

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

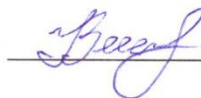
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект інформаційної системи управління
завданнями та доступом до ресурсів компанії на базі
рішень Microsoft та Cisco»

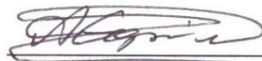
Виконав студент 4-го курсу групи КІ-4
спеціальності 123 «Комп'ютерна інженерія»

 Вадим ЗАГАЦЬКИЙ

Керівник доцент кафедри КН, к.т.н.

 Ірина ПАНАРІНА

Рецензент завідувач кафедри КІ та КБ, к.т.н., доцент

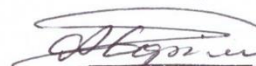
 Андрій ЄФІМЕНКО

Житомир – 2022

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій ЄФІМЕНКО

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Загацький Вадим Валентинович

Тема роботи: «Проект інформаційної системи управління завданнями та доступом до ресурсів компанії на базі рішень Microsoft та Cisco»

затверджена Наказом університету від 1 березня 2022 р. № 127/с

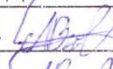
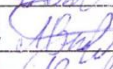
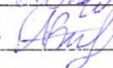
Термін здачі студентом закінченої роботи 10 червня 2022 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
Об'єктом дослідження є автоматизація процесу управління завданнями та доступом до ресурсів компанії. Предметом дослідження є використання технологій розробки веб-додатків, збереження даних, системи міжмережевих екранів для автоматизації процесу управління завданнями та доступом до ресурсів компанії на базі рішень Microsoft та Cisco.

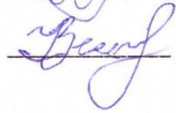
Обладнання та програмне забезпечення:

1. Cisco ISR4331, Cisco 1941-SEC/K9, Cisco WS-C2960-24TC-L
2. Windows Server 2019 Standard, Ubuntu 20.04 LTS, Windows 7
3. GNS, Apache2, MySQL 8.0, PHP 7.4

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Віталій ЛЕВКІВСЬКИЙ	02.03.22 	02.03.22 
2	Віталій ЛЕВКІВСЬКИЙ	15.04.22 	15.04.22 
3	Віталій ЛЕВКІВСЬКИЙ	10.05.22 	10.05.22 

Студент  Вадим ЗАГАЦЬКИЙ

Керівник  Ірипа ПАНАРИНА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	14.02.22 – 20.02.22	виконано
2	Аналіз літературних джерел	21.02.22 – 06.03.22	виконано
3	Аналіз об'єкта дослідження	07.03.22 – 13.03.22	виконано
4	Пошук, огляд та аналіз аналогічних розробок	14.03.22 – 20.03.22	виконано
5	Розробка захищеної КМ	21.03.22 – 03.04.22	виконано
6	Написання програмного коду	04.04.22 – 24.05.22	виконано
7	Налаштування мережі	25.05.22 – 08.05.22	виконано
8	Адміністрування мережі	09.05.22 – 15.05.22	виконано
9	Перевірка працездатності	16.05.22 – 22.05.22	виконано
10	Оформлення пояснювальної записки	23.05.22 – 10.06.22	виконано

Студент  Вадим ЗАГАЦЬКИЙ

Керівник  Ірина ПАНАРИНА

РЕФЕРАТ

Пояснювальна записка до випускної кваліфікаційної роботи бакалавра на тему «Проект інформаційної системи управління завданнями та доступом до ресурсів компанії на базі рішень Microsoft та Cisco» складається з вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Текстова частина викладена на 57 сторінках друкованого тексту. Пояснювальна записка має 22 сторінки додатків. Список використаних джерел містить 20 найменувань і займає 2 сторінки. В роботі наведено 55 рисунків. Загальний обсяг роботи – 79 сторінок.

У першому розділі було проведено аналіз завдання, порівняно існуючі аналоги, обґрунтовано вибір інструментарію та архітектури додатку, наведено теоретичні основи захисту мереж з використанням брандмауерів зональних політик.

У другому розділі визначено варіанти використання та структуру системи, розроблено базу даних, реалізовано веб-додаток та спроектовано топологію комп'ютерної мережі.

У третьому розділі було розгорнуто служби Active Directory, налагоджено обладнання мережі, описано порядок та способи роботи з системою управління завданнями, протестовано програмне забезпечення та мережа.

Висновки містять в собі результати виконаної роботи проектування, розробки та тестування інформаційної системи управління завданнями та доступом до ресурсів компанії на базі рішень Microsoft та Cisco.

У додатку представлені характеристики мережевих пристроїв та лістинг їх конфігураційних файлів.

Ключові слова: ЗАДАЧІ, УПРАВЛІННЯ, ПІДПРИЄМСТВО, MVC, ДАНІ, КОМП'ЮТЕРНА МЕРЕЖА, ACTIVE DIRECTORY.

					КІК.КР.Б – 123 – 12 – ПЗ				
Змн.	Арк.	№ докум.	Підпис	Дата	Проект інформаційної системи управління завданнями та доступом до ресурсів компанії на базі рішень Microsoft та Cisco	Літ.	Арк.	Аркуші	
Розроб.		В.Загацький		14.06					
Керівник		І. Панаріна		14.06					
Реценз.		А. Єфіменко		20.06					
Н. Контр.									
Затверд.		А. Єфіменко		20.06					
					ФІКТ, гр. КІ-4				

ABSTRACT

An explanatory note to the bachelor's thesis on "Project management information system and access to company resources based on Microsoft and Cisco solutions" consists of an introduction, three chapters, conclusions, references and appendix.

The text is set out on 57 pages of printed text.

The explanatory note has 22 pages of appendices. The list of used sources contains 20 names and occupies 2 pages. The paper presents 55 pictures. The total volume of work is 79 pages.

In the first section the initial analysis of the task was carried out, the existing analogues were compared, the choice of tools and architecture of the application was substantiated, the theoretical bases of network protection with the use of firewalls of zonal policies were given.

The second section identifies usage options and system structures, develops a database, implements a web application, and designs a computer network topology.

In the third section, Active Directory services were deployed, network equipment was configured, the procedure and methods of working with the task management system were described, software and network were tested.

The conclusion contains the results of the work performed by the design, development and testing of information management system for tasks and access to company resources based on Microsoft and Cisco solutions.

The appendix presents the characteristics of network devices and a list of their configuration files.

Keywords: TASKS, MANAGEMENT, ENTERPRISE, MVC, DATA, COMPUTER NETWORK, ACTIVE DIRECTORY.

		<i>В.Загацький</i>			<i>КІК.КР.Б – 123 – 12 – ПЗ</i>	<i>Арк.</i>
		<i>І. Панаріна</i>				
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<i>5</i>

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП	8
РОЗДІЛ 1. АНАЛІЗ НАПРЯМКІВ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ СИСТЕМИ УПРАВЛІННЯ ТА РОЗМЕЖУВАННЯ ДОСТУПУ В МЕРЕЖІ	10
1.1. Постановка задачі	10
1.2. Порівняння існуючих аналогів програмного продукту	12
1.3. Обґрунтування вибору інструментальних засобів та архітектури системи.....	17
1.4. Застосування міжмережевих екранів для підвищення рівня захисту мережі	18
РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ ЗАВДАННЯМИ ТА ДОСТУПОМ ДО РЕСУРСІВ КОМПАНІЇ НА БАЗІ РІШЕНЬ MICROSOFT ТА CISCO	22
2.1. Визначення варіантів використання, структури системи та функціональних алгоритмів.....	22
2.2. Розробка бази даних системи	26
2.3. Реалізація додатку управління завданнями та доступом до ресурсів компанії.....	28
2.4. Розробка топології комп'ютерної мережі та проекту підсистеми мережного екранування трафіку	32
РОЗДІЛ 3. РОЗГОРТАННЯ СТРУКТУРИ ТА ПОРЯДОК РОБОТИ З СИСТЕМОЮ УПРАВЛІННЯ ЗАВДАННЯМИ ТА ДОСТУПОМ ДО РЕСУРСІВ КОМПАНІЇ НА БАЗІ РІШЕНЬ MICROSOFT ТА CISCO	36
3.1. Розгортання структури Active Directory та налагодження обладнання мережі.....	36
3.2. Інтерфейс та порядок роботи з системою управління завданнями та доступом до ресурсів компанії на базі рішень Microsoft та Cisco.	45
3.3. Тестування роботи програмного забезпечення. Перевірка працездатності мережі.....	50
ВИСНОВКИ	55
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	56
ДОДАТКИ	58

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

AD – Active Directory Domain Services – служба каталогів, розроблена Microsoft для доменних мереж Windows.

DMZ – Demilitarized Zone – сегмент мережі, що містить загальнодоступні сервіси та відокремлює їх від приватних.

DNS – Domain Name System – комп'ютерна розподілена система для отримання інформації про домени.

FTP – File Transfer Protocol – протокол для передачі файлів у мережі між комп'ютерами.

HTTP – HyperText Transfer Protocol – протокол прикладного рівня передачі даних у вигляді гіпертекстових документів у форматі HTML.

ICMP – Internet Control Message Protocol – протокол третього рівня моделі OSI, який використовується для діагностики проблем зі зв'язністю у мережі.

IP – Internet Protocol.

LPAD – Lightweight Directory Access Protocol – стандартизований прикладний протокол для доступу та обслуговування розподілених по мережі інформаційних служб каталогів.

ZPF – Zone-based firewall – міжмережевий екран, що є одним із компонентів програмного забезпечення Cisco IOS.

ІКС – Інформаційно-комунікаційна система

ЛКМ – Локальна комп'ютерна мережа

ПК – Персональний комп'ютер

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ВСТУП

Нині сфера послуг є надзвичайно розвиненою, вона є невіддільною потребою сучасної людини. Ми постійно розвиваємося й рухаємося вперед, при цьому збільшуючи свої вимоги. Задачі, які виконуються мають надзвичайно широку класифікацію та способи їх реалізації.

В даній області одним з найбільших активів компанії є споживачі та відносини з ними. Відповідно до вимог замовників складаються проекти, які описують всю подальшу концепцію співпраці. Розробка координаційних процесів вимагає значного витраченого часу, співпраці багатьох співробітників та керівників відділів, причому, надалі для них потребується постійний контроль та вдосконалення методів роботи. Зі збільшенням розмірів та розвитком багатозадачності компаній для багатьох з них стало очевидним, що використовуючи автоматизовані інформаційні системи, стає можливим підвищення ефективності та прибутковості бізнесу. Це також дає змогу удосконалити систему звітності та зменшити залежність від роботи менеджерів.

У наш час управління проектами застосовується майже у всіх галузях. Наприклад вони здатні допомогти ІТ-команді розроблювати інноваційне програмне забезпечення в рекордно короткі терміни, правильно розділяючи завдання та ресурси, або, допомогти державній установі покращити швидкість надання послуг.

Для взаємодії будь-якої інформаційної системи, як для великих, так і малих компаній використовують технології комп'ютерних мереж. При чому, досить часто корпоративні мережі знаходяться фізично віддалено один від одного. Для з'єднання між собою використовують ті ж самі глобальні мережі. Правильне проектування мережі, налаштування технологій міжмережевих екранів є одними з важливих моментів та актуальних тем безпеки ресурсів. Важливо не допускати критичних помилок у захисті мереж, уміти передбачати вразливості, мати інші способи розв'язання поставлених задач.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		8

Метою кваліфікаційної роботи є розробка додатка для управління задачами, проектування підсистеми міжмережевого екранування трафіку, дослідження та налаштування служб Active Directory для потреб компанії.

Об'єктом дослідження є автоматизація процесу управління завданнями та доступом до ресурсів компанії.

Предметом дослідження є використання технологій розробки веб-додатків, збереження даних, системи міжмережевих екранів для автоматизації процесу управління завданнями та доступом до ресурсів компанії на базі рішень Microsoft та Cisco.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1. АНАЛІЗ НАПРЯМКІВ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ СТВОРЕННЯ СИСТЕМИ УПРАВЛІННЯ ТА РОЗМЕЖУВАННЯ ДОСТУПУ В МЕРЕЖІ

1.1. Постановка задачі

Управління задачами є однією із частин загальної системи керівництва діяльністю компанії, в якій так чи інакше, все зав'язано на виконання роботи для замовників. Завдяки системам управління проектами можливі значні покращення у координації опрацювання внутрішніх процесів, створення необхідних умов та людських ресурсів для успішного планування проектної промисловості.

При реалізації поставлених цілей одним з важливих аспектів є вплив людського фактору. Тобто, в цілому, терміни та якість готового продукту залежать від виконавців та їх комунікації у команді. Часто невдачі стаються через труднощі у розплануванні, неефективному управлінні, недостатньому використанню методології та інструментів.

При створенні системи управління проектами потрібно враховувати своєрідність роботи такого типу. Для цього здійснюється поділ на замовника та виконавця. Особа, бізнес або державна установа, що ставить завдання, вимоги та складає технічне завдання називають замовником. Компанія, що повинна виконати всі вимоги та побажання за встановленими договором називають виконавцем. У цьому випадку це ІТ-фахівці. На початкових етапах співпраці можуть виникати проблеми з встановленням вимог, не чітко сформульованих очікувань та складності з формуванням технічного завдання. Для замовника реалізація ІТ-проекту означає залученість безлічі людей та підрозділів, може включати зміни у структурі підприємства, що однозначно призводить до непорозумінь та конфліктів між працівниками та вищим керівництвом, тим самим викликаючи постійну зміну умов [1].

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Відповідно, відповідальність за кінцевий продукт лежить на обох сторонах, які складали договір, При неефективних комунікаціях, невідповідних умовах взаємодії сторін – часто стаються невдачі.

Аналізуючи призначення системи, було виявлено, що насамперед, потрібно розробити додаток, який матиме можливості створення, редагування, пошуку завдань, отримання детальної інформації про проект, надавати доступ до даних клієнта. Також побажаннями до веб-сайту будуть:

- інтуїтивно зрозумілий інтерфейс користувача;
- зручний інструментарій для управління персоналом;
- зобов'язаний збільшувати ефективність виконання доручень;
- надійність: система має працювати безперебійно;
- ефективність: додатку варто мати мінімальні вимоги до апаратного забезпечення, для використання цього програмного засобу потрібен тільки браузер та доступ в Інтернет;
- адаптивність: безпроблемне використання сайту на різних платформах – комп'ютери, планшети, мобільні пристрої
- легко модифікований (додавання, зміна функціонала).

Для ефективності, зручності та безпеки, буде вводиться система аутентифікації за допомогою облікових записів Active Directory. У будь-який час користувач повинен мати змогу увійти в робочий простір під своїм обліковим записом.

Також у налаштуваннях потрібна можливість заповнити або змінити прізвище, ім'я, фото профілю та іншу основну інформацію, яка буде відображатися у визначених місцях та синхронізуватись з контролерами домену.

Кожен проект має свої терміни початку роботи та дату завершення. Дотримання їх особливо важливе для проектів в ІТ-галузі. Тому в функціоналі обов'язково має бути присутній інструмент для задавання дат виконання тих чи інших доручень, фільтрація задач та проектів за крайніми термінами.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Трекінг часу це одна з доручень менеджерів, які відповідають за роботу працівників над розробкою рішень будь-якої складності. Вона може допомагати у як і працівникам, і керівникам і клієнтам. За допомогою даного інструменту стає можливим швидке складання звітності, правильне виставлення рахунків. Також перевагами для використання інструментів для обліку часу є:

- фокусування на поставленій цілі для працівників (перемикання між різними задачами значно знижує ефективність);
- ефективне управління командою (підбір для конкретної сфери відповідного працівника, виділення часу для навчання)
- мотивування співробітників виконати завдання швидше, не відволікаючись.
- розставлення пріоритетів;
- зберігання даних в одному місці;
- прозора звітність для замовників;
- зниження кінцевої вартості;

Для візуалізації виробничого процесу потрібна віртуальна дошка, яка класифікує роботу на етапи. Застосування канбан-дошок в управлінні ІТ-проектами може допомогти вашій команді збалансувати свої робочі обов'язки та побачити доступні ресурси інших членів команди [2]. Коли деякий виконавець закінчує свою частину, він переміщує карточку на наступну фазу процесу. Це допомагає однозначно бачити прогрес у вирішенні тих чи інших завдань.

1.2 Порівняння існуючих аналогів програмного продукту

На сьогодні, використання систем управління задач стають усе популярнішими, тому кількість таких платформ постійно зростає. Як і великих так і малих проектів.

		<i>В.Загацький</i>			<i>КІК.КР.Б – 123 – 12 – ПЗ</i>	Арк.
		<i>І. Панаріна</i>				
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		12

Багато з них надають можливості організації роботи в компанії, внесення інформації про клієнтів, стеження за прогресом виконання та контролю робочого часу.

Розглянемо декілька з них:

1. Grow CRM – Laravel Project Management [3].

Позитивними якостями є:

- управління клієнтами та проектами (рис. 1.1, рис. 1.2);
- виставлення рахунків і підписок;
- підтримка платіжних систем;
- підтримка багатьох мов інтерфейсу;
- довідки та навчальні статті;
- відстежування робочого часу.

Недоліками є:

- відсутність можливості інтеграції з Active Directory.

ID	Company Name	Account Owner	Projects	Invoices	Tags	Category	Status	Action
20	Bella Shoes & Bags Pvt	Judith	1	\$75.00	seo-marketing	Default	Active	[Icons]
1	Dellon Inc	Jill	1	\$810.00	web-design	Default	Active	[Icons]
8	Enco Power Company	Elleno	0	\$0.00	website-mainten...	Default	Active	[Icons]
6	EverBright Inc	Ken	0	\$1,600.00	product-design	Default	Active	[Icons]
7	Fast Applications Inc	Amy	1	\$490.00	infographic-des...	Default	Active	[Icons]
9	House & Home Co	Jordan	1	\$1,035.00	website-design	Default	Active	[Icons]
11	Jolly Juice Inc	James	1	\$0.00	packaging-design...	Default	Active	[Icons]
2	Malvo Holidays Co	Mike	1	\$2,183.37	web-development	Default	Active	[Icons]
17	Rapid Software Inc	Megan	2	\$1,112.20	logo-design	Default	Active	[Icons]
4	Wholesome Foods Inc	Amanda	1	\$1,741.70	branding-servic...	Default	Active	[Icons]

Рис. 1.1. Сторінка клієнтів Grow CRM

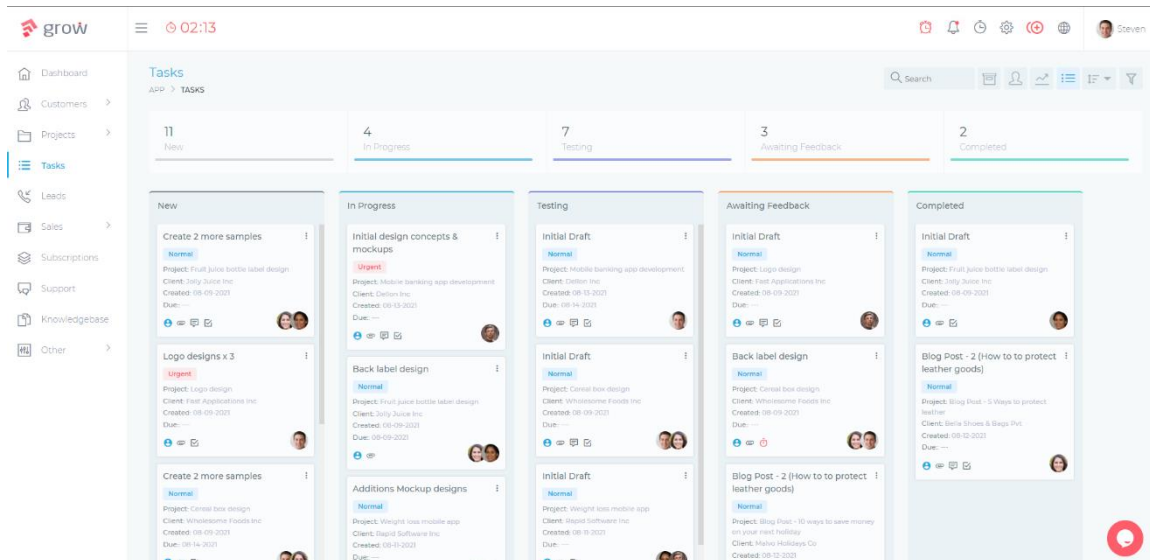


Рис. 1.2. Канбан-дошка Grow CRM

2. Perfex – Powerful Open Source CRM [4].

Головними позитивними якостями є:

- вбудований календар;
- аналітика витраченого часу на завдання (рис. 1.3);
- підтримка обліку витрат (рис. 1.4);
- управління завданнями та проектами;
- повноцінний портал для клієнтів;
- вбудовані опитування для клієнтів.

Недоліками є:

- досить давно не оновлюється розробником

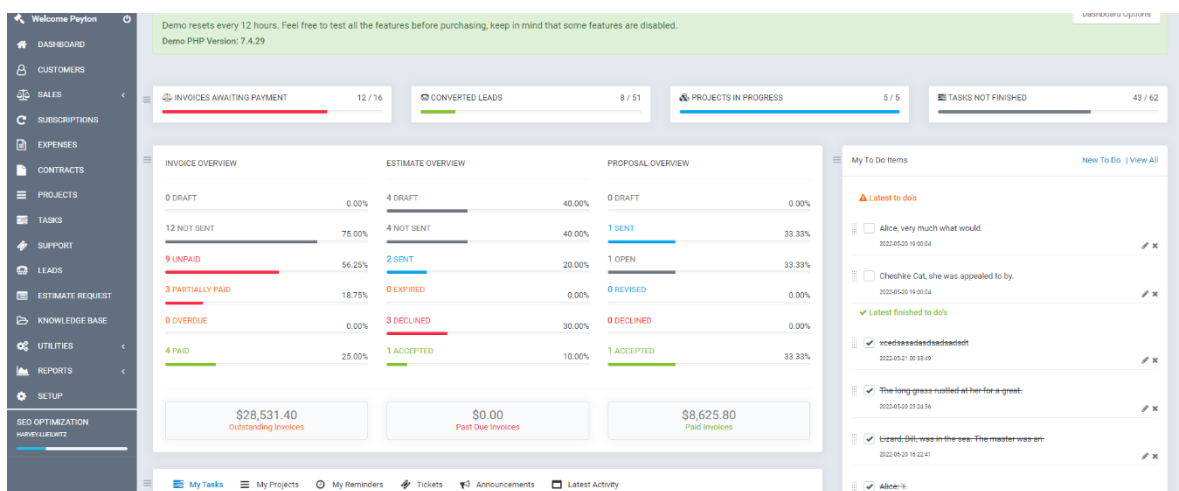


Рис. 1.3. Вигляд основної аналітики Perfex

		В.Загацький							Арк.
		І. Панаріна							
Змн.	Арк.	№ докум.	Підпис	Дата					14

КІК.КР.Б – 123 – 12 – ПЗ

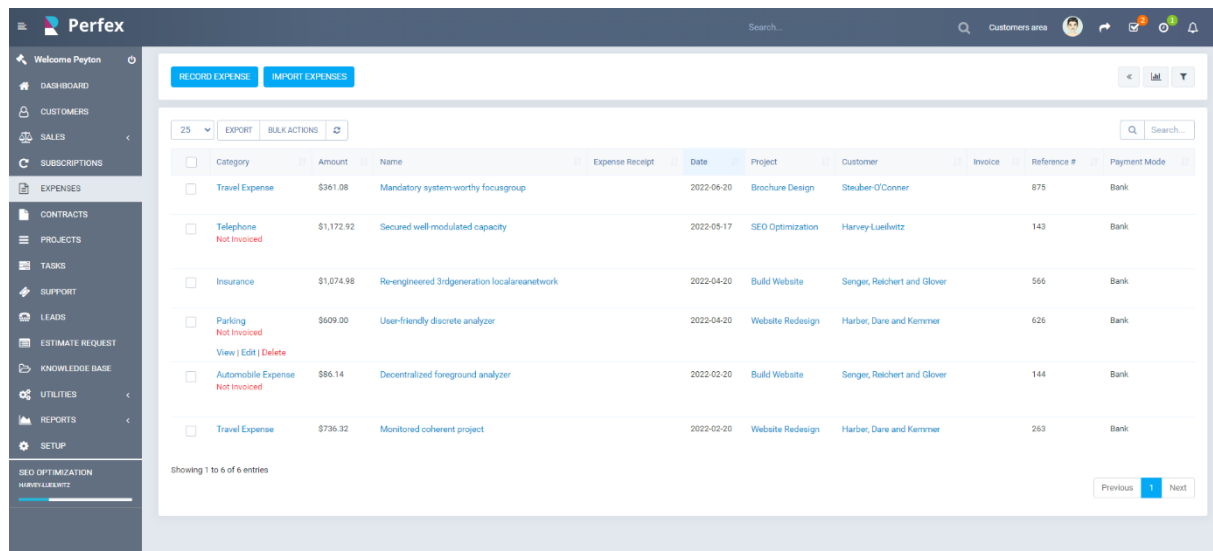


Рис. 1.4. Функції для відслідковування поточних витрат Perfex

3. Ekushey Project Manager CRM [5].

Головними позитивними якостями є:

- працівники можуть управляти назначеними проектами (рис. 1.5);
- система прогресу й обговорення проекту (рис 1.6);
- внутрішні повідомлення.

