
Приклад створення об’єднаного каналу (группа 1)
Sinepostol_Switch_5(config)#interface range fastEthernet 0/1-2
Sinepostol_Switch_5(config-if-range)# shutdown
Sinepostol_Switch_5(config-if-range)#channel-group 1 mode on // об’єднання фізичних каналів в один логічний
Sinepostol_Switch_3(config)#interface range fastEthernet 0/1-2
Sinepostol_Switch_3(config-if-range)#channel-group 1 mode on
Sinepostol_Switch_5(config-if-range)#no shutdown
Приклад створення об’єднаного каналу (группа 2)
Sinepostol_Switch_5(config)#interface range fastEthernet 0/3-4
Sinepostol_Switch_5(config-if-range)# shutdown
Sinepostol_Switch_5(config-if-range)#channel-group 2 mode on
Sinepostol_Switch_4(config)#interface range fastEthernet 0/3-4
Sinepostol_Switch_4(config-if-range)#channel-group 2 mode on
Sinepostol_Switch_5(config-if-range)#no shutdown
Приклад створення об’єднаного каналу (группа 3)
Sinepostol_Switch_3(config)#interface range fastEthernet 0/3-4
Sinepostol_Switch_3(config-if-range)# shutdown
Sinepostol_Switch_3(config-if-range)#channel-group 3 mode on
Sinepostol_Switch_4(config-if-range)#interface range fastEthernet 0/1-2
Sinepostol_Switch_4(config-if-range)#channel-group 3 mode on
Sinepostol_Switch_3(config-if-range)#no shutdown

Програмування процесу створення VLAN і розподілу портів між ними на прикладі
Sinepostol_Switch_0
Sinepostol_Switch_0(config)#vlan 16 // створення vlan на комутаторі
Sinepostol_Switch_0(config-vlan)#name Accounting // ім’я для vlan
Sinepostol_Switch_0(config-vlan)#vlan 36
Sinepostol_Switch_0(config)#vlan 26
Sinepostol_Switch_0(config-vlan)#name ResourcesDepartment
Sinepostol_Switch_0(config-vlan)#name Guest
Sinepostol_Switch_0(config-vlan)#vlan 99
Sinepostol_Switch_0(config-vlan)#name Management
Sinepostol_Switch_0(config-vlan)#vlan 100
Sinepostol_Switch_0(config-vlan)#name Native
Sinepostol_Switch_0(config-vlan)#exit
Sinepostol_Switch_0(config)#interface range f0/6-11 // налаштування 5 інтерфейсів
Sinepostol_Switch_0(config-if-range)#switchport mode access // режим інтерфейсів для отримання доступу
Sinepostol_Switch_0(config-if-range)#switchport access vlan 16 // достув до портів тільки для vlan 16
Sinepostol_Switch_0(config-if-range)#interface range f0/12-14
Sinepostol_Switch_0(config-if-range)#switchport mode access
Sinepostol_Switch_0(config-if-range)#switchport access vlan 36
Sinepostol_Switch_0(config-if-range)#exit

Програмування trunk портів
Sinepostol_Switch_0(config)#interface f0/1
Sinepostol_Switch_0(config-if)#switchport mode trunk // перехід в режим транкового порта
Sinepostol_Switch_0(config-if)#switchport trunk native vlan 100 // vlan для пакетів без міток
Sinepostol_Switch_0(config-if)#switchport trunk allowed vlan 16,26,36,99,100 // список мереж які мають доступ до транкового каналу
Sinepostol_Switch_0(config-if)#exit
Sinepostol_Switch_0(config)#interface gig0/1
Sinepostol_Switch_0(config-if)#switchport mode trunk
Sinepostol_Switch_0(config-if)#switchport trunk native vlan 100
Sinepostol_Switch_0(config-if)#switchport trunk allowed vlan 16,26,36,99,100
Sinepostol_Switch_0(config-if)#exit
Sinepostol_Switch_0(config)#interface vlan 99
Sinepostol_Switch_0(config-if)#ip address 192.168.40.98 255.255.255.224
Sinepostol_Switch_0(config-if)#exit
Sinepostol_Switch_0(config)#ip default-gateway 192.168.40.97
Sinepostol_Switch_0(config)#exit
Sinepostol_Switch_0# copy running-config startup-config

