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 Строценко Віталій Русланович
(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 з блокчейн технологією підтримки реєстру студентів ВНЗ першого рівня акредитації НТУ «ДП» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі
(назва за наказом ректора)

Керівник	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинг.	**інституційною**	
кваліфікаційної роботи	проф. Коротенко Г.М.			
розділів:				
апаратний розділ	доц. Ткаченко С.М.			
розрахунок мережі	ас. Панферова Я.В.			
Економічний розділ	ст. викл. Яремчук І.О.			
охорона праці	доц. Іконніков М.Ю.			

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 Строценко В.Р. **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 з блокчейн технологією підтримки реєстру студентів ВНЗ першого рівня акредитації НТУ «ДП» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі

затверджену наказом ректора НТУ «Дніпровська політехніка» від № ___

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 _____ проф. Коротенко Г.М.
(підпис п. керівника) (прізвище, ініціали)

Дата видачі 27.01.2020

Дата подання до екзаменаційної комісії 18.05.2020

Прийнято до виконання _____ Строценко В.Р..
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 121 с., 31 рис., _19_ табл., _1_ додаток, _6_ дж.

Об’єкт розробки: Комп’ютерна система з блокчейн технологією підтримки реєстру студентів ВНЗ першого рівня акредитації НТУ «ДП» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета: створення комп’ютерної системи з блокчейн технологією підтримки реєстру студентів ВНЗ першого рівня акредитації НТУ «ДП» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

У роботі викладені результати обстеження ВНЗ першого рівня акредитації НТУ «ДП».

Розроблена комп’ютерної системи з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, яка орієнтована на побудову системи реєстру студентів ВНЗ першого рівня акредитації НТУ «ДП» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі, а також для збору і підготовки статистичної інформації.

В спеціальній частині розроблені вимоги до кожної складової комплексу, здійснено 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

Розвиток інформаційного суспільства забезпечує швидкий доступ до інформаційних ресурсів у всьому світі. Інформаційно-комунікаційні технології значно змінюють зміст і практику освіти. Сьогодні значна частина матеріалів, за допомогою яких здійснюється навчальний процес, подається в електронному вигляді. Використання телекомунікацій, мультимедійних навчальних інформаційних ресурсів, інтернет-технологій, застосування штучного інтелекту сприяють істотним удосконаленням в освітній галузі.

В контексті актуальних напрямків розвитку української освіти в умовах переходу до цифрової економіки та освіти розглядається специфіка і особливості використання технології реплікованих розподілених баз даних («ланцюжків блоків» / "blockchain"). Пропонується використати цю технологію для вирішення як традиційних педагогічних завдань навчально-виховного процесу різного класу і рівня, так і інноваційних.

Дана технологія, широко застосовувана за кордоном і до сих пір не знайшла належного застосування в українській освітній практиці, заслуговує на увагу педагогів і дослідників як варіант передовий основи для пошуку нових ідей оновлення існуючих і популярних сьогодні в педагогічній практиці методик навчання і технологій використання в якості засобу навчання досягненням інформаційних технологій і науки «Інформатика», таким як, наприклад: штучний інтелект, віртуальна і доповнена реальність, а також масові навчальні онлайн курси, або МУК (MOOC, massive open online course).

На основі описаних в даній роботі матеріалів про використання «ланцюжків блоків» можливе проектування не тільки нових освітніх ресурсів для школи, а й нових освітніх курсів для навчання майбутніх учителів в умовах «цифрового освіти».

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика підприємства та умов застосування КС

Відповідно до наказу Міністерства освіти і науки України № 1636 від 20.12.2017 р. Державний вищий навчальний заклад «Національний гірничий університет» перейменовано в Національний технічний університет «Дніпровська політехніка». Політехнічний тренд розвитку університету є наслідком розширення спектра спеціальностей, пропонованих для здобуття вищої освіти по всіх щаблях і надає широкі можливості для здійснення закордонних стажувань, отримання міжнародних грантів і дипломів університетів-партнерів, а також паралельного навчання за іншою спеціальністю з метою отримання другої вищої освіти.

Університет був заснований в 1899 році як Катеринославське вище гірниче училище. Перший набір склав всього 77 осіб. Сьогодні загальна кількість студентів «Дніпровської політехніки» становить понад десяти тисяч. Університет готує висококваліфікованих фахівців за 40 спеціальностями, серед яких інженерні, комп'ютерні, філологічні та економічні. НТУ «ДП» - визнаний і відомий не тільки в межах України, а й в усьому світі, як навчальний і науковий центр.

В структуру університету входять: п'ять інститутів і дев'ять факультетів; три технікуму; аспірантура і докторантура.

Вища освіта, яку пропонує «Дніпровська політехніка» - це поєднання багаторічного досвіду, майже за 120 років існування, в підготовці висококваліфікованих фахівців, і новітніх методів навчання. Інформаційне забезпечення в університеті здійснюється за допомогою підручників, навчальних посібників і електронних ресурсів. Фонд бібліотеки університету складає близько 1,5 млн. Примірників. Бібліотека «Дніпровської політехніки» є одним з найбільших інформаційних центрів навчальних закладів в країні. Студенти, які навчаються в нашому університеті, мають великі можливості і широку мобі-

льність в європейському просторі. Важливе значення в НТУ «ДП» надається міжнародному обміну та стажування студентів і викладачів. Студенти мають можливість отримати два дипломи - нашого і університету, який є його міжнародним партнером.

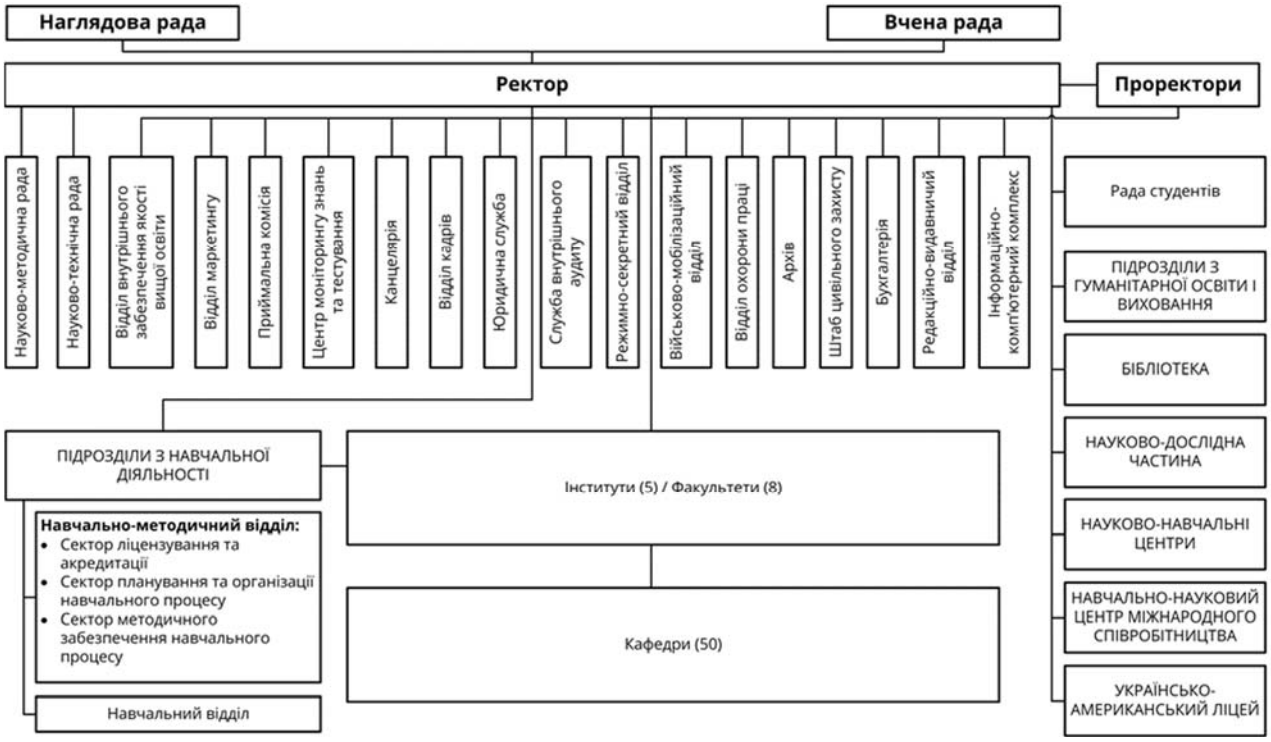

Рисунок 1.1 – Організаційна структура управління

Сьогодні в структурі вузу 9 профбюро, 468 профгруп, які об`єднують близько 9 тисяч членів профспілки.

Навчальний процес забезпечують близько тисячі викладачів, більше половини з яких мають науковий ступінь або вчене звання. Серед них: 25 лауреатів Державних премій в галузі науки і техніки України, кожен шостий - заслужений діяч науки і техніки, або відмінник освіти України.

Навчання передбачає ґрунтовну мовну підготовку під керівництвом досвідчених викладачів університету та запрошених з-за кордону. Рівень знань студентів достатній для складання іспитів і отримання сертифікатів міжнародного рівня, наприклад, TOEFL або Zertifikat Deutsch.

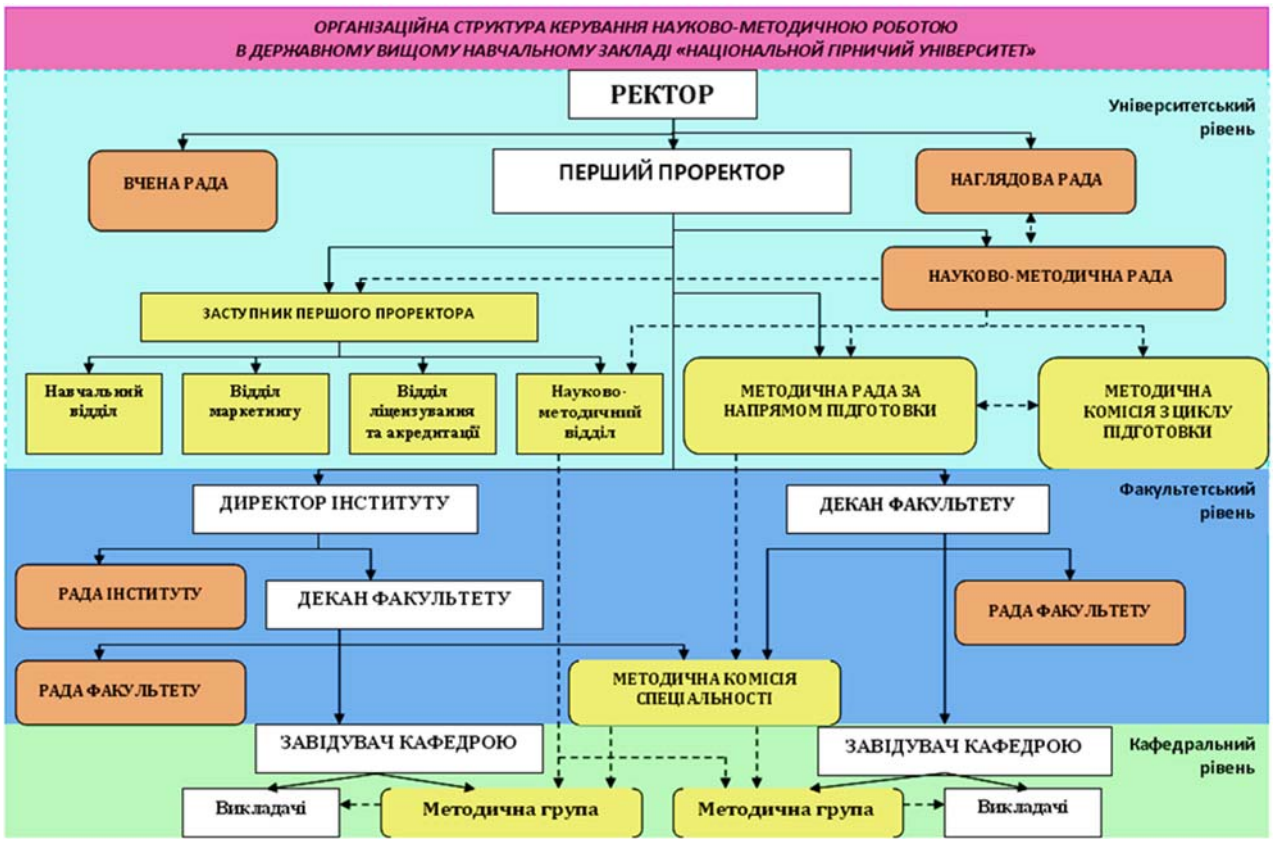

Рисунок 1.2 – Організаційна структура керування науково методичною роботою

Міжнародна діяльність «Дніпровської політехніки» спрямована на досягнення головної мети - визнання його наукових шкіл на світовій арені в сфері науки і підготовки фахівців.

«Дніпровської політехніка» прийнято в ряд престижних міжнародних освітніх і наукових організацій. Дев'яте місце згідно з рейтингом Webometrics свідчить про значне зміцнення позицій університету в інформації на просторі. За оцінкою міжнародної групи експертів ЮНЕСКО та центру «Евроосвіта», які становлять академічний рейтинг «Топ-200 Україна» (2017).

«Дніпровської політехніка» сьомий рік поспіль увійшов в десятку кращих і посідає шосте місце серед 200 університетів країни.

«Дніпровської політехніка» забезпечує взаємодію з вищими навчальними закладами першого рівня акредитації – структурними підрозділами Державного ВНЗ «НГУ» та суб’єктами навчальних та навчально-науково-

виробничих комплексів, що створені при НГУ з іншими ВНЗ І-ІІ рівнів України. До складу Національного ТУ «Дніпровська політехніка» на теперішній час входить такі структурні підрозділи:

- Павлоградський коледж Національного ТУ «Дніпровська політехніка»;
- Автотранспортний коледж Національного ТУ «Дніпровська політехніка»;
- Марганецький коледж Національного ТУ «Дніпровська політехніка»;
- НКЦ «Дніпровська політехніка» у м. Жовті Води.

Павлоградський коледж Національного ТУ «Дніпровська політехніка» є державним вищим навчальним закладом освіти першого рівня акредитації, що займає провідне місце в регіоні і здійснює підготовку молодших спеціалістів. Був заснований у вересні 1955 року як Павлоградський філіал Дніпропетровського механічного технікуму. Наказом Дніпропетровського Раднаргоспу від 05.01.61 № 107 технікум було перейменовано в Павлоградський машинобудівний технікум.

Автотранспортний коледж Національного ТУ «Дніпровська політехніка» є державним вищим навчальним закладом освіти першого рівня акредитації, здійснює підготовку молодших спеціалістів автомобільного транспорту. Створений на базі Дніпропетровського автотракторного технікуму, який був організований згідно з постановою ЦВК і РНК СРСР № 237 від 23 червня 1930 року і мав назву Дніпропетровський автомобільний технікум (з робочим вечірнім відділенням), який був підпорядкований Головному дорожньому управлінню УРСР.

Марганецький коледж Національного ТУ «Дніпровська політехніка» є державним вищим навчальним закладом освіти першого рівня акредитації, здійснює підготовку молодших спеціалістів. Створений на базі Марганецького гірничого технікуму відповідно до Постанови Ради Міністрів СРСРС від

03.02.1955р. № 661 та наказу Міністерства чорної металургії УРСР № 32 от 26.02.1955р.

Усі три коледжі мають приблизно одну типова організаційну структура управління (рис 1.3).

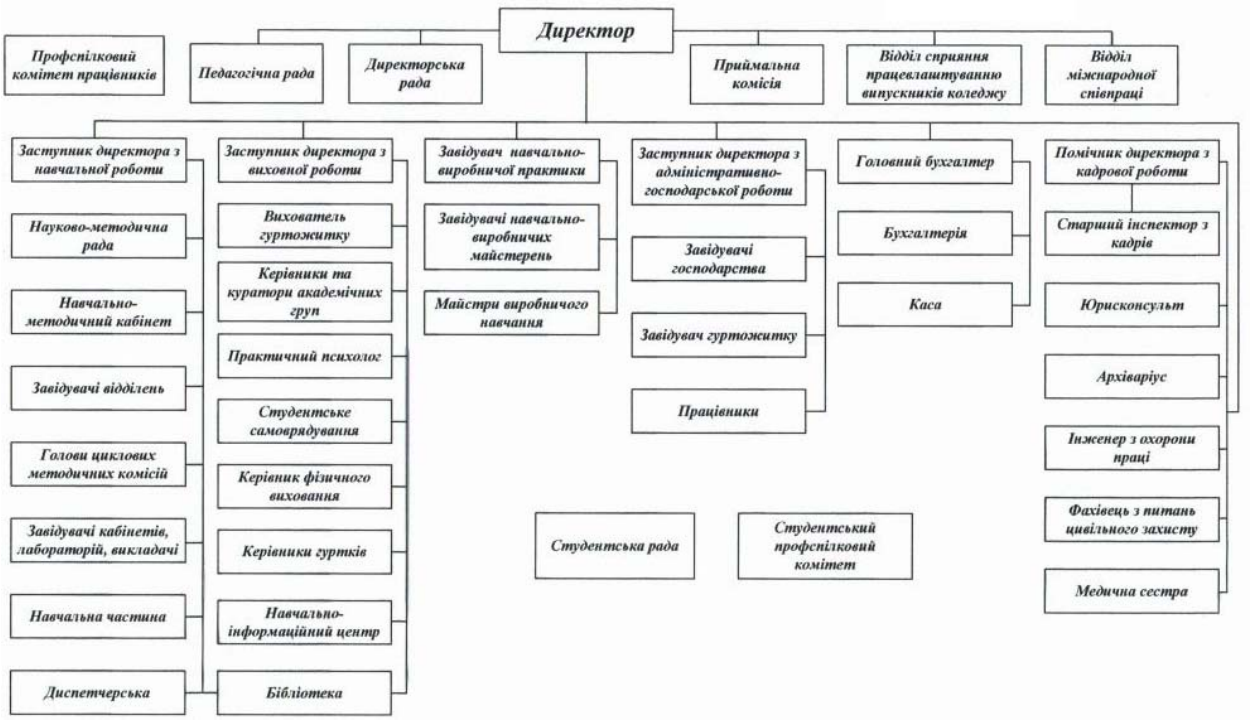

Рисунок 1.3 – Типова організаційна структура управління для коледжу

Об’єктом дослідження є Національний ТУ «Дніпровська політехніка» та його структурні підрозділи».

Об’єкт представляє собою багато будівель, розподілених по четирьох містах області: Дніпрі, Павлограді, Марганці та Жовтих водах. Топологічне розміщення об’єктів представлено на рис. 1.1.

До складу Національного ТУ «Дніпровська політехніка» на теперішній час входить такі структурні підрозділи:

- Павлоградський коледж Національного ТУ «Дніпровська політехніка»;
- Автотранспортний коледж Національного ТУ «Дніпровська політехніка»;

– Марганецький коледж Національного ТУ «Дніпровська політехніка»;
– НКЦ «Дніпровська політехніка» у м. Жовті Води.

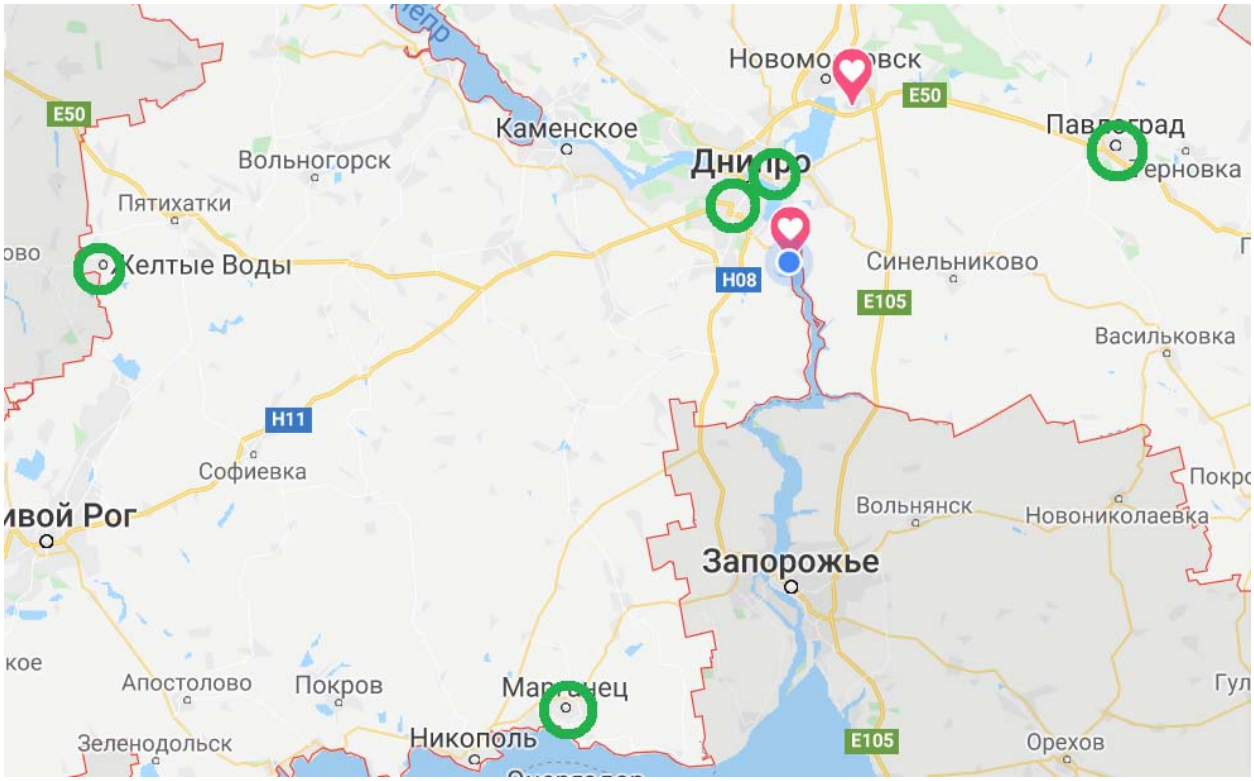

Рисунок 1.4 – Топологічна схема розміщення об’єктів у Дніпропетровській області

Топологічна схема розміщення структурних підрозділів Павлоградського коледжу Національного ТУ «Дніпровська політехніка» показано на рис. 1.5.

Адміністрація розташована на другому поверсі адміністративної будівля площею забудови 1433,8 кв.м, загальною площею 1211,9 кв.м., основною площею 990,7 кв.м..

Рисунок 1.5 - Топологічна схема розміщення структурних підрозділів Павлоградського коледжу Національного ТУ «Дніпровська політехніка»

1 - Директор
2 - Заступник директора з навч. роботи
3 - Помічники директора з кадрової роботи
4 - Відділ міжнародної співпраці
5 - Відділ сприяння працевл. випускників
6 - Навчально методичний кабінет
7 - Заступник директора з виховної роботи
8 - Заст. директора з госп. роботи
9 - Інженери з охорони праці
10 - Курівн. та куратори академ. груп
11 - Каса
12 - Директорська рада

1.2 Характеристика підприємства та умов застосування КС

1.2.1 Інформаційно-комунікаційних технології управління

Впровадження інформаційно-комунікаційних технологій управління змістом і організацією вищої освіти відбувається в таких напрямах:

– реалізація інформаційних процесів збирання, опрацювання, трансформації, зберігання науково-освітньої інформації;

– застосування програмних продуктів і апаратного обладнання для переробки інформації; вжиття організаційно-технічних заходів щодо забезпечення функціонування програмно-технічного комплексу (підтримка повноти, цілісності інформаційного навчально-наукового середовища та його оновлення).

Побудова взаємовигідних відносин ВНЗ з іншими навчальними закладами на принципах безперервного обміну досвідом освітньої й наукової діяльності шляхом створення кластерів – мереж знань – є знаковою тенденцією сьогодення. Кластер – це сконцентрована на певній території група взаємопов'язаних організацій, профільних за змістом діяльності та інноваційних за суттю.

Основна мета діяльності кластерів – створення конкурентних переваг і застосування нових знань, впровадження технологічних інновацій і збільшення інвестицій у знання, що передбачає високу мобільність, прогресивність, підприємливість.

Реалізація кластерної стратегії можлива за умови об'єднання та взаємопроникнення процесів діяльності сучасних підприємств, наукових установ і ВНЗ.

Ефективна інноваційна система (мережа дослідних центрів, університетів, центрів трансферу технологій, технопарків, фірм) на базі сучасної й адекватної інформаційної інфраструктури сприяє інтеграції організацій-конкурентів у споріднених галузях і сферах послуг з метою співпраці.

Інформаційна інфраструктура дає змогу керувати бізнес-процесами кластеру знань і контролювати їх, вирішувати й координувати основні завдання, забезпечує технології, всі інформаційні ресурси, загальні бази даних, центри з опрацювання й пошуку інформації, методи доступу до ресурсів, мережі передавання даних тощо.

Завдання інформатизації ВНЗ полягає: на рівні управління – в ефективному забезпеченні вищого керівництва і керівників підрозділів вірогідною стратегічною й оперативною інформацією та підтримці прийняття рішень адміністративно-управлінським персоналом; на рівні викладачів – в інформаційному забезпеченні навчальної й наукової діяльності та впровадженні сучасних ІКТ; на рівні студентів – у наданні доступу до навчально-методичної і наукової інформації.