Недоліками є:

- досить застарілий інтерфейс;
- відсутність канбан-дошок.

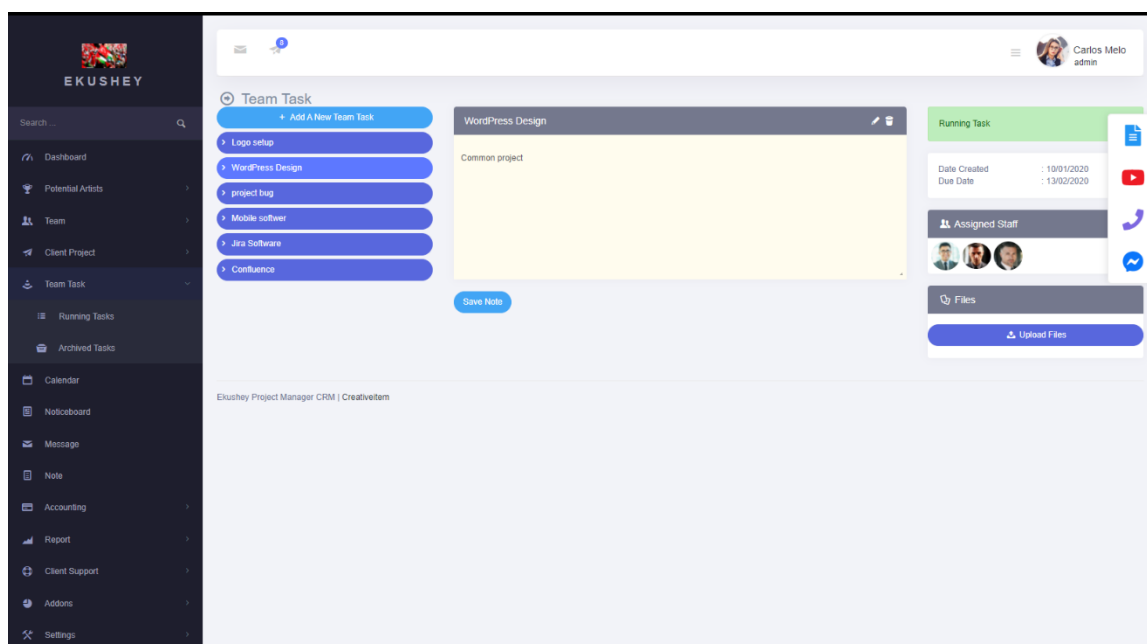


Рис. 1.5. Інтерфейс додатку Ekushey Project Manager CRM

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		15

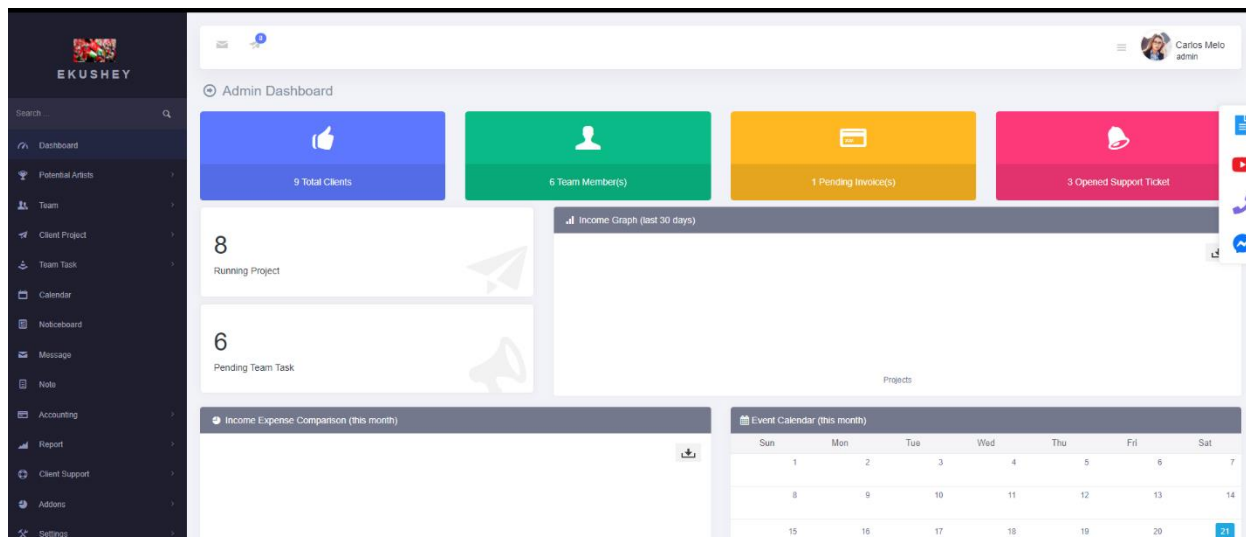


Рис. 1.6. Головна сторінка Ekushey Project Manager CRM

В таблиці 1.1 проведено порівняння вище наведених аналогів.

Таблиця 1.1

Порівняння існуючих аналогів

Назва		Grow CRM	Powerful Open Source CRM	Ekushey Project Manager CRM
Управління	Задачами	+	+	+
	Проектами	+	+	+
	Клієнтами	+	+	+
Канбан-дошка		+	+	—
Можливість інтеграції з Active Directory		—	Плагіни	—
Інтерфейс	Адаптивність	+	+	±
	Дизайн	+	±	—
	Продуманість	+	+	—
Швидкодія		+	+	±

1.3. Обґрунтування вибору інструментальних засобів та архітектури системи

Під час створення програмного продукту фігуруватиме серверна мова програмування PHP, розробка повинна проходити дотримуючись об'єктно-орієнтованого підходу та використовуючи патерн MVC (рис. 1.7) – розділення, й на три окремі частини: модель (дані додатку), представлення (користувацький інтерфейс) і контролер (управляюча логіка), з можливістю незалежної модифікації кожного сегменту.

CodeIgniter4 – PHP MVC фреймворк, яке використовується для швидкої розробки веб-додатків. CodeIgniter надає готові бібліотеки для підключення до бази даних та виконання різних операцій, таких як надсилання електронних листів, завантаження файлів, керування сесіями тощо [6].

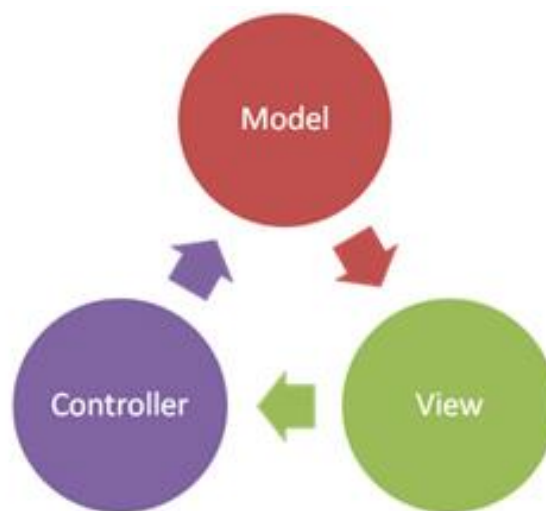


Рис. 1.7. Архітектурний патерн MVC

За зберігання основних даних відповідатиме реляційна система управління базами даних MySQL. Одним із ліцензувань являється безкоштовним програмним забезпеченням з відкритим кодом. Використовує SQL для виконання створення, модифікації та управління інформацією в базах даних.

Для співпраці з Active Directory будемо застосовувати протокол LDAP (Lightweight Directory Access Protocol). Це відкритий протокол, який вміє зберігати та отримувати дані від сервера каталогів ієрархічної структури.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Зазвичай зберігають імена користувачів, паролі, адреси електронної пошти, підключення до принтерів та інші статичну інформацію у даних каталогах (рис. 1.8).

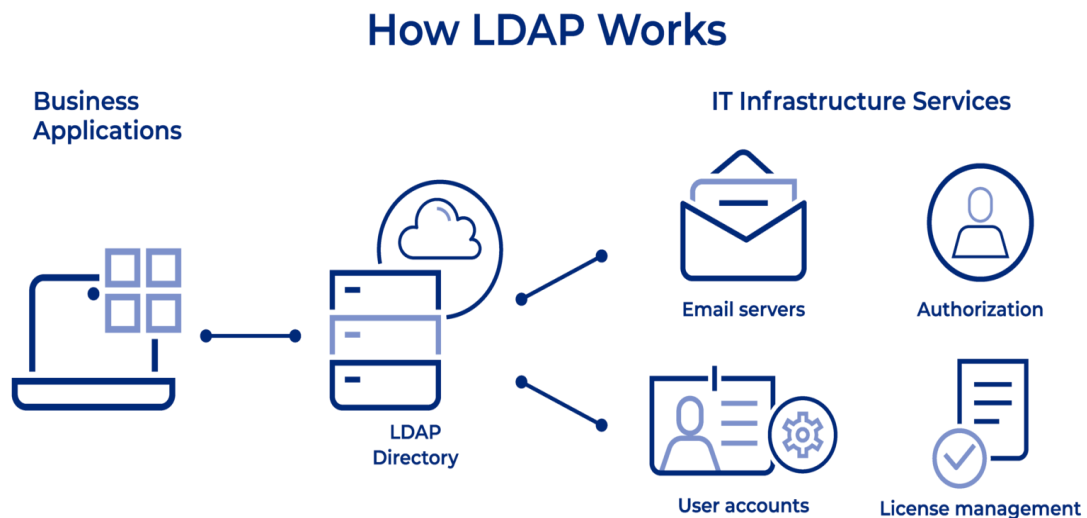


Рис. 1.8. Як працює LDAP

Створення графічних елементів здійснюватиметься за допомогою Bootstrap - безкоштовного набору інструментів з відкритим кодом, призначених для створення веб-сайтів та веб-додатків, які містять шаблони CSS та HTML для типографіки, форм, кнопок, навігації та інших компонентів інтерфейсу, а також додаткові розширення JavaScript [7]. Він спрощує розроблення динамічних веб-сайтів і веб-додатків. Докладніше про бібліотеку можна ознайомитися на сайті розробника.

1.4. Застосування міжмережевих екранів для підвищення рівня захисту мережі

Мережа Internet є одним із найбільш зручних способів комунікації. Водночас вона містить досить велику кількість проблем з безпекою. Нелегальний доступ до інформації, викрадення даних, порушення у роботі локальних мереж, це все вже давно стало серйозними загрозами для бізнесу, діяльності компаній та державних структур. Потенційними об'єктами

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		18

зловмисників можуть стати сервери, персональні станції або будь-які інший пристрій, що має зв'язок з мережею Інтернет.

За підвищення рівнів безпеки при підключенні до глобальних мереж використовують наступні спеціалізовані засоби:

- міжмережеві екрани;
- системи запобігання вторгненням;
- сканери безпеки (пошук вразливих ділянок мережі);
- сніфери, аналізаторів протоколів (аналіз вхідних, вихідних пакетів);
- засоби протоколювання та аудиту подій;
- засоби VPN (Virtual Private Network) та закриті канали обміну даними.

Міжмережевий екран – це система захисту, що відстежує вхідний і вихідний трафік, таким чином розділивши кожную мережу на дві. За допомогою встановлених наборів правил безпеки, брандмауер вирішує дозволяти чи забороняти пересилання пакетів з даними.

Завдяки відповідним рішенням для мереж компанії, стає доступним отримати досить високий рівень захисту й отримати можливості з:

- фільтрації усіх потоків інформації;
- приховання структури та компонентів локальних мереж від клієнтів з глобальної мережі;
- фільтрації на базі MAC або IP-адрес;
- забезпечення авторизації маршрутизатора та маршрутів, тунелі для маршрутів, шифрування даних;
- фільтрації запитів на транспортному рівні для встановлення віртуальних з'єднань.

Але потрібно враховувати, що нині більшість атак та способів заволодіння даними здійснюється зсередини ЛКМ. Відповідно, необхідно мати засоби від несанкціонованого доступу як для захисту точок з боку Інтернету, так і для серверів, окремих комп'ютерів (наприклад адміністратора або керівників), що знаходяться у локальній мережі компанії.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		19

Zone-Based Policy Firewall (ZPF) – міжмережевий екран для маршрутизаторів (версії Cisco IOS 12.4+), що встановлює правила перетину пакетів між ділянками мережі. Своєю реалізацією мав на увазі заміну технологій Access Control List (списки доступу) та Context-Based Access Control (динамічна інспекція трафіку) (СВАС). Обидва набори правил конфігурувались кожному інтерфейсі, відповідно створюючи проблеми для ефективності та масштабованості налаштувань [8].

Zone Based Firewall змінює конфігурацію міжмережевого екрана від інтерфейсної на більш гнучку та зручнішу у налаштуванні конфігурацію на базі зон (рис. 1.9). Вони встановлюють межі безпеки, тобто вказують кордон, де трафіку, що його перетинає, дозволено чи заборонено проходження обмежуючими політиками.

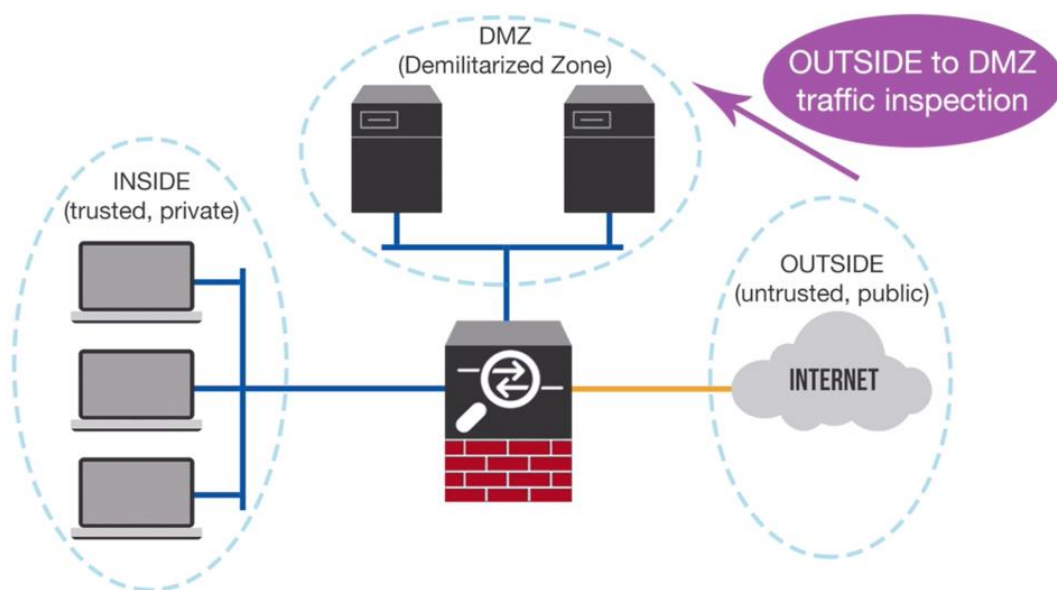


Рис. 1.9. Приклад визначення зон

Базові етапи конфігурації ZPF:

- 1) Сконфігурувати зони (zone);
- 2) Присвоїти зони для інтерфейсів;
- 3) Визначити пари зон (zone-pair);
- 4) Налаштувати карти класів (class-map), які вказують пакети, до якого застосовується політика при проходженні пари зон;

- 5) Встановити карти політик (policy-map) – дії до трафіку карт класів;
- 6) Задіяти карти політик до пар зон

Брандмауер може приймати наступні рішення щодо трафіку – відкинути (DROP), пропустити (PASS) або перевірити (INSPECT). Відкидання (DROP) застосовується до будь-якого стандартного трафіку. Йому забороняють проходження без повідомлення про відкидання для вузла-ініціатора. Пропускання (PASS) – при успішному проходженні даних з зони “А” до “Б”, то навпаки, з “Б” до “А”, трафік буде заборонено. Тобто, “PASS” відпрацьовує в одному напрямку (дозволи проходження в інший потрібно проводити відповідну конфігурацію) [8].

Перевірка (inspect) – трафік перевіряється на підставі стану. Брандмауер записує у пам’ять дані підключення та сеанс для запиту. Наприклад, при проходженні трафіку з “А” до “Б”, автоматично надається дозвіл на зворотний трафік з “Б” зони у відповідь на запити зони “А”.

Висновки до першого розділу

У результаті досліджень, проведених у першому розділі було охарактеризовано головні особливості майбутнього веб-додатку для управління завданнями та захисту мережі для ресурсів компанії. Відповідно, зазначено який функціонал повинен мати додаток, основний шаблон для інтерфейсу та як робочі станції користувачів будуть взаємодіяти з системою.

Було обрано архітектури та фреймворки для створення системи: мову програмування PHP, фреймворк CodeInteger4; реляційну базу даних MySQL; службу каталогів Active Directory. Проведено дослідження аналогів, виявлено основні можливості та недоліки наявних систем.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		21

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТА РОЗРОБКА СИСТЕМИ УПРАВЛІННЯ ЗАВДАННЯМИ ТА ДОСТУПОМ ДО РЕСУРСІВ КОМПАНІЇ НА БАЗІ РІШЕНЬ MICROSOFT ТА CISCO

2.1. Визначення варіантів використання, структури системи та функціональних алгоритмів

Проаналізувавши завдачу отримаємо блок-схему використання системи управління завданнями (рис. 2.1).

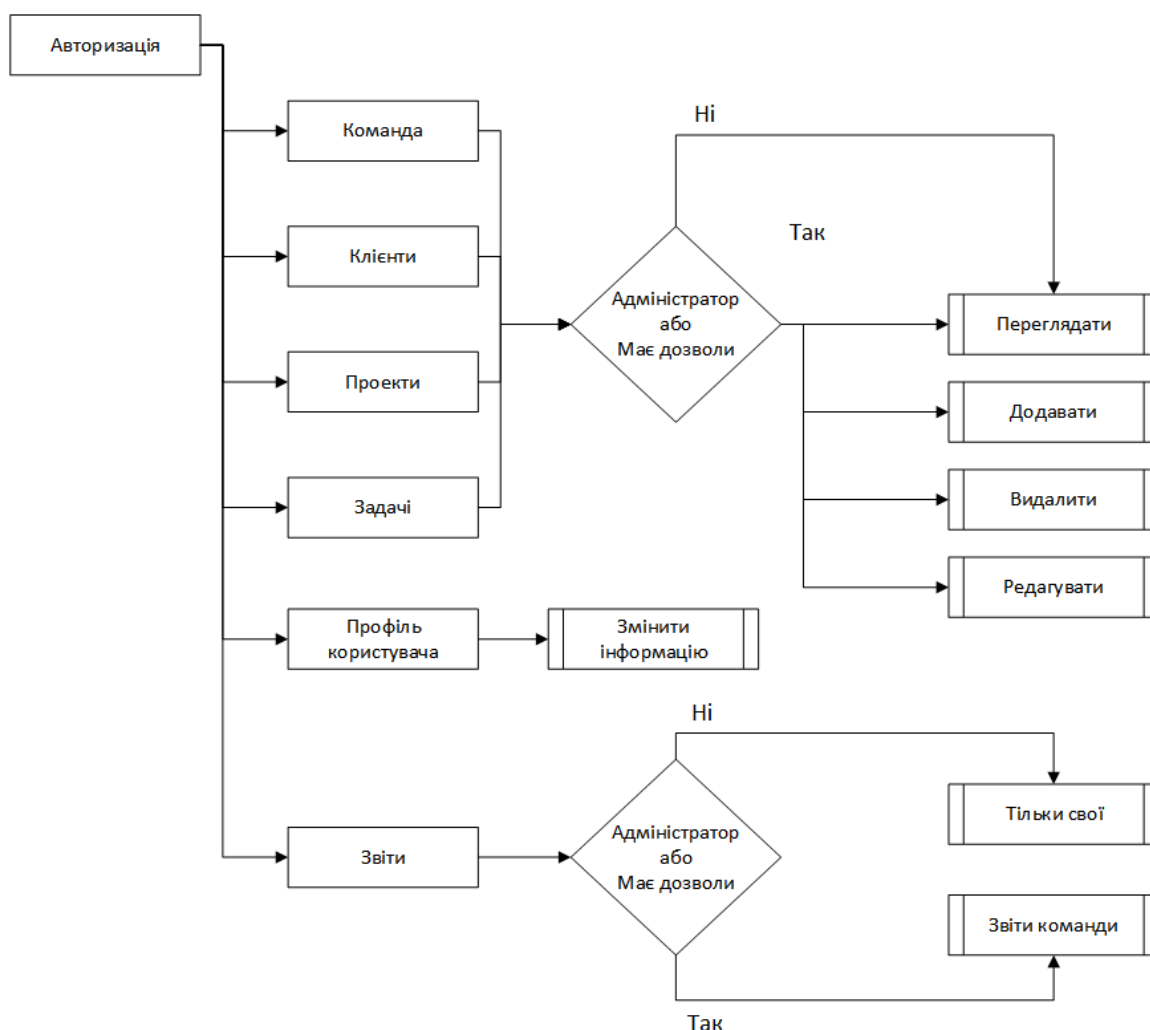


Рис. 2.1. Блок-схема взаємодії з веб-сайтом

Початком алгоритму буде завантаження сторінки автентифікації до системи, від якої користувач зможе здійснити перехід до свого профілю або звітів з використання робочого часу, або ж переглядати завдання, призначені для нього. Адміністратору або користувачу, якому надано відповідні дозволи,

може додатково створювати, редагувати, видаляти записи з вказаними типами даних.

Після погодження загального алгоритму роботи, можна переходити до проектування підпрограм. У результаті отримаємо алгоритми, які більш детально описують роботу деяких функцій веб-додатку.

Під час запуску сайту одразу викликається контролер за замовчуванням із головною сторінкою веб-сайту. На головній сторінці знаходяться основні показники, такі як відпрацьовані години, останні зміни в завданнях, нові подробиці проектів.

Якщо користувач ще не авторизувався, йому пропонується увійти або зареєструватись. Алгоритм входу до системи або реєстрації користувача зображений на рисунку 2.2.