Програмування маршрутизатора router on a stick
Sinepostol_Router_2(config)#interface g0/0
Sinepostol_Router_2(config-if)#no shut
Sinepostol_Router_2(config-if)#exit
Sinepostol_Router_2(config)#interface g0/0.16 // налаштування підінтерфейсу для маршрутизації трафіку між vlan
Sinepostol_Router_2(config-subif)#encapsulation dot1Q 16 // тегування пакетів для данного підінтерфейсу
Sinepostol_Router_2(config-subif)#ip address 192.168.40.1 255.255.255.224
Sinepostol_Router_2(config-subif)#interface g0/0.26

Sinepostol_Router_2(config-subif)#encapsulation dot1Q 26
Sinepostol_Router_2(config-subif)#ip address 192.168.40.33 255.255.255.224
Sinepostol_Router_2(config-subif)#interface g0/0.36
Sinepostol_Router_2(config-subif)#encapsulation dot1Q 36
Sinepostol_Router_2(config-subif)#ip address 192.168.40.65 255.255.255.224
Sinepostol_Router_2(config-subif)#interface g0/0.99
Sinepostol_Router_2(config-subif)#encapsulation dot1Q 99
Sinepostol_Router_2(config-subif)#ip address 192.168.40.97 255.255.255.224
Sinepostol_Router_2(config-subif)#exit
Sinepostol_Router_2(config)#exit
Sinepostol_Router_2# copy running-config startup-config

Програмування протоколу DHCP для мереж VLAN на прикладі Sinepostol_Router_2
// виключення перших 10 адрес з пулів адрес для кожної vlan
Sinepostol_Router_2(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.10
Sinepostol_Router_2(config)#ip dhcp excluded-address 192.168.40.33 192.168.40.42
Sinepostol_Router_2(config)#ip dhcp excluded-address 192.168.40.65 192.168.40.74
Sinepostol_Router_2(config)#ip dhcp pool pollvlan16 // створення пулу адрес для vlan 16
Sinepostol_Router_2(dhcp-config)#network 192.168.40.0 255.255.255.224 // адреса підмережі з якої будуть видаватися IP–адреси для вузлів
Sinepostol_Router_2(dhcp-config)#default-router 192.168.40.1 // адреса порту маршрутизатора через який будуть видаватися адреси
Sinepostol_Router_2(dhcp-config)#dns-server 192.168.42.16 // адреса для звертання до dns-серверу
Sinepostol_Router_2(dhcp-config)#exit
Sinepostol_Router_2(config)#ip dhcp pool pollvlan26
Sinepostol_Router_2(dhcp-config)#network 192.168.40.32 255.255.255.224
Sinepostol_Router_2(dhcp-config)#default-router 192.168.40.33
Sinepostol_Router_2(dhcp-config)#dns-server 192.168.42.16
Sinepostol_Router_2(dhcp-config)#exit
Sinepostol_Router_2(config)#ip dhcp pool pollvlan36
Sinepostol_Router_2(dhcp-config)#network 192.168.40.64 255.255.255.224
Sinepostol_Router_2(dhcp-config)#default-router 192.168.40.65
Sinepostol_Router_2(dhcp-config)#dns-server 192.168.42.16
Sinepostol_Router_2(dhcp-config)#exit
Sinepostol_Router_2(config)#exit
Sinepostol_Router_2# copy running-config startup-config

Програмування функції безпеки портів
Sinepostol_Switch_0(config)#interface fa0/6 // вхід в інтерфейс
Sinepostol_Switch_0(config-if)#switchport mode access // режим інтерфейса для отримання доступу
Sinepostol_Switch_0(config-if)# switchport port-security // ввімкнення засобів безпеки
Sinepostol_Switch_0(config-if)# switchport port-security maximum 2 // забезпечення доступу до порту тільки для двох вузлів
Sinepostol_Switch_0(config-if)# switchport port-security violation restrict // при перевищенні кількості дозволених MAC-адрес забезпечує відкидування пакетів з невідомими адресами