Напрямами інформатизації ВНЗ можуть бути:

– розроблення й реалізація науково-технічної політики ВНЗ у сфері інформатизації; проектування й поетапне створення інформаційної інфраструктури ВНЗ; формування й розвиток компонентів автоматизованої системи управління (АСУ) ВНЗ, підсистем управління якістю підготовки фахівців і навчальним процесом, систем інформаційної підтримки освіти;
– створення, підтримка й розвиток корпоративної або локальної мережі ВНЗ; забезпечення якісного доступу до кластерів знань та мережі Інтернет зі всіх робочих станцій корпоративної мережі тощо.

На якість інформаційного забезпечення ВНЗ впливають такі чинники:

– впровадження електронних навчально-методичних комплексів дисциплін;
– створення єдиного освітнього інформаційного простору (ЄОІП), що сприятиме формуванню веб-представництва ВНЗ у світовому інформаційному просторі (сукупність інформації, технологій її опрацювання, збереження й передачі, що функціонує на основі єдиних принципів і за спільними правилами).

Єдиний освітній інформаційний простір забезпечуватиме інформаційну взаємодію всіх автоматизованих робочих місць, користувачів ВНЗ згідно з їхніми інформаційними потребами й санкціонованим доступом, а також взаємодію всіх учасників шляхом електронного документообігу у розподіленому інформаційному середовищі на основі єдиного сховища даних ВНЗ.

Сьогодні у вітчизняних ВНЗ у процес навчання активно впроваджуються новітні ІКТ: веб- та інтернет-технології; електронні підручники та електронні навчальні системи e-learning, e-education для дистанційного навчання; системи автоматизованого проектування; системи мультимедіа; технологія навчання із застосуванням міжнародних інформаційних архівів, електронних бібліотек; кластерні технології тощо.

Розвиток ІКТ, пов’язаний із використанням агентних технологій, визначає нові перспективи як у дистанційній освіті (remote education), так і в електронному навчанні.

Вирішення завдань інформатизації навчального закладу потребує створення відповідної інформаційної інфраструктури, для чого необхідно розробити і створити: телекомунікаційну мережу, що охоплює різноманітні засоби зв’язку й передачі даних, технології використання цього середовища та забезпечує доступ до регіональних, загальнодержавних і міжнародних телекомунікаційних мереж; систему баз даних різного призначення (адміністративних, наукових, методичних, інформаційно-довідкових) або єдине сховище даних; локальні мережі факультетів і корпусів.

Інформатизація є одним із важливих аспектів діяльності вищого навчального закладу, що сприяє підвищенню ефективності його основної діяльності та інтеграції в міжнародний освітній простір. Для цього насамперед потрібно забезпечити технічну основу для вирішення: оперативних завдань на кафедрах (належна база комп’ютерів, телекомунікаційне обладнання); завдань на рівні факультету (створення підмереж факультетів); на рівні вищого навчального закладу (створення корпоративної інформаційної мережі закладу) та на рівні науково-освітнього об’єднання у вигляді кластеру, регіонального (освітні портали, кластери знань) та міжнародного (віртуальні організації / кампуси) центрів дистанційного навчання.

Створення інформаційного середовища, що сприяє підвищенню ефективності основних напрямів діяльності ВНЗ (освіта, наука, управління, економічна діяльність), полягає у впровадженні інформаційних ресурсів, орієнтованих на певні групи користувачів, включаючи керівництво, професорсько-викладацький склад, аспірантів і студентів навчального закладу. Новітні ІКТ дають змогу основним користувачам швидко розв’язувати проблеми пошуку, подання та зберігання інформації. Нині у ВНЗ в електронному вигляді накопичено потужні інформаційні ресурси.

Водночас немає узагальненого підходу щодо розроблення та застосування єдиної концепції побудови освітнього інформаційного середовища ВНЗ.

Розроблення методів проектування і впровадження АСУ в навчальний процес із метою подальшого підвищення ефективності навчання має розрізнений характер: кожен навчальний заклад вирішує це завдання в індивідуальному порядку.

В єдиному освітньому інформаційному просторі зосереджуються основні процеси діяльності ВНЗ.

Система загалом забезпечує:

- масштабованість;
- розмежування прав доступу до інформації;
- розподілений доступ;
- належну інформаційну безпеку.

Архітектура АСУ будується за принципом «клієнт-сервер» із використанням єдиного інформаційного сховища ВНЗ, що дає змогу розв’язувати функціональні проблеми всіх структурних компонент.

1.2.2 Комп’ютерне забезпечення у вищих навчальних закладах

Стрімка інформація суспільства неминуче створює нові освітні стандарти, вимагає впровадження сучасних технологій у сферу освіти. Тому сучасне життя неможливо уявити без такого технічного засобу як комп'ютер, а особливо без нього не можливо уявити навчання.

Використання комп'ютерних програм на заняттях породжує в студентів інтерес, якого так часто не вистачає під час навчання. Сама присутність комп'ютера робить заняття незвичним, а значить, запам'ятається значна частина того, про що йшлося.

Основними перевагами використання інформаційних технологій в школі є:

- гнучкість у навчанні;
- індивідуальний підхід до кожного студента;
- широкі можливості для самостійного навчання студентів;
- широкі можливості для самоконтролю;
- пожвавлення заняття за рахунок використання мультимедіа (відео, звук, анімації), інтерактивні засобів, комп'ютерного моделювання;
- доступ до великої кількості інформаційних ресурсів;
- забезпечення можливостей для віддаленого навчання.

Загальна кількість комп’ютерів у вищих навчальних закладах складає ~ 95–100 тисяч одиниць; із них ~ 80 тис. – у ВНЗ III–IV рівня акредитації. Деякі кількісні показники комп’ютерного забезпечення у вищих навчальних закладах наведені у табл. 1.1.

Таблиця 1.1 - Кількісні показники комп’ютерного забезпечення у вищих навчальних закладах

Комп’ютерне забезпечення	Середня кількість комп’ютерів у ВНЗ, шт.	
	по Україні	на 1000 студентів
Комп’ютери у ВНЗ	967	92
Комп’ютери, під’єднанні до локальної мережі ВНЗ, з них: – у навчальних корпусах; – у студентських гуртожитках.	829 685 144	81 65 16
Комп’ютери, задіяні у дистанційному навчанні, з них: – комп’ютерні місця для розробників курсів; – комп’ютерні місця для працівників, які проводять дистанційне навчання.	77 38 39	– – –
Сервери із цілодобовим режимом роботи для накопичення та обміну інформаційними ресурсами	3	–

1.2.3 Програмне забезпечення

В силу широкого спектру напрямів підготовки, спеціальностей та спеціалізацій, організаційно-правових і господарських особливостей діяльності у ВНЗ використовується дуже багато різних програмних продуктів системного і прикладного характеру як власної розробки, так і сторонніх розробників. Ці

продукти в той чи інший спосіб задіяні у забезпеченні навчального процесу, наукової, проектно-технічної, організаційної, фінансової та іншої діяльності, а також забезпеченні мережевої взаємодії комп'ютерів і доступу до комунікаційних мереж.

У даному аналітичному огляді вирішено приділити увагу лише тим програмним продуктам, що стосуються забезпечення навчального процесу.

Їх умовно можна розділити на три основні групи:

1) програмні засоби, що використовуються для організації і керування навчальним процесом (умовна назва – Система "Деканат");
2) програмні засоби, що використовуються для забезпечення навчального процесу дистанційної форми навчання або її елементів (умовна назва – Система ДН);
3) Програмні засоби, що використовуються для контролю знань та оцінювання успішності навчання (умовна назва – Система тестування).

На рис. 1.6 показано відносний склад ВНЗ (у розрізі регіонів), що використовують для організації і керування навчальним процесом програмні засоби.

Рисунок 1.6 – Відносний склад ВНЗ (у розрізі регіонів), що використовують для організації і керування навчальним процесом програмні засоби

Результати вираховувалися як відношення кількості тих ВНЗ, що мають такі засоби, до загальної кількості ВНЗ, які взяли участь в анкетуванні.

На рис. 1.7 показано, що переважна кількість ВНЗ, які використовують системи керування навчальним процесом, мають власні програмні розробки (19%), решта ВНЗ використовують програми сторонніх виробників.

У той же час (див. рис. 1.8), власну платформу дистанційного навчання використовують лише 9% ВНЗ, більшість з них використовують платформи ДН визнаних виробників, а саме: 35% ВНЗ використовують платформу з відкритими кодами Moodle, 6% ВНЗ –систему дистанційного навчання “ПРОМЕТЕЙ”, решта використовує 20 програмних продуктів інших виробників.

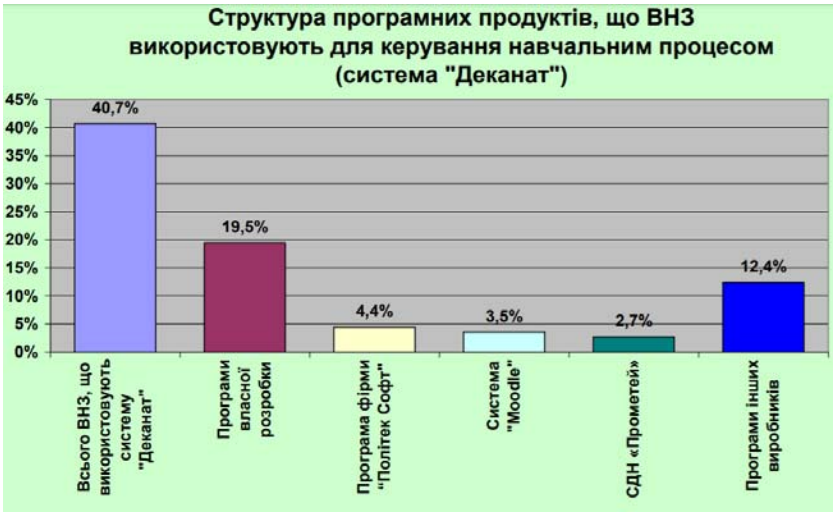

Рисунок 1.7 – Кількість ВНЗ, які використовують системи керування навчальним процесом

Дещо більший розкид спостерігається при аналізі даних стосовно використання у ВНЗ програмного забезпечення для систем тестування (див. діаграму 4). Так, наявність таких систем зазначили 63% ВНЗ, із них 19% – власного розроблення, 22% ВНЗ використовують платформу Moodle, 4% – платформу "Прометей", решта ВНЗ використовує 26 програм інших виробників.

На рис. 1.9 проілюстровано ступінь "ліцензованості" програмного забезпечення, що використовується для забезпечення дистанційної форми навчання або її елементів.

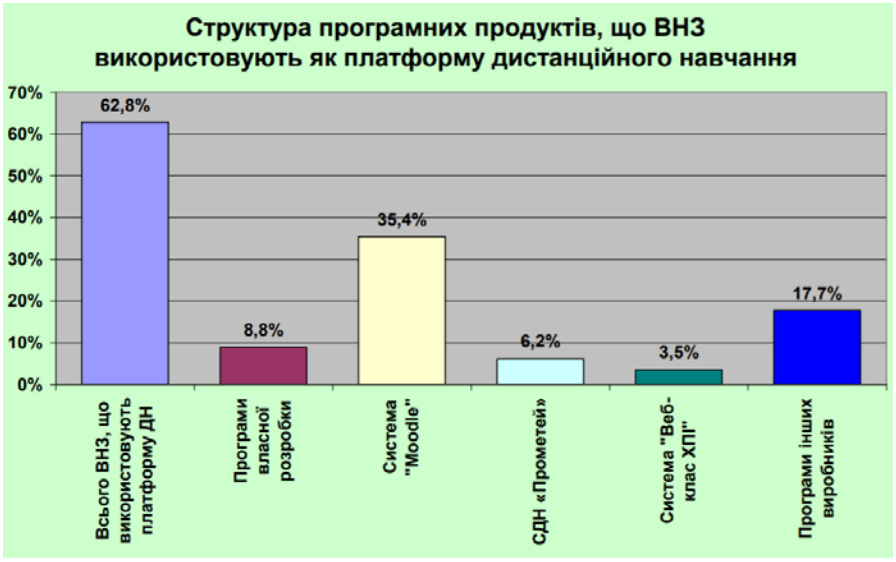

Рисунок 1.7 – Відносний склад ВНЗ які використовують платформу дистанційного навчання

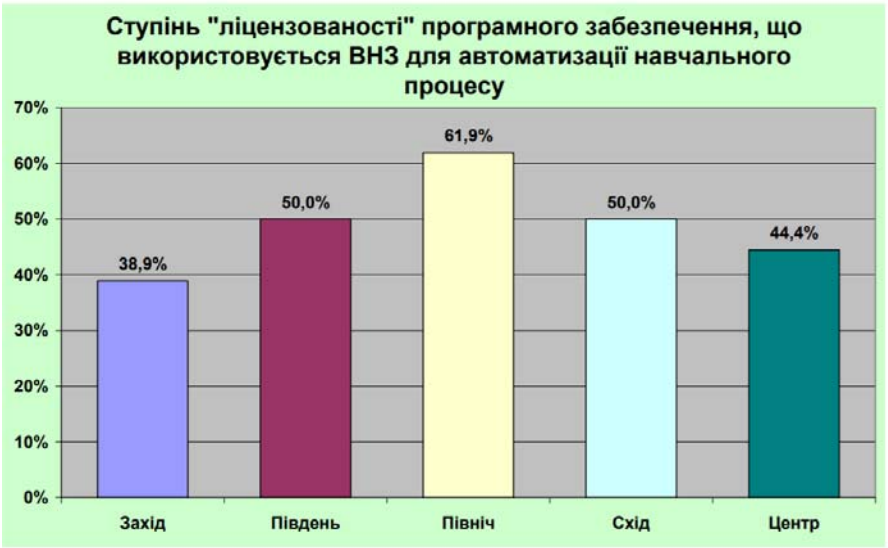

Рисунок 1.9 –"Ліцензованність" програмного забезпечення, що використовується для забезпечення дистанційної форми навчання або її елементів

Зазначені результати свідчать про те, що програмне забезпечення, яке використовується у сфері дистанційного навчання, представлене досить широким спектром програмних продуктів, які, у більшості своїй, не є сумісними між собою як на технологічному, так і на інформаційному рівні.

Тому, у разі їх подальшого використання, буде важко, забезпечити обмін між ВНЗ уже напрацьованими інформаційними ресурсами, а тим більше – створити спільний уніфікований доступ до цих ресурсів.

1.2.4 Доступ до телекомунікаційних мереж

Одним із важливих показників рівня впровадження ІКТ в навчальний процес і процес управління ВНЗ є забезпечення доступу викладачам і студентам до телекомунікаційних мереж: локальних (Інтранет), корпоративної в науково-освітній сфері (Українська науково-освітня телекомунікаційна мережа УРАН), глобальної мережі (Інтернет).

Аналіз даних показав, що майже кожний вищий навчальний заклад має локальну мережу і в середньому до 830 комп'ютерів ВНЗ під'єднанні до цієї мережі. Всі ВНЗ мають під'єднання до Інтернету. При цьому середня кількість провайдерських каналів для підключення одного ВНЗ до Інтернету складає ~ 1,9. Пропускна здатність каналів, в середньому, складає 150 Мбіт/с.

Кількість користувачів електронної пошти в одному ВНЗ, в середньому, дорівнює 980.

Особливий інтерес представляють дані про використання інформаційних можливостей мережі УРАН. Зупинимось на цьому питанні детальніше.

Створення і функціонування Української науково-освітньої телекомунікаційної мережі УРАН.

Українська науково-освітня телекомунікаційна мережа УРАН (Мережа УРАН) створена за рішенням Міністерства освіти України та Національної академії наук України за підтримки університетів, інститутів Міністерства освіти та Національної Академії наук згідно зі Спільною Постановою Прези-

дії Національної Академії наук України і Колегії Міністерства освіти України від 20 червня 1997 р.

Експлуатація та подальший розвиток Мережі УРАН здійснюється Асоціацією УРАН згідно із Концепцією Національної програми інформатизації та Державною Програмою «Інформаційні та комунікаційні технології в освіті і науці» на 2016-2020 роки.

Діяльність Асоціації є неприбутковою, а розвиток мережевої інфраструктури забезпечується в основному за рахунок цільового державного фінансування або міжнародних грантів. Асоціація УРАН налічує 67 вищих навчальних закладів та наукових установ.

Головним призначенням Мережі УРАН є забезпечення установ, організацій та фізичних осіб в сферах освіти, науки та культури України інформаційними послугами на основі Інтернет-технологій для реалізації професійних потреб та розвитку зазначених галузей. Такі послуги передбачають, зокрема, оперативний доступ до інформації, обмін нею, її розповсюдження, накопичення та оброблення для проведення наукових досліджень, електронного навчання, електронного тестування, використання методів телематики, функціонування електронних бібліотек, віртуальних лабораторій, проведення телеконференцій, реалізації дистанційних методів моніторингу тощо.

Мережа УРАН будується за ієрархічним принципом: у кожному місті України, що є значним осередком наукової та освітньої діяльності, створюється регіональний вузол мережі на базі університету або наукової установи.

Базовою організацією Головного центру керування Мережею УРАН є Міністерство освіти і науки у м. Києві.

Головний центр керування Мережі УРАН забезпечує основний інформаційний сервіс мережі та функціонування її бекбону. Крім того, Головний центр керування забезпечує функції регіонального вузла для користувачів Київського регіону.

Базовими організаціями Регіональних вузлів є: 16 ВНЗ в різних регіонах та 2 установи НАН України.

Розбудову міських волоконно-оптичних сегментів було здійснено протягом 1997-2007 років в рамках інфраструктурних грантів НАТО (NIG 971779 у 1997, NIG 975961 у 2000, NIG 978384 у 2001, NIG 981531 у 2004) і державного замовлення з боку Міністерства освіти і науки.

Сьогодні Мережа УРАН фізично об‘єднує понад 100 науково-дослідницьких та освітніх закладів у 18 із 25 областей України та експлуатує волоконно-оптичні мережі у 12 містах загальною довжиною близько 200 тис. км. Топологію мережі УРАН наведено на рис. 1.8.

Рисунок 1.10 – Топологія мережі УРАН

В рамках реалізації Державної програми «Інформаційні і комунікаційні технології в освіті і науці» на 2006-2010 рр., у 2007 році був підписаний договір про підключення Мережі УРАН до пан-Європейської науково-освітньої мережі GÉANT2 і було організовано взаємо-з’єднання мереж УРАН та

GÉANT2 у Польщі через канал 155 Мбіт/с, організований провідним оператором зв'язку для GÉANT2 компанією Memorex Telecommunication (Австрія).

GÉANT2 – це високошвидкісна мережа Європи, що об'єднує каналами пропускної спроможності 10-40 Гбіт/с національні наукові мережі європейських країн. Крім європейських країн GÉANT2 пропонує глобальні зв'язки з повністю інтегрованим сервісом з національними науковими мережами у Північній (Internet2) та Південній (ALICE) Америці, Азії (TEIN2), Середземномор'ї (EUMEDCONNECT), Африці.

Сьогодні до GEANT2 підключено 34 європейські країни.

Національні науково-освітні мережі країн-членів GEANT (за принципом «одна національна мережа»-«одна країна») мають високошвидкісний доступ до інформаційних і обчислювальних ресурсів по спеціалізованих каналах передачі даних із швидкістю більше 500 Гб/с. Загалом до GEANT мають доступ більше 3 млн. науковців, які представляють більше 3 500 університетів і наукових установ Європи.

Інтеграція з європейськими науково-освітніми мережами у рамках GEANT відкриває нові можливості України доступу до наукових і освітніх інформаційних ресурсів, зокрема, до віддалених центрів супер-комп`ютерних обчислень і наукових даних, електронних бібліотек, баз даних і знань, інформаційних пошукових систем, ресурсів дистанційного навчання тощо.

1.2.5 Електронні інформаційні ресурси навчального призначення

Звернення до пошукових систем дозволяє констатувати, що існує значна кількість освітніх ресурсів. Умовно каталоги освітніх ресурсів можна класифікувати в залежності від: цільового призначення та кола користувачів; форми представлення ресурсів; виду освіти (дошкільна, шкільна, вища, післядипломна, аспірантура, самоосвіта та інші); форм навчання (дистанційна,

допоміжна до аудиторних занять, підготовка самостійних завдань, у тому числі рефератів, конкурси, олімпіади, тести тощо).

У межах цього аналітичного огляду розглядатимуться лише електронні інформаційні ресурси навчального призначення для потреб вищої школи(рис. 1.11) .

Як показує практичний досвід, створення електронних навчальних матеріалів потребує високої кваліфікації розробників та значних витрат фінансових і часових ресурсів. Так, вартість створення електронного курсу може складати від 5 до 50 тис. доларів США, термін створення у середньому – 6-8 місяців.

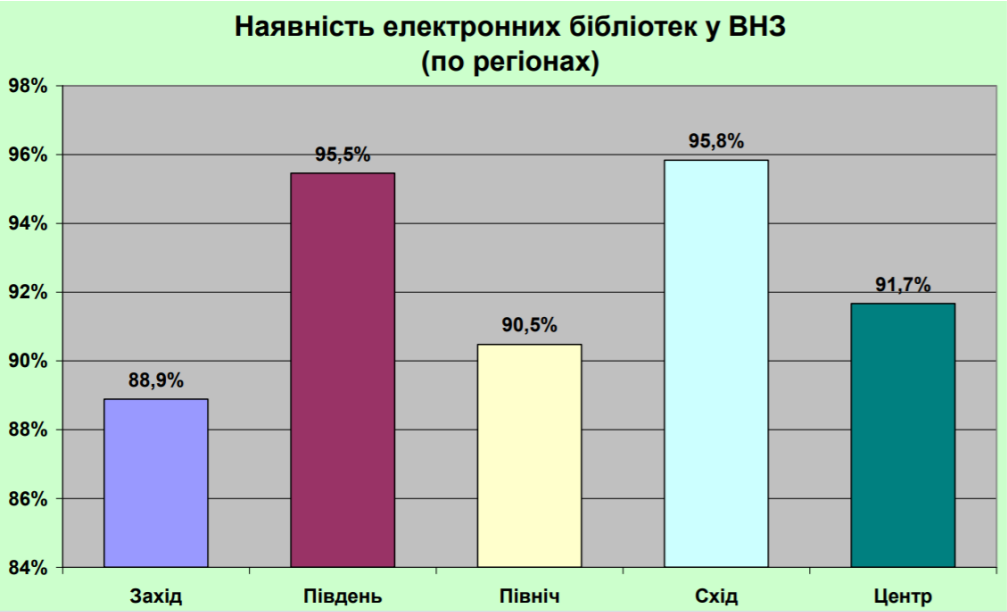

Рисунок 1.11 – Електронні бібліотеки

Тим не менше, для забезпечення відповідності якості навчання сучасним потребам навчальні заклади йдуть на такі витрати, де процес напрацювання інформаційних ресурсів відбувається за рахунок власних можливостей, у тому числі фінансових. При цьому значна кількість цих ресурсів створюється ініціативна педагогами, науковцями, інженерами та студентами.

У більшості ВНЗ акумуляторами напрацьованих інформаційних ресурсів є електронні бібліотеки, де вони накопичуються, у більшості своїй, у вигляді файлів різного формату.

1.2.6 Використання ІКТ в управлінні освітньою сферою

Автоматизація управління навчальним закладом є одним з пріоритетів будь-якого сучасного університету.

Нагальною і можливою комплексна автоматизація стала з моменту широкого впровадження ІКТ і новітніх засобів навчання у організацію навчального процесу.

На поточний момент на різних етапах впровадження комплексної автоматизації управління навчальним закладом знаходяться близько 34% ВНЗ III-IV рівня акредитації (рис. 1.12).

Найбільш показовими в цьому плані є проекти автоматизації, що реалізовані в Київському національному університеті імені Тараса Шевченка і Східноукраїнському національному університеті імені Володимира Даля.