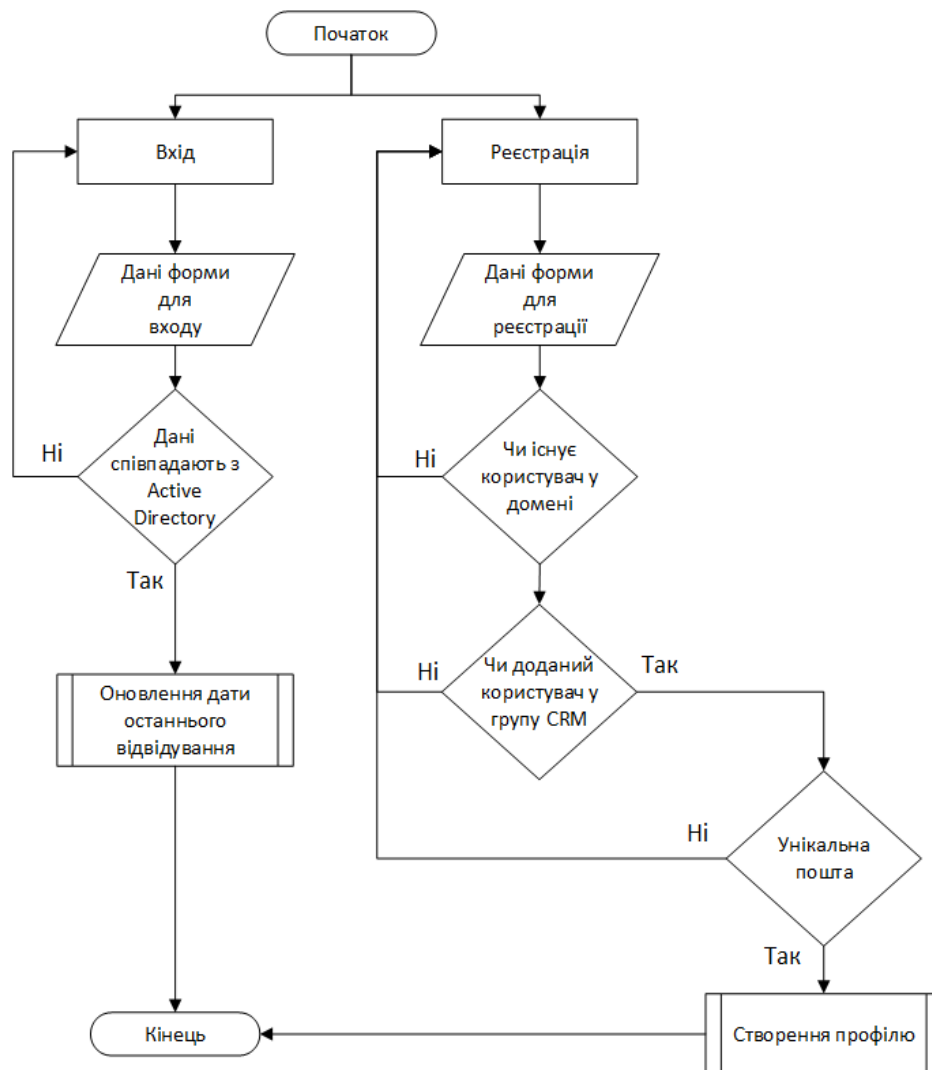


Рис. 2.2. Блок-схема алгоритму входу або реєстрації користувача

У разі переходу до розділу створення нового клієнта система повинна вивести усі чинні записи. Далі дані, які надав користувач, перевіряються на вимоги. Після перевірок, в базі даних створюються відповідні записи (рис. 2.3).

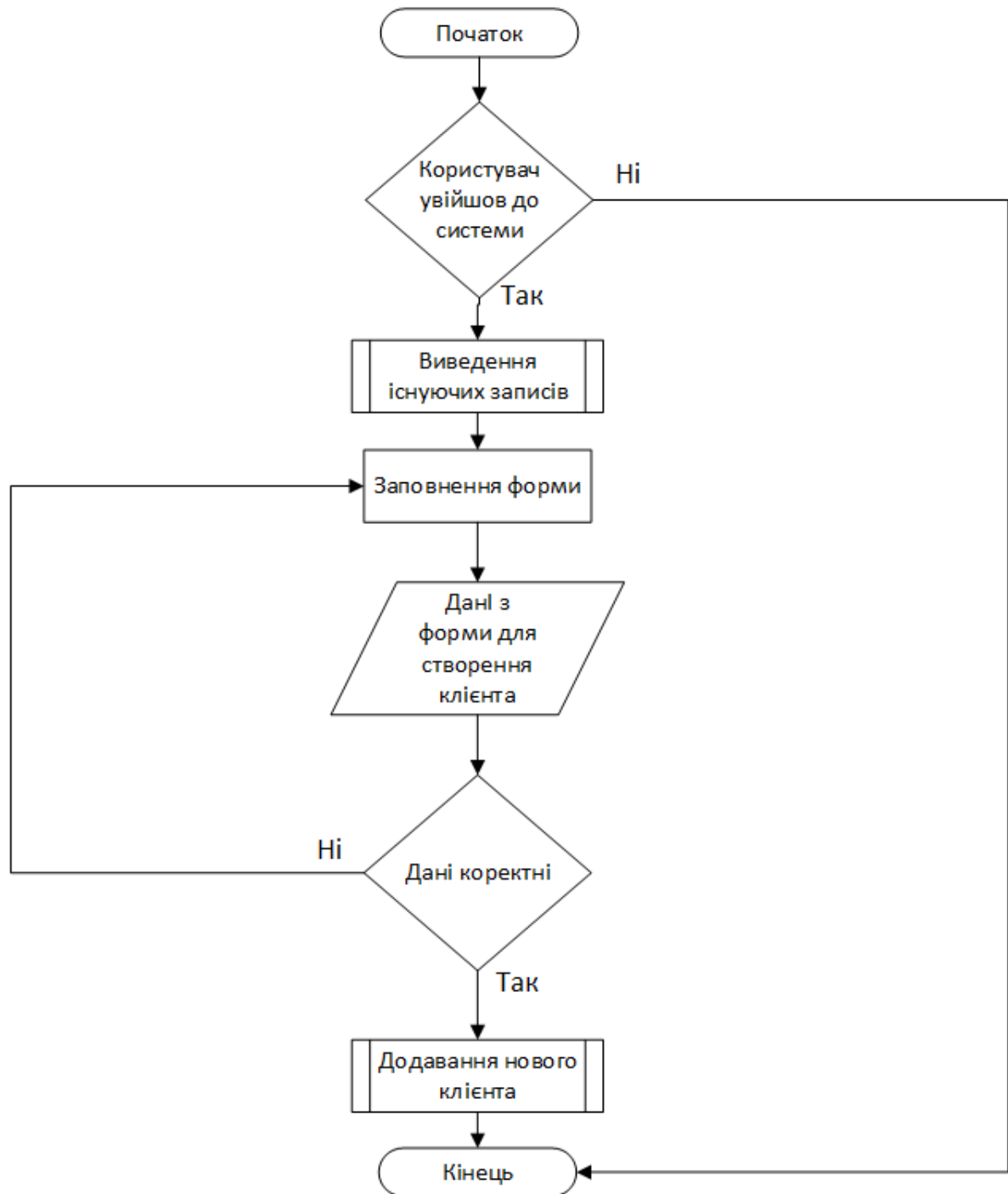


Рис. 2.3. Блок-схема роботи розділу створення запису клієнта

Для створення задачі повинно виконуватись декілька умов (рис. 2.4):

- вказана назва задачі;
- створені відповідні проекти, для яких ставиться завдання;

- встановити відповідального за виконання;
- встановити статус завдання;
- встановити дати початку та крайнього строку (необов'язково).

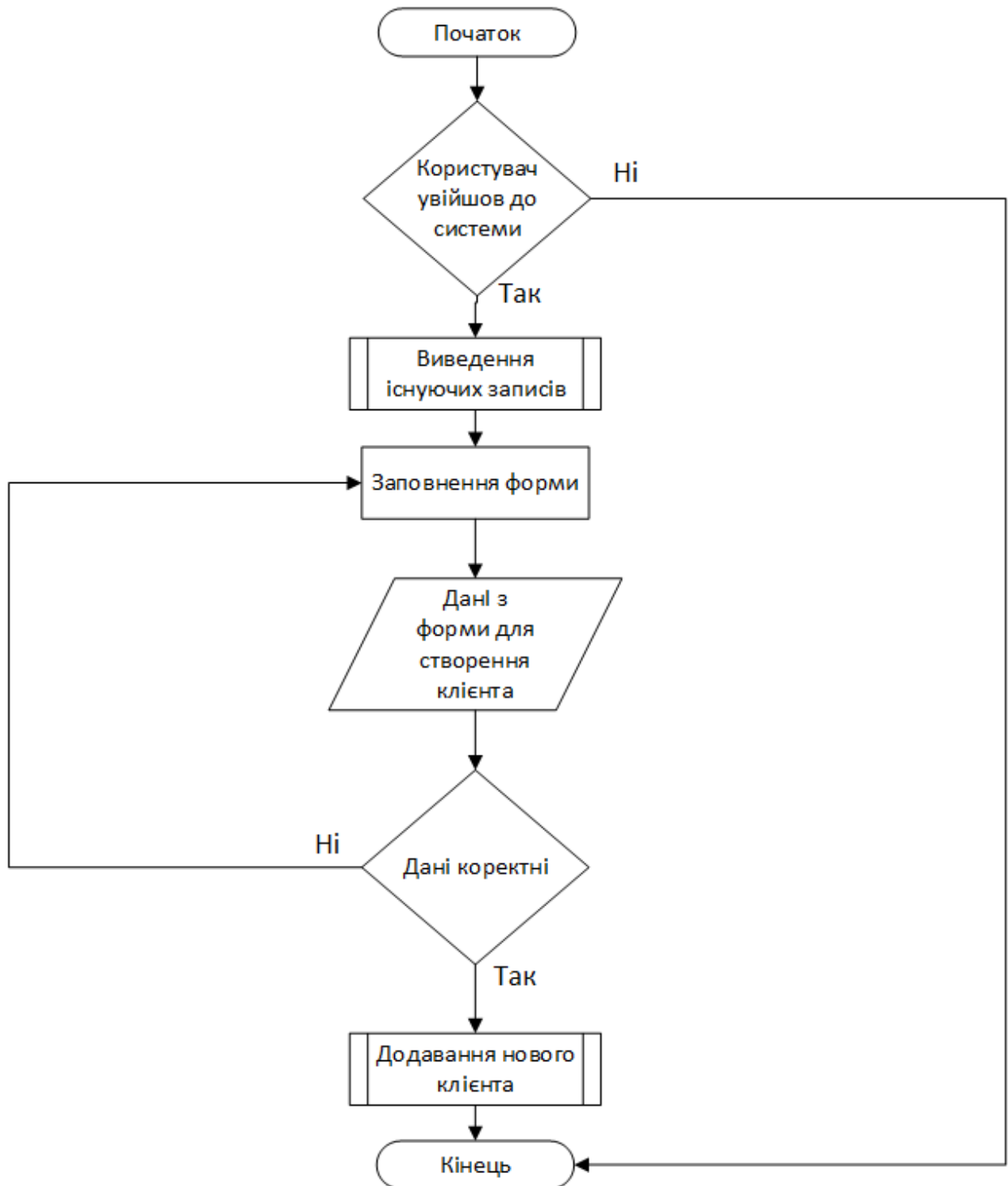


Рис. 2.4. Блок-схема роботи розділу створення запису клієнта

2.2. Розробка бази даних системи

Для зберігання інформації будемо використовувати реляційні бази даних. Дані містяться у таблицях, при цьому кожен рядок має унікальний ідентифікатор (первинний ключ), а таблиці пов'язані між собою зовнішніми ключами (рис. 2.5).

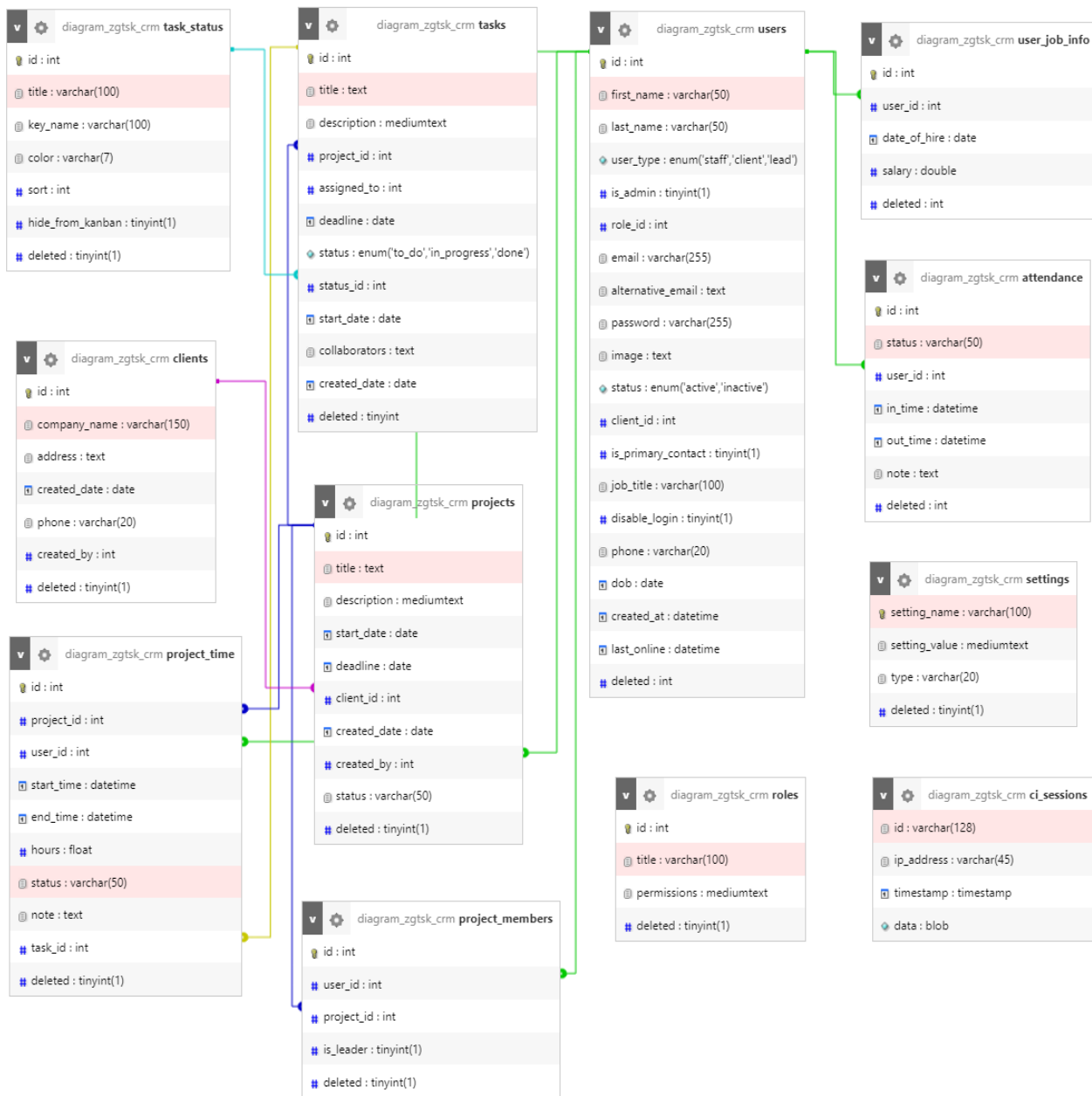


Рис. 2.5. Схема базы данных

Нижче приведено основні таблиці бази даних, їх опис та за які функції вони відповідатимуть.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				26
Змн.	Арк.	№ докум.	Підпис	Дата		

Опис таблиць бази даних

Назва	Опис
attendance	Зведення про робочий час
ci_sessions	Дані про сесії користувачів
clients	Збереження інформації про клієнтів
projects	Збереження інформації про проекти
project_members	Учасники проекту
roles	Ролі для працівників
settings	Налаштування системи
tasks	Збереження інформації про завдання
task_status	Статуси завдань (в т. ч. створені користувачем)
users	Інформація про працівників
user_job_info	Інформація про опис роботи користувача

Таблиця Clients містить довідку про клієнтів – назву компанії, адресу, коли та ким створено.

Таблиця Project відповідає за збереження: назви, дати початку та дедлайну, ідентифікатор клієнта та ким створено. Project_Members зберігає інформацію про учасників проекту та відповідального за нього.

Таблиця Tasks містить поля ідентифікатора назви, опису, відповідального працівника, статус, дату початку та бажаного кінця роботи над завданням, список учасників.

Одна із найбільших таблиць – Users. В ній зберігаються ім'я, прізвище працівника, тип користувача, основну та альтернативну електронну адресу, пароль, статус, назву посади, телефон, дату створення облікового запису.

Roles зберігає у собі надані дозволи для конкретного працівника та назву ролі. Setting відповідає за налаштування системи (домен AD, іконку, вибір мови за замовчуванням і т. п.).

2.3. Реалізація додатку управління завданнями та доступом до ресурсів компанії

Основним прийомом для розроблення веб-додатку буде слідування патерну MVC, у якому розділена бізнес-логіка від інтерфейсу користувача. Роутінгом, сесіями, роботою конфігурацій буде займатись фреймворк CodeIgniter4. Одним із перших взаємодіятиме контролер для аутентифікації працівника. Спочатку викликається метод для ініціалізації, далі в залежності від заданого шляху виводиться на сторінку форма або відбувається автентифікація користувача.

```
class Signin extends App_Controller
{
    private $signin_validation_errors;

    function __construct()
    {
        parent::__construct();
        $this->signin_validation_errors = array();
        helper('email');
    }
    function index()
    {
        if ($this->Users_model->login_user_id()) {
            app_redirect('dashboard/view');
        } else {

            $view_data["redirect"] = "";
            if (isset($_REQUEST["redirect"])) {
                $view_data["redirect"] = $_REQUEST["redirect"];
            }
            $view_data["domain"] = config('Ldap')->domain;
            return $this->template->view('signin/index',
$view_data);
        }
    }
    function authenticate()
    {
        $validation = $this->validate_submitted_data(array(
            "email" => "required",
            "password" => "required"
        ), true);

        $email = $this->request->getPost("email");
        $password = $this->request->getPost("password");
```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		28

```

        if (!$email) {
            app_redirect('signin');
        }
        if (is_array($validation)) {
            $this->signin_validation_errors = $validation;
        }
        if ($this->signin_validation_errors) {
            $this->session-
>setFlashdata("signin_validation_errors",                $this-
>signin_validation_errors);
            app_redirect('signin');
        }
        $auth = $this->Users_model->authenticate($email,
$password);
        if (!$auth || isset($auth['error_dc'])) {
            if (isset($auth['error_dc']) && $auth['error_dc']) {
                array_push($this->signin_validation_errors,
app_lang("domain_controller_error_login"));
            } else {
                array_push($this->signin_validation_errors,
app_lang("authentication_failed"));
            }
            $this->session-
>setFlashdata("signin_validation_errors",                $this-
>signin_validation_errors);
            app_redirect('signin');
        }
        $redirect = $this->request->getPost("redirect");
        if ($redirect) {
            return redirect()->to($redirect);
        } else {
            app_redirect('dashboard/view');
        }
    }
    function sign_out()
    {
        $this->Users_model->sign_out();
    }
}

```

Для реалізації синхронізації з користувачами Active Directory, встановленому на Windows Server буде використовуватись протокол LDAP.

LDAP-система зберігає інформацію схоже чином на базу даних, але для цього використовує атрибути (пара ключ-значення). Будь-яка конкретна частина інформації пов'язані з описовим атрибутом. Аутентифікація LDAP включає перевірку наданих імен користувачів та паролів шляхом підключення

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		29

до служби каталогів, що використовує протокол LDAP (наприклад сервери каталогів Microsoft Active Directory, OpenLDAP та OpenIdentityPlatform) [9].

Запит LDAP - це команда, яка запитує у служби каталогів певну інформацію. Наприклад, якщо ви хочете побачити, до яких груп входить конкретний користувач, потрібно надіслати запит, який виглядає так:

```
(&(objectClass=user)(sAMAccountName=yourUserName)(memberof=CN=YourGroup,OU=Users,DC=YourDomain,DC=com))
```