Програмування протоколу NAT на прикладі Sinepostol_Router_3
Sinepostol_Router_3(config)#ip access-list extended _6 // іменований розширений список контролю доступу

Sinepostol_Router_3(config-ext-nacl)#deny ip 192.168.41.128 0.0.0.127 192.168.40.128 0.0.0.127 // заборона для видачі адреси, якщо пакет має дані адреси відправника і отримувача
Sinepostol_Router_3(config-ext-nacl)#permit ip 192.168.40.0 0.0.3.255 any // дозвіл для видачі адреси, якщо пакет має дані адреси відправника і будь-яку адресу отримувача
Sinepostol_Router_3(config)#ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224 // пул для динамічного виділення інтернет адрес
Sinepostol_Router_3(config)#ip nat inside source list 6 pool Internet overload // підміна адреси внутрішньої мережі на інтернет адреси згідно з списком контролю доступу
Sinepostol_Router_3(config)#ip nat inside source static 192.168.42.17 209.165.200.4 // статичний NAT для серверу
Sinepostol_Router_3(config)#interface Serial0/1/0
Sinepostol_Router_3(config-if)#ip nat outside // коли пакет надходить на порт то відбувається заміна інтернет адреси на адресу внутрішної мережі при проходженні через порт
Sinepostol_Router_3(config-if)#interface Serial0/0/0
Sinepostol_Router_3(config-if)#ip nat inside // коли пакет надходить на порт то відбувається заміна адреси внутрішної мережі на інтернет адресу
Sinepostol_Router_3(config-if)#interface Serial0/0/1
Sinepostol_Router_3(config-if)#ip nat inside
Sinepostol_Router_3(config-if)#interface g0/0
Sinepostol_Router_3(config-if)#ip nat inside

Програмування протоколу VPN
Sinepostol_Router_3
Sinepostol_Router_3(config)#access-list 110 permit ip 192.168.41.128 0.0.0.127 192.168.40.128 0.0.0.127 // список доступу для дозволу передачі трафіку через vpn тунель
Sinepostol_Router_3(config)#crypto isakmp policy 10 // створення IKE політики в якій вказуються бажані алгоритми і параметри створюваного захищеного каналу, які будуть запропоновані партнеру для узгодження..
Sinepostol_Router_3(config-isakmp)#encryption aes 256 // використовується для вказівки алгоритму шифрування повідомлень (в якості алгоритму шифрування використовується 256-bit AES)
Sinepostol_Router_3(config-isakmp)#authentication pre-share // призначено для вказівки методу аутентифікації сторін (pre-share аутентифікація здійснюється за допомогою визначених ключів)
Sinepostol_Router_3(config-isakmp)#hash sha // застосовується для вказівки хеш-алгоритму, який використовується в рамках IKE policy (sha вказує, що в якості хеш-алгоритму повинен використовуватися алгоритм SHA-1)
Sinepostol_Router_3(config-isakmp)#group 5 // забезпечує безпечний обмін ключами, які використовуються для шифрування даних
Sinepostol_Router_3(config-isakmp)#exit
Sinepostol_Router_3(config)#crypto isakmp key cisco address 64.100.13.2 // створення визначеного ключа для взаємодії з партнером за вказаною адресою
Sinepostol_Router_3(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac // використовується для формування набору перетворень - комбінації протоколів захисту і криптографічних алгоритмів, що застосовуються в захищуваному IPsec трафіку
Sinepostol_Router_3(config)#crypto map VPN-MAP 10 ipsec-isakmp створення криптографічної карти
Sinepostol_Router_3(config-crypto-map)#description VPN connection to Sinepostol_Router_0 // опис vpn з’єднання
Sinepostol_Router_3(config-crypto-map)#set peer 64.100.13.2 // адреса партнера по захищеному з’єднанню в криптографічній карті