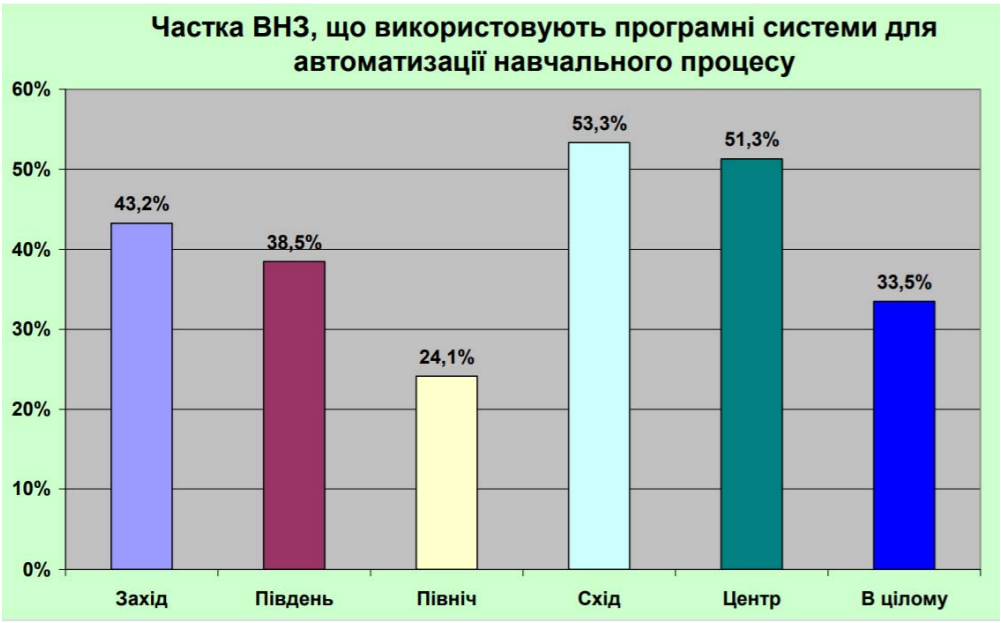

Рисунок 1.12 – Комплексна автоматизація управління навчальним закладом

1.3 Огляд існуючих інженерних рішень КС в галузі

У загальному випадку структура інформаційних підсистем у складі АСУ ВНЗ має виглядати так:

- підсистема «Управління ВНЗ»;
- підсистема «Організаційно-адміністративне забезпечення»;
- підсистема «Управління документообігом»;
- підсистема «Управління персоналом»;
- підсистема «Матеріально-технічне забезпечення»; підсистема «Управлінський облік»;
- підсистема «Маркетингові дослідження»;
- підсистема «Викладання і навчання»;
- підсистема «Управління дослідженнями і грантами»;
- підсистема «Академічні та студентські служби».

Отже, функціонують два рівні організації інформаційних процесів у ВНЗ: навчальний процес та економічна діяльність ВНЗ у цілому.

Для прикладу розглянемо автоматизацію діяльності в нашому університеті, де впроваджено спеціалізований програмний продукт «Автоматизація навчальної частини», розроблений із використанням компонент «Оперативний облік» програмного комплексу «1С: підприємство 7.7» (програмний продукт використано саме з метою автоматизації управління навчальним закладом, а не для обліку бухгалтерської інформації). Програма «Автоматизація навчальної частини» призначена для автоматизації ведення бази студентів і викладачів, роботи приймальної комісії і навчального відділу закладу, оформлення результатів складання сесії і призначення стипендій.

У програмі реалізовано можливості з управління діяльністю навчально-методичного відділу вищого навчального закладу. Ця функція дає змогу працювати зі списками факультетів і кафедр, списком дисциплін, які можуть викладатися на кафедрі, а також списком груп студентів з кожного факультету.

Є можливість ведення кадрового обліку викладачів, що базується на реєстрації інформації про співробітників навчального закладу. Для роботи з абітурієнтами передбачено ведення списку вступників з їхніми персональними даними. Програма забезпечує опрацювання навчальних планів і графіків навчального процесу. Користувач може вводити навчальні плани для кожної спеціальності, зазначати дисципліни, які викладаються за семестрами, виконувати розподіл за годинами для лекційних і семінарських занять, зазначати час для самостійної підготовки. Отримані дані дають змогу сформувати звіт «Навчальний семестровий план» для кожної навчальної групи. Внесення змін до навчальних планів автоматично відображається також у документах, де фіксується поточна академічна заборгованість студентів. Передбачено й формування звіту «Графік навчального процесу».

Переваги, які надає комплексна автоматизація вищого навчального закладу за всіма видами його діяльності, є очевидними, проте у більшості ВНЗ нашої країни вона так і не відбулася з багатьох причин: брак коштів, спеціалістів тощо. Тому створено лише фрагменти подібних систем, адаптованих до специфіки певного вищого навчального закладу.

АСУ ВНЗ є великою складною динамічною системою, яка потребує передусім розроблення й реалізації концепції системи управління ВНЗ; створення, підтримки й розвитку комплексу технічних засобів інформаційної інфраструктури АСУ ВНЗ (що потім може бути компонентою кластера знань).

АСУ закладу вищої освіти зазвичай відображає його функціонально-структурну схему.

Керівництво вищого навчального закладу має добре усвідомлювати перспективність і вигоди автоматизації навчального закладу, які полягають, зокрема, у запровадженні дистанційної освіти; створенні підсистеми управління якістю освіти, мультимедійних та електронних навчальних посібників, програмно-методичних комплексів; автоматизації науково-інноваційної, кадрової, планово-економічної та фінансової діяльності, а також поліпшенні пе-

репідготовки фахівців. Кінцевою метою інформатизації є забезпечення якісного доступу до університетських і світових інформаційних ресурсів для керівництва, професорсько-викладацького складу, аспірантів і студентів навчального закладу.

Отже, очевидною є потреба в розробленні єдиної уніфікованої концепції побудови освітнього інформаційного середовища ВНЗ, що повною мірою враховувала б можливості створення, поширення й застосування розподілених та інтегрованих баз даних і знань, орієнтованих на освітні послуги з урахуванням національних вимог та міжнародних стандартів системи освіти.

Комп'ютеризація й доступ до мережі Інтернет – це не лише нові технічні можливості для сфери освіти, а й дружній інтерфейс машинно-діалогового режиму, доступ до гігантських обсягів інформації та можливість її візуалізації.

У структурі освітнього інформаційного середовища вищого навчального закладу проект компоненти «Освітнє інформаційне середовище» складається з блоків: управління навчанням (інструктивний блок), інформаційного (модуль інформаційних ресурсів), контрольного (модуль тестування й оцінювання) та комунікативного (система інтерактивного викладання), – а також сервісної системи.

Наявність розвиненої інформаційно-довідкової бази скорочує витрати часу під час вивчення певних питань, оптимізує процес пошуку додаткової й довідкової літератури, дає змогу оперативно за допомогою системи зв'язків звернутися до необхідного розділу бази.

Сучасні інструментальні засоби відкривають широкі перспективи для візуалізації та інтерактивності навчального процесу. Однією з дидактичних функцій освітнього інформаційного середовища є можливість використання у навчальному процесі універсального програмного забезпечення (Statistica, Mathematica, Eviews тощо).

Завдяки новому рівню інформаційного забезпечення стає можливим прийняття таких управлінських рішень, які б сприяли: удосконаленню методів освітньої діяльності; раціональному використанню праці педагогів та адміністрації ВНЗ; підвищенню якості та оперативності вирішення планово-економічних, методичних та інших завдань; формуванню загального інформаційного простору в системі освіти.

Нині дедалі важливішим стає адекватне інформаційне представництво вищого навчального закладу в мережі Інтернет, що передбачає створення офіційного сайту з розробкою його концепції, визначення цільової аудиторії: студенти, викладачі, споживачі освітніх послуг, ЗМІ, учасники кластерів знань.

Метою створення офіційного сайту є:

- представлення навчального закладу в глобальній мережі;
- формування його іміджу, інвестиційної привабливості;
- забезпечення входу в освітній портал та на інші сайти; створення інформаційного середовища для абітурієнтів, студентів і працівників закладу;
- забезпечення відкритості й доступності інформації про діяльність ВНЗ;
- представлення інтересів навчального закладу в інформаційному просторі світу.

Завданнями офіційного сайту є: надання інформації про структуру вищого навчального закладу і його діяльність завдяки розробленій організаційній онтології закладу, навчально-методичної та нормативної інформації для студентів, викладачів і співробітників, інформації для абітурієнтів; підтримка зв’язків з іншими науково-освітніми закладами і підприємствами.

За достовірність, актуальність і коректність викладу інформації і матеріалів, наданих для публікації на офіційному сайті, відповідають керівники підрозділів, які надали інформацію. Основними джерелами інформації офі-

ційного сайту університету можуть бути: рішення вченої ради; накази й розпорядження ректора; бази даних системи електронного документообігу; офіційні видання; інформація про заплановані заходи (конференції, семінари).

Сучасним засобом веб-представництва вищого навчального закладу є його організаційна онтологія (формалізоване подання знань щодо структурних підрозділів навчального закладу, зв'язків між ними, взаємної підпорядкованості і призначення).

Організаційна онтологія дає змогу відобразити основні відомості про спектр освітніх послуг, кадровий склад закладу, посадові обов'язки і сферу відповідальності його персоналу.

Гносеологічні й онтологічні концепції структуризації знань в економічних відносинах визначаються тим, що вони є частиною інтелектуального капіталу. В загальнонауковому аспекті знання – це перевірений суспільно-історичною практикою і засвідчений логікою результат процесу пізнання дійсності, адекватне її відображення у свідомості людини у вигляді уявлень, понять, думок, теорій.

При цьому структура знань має гносеологічну основу залежно від природи їх формування – наукові, житейські, художні тощо. Водночас є підстави для застосування й онтологічного підходу до структуризації знання і близьких до нього категорій щодо напряму їх використання.

Якщо йдеться про інтелектуальний капітал, з цією метою можна вживати поняття «корпоративні знання» (КЗ) як сукупність загальнонаукових і спеціальних знань, виробничого досвіду і навичок, баз знань і даних, що використовуються організацією для отримання економічних і технологічних результатів.

У загальному випадку в КЗ треба виокремити нормативні знання, ноу-хау, технологічні інструкції.

Іншу групу знань – дескриптивних – утворюють загальнонаукові та спеціальні знання.

Онтологію, яка відображає структуру певної організації, тобто знання про організаційну й функціональну структуру суб'єкта економічної діяльності, його основні компоненти і зв'язки між ними, називають організаційною онтологією. Основні два класи організаційної онтології – це працівник і підрозділ.

Особливістю організаційної онтології є те, що їй відповідає зв'язний граф, тобто елементи, які входять до складу онтології, пов'язані між собою.

Вона містить:

- інформацію про працівників підприємства, ієрархію виробничих відносин;
- ресурси, що використовуються в організації;
- продукцію та послуги, створення яких є результатом роботи організації;
- структурні одиниці й зв'язки між ними.

Приклад організаційної онтології для Переяслав-Хмельницького ДПУ імені Григорія Сковороди подано на рис. 1.13.

Відомості подаються мовою OWL, що зрозуміла для сучасних пошукових механізмів у мережі Інтернет.

Наприклад, якщо перед інтелектуальним програмним агентом у вебсередовищі постає завдання пошуку вищого навчального закладу, в якому можна отримати декілька спеціальностей та кваліфікацій, або факультету, на якому викладають певну дисципліну, така організаційна онтологія дасть змогу пошуковому механізму виконати інформаційний пошук, а за потреби – надати користувачеві інформацію про тих осіб, з якими потрібно зв'язатися для отримання детальнішої інформації.

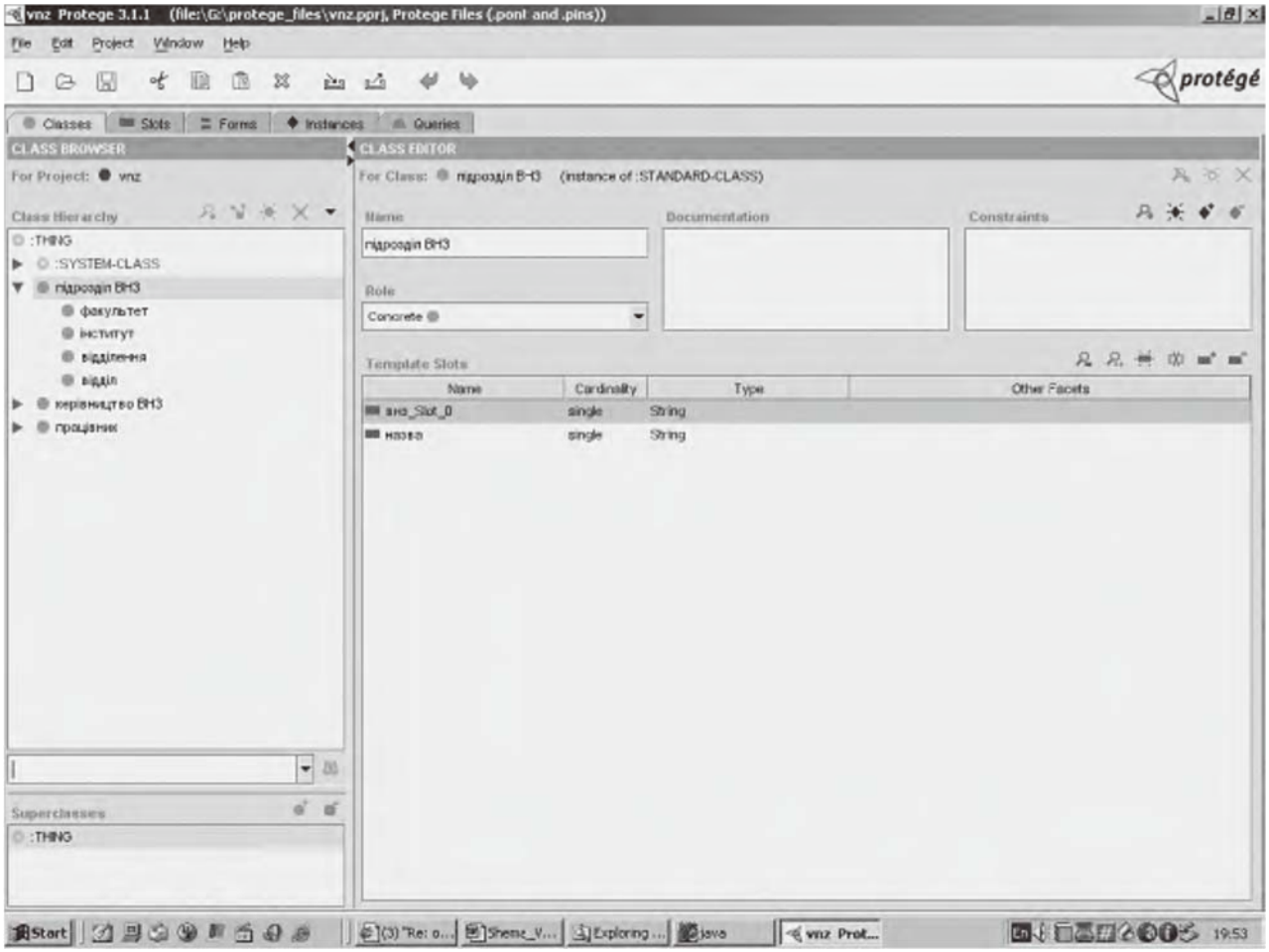

Рисунок 1.13 - Приклад організаційної онтології вищого навчального закладу

Важливим аргументом на користь використання онтології для описування організаційної структури вищого навчального закладу є можливість посилання на зовнішні бази знань, також представлені у вигляді онтологій. Інформація про осіб, які тут працюють або навчаються, може супроводжуватися посиланнями на персональні веб-сторінки, профілі тощо. Це розширює сферу застосування організаційної онтології навчального закладу.

Організаційна онтологія має розміщуватися на сайті або порталі закладу (головній сторінці) для того, щоб інформаційно-пошукові системи коректна індексували сайт і забезпечували доступ користувачів, котрим ця інформація потрібна. Це сприяє відкритості й доступності знань про вищий навчальний заклад.

Отже, процес інформатизації вищого навчального закладу має враховувати такі пріоритети:

- інформатизацію органів управління ВНЗ, що забезпечує виконання їхніх важливих функцій; інформатизацію навчального процесу, що значно розширює можливості підвищення його якості;
- інформатизацію наукової діяльності, що надає можливість для публікації наукових і методичних робіт в інформаційному середовищі, доступу до різних баз даних і електронних бібліотечних фондів навчального закладу, а також кластерів знань, грантів, міжнародних наукових програм.

Підсумовуючи викладене вище, варто зазначити, що адекватне інформаційне представництво вищого навчального закладу у мережі Інтернет нині набуває важливого значення. При цьому ефективним інформаційним засобом представлення навчального закладу в світовому інформаційному розподіленому середовищі є організаційна онтологія.

1.4 Визначення можливих напрямків рішення поставлених завдань

Таким чином в контексті актуальних напрямків розвитку української освіти в умовах переходу до цифрової економіки та освіти треба розглянути специфіку і особливості використання технології реплікованих розподілених баз даних, та використати цю технологію для вирішення, як традиційних педагогічних завдань навчально-виховного процесу різного класу і рівня, так і інноваційних.

У даній роботі планується розглянути реалізацію захищеного з’єднання на базі технології яка добре себе зарекомендувала у сфері криптовалют – блокчейн. В її основі лежать алгоритми, що дозволяють запобігти підміні інформації та несанкціонованому доступу. Ці особливості блокчейн можуть створити нові принципи взаємодії з інформацією та дати розвиток новому поколінню мереж.

Для створення комп'ютерної система з блокчейн технологією підтримки реєстру студентів ВНЗ першого рівня акредитації НТУ «ДП» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі розглянимо детально технологію блокчейн.

1.4.1 Аналіз принципів структурної побудови блокчейн мереж

Блокчейн, тобто ланцюжок блоків транзакцій (англ. Blockchain, від block –блок, chain – ланцюг) – розподілена база даних, яка підтримує перелік записів, так званих блоків, що постійно зростає. База захищена від підробки та переробки. Кожен блок містить мітку часу та посилання на попередній блок хеш дерева.

1.4.2 Визначення складових блокчейн.

Особливості роботи технології, основні принципи функціонування мережі та технологій в її складі.

Технологія блокчейн стала дійсно винахідливим творінням думки людини, або групи людей, що працювали під псевдонімом Satoshi Nakamoto. З моменту винайдення та формулювання принципів роботи мережі ця технологія зазнала чималих змін та популярності в світі.

Можливість поширювати інформацію по мережі без її копіювання між учасниками мережі – так блокчейн створив нову основу для нового типу всесвітнього інтернету. Оригінальна розробка технології була спрямована на винайдення нового слова в сфері цифрових валют – криптовалют, таких як Bitcoin (укр., дослівно, Цифрова бітова монета), ETH (Ethereum), та інших. Але, з часом, спеціалісти в технічній сфері почали винаходити нові варіації і потенціали такого методу.

Блокчейн це незламний цифровий кластер для запису змін в мережі, що може бути запрограмована не тільки на запис фінансових транзакцій, але й будь яких інших існуючих значень – будь-якої інформації в світі. (Don &

Alex Tapscott, автори “Blockchain Revolution” ,“Революція Блокчейн”, 2016 р.).

В основу технології блокчейн – роботу всіх механізмів закладено використання таких технологій та методів роботи і шифрування даних:

- асиметричні алгоритми шифрування або «асиметричні криптосистеми» (пари “приватних” та “публічних” ключів);
- хеш-функції або “хешування” даних (функції MD та SHA);
- хеш-таблиці для запису результатів хешування – операцій в блоках транзакцій (використання хеш-дерева типу “Дерево Меркла”);
- смарт-контракти (англ. Smart Contracts) – метод передачі даних (цифрових цінностей) від однієї особи до іншої;
- токени та реалізація механізму Proof of concept (POC) – доказ концепції, як методу верифікації події (затвердження угоди) в системі.

Визначимо поняття кожного вище зазначеного терміну з переліку.

Асиметричні алгоритми шифрування – захист даних користувача, що передаються в мережу блокчейн. Асиметричні криптосистеми – ефективні системи криптографічного захисту даних, які також називають криптосистемами з відкритим ключем. В таких системах для зашифровування даних використовують один ключ, а для розшифровування – інший (звідси і назва – асиметричні). Перший ключ є відкритим і може бути опублікованим для використання усіма користувачами системи, які шифрують дані.

Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних отримувач зашифрованої інформації використовує другий ключ, який є секретним (закритим). Ключ розшифровування не може бути визначеним з ключа зашифровування.

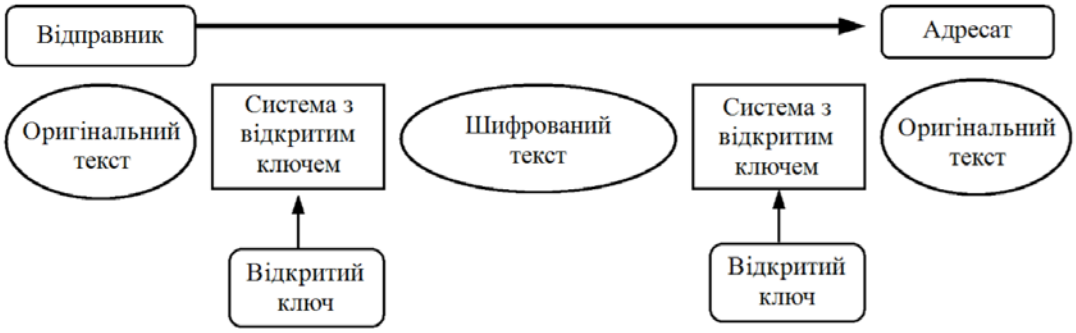

Рисунок 1.14 - Схема передачі даних в асиметричних криптосистемах

Щоб гарантувати надійний захист інформації, системи з відкритим ключем (СВК) обов'язково мають відповідати двом очевидним та важливим правилам:

1. Перетворення вихідного тексту повинно бути незворотнім і виключати можливість відтворення зашифрованої інформації за допомогою відкритого ключа;
2. Визначення закритого ключа на основі відкритого повинно бути неможливим з врахуванням сучасних досягнень та можливостей обчислювальної техніки. При цьому, обов'язковою є точна оцінка складності (кількості операцій та часу) для зламу шифру.

Ідея криптографії з відкритим ключем тісно пов'язана з ідеєю односторонніх функцій, або таких функцій f(x), що знаючи значення аргументу 'x' достатньо легко знайти значення функції, тоді як визначення аргументу з функції досить складне в сенсі теорії. Тому, фактично, для знаходження аргументу з функції користувачеві необхідно мати додатковий спосіб облегшити розшифрування і мати спосіб легко відтворити початкове значення.

Цим способом і виступає ключ користувача та на даному прикладі виступає значенням функції так, що f(x) = y, де 'y' – закритий ключ в системі СВК.

В цілому, всі сучасні криптосистеми з відкритим ключем використовують один з даних типів незворотних перетворень:

1. розбиття великих чисел на прості множники;

2. розрахунок логарифмічної функції в скінченному просторі;
3. розрахунок коренів алгебраїчних рівнянь.

Також, кажучи про практичну цінність СВК, слід зазначити можливі застосування таких алгоритмів:

1. як самостійні засоби захисту передавання та зберігання даних;
2. як засіб для розподілення ключів. Алгоритми СВК достатньо складні у порівнянні з іншими традиційними криптосистемами і на практиці за допомогою СВК зручно поширювати ключі, об'єм інформації котрих незначний. А, згодом, за допомогою хмарних технологій здійснювати обмін великими інформаційними потоками.
3. як засіб автентифікації користувачів.

Системи з відкритим ключем можуть використовувати найрізноманітніші алгоритми криптування. Одними з найпопулярніших при цьому є криптосистеми RSA, Ель-Гамаля або Діффі-Геллмана та криптосистеми на основі еліптичних рівнянь.

Фактично, вибір алгоритму лише визначає спосіб та складність шифрування ключа, а не принципову різницю між методом передачі інформаційних потоків. Цифрова сигнатура або електронний підпис – треба для перевірки того, що повідомлення або інформація дійсно належить тому чи іншому учаснику мережі, до повідомлень мають бути приписані так звані цифрові сигнатури.

Цифрова сигнатура або електронний підпис (англ. signature – підпис) – це рядок символів, що залежить як від відправника так і від змісту повідомлення (рис. 1.15).

Жоден учасник мережі крім користувача А (відправника) не може визначити формат підпису для кожного конкретного повідомлення. Жоден, включаючи самого користувача, не може змінити змісту повідомлення так, щоби підпис залишався незмінним. Хоч і отримувач повідомлення мусить мати змогу перевірки підпису на належність до відправника. Для перевірки

валідності цифрового підпису користувач В (отримувач), має надати інформацію третій особі С (мережа або сервер верифікації підписів) про те, які самі дані було використано для перевірки сигнатури. Якщо повідомлення передається безпосередньо від відправника до адресата, виключаючи третю сторону, то в такому випадку мова йде про “самобутній цифровий підпис”.

Рисунок 1.15 - Цифрова сигнатура як частина самого повідомлення

Ряд недоліків наведеної вище моделі:

- в ланцюжку передбачається наявність третьої особи – клієнта котрому однаково довіряють як відправник так і отримувач;
- відправник, отримувач та клієнт верифікації мають обмінятися істотною кількістю службової інформації до того, як буде передано саме повідомлення;
- передача такої інформації має відбуватися у закритому вигляді, її використання в даному випадку малоефективне.

Тим не менш, навіть така схема цифрового підпису успішно використовується в цифрових системах, де має виконуватися два простих правила: необхідність автентифікації / інформаційного впізнання та обов'язкове шифрування повідомлень, що передаються в мережі.

Хеш-функції – дані блокчейн мереж, хешування – перетворення первинних даних у дані мережі.

Використання цифрової сигнатури передбачає використання певних функцій шифрування:

$$S = H\times(k, T), \qquad (1.1)$$

де S – сигнатура;

k – ключ;

T – оригінальний текст.

Функція H(k, T) при цьому є хеш-функцією якщо вона відповідає наступним вимогам:

1. Оригінальний текст може бути довільного розміру або довжини;
2. Значення H(k, T) має фіксовану довжину;
3. Значення функції H(k, T) легко розраховується для будь-якого
4. аргументу;
5. Відтворити аргумент по значенню з точки зору розрахункової
6. потужності та прикладених сил – майже неможливо;
7. Функція H(k, T) – однозначна.