Подана частина лістинга нижче демонструє взаємодію за допомогою даної моделі LDAP з контролером домену:

```
class Ldap_model extends Model
{
    private function connect($username = '', $password = '') {
        if (!$username) {
            $username = $this->ldap_username;
        }
        if (!$password) {
            $password = $this->ldap_password;
        }
        $this->connection = ldap_connect($this->uri, $this->port);
        ldap_set_option($this->connection,
LDAP_OPT_NETWORK_TIMEOUT, 2);
        ldap_set_option($this->connection,      LDAP_OPT_TIMELIMIT,
2);

        if (@ldap_bind($this->connection, $username, $password)) {
            $this->test = $username;
            ldap_set_option($this->connection,
LDAP_OPT_PROTOCOL_VERSION, 3);
            ldap_set_option($this->connection,
LDAP_OPT_REFERRALS, 0);
            $this->active = true;
        } else {
            $this->active = false;
        }
    }
    public function bind($username, $password) {
        if (!strpos($username, $this->domain) && strpos($username,
'@') == false) { $username .= '@' . $this->domain; }
        if (@ldap_bind($this->connection, $username, $password)) {
            $this->currentUserInfo($username);
            return true;
        }
        return false;
    }
}
```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		30

```

private function getAdUserInfo($username) {

    $search_filter =
    "(&(objectCategory=person)(samaccountname=$username))";

    ldap_bind($this->connection, $this->ldap_username, $this->ldap_password);
    return $this->get_entries($search_filter)[0];

}

public function search($filter) {
    ldap_bind($this->connection, $this->ldap_username, $this->ldap_password);
    return ldap_search($this->connection, $this->dn, $filter);
}

public function get_entries($filter) {
    return ldap_get_entries($this->connection, $this->search($filter));
}

public function updateUserInfo($user_id, $user_data) {
    $user_model = new Users_model();
    $username = $user_model->get_details(['id' => $user_id])->getResult('array')[0]['ad_login'];
    $user_info = $this->getAdUserInfo($username);
    $dn = $user_info['dn'];

    $entry['givenName'] = $user_data['first_name'];
    $entry['sn'] = $user_data['last_name'];
    $entry['displayName'] = "{$user_data['first_name']} {$user_data['last_name']}";
    if ($user_data['phone']) {
        $entry['telephoneNumber'][0] = $user_data['phone'];
    }
    if ($user_data['address']) {
        $entry['mail'] = $user_data['address'];
    }
    if (!@ldap_modify($this->connection, $dn, $entry)) {
        return false;
    }
    $new_dn = "cn={$entry['displayName']}";
    $new_parent = explode(',', $dn);
    unset($new_parent[0]);
    $new_parent = implode(',', $new_parent);
    if (!@ldap_rename($this->connection, $dn, $new_dn, $new_parent, true)) {
        return false;
    }
    return false;
}
}

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		31

2.4. Розробка топології комп'ютерної мережі та проекту підсистеми мережного екранування трафіку

Спроектована мережа складає собою три зони:

- INTERNET;
- WEST;
- EAST.

Спроектована мережа представлена на рисунку 2.6:

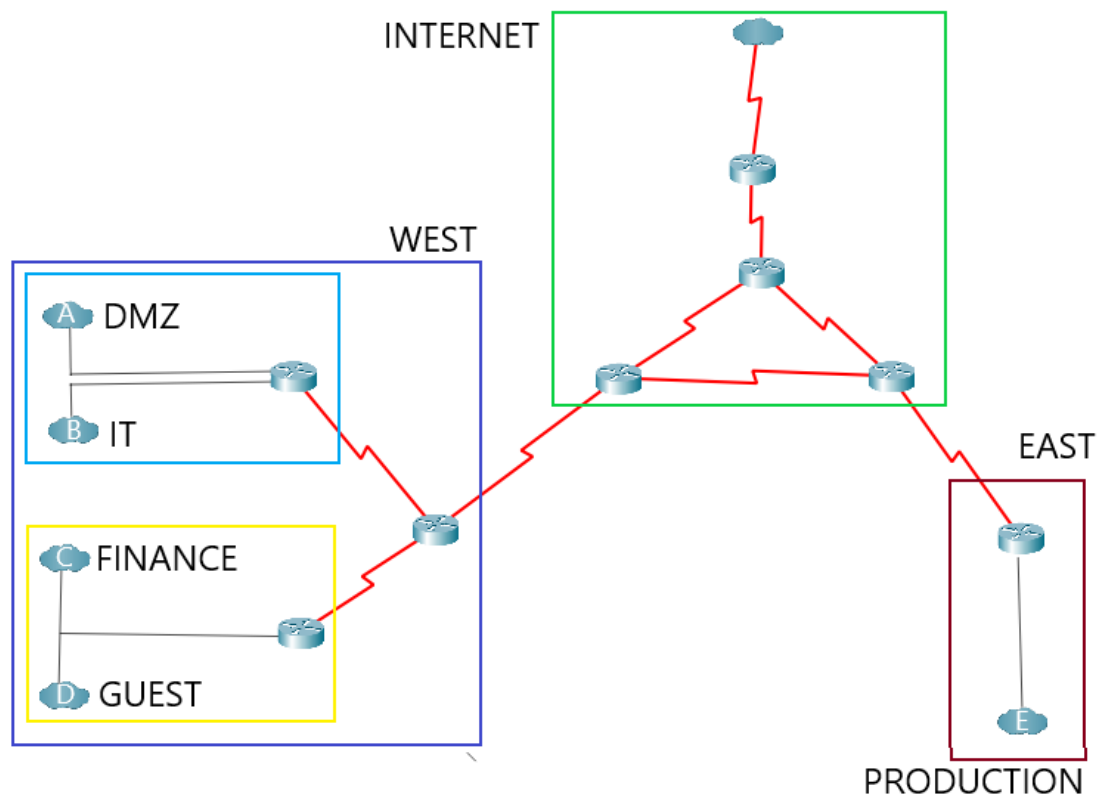


Рис. 2.6. Загальна топологія мережі та розподілення зон

Частини мережі EAST та WEST з'єднуються між собою через глобальну мережу INTERNET. Західна частина являє собою досить велику підмережу організації в якій містяться декілька відділів з працівниками, зона для відвідувачів та сегмент мережі, що містить загальнодоступні сервіси для працівників компанії.

Східна частина це відокремлений офіс, який повинен мати доступ до DMZ-зони для роботи з системою компанії. Зі західної сторони повинен доставлятися трафік для централізованого адміністрування мережі.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Мережа складається з 5 підмереж. Розглянемо детальніше кожен з них. Схеми підмереж А, В зображено на рисунку 2.7.

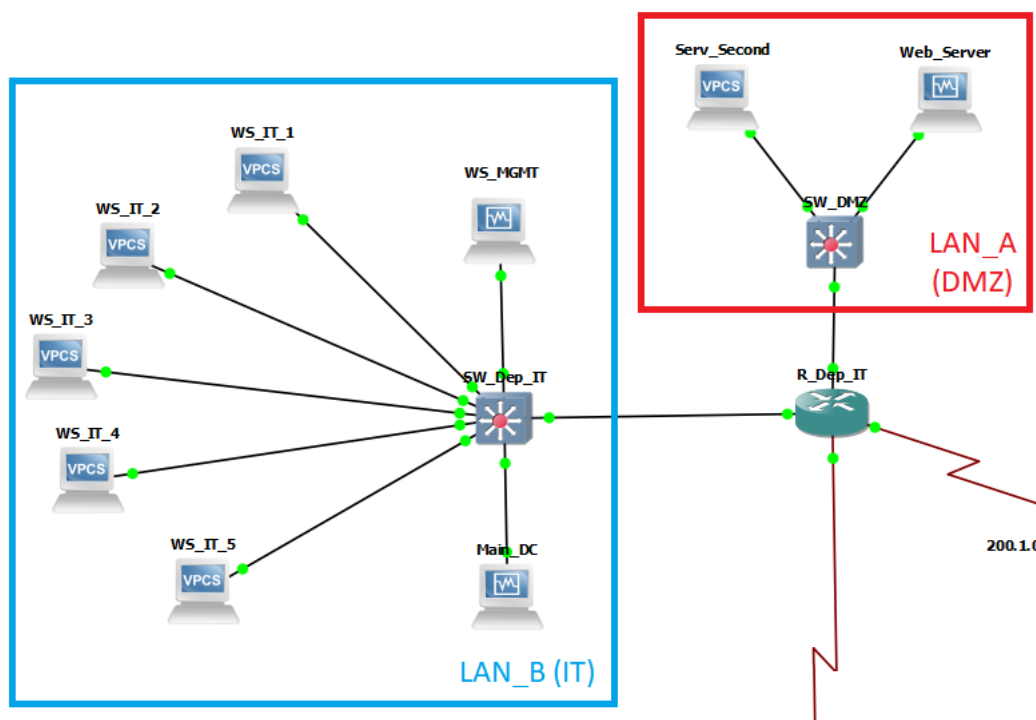


Рис. 2.7. Підмережі А та В

Підмережа А відіграє роль серверної зони, яка надає для усіх працівників доступ до інформаційних ресурсів та забезпечує роботу компанії. Сервери повинні підтримувати веб-протоколи та надавати доступ до системи управління завданням. Підмережа В це відділ ІТ, має можливість роботи з серверами та з глобальною мережею Інтернет. Відповідно, доступ від мережі А до В обмежений веб-трафіком. Від DMZ та ІТ до зони INTERNET трафік не має заборон для основних протоколів. Від глобальної мережі до інформаційних ресурсів повинні мати доступ усі працівники компанії.

Підмережі С, D (рис. 2.8) являють собою простір іншого відділу компанії, мають у своєму складі два комутатори, до яких підключені робочі станції працівників та гостей. Від зони FINANCE повинен бути зв'язок з глобальними мережами, трафік не обмежується. Для користувачів-гостей, які за замовчуванням є не довіреними, встановлено правила, які забороняють будь-який трафік до LAN_C та дозволяють проводити операції тільки за

допомогою протоколів HTTPS, HTTP, DNS до мережі Інтернет. Протокол маршрутизації – OSFP. Призначення адрес – динамічне.

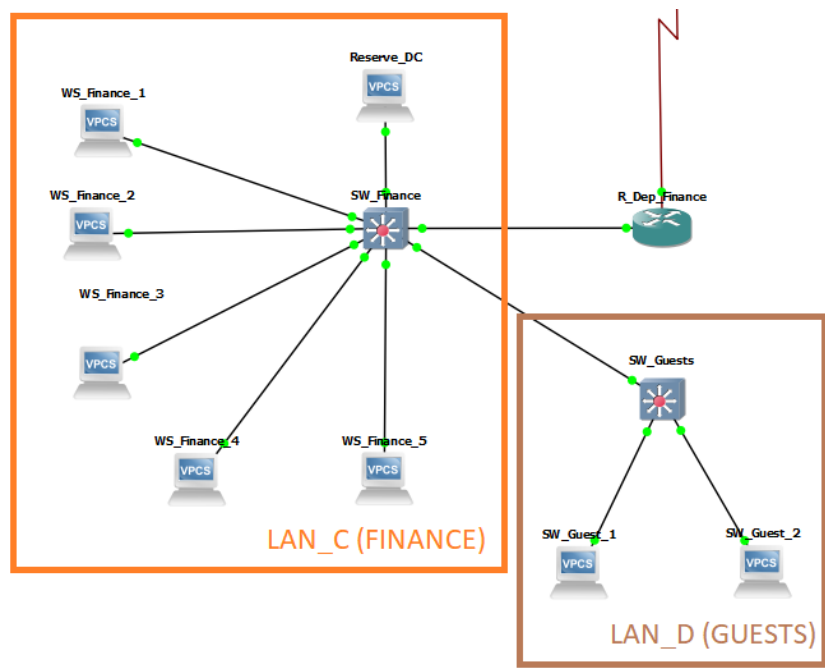


Рис. 2.8. Підмережі C та D

Іншу ділянку корпоративної мережі складатиме підмережа E (рис. 2.9) – відділ Production, який повинен мати вільний доступ до інтернету та до зони DMZ частини мережі EAST. Аби забезпечити максимальну безпеку та цілісність зв’язку налаштовано Site-to-Site VPN [10]. Це забезпечить шифрування даних, що передаються. Відповідно із зворотної сторони повинні проходити та інспектуватись дані від мережевих адміністраторів.

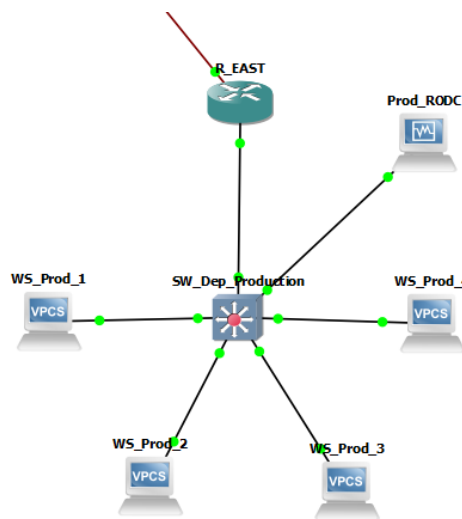


Рис. 2.9. Підмережа E

Таблиця 2.1

Матриця доступу

Вхід \ Вихід	LAN_A	LAN_B	LAN_C	LAN_D	LAN_E	MGMT	LAN_S	INTER NET
LAN_A (DMZ)		—	—	—	—	—	+	+
LAN_B (IT)	1		—	—	—	—	+	+
LAN_C (Finance)	1	—		—	—	—	+	+
LAN_D (Guest)	—	—	—		—	—	—	+
LAN_E (Production)	1	—	—	—		—	+	+
MGMT	+	+	+	+	+		+	+
LAN_S	+	+	+	—	+	+		+
INTERNET	1	—	—	—	—	—	—	

*1 – тільки обмежений трафік (протоколи HTTP, HTTPS, DNS)

*2 – тільки обмежений трафік (протоколи LDAP/S, HTTP, HTTPS, ICMP, DNS)

Висновки до другого розділу

Відповідно до вимог, описаних у першому розділі було створено блок-схеми взаємодії з додатком та деякі алгоритми, за яким він повинен працювати.

Також розроблено базу даних, яка відповідає вимогам, щодо зберігання даних клієнтів, завдань, проектів тощо. Було наведено програмну реалізацію деяких компонентів системи.

Розроблено топологію комп'ютерної мережі, визначено зони, вимоги до них та взаємодію між собою.

РОЗДІЛ 3. РОЗГОРТАННЯ СТРУКТУРИ ТА ПОРЯДОК РОБОТИ З СИСТЕМОЮ УПРАВЛІННЯ ЗАВДАННЯМИ ТА ДОСТУПОМ ДО РЕСУРСІВ КОМПАНІЇ НА БАЗІ РІШЕНЬ MICROSOFT ТА CISCO

3.1. Розгортання структури Active Directory та налагодження обладнання мережі

Active Directory допоможе спростити роботу як адміністраторам, так і працівникам, забезпечуючи комфорт (єдиний вхід до систем) та підвищуючи безпеку ресурсів. Всі користувачі, комп'ютери, принтери управляються з одного центру відповідно до групових політик [11].

Для нашого проекту було вибрано редакція Windows Server 2019 Standard (Desktop Experience) (рис. 3.1) з графічним інтерфейсом для швидшого та зручного налаштування.

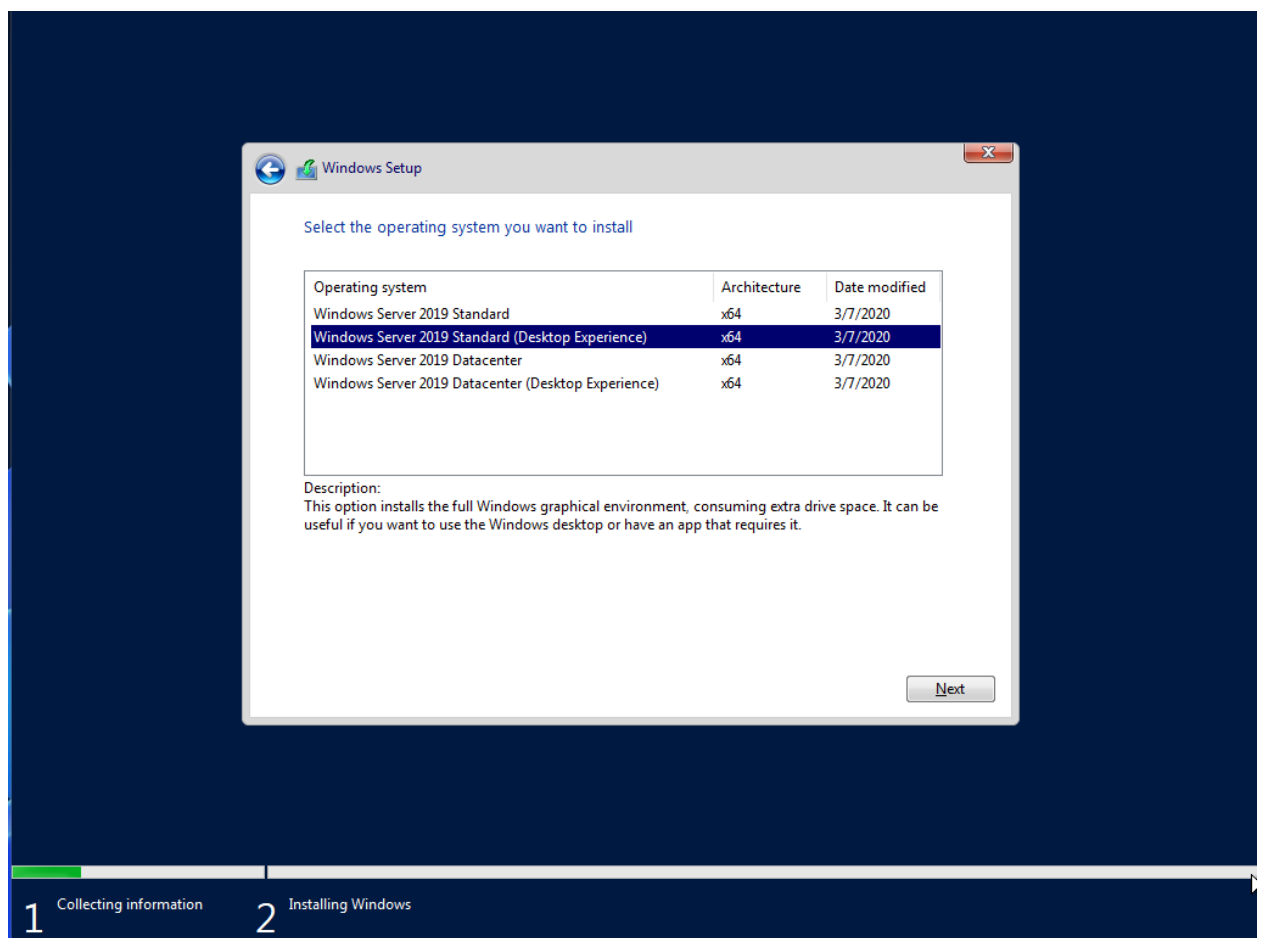


Рис. 3.1. Вибір версії Windows Server

На кроці вибору серверних ролей (рис. 3.2) нам потрібні:

- AD Domain Services - основні функції Active Directory, які керують користувачами та комп'ютерами та дозволяють системним адміністраторам організовувати дані в логічні ієрархії. AD DS забезпечує сертифікати безпеки, єдиний вхід (SSO), LDAP та керування правами.;
- DHCP Server – відповідає за видачу IP-адрес робочим станціям;
- DNS Server – використовується для виявлення контролерів домену або інших вказаних ресурсів за доменним іменем;
- Print and Document Services – для централізованого управління принтерами

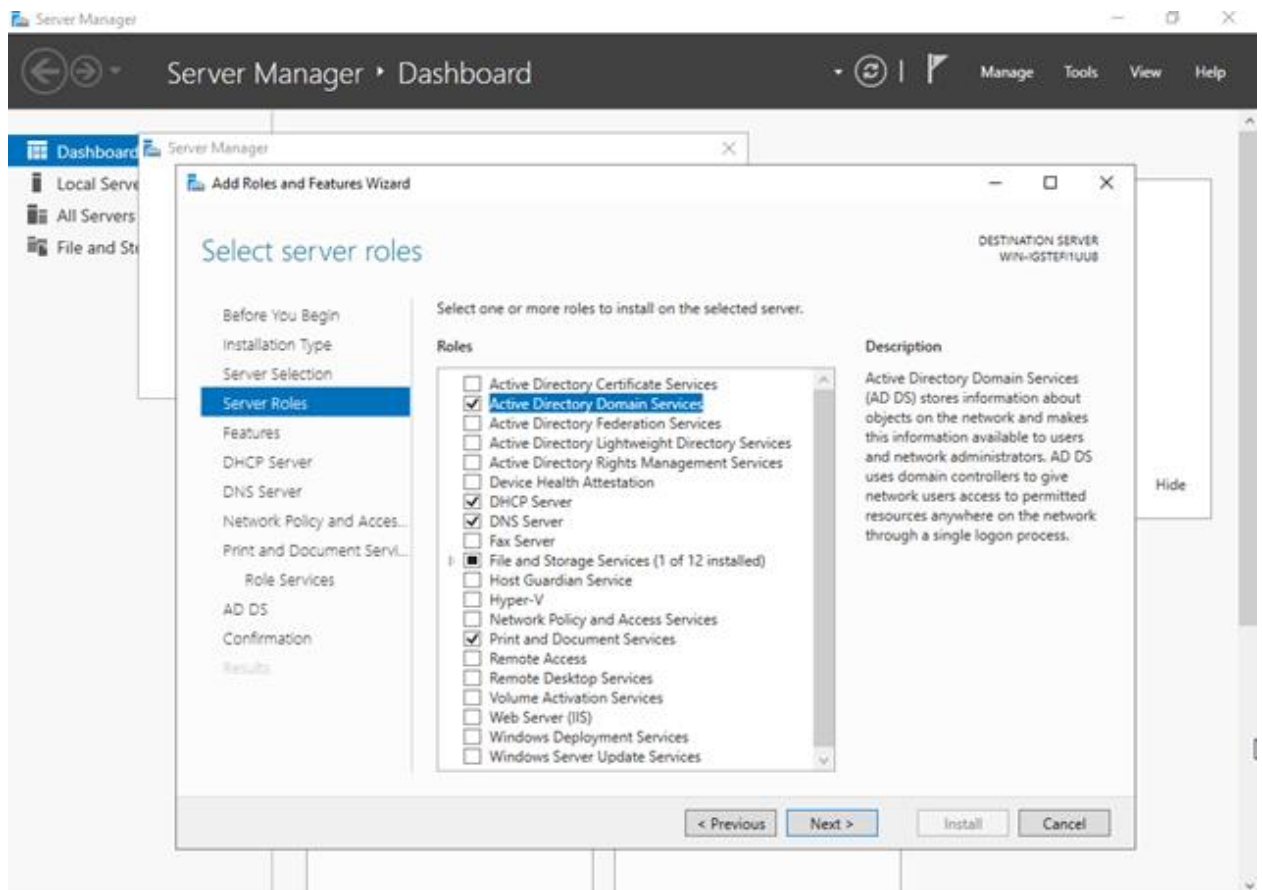


Рис. 3.2. Встановлення серверних ролей

Так як це основний контролер домену, нам потрібно створити новий «ліс» з доменним ім'ям «zgtsk.com» (рис. 3.3).

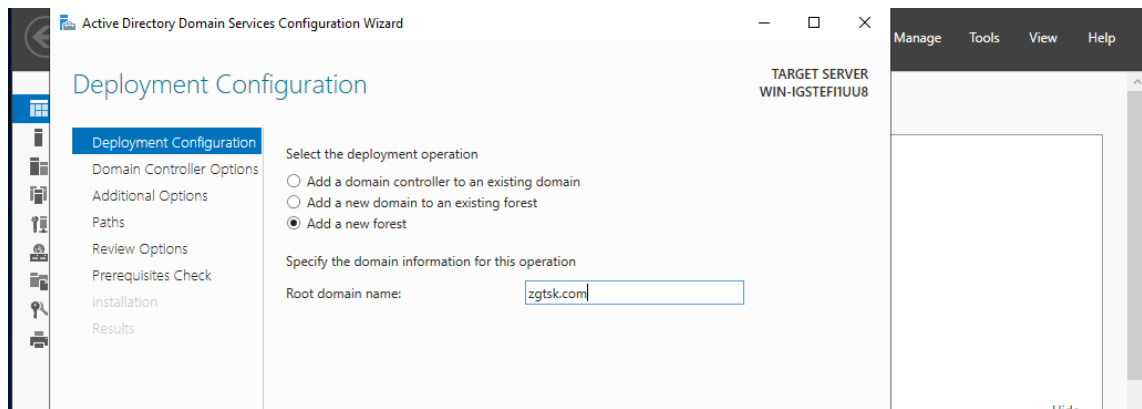


Рис. 3.3. Встановлення серверних ролей

Далі за допомогою AD Users and Computers (рис. 3.4), створимо окремі організаційні одиниці (OU) для користувачів та комп'ютерів домену.

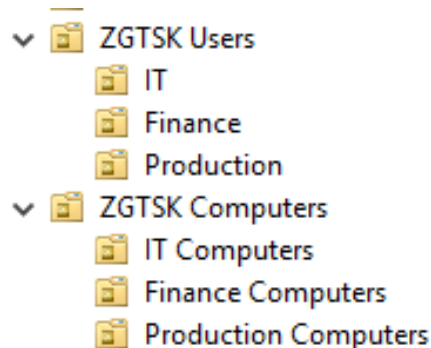


Рис. 3.4. Створення організаційних одиниць

Наступним кроком стане зображене на рисунку 3.5 налаштування RODC (read-only domain controller) для віддаленого офісу “Production”, який має доступ тільки на читання даних групи “Production Users”.

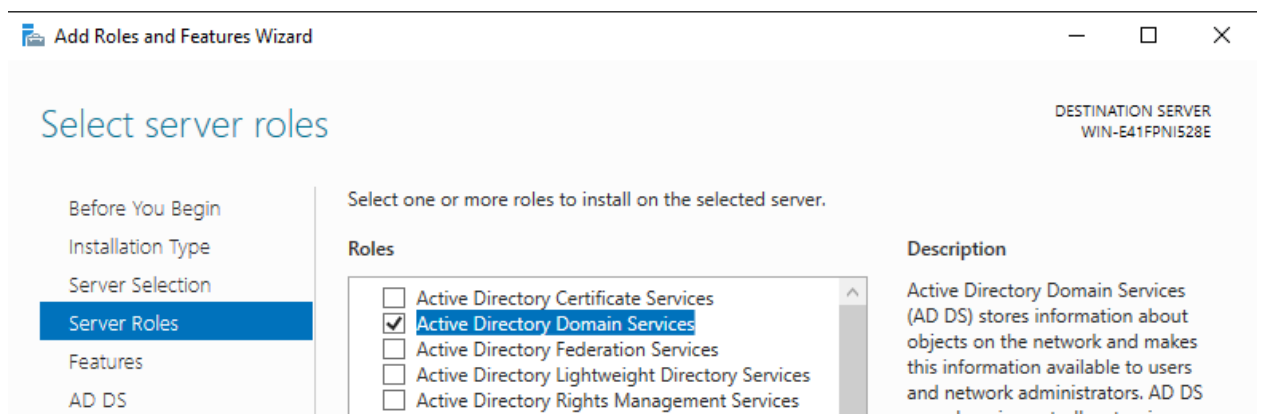


Рис. 3.5. Встановлення серверних ролей (RODC)

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Додаємо новий сервер до існуючого домену, вказуючи доменне ім'я «zgtsk.com» (рис. 3.6).

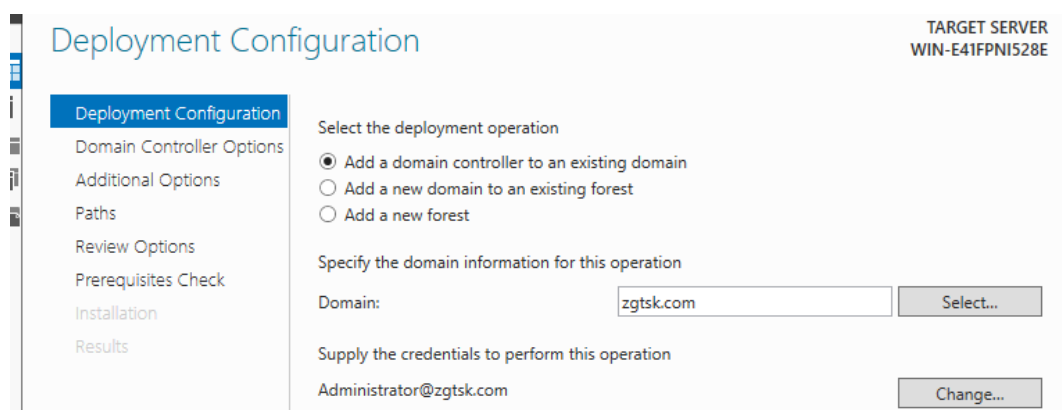


Рис. 3.6. Додавання контролеру у існуючий домен

На етапі вибору опцій контролеру відмічаємо RODC, DNS, GC налаштування (рис. 3.7).

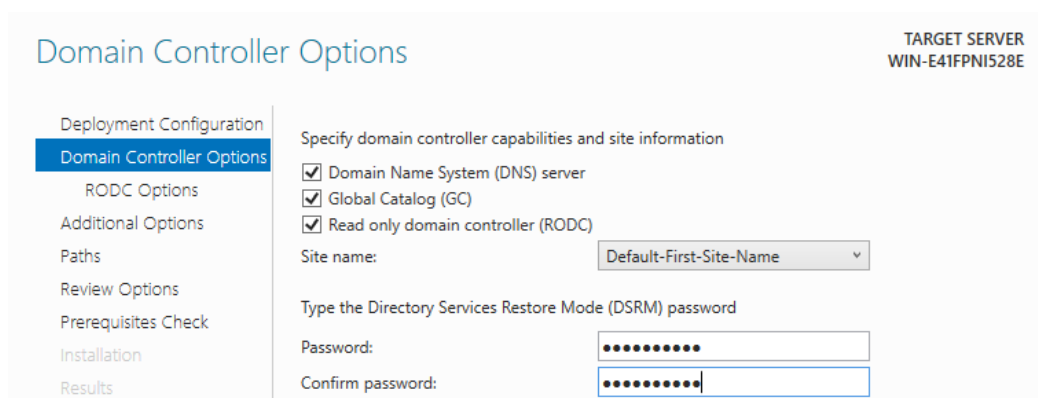


Рис. 3.7. Додавання контролеру у існуючий домен

Додаємо групу «Production Users» до списку реплікацій (рис. 3.8) та обираємо опцію реплікації з будь-якого домену (рис. 3.9).

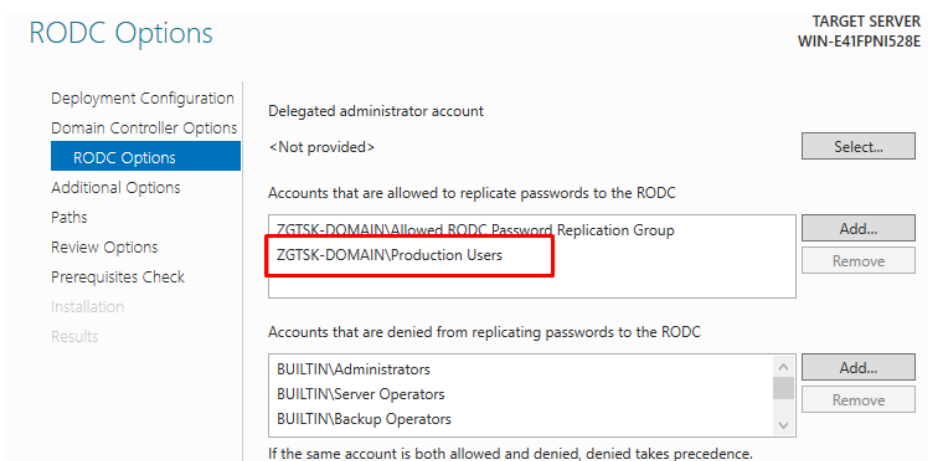


Рис. 3.8. Вибір груп для реплікування

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		39

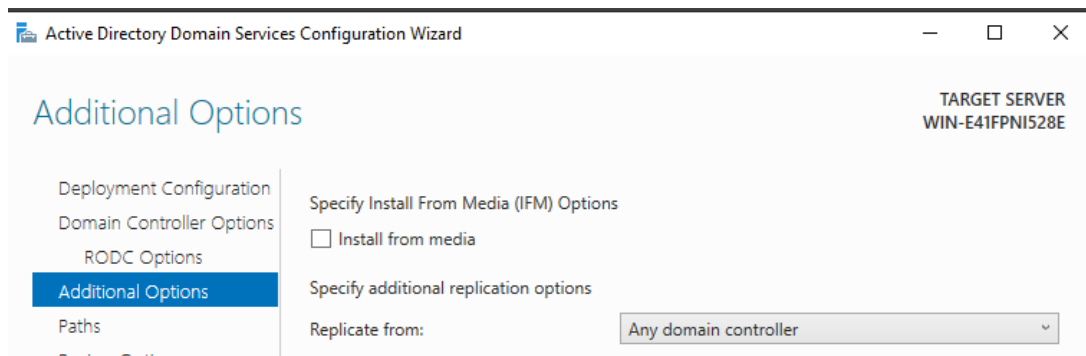


Рис. 3.9. Вибір контролера для реплікації

Відповідно до схеми мережі наведеної у додатку А, сервери знаходяться у різних частинах глобальної мережі. Відповідно, потрібно налаштувати сайти (рис. 3.10) та міжсайтові зв'язки (рис. 3.11), завдяки яким реплікація буде виконуватись періодично та з стисненням трафіку

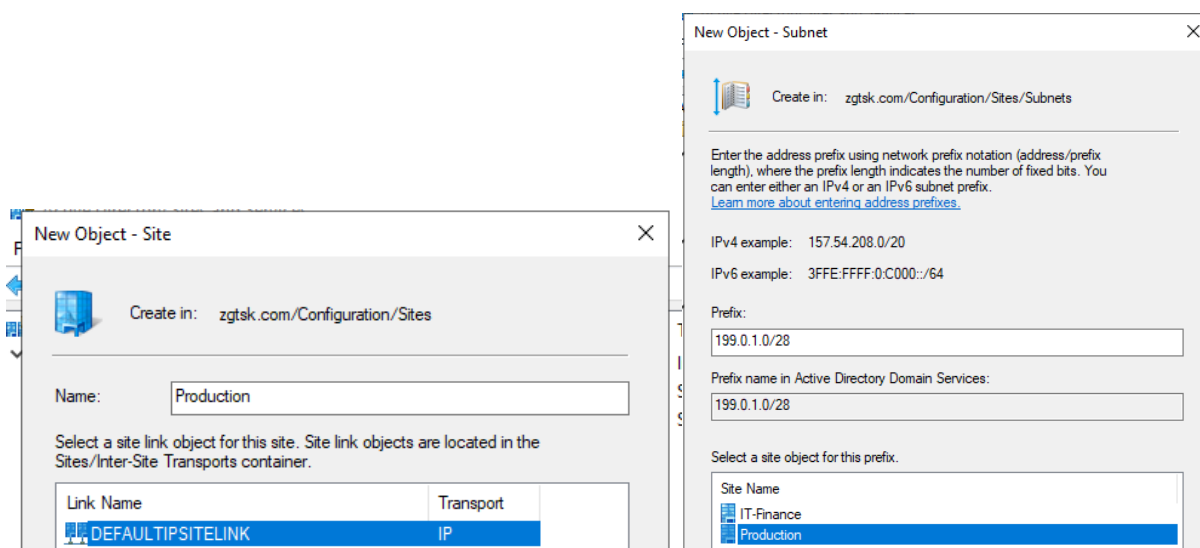


Рис. 3.10. Створення сайту та додавання підмережі

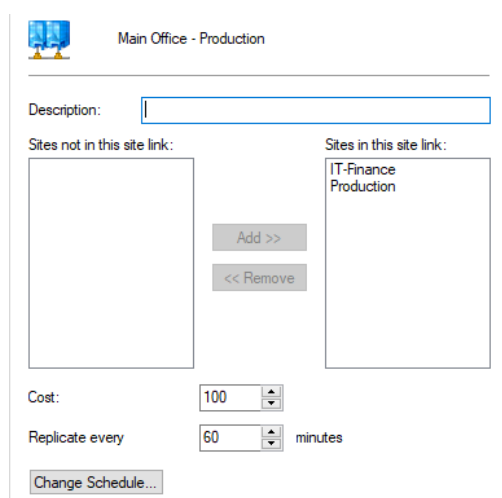


Рис. 3.11. Створення міжсайтового зв'язку

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		40

Після цього перевіряємо на правильність конфігурації (рис. 3.12).