Sinepostol_Router_3(config-crypto-map)#set transform-set VPN-SET // вказує, які набори перетворень можуть використовуватися з даним записом криптографічної карти
Sinepostol_Router_3(config-crypto-map)#set pfs group5 // використовується для установки опції PFS. Використання даної опції дозволяє підвищити рівень захищеності трафіку - при створенні кожного IPsec SA відбувається регулярна подача нових сесійних ключів.
Sinepostol_Router_3(config-crypto-map)#match address 110 // здійснює прив'язку списку доступу до запису криптографічної карти
Sinepostol_Router_3(config-crypto-map)#exit
Sinepostol_Router_3(config)#interface S0/1/0
Sinepostol_Router_3(config-if)#crypto map VPN-MAP // застосування криптографічної карти на інтерфейсі
Sinepostol_Router_0
Sinepostol_Router_0(config)#access-list 110 permit ip 192.168.40.128 0.0.0.127 192.168.41.128 0.0.0.127
Sinepostol_Router_0(config)#crypto isakmp policy 10
Sinepostol_Router_0(config-isakmp)#encryption aes 256
Sinepostol_Router_0(config-isakmp)#authentication pre-share
Sinepostol_Router_0(config-isakmp)#hash sha
Sinepostol_Router_0(config-isakmp)#group 5
Sinepostol_Router_0(config-isakmp)#exit
Sinepostol_Router_0(config)#crypto isakmp key cisco address 209.165.202.1
Sinepostol_Router_0(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac
Sinepostol_Router_0(config)#crypto map VPN-MAP 10 ipsec-isakmp
Sinepostol_Router_0(config-crypto-map)#description VPN connection to Sinepostol_Router_3
Sinepostol_Router_0(config-crypto-map)#set peer 209.165.202.1
Sinepostol_Router_0(config-crypto-map)#set transform-set VPN-SET
Sinepostol_Router_0(config-crypto-map)#set pfs group5
Sinepostol_Router_0(config-crypto-map)#match address 110
Sinepostol_Router_0(config-crypto-map)#exit
Sinepostol_Router_0(config)#interface Gig0/0
Sinepostol_Router_0(config-if)#crypto map VPN-MAP

ВІДГУКИ КОНСУЛЬТАНТІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

ВІДГУК

на кваліфікаційну роботу ступеню бакалавра на тему: “Комп'ютерна система обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі ”
студента гр. 123-17ск-1 Сенипостол Ілля Васильович

Завдання і зміст кваліфікаційної роботи ступеню бакалавра відповідає Об'єкт розробки: Комп'ютерна система обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета роботи розробка комп’ютерної системі обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Розроблена система вирішує наступні завдання:

- вимірювання активної потужності;
- вимірювання реактивної потужності;
- реєстрацію отриманої інформації;
- передачу інформації до серверу;
- візуалізацію отриманої інформації.

Розробка комп’ютерної мережі виконана відповідно до завдання на кваліфікаційну роботу бакалавра. Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота. Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці або додатках. В цілому кваліфікаційна робота ступеню бакалавра заслуговує оцінки “_____” балів при відповідному захисті, а студент Сенипостол І.В. присвоєння кваліфікації “бакалавр” за спеціальністю “123 Комп’ютерна інженерія ”.

Провідний консультант, _____ Бешта Д.О.
ас. каф. ІСтЕ ___.06.2020

РЕЦЕНЗІЯ

на кваліфікаційну роботу ступеню бакалавра на тему: “Комп'ютерна система обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі ”
студента гр. 123-17ск-1 Сенипостол Ілля Васильович

Завдання і зміст кваліфікаційної роботи ступеню бакалавра відповідає Об'єкт розробки: Комп'ютерна система обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета роботи розробка комп’ютерної системі обліку електричної енергії для коксохімічного підприємства з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Розроблена система вирішує наступні завдання:

- вимірювання активної потужності;
- вимірювання реактивної потужності;
- реєстрацію отриманої інформації;
- передачу інформації до серверу;
- візуалізацію отриманої інформації.

Розробка комп’ютерної мережі виконана відповідно до завдання на кваліфікаційну роботу бакалавра. Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота. Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці або додатках. В цілому кваліфікаційна робота ступеню бакалавра заслуговує оцінки “_____” балів при відповідному захисті, а студент Сенипостол І.В. присвоєння кваліфікації “бакалавр” за спеціальністю “123 Комп’ютерна інженерія ”.

Рецензент _____ _____

___.06.2020