Однозначність розділяють на слабку та сильну. При слабкій однозначності для заданого значення T майже неможливо знайти інший текст T′, для якого H(k, T) = H(k, T′). При сильній однозначності для будь-якого тексту T неможливо знайти інший задовольняючий текст, що мав би те саме значення хеш-функції.

Хешуванням (англ. hashing) при цьому називають перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини.

Такі перетворення також називаються хеш-функціями або функціями згортання, а їхні результати називають хешем, хеш-кодом, хеш-сумою, або дайджестом повідомлення (англ. message digest), рис. 1.16.

З визначення хеш-функції випливає, що для будь-якої функції є тексти-близнюки, що мають однакове значення хеш-функції, тому що потужність безлічі аргументів незрівнянно більша потужності кількості значень.

Хеш-функції слугують з метою оптимізації даних за рахунок того, що у однакових значень (записів в базі даних) однакові значення хеш-функції. Такий підхід пошуку дублікатів ефективний для файлів великого розміру.

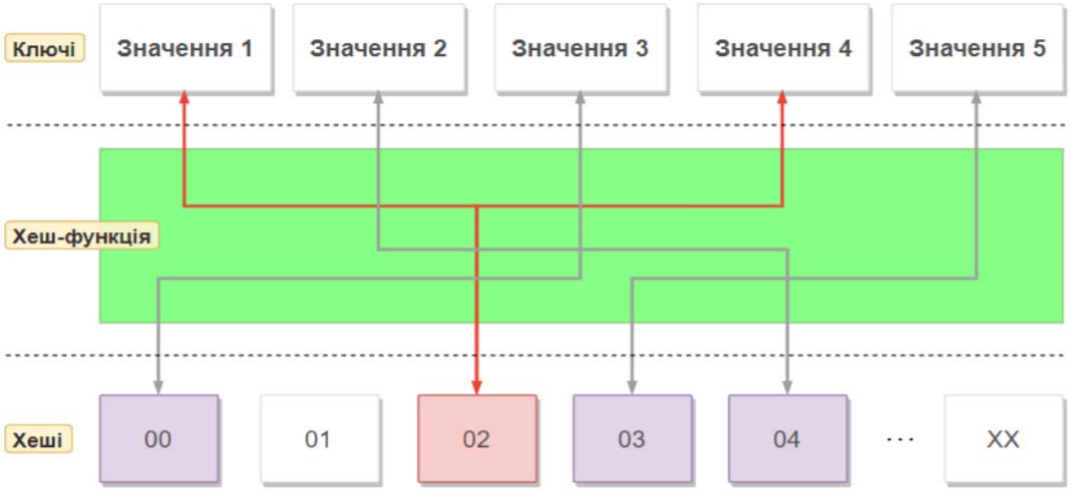

Рисунок 1.16 - Хеш-функція ставить у відповідність значенням ціле число від 0 до XX. Є суперечність (колізія) між Значенням 1 та Значенням 4, яким відповідає однакове значення даних

Криптографічна хеш-функція дозволяє перевірити, що певні вхідні дані зіставляються із заданим значенням хешу, але, якщо вхідні дані невідомі, то відновити вхідне значення видається майже неможливим за умови знання лише про збережене значення хеш-функції. Даний механізм використовується для перевірки та забезпечення цілісності переданих даних, і є основним блоком для автентифікації повідомлень з використанням хешу.

Найбільш відомими хеш-функціями є MD2/4/5 та SHA.

Три алгоритми серії MD працюють за принципом перетворення тексту довільної довжини в 128-бітну сигнатуру. Вони отримали широке поширення в сучасних мережах як спосіб перевірки цілісності файлу або посилання за допомогою порівняння даних з розрахованим попередньо хешем.

Алгоритм MD5 передбачає:

1. доповнення тексту до довжини, що дорівнює 448 біт по модулю 512;
2. додавання довжини тексту в 64-бітному представленні;

3. 512-бітні блоки мають пройти процедуру Damgard-Merkle (цей клас перетворень передбачає розрахунок аргументів фіксованої довжини для фіксованих по довжині значень), при чому кожний блок проходить цю операцію в чотирьох різних циклах.

Сімейство алгоритмів SHA SHA-256 – це алгоритм, або, іншими словами, криптографічна хешфункція, яка була розроблена Агентством національної безпеки Сполучених Штатів Америки. Технічні параметри SHA-256:

- показник розміру блока – 64.
- максимально допустима довжина повідомлень (байт) – 33.
- характеристика розміру дайджесту повідомлення (байт) – 32.
- стандартний розмір слова (байт) – 4.
- параметр довжини внутрішнього положення (байт) – 32.
- число ітерацій в одному циклі – всього 64.
- швидкість при стандартних умовах (MiB/s) – близько 140.

Робота алгоритму SHA-256 базується на принципі процедури DamgardMerkle (так само, як і в випадку з алгоритмом MD5), в згідності з яким початковий показник відразу після внесення правок розділяється на блоки, а ті в свою чергу на 16 слів.

Даний протокол працює з даними, що розподілені на блоки по 512 біт (64 байти). Він виконує їх криптографічне “змішування” та на виході видає 256- бітний хеш-код.

Набір даних проходить через цикл, що нараховує 80 або 64 ітерації.

Кожен етап характеризується запуском хешування зі слів, що складають блоки.

Пара з них оброблюється за допомогою інструментів функції. Надалі, результати перетворення утворюють суму, що в результаті видають правильний показник хеш-коду. Для генерації кожного наступного блоку використовується значення попереднього. Перетворення цих блоків ізольовано – недопустима операція.

Основна робота даної хеш-функції полягає в хешуванні даних. Але для повного занурення в сенс та мету роботи даної хеш-функції слід визначити поняття терміну “майнінг” (англ. mining – видобуток).

Майнінг – головна компонента механізму захисту будь-яких цифрових валют. Принцип дії полягає в об’єднанні “майнерами” здійснених операцій в єдиний блок, який вже було перетворено сотні разів з метою встановлення виключно рідкісного хеш-коду, що відповідає певним встановленим вимогам мережі. Якщо подібне значення визнають знайденим, то блок “добувається” (тобто, потребує знаходження) і додається до блокчейну цифрової валюти. Така розрахункова діяльність не дає будь-якої користі окрім підвищення складності розрахунку та генерації необхідного блоку в подальшому. З іншої сторони, тільки завдяки їй користувачі даної системи можуть бути впевнені в тому, що їх платформу (блокчейн) не буде взято під контроль зловмисниками та централізовано. Мережа не має єдиного центру і розподілена, зменшується кількість переходів від одної точки до іншої, що також діє на благо усієї структури (рис. 1.17).

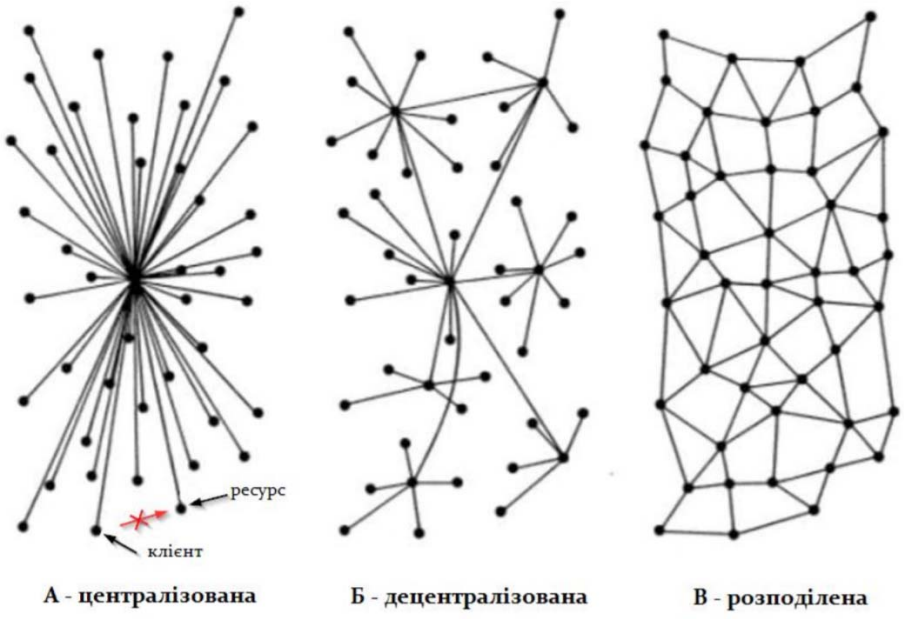

Рисунок 1.17 - Види мереж за структурою з’єднань

Стандартна хеш-функція приймає на вхід блок з певною інформацією, видаючи на виході випадкове та непередбачуване значення. Вона розроблена таким чином, що не існує оптимального та однозначно вірного методу знайти необхідний показник без продовження перебору значень знову і знову до тих пір, доки не буде знайдено відповідний хеш-код.

Одним з найпопулярніших алгоритмів розрахунку блоків є саме SHA-256.

Саме цим алгоритмом користується найдорожча криптовалюта в світі – Bitcoin.

Причому, для підвищення рівню безпеки даний алгоритм задіюється два рази та іменується в даному випадку подвійним.

В Bitcoin критерієм оцінки правильності хешу вважають кількість “0” записаних на початку хешу. Віднайти таке значення також вкрай важко як і, наприклад, знайти банківський рахунок що містить декілька нулів наприкінці.

Зрозуміло, що для хеш-функції дана операція в багато разів ускладняється і приблизному еквіваленті на даний момент дорівнює ймовірності знайти необхідне значення в масиві з значень, що приблизно дорівнює 1,4 помножене на 10 у 21 ступені.

Хеш-таблиці як структури даних в блокчейні. Хеш-таблиця – структура даних, що реалізує інтерфейс асоціативного масиву, вона дозволяє зберігати пари (ключ та значення) і здійснювати три операції: операцію додавання нової пари, операцію пошуку і операцію видалення за ключем.

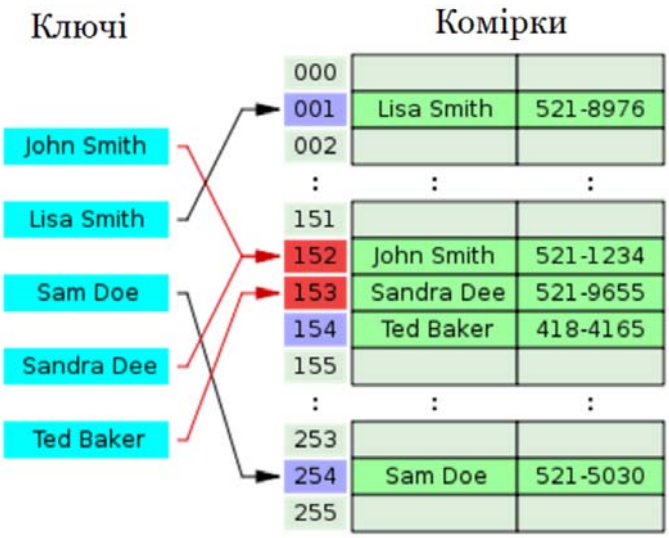

Рисунок 1.18 - Розв’язання колізій хеш-таблиці методом лінійного перебору

Дерево Меркла (англ. Merkle tree) представляє собою особливу структуру даних (хеш-дерево), яка зберігає підсумкову інформацію про певний більший обсяг даних. Використовується для перевірки цілісності даних і застосовується для збереження хешів транзакцій у єдиний блок з мульти-хеш значенням.

Принцип, за яким це відбувається наведено на рис. 1.19.

Смарт-контракти як спосіб обміну цифровими цінностями (даними) в блокчейні. Усі криптовалюти успішно застосовуються для проведення щоденних валютних транзакцій. Але, ті ж самі мережі, де вони реалізуються, можливо використовувати в цілях розподіленої роботи програмного забезпечення та розповсюдження даних за принципами анонімності та простих договорів.

Для даних цілей в блокчейні створюється спеціальний об'єкт – смарт-контракт. Такі програми записуються в мережі та залишаються дійсними назавжди. Крім того, у всіх учасників мережі залишається копія проведеної операції. При цьому роботу контракту можна зіставляти з управлінням грошовими операціями: створенням аукціону, гри з грошовою винагородою, парі, тощо.

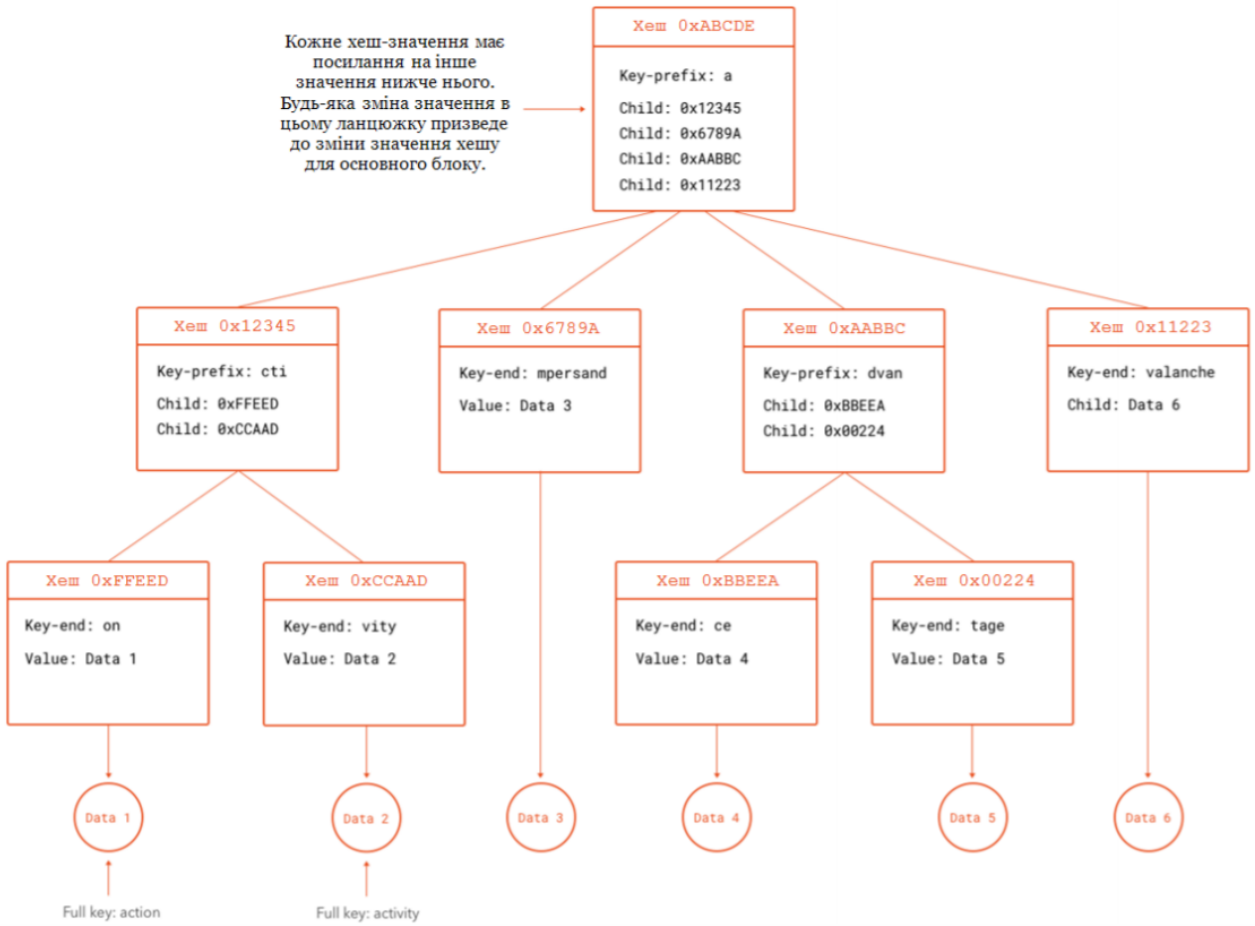

Рисунок 1.19 - Побудова мульти-хеш блоку з дочірніх хеш-значень

Також, смарт-контракти відмінно пасують для автоматизації бухгалтерського обліку: контракт може записувати у собі, від кого і скільки прийшло грошей та планувати на цій основі фінансові прогнози на прибутки та втрати підприємства. Усі учасники мережі мають доступ до кількості операцій та їх призначення – блокчейн захищає від несанкціонованих та прихованих спекуляцій.

Розглянемо реалізацію смарт-контрактів на базі блокчейну Ethereum.

В проектування цієї мережі, на відміну від блокчейну Bitcoiny, з самого початку були закладені можливості впровадження даної технології та застосування її для розподіленої роботи програм на основі блокчейну, зокрема, як єдиної децентралізованої віртуальної машини Turing Complete. Фактично, Etherium це платформа для створення практично будь-яких децентралізова-

них онлайн-сервісів на базі блокчейну, що працюють на базі розумних контрактів.

Зацікавленість даним проектом вже виявили такі компанії як Microsoft, IBM, Acronis та багато організацій-стартапів.

Смарт-контракт – це програмний код, який містить інформацію про транзакцію (або, простіше, угоду) у форматі “якщо … тоді …”. Наприклад, “Якщо користувачем X буде занесено в систему 100 ETH, тоді він отримає 10 токенів N від користувача Y”.

Токен – це внутрішня валюта компанії або особи, яка випускається та розповсюджується за методом залучення інвестицій. За дану валюту, в кожному конкретному випадку, інвестор може отримати різноманітні блага, що пропонує ініціатор компанії. Процедура проводиться на манер первинної публічної пропозиції акцій, за виключенням відсутності юридичних прав або державного регулювання поширення ICO (Initial Coin Offering, укр. “Первинне розміщення монет”, маючи на увазі новий підвид цифрової валюти в котру вкладено певний процент прав та бонусів інвесторами проекту).

Тобто, повертаючись до вищевикладеного прикладу, якщо X та Y виконують свої зобов'язання, то кожен з них отримує попередньо визначений ресурс. Якщо хтось з учасників даної процедури спробує уникнути виконання своїх зобов’язань, то угода буде вважатися не завершеною і сторони залишаться при своїх інтересах та майнових правах.

Для мережі Etherium принцип роботи смарт-контрактів достатньо прозорий: актив потрапляє у програму і вона сама слідкує за виконанням умов угоди. Коли вони будуть виконані, то компанія (продавець) отримає крипто валюту у встановленому еквіваленті до товару, що перейде у власність інвестора (покупця). Основними атрибутами будь-якого смарт-контракту є:

– підписанти – сторони домовленості, що приймають оговорені умови (для цього використовуються адреси облікових записів та циф-

рова сигнатура, або цифровий мульти-підпис, якщо підписантів контракту більше ніж два);

– предмет домовленості – власне, ресурси для обміну (значення), при цьому, вони мають бути частиною системи, в рамках якої реалізується контракт. Якщо X та Y бажають скласти домовленість в мережі Etherium, то X повинен мати оговорену суму на рахунку, а Y – розмістити обмовлену кількість токенів в межах платформи;
– умови домовленості – математично підтверджений опис умов (станів та функцій даного смарт контракту), за яких контракт буде вважатися можливим для виконання та функціональним.

Графічне порівняння смарт-контракту та звичайного паперового смарт контракту наведено на рис. 1.20. Звичайний контракт не підкріплено жодним іншим доказом аніж папером, смарт-контракт – точно перевірена та прозора одиниця в складі мережі блокчейн.

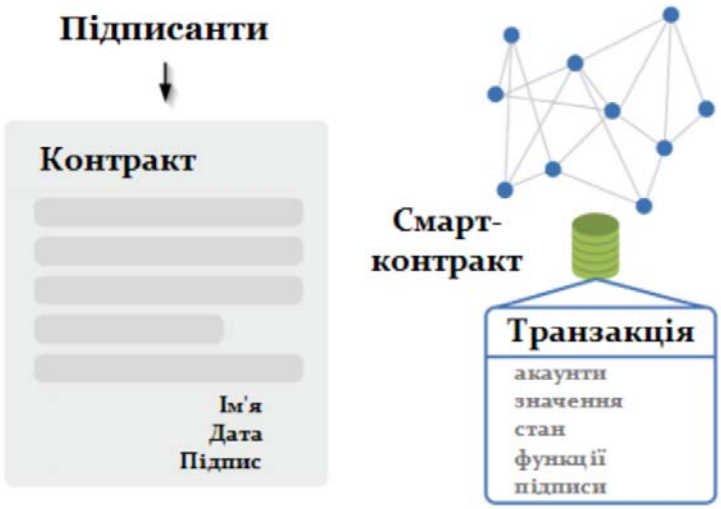

Рисунок 1.20 - Звичайний контракт та смарт-контракт в спрощеному вигляді

Ключові переваги смарт контрактів Доказ концепції (англ. Proof of concept, PoC) є реалізацією методу або ідеєю демонстрування здійсненності або демонстрації можливості виконання домовленості в принципі з метою перевірки того, що певна угода (інформація та дані, в широкому розумінні)

мають практичний потенціал або достовірність та здійсненність. Доказ в такому випадку не обов'язково має бути повним або затвердженим в повному обсязі.

Одним з найголовніших критеріїв успіху смарт-контрактів є проведення угод без залучення третьої сторони (зазвичай, в реальному світі вони виступають гарантами виконання угоди та усіх умов домовленості).

Смартконтракти працюють за іншим принципом: лиш тільки реальні складові угоди потраплять в єдиний простір-платформу для обміну та мають відповідні електронні підписи сторін угоди – домовленість вважається закритою та відбувається автоматичний обмін цінностями.

Друга перевага – безпека та конфіденційність угод. Усі контракти зберігаються в блокчейні у зашифрованому вигляді. Про умови та предмет угоди знають тільки сторони домовленості, а зробити несанкціоновані зміни у програмний код виявляється неможливим на практиці. Третьою перевагою смарт-контрактів є зниження витрат часу та матеріальних благ на проведення угод. Якщо усі умови домовленості виконані, то користувачі здійснюють обмін активами миттєво.

Але, не дивлячись на всі переваги, смарт-контракти мають і ряд правил, що мають бути виконаними для їх реалізації. Обов'язковими умовами в даному випадку виступають:

- наявність децентралізованої інформаційної середи (блокчейн), в межах якої буде знаходитись достатня кількість клієнтів для отримання та виконання запитів у всесвітньому цифровому просторі;
- наявність автоматичної бази даних (хеш-таблиці) для проведення транзакцій (укладання контрактів) в мережі;
- наявність спеціальних інструментів та алгоритмів для виконання смарт-контрактів (хеш-функції), що б задовольняли вимогам безпечного розрахунку та однозначного визначення складових угоди, запису даних в БД;

- використання методів асиметричного шифрування (закритого та відкритого ключів) за допомогою яких генеруються цифрові сигнатури клієнтів мережі;
- математично доведена цілісність по Тюрінгу (можливість реалізації в системі будь-якої обчислюваної функції, що не порушує законів логіки даної системи).

Смарт-контракт – це, перш за все, програма. І, як і будь-яка програма, в ньому присутні певні недоліки:

- складність самостійного впровадження смарт-контракту;
- висока залежність від людського фактору (робота смарт-контракту та його безпечність ціликом залежать від правильності написаного програмного коду);
- недостатня адаптивність (дані, що вже занесено в блокчейн, неможливо змінити);
- погане масштабування. При одночасному запуску декількох контрактів пропускна здатність системи знижується пропорційно.

Також, знову слід зазначити, що використання смарт-контракту, як і здійснення будь-якої операції у блокчейні мають бути перевірені учасниками мережі.

Ether (ETH) це ‘паливо’ для мережі Ethereum. Коли існує необхідність надіслати токени, виконати операцію з смарт-контрактом, надіслати ETH або зробити будь що ще – ініціатор має заплатити за розрахунок такої операції. Ця плата розраховується в умовній одиниці Gas з конвертуванням у ETH.

Користувач завжди сплачує за розрахунки (перевірку хешу) незалежно від того, чи була успішною ваша операція, чи ні. Навіть якщо операція нездійсненна, майнери мають перевірити та виконати таку транзакцію (розрахувати) і саме за це має сплачувати ініціатор. Механізм дуже схожий до того, що відбувається з будь-якими банківськими операціями.

Користувач може переглянути прикріплені ‘чайові’ (gas limit × gas price) до утвореної транзакції з конвертацією по курсу. Саме ця сума буде винагородженням для майнерів, що роблять роботу з розрахунків та розміщують такі операції в блоках та захищають постійність блокчейну.

Ознайомившись зі всім вищесказаним, час перейти до визначення самого блокчейну та принципів організації мережі на базі існуючого “всесвітнього павутиння”.

Блокчейн структура та її особливості. Уявіть таблицю значень яка дублюється тисячі разів у мережі комп'ютерів. Тепер, уявіть що ця мережа спроектована таким чином, щоб регулярно оновлювати цю таблицю даних. Ці два поняття дають базове уявлення про те, що саме складає основу технології Блокчейн.

Інформація що зберігається в блокчейні існує за принципом загальнодоступної та постійно обновлюваної бази даних. Фактично, це новий принцип використання мережі, що має свої переваги та недоліки. База даних блокчейну не зберігається на єдиному носії – це означає що всі його записи є дійсно загальнодоступними та легко верифікованими. Не існує жодної централізованої та основної копії яку б могли викрасти та зламати. Інформація поширюється через тисячі комп'ютерів одночасно, уся інформація блокчейну доступна одразу всім учасникам інтернету.