```
PS C:\Users\Administrator> repadmin /replsum
Replication Summary Start Time: 2022-05-27 00:12:54

Beginning data collection for replication summary, this may take awhile:
.....

Source DSA          largest delta    fails/total %%   error
WIN-IGSTEF11UU8      :04s           0 / 5  0

Destination DSA     largest delta    fails/total %%   error
WIN-E41FPNI528E      :04s           0 / 5  0
```

Рис. 3.12. Успішна реплікація

Також для робочих станцій проведемо налагодження DHCP-серверу для динамічної видачі IP-адрес (рис. 3.13).

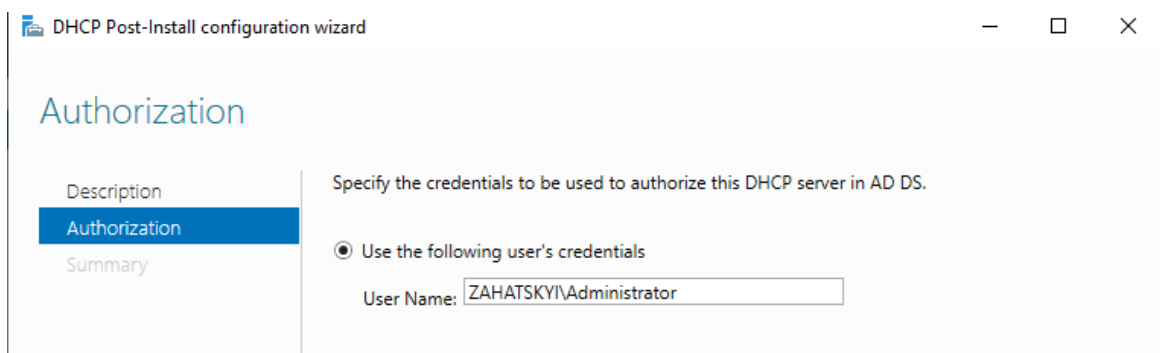


Рис. 3.13. Метод авторизації доступу до DHCP-серверу

Створюємо області (рис. 3.14) для кожної з підмереж (адресація підмереж наведена у додатку Б.

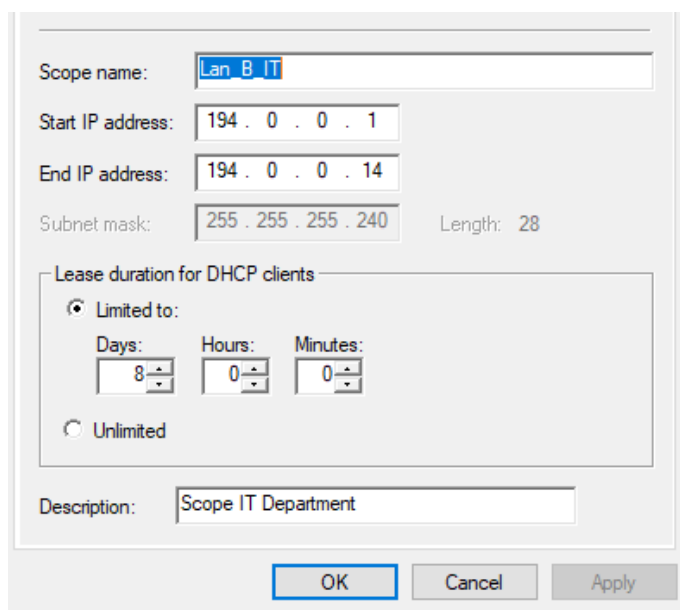


Рис. 3.14. Налаштування області

Вмикаємо робочу станцію та перевіряємо існуючі записи оренди адрес (рис. 3.15).

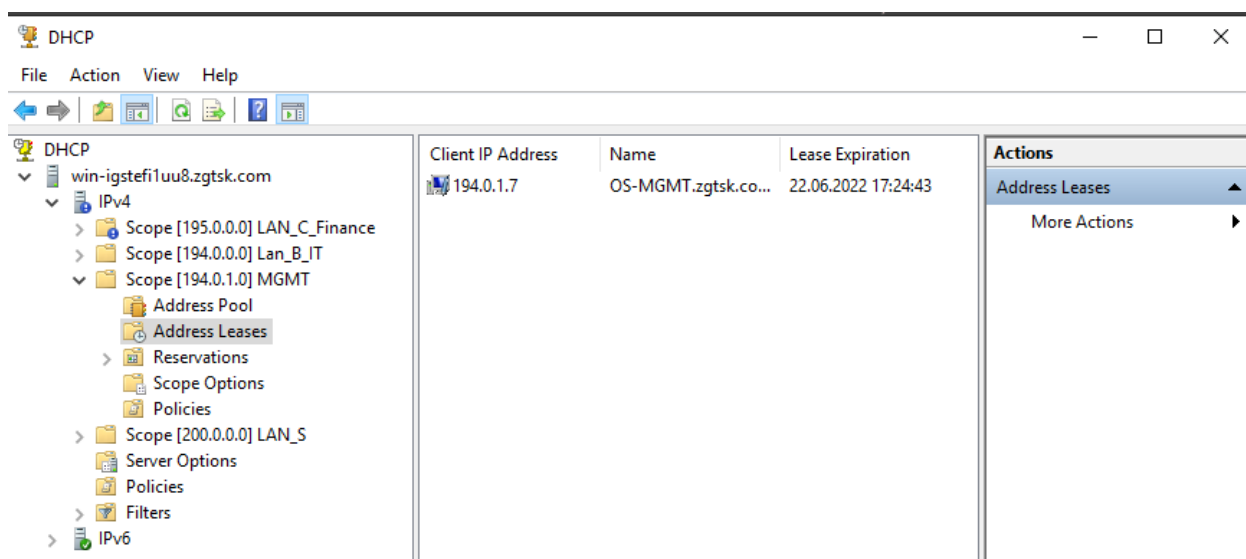


Рис. 3.15. Успішне налаштування DHCP

Одночасно налаштуваннями Active Directory налаштовуємо мережу компанії. Для комутаторів створюємо VLAN, налаштовуємо інтерфейси, підключаємо віддалене управління через SSH, вмикаємо протокол Syslog.

Для маршрутизаторів, які знаходяться на рівні доступу, налаштовуємо Inter-Vlan Routing, протоколи маршрутизації, підключаємо SSH та Syslog. Для прикладу наведемо деякі команди, виконані на маршрутизаторі R_Dep_IT (лістинги конфігурацій інших маршрутизаторів наведені у додатках):

```
R_Dep_IT(config)#hostname R_Dep_IT
R_Dep_IT(config)#int e0/1.101
R_Dep_IT(config-subif)#encapsulation dot1q 101
R_Dep_IT(config-subif)#desc LAN_Server
R_Dep_IT(config-subif)#ip add 200.1.2.14 255.255.255.240
R_Dep_IT(config-subif)# ip helper-address 200.0.0.1
R_Dep_IT(config)#int s2/0
R_Dep_IT(config-if)#desc LINK_TO_R_WEST
R_Dep_IT(config-if)#ip add 200.1.0.2 255.255.255.252
R_Dep_IT(config-if)#ip ospf message-digest-key 1 md5 zgtskpass
R_Dep_IT(config-if)#ip ospf authentication message-digest
R_Dep_IT(config-if)#no shut
R_Dep_IT(config-if)#ex
R_Dep_IT(config)#router ospf 1
R_Dep_IT(config-router)#area 1 authentication message-digest
R_Dep_IT(config-router)#network 200.1.0.0 0.0.0.3 area 1
R_Dep_IT(config-router)#passive-int e0/2.10
R_Dep_IT(config-router)#ex
R_Dep_IT(config)#router eigrp 101
```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		42

```

R_Dep_IT(config-router)#network 172.16.0.0 0.0.0.255
R_Dep_IT(config-router)#network 200.1.1.0 0.0.0.15
R_Dep_IT(config)#ip domain name zgtsk.com
R_Dep_IT(config)#crypto key generate rsa general-keys modulus 1024
R_Dep_IT(config)#service password-encryption
R_Dep_IT(config)#username admin privilege 15 secret admin
R_Dep_IT(config)#enable secret admin
R_Dep_IT(config)#aaa new-model
R_Dep_IT(config)#line vty 0 4
R_Dep_IT(config-line)#transport input ssh
R_Dep_IT(config-line)#transport out ssh
R_Dep_IT(config-line)#logging synchronous
R_Dep_IT(config-line)#exec-timeout 60 0
R_Dep_IT(config-line)#exit
R_Dep_IT(config)#ip ssh version 2
R_Dep_IT(config)#logging 200.0.0.1
R_Dep_IT(config)#service timestamps log datetime msec
R_Dep_IT(config)#service timestamps debug datetime msec
R_Dep_IT(config)#logging on
R_Dep_IT(config)#logging trap notifications
R_Dep_IT(config)#logging origin-id hostname

```

Далі налаштовуємо Site-to-Site VPN для з'єднання EAST та WEST ділянок мережі.

```

R_Dep_IT(config)#crypto isakmp policy 1
R_Dep_IT(config-isakmp)#encr 3des
R_Dep_IT(config-isakmp)#authentication pre-share
R_Dep_IT(config-isakmp)#group 2
R_Dep_IT(config-isakmp)#exit
R_Dep_IT(config)#crypto isakmp key zgtskpass address 10.2.0.2
R_Dep_IT(config)#crypto ipsec transform-set TS-S2S-VPN esp-aes esp-sha-hmac
R_Dep_IT(cfg-crypto-trans)#mode transport
R_Dep_IT(cfg-crypto-trans)#exit
R_Dep_IT(config)#crypto ipsec profile IPSEC-S2S-VPN
R_Dep_IT(ipsec-profile)#set security-association lifetime seconds 86400
R_Dep_IT(ipsec-profile)#set transform-set TS-S2S-VPN
R_Dep_IT(ipsec-profile)#ip access-list extended VPN-TRAFFIC
R_Dep_IT(config-ext-nacl)#permit ip 200.1.1.0 0.0.0.15 199.0.1.0 0.0.0.15
R_Dep_IT(config-ext-nacl)#exit
R_Dep_IT(config)#crypto map IPSEC-SITE-TO-SITE-VPN 10 ipsec-isakmp
R_Dep_IT(config-crypto-map)#set peer 10.2.0.2
R_Dep_IT(config-crypto-map)#set transform-set TS-S2S-VPN
R_Dep_IT(config-crypto-map)#match address VPN-TRAFFIC
R_Dep_IT(config-crypto-map)#exit
R_Dep_IT(config)#interface Tunnel0
R_Dep_IT(config-if)#ip address 172.16.0.1 255.255.255.0
R_Dep_IT(config-if)#tunnel source 200.1.0.2
R_Dep_IT(config-if)#tunnel destination 10.2.0.2
R_Dep_IT(config-if)#tunnel protection ipsec profile IPSEC-S2S-VPN
R_Dep_IT(config)#int s2/0
R_Dep_IT(config-if)#crypto map IPSEC-SITE-TO-SITE-VPN

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Останнім кроком налаштування даного маршрутизатора стане конфігурація ZPF: визначаємо зони (zone); присвоюємо їх для інтерфейсів; визначаємо пари зон (zone-pair); визначаємо карти класів (class-map), що описують трафік, до якого буде застосована політика при перетині пари зон; визначаємо карти політик (policy-map), де вказуємо, яку дію потрібно застосовувати щодо трафіку карт класів; застосовуємо карти політик до пар зон:

```
R_Dep_IT(config)#int s2/0
R_Dep_IT(config)#zone security INTERNET
R_Dep_IT(config-sec-zone)#exit
R_Dep_IT(config)#zone security LAN
R_Dep_IT(config-sec-zone)#exit
R_Dep_IT(config)#zone security MGMT
R_Dep_IT(config-sec-zone)#exit
R_Dep_IT(config)#zone security AD
R_Dep_IT(config-sec-zone)#exit
R_Dep_IT(config)#zone security DMZ
R_Dep_IT(config-sec-zone)#exit
...
R_Dep_IT(config)#interface s2/0
R_Dep_IT(config-if)#zone-member security INTERNET
...
R_Dep_IT(config)#class-map type inspect match-any INTERNET-PROTOCOLS
R_Dep_IT(config-cmap)#match protocol https
R_Dep_IT(config-cmap)#match protocol http
R_Dep_IT(config-cmap)#match protocol dns
...
R_Dep_IT(config)#policy-map type inspect LAN-TO-INTERNET-POLICY
R_Dep_IT(config-pmap)#class type inspect LAN-PROTOCOLS
R_Dep_IT(config-pmap-c)#inspect
R_Dep_IT(config-pmap-c)#exit
...
R_Dep_IT(config)# zone-pair security ZP-LAN-TO-INTERNET source LAN destination
INTERNET
R_Dep_IT(config-sec-zone-pair)# service-policy type inspect LAN-TO-INTERNET-
POLICY R_Dep_IT(config-sec-zone-pair)#exit
R_Dep_IT(config)#zone-pair security ZP-LAN-TO-DMZ source LAN destination DMZ
R_Dep_IT(config-sec-zone-pair)#service-policy type inspect TO-DMZ-POLICY
R_Dep_IT(config-sec-zone-pair)#exit
R_Dep_IT(config)#$-MGMT-TO-INTERNET source MGMT destination INTERNET
R_Dep_IT(config-sec-zone-pair)#$icy type inspect LAN-TO-INTERNET-POLICY
R_Dep_IT(config-sec-zone-pair)#exit
R_Dep_IT(config)#$security ZP-MGMT-TO-LAN source MGMT destination LAN
R_Dep_IT(config-sec-zone-pair)#$icy type inspect LAN-TO-INTERNET-POLICY
R_Dep_IT(config-sec-zone-pair)#exit
...
```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		44

3.2. Інтерфейс та порядок роботи з системою управління завданнями та доступом до ресурсів компанії на базі рішень Microsoft та Cisco.

При першому запуску додатку нас зустрічає екран автентифікації користувача (рис. 3.16).

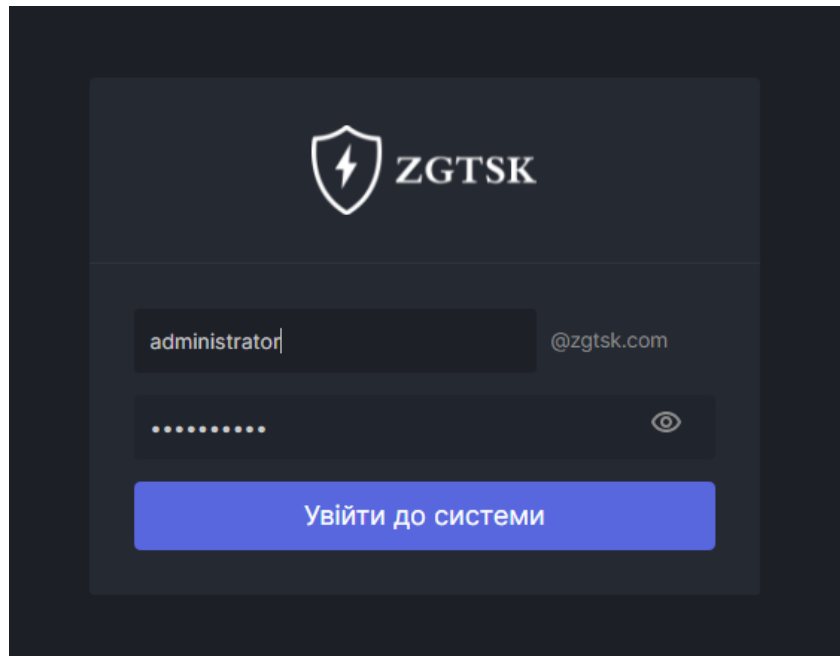


Рис. 3.16. Сторінка автентифікації

Головна сторінка (рис. 3.17) відображає ваші останні завдання, кругову діаграму про їх статус, статистику по загальному та витраченому часу на всі доручення.

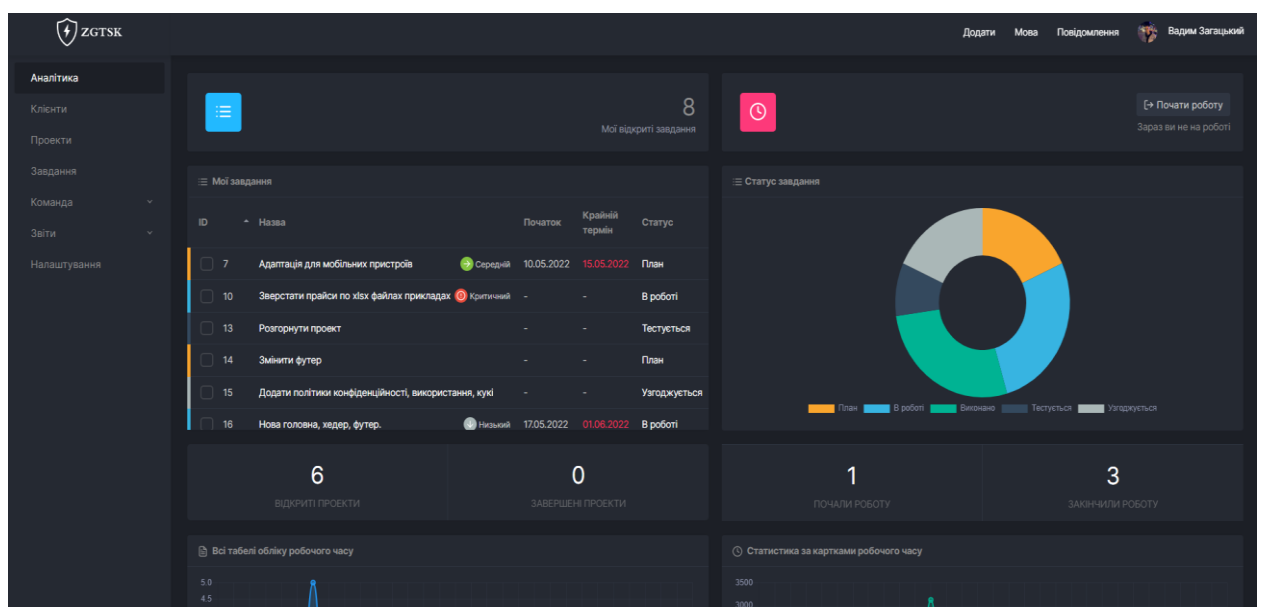


Рис. 3.17. Головна сторінка

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				45
Змн.	Арк.	№ докум.	Підпис	Дата		

Після авторизації користувач може здійснити перехід до своїх налаштувань профілю (рис. 3.18) – заповнити основні поля, змінити пароль.