Технологія Блокчейн, так само як й інтернет, має свої вбудовані механізми захисту. Шляхом зберігання однакових блоків інформації по всій мережі, блокчейн:

- не може бути контрольованим єдиною організацією;
- не має єдиного “вразливого” центру для атак хакерів;
- постійно оновлює інформацію так, що не існує застарілих або більш нових копій даних.

Bitcoin було винайдено у 2008 році. З того часу блокчейн Bitcoin-у працює без жодних суттєвих проблем (на сьогоднішній день будь-які проблеми, пов'язані з транзакціями в блокчейні, були пов'язані з викраденням даних користувачів чи неправильним управлінням системою. Інакше кажучи, ці проблеми випливають з людських помилок, а не з недоліків основних принципів роботи системи). Але існує декілька видів блокчейнів з іншими концепціями.

Структура Ethereum блокчейну має дуже схожі принципи до вищезазначених: вона зберігає записи про все що тільки відбувається в мережі. І 61 при цьому кожен учасник має локальну копію цих даних разом з історією усіх подій.

Велика різниця двох блокчейнів полягає в тому, що ноди зберігають останній стан кожного смарт-контракту додатково до значень і транзакцій в мережі. Для роботи будь якого ПЗ в мережі Ethereum треба вислідити стан або нинішні показники інформації для всіх подій, включаючи баланс кожного з користувачів, код смарт-контракту та як саме до нього можна звернутися.

В блокчейні біткоіну використовується трохи інший принцип: кожного разу як відбувається якась подія, мережа ‘забирає’ необхідні дані та розраховує їх за принципом схожим до реальних валют визначаючи, яка кількість будь-чого існує та кому саме належить. Таким чином відбувається маркування на витрачені та здобуті дані.

Ethereum мережа усе виконує за принципом створення облікових записів (акаунтів) користувачів та точно зберігає, які саме події відбуваються з даним ‘віртуальним гаманцем’. Усі дані завжди перебувають десь у мережі, але не мають точного зв’язку з будь-ким для продовження лінії операцій з ними (рис. 1.21).

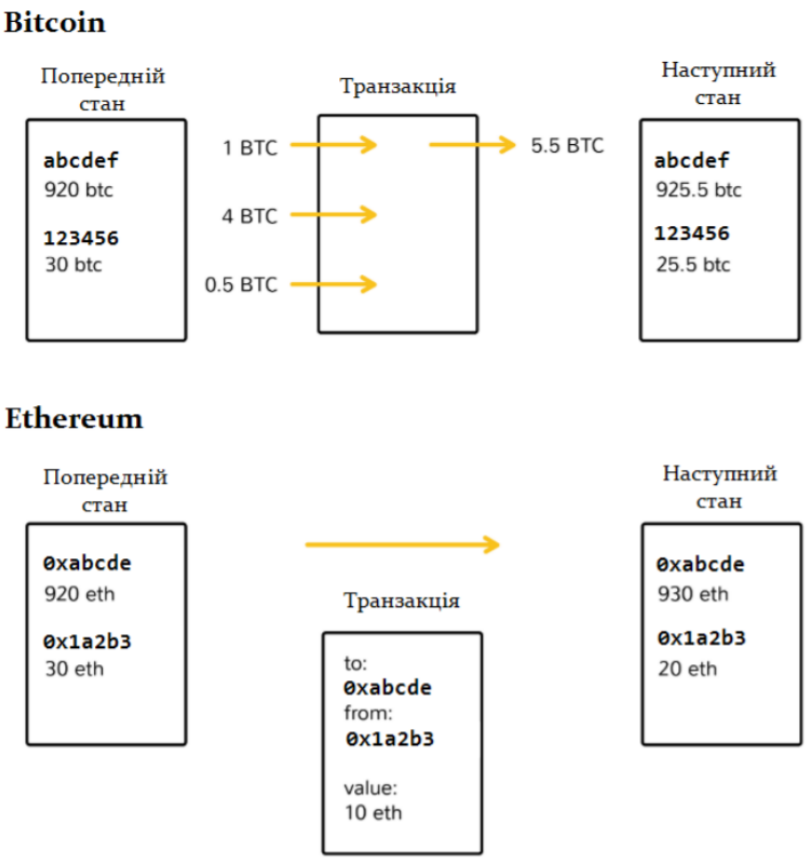

Рисунок 1.21 - Різниця в принципах транзакцій в Bitcoin та Ethereum блокчейнах

Блокчейн система постійно погоджена – кожні десять хвилин вона перевіряє сама себе. У вигляді само-контрольованої вбудованої системи в складі блокчейну працює механізм, що перевіряє та затверджує всі транзакції в даному інтервалі. Кожна група таких транзакцій оцінюється як один “блок”.

З цих двох властивостей системи випливає:

– дані про прозорість вбудовуються в мережу в цілому, за визначенням вона є загальнодоступною;
– мережа не може бути зламаною одним з учасників мережі - для внесення змін у мережу знадобиться участь чималої кількості розрахункових потужностей в складі блокчейну.

Приватний ключ, так само як і пароль, дає доступ користувачеві до зашифрованих персональних даних. І безпека цих даних цілком і повністю бу-

де належати особі, яка володіє цим ключем, без нього доступ до даних буде втрачено.

Мережа з комп'ютерів-учасників, так званих "нод" або "вузлів" і складає усю блокчейн систему. Вузол – комп'ютер під'єднаний до Blockchain мережі, що використовує клієнт (програму) за допомогою якого виконує задачі перевірки та передачі інформації про транзакції. Він отримує копію блокчейну, що завантажується автоматично під час підключення до загальнодоступної мережі. Разом усі вузли формують потужну мережу другого рівня – зовсім інакше представлення того, як функціонує інтернет на сьогоднішній день.

Кожен вузол виступає адміністратором мережі і під'єднується до неї добровільно (в цьому сенсі уся мережа залишається децентралізованою, рис. 1.22).

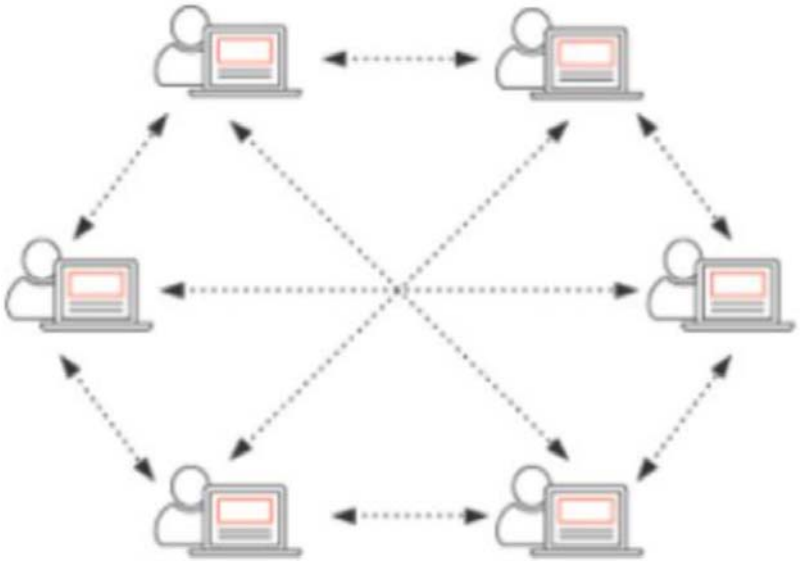

Рисунок1.22 - Схема зв'язків клієнтів в блокчейні

Крім того, кожен вузол в блокчейні бере участь в тому, що може отримати винагороду у вигляді зарахування частини криптовалюти на власний рахунок.

Вузли часто представляють як центри для “майнінгу” криптовалюти (укр. – добування; такий термін застосовують у зв’язку з необхідністю прикладати певні технічні потужності для отримання винагород в системі блокчейн), але це поняття не зовсім вірне. Фактично, ці ноди постійно конкурують між собою за отримання винагороди шляхом вирішення математичних виразів (знайдення необхідного хешу). Криптовалюта є основним сенсом існування таких нод в системі, ідейним елементом розвитку blockchain. Зараз, цифрові валюти існують лише як перший, але не єдиний спосіб застосування цієї технології.

За приблизними оцінками, зараз існує близько 1600 Bitcoin-подібних криптовалют (і їх кількість постійно зростає). Також, на даний момент в розробці існує цілий ряд інших потенційних адаптацій оригінальної концепції мережі блокчейн.

Так само як і з веб-структурами, користувач не мусить знати все про блокчейн для його використання. На даний момент, фінансова галузь пропонує найбільший перелік сценаріїв з використання технології. Міжнародні грошові перекази, наприклад. За оцінками світового банку в 2015 році було надіслано близько 430 мільярдів доларів США таким способом. І на даний момент ця галузь шукає нових розробників проектів, blockchain розробників.

Потенційно, блокчейн усуває будь-яких посередників при грошовому переказі, користувачеві доступний графічний інтерфейс користувача (GUI) через власний персональний комп’ютер або інший пристрій. Аналогічним функціоналом зараз оперують так звані “гаманці” для різноманітних криптовалют на ринку.

1.5 Висновки до розділу

У даній роботі планується розглянути реалізацію захищеного з’єднання на базі технології – блокчейн, що дозволить запобігти підміні інформації та несанкціонованому доступу. Ця особливість буде в подальшому використана

для створення комп’ютерної система з блокчейн технологією підтримки реєстру студентів ВНЗ першого рівня акредитації НТУ «ДП» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі розглянимо детально технологію блокчейн.

Ці особливості блокчейн можуть створити нові принципи взаємодії з інформацією та дати розвиток новому поколінню мереж.

Можна зазначити:

1. Визначення видів побудови топологій та їх основних особливостей вказує на прийнятність даних рішень для використання в складі структури блокчейн. Ці рішення можуть бути успішно застосовані при розробці основи комунікації клієнтів, як рівень транспортного зв’язку та мають допомогти у створенні основи для успішної розбудови мережі;
2. Складові структури блокчейн та особливості її роботи можуть бути використані для створення сучасного рішення у сфері приватних та надійних у роботі клієнтів з повноцінними механізмами забезпечення конфіденційності користувачів, вбудованими засобами збереження оригінальності даних та можуть створити нові принципи роботи з інформаційними потоками в мережі інтернет.

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, програмне забезпечення, яке реалізує алгоритм управління, персональний комп'ютер, 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 іншими системами.

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

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 системах 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, 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 є критерії якості доступу, продуктивності, 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 приміщення.

До конфіденційної інформації, що 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.

Частина комп’ютерної системи, що відповідає за перебіг технологічного процесу, повинна функціонувати в реальному масштабі часу. Час реакції системи має бути не більше 500 мс.

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.

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 ПІДРОЗДІЛІВ ВНЗ З БЛОКЧЕЙН ТЕХНОЛОГІЄЮ

3.1 Розробка схеми організаційної структури

3.1.1 Розробка схеми організаційної структури комп'ютерної системи підрозділів ВНЗ з блокчейн технологією

Згідно з організаційною структурою та територіальним положенням мережу підрозділів ВНЗ доцільно розділити на п'ять підмереж:

- НТУ «Дніпровська політехніка», підмережа 1;
- Автотранспортний технікум, м. Дніпро, підмережа 2;
- Павлоградський технікум, м. Павлоград, підмережа 3;
- Марганецький коледж, м. Марганець, підмережа 4;
- НКЦ, м. Жовті Води, підмережа 5.
-

3.2 Розробка специфікації апаратних засобів комп'ютерної системи підрозділів ВНЗ з блокчейн технологією

В табл. 3.1 наведено обладнання, яке буде використовуватись у комп'ютерній системі підрозділів ВНЗ. Згідно з вимогами замовника використовується обладнання компанії Cisco.

Таблиця 3.1 – Специфікація обладнання

№	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість
1	2	3	4	5
1	CISCO1941W-E/K9 RAM: • Укомплектовано- 512 МБ. Max 2,5 ГБ. Флеш пам'ять: • Укомплектовано- 256 МБ.	Маршрутизатор	шт	6

Продовження таблиці 3.1

1	2	3	4	5
	• Max 4 ГБ. Технологія з’єднання: Безпровідна			
	Протокол передачі даних: • Ethernet, Fast Ethernet, Gigabit Ethernet. Протокол мережі: • IPSec Індикатори: • Живлення, статус з’єднання Протоколи маршрутизації: • BGP, GRE, OSPF, DVMRP, EIGRP, IS-IS, IGMPv3, PIM-SM, PIM-SSM, статична IPv4 и IPv6 маршрутизація. Особливості конфігурації: • підтримує: VPN, DMVPN, IPv6, MPLS, Syslog; • Встановлені: firewall, функція фільтрації контента, DMVPN, WRED, CBWFQ. • Відповідність стандартам IEEE 802.1ag, IEEE 802.1ah. Кількість безпровідних VLAN: • 16 Слоти розширення: • 2 слоти для EHWIC; • 1 слоти Double-Wide EHWIC. Інтерфейси: • 2 порта Ethernet 10Base-T/100Base-TX/1000Base-T, разъем RJ-45; • 1 консольний порт управління, розєъем RJ-45; • 1 консольный порт управління, конектор Mini-USB тип B; • 1 послідовний допоміжний порт, роз’єм RJ-45; • 2 порта USB тип A			

Продовження таблиці 3.1

1	2	3	4	5
	Алгоритм шифрування: SSL			
2	WS-C2960-24-S Порти Кількість портів 24 Фіксовані порти 24 Ethernet 10/100 Характеристики Рівень (L2, L3) L2 Пропускна здатність 16 Gbps Продуктивність (pps) 3.6 mpps	Комутатор	шт	7
3	WS-C2960-8TC-S Порти Кількість портів 8 Фіксовані порти 8 Ethernet 10/100 Аплінки - Характеристики Рівень (L2, L3) L2 Пропускна здатність 16 Gbps Продуктивність (pps) 3.6 mpps	Комутатор	шт	58
4	CISCO UCS C240 M4 RACK Процесор: 1 x Intel Xeon E5-2620, 2.00 ГГц, 95 Вт 6C, 15 МБ кеш-пам'яті, DDR3 1333 МГц, до 2-х процесорів Кеш-пам'ять: 3-й рівень, 15 МБ Пам'ять: 8 ГБ DDR3, 1600 МГц RDIMM, PC3-12800, dual rank, 1.35v, до 512 ГБ	Серверне обладнання	шт	5

Продовження таблиці 3.1

1	2	3	4	5
	Мережевий контролер: 2-портовий гігабітний Контролер сховища: Програмний контролер, RAID 0/1/10/5, 4 порту SAS / SATA Відсіки для жорстких дисків: 4 x 3.5 "LFF SAS / SATA Оптичний привід: Відсутній Слоти PCI-Express: 2 слота PCI-Express: 1 половинної висоти і половинній довжини x8, 1 повної висоти і половинній довжини x16 Джерело живлення: 2 x 650 Вт Форм-фактор: Монтуємий в стійку 1U			
5	Cisco Server DC Xeon 5140 Процесор: 1 x Intel Xeon, 2.33 ГГц, 95 Вт 6C, 15 МБ кеш-пам'яті, DDR3 1333 МГц, до 2-х процесорів Кеш-пам'ять: 3-й рівень, 15 МБ Пам'ять: 4 ГБ DDR3, 1600 МГц RDIMM, PC3-12800, dual rank, 1.35v, до 512 ГБ Мережевий контролер: 2-портовий гігабітний Контролер сховища: Програмний контролер, RAID 0/1/10/5, 4 порту SAS / SATA Відсіки для жорстких дисків: 4 x 3.5 "LFF SAS / SATA Оптичний привід: Відсутній			

Продовження таблиці 3.1

1	2	3	4	5
	Слоти PCI-Express: 2 слота PCI-Express: 1 половинної висоти і половиннійдовжини x8, 1 повної висоти і половиннійдовжини x16 Джерело живлення: 2 x 650 Вт Форм-фактор: Монтуємий в стійку 7U Управління: Cisco UCS Integrated Management Controller (CIMC)			

3.3 Вибір структурної схеми підрозділів ВНЗ з блокчейн технологією

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 без-

посереднє підключення кінцевих вузлів мережі, таких як сервери, персональні комп’ютери, та принтери.

Структурна схема корпоративної мережі підрозділів ВНЗ зображена на рис. 3.1.

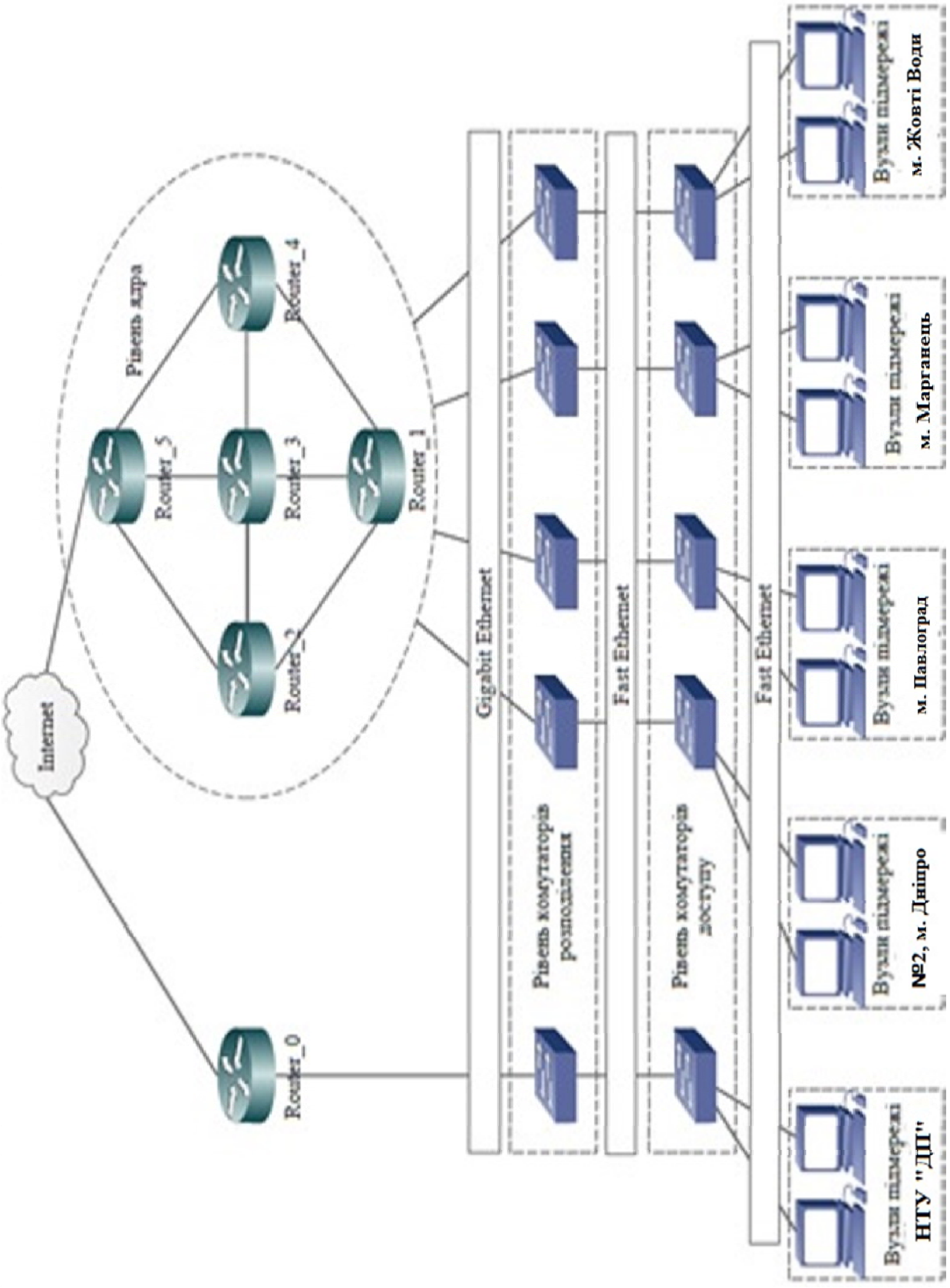

Рисунок 3.1 – Структурна схема корпоративної мережі підрозділів ВНЗ

3.4 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Дано:

- кількість вузлів в найбільшій мережі: 112
- середня інтенсивність трафіку: μ = 148 (кадрів/с)
- середня довжина повідомлення: l = 650 байт;
- вимоги до затримки передачі пакету – ≤5 мс.

Згідно кількості вузлів (112) для їх підключення на рівні розподілу обираємо комутатор Cisco Catalyst 1911 серії. (1 шт), на рівні доступу комутатор WS-C2960-8TC-S - Catalyst 2960 8 10/100 (17 шт).

Рішення:

Вихідний трафік пересилається на маршрутизатор в лінію з пропускною здатністю 100Мбіт/с.

Для того, щоб комутатор рівня розподілу не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку μ=148 (кадрів/с), а середня довжина повідомлення – 650 байт.

Розрахуємо пропускну здатність мережі на рівні доступу допускаючи, що послугами одночасно користуються 100% користувачів.

$P_{р.д} = \mu \cdot l \cdot n \cdot 8 = 148 \cdot 650 \cdot 8 \cdot 8 = 6{,}2$ (Мбіт/с),

де n – кількість портів в комутаторі рівня доступу.

Пропускна здатність мережі на рівні розподілу розраховується наступним чином. Так як до одного комутатора рівня розподілу підходять декілька комутаторів рівня доступу, а загальна кількість користувачів дорівнює 112, то пропускна здатність мережі на рівні розподілу буде дорівнює:

$P_{р.р} = \mu \cdot l \cdot N \cdot 8 = 148 \cdot 650 \cdot 112 \cdot 8 = 86{,}2$ (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.

Комутатор рівня розподілу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 100 Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих} = \frac{100\,000\,000}{650 \cdot 8} = 19\,231 \text{ пакетів/с.}$$

Оскільки кожне джерело виробляє в середньому 148 пакетів/с, то ми обмежені приєднанням до комутатора рівня розподілу максимум:

$$N = \frac{19\,231}{148} = 129 \text{ джерел.}$$

Що задовольняє нашу мережу на 112 ПК.

Кожен з 112 ПК посилає потік заявок з інтенсивністю 148 кадрів/с. Інтенсивність вихідного трафіку від всіх користувачів:

$\lambda = N \cdot \mu = 112 \cdot 148 = 16\,576$ (пакетів/с).

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

$$\rho = \frac{\lambda}{\mu_{вих}} = \frac{16\,576}{19\,231} = 0{,}86$$

Коефіцієнт зайнятості комутатора рівня розподілу:

$$r = \frac{\rho}{1 - \rho} = \frac{0{,}86}{1 - 0{,}86} = 6{,}14$$

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

$$T = \frac{1}{(\mu - \lambda)} = \frac{1}{19\,231 - 16\,576} = 0{,}38 \text{ мкс}$$

Середня довжина черги:

$$L_{чер} = \frac{\rho^2}{1 - \rho} = \frac{0{,}86^2}{1 - 0{,}86} = 5{,}28$$

Середній час перебування пакета в черзі

$$T_{оч} = \frac{L_{чер}}{\lambda} = \frac{5{,}28}{16\,576} = 0{,}32 \text{ мс}$$

Це значення менше необхідного значення ≤5 мс, що задовольняє вимогам.

Пропускна здатність каналу:

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

$$b = \lambda \cdot l = 16\,576 \cdot 650 \cdot 8 = 86\,195\,200 \text{ біт/с} = 86{,}2 \text{ Мбіт/с}$$

Що задовольняє пропускній здатності вихідного каналу в 100 Мбіт/с.

4 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДРОЗДІЛІВ ВНЗ

4.1 Розрахунок схеми адресації корпоративної мережі

Для адресації мережі комп'ютерної системи підрозділів ВНЗ у Дніпропетровській області виділено блок адрес 192.168.144.0/21.

Для розділення мережі на підмережі використаємо метод VLSM. Використання цього методу дозволяє економно використовувати обмежений ресурс IP-адрес, оскільки можливе застосування різних масок підмереж до різних підмереж. Згідно з вимогами замовника мережа розділяється на п'ять підмереж.

Таблиця 4.1 – Кількість вузлів для кожної підмережі

Підмережа	НТУ «Дніпровська політехніка»	Автотранспортний технікум, м. Дніпро	Павлоградський технікум, м. Павлоград	Марганецький коледж, м. Марганець	НКЦ, м. Жовті Води
Кількість вузлів	85	100	40	112	80

Таким чином, необхідно організувати п'ять підмереж для 417 пристроїв.

Оскільки метод VLSM дозволяє виділяти мережі розміром у 2n, то заданий діапазон ділимо так: 4x128, 1x64.

Для максимально ефективного використання адресного простору, виділимо спочатку великі діапазони, а потім менші. Спочатку вибираємо блоки розміром 128 адрес, розмір якого 27. Для отримання маски підмережі оставимо чотири октети у бітовому вигляді, де останні сім бітів заповнимо нулями, а решту – одиницями і переведемо у десятковий вигляд:

11111111.11111111.11111111.10000000

255.255.255.128

Запишемо останній октет адреси в бітовому вигляді, та відділимо останні 7 бітів, які будуть відповідати за адресу вузла у даній підмережі, а інші – за адресу мережі:

192.168.144.0|0000000

Замінимо останній біт адреси мережі на 1 та запишемо її у десятковому вигляді. Таким чином ми отримаємо адресу першої підмережі:

192.168.144.1|0000000

192.168.144.128

Запишемо два останні октети адреси в бітовому вигляді і змінюючи комбінації останніх бітів адреси мережі отримаємо адреси для трьох інших підмереж:

192.168.10010001.0|0000000

192.168.145.0

192.168.10010001.1|0000000

192.168.145.128

192.168.10010010.0|0000000

192.168.146.0

Вибираємо останній блок розміром 64 адреси, розмір якого 26. Для отримання маски підмережі запишемо чотири октети у бітовому вигляді, де останні шість бітів заповнимо нулями, а решту – одиницями і переведемо у десятковий вигляд:

11111111.11111111.11111111.11000000

255.255.255.192

Запишемо останній октет адреси в бітовому вигляді, та відділимо останні 6 бітів, які будуть відповідати за адресу вузла у даній підмережі, а інші – за адресу мережі:

192.168.144.00|000000

Замінимо останній біт адреси мережі на 1 та запишемо її у десятковому вигляді. Таким чином ми отримаємо адресу останньої підмережі:

192.168.144.01|000000

192.168.144.64

Якщо замість всіх бітів, крім останнього адреси вузла записати 0, а у останньому 1, то отримаємо першу адресу з діапазону, яку можна назначати вузлам, а якщо замість всіх бітів, крім останнього адреси вузла записати 1, а у останньому 0, то отримаємо останню адресу з діапазону:

192.168.144.1|0000001

192.168.144.129

192.168.144.1|1111110

192.168.144.254

Доступний діапазон вузлів для мережі 192.168.144.1: 192.168.144.129-192.168.144.254.

192.168.10010001.0|0000001

192.168.145.1

192.168.10010001.0|1111110

192.168.145.126

Доступний діапазон вузлів для мережі 192.168.145.0: 192.168.145.1-192.168.145.126.

192.168.10010001.1|0000001

192.168.145.129

192.168.10010001.1|1111110

192.168.145.254

Доступний діапазон вузлів для мережі 192.168.145.128: 192.168.145.129-192.168.145.254.

192.168.10010010.0|0000001

192.168.146.1

192.168.10010010.0|1111110

192.168.146.126

Доступний діапазон вузлів для мережі 192.168.146.0: 192.168.146.1-192.168.146.126.

192.168.144.01|000001

192.168.144.65

192.168.144.01|111110

192.168.144.127

Доступний діапазон вузлів для мережі 192.168.144.64: 192.168.144.65-192.168.144.127.

Результати розрахунку подані у табл. 4.2.

Таблиця 4.2 − Схема адресації мережі 192.168.144.0/21

Назва мережі	Кіль-кість вузлів	Номер мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
1	2	3	4	5	6
НТУ «Дніпровська політехніка»	85	LAN 1	255.255.255.128	192.168.144.129	192.168.144.254
Автотранспортний технікум, м. Дніпро	100	LAN 2	255.255.255.128	192.168.145.1	192.168.145.126
Павлоградський технікум, м. Павлоград	40	LAN 3	255.255.255.192	192.168.144.65	192.168.144.126
Марганецький коледж, м. Марганець	112	LAN 4	255.255.255.128	192.168.145.129	192.168.145.254
НКЦ, м. Жовті Води	80	LAN 5	255.255.255.128	192.168.146.1	192.168.146.126

Схема IP-адресації послідовних каналів між маршрутизаторами з діапазону 10.0.18.0/24 представлена у табл. 4.3, яка теж виконана за технологією VLSM.

Таблиця 4.3 – Підмережі каналів WAN між маршрутизаторами

Адреса підмережі	Маска підмережі у десятковому форматі	Префікс	Діапазон допустимих IP-адрес вузлів	Широкомовна адреса
1	2	3	4	5
Канал WAN між маршрутизаторами Strotsenko_Router_1 та Strotsenko_Router_3				
10.0.18.4	255.255.255.252	/30	10.0.18.5-10.0.18.6	10.0.18.7
Канал WAN між маршрутизаторами Strotsenko_Router_2 та Strotsenko_Router_3				
10.0.18.8	255.255.255.252	/30	10.0.18.9-10.0.18.10	10.0.18.11
Канал WAN між маршрутизаторами Strotsenko_Router_3 та Strotsenko_Router_4				
10.0.18.12	255.255.255.252	/30	10.0.18.13-10.0.18.14	10.0.18.15
Канал WAN між маршрутизаторами Strotsenko_Router_3 та Strotsenko_Router_5				
10.0.18.16	255.255.255.252	/30	10.0.18.17-10.0.18.18	10.0.18.19
Канал WAN між маршрутизаторами Strotsenko_Router_1 та Strotsenko_Router_2				
10.0.18.20	255.255.255.252	/30	10.0.18.21-10.0.18.22	10.0.18.23
Канал WAN між маршрутизаторами Strotsenko_Router_1 та Strotsenko_Router_4				
10.0.18.24	255.255.255.252	/30	10.0.18.25-10.0.18.26	10.0.18.27
Канал WAN між маршрутизаторами Strotsenko_Router_2 та Strotsenko_Router_5				
10.0.18.28	255.255.255.252	/30	10.0.18.29-10.0.18.30	10.0.18.31
Канал WAN між маршрутизаторами Strotsenko_Router_4 та Strotsenko_Router_5				
10.0.18.32	255.255.255.252	/30	10.0.18.33-10.0.18.34	10.0.18.35
Канал WAN між маршрутизаторами Strotsenko_Router_1 та Strotsenko_Router_IPS				
209.165.200.0	255.255.255.224	/27	209.165.200.1-209.165.200.30	209.165.202.31
Канал WAN між маршрутизаторами Strotsenko_Router_0 та Strotsenko_Router_IPS				
64.100.13.0	255.255.255.224	/27	64.100.13.1-64.100.13.30	64.100.13.3

4.2 Розрахунок схеми адресації пристроїв

У табл. 4.4 наведена адресація всіх маршрутизаторів мережі з дотриманням всіх необхідних вимог.

Таблиця 4.4 − Схема адресації маршрутизаторів

Пристрій	Інтерфейс	IP-адреса	Маска	LAN
Strotsenko_ Router_1	Gig0/0	192.168.144.129	255.255.255.128	192.168.144.128
	S0/2/0	10.0.18.21	255.255.255.252	10.0.18.20
	S0/3/0	10.0.18.5	255.255.255.252	10.0.18.4
	S0/3/1	10.0.18.25	255.255.255.252	10.0.18.24
Strotsenko_ Router_2	S0/2/0	10.0.18.22	255.255.255.252	10.0.18.20
	S0/2/1	10.0.18.29	255.255.255.252	10.0.18.28
	S0/3/1	10.0.18.9	255.255.255.252	10.0.18.8
Strotsenko_ Router_3	Gig0/0.28	192.168.144.113	255.255.255.248	192.168.144.112
	Gig0/0.38	192.168.144.121	255.255.255.248	192.168.144.120
	Gig0/0.48	192.168.144.65	255.255.255.224	192.168.144.64
	S0/2/0	10.0.18.17	255.255.255.252	10.0.18.16
	S0/2/1	10.0.18.13	255.255.255.252	10.0.18.12
	S0/3/0	10.0.18.6	255.255.255.252	10.0.18.4
	S0/3/1	10.0.18.10	255.255.255.252	10.0.18.8
Strotsenko_ Router_4	Gig0/0	192.168.145.129	255.255.255.128	192.168.145.128
	S0/2/1	10.0.18.14	255.255.255.252	10.0.18.12
	S0/3/0	10.0.18.33	255.255.255.252	10.0.18.32
	S0/3/1	10.0.18.26	255.255.255.252	10.0.18.24
Strotsenko_ Router_5	Gig0/0	192.168.146.1	255.255.255.128	192.168.146.0
	S0/2/0	10.0.18.18	255.255.255.252	10.0.18.16
	S0/2/1	10.0.18.30	255.255.255.252	10.0.18.28
	S0/3/0	10.0.18.34	255.255.255.252	10.0.18.32
	S0/3/1	209.165.200.1	255.255.255.224	209.165.200.0
IPS	S0/3/1	209.165.200.2	255.255.255.224	209.165.200.0
	Gig0/0	209.165.201.1	255.255.255.240	209.165.201.0
	Gig0/1	64.100.13.2	255.255.255.224	64.100.13.0
Strotsenko_ Router_0	Gig0/0	192.168.145.1	255.255.255.128	192.168.145.0
	Gig0/1	64.100.13.1	255.255.255.224	64.100.13.0

Адреси, що налаштовані SVI інтерфейсам комутаторів та серверів, внесені до табл. 4.5. Адресація всіх інших вузлів виконано за допомогою протоколу DHCP.

Таблиця 4.5 − Схема адресації пристроїв

Підмережа	Пристрій	IP-адреса	Маска підмережі	Адреса шлюзу
LAN 1	Strotsenko_Switch_9	192.168.144.130	255.255.255.128	192.168.144.129
	Server1	192.168.144.130	255.255.255.128	192.168.144.129
LAN 2	Strotsenko_Switch_8	192.168.145.2	255.255.255.128	192.168.145.1
	Strotsenko_Switch_7	192.168.145.3	255.255.255.128	192.168.145.1
	Server2	192.168.145.4	255.255.255.128	192.168.145.1
LAN 4	Strotsenko_Switch_10	192.168.145.130	255.255.255.128	192.168.145.129
	Strotsenko_Switch_13	192.168.145.131	255.255.255.128	192.168.145.129
	Server4	192.168.145.132	255.255.255.128	192.168.145.129
LAN 5	Strotsenko_Switch_11	192.168.146.2	255.255.255.128	192.168.146.1
	Server3	192.168.146.3	255.255.255.128	192.168.146.1
VLAN 38	Server0	192.168.144.122	255.255.255.248	192.168.144.121
	Server DNS	192.168.144.123	255.255.255.248	192.168.144.121
	Server HTTP	192.168.144.124	255.255.255.248	192.168.144.121
VLAN 48	Strotsenko_Switch_0	192.168.144.66	255.255.255.224	192.168.144.65
	Strotsenko_Switch_1	192.168.144.67	255.255.255.224	192.168.144.65
	Strotsenko_Switch_16	192.168.144.68	255.255.255.224	192.168.144.65

4.3 Налаштування моделі комп’ютерної системи корпоративної мережі

На рис. 4.1 показана топологічна схема корпоративної мережі підрозділів ВНЗ. Мережа складається з п’яти підмереж:

- НТУ «Дніпровська політехніка», підмережа 1;
- Автотранспортний технікум, м. Дніпро, підмережа 2;
- Павлоградський технікум, м. Павлоград, підмережа 3;
- Марганецький коледж, м. Марганець, підмережа 4;
- НКЦ, м. Жовті Води, підмережа 5.

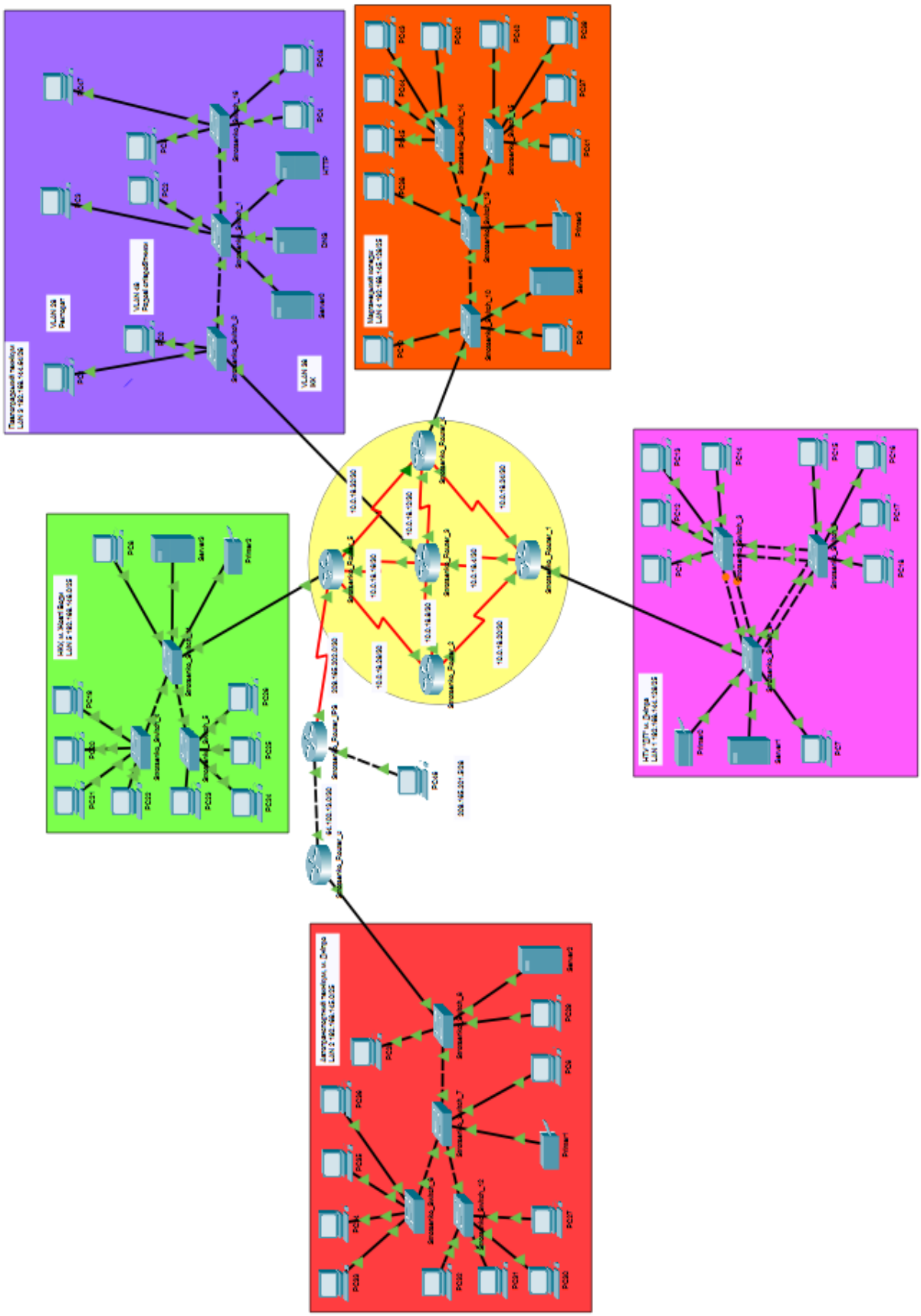

Рисунок 4.1 – Схема корпоративної мережі підрозділів ВНЗ

4.4 Налаштування та перевірка роботи комп'ютерної системи підрозділів ВНЗ

4.4.1 Базове налаштування конфігурації пристроїв

В табл. 4.6 продемонстровані використані команди для виконання базових налаштувань на прикладі маршрутизатора Strotsenko_Router_1.

Таблиця 4.6 – команди для базового налаштування пристроїв

Команда	Функції команди
Router>enable	Перехід в привілегірованний режим EXEC
Router#configure terminal	Перехід в режим налаштування параметрів пристрою
Router(config)# hostname Strotsenko_Router_1	Присвоєння імені пристрою
Strotsenko_Router_1(config)# line console 0 *Strotsenko_Router_1(config-line)# password cisco* *Strotsenko_Router_1(config-line)#login*	Установка пароля для консолі
Strotsenko_Router_1(config)#line vty 0 15 *Strotsenko_Router_1(config-line)#password cisco* *Strotsenko_Router_1(config-line)#login*	Установка пароля vty лінії
Strotsenko_Router_1(config)#enable password class	Установка зашифрованого пароля для привілейованого режиму
Strotsenko_Router_1(config)#service password-encryption	Шифрування всіх паролей
Strotsenko_Router_1(config)#banner motd "This is a secure system. Authorized Access Only!"	Налаштування банера MOTD
Strotsenko_Router_1(config)#line vty 0 15 *Strotsenko_Router_1(config-line)#login local* *Strotsenko_Router_1(config-line)#transport input ssh*	Налаштування на всіх лініях vty використання протоколу ssh
Strotsenko_Router_1(config)#username 123161_Strotsenko password admincisco *Strotsenko_Router_1(config)# line console 0* *Strotsenko_Router_1(config-line)# login local*	Створення та призначення користувача та пароля
Strotsenko_Router_1(config)#ip domain-name Strotsenko_Router_1 *Strotsenko_Router_1(config)#crypto key generate rsa* *1024*	Налаштування імені домена та шифрування даних за допомогою ключа RSA
Strotsenko_Router_1(config)#interface Serial0/2/0 *Strotsenko_Router_1(config-if)#clock rate 128000*	Налаштування значення тактової частоти на DCE-інтерфейсах маршрутизаторів

4.4.2 Налаштування роботи Інтернет

4.4.2.1 Налаштування динамічного NAT

Для виходу робочих станцій в Інтернет необхідно настроїти пограничний маршрутизатор з динамічним NAT. В таблиці 4.7 продемонстровані використані команди для налаштування динамічного NAT.

Таблиця 4.7 – команди для налаштування динамічного NAT

Команда	Функції команди
Strotsenko_Router_5 (config)#interface s0/3/1 *Strotsenko_Router_5 (config-if)#ip nat outside* *Strotsenko_Router_5 (config-if)#ex* *Strotsenko_Router_5 (config)#interface s0/2/0* *Strotsenko_Router_5 (config-if)#ip nat inside* *Strotsenko_Router_5(config-if)#ex* *Strotsenko_Router_5(config)#interface s0/2/1* *Strotsenko_Router_5(config-if)#ip nat inside* *Strotsenko_Router_5(config-if)#ex* *Strotsenko_Router_5(config)#interface s0/3/0* *Strotsenko_Router_5(config-if)#ip nat inside* *Strotsenko_Router_5(config-if)#ex* *Strotsenko_Router_5(config)#interface Gig0/0* *Strotsenko_Router_5(config-if)#ip nat inside* *Strotsenko_Router_5(config-if)#ex* *Strotsenko_Router_5(config)#router eigrp 16* *Strotsenko_Router_5(config-router)#redistribute static*	Налаштування внутрішніх і зовнішніх інтерфейсів NAT
Strotsenko_Router_5(config)#access-list 18 permit 192.168.144.0 0.0.7.255	Визначення переліку доступу, відповідного внутрішнім приватним IP-адресам мереж
Strotsenko_Router_5(config)# ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224	Визначення пулу придатних до використання публічних IP-адрес
Strotsenko_Router_5(config)#ip nat inside source list 18 pool Internet	Визначення NAT зі списку внутрішніх адрес в пул зовнішніх адрес

4.4.2.2 Налаштування HTTP сервера

Також необхідно налаштувати сервер HTTP, щоб на вузлах при вводі в рядку браузера http://123.dnipro.ua відкривався веб-сайт. Для цього необхідно відкрити налаштування серверу налаштувати його адресацію, увімкнути HTTP та вписати файл index.html інформацію про роботу.

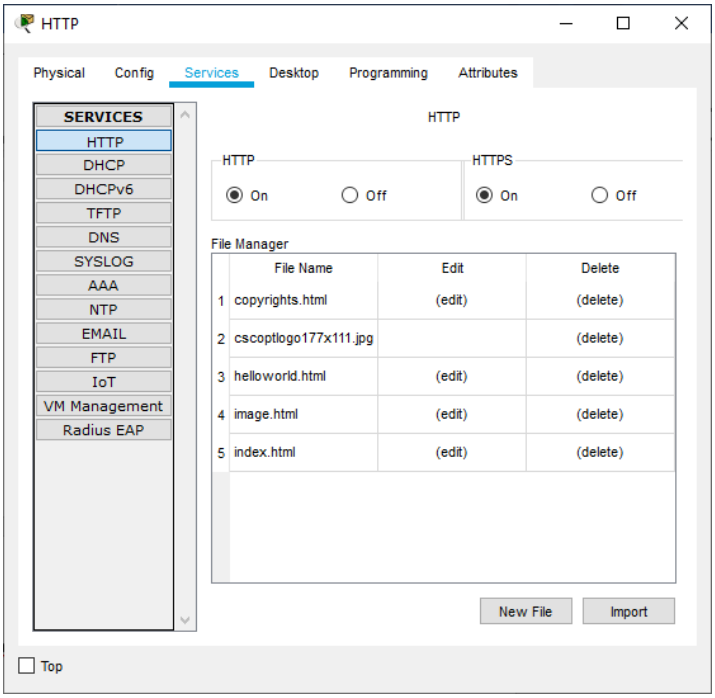

Рисунок 4.2 – Вікно налаштувань сервера HTTP

До того ж необхідно налаштувати DNS сервер, у налаштуваннях якого необхідно додати запис з доменним ім’ям та адресою HTTP сервера.

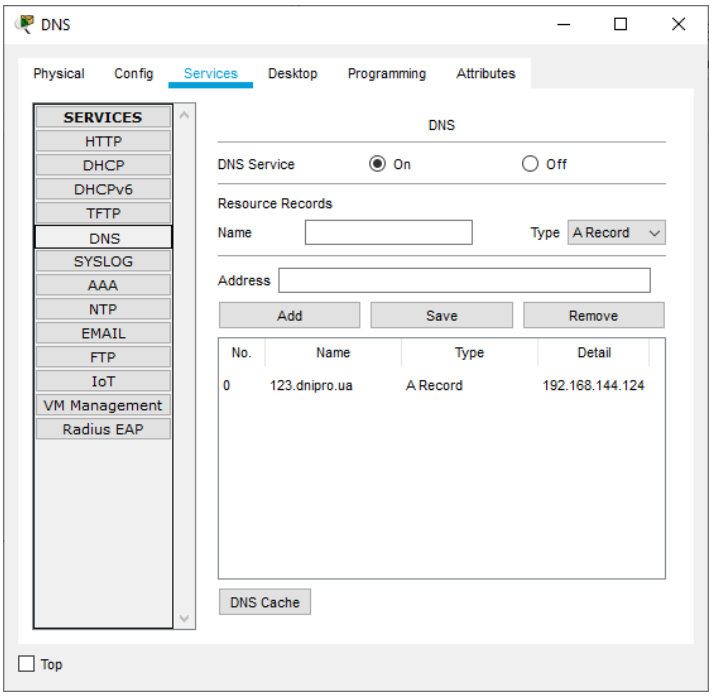

Рисунок 4.2 – Вікно налаштувань сервера DNS

4.4.2.3 Налаштування віртуальної приватної мережі

Для обміну інформацією між підмережою підрозділу ВНЗ з віддаленою підмережею необхідно налаштувати віртуальну приватну мережу site-to-site VPN. В таблиці 4.8 продемонстровані використані команди для налаштування динамічного VPN на маршрутизаторі Strotsenko_Router_5. Аналогічно налаштовується маршрутизатор Strotsenko_Router_0.

Таблиця 4.8 – команди для налаштування VPN

Команда	**Функції команди**
Strotsenko_Router_5(config)#license boot module c2900 technology-package securityk9	Введення ліцензії для можливості подальших налаштувань
Strotsenko_Router_5(config)#crypto isakmp policy 1	Створення політики
Strotsenko_Router_5(config-isakmp)#encryption 3des	Налаштування алгоритму шифрування
Strotsenko_Router_5(config-isakmp)#hash md5	Налаштування алгоритму хешування
Strotsenko_Router_5(config-isakmp)#authentication pre-share	Налаштування типу аутентифікації
Strotsenko_Router_5(config-isakmp)#group 2	Налаштування алгоритму для обміну ключами pre-share
Strotsenko_Router_5(config)#crypto isakmp key cisco address 209.165.200.1	Налаштування pre-share key
Strotsenko_Router_5(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac	Налаштування параметрів IPsec тунелю
Strotsenko_Router_5(config)#ip access-list extended FOR-VPN *Strotsenko_Router_5(config-ext-nacl)#permit ip 192.168.144.0 0.0.7.255 192.168.145.0 0.0.0.127* *Strotsenko_Router_5(config)#ip access-list extended Internet* *Strotsenko_Router_5(config-ext-nacl)#deny ip 192.168.144.0 0.0.7.255 192.168.145.0 0.0.0.127* *Strotsenko_Router_5(config-ext-nacl)#permit ip 192.168.144.0 0.0.7.255 any*	Налаштування списку доступу
Strotsenko_Router_5(config)#crypto map CMAP 10 ipsec-isakmp	Створення крипто-карти
Strotsenko_Router_5(config-crypto-map)#set peer 64.100.13.1	Налаштування peer, де вказується адреса зовнішнього порту маршрутизатора підмережі, до якої йде підключення
Strotsenko_Router_5(config-crypto-map)#set transform-set TS	Вказання параметрів IPsec тунелю
Strotsenko_Router_5(config-crypto-map)#match address FOR-VPN	Вказання трафіку який необхідно шифрувати
Strotsenko_Router_5(config)#int S0/3/1 *Strotsenko_Router_5(config-if)#crypto map CMAP*	Прив'язка крипто-карти до зовнішнього інтерфейсу маршрутизатора

4.4.3 Налаштування роботи AAA

Для налаштування служби AAA спочатку необхідно налаштувати Radius сервер. Для цього треба перейти налаштувань сервісу AAA на сервері та додати записи вузлів на яких буде застосована служба. В цих записах міститься ім’я вузлу, його IP-адреса, тип серверу Radius та ключ. Також необхідно додати користувачів та паролі для них. Вікно необхідних налаштувань приведено на рис. 4.3.