The screenshot displays the 'Мій профіль' (My Profile) page for user Vadym Zagachytskyi. The interface includes a sidebar with navigation options like 'Аналітика', 'Клієнти', 'Проекти', 'Завдання', and 'Команда'. The main content area shows a profile card with a photo, name, and contact information. Below this, there are tabs for 'Загальна інформація', 'Інформація про роботу', 'Налаштування облікового запису', and 'Таймінг'. The 'Загальна інформація' tab is active, showing fields for Name, Surname, Email, and Phone. To the right, a summary box displays project statistics: 6 open projects, 0 completed projects, 53.73 total hours, and 92.27 total hours for projects. A 'Зберегти' (Save) button is visible at the bottom of the form.

Рис. 3.18. Сторінка особистого профілю

Далі можна перейти до додавання клієнта, де вказуються контактні дані для подальшої роботи (рис. 3.19).

The screenshot shows the 'Додати клієнта' (Add Client) modal form. It features four input fields: 'Назва компанії' (Company Name), 'Менеджер' (Manager) with a dropdown menu showing 'Анна Степаненко', 'Адреса' (Address), and 'Телефон' (Phone). At the bottom right, there are two buttons: 'Закрити' (Close) and 'Зберегти' (Save).

Рис. 3.19. Додавання клієнта

Одразу після створення нового запису можна перейти до перегляду новоствореної компанії, до проектів що належать та зміни інформації про клієнта (рис. 3.20).

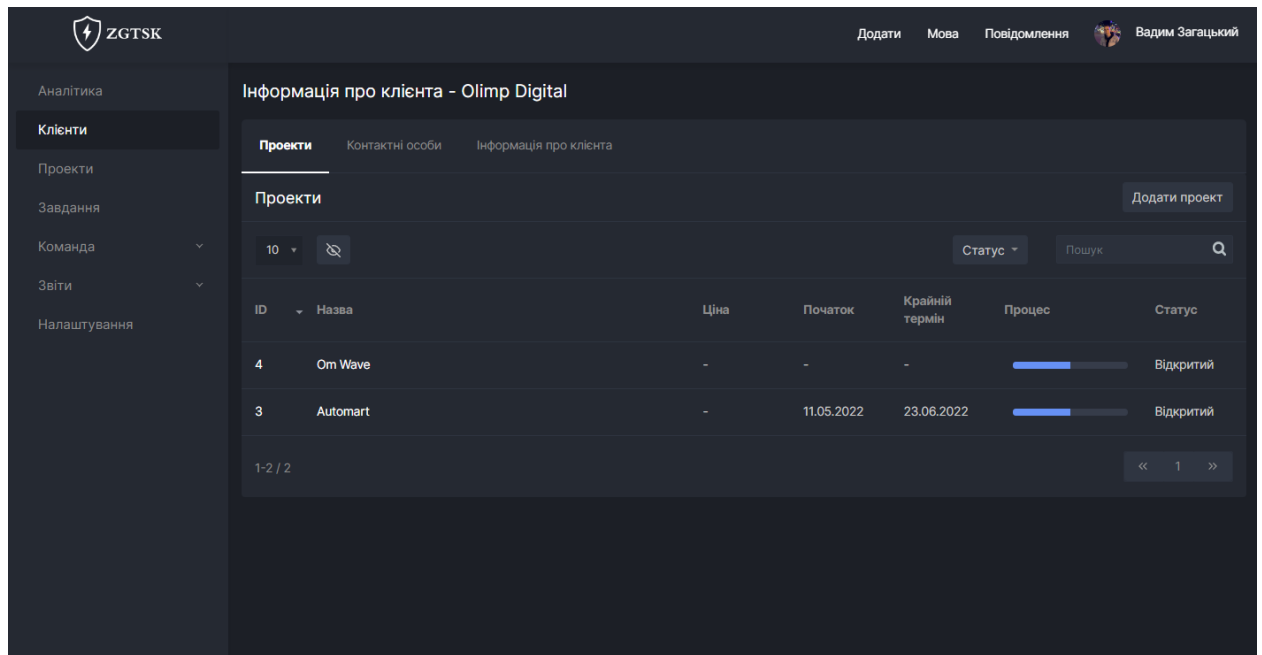


Рис. 3.20. Інформаційна сторінка про клієнта

Схожим способом створюються проекти, де зазначається назва, клієнт, деякий опис та дати початку та очікуваного кінця (рис. 3.21).

Рис. 3.21. Створення проекту

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		47

На сторінці проекту можна дізнатись про поточний статус виконання, хто є учасниками (додати або видалити), переглянути список завдань (рис. 3.22).

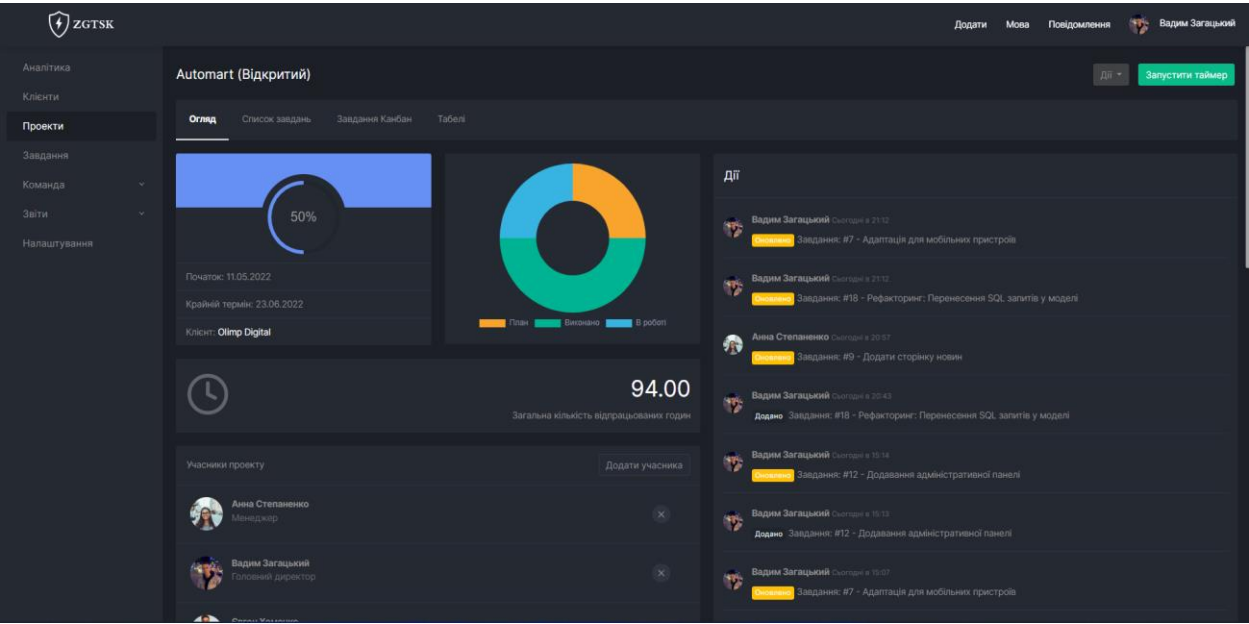


Рис. 3.22. Інформаційна сторінка про проект

Для завдань також доступна інтерактивна дошка (рис. 3.23), де можна перетягувати завдання до відповідного статусу (можна додавати в загальних налаштуваннях).

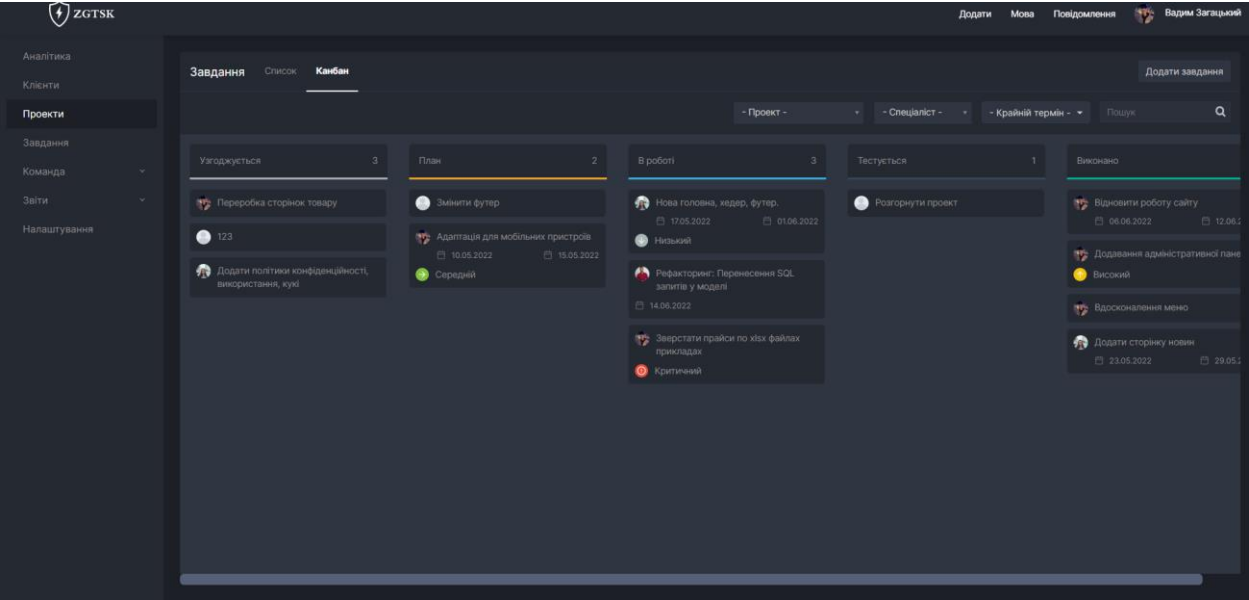


Рис. 3.23. Канбан-дошка з поточними завданнями

У будь-який момент при відповідних дозволах можна редагувати завдання, змінюючи поля на власний розсуд (рис. 3.24).

Рис. 3.24. Редагування завдань

Для правильного менеджменту персоналом, виставлення рахунків і іншої звітності потрібно додавати час виконання того чи іншого завдання (рис. 3.25).

Рис. 3.25. Додавання звіту про виконану роботу

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		49

3.3. Тестування роботи програмного забезпечення. Перевірка працездатності мережі

Одним з перших функцій протестуємо вхід до системи. Почнемо зі введення неправильних даних для аутентифікації (рис. 3.26).

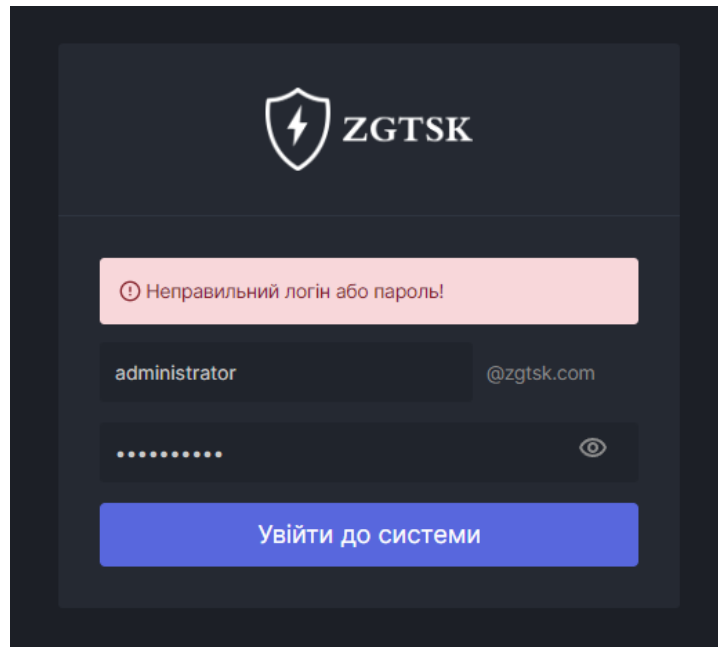


Рис. 3.26. Помилка з'єднання з сервером

Далі спробуємо увійти при втраті з'єднання з сервісами Active Directory. Отримаємо наступну помилку зображену на рисунку 3.27.

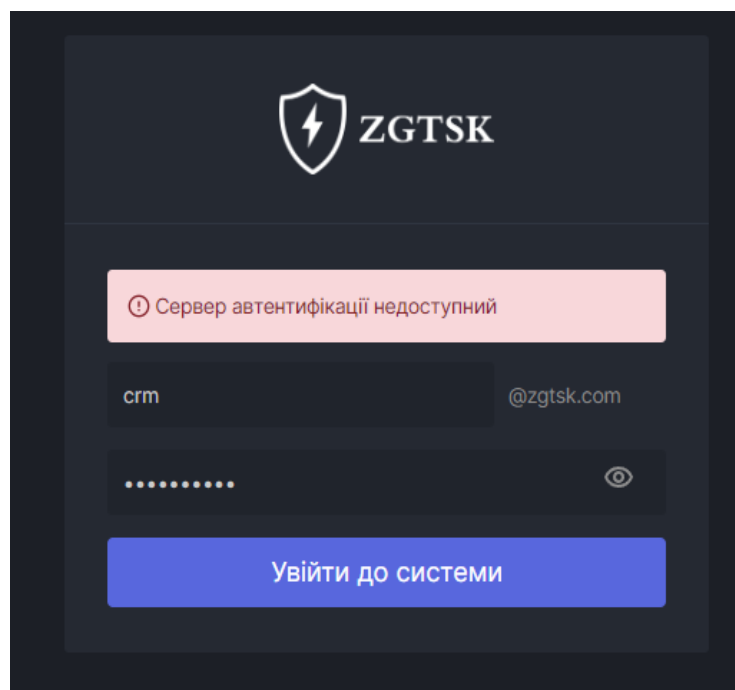


Рис. 3.27. Помилка з'єднання з сервером

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		50

Наступним кроком перевіримо чи можливо створити пусте завдання (рис. 3.28).

Рис. 3.28. Обов'язкові поля для заповнення

При втраті з'єднання з сервером (рис. 3.29), можна продовжувати роботу (окрім зміни інформацій про користувача та входу до системи).

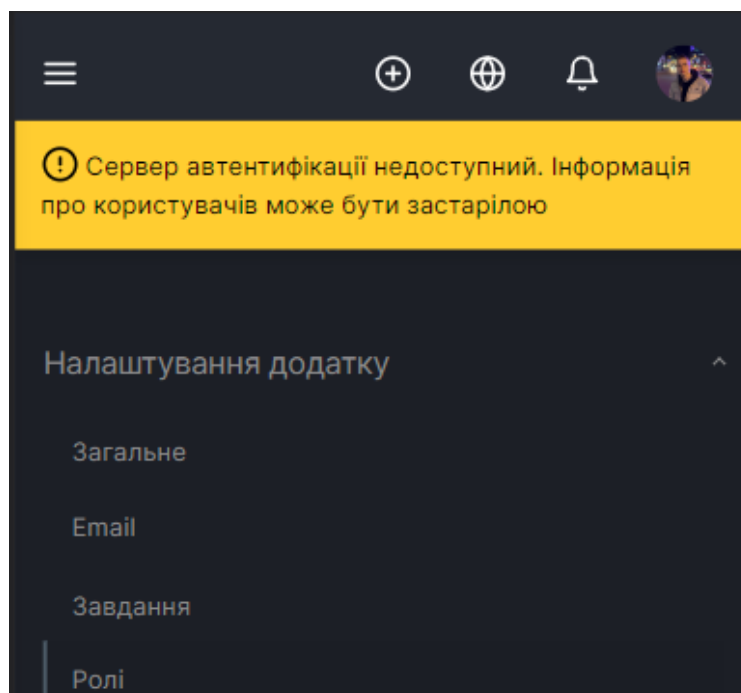


Рис. 3.29. Втрата з'єднання з сервером

Перевіримо також з’єднання та проходження трафіку між пристроями у спроектованій мережі (рис. 3.30).

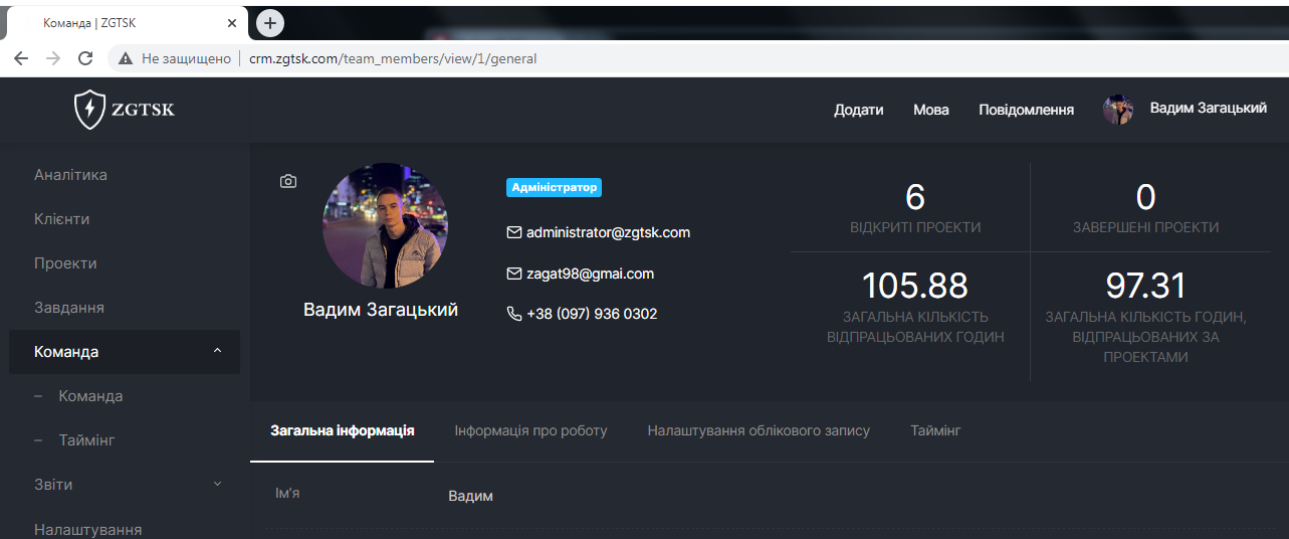


Рис. 3.30. Перевірка наявності зв’язку з сервером компанії
(WS_Finance_1 – WEB_Server)

Відповідно до таблиці 2.1 намагаємось отримати доступ до файлів від робочої станції підмережі MGMT до серверу DMZ зони (рис. 3.31) та SSH-з’єднання до комукаційних пристроїв мережі (рис. 3.32).

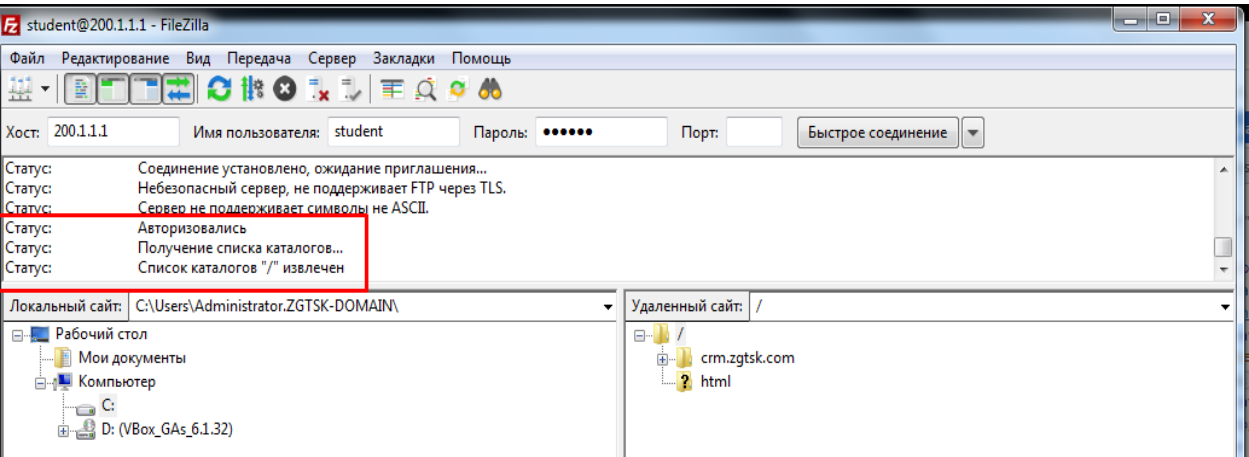


Рис. 3.31. Доступ за допомогою FTP з WS_MGMT до WEB_Server

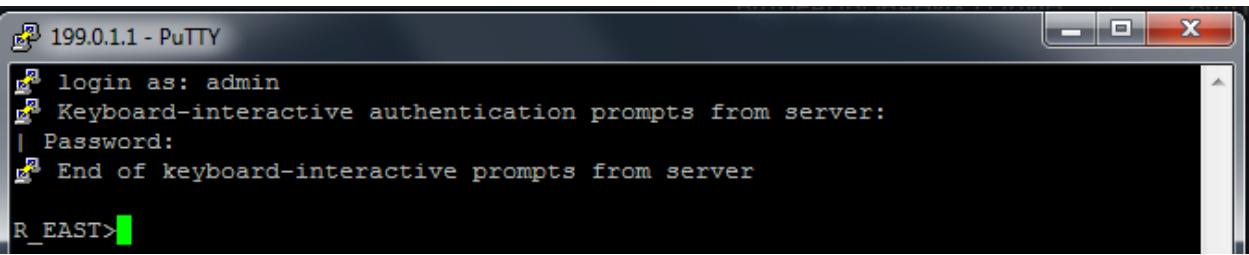


Рис. 3.32. Доступ за допомогою SSH (WS_MGMT – R_EAST)

Переріряємо шлях, що проходить трафік від LAN_S до LAN_E через глобальну мережу (рис. 3.33).

```
PS C:\Users\Administrator> tracert prod_rodc

Tracing route to prod_rodc.zgtsk.com [199.0.1.2]
over a maximum of 30 hops:

  1      1 ms      1 ms      1 ms  r_dep_it.zgtsk.com [200.0.0.14]
  2     38 ms     41 ms     39 ms  172.16.0.2
  3     41 ms     42 ms     39 ms  199.0.1.2

Trace complete.
```

Рис. 3.33. Перевірка наявності зв'язку через тунель між (Main_DC – Prod_RODC)

На маршрутизаторі R_EAST виводимо відомості про активні підключення до механізму шифрування (рис. 3.34).

```
R_EAST#show crypto engine connection act
Crypto Engine Connections

  ID  Type      Algorithm      Encrypt  Decrypt  LastSeqN  IP-Address
  --  --      -
  1   IPsec     AES+SHA        0        5809     5809      10.2.0.2
  2   IPsec     AES+SHA       7356      0         0        10.2.0.2
1001  IKE       SHA+3DES        0         0         0        10.2.0.2
```

Рис. 3.34. Виконання команди **show crypto engine connection act** (R_EAST)

Інформація про зони наведена на рисунку 3.35.

```
R_Dep_IT#show zone security
zone self
Description: System Defined Zone

zone INTERNET
Member Interfaces:
Serial2/0
Serial3/0

zone LAN
Member Interfaces:
Ethernet0/2.10

zone S2SVPN
Member Interfaces:
Tunnel0

zone DMZ
Member Interfaces:
Ethernet0/1.100

zone MGMT
Member Interfaces:
Ethernet0/2.99

zone AD
Member Interfaces:
Ethernet0/2.50
```

Рис. 3.35. Виконання команди **show zone security** (R_Dep_IT)

Статистика щодо пропущених пакетів наведена на рисунку 3.36.

```

policy exists on zp ZP-AD-TO-INTERNET
Zone-pair: ZP-AD-TO-INTERNET

Service-policy inspect : LAN-TO-INTERNET-POLICY

Class-map: LAN-PROTOCOLS (match-any)
  Match: protocol icmp
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol dns
    618 packets, 34506 bytes
    30 second rate 0 bps
  Match: protocol ftp
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol https
    49 packets, 1568 bytes

```

Рис. 3.36. Виконання команди **show policy-map type inspect zone-pair** (R_Dep_IT)

Також переконаємось, що маршрутизація працює нормально, виконавши команду «**show ip route**» (рис. 3.37).

```

Gateway of last resort is 200.1.0.1 to network 0.0.0.0

>*E2  0.0.0.0/0 [110/1] via 200.1.0.1, 01:36:26, Serial2/0
      10.0.0.0/30 is subnetted, 6 subnets
> IA   10.0.1.0 [110/192] via 200.1.0.1, 01:46:03, Serial2/0
> IA   10.0.2.0 [110/256] via 200.1.0.1, 01:46:03, Serial2/0
> IA   10.0.3.0 [110/192] via 200.1.0.1, 01:46:03, Serial2/0
> IA   10.1.0.0 [110/128] via 200.1.0.1, 01:46:03, Serial2/0
> IA   10.1.1.0 [110/256] via 200.1.0.1, 01:36:31, Serial2/0
> IA   10.2.0.0 [110/256] via 200.1.0.1, 01:30:38, Serial2/0
      11.0.0.0/24 is subnetted, 1 subnets
> IA   11.1.1.0 [110/202] via 200.1.0.1, 01:46:03, Serial2/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
>      172.16.0.0/24 is directly connected, Tunnel0
>      172.16.0.1/32 is directly connected, Tunnel0
      194.0.0.0/24 is variably subnetted, 2 subnets, 2 masks
>      194.0.0.0/28 is directly connected, Ethernet0/2.10
>      194.0.0.14/32 is directly connected, Ethernet0/2.10
      194.0.1.0/24 is variably subnetted, 2 subnets, 2 masks
>      194.0.1.0/28 is directly connected, Ethernet0/2.99
>      194.0.1.14/32 is directly connected, Ethernet0/2.99
      195.0.0.0/28 is subnetted, 1 subnets
>      195.0.0.0 [110/74] via 200.3.0.2, 00:42:02, Serial3/0
      195.0.1.0/28 is subnetted, 1 subnets
>      195.0.1.0 [110/74] via 200.3.0.2, 00:42:02, Serial3/0

```

Рис. 3.37. Частина таблиці маршрутизації R_Dep_IT

Висновки до третього розділу

У даному розділі було розгорнуто структуру Active Directory, налаштовано мережу організації. Розглянуто структуру інтерфейсу веб-додатку, порядок роботи з ним.