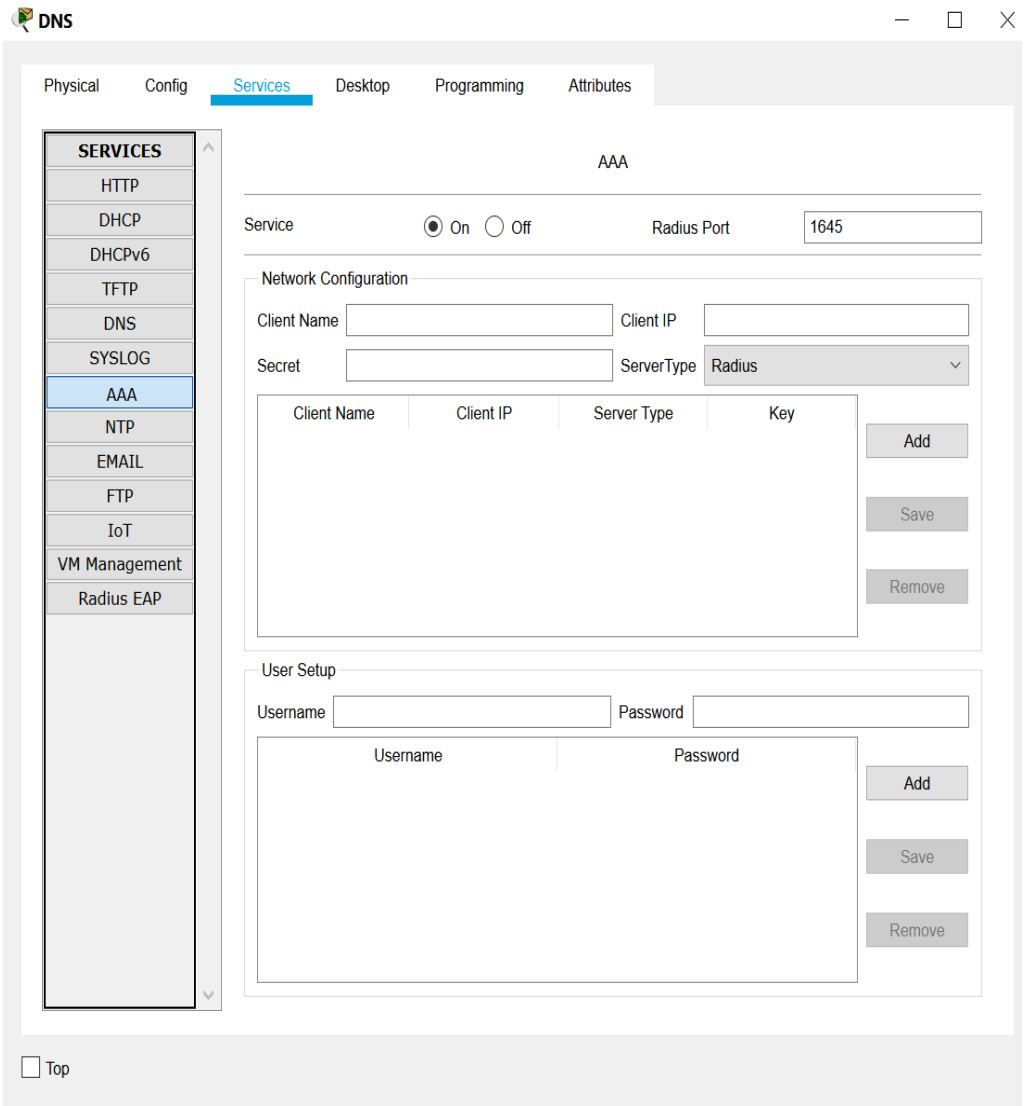

Рисунок 4.3 – Налаштування Radius серверу

Тепер необхідно налаштувати вузли на яких повинна бути налаштована служба AAA. Команди для налаштування приведені в табл. 4.9

Таблиця 4.9 – команди для служби AAA

Команда	**Функції команди**
Strotsenko_Router_3(config)#aaa new-model	Запуск служби AAA
Strotsenko_Router_3(config)#aaa authentication login default group radius local	Налаштування аутентифікації за допомогою служби AAA. У разі відсутності доступу до Radius серверу буде використана локальна база користувачів вузла
Strotsenko_Router_3(config)#radius-server host 192.168.144.91 key radius123	Налаштування алгоритму шифрування

5 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ПІДРОЗДІЛІВ ВНЗ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

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

Для захисту інформації в комп'ютерній системі підрозділів ВНЗ 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 у НТУ «ДП» у м. Дніпро 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 таблиці 5.1.

Таблиця 5.1 – Мережі VLAN и призначень портів

Номер VLAN	Ім'я VLAN	Порт	Примітка
1	Default	-	Не використовується
28	Rectorat	Strotsenko_Switch_0 – fa0/1-2 Strotsenko_Switch_1 – fa0/1-2 Strotsenko_Switch_16 – fa0/1-2	Для «Ректорату»
38	Admins	Strotsenko_Switch_1 – fa0/3-5 Strotsenko_Switch_16 – fa0/3-5	Для «ІКК»

Продовження таблиці 5.1

Номер VLAN	Ім’я VLAN	Порт	Примітка
48	Ordinary_empoyees	Strotsenko_Switch_0 – fa0/6-18 Strotsenko_Switch_1 – fa0/6-18 Strotsenko_Switch_16 – fa0/6-18	Для «Рядові співробітники»
99	Management	SVI	Для управління пристроями
100	Native	Strotsenko_Switch_0 – Gig0/1-2 Strotsenko_Switch_1 – Gig0/1-2 Strotsenko_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 під-мережі	Необхідний Розмір	Виді-лений розмір	Адреса	Маска	Діапазон досту-пних 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_em poyees	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 Strotsenko_Switch_1. Аналогічне налаштування виконується для інших мереж VLAN на відповідних портах.

Таблиця 5.3 – команди для базового налаштування пристроїв

Команда	Функції команди
Strotsenko_Switch_1(config)#vlan 28	Створення мережі VLAN 28
Strotsenko_Switch_1(config-vlan)# name Directorate	Надання імені мережі VLAN 28
Strotsenko_Switch_1(config)# interface range FastEthernet0/1-2	Вибір інтерфейсів для налаштувань
Strotsenko_Switch_1(config-if)# switchport mode access	Налаштування портів в якості портів доступу
Strotsenko_Switch_1(config-if)# switchport access vlan 28	призначте портам мережі VLAN
Strotsenko_Switch_1 (config)#vlan 100 *Strotsenko_Switch_1 (config-vlan)#name Native*	Налаштування мережі VLAN 100 як native VLAN
Strotsenko_Switch_1 (config)#interface range Gig0/1-2 *Strotsenko_Switch_1 (config-if)#switchport mode trunk* *Strotsenko_Switch_1 (config-if)#switchport trunk native vlan 100* *Strotsenko_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 Strotsenko_ Router _3 у якості DHCP-сервера. В таблиці 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
Strotsenko_Router_3(config)#ip dhcp pool pollvlan38	Створення пулу DHCP
Strotsenko_Router_3(dhcp-config)#network 192.168.144.120 255.255.255.248	Вказання пулу адрес для використання
Strotsenko_Router_3(dhcp-config)#default-router 192.168.144.121	Налаштування шлюзу за замовчуванням
Strotsenko_Router_3(dhcp-config)#dns-server 192.168.144.92	Налаштування адреси DNS-серверу
Strotsenko_Router_3(config)#ip dhcp excluded-address 192.168.144.121 *Strotsenko_Router_3(config)#ip dhcp excluded-address 192.168.144.122* *Strotsenko_Router_3(config)#ip dhcp excluded-address 192.168.144.123* *Strotsenko_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 таблиці 5.5 наведені відповідні команди.

Таблиця 5.5 – команди для налаштування функції безпеки портів

Команда	Функції команди
Strotsenko_Switch_1(config-if)#switchport mode access	Переведення порту в режим доступу
Strotsenko_Switch_1(config-if)#switchport port-security	Увімкнення port security на інтерфейсі
Strotsenko_Switch_1(config-if)#switchport port-security max 2	Дозвіл доступу до порту тільки двом унікальним пристроям
Strotsenko_Switch_1(config-if)#sw port mac-address sticky	Розпізнавання MAC-адреси пристрою динамічно і додавання в поточну конфігурацію
Strotsenko_Switch_1(config-if)#sw port violation restrict	Поява повідомлення під час порушенні системи безпеки та залишання порту включеним

6 ЕКОНОМІЧНА ЧАСТИНА

Розвиток технічних, апаратних і програмних засобів, дає можливість підприємствам зменшувати витрати, підвищувати якість продукції, збільшувати швидкість виробництва, автоматизувати процеси і безліч інших рішень.

У цьому розділі приведено економічне обґрунтування доцільності використання комп'ютерної системи.

6.1 Розрахунок капітальних витрат

6.1.1 Розрахунок трудомісткості розробки програмного забезпечення

Нормування праці в процесі створення програмного забезпечення ускладнене із-за творчого характеру праці програмістів. Тому трудомісткість обробки програмного забезпечення може бути розрахована на основі системи моделей з різною точністю оцінки.

Трудомісткість обробки праці програмного забезпечення можна розрахувати по формулі:

$$t = t0 + tд + ta + tn + tопл + tд, \text{ людино-годин} \qquad (6.1)$$

де *t0* − витрати праці на підготовку і опис поставленого завдання;

tд − витрати праці на дослідження алгоритму рішення завдання;

ta − витрати праці на обробку блок-схеми алгоритму;

tn − витрати праці на програмування по готовій блок-схемі;

tопл − витрати праці на налаштування програм на ЕОМ;

tд − 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:

$$Q = q \cdot c \cdot (1 + p), \tag{6.2}$$

де q − кількість операторів, використовуваних в програмі;

$з$ − коефіцієнт складності програми;

p − коефіцієнт корекції програми в процесі її обробки.

За узгодженням з керівником проекту, значення коефіцієнтів *з* і *p* були узяті відповідно до 1,25 і 0,2.

Таким чином, для програми, описаній в кваліфікаційній роботі:

$Q = 1200\,1{,}25 \cdot (1 + 0{,}2) = 1800$ операторів.

Оцінка витрат праці на підготовку і опис завдання в цьому д кваліфікаційній роботі складають t0=10.

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

$$t_u = \frac{Q \cdot B}{(75...85) \cdot k}, \textit{людино–годин}, \tag{6.3}$$

де B − коефіцієнт збільшення витрат праці *B=1,2.1,5*;

k − коефіцієнт програміста, які визначається залежно від стажу роботи за фахом.

В даному випадку коефіцієнт *k = 0,8* - при стажі роботи до 2 років.

Таким чином, витрати праці на вивчення опису завдання :

$$t_д = \frac{1800 \cdot 1{,}3}{85 \cdot 0{,}8} = 34.4 \ \textit{людино–годин}$$

Витрати праці на обробку алгоритму рішення задачі :

$$t_a = \frac{Q}{(20...25) \cdot k}, \textit{людиног–годин}, \tag{6.4}$$

$$t_a = \frac{1800}{25 \cdot 0{,}8} = 90 \ \textit{человеко – часов}.$$

Витрати праці на складання програми по готовій блок-схемі:

$$t_n = \frac{Q}{(20...25)\cdot k}, людино-годин, \quad (6.5)$$

$$t_n = \frac{1800}{25\cdot 0{,}8} = 90 \ людино-годин.$$

Витрати праці на налаштування програм ЕОМ розраховуються по формулі, за умови автономного налаштування одного завдання :

$$t_{отл} = \frac{Q}{(4...5)\cdot k}, людино-годин, \quad (6.6)$$

$$t_{отл} = \frac{1800}{5\cdot 0{,}8} = 450 \ людино-годин$$

Витрати праці на підготовку документації за завданням визначаються по формулі:

$$t_д = t_{др} + t_{до}, людино-годин, \quad (6.7)$$

де $t_{др}$ – трудомісткість підготовки матеріалів до рукопису;

$t_{до}$ – трудомісткість редагування, друку і оформлення документації.

$$t_{др} = \frac{Q}{(15...20) * k}; \quad (6.8)$$

$$t_{др} = \frac{1800}{20\cdot 0{,}8} = 112.5 \ людино-годин,$$

$$t_{др} = 0{,}75 \cdot t_{др}; \quad (6.9)$$

$t_{др} = 0{,}75 \cdot 112.5 = 84,4$ *людино − годин,*

$t_д = 112.5 + 84.4 = 196.9$ *людино-годин,*

t= 10 + 34,4 + 90 + 90 + 450 + 196,9 = 871,3 людино-годин.

Таким чином, трудомісткість розробки програмного забезпечення складає 871,3 людино-годин.

6.1.2 Розрахунок витрат на створення програмного забезпечення

Витрати на створення програмного забезпечення (*Кпз*) включають витрати на заробітну плату розробника програми і вартість машинного часу, необхідного для налаштування програми на ЕОМ (Змн) :

$$Кпз = Ззп + Змн, грн. \quad (6.10)$$

Заробітну плату розробника програми визначається по формулі:

$$З_{зп} = t \cdot C_{пр}, грн, \quad (6.11)$$

де t − загальна трудомісткість розробки програмного забезпечення;

$C_{пр}$ − середньо-годинна заробітна плата програміста (основна і додаткова) з нарахуваннями, грн/годину. *Спр*=45 грн/годину.

$З_{зп} = 871{,}3 * 45 = 37\ 408{,}5\ грн$.

Вартість машинного часу, необхідного для налаштування програми на ЕОМ:

$$З_{мв} = t_{отл} \cdot C_{мч}, грн \quad (6.12)$$

де _ − трудомісткість відладки програм на ЕОМ;

$C_{мч}$ − вартість машино-години ЕОМ, грн/годину.

Смч=15 грн/годину.

$З_{мв} = 450 \cdot 15 = 6750\ грн,$

$К_{по} = 37\ 405.5 + 6750 = 44\,158{,}5\ грн.$.

Таким чином, витрати на створення програмного забезпечення складають 44 158,5 грн

6.1.3 Розрахунок додаткових капітальних витрат

Капітальні витрати - це засоби, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Капітальні витрати на розробку створюваної системи видаленого контролю відбиті в табл. 6.1.

Таблиця 6.1 - Розрахунок капітальних витрат при розробці

№	Устаткування	Кількість, шт.	Ціна, грн	Монтажне-налагоджувальні роботи, грн	Всього
1	Ubiquiti UB-AM Universal Arm Bracket Кріплення універсальне	1	527,00	42,16	569,16
2	Маршрутизатор EdgeRouter 12 (ER-12)	2	7425,00	594,0	8019,00
3	EP-16 Ubiquiti EdgePoint-S16 Комутатор [EP-S16]	2	4125,00	330,00	4455,00
4	Комутатор UbiQuiti US-48-500W UniFi 48-500W [US-48-500W]	1	20825,00	1666,00	22491,00
5	Антена для засобів зв'язку Ubiquiti Ethernet Surge Protector захист від статики [ETH-SP]	1	510,00	40,80	550,80
6	Комутатор UbiQuiti ES-16-150W EdgeSwitch 16-150W [ES-16-150W]	1	9800,00	784,00	10584,00
7	Серверна платформа FWS-7160 (FWS-816B)	1	4050,00	324,00	4374,00
8	Серверна платформа FWS-215	1	2500,00	200,00	2700,00
9	Радіо-міст для сервера Ubiquiti PowerBeam 5AC-Gen2	1	9800,00	784,00	10584,00
10	Серверна платформа FWS-7600	1	2500,00	200,00	2700,00
11	Серверна платформа GCS-1100i	1	2500,00	200,00	2700,00
	Всього	**-**	**64562,00**	**5164,96**	**69726,96**

6.2 Експлуатаційні витрати

Експлуатаційні витрати - це поточні витрати на експлуатацію і обслуговування об'єкту проектування за певний період (наприклад, рік), виражені в грошовій формі:

$$З_{тек} = C_а + C_з + C_с + C_т + C_э, \quad (6.13)$$

де Ca − амортизаційні відрахування;

$Сз$ − заробітна плата обслуговуючого персоналу;

Сс − відрахування на соціальні заходи від заробітної плати (22% від *Сз*);

Ст − витрати на технічне обслуговування і поточний ремонт устаткування;

Сэ − вартість електроенергії, споживаної об'єктом.

Устаткування, розробленої в кваліфікаційній роботі системи управління, відноситься до 4 групи по мінімальних термінах корисного використання. Передбачуваний термін експлуатації системи складає 5 років.

Розрахунок амортизаційних відрахувань зробимо по методу прискореного зменшення залишкової вартості, де використовується подвоєна норма амортизації:

$$H_{\text{А}} = \frac{2}{t} \cdot 100,\ \%, \tag{6.14}$$

де На - коефіцієнт амортизації, долі одиниць.

Перевагою цього методу є те, що впродовж перших років експлуатації об'єкту проектування накопичується значна сума коштів, необхідних для його відновлення.

Отже, норма амортизації для проектованої і альтернативної системи управління складе:

$$H_{а\,а} = \frac{2}{5} \cdot 100 = 40\%,\ H_{а\,\text{пр}} = \frac{2}{5} \cdot 100 = 40\%.$$

$$\text{С}_а = \frac{\text{ПС} \cdot H_а}{100\%},\ \text{грн} \tag{6.15}$$

де Са - річна сума амортизації, грн;

ПС - первинна вартість (капітальні витрати − К), грн.

Са=Сз*0,4=69726,96*0,4=27 890,78грн.

Розрахуємо заробітну плату обслуговуючого персоналу :

$$C_з = ((T_к - T_{пр} - T_{вых} - T_{отп}) \cdot t_{см}) \cdot T_ч\ ,грн, \tag{6.16}$$

де $T_к$ − кількість календарних днів у році;

$T_{пр}$ − кількість днів празників у році;

$T_{отп}$ − кількість днів відпустки у році;

$T_{вых}$ − кількість вихідних днів у році;

$t_м$ − термін зміни;

$T_ч$ − середньо-годинна заробітна плата.

$C_з$ = (((365−10−104−20) · 8) · 42 = 77 616 *грн.*

Розрахуємо відрахування на соціальні заходи від заробітної плати:

Сс=0,22*Сз=0,22*77 616=17 075,52 грн.

Розрахуємо витрати на технічне обслуговування і поточний ремонт устаткування:

Ст=0,01*К=0,01*69726,96=697,27 грн.

Розрахуємо вартість електроенергії, споживаної об'єктом:

Сэ=Кэ*ds*Кд*Км*Т, грн. (6.17)

де Кэ - кількість електроенергії, споживаної на робочому місці за годину;

Км − кількість місяців в році;

Км − кількість робочих днів за місяць;

ds − тривалість зміни;

Т − тариф на електроенергію для підприємств (для підприємств 2 класу 0,64272 грн. з ПДВ).

Сэ = 1 * 8 * 21 * 12 * 0,64272 = 3 310,53 грн.

Експлуатаційні витрати складуть:

Зтек=27 890,78+77 616+17 075,52+697,27+3 310,53=126 590,1 грн.

Таким чином, річні експлуатаційні витрати, пов'язані із застосуванням системи, що розробляється, складатимуть 126 590,1 грн.

Річну економію на поточних витратах (*Рэк*), визначається по формулі:

Рэк = Зр - (Зтек + Зэ) (6.18)

де *Зтек* - річні поточні витрати, пов'язані із застосуванням системи4

Зр - витрати без застосування системи;

Зэ - витрати після застосування системи.

Розрахуємо річні витрати на рішення задачі без застосування розробленої системи.

За джерельними даними собівартість випуску продукції у середньому зменшиться на 1% (об'єм випуску дорівнює Зр = 72 000 000 грн.).

Розрахуємо річні витрати на рішення задачі без застосування розробленої системи;

Витрати на рішення задачі після застосування системи:

Зэ=0,72*100 000 000*(1,00-0,01)= 71 280 000 грн.

Визначимо річну економію на поточних витратах:

Рэк = 72 000 000 – (126 590,1 + 71 280 000) = 593 409,9 грн.

Таким чином, річна економія на експлуатаційних витратах складає 593,4 тис. грн.

6.3 Оцінка економічної ефективності

Оцінка економічної ефективності здійснюється на основі визначення і аналізу наступних показників :

1) розрахункового коефіцієнта ефективності капітальних витрат *Ер*;
2) терміну окупності капітальних витрат *Тэк*.

Коефіцієнт ефективності капітальних витрат показує, скільки гривен додаткової економії приносить одна гривна капітальних витрат:

$$Ер = \frac{Рэк}{К}, \tag{6.19}$$

де *До* - капітальні витрати на придбання і впровадження системи видаленого контролю;

Рэк - річна економія.

Ер = 593 409,9 / 69 726,96 = 8,51 (долі одиниць).

Таким чином, коефіцієнт ефективності капітальних витрат складе 8,51.

Термін окупності капітальних витрат на придбання і впровадження проекту за рахунок загальної економії розраховується по формулі:

$$Тэк = \frac{К}{Рэк}, \quad (6.20)$$

Тэк = 69 726,96 / 593 409,9 = 0,12.

Таким чином, термін окупності капітальних витрат складе 0,12 року.

Фінансово-економічні показники, що характеризують ефективність створення і використання розробленого проекту відображені в табл. 6.2.

Таблиця 6.2 - Фінансово-економічні показники використання системи, що розробляється

Найменування	**Одиниця виміру**	**Значення показника**
Капітальні витрати на придбання і впровадження системи	грн	69 726,96
Річні поточні витрати, пов'язані з використанням системи	грн	126 590,1
Річна економія від впровадження системи	грн	593 409,9
Коефіцієнт ефективності	долі од.	8,51
Розрахунковий термін окупності капітальних витрат	років	0,12

6.4 Висновок

У цьому розділі кваліфікаційної роботи були розраховані економічні показники, які показують економічну доцільність системи, що розробляється.

При впровадженні проектованої комп’ютерної системи капітальні витрати складуть 69,7 тис. грн. Річні поточні витрати складають 126,6 тис. грн. Річна економія на поточних витратах складає 593,4 тис. грн. Термін окупності проектних капітальних вкладень за рахунок скорочення експлуатаційних витрат складає 0,12 років. Коефіцієнт ефективності 8,51, тобто кожна гривна капітальних витрат принесе 8,51 грн. прибутку.

Виходячи з розрахованих даних, можна зробити висновок, що впровадження і використання проектованої системи економічно доцільне.

7 ОХОРОНА ПРАЦІ

7.1 Аналіз умов праці користувачів ПЕОМ

Приміщення управління Марганецького коледжу знаходиться на 1 поверсі будинку. У приміщенні працюють директор, головний бухгалтер, менеджери, оператори. Загальна площа приміщення складає 96 кв.м., обсяг – 288 м. куб. Висота приміщення – 3 м. У приміщенні постійно працює 6 чоловік. Використовуючи, ці данні можна зробити висновок, що на одного службовця приходитися 16 кв. м. площі і 19,2 куб. м. обсягу.

У приміщенні верхня частина стіни обшиті ДВП панелями, підлога покрита кахлем, стеля білого кольору. Інтер'єр приміщення оформлений відповідно з вимогами, без надмірностей (рис. 7.1). Приміщення прикрашено великою кількістю кімнатних рослин та рекламними плакатами.

Рисунок - 7.1 Загальний вигляд інтер'єр приміщення

У приміщенні відділу температура повітря в холодну пору складає 22–24° С, а в перехідний період – 21–24°С, відносна вологість складає 40–60%,

швидкість руху повітря – 0,1–0,2 м/с, що цілком відповідає стандартам, при яких людина добре себе почуває.

Для забезпечення чистоти повітря і підтримки метеорологічних умов у приміщенні відділу використовується комбінована вентиляція.

Природна вентиляція створює необхідний обмін повітря за рахунок різниці щільності теплого повітря, що знаходиться в приміщенні, і більш холодного повітря зовні, а також за рахунок вітру. Також, для створення автоматичної підтримки у відділі незалежно від зовнішніх умов постійної температури і вологості, установлений кондиціонер типу «Samsung».

Рівень шуму в приміщенні відповідає встановленим стандартам і дорівнює 70–60 дБ. Основними джерелами шуму є комп'ютери і принтери .

Комп'ютери є джерелом електромагнітного випромінювання, тому для захисту людей, що користаються комп'ютером, від випромінювання на моніторах встановлені захисні екрани.

Відповідно ДБН В.2.5-28-2006 штучне освітлення повинно бути 300 лк, для цього у кожній кімнаті встановлено по два світильники марки ЛПО 4 з потужністю 18 Вт. Світильники розташовані над робітниками місцями на відстані 2,8 м від рівня підлоги.

Працівники операторської використовують шість персональних комп’ютерів, два лазерні принтери Canon MF-211 та Canon LBP-2900, що мають невеликі габарити: монітор – 35х40х27 см, системний блок – 42х34х18 см, клавіатура – 46х15х2 см, принтер – 31х26х27 см. Зазначені пристрої живляться від мережі змінного струму напругою 220 В із застосуванням спеціального подовжувача – мережного фільтра, що стабілізує перепади напруги. Комп’ютери перебувають в експлуатації 4 роки; принтери – 3 роки.

Небезпека падіння з висоти при розташуванні робочого місця на значній висоті щодо поверхні землі або рівня підлоги повністю відсутня.

У приміщенні також є побутові приміщення – туалет, умивальник – розташовані в окремих кімнатах та кухня (рис. 7.2). Санітарний стан приміщен-

ня добрий: чисто, стіни оброблені плиткою, мається дзеркало. Також у приміщенні маються шафи для зберігання власних речей. Вони добре поєднуються з інтер'єром і мають відповідне розташування щоб не заважати переміщенню.

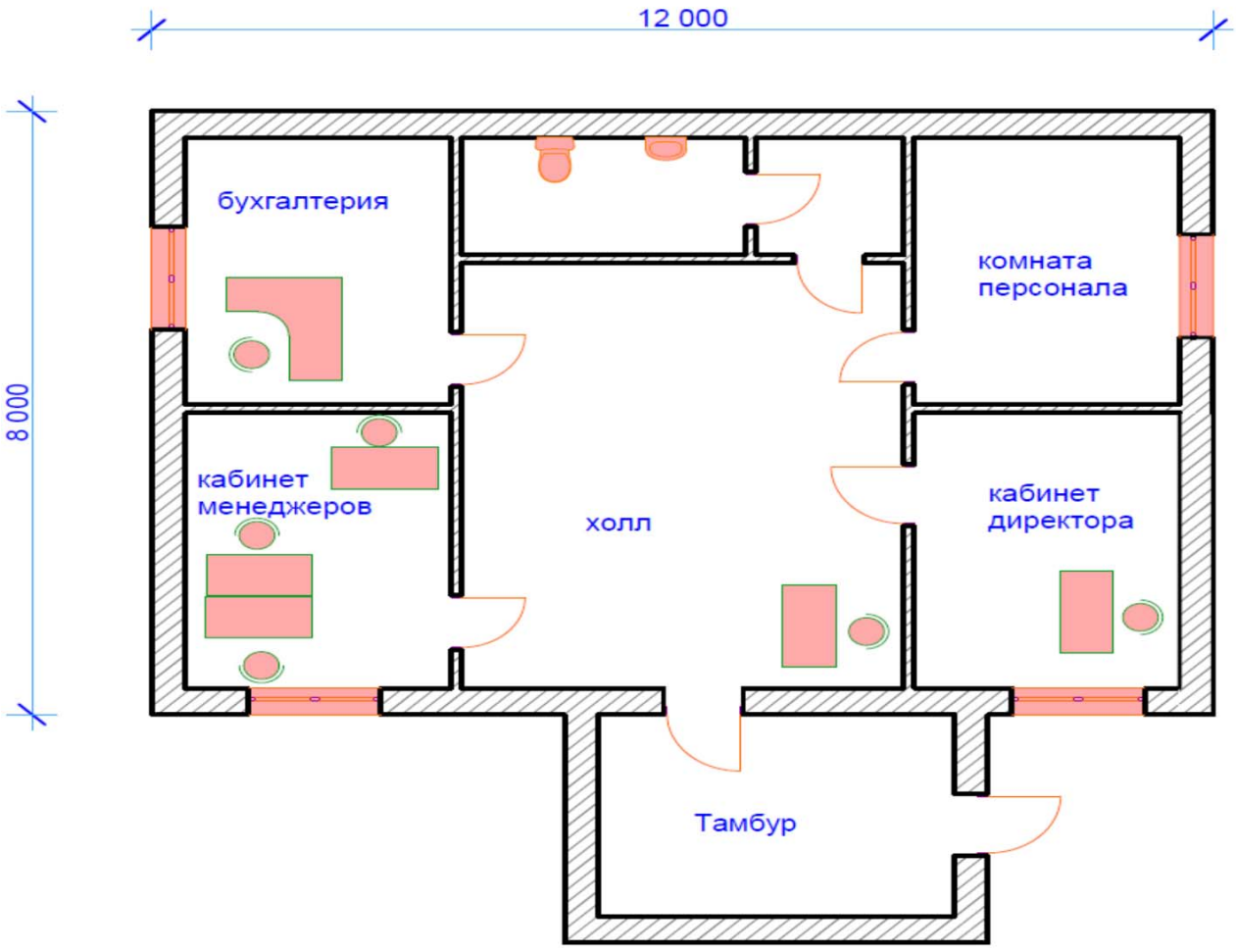

Рисунок 7.2 - Загальний вигляд приміщення

Загальні параметри умов праці в приміщенні відділу приведені в табл. 7.1, де вони порівнюються з затвердженими нормами і стандартами.

Таблиця 7.1 - Характеристика санітарно-гігієнічних умов праці

Параметр	**Фактичне значення**	**Норматив по Держстандарту**	**Відповідність параметра Держстандарту**
Шум, дБ	50–40	50–40	відповідає
Температура повітря, °С: холодного періоду перехідного періоду	 22–24 21–24	 23–25 22–24	 відповідає відповідає
Швидкість руху повітря, м/с	0,1–0,2	0,1–0,2	відповідає
Відносна вологість повітря, %	40–60	40–60	відповідає

7.2 Пропозиції стосовно охорони праці на робочому місці

Для зменшення рівня звуку і вібрації застосовуються демпфуючі матеріали (гумова прокладка під принтер). Шумопоглинальні засоби застосовуються не спаленні або тяжко спаленні спеціальні перфоровані плити, панелі, мінеральна вата та інші.

Комп'ютер і в першу чергу монітор є джерелами:

- електростатичного поля;
- слабих електромагнітних випромінювань в низькочастотному і високочастотному діапазонах (2 Гц …400 Гц);
- рентгенівського випромінювання;
- ультрафіолетового, інфрачервоного і випромінювання видимого діапазону.

Згідно, встановлюються гранично допустимі значення напруженості електричного і магнітного полів частотою 50 Гц залежно від часу перебування персоналу в приміщенні. Напруженість електричного поля не перевищує 5 кВ/м, напруженість магнітного поля на робочому місці не перевищує 8 кА/м, а напруженість електростатичного поля не перевищує 20 кВ/м, що дозволяє не регламентувати час перебування в приміщенні.

Потужність експозиційної дози рентгенівського випромінювання на відстані 0,05 м від екрану не перевищує 0,1 мбер/час. Рівні всіх можливих ви-

промінювань достатньо низькі і не перевищують діючі норми. На робочому місці, що вивчається, розміщений найбезпечніший монітор, в якому створений додатковий металевий внутрішній контур, замкнутий на вбудований захисний екран.

При організації робочого місця за комп'ютером дотримувалися наступні розміри:

- відстань від підлоги до сидіння крісла дорівнює 440 мм;
- відстань від сидіння крісла до нижнього краю робочої поверхні 330 мм;
- відстань від очей до дисплея 550 мм;
- простір для ніг 770 мм;
- відстань від ніжки столу до краю робочої поверхні столу 640 мм;
- М - відстань між передньою поверхнею тіла і краєм робочої поверхні столу 80 мм;
- відстань від очей до документації 500 мм;
- оптимальна зона моторного поля 360 мм;
- висота робочої поверхні 800 мм;
- кут огляду документів 30.

Екран дисплея по висоті розташований на столі так, що кут між нормаллю до центру екрану і горизонтальною лінією погляду складає 20. Кут спостереження екрану в горизонтальній площині не перевищує 60°. Передбачені перерви, що регламентуються, для відпочинку тривалістю 15 хвилин після кожних двох годин роботи.

При роботі з комп’ютерами і друкувальними пристроями потрібно дотримуватися певних правил безпеки:

- до включення електроживлення необхідно перевірити візуально цілісність сполучних кабелів;
- не підключати й не відключати кабелі електроживлення при поданій напрузі мережі;

- не залишати комп’ютер включеним без нагляду;
- не відкривати корпус і витягати елементи системи комп’ютера при включеному живленні;
- по закінченню роботи відключати техніку від мережі.

Для захисту співробітників від поразки застосовується такий тип захисту, як заземлення електроприладів, головним призначенням якого є понизити потенціал на корпусі електроустаткування до безпечної величини.

Також варто помітити, що електропроводка в приміщенні улаштована правильно: схована в стінах, виконана відповідно до норм.

Значне місце в комплексі засобів, спрямованих на охорону праці, займають інструктаж і навчання правилам безпечних прийомів і методів роботи.

Для проведення інструктажу використовується хол зі плакатами з охорони праці, де проводиться первинний ознайомлювальний інструктаж. Проведення інструктажу реєструється в спеціальному журналі по техніки безпеки і завіряється підписом інструктованого. Періодично проводяться огляди електроустаткування.

Конструкція робочого місця користувача відеотермінала (при роботі сидячи) має забезпечувати підтримання оптимальної робочої пози з такими ергономічними характеристиками: ступні ніг – на підлозі або на підставці для ніг; стегна – в горизонтальній площині; передпліччя – вертикально; лікті – під кутом 70–90^{o} до вертикальної площини; зап’ястя зігнуті під кутом не більше 20^{o} відносно горизонтальної площини, нахил голови –15–20^{o} відносно вертикальної площини.

Висота робочої поверхні столу для відеотермінала має бути в межах 625–800 мм, а ширина – забезпечувати можливість виконання операцій в зоні досяжності моторного поля. Рекомендовані розміри столу: висота –725 мм, ширина –800–1200 мм, глибина –800–1000 мм (рис. 7.3).

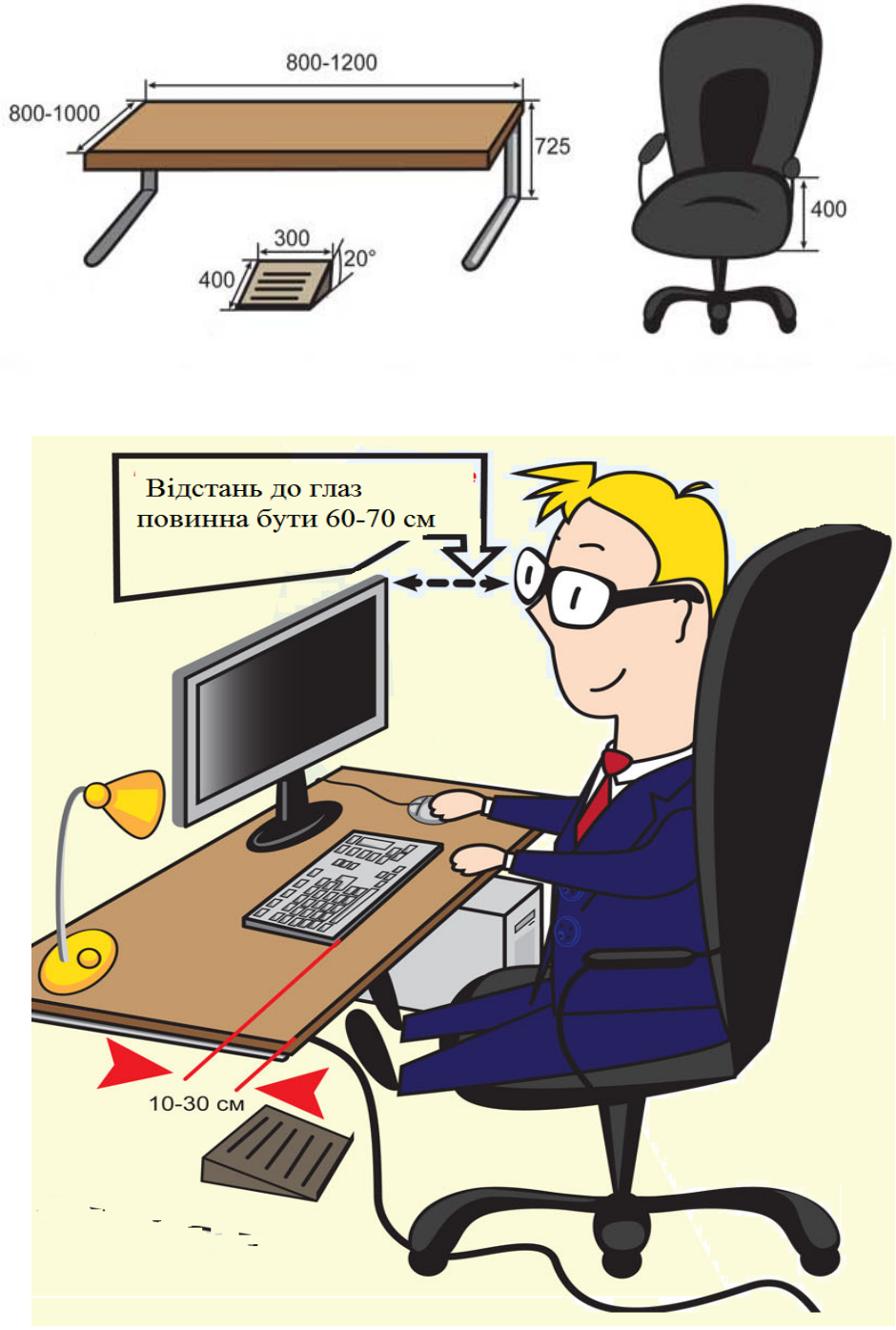

Рисунок 7.3 - Рекомендації щодо організації робочого місця

Для зниження статичного напруження м’язів рук необхідно застосовувати стаціонарні або знімні підлокітники довжиною не менше 250 мм, шириною – 50 – 70 мм, що регулюються по висоті над сидінням у межах230 ± 3О мм та по відстані між підлокітниками в межах 350–500 мм.

Екран відеотермінала та клавіатура мають розташовуватися на оптимальній відстані від очей користувача, але не ближче 600 мм, з урахуванням розміру алфавітно–цифрових знаків та символів. Відстань від екрана до ока працівника повинна складати:

- при розмірі екрану по діагоналі 35/38 см (14" /15") – 600 – 700 мм
- при розмірі екрану по діагоналі 43 см (17") – 700 – 800 мм
- при розмірі екрану по діагоналі 48 см (19") – 800 – 900 мм
- при розмірі екрану по діагоналі 53 см (21") – 900 – 1000 мм

Клавіатуру слід розміщувати на поверхні столу або на спеціальній, регульованій за висотою, робочій поверхні окремо від столу на відстані 100–300 мм від краю(Рис 3), ближчого до працівника. Кут нахилу клавіатури має бути в межах $5–15^0$.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрану відеотермінала, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля: по висоті 900 – 1300 мм, по глибині 400 – 500 мм.

При потребі високої концентрації уваги під час виконання робіт з високим рівнем напруженості суміжні робочі місця з відеотерміналами та персональними ЕОМ необхідно відділяти одне від одного перегородками висотою 1,5 – 2 м.

При розміщенні робочих місць з відеотерміналами та персональними ЕОМ необхідно дотримуватись таких вимог:

- робочі місця з відеотерміналами та персональними ЕОМ розміщуються на відстані не менше 1 м від стін зі світловими прорізами;
- відстань між бічними поверхнями відеотерміналів має бути не меншою за 1,2 м;

- відстань між тильною поверхнею одного відео термінала та екраном іншого не повинна бути меншою 2,5 м;
- прохід між рядами робочих місць має бути не меншим 1 м.

Для забезпечення раціонального розміщення працівників в приміщенні відповідно вимог було розроблено схему наведену на рис. 7.4.

Рисунок 7.4 - Рекомендоване розміщення працівників в приміщенні

7.3 Міри пожежної профілактики

Дане приміщення за ступенем пожежної небезпеки можна віднести до категорії «В», тому що в роботі відділу використовується папір, пластикові меблі й меблі із ДВП (НАПБ Б.03.002-2014). За ступенем вогнестійкості приміщення відноситься до І категорії. Це відповідає вимогам пожежної безпеки, зазначеним у ДБН В.1.1-7-2002. За ступенем небезпеки враження електричним струмом приміщення можна класифікувати як таке, що має категорію "без підвищеної небезпеки", оскільки вся зазначена офісна техніка має захисне заземлення, передбачене її конструкцією, і повністю виключає можливість випадкового контакту із частинами, що перебувають під небезпечною для людини напругою.

У приміщенні повністю відсутня небезпека контакту з рухомими частинами обладнання, оскільки характер діяльності підрозділу не пов’язаний із транспортуванням яких-небудь виробів і не має обладнання з рухливими частинами, здатними травмувати людину.

Майже вся офісна техніка має запобіжний механізм, що змушує її відключатися при проникненні усередину корпусу. Тому небезпека враження електричним струмом майже повністю відсутня. Однак така можливість існує у випадках порушення працівниками правил користування офісною технікою, зокрема при самостійних спробах усунення яких-небудь несправностей без наявності для цього необхідної кваліфікації й навичок, особливо якщо техніка при цьому не відключена від електромережі.

Небезпека одержання термічних опіків при дотику до нагрітої до високої або охолодженої до низької температури поверхні обладнання майже повністю відсутня. Друкуючий фотоелемент принтера при тривалій роботі може сильно нагріватися й при дотику до неї працівник може одержати незначний опік. Однак конструкція принтера не допускає можливості випадкового дотику до нього. Про небезпеку дотику до нагрітого фотоелемента є відповідний попереджуючий напис на поверхні принтера.

Небезпека вибуху повністю відсутня, тому що відсутні речовини, здатні викликати вибухи. Небезпека пожежі незначна. Хоча в приміщенні й присутні легкозаймисті матеріали і предмети, здатні спричинити пожежу, паперові документи зберігаються у вогнетривкому сейфі й працівники планово-виробничого відділу пройшли інструктаж із протипожежної безпеки. У приміщенні є протипожежна сигналізація.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи була розроблена комп'ютерна з блокчейн технологією підтримки реєстру студентів ВНЗ першого рівня акредитації НТУ «ДП», метою якої є полегшення роботи працівників підрозділів, збільшення їх продуктивності, покращення сервісу для студентів та збільшення іміджу ВНЗ, що в подальшому збільшить його прибутки.

Згідно з розробленими технічними вимогами до комп'ютерної системи, організаційної структури та топологічними особливостями об’єкту розробки була розроблена структурної схеми комплексу технічних засобів комп’ютерної системи та виконаний підбір необхідного обладнання для створення комп'ютерної системи.

Для комп’ютерної мережі був проведений розрахунок налаштувань маршрутизації, втілені методи для захисту інформації в комп’ютерній системі відповідно до вимог налаштування параметрів безпеки і виконана перевірка її роботи методом моделювання комп’ютерної системи у багатофункціональній програмі моделювання мереж Cisco Packet Tracer.

Кваліфікаційна робота виконана повністю відповідно до теми і завдання, оформлена відповідно до нормативних документів і методичного керівництва.

Цілі, поставлені перед кваліфікаційною роботою, повністю виконані.

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.

ДОДАТОК А

ТЕКСТ ПРОГРАМИ НАЛАШТУВАННЯ МАРШРУТИЗАТОРА STROTSENKO_ROUTER_5 ТА КОМУТАТОРА STROTSENKO_SWITCH_1

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.20017-01 12 18

Листів 10

2020

АНОТАЦІЯ

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

Програма призначена для забезпечення налаштування DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену и ssh комп’ютерної системи.

ЗМІСТ

1. Налаштування маршрутизатора Strotsenko_Router_5

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption // Шифрування паролів
!
hostname Strotsenko_Router_5 // Ім'я пристрою
!
enable password 7 0822404F1A0A // Пароль до привілейованого режиму
!
ip dhcp excluded-address 192.168.146.1 // Виключення адрес з пулу DHCP
ip dhcp excluded-address 192.168.146.2
ip dhcp excluded-address 192.168.146.3
!
ip dhcp pool LAN5 //Створення та налаштування пулу для локальної мережі
network 192.168.146.0 255.255.255.128
default-router 192.168.146.1
dns-server 192.168.144.123
!
aaa new-model // Налаштування аутентифікації через AAA-сервер
!
aaa authentication login default group radius local
!
no ip cef
no ipv6 cef
!
username 123161_Strotsenko password 7 082048430017061E010803 // Створення користувача та пароля
! //Налаштування VPN
license udi pid CISCO2911/K9 sn FTX15241V68-
license boot module c2900 technology-package securityk9
!
crypto isakmp policy 1
encr 3des
hash md5
authentication pre-share
group 2
!
crypto isakmp key cisco address 64.100.13.1
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map CMAP 10 ipsec-isakmp
```

```
set peer 64.100.13.1
set transform-set TS
match address FOR-VPN
!
ip domain-name Strotsenko_Router_5 // Створення домену
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0 // Налаштування інтерфейсів
ip address 192.168.146.1 255.255.255.128
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/2/0
ip address 10.0.18.18 255.255.255.252
ip nat inside
clock rate 128000
!
interface Serial0/2/1
ip address 10.0.18.30 255.255.255.252
ip nat inside
!
interface Serial0/3/0
ip address 10.0.18.34 255.255.255.252
ip nat inside
!
interface Serial0/3/1
ip address 209.165.200.1 255.255.255.224
ip access-group ACL_LAN4 out
ip nat outside
ip summary-address eigrp 16 192.168.144.0 255.255.248.0 5
crypto map CMAP
```

```
!
interface Vlan1
no ip address
shutdown
! // Налаштування динамічної маршрутизації
router eigrp 16
eigrp router-id 5.5.5.5
redistribute static
passive-interface GigabitEthernet0/0
network 192.168.146.0 0.0.0.127
network 10.0.18.28 0.0.0.3
network 10.0.18.16 0.0.0.3
network 10.0.18.32 0.0.0.3
network 209.165.202.0 0.0.0.3
! // Налаштування NAT
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list 18 pool Internet
ip nat inside source list Internet interface Serial0/3/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.2
!
ip flow-export version 9
! // Налаштування списків доступу
ip access-list extended FOR-VPN
permit ip 192.168.144.0 0.0.7.255 192.168.145.0 0.0.0.127
ip access-list extended Internet
deny ip 192.168.144.0 0.0.7.255 192.168.145.0 0.0.0.127
permit ip 192.168.144.0 0.0.7.255 any
ip access-list standard ACL_LAN4
deny 192.168.145.128 0.0.0.127
!
banner motd ^CThis is a secure system. Authorized Access Only!^C // Налаштування банеру MOTD
! // Налаштування Radius сервера
radius-server host 192.168.144.91 auth-port 1645 key radius123
radius-server host 192.168.144.122 auth-port 1645 key radius123
! // Налаштування ліній консолі та vty і ssh
line con 0
password 7 0822455D0A16
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
transport input ssh
```

```
line vty 5 15
password 7 0822455D0A16
transport input ssh
!
End
```

2. Налаштування коммутатора Strotsenko_Switch_1

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption // Шифрування паролів
!
hostname Strotsenko_Switch_1 // Ім'я пристрою
!
enable password 7 0822404F1A0A //Пароль до привілейованого режиму
!
ip domain-name Strotsenko_Switch_1 // Створення домену
!
username 123161_Strotsenko privilege 1 password 7 082048430017061E010803 //
Створення користувача та пароля
!
spanning-tree mode pvst
spanning-tree extend system-id
! // Налаштування інтерфейсів
interface FastEthernet0/1
switchport access vlan 28
!
interface FastEthernet0/2
switchport access vlan 28
! // Налаштування безпеки на портах, до яких підключені сервери
interface FastEthernet0/3
switchport access vlan 38
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
!
interface FastEthernet0/4
switchport access vlan 38
switchport mode access
switchport port-security
switchport port-security maximum 2
```

```
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 0090.2BE6.564D
!
interface FastEthernet0/5
switchport access vlan 38
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
switchport port-security mac-address sticky 00D0.D38C.1AA9
!
interface FastEthernet0/6
switchport access vlan 48
!
interface FastEthernet0/7
switchport access vlan 48
!
interface FastEthernet0/8
switchport access vlan 48
!
interface FastEthernet0/9
switchport access vlan 48
!
interface FastEthernet0/10
switchport access vlan 48
!
interface FastEthernet0/11
switchport access vlan 48
!
interface FastEthernet0/12
switchport access vlan 48
!
interface FastEthernet0/13
switchport access vlan 48
!
interface FastEthernet0/14
switchport access vlan 48
!
interface FastEthernet0/15
switchport access vlan 48
!
interface FastEthernet0/16
switchport access vlan 48
```

```
!
interface FastEthernet0/17
switchport access vlan 48
!
interface FastEthernet0/18
switchport access vlan 48
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
! // Налаштування транкових портів
interface GigabitEthernet0/1
switchport trunk native vlan 100
switchport trunk allowed vlan 1,28,38,48,99-100
switchport mode trunk
!
interface GigabitEthernet0/2
switchport trunk native vlan 100
switchport trunk allowed vlan 1,28,38,48,99-100
switchport mode trunk
!
interface Vlan1
no ip address
shutdown
! // Налаштування інтерфейсу керування
interface Vlan99
mac-address 0030.a313.1801
ip address 192.168.144.99 255.255.255.248
!
banner motd ^CThis is a secure system. Authorized Access Only!^C // Налашту-
вання банеру MOTD
! // Налаштування ліній консолі та vty і ssh
line con 0
password 7 0822455D0A16
login local
!
line vty 0 4
```

```
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh
!
end
```