Проведено тестування додатку на вразливості до неправильних даних, виконані основні діагностичні команди на комунікаційних пристроях. В результаті встановлено, що система працює відповідно до вимог правил та алгоритмів.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		54

ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи бакалавра було запропоновано проект інформаційної системи управління завданнями та доступом до ресурсів компанії на базі рішень Microsoft та Cisco.

Було проведено аналіз поставленого завдання, досліджено наявні аналоги, їх переваги та недоліки. Обґрунтований вибір інструментарію, їх призначення та особливості. Вказано як саме можна підвищити рівень безпеки мережі за допомогою міжмережевих екранів.

Побудовано та спроектовано уявлення про роботу додатку, його окремі алгоритми та функціонал, а також спроектовано базу даних та зв'язки між таблицями, графічний інтерфейс користувача. Наведено матрицю доступу, за допомогою якої надалі можна налаштовувати пристрої та доповнюючи її розширювати мережу.

Проведено налаштування Windows Server зі службами Active Directory та іншими додатковими компонентами. У процесі тестування, потрібно було виявити різноманітні помилки та збоїв в роботі, у разі введені невірних даних або неочікуваних дій від користувача. Було побудовано та налагоджено запропоновану мережу в симуляторі Graphical Network Simulator. Протестоване на коректність налаштування та особливості роботи міжмережевого екранування трафіку.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		55

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- 1) The Basics of Project Management [Електронний ресурс]. – 2021. – Режим доступу: <https://kissflow.com/project/project-management-basics/>
- 2) Kanban Methodology: The Simplest Agile Framework [Електронний ресурс]. – 2021. – Режим доступу: <https://kissflow.com/project/agile/kanban-methodology/>
- 3) Grow CRM - A Self Hosted CRM & Project Management Software [Електронний ресурс]. – 2022. – Режим доступу: <https://growcrm.io/>
- 4) Perfex – Powerful Open Source CRM [Електронний ресурс]. – 2022. – Режим доступу: <https://www.perfexcrm.com/>
- 5) Ekushey Project Manager CRM [Електронний ресурс]. – 2022. – Режим доступу: <https://codecanyon.net/item/ekushey-project-manager-crm/9492104>
- 6) CodeIgniter4 User Guide [Електронний ресурс]. – 2022. – Режим доступу: https://codeigniter.com/user_guide/index.html.
- 7) jQuery API [Електронний ресурс]. – 2022. – Режим доступу: <https://api.jquery.com/>
- 8) Security Configuration Guide: Zone-Based Policy Firewall [Електронний ресурс]. – 2018. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/15-mt/sec-data-zbf-15-mt-book/sec-zone-pol-fw.html.
- 9) What Is LDAP? [Електронний ресурс]. – 2022. – Режим доступу: <https://jumpcloud.com/blog/what-is-ldap>
- 10) Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – 5-е вид. – СПб.: Питер, 2016. – 996 с.
- 11) Хендерсон М. Windows Server 2019 Cookbook / М. Хендерсон, Д. Краус., 2020. – 651 с.
- 12) Орін Т. Windows Server 2016 Inside Out / Томас Орін., 2017. – 1053
- 13) Active Directory Domain Services [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services>.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		56

14) CCNAS2: CCNA Security [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: <https://lms.netacad.com/course/view.php?id=223495>.

15) Cisco IOS Site-to-Site and Extranet VPN Business Scenarios [Електронний ресурс]. – 2021. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/vpn_modules/6342/vpn_cg/6342site3.html.

16) Configure Commonly Used ACLs [Електронний ресурс]. – 2021. – Режим доступу: <https://lms.netacad.com/course/view.php?id=223495>.

17) How To Install Linux, Apache, MySQL, PHP (LAMP) stack on Ubuntu 18.04 [Електронний ресурс]. – 2021. – Режим доступу: <https://www.digitalocean.com/community/tutorials/how-to-install-linux-apache-mysql-php-lamp-stack-ubuntu-18-04>.

18) PHP Lightweight Directory Access Protocol [Електронний ресурс]. – 2022. – Режим доступу: <https://www.php.net/manual/en/book.ldap.php>.

19) Vsftpd, installation and basic configuration of an FTP server [Електронний ресурс]. – 2018. – Режим доступу: <https://ubunlog.com/en/vsftpd-install-a-ubuntu-ftp-server/>

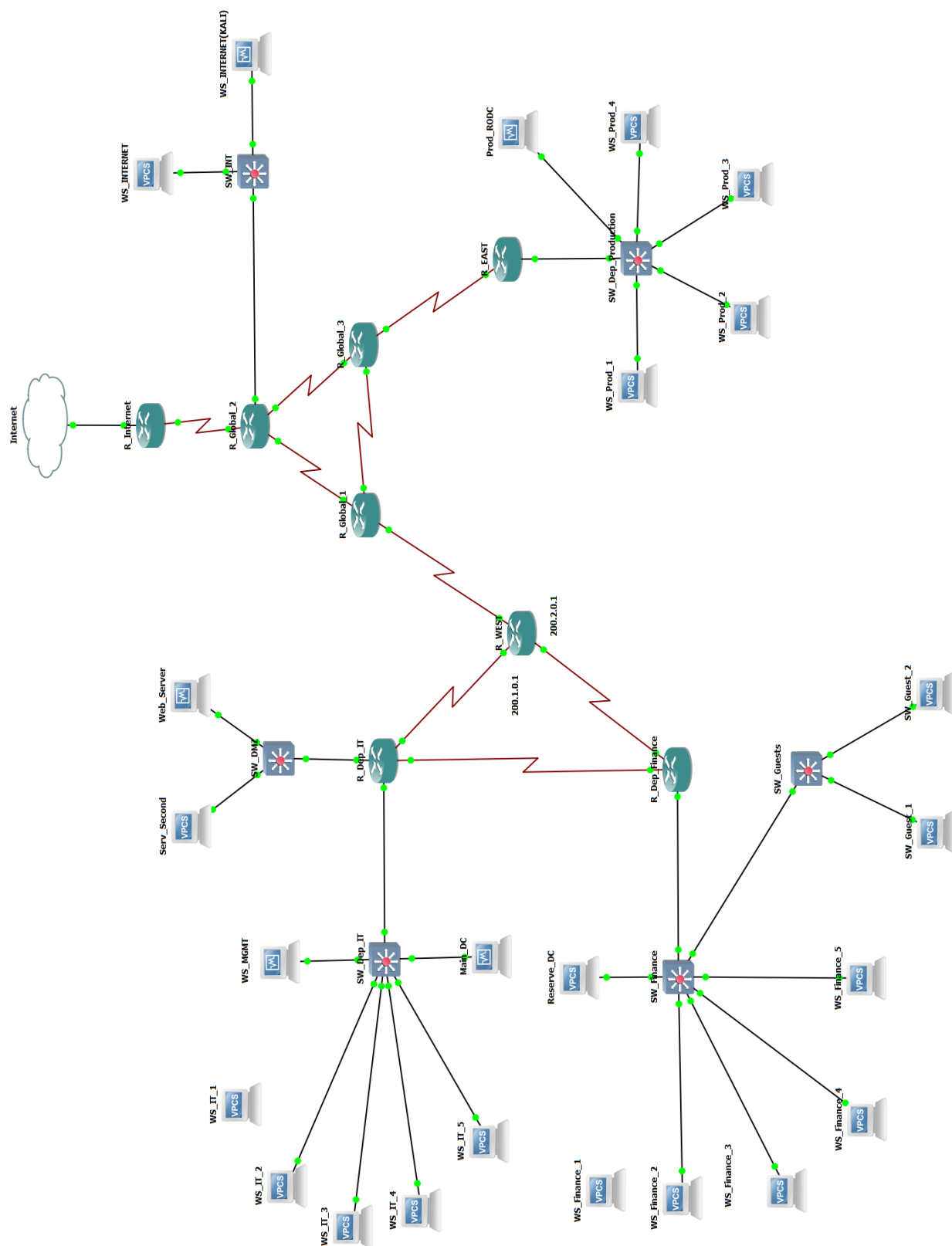
20) Типовая конфигурация для маршрутизатора Cisco в малом офисе [Електронний ресурс]. – 2017. – Режим доступу: <https://uzverss.livejournal.com/85470.html>.

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		57

ДОДАТКИ

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		58

Детальна схема побудованої мережі



		В.Загацький		
		І. Панаріна		
Змн.	Арк.	№ докум.	Підпис	Дата

КІК.КР.Б – 123 – 12 – ПЗ

Арк.

59

Додаток Б

Таблиця Б.1

Адресація підмереж А, С, D, E

Призначення	Підмережа			
	A	C	D	E
Адреса мережі	200.1.1.0	195.0.0.0	195.0.1.0	199.0.1.0
Маска мережі	255.255.255.240 /28	255.255.255.240 /28	255.255.255.240 /28	255.255.255.240 /28
Мінімальна адреса	200.1.1.1	195.0.0.1	195.0.1.1	199.0.1.1
Максимальна адреса	200.1.1.14	195.0.0.14	195.0.1.14	199.0.1.14
Широкомовна адреса	200.1.1.15	195.0.0.15	195.0.1.15	199.0.1.15
Шлюз по замовчуванню	200.1.1.14	195.0.0.14	195.0.1.14	199.0.1.14
Діапазон адрес комутаторів	200.0.1.13 200.0.1.13	195.0.0.13 195.0.0.13	195.0.1.11 195.0.1.13	199.0.1.11 199.0.1.13

Таблиця Б.2

Адресація підмережі В

VLAN	Адреса мережі	Маска мережі	Шлюз по замовчуванню	Min/Max/Широкомовна	Вільні адреси
VLAN 10 (VLAN_A)	194.0.0.0	255.255.255.240 /28	194.0.0.14	194.0.0.1 194.0.0.14 194.0.0.15	194.0.0.7 194.0.0.13
VLAN 99 (VLAN_MGMT)	194.0.1.0	255.255.255.240 /28	194.0.1.14	194.0.1.1 194.0.1.14 194.0.1.15	194.0.1.7 194.0.1.13

Таблиця Б.3

Адресація підмережі S

Призначення	IP-адреса
Адреса мережі	200.0.0.0
Маска мережі	255.255.255.240/28
Мінімальна адреса	200.0.0.1
Максимальна адреса	200.0.0.14
Широкомовна адреса	200.0.0.15
Шлюз по замовчуванню	200.0.0.14

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		60

Лістинг файлу “Ldap_model.php”:

```

<?php

namespace App\Models;

use CodeIgniter\Model;
use mysql_xdevapi\TableUpdate;

class Ldap_model extends Model
{
    protected $ldap_username = 'Administrator';
    protected $ldap_password = 'Adm1nAdm1n';
    protected $uri = '192.168.1.10';
    protected $port = 389;
    protected $connection;
    protected $dn = 'DC=zahatskyi,DC=net';
    public $active = false;
    public $domain = 'zahatskyi.net';
    protected array $currentUser = [];

    function __construct()
    {
        $this->ldap_username .= '@' . $this->domain;
        $this->connect();
    }
    private function connect($username = "", $password = "")
    {
        if (!$username) {
            $username = $this->ldap_username;
        }
        if (!$password) {
            $password = $this->ldap_password;
        }
        $this->connection = ldap_connect($this->uri, $this->port);
        ldap_set_option($this->connection, LDAP_OPT_NETWORK_TIMEOUT, 2);
        ldap_set_option($this->connection, LDAP_OPT_TIMELIMIT, 2);

        if (@ldap_bind($this->connection, $username, $password)) {
            $this->test = $username;
            ldap_set_option($this->connection, LDAP_OPT_PROTOCOL_VERSION, 3);
            ldap_set_option($this->connection, LDAP_OPT_REFERRALS, 0);
            $this->active = true;
        } else {
            $this->active = false;
        }
    }

    public function login($username, $password)
    {
        $login = $username;
        if (!strpos($login, $this->domain) && strpos($login, '@') == false) {
            $login .= '@' . $this->domain;
        }
        if (@ldap_bind($this->connection, $login, $password)) {
            $this->currentUserInfo($username);
            return true;
        }

        return false;
    }
}

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		61

```

}
public function bind($username, $password)
{
    if (!strpos($username, $this->domain) && strpos($username, '@') == false) {
        $username .= '@' . $this->domain;
    }
    if (@ldap_bind($this->connection, $username, $password)) {

        $this->currentUserInfo($username);
        return true;
    }
    return false;
}
private function getAdUserInfo($username)
{
    $search_filter = "(&(objectCategory=person)(samaccountname=$username))";
    ldap_bind($this->connection, $this->ldap_username, $this->ldap_password);
    return $this->get_entries($search_filter)[0];
}
public function getUserInfo($username) {
    $search_filter = "(&(objectCategory=person)(samaccountname=$username))";
    $res = $this->get_entries($search_filter)[0];
    $data = array();
    if ($res) {
        $data['email'] = "$username@$this->domain";
        $data['first_name'] = $this->getValue($res, 'givenname');
        $data['last_name'] = $this->getValue($res, 'sn');
        $data['address'] = $this->getValue($res, 'mail');
        $data['phone'] = $this->getValue($res, 'telephonenumber');
        $data['job_title'] = $this->getValue($res, 'title');
        $data['department'] = $this->getValue($res, 'department');
        $data['ad_login'] = $username;
    }
    return (object)$data;
}
private function currentUserInfo($username)
{
    $search_filter = "(&(objectCategory=person)(samaccountname=$username))";
    $res = $this->get_entries($search_filter)[0];
    if ($res) {
        $this->currentUser['email'] = "$username@$this->domain";
        $this->currentUser['first_name'] = $this->getValue($res, 'givenname');
        $this->currentUser['last_name'] = $this->getValue($res, 'sn');
        $this->currentUser['job_title'] = $this->getValue($res, 'title');
        $this->currentUser['ad_login'] = $username;
    }
}
public function search($filter)
{
    ldap_bind($this->connection, $this->ldap_username, $this->ldap_password);
    return ldap_search($this->connection, $this->dn, $filter);
}
public function get_entries($filter)
{
    return ldap_get_entries($this->connection, $this->search($filter));
}
private function getValue($entry, $key)
{
    $data = "";
    if (!empty($entry[$key][0])) {
        $data = $entry[$key][0];
        if ($data == "NULL") {
            $data = "";
        }
    }
}

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		62

```

    }
}
return $data;
}

public function getCurrentUserInfo()
{
    return $this->currentUser;
}

public function updateUserInfo($user_id, $user_data)
{
    $user_model = new Users_model();
    $username = $user_model->get_details(['id' => $user_id])->getResult('array')[0]['ad_login'];
    $user_info = $this->getAdUserInfo($username);
    $dn = $user_info['dn'];
    $entry['givenName'] = $user_data['first_name'];
    $entry['sn'] = $user_data['last_name'];
    $entry['displayName'] = "{$user_data['first_name']} {$user_data['last_name']}";
    if ($user_data['phone']) {
        $entry['telephoneNumber'][0] = $user_data['phone'];
    }
    if ($user_data['address']) {
        $entry['mail'] = $user_data['address'];
    }
    if (!@ldap_modify($this->connection, $dn, $entry)) {
        return false;
    }
    $new_dn = "cn={$entry['displayName']}";
    $new_parent = explode(',', $dn);
    unset($new_parent[0]);
    $new_parent = implode(',', $new_parent);
    if (!@ldap_rename($this->connection, $dn, $new_dn, $new_parent, true)) {
        return false;
    }
    return false;
}

public function updateUserJobInfo($user_id, $user_data)
{
    $user_model = new Users_model();
    $username = $user_model->get_details(['id' => $user_id])->getResult('array')[0]['ad_login'];
    $dn = $this->getAdUserInfo($username)['dn'];
    $entry = [];
    if ($user_data['job_title']) {
        $entry['title'] = $user_data['job_title'];
    }
    if ($user_data['department']) {
        $entry['department'] = $user_data['department'];
    }
    if ($entry) {
        if (ldap_modify($this->connection, $dn, $entry)) {
            return true;
        }
    }
    return false;
}

public function getInactiveUsers()
{
    $search_filter = "(objectCategory=person)";
    $res = $this->get_entries($search_filter);
    $user_model = new Users_model();
    for ($i = 0; $i < $res['count']; $i++) {

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		63

```

        $email = $res[$i]['samaccountname'][0] . '@' . $this->domain;
        if ($user_model->is_email_exists($email)) {
            $res[$i]['crm_exist'] = true;
        }
    }
    return $res;
}

public function changeProfileImage($user_id, $user_data) {
    $user_model = new Users_model();
    $username = $user_model->get_details(['id' => $user_id])->getResult('array')[0]['ad_login'];
    $dn = $this->getAdUserInfo($username)['dn'];
    $entry = [];
    if ($user_data) {
        $entry['thumbnailPhoto'] = $user_data;
        $entry['jpegPhoto'] = $user_data;
    }
    if ($entry) {
        if (ldap_modify($this->connection, $dn, $entry)) {
            return true;
        }
    }
    return false;
}

public function changePassword($user_id, $password, $is_user_register = true)
{
    if ($is_user_register) {
        $user_model = new Users_model();
        $username = $user_model->get_details(['id' => $user_id])->getResult('array')[0]['ad_login'];
        $dn = $this->getAdUserInfo($username)['dn'];
    }
    $userpassword = "{SHA}" . base64_encode(pack("H*", sha1($pass)));
    $newEntry = array('unicodePwd' => $userpassword);

    if (ldap_mod_replace($this->connection, $dn, $newEntry)) {
        return true;
    }
    return false;
}

public function close()
{
    ldap_close($this->connection);
}
}

```

Лістинг файлу “Signin.php”:

```

<?php

namespace App\Controllers;

class Signin extends App_Controller
{
    private $signin_validation_errors;
    function __construct()
    {
        parent::__construct();
        $this->signin_validation_errors = array();
        helper('email');
    }
    function index()
    {
        if ($this->Users_model->login_user_id()) {
            app_redirect('dashboard/view');
        }
    }
}

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		64

```

    } else {
        $view_data["redirect"] = "";
        if (isset($_REQUEST["redirect"])) {
            $view_data["redirect"] = $_REQUEST["redirect"];
        }
        $view_data["domain"] = config('Ldap')->domain;
        return $this->template->view('signin/index', $view_data);
    }
}

function authenticate()
{
    $validation = $this->validate_submitted_data(array(
        "email" => "required",
        "password" => "required"
    ), true);
    $email = $this->request->getPost("email");
    $password = $this->request->getPost("password");
    if (!$email) {
        app_redirect('signin');
    }
    if (is_array($validation)) {
        $this->signin_validation_errors = $validation;
    }
    if ($this->signin_validation_errors) {
        $this->session->setFlashdata("signin_validation_errors", $this->signin_validation_errors);
        app_redirect('signin');
    }
    $auth = $this->Users_model->authenticate($email, $password);
    if (!$auth || isset($auth['error_dc'])) {
        if (isset($auth['error_dc']) && $auth['error_dc']) {
            array_push($this->signin_validation_errors, app_lang("domain_controller_error_login"));
        } else {
            array_push($this->signin_validation_errors, app_lang("authentication_failed"));
        }
        $this->session->setFlashdata("signin_validation_errors", $this->signin_validation_errors);
        app_redirect('signin');
    }
    $redirect = $this->request->getPost("redirect");
    if ($redirect) {
        return redirect()->to($redirect);
    } else {
        app_redirect('dashboard/view');
    }
}

function sign_out()
{
    $this->Users_model->sign_out();
}
}

```

Лістинг файлу “Users_model.php”:

```

<?php

namespace App\Models;
use App\Controllers\Signup;

class Users_model extends Crud_model
{
    protected $table = null;
    protected $user_ad_fl = false;

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		65

```

function __construct()
{
    $this->table = 'users';
    parent::__construct($this->table);
}
function authenticate($email, $password)
{
    if ($email) {
        $email = $this->db->escapeString($email);
    }
    $ldap = new \App\Models\Ldap_model();
    if ($ldap->active) {
        if ($ldap->login($email, $password)) {
            $email .= '@' . $ldap->domain;
            $this->user_ad_fl = true;
            $ldap->close();
        } else { return false ;
        }
    } else { return array('error_dc' => '1'); }
    $this->db_builder->select("id,user_type,client_id,password");
    $result = $this->db_builder->getWhere(array('email' => $email, 'status' => 'active', 'deleted' => 0,
'disable_login' => 0));
    if ($this->user_ad_fl && count($result->getResult()) == 0) {
        $signup = new Signup();
        $id = $signup->create_from_ad_account($ldap->getCurrentUserInfo());
    } else if (count($result->getResult()) != 1) {
        return false;
    }
    $user_info = $result->getRow();
    $session = \Config\Services::session();
    $session->set('user_id', $user_info->id);
    return true;
}
function login_user_id()
{
    $session = \Config\Services::session();
    return $session->has("user_id") ? $session->get("user_id") : "";
}
function sign_out()
{
    $session = \Config\Services::session();
    $session->destroy();
    app_redirect('signin');
}
function sync_with_ad($entry)
{
    $user_info = $entry->getResult()[0];
    $ldap = new Ldap_model();
    $user_id = $user_info->id;
    if ($ldap->active) {
        $ad_data = (array)$ldap->getUserInfo($user_info->ad_login);
        $job_data = array(
            "user_id" => $user_id,
        );
        $user_data = array(
            "job_title" => $ad_data['job_title'],
            'first_name' => $ad_data['first_name'],
            'last_name' => $ad_data['last_name'],
            "department" => $ad_data['department'],
        );
        $this->ci_save($user_data, $user_id);
        $this->save_job_info($job_data);
    }
}

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		66

```

function get_details($options = array())
{
    $users_table = $this->db->prefixTable('users');
    $team_member_job_info_table = $this->db->prefixTable('team_member_job_info');
    $clients_table = $this->db->prefixTable('clients');
    $roles_table = $this->db->prefixTable('roles');
    $where = "";
    $id = get_array_value($options, "id");
    $status = get_array_value($options, "status");
    $user_type = get_array_value($options, "user_type");
    $client_id = get_array_value($options, "client_id");
    $exclude_user_id = get_array_value($options, "exclude_user_id");
    $first_name = get_array_value($options, "first_name");
    $last_name = get_array_value($options, "last_name");
    if ($id) {
        $where .= " AND $users_table.id=$id";
    }
    if ($status === "active") {
        $where .= " AND $users_table.status='active'";
    } else if ($status === "inactive") {
        $where .= " AND $users_table.status='inactive'";
    }
    if ($user_type) {
        $where .= " AND $users_table.user_type='$user_type'";
    }
    if ($user_type == 'client') {
        $where .= " AND $clients_table.deleted=0";
    }
    if ($first_name) {
        $where .= " AND $users_table.first_name='$first_name'";
    }
    if ($last_name) {
        $where .= " AND $users_table.last_name='$last_name'";
    }
    if ($client_id) {
        $client_id = $this->db->escapeString($client_id);
        $where .= " AND $users_table.client_id=$client_id";
    }
    if ($exclude_user_id) {
        $where .= " AND $users_table.id!=$exclude_user_id";
    }
    $non_admin_users_only = get_array_value($options, "non_admin_users_only");
    if ($non_admin_users_only) {
        $where .= " AND $users_table.is_admin=0";
    }
    $show_own_clients_only_user_id = get_array_value($options, "show_own_clients_only_user_id");
    if ($user_type == "client" && $show_own_clients_only_user_id) {
        $where .= " AND $users_table.client_id IN(SELECT $clients_table.id FROM $clients_table
WHERE $clients_table.deleted=0 AND $clients_table.created_by=$show_own_clients_only_user_id)";
    }
    $quick_filter = get_array_value($options, "quick_filter");
    if ($quick_filter) {
        $where .= $this->make_quick_filter_query($quick_filter, $users_table);
    }
    $sql = "SELECT $users_table.*, $roles_table.title AS role_title,
        $team_member_job_info_table.date_of_hire, $team_member_job_info_table.salary,
$team_member_job_info_table.salary_term $select_custom_fieds FROM $users_table
LEFT JOIN $team_member_job_info_table ON
$team_member_job_info_table.user_id=$users_table.id
LEFT JOIN $clients_table ON $clients_table.id=$users_table.client_id
LEFT JOIN $roles_table ON $roles_table.id=$users_table.role_id
WHERE $users_table.deleted=0 $where $custom_fields_where
ORDER BY $users_table.first_name";

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		67

```

$res = $this->db->query($sql);
if ($options['user_type'] == 'staff') { $this->sync_with_ad($res); }
return $this->db->query($sql);
}
function is_email_exists($email, $id = 0)
{
    $users_table = $this->db->prefixTable('users');
    $id = $id ? $this->db->escapeString($id) : $id
    $sql = "SELECT $users_table.* FROM $users_table
    WHERE $users_table.deleted=0 AND $users_table.email='$email'";
    $result = $this->db->query($sql);
    if ($result->resultID->num_rows && $result->getRow()->id != $id) {
        return $result->getRow();
    } else { return false; }
}
function get_job_info($user_id)
{
    parent::use_table("team_member_job_info");
    return parent::get_one_where(array("user_id" => $user_id));
}
function save_job_info($data)
{
    parent::use_table("team_member_job_info");
    $where = array("user_id" => get_array_value($data, "user_id"));
    $exists = parent::get_one_where($where);
    if ($exists->user_id) {
        return parent::update_where($data, $where);
    } else {
        return parent::ci_save($data);
    }
}
function get_team_members($member_ids = "")
{
    $users_table = $this->db->prefixTable('users');
    $sql = "SELECT $users_table.* FROM $users_table
    WHERE $users_table.deleted=0 AND $users_table.user_type='staff' AND
    FIND_IN_SET($users_table.id, '$member_ids') ORDER BY $users_table.first_name";
    return $this->db->query($sql);
}
function get_online_user_ids()
{
    $users_table = $this->db->prefixTable('users');
    $now = get_current_utc_time();
    $sql = "SELECT $users_table.id
    FROM $users_table WHERE TIMESTAMPDIFF(MINUTE, users.last_online, '$now')<=0";
    return $this->db->query($sql)->getResult();
}
function get_one($id = 0)
{
    $user_info = parent::get_one($id);
    $ldap = new Ldap_model();
    if ($ldap->active) {
        $ad_data = $ldap->getUserInfo($user_info->ad_login);
        $user_info = (object)array_merge((array)$user_info, (array)$ad_data);
    }
    return $user_info;
}
}

```

Лістинги конфігурацій

R_Dep_IT:

```

R_Dep_IT#show start
Using 8717 out of 32768 bytes
!
! Last configuration change at 23:49:41
UTC Wed Jun 15 2022
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R_Dep_IT
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$HDI$UnFVr/FO.xHt9IzOGbINS.
!
aaa new-model
!
!
!
!
!
!
!
aaa session-id common
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
!
!
!
!
no ip domain lookup
ip domain name zgtsk.com
ip cef
no ipv6 cef
!
parameter-map type inspect
DoS_PARAM_MAP
max-incomplete low 200
max-incomplete high 200
one-minute low 1000
one-minute high 1000
tcp max-incomplete host 100 block-time 5
multilink bundle-name authenticated
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$aZJJ$cgWq98sqV/Oa.oZnQA9z1/
!
redundancy
!
!
ip ssh version 2
!
class-map type inspect match-any LAN-
PROTOCOLS
match protocol icmp
match protocol dns
match protocol ftp
match protocol https
match protocol http
match protocol tcp
match protocol udp
class-map type inspect match-any DMZ-
PROTOCOLS
match protocol icmp
match protocol dns
match protocol ldap
match protocol ldaps
class-map type inspect match-all LAN-C-
CLASS
match access-group name LAN_C_ACL
class-map type inspect match-all IPSEC-
POLICY
match access-group name ISAKMP_IPSEC
class-map type inspect match-any
INTERNET-PROTOCOLS
match protocol icmp
match protocol https
match protocol http
match protocol dns
match protocol syslog
match protocol syslog-conn
!
policy-map type inspect LAN_C-TO-DMZ-
POLICY
class type inspect LAN-C-CLASS
inspect DoS_PARAM_MAP
class type inspect INTERNET-
PROTOCOLS
inspect DoS_PARAM_MAP
class class-default

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

drop
policy-map type inspect LAN-TO-
INTERNET-POLICY
class type inspect LAN-PROTOCOLS
inspect
class class-default
drop
policy-map type inspect INTERNET-TO-
SELF-POLICY
class type inspect IPSEC-POLICY
pass
class class-default
drop
policy-map type inspect TO-DMZ-POLICY
class type inspect INTERNET-
PROTOCOLS
inspect DoS_PARAM_MAP
class class-default
drop
policy-map type inspect DMZ-TO-AD-
POLICY
class type inspect DMZ-PROTOCOLS
inspect DoS_PARAM_MAP
class class-default
drop
!
zone security INTERNET
zone security LAN
zone security S2SVPN
zone security DMZ
zone security MGMT
zone security AD
zone-pair security ZP-LAN-TO-INTERNET
source LAN destination INTERNET
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-AD-TO-INTERNET
source AD destination INTERNET
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-DMZ-TO-AD source
DMZ destination AD
service-policy type inspect DMZ-TO-AD-
POLICY
zone-pair security ZP-AD-TO-DMZ source
AD destination DMZ
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-LAN-TO-AD source
LAN destination AD
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-AD-TO-LAN source
AD destination LAN
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-MGMT-TO-AD
source MGMT destination AD
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-AD-TO-MGMT
source AD destination MGMT

```

```

service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-LAN-TO-DMZ
source LAN destination DMZ
service-policy type inspect TO-DMZ-
POLICY
zone-pair security ZP-MGMT-TO-
INTERNET source MGMT destination INTERNET
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-MGMT-TO-LAN
source MGMT destination LAN
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-MGMT-TO-S2SVPN
source MGMT destination S2SVPN
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-MGMT-TO-DMZ
source MGMT destination DMZ
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-S2SVPN-TO-DMZ
source S2SVPN destination DMZ
service-policy type inspect TO-DMZ-
POLICY
zone-pair security ZP-S2SVPN-TO-AD
source S2SVPN destination AD
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-AD-TO-S2SVPN
source AD destination S2SVPN
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-DMZ-TO-
INTERNET source DMZ destination INTERNET
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-LAN_C-TO-DMZ
source INTERNET destination DMZ
service-policy type inspect LAN_C-TO-
DMZ-POLICY
zone-pair security ZP-LAN_C-TO-AD
source INTERNET destination AD
service-policy type inspect LAN_C-TO-
DMZ-POLICY
zone-pair security ZP-INTERNET-TO-
SELF source INTERNET destination self
service-policy type inspect INTERNET-
TO-SELF-POLICY
!
!
!
!
!
crypto isakmp policy 1
encr 3des
authentication pre-share
group 2
crypto isakmp key zgtskpass address
10.2.0.2
!
!

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		70

```

crypto ipsec transform-set TS-S2S-VPN
esp-aes esp-sha-hmac
mode transport
!
crypto ipsec profile IPSEC-S2S-VPN
set security-association lifetime seconds
86400
set transform-set TS-S2S-VPN
!
!
!
crypto map IPSEC-SITE-TO-SITE-VPN 10
ipsec-isakmp
set peer 10.2.0.2
set transform-set TS-S2S-VPN
match address VPN-TRAFFIC
!
!
!
!
interface Tunnel0
ip address 172.16.0.1 255.255.255.0
zone-member security S2SVPN
tunnel source 200.1.0.2
tunnel destination 10.2.0.2
tunnel protection ipsec profile IPSEC-S2S-
VPN
!
interface Ethernet0/0
no ip address
shutdown
!
interface Ethernet0/1
no ip address
!
interface Ethernet0/1.100
description LAN_Server
encapsulation dot1Q 100
ip address 200.1.1.14 255.255.255.240
ip helper-address 200.0.0.1
zone-member security DMZ
!
interface Ethernet0/1.101
description LAN_Server
encapsulation dot1Q 101
ip address 200.1.2.14 255.255.255.240
ip helper-address 200.0.0.1
!
interface Ethernet0/2
no ip address
!
interface Ethernet0/2.10
description LAN_B_IT
encapsulation dot1Q 10
ip address 194.0.0.14 255.255.255.240
ip helper-address 200.0.0.1
zone-member security LAN
!
interface Ethernet0/2.50
description AD_SERVER
encapsulation dot1Q 50
ip address 200.0.0.14 255.255.255.240

ip helper-address 200.0.0.1
zone-member security AD
!
interface Ethernet0/2.99
description LAN_MGMT
encapsulation dot1Q 99
ip address 194.0.1.14 255.255.255.240
ip helper-address 200.0.0.1
zone-member security MGMT
!
interface Ethernet0/3
no ip address
shutdown
!
interface Ethernet1/0
no ip address
shutdown
!
interface Ethernet1/1
no ip address
shutdown
!
interface Ethernet1/2
no ip address
shutdown
!
interface Ethernet1/3
no ip address
shutdown
!
interface Serial2/0
description LINK_TO_R_WEST
ip address 200.1.0.2 255.255.255.252
zone-member security INTERNET
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7
031E5C1F1504314D5D1A
serial restart-delay 0
crypto map IPSEC-SITE-TO-SITE-VPN
!
interface Serial2/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial2/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial2/3
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/0
description LINK_TO_R_Dep_Finance
ip address 200.3.0.1 255.255.255.252
zone-member security INTERNET
ip ospf message-digest-key 1 md5 7
010901104800160E325F
serial restart-delay 0
!

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		71


```

!
!
ip dhcp excluded-address 195.0.1.14
!
ip dhcp pool LAN_D_Guests
network 195.0.1.0 255.255.255.240
default-router 195.0.1.14
dns-server 195.0.1.14 8.8.8.8
!
!
!
ip domain name zgtsk.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$ioEo$A0dBkZuDHT1N8SFHkS1Ef0
!
redundancy
!
!
ip ssh version 2
!
class-map type inspect match-all LAN-
ADMIN
match access-group name LAN_ADMINs
class-map type inspect match-any LAN-
PROTOCOLS
match protocol icmp
match protocol dns
match protocol ftp
match protocol https
match protocol http
match protocol tcp
match protocol udp
class-map type inspect match-any
INTERNET-PROTOCOLS
match protocol https
match protocol http
match protocol dns
!
policy-map type inspect GUEST-TO-
INTERNET-POLICY
class type inspect INTERNET-
PROTOCOLS
inspect
class class-default
drop
policy-map type inspect LAN-TO-
INTERNET-POLICY
class type inspect LAN-PROTOCOLS
inspect
class class-default
drop
policy-map type inspect INTERNET-TO-
LAN-POLICY
class type inspect LAN-ADMIN
inspect
class class-default
drop
!
zone security INTERNET
zone security LAN
zone security GUEST
zone-pair security ZP-GUEST-TO-
INTERNET source GUEST destination INTERNET
service-policy type inspect GUEST-TO-
INTERNET-POLICY
zone-pair security ZP-LAN-TO-INTERNET
source LAN destination INTERNET
service-policy type inspect LAN-TO-
INTERNET-POLICY
zone-pair security ZP-INTERNET-TO-LAN
source INTERNET destination LAN
service-policy type inspect INTERNET-
TO-LAN-POLICY
!
!
!
!
!
!
interface Ethernet0/0
no ip address
shutdown
!
interface Ethernet0/1
no ip address
shutdown
!
interface Ethernet0/2
no ip address
!
interface Ethernet0/2.10
description LAN_C
encapsulation dot1Q 10
ip address 195.0.0.14 255.255.255.240
ip helper-address 200.0.0.1
zone-member security LAN
!
interface Ethernet0/2.20
description LAN_D_Guests
encapsulation dot1Q 20
ip address 195.0.1.14 255.255.255.240
zone-member security GUEST
!
interface Ethernet0/3
no ip address
shutdown
!
interface Ethernet1/0
no ip address
shutdown
!

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		73

```

interface Ethernet1/1
no ip address
shutdown
!
interface Ethernet1/2
no ip address
shutdown
!
interface Ethernet1/3
no ip address
shutdown
!
interface Serial2/0
description LINK_TO_R_WEST
ip address 200.2.0.2 255.255.255.252
zone-member security INTERNET
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7
061C08355F4519181604
serial restart-delay 0
!
interface Serial2/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial2/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial2/3
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/0
description LINK_TO_R_Dep_IT
ip address 200.3.0.2 255.255.255.252
zone-member security INTERNET
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7
140D151F1F0F3A2A373B
serial restart-delay 0
!
interface Serial3/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/3
no ip address
shutdown
serial restart-delay 0
!
router ospf 1
area 1 authentication message-digest
passive-interface Ethernet0/2

```

```

passive-interface Ethernet0/2.10
passive-interface Ethernet0/2.20
network 195.0.0.0 0.0.0.15 area 1
network 195.0.1.0 0.0.0.15 area 1
network 200.2.0.0 0.0.0.3 area 1
network 200.3.0.0 0.0.0.3 area 1
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
ip access-list extended LAN_ADMINS
permit ip 194.0.1.0 0.0.0.15 any
permit ip 200.0.0.0 0.0.0.15 any
!
logging trap notifications
logging origin-id hostname
logging host 200.0.0.1
!
!
!
control-plane
!
!
!
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh
transport output ssh
!
!
end

R_WEST:

R_WEST#show start
Using 2785 out of 32768 bytes
!
! Last configuration change at 12:58:17
UTC Thu Jun 16 2022
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R_WEST
!
boot-start-marker
boot-end-marker
!
!

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		74

```

enable secret 5
$1$SRSt$uXGnDTVDa5vnKIOZme2.41
!
aaa new-model
!
!
!
!
!
!
!
aaa session-id common
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no ip icmp rate-limit unreachable
!
!
!
!
!
!
no ip domain lookup
ip domain name zgtsk.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
username admin privilege 15 secret 5
$1$bHqH$D.dfgOO4kysbVqVCtkKFk0
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh version 2
!
!
!
!
!
!
!
interface Ethernet0/0
no ip address
shutdown
!
interface Ethernet0/1
no ip address
shutdown
!
interface Ethernet0/2

```

```

no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
interface Ethernet1/0
no ip address
shutdown
!
interface Ethernet1/1
no ip address
shutdown
!
interface Ethernet1/2
no ip address
shutdown
!
interface Ethernet1/3
no ip address
shutdown
!
interface Serial2/0
description LINK_TO_R_Global_1
ip address 10.1.0.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7
1100171112000509103A2A373B
serial restart-delay 0
!
interface Serial2/1
description LINK_TO_R_Dep_IT
ip address 200.1.0.1 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7
131F10061807142B3837
serial restart-delay 0
!
interface Serial2/2
description LINK_TO_R_Dep_Finance
ip address 200.2.0.1 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7
0956491D0A0E0713181F
serial restart-delay 0
!
interface Serial2/3
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/0
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial3/2

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		75

```

no ip address
shutdown
serial restart-delay 0
!
interface Serial3/3
no ip address
shutdown
serial restart-delay 0
!
router ospf 1
area 0 authentication message-digest
area 1 authentication message-digest
network 10.1.0.0 0.0.0.3 area 0
network 200.1.0.0 0.0.0.3 area 1
network 200.2.0.0 0.0.0.3 area 1
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
logging trap notifications
logging origin-id hostname
logging host 200.0.0.1
!
!
!
!
!
control-plane
!
!
!
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
access-class LAN_ADMINS in
exec-timeout 60 0
logging synchronous
transport input ssh
transport output ssh
!
!
end

R_EAST:

R_EAST#show start
Using 5164 out of 32768 bytes
!
! Last configuration change at 23:49:13
UTC Wed Jun 15 2022
!
version 15.4

```

```

service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R_EAST
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$0Oyc$PddMxKpWx9jm/Pq9sZiCo1
!
aaa new-model
!
!
!
!
!
aaa session-id common
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
!
ip dhcp excluded-address 199.0.1.1
!
ip dhcp pool LAN_E_Prod
network 199.0.1.0 255.255.255.240
default-router 199.0.1.1
dns-server 200.0.0.1 8.8.8.8
!
!
!
!
ip domain name zgtsk.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
username admin privilege 15 secret 5
$1$YgrZ$Q.XTM4zy2ik.qh5tDZnLa.
!
redundancy
!
!
ip ssh version 2
!
class-map type inspect match-all LAN-
ADMIN
match access-group name LAN_ADMINS
class-map type inspect match-any LAN-
PROTOCOLS
match access-group name ISAKMP_IPSEC
match protocol icmp

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		76

```

match protocol dns
match protocol ftp
match protocol https
match protocol http
match protocol tcp
match protocol udp
class-map type inspect match-all IPSEC-
POLICY
    match access-group name ISAKMP_IPSEC
    !
    policy-map type inspect LAN-TO-
INTERNET-POLICY
        class type inspect LAN-PROTOCOLS
        inspect
        class class-default
        drop
    policy-map type inspect INTERNET-TO-
SELF-POLICY
        class type inspect IPSEC-POLICY
        pass
        class class-default
        drop
    policy-map type inspect S2SVPN-POLICY
        class type inspect LAN-PROTOCOLS
        inspect
        class class-default
        drop
    policy-map type inspect INTERNET-TO-
LAN-POLICY
        class type inspect LAN-ADMIN
        inspect
        class class-default
        drop
    !
    zone security INTERNET
    zone security LAN
    zone security S2SVPN
    zone-pair security ZP-LAN-TO-INTERNET
source LAN destination INTERNET
    service-policy type inspect LAN-TO-
INTERNET-POLICY
    zone-pair security ZP-INTERNET-TO-LAN
source INTERNET destination LAN
    service-policy type inspect INTERNET-
TO-LAN-POLICY
    zone-pair security ZP-INTERNET-TO-
SELF source INTERNET destination self
    service-policy type inspect INTERNET-
TO-SELF-POLICY
    zone-pair security ZP-LAN-TO-S2SVPN
source LAN destination S2SVPN
    service-policy type inspect S2SVPN-
POLICY
    zone-pair security ZP-S2SVPN-TO-LAN
source S2SVPN destination LAN
    service-policy type inspect INTERNET-
TO-LAN-POLICY
    !
    !
    !
    !
    !
    crypto isakmp policy 1

```

```

encr 3des
authentication pre-share
group 2
crypto isakmp key zgtskpass address
200.1.0.2
!
!
crypto ipsec transform-set TS-S2S-VPN
esp-aes esp-sha-hmac
mode transport
!
crypto ipsec profile IPSEC-S2S-VPN
set security-association lifetime seconds
86400
set transform-set TS-S2S-VPN
!
!
!
crypto map IPSEC-SITE-TO-SITE-VPN 10
ipsec-isakmp
set peer 200.1.0.2
set transform-set TS-S2S-VPN
match address VPN-TRAFFIC
!
!
!
!
interface Tunnel0
ip address 172.16.0.2 255.255.255.0
zone-member security S2SVPN
tunnel source 10.2.0.2
tunnel destination 200.1.0.2
tunnel protection ipsec profile IPSEC-S2S-
VPN
!
interface Ethernet0/0
description
LINK_TO_SW_Dep_Production
ip address 199.0.1.1 255.255.255.240
zone-member security LAN
!
interface Serial2/0
description LINK_TO_R_Global_3
ip address 10.2.0.2 255.255.255.252
zone-member security INTERNET
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7
060F0135495C071C110713181F
serial restart-delay 0
crypto map IPSEC-SITE-TO-SITE-VPN
!
interface Serial2/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial2/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial2/3

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		77

0.0.0.15

SW_Dep_IT:

```

SW_Dep_IT>en
Password:
SW_Dep_IT#show start
Using 1344 out of 8192 bytes,
uncompressed size = 2446 bytes
!
! Last configuration change at 15:26:40
UTC Wed Jun 15 2022
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
service compress-config
!
hostname SW_Dep_IT
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$W1wz$CdWRHCZuHbrTXXhu9IOXz1
!
username admin privilege 15 secret 5
$1$v/n4$OkN5aDGEuCud3jHO4NPB6/
aaa new-model
!
!
!
!
!
!
aaa session-id common
!
!
!
!
!
!
no ip domain-lookup

```

		<i>В.Загацький</i>			<i>КІК.КР.Б – 123 – 12 – ПЗ</i>	<i>Арк.</i>
		<i>І. Панаріна</i>				
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<i>78</i>

```

ip domain-name zgtsk.com
ip cef
no ipv6 cef
!
!
errdisable recovery cause psecure-violation
errdisable recovery interval 500
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
switchport nonegotiate
!
interface Ethernet0/1
switchport access vlan 10
switchport mode access
switchport nonegotiate
!
interface Ethernet0/2
switchport access vlan 10
switchport mode access
switchport nonegotiate
!
interface Ethernet0/3
switchport access vlan 10
switchport mode access
switchport nonegotiate
!
interface Ethernet1/0
switchport access vlan 10
switchport mode access
switchport nonegotiate
!
interface Ethernet1/1
switchport access vlan 10
switchport mode access
switchport nonegotiate
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
switchport access vlan 99
switchport mode access
switchport nonegotiate
switchport port-security mac-address sticky
switchport port-security
!
interface Ethernet2/1
!
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
switchport access vlan 50
switchport mode access
switchport nonegotiate
switchport port-security mac-address sticky
switchport port-security
!
interface Vlan10
description LAN_B
ip address 194.0.0.13 255.255.255.240
!
interface Vlan50
description LAN_S
ip address 200.0.0.13 255.255.255.240
!
interface Vlan99
description LAN_MGMT
ip address 194.0.1.13 255.255.255.240
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip ssh version 2
!
!
logging trap notifications
logging origin-id hostname
logging host 200.0.0.1
!
!
!
!
!
control-plane
!
!
line con 0
logging synchronous
line aux 0
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh
transport output ssh
!
!
end

```

		В.Загацький			КІК.КР.Б – 123 – 12 – ПЗ	Арк.
		І. Панаріна				
Змн.	Арк.	№ докум.	Підпис	Дата		79