Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних систем та технологій
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра
(бакалавра, спеціаліста, магістра)

студента Сафонова Леоніда Вадимовича
(ПІБ)
академічної групи 123-17ск-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

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

на тему «Комп'ютерна система компанії "Эвропа-Днепр" з детальним опрацюванням міграції локальних структур баз даних на платформу Microsoft SQL Azure»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	ас. Панферова Я.В.			
розділів:				
апаратний розділ	доц. Ткаченко С.М.			
розрахунок мережі	ас. Панферова Я.В.			
економічний розділ	ст. викл. Яремчук І.О.			
охорона праці	доц. Іконніков М.Ю.			
Рецензент				
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
__інформаційних систем_
_____та технологій__ ___
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

«_27_» _січня___2020 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Сафонов Л.В. **академічної групи** 123-17ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

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

на тему «Комп'ютерна система компанії "Эвропа-Днепр" з детальним опрацюванням міграції локальних структур баз даних на платформу Microsoft SQL Azure»

затверджену наказом ректора НТУ «Дніпровська політехніка» від №

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати завдання, конкретизувати предмет та мету роботи	10.05.2020
Технічні вимоги до комп'ютерної системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи	17.05.2020
Спеціальна частина	Розв'язати завдання з розробки комп'ютерної системи з опрацюванням побудови і захисту інформації та налаштуванням корпоративної мережі	24.05.2020
Економічна частина	Економічно обґрунтувати доцільність витрат на створення та дослідження системи керування	30.06.2020
Охорона праці	Розробити організаційно-технічні заходи, щодо реалізації правил безпеки при експлуатації системи	1.06.2020

Завдання видано _____ ас. Панферова Я.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі _27 січня_2020 р._

Дата подання до екзаменаційної комісії 10.06.2020 р.

Прийнято до виконання _____ Сафонов Л.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 79 с., 42 рис., 7 табл., 3 додаток, 4 джерела.

Об’єкт розробки: Комп’ютерна система компанії “Эвропа-Днепр” з детальним опрацюванням міграції локальних структур баз даних на платформу Microsoft SQL Azure.

Мета: Міграція локальних структур баз даних на платформу Microsoft SQL Azure.

Розробка комп’ютерної системи з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову систем роботи з програмою 1с, а також для зн иження початкових витрат на розгортання системи та при її модернізації.

Система виконана відкритою і дозволяє здійснювати технічну і програмну модернізацію системи, а так само забезпечує виконання наступних функцій:

– Доступ до даних з будь якої точки світу де є доступ до інтернету;

– Збільшення надійності зберігання інформації;

– Зменшення витрат на електроенергію та оренду приміщень.

Розробка комп’ютерної мережі виконана відповідно до завдання на дипломну роботу бакалавра.

Розроблена схема мережі реалізована за допомогою порталу MS Azure. Робота протестована за допомогою програми 1с:Підприемство.

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

УМОВНІ ПОЗНАЧЕННЯ

MS – Microsoft

AWS – Amazon Web Service

VPN – Vitual Private Network

SSTP – Secure Socket Tunneling Protocol

IKEv2 – Internet Key Exchange version 2

ЗМІСТ

ВСТУП

Робота містить характеристику та аналіз діяльності салон-магазину “Європа-Дніпро”.

Актуальність даної роботи обумовлена виробничою необхідністю в зв’язку з відкриттям нового магазину та подальшого розвитку комп’ютерної системи компанії. Об'єднання територіально віддалених офісів компанії в єдину телекомунікаційну мережу значно підвищить ефективність та швидкість взаємодії віддалених підрозділів.

Мета роботи - вивчити хмарні сервіси для автоматизації бізнесу і обгрунтувати переваги переходу на хмарну обробку даних.

Головним завданням є перенесення бази даних до хмарної платформи . Для досягнення поставленої мети необхідно вирішити такі завдання:

– привести опис компанії та його інформаційних потоків;

– розглянути основні недоліки в організації корпоративної мережі;

– сформувати вимоги до перенесення інформації до хмарної платформи

Практична значимість роботи полягає в можливості впровадження результатів модернізації не тільки в даному салон-магазині, а при деяких масштабуваннях і на будь-якому іншому підприємстві, що має в своєму складі територіально віддалені підрозділі.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика та аналіз діяльності салон-магазину «Європа-Дніпро»

Салон-магазин «Європа-Дніпро» знаходиться за адресою: м. Дніпро, пр. Д.Яворницького, 111. Повне найменування юридичної особи: товариство з обмеженою відповідальністю «Європа-Дніпро». Було зареєстровано в 2016 році.

Компанія займається наступними видами діяльності:

основний:

– 47.78 Інші види роздрібної торгівлі новими товарами в спеціалізованих магазинах;

інші:

– 46.73 Оптова торгівля лісоматеріалами, будівельними матеріалами та сантехнічним обладнанням;

– 46.90 Неспеціалізована оптова торгівля;

– 47.19 Інша роздрібна торгівля в неспеціалізованих магазинах;

– 47.52 Роздрібна торгівля залізними виробами, лакофарбовими матеріалами і склом в спеціалізованих магазинах;

– 47.59 Роздрібна торгівля меблями, освітлювальним обладнанням та іншими побутовими речами в спеціалізованих магазинах;

– 68.20 Оренда і управління власною або орендованої нерухомістю- основний вид діяльності компанії.

«Європа-Дніпро» є офіційним представником елітного Іспанського концерну PORCELANOSA. PORCELANOSA вже 45 років є PORCELANOSA є лідером в сфері виробництва для підлоги та стін керамічної плитки. Відмінні характеристики компанії - висока технологія, інноваційний дизайн і чудова якість. До складу концерну PORCELANOSA входять компанії VENIS, GAMADECOR, SYSTEMPOOL, L'ANTIC COLONIAL, BUTECH, NOKEN, URBATEK, які пропонують велику гаму

продукції, від обладнання для кухонь і ванних кімнат до передових конструктивних рішень для сучасної архітектури.

Салон «Європа-Дніпро» пропонує більше 50000 видів кахлю підлогового і настінного, всіх кольорів і розмірів. Представлена продукція більше 20 фабрик Іспанії, Італії, 5 фабрик Польщі, 2 фабрики Китаю, України. Також в наявності є керамо-граніт, грес, кахель для ванної кімнати і басейну. Компанія працює і в роздріб і оптом з великими будівельними компаніями, включаючи послуги ванних кімнат під ключ не тільки за готовими ескізами, а й з можливістю розробки індивідуального дизайн-проекту.

Основними клієнтами компанії є архітектори, дизайнери інтер'єрів, проектні відділи, колективи та архітектурні майстерні.

1.2 Організаційна структура салон-магазину «Європа-Дніпро»

Організаційна структура ТОВ «Європа-Дніпро» є лінійно-функціональною. На даний час компанія представлена одним магазином в м. Дніпро. Планується влітку відкриття нового магазину в м. Харків.

Компанія є невеликою організацією, з чіткою системою єдиноначальності, чітко висловленої відповідальністю кожного працівника та його функціями. Організаційна структура представлена на рисунку 1.1, в філіалі планується аналогічна структура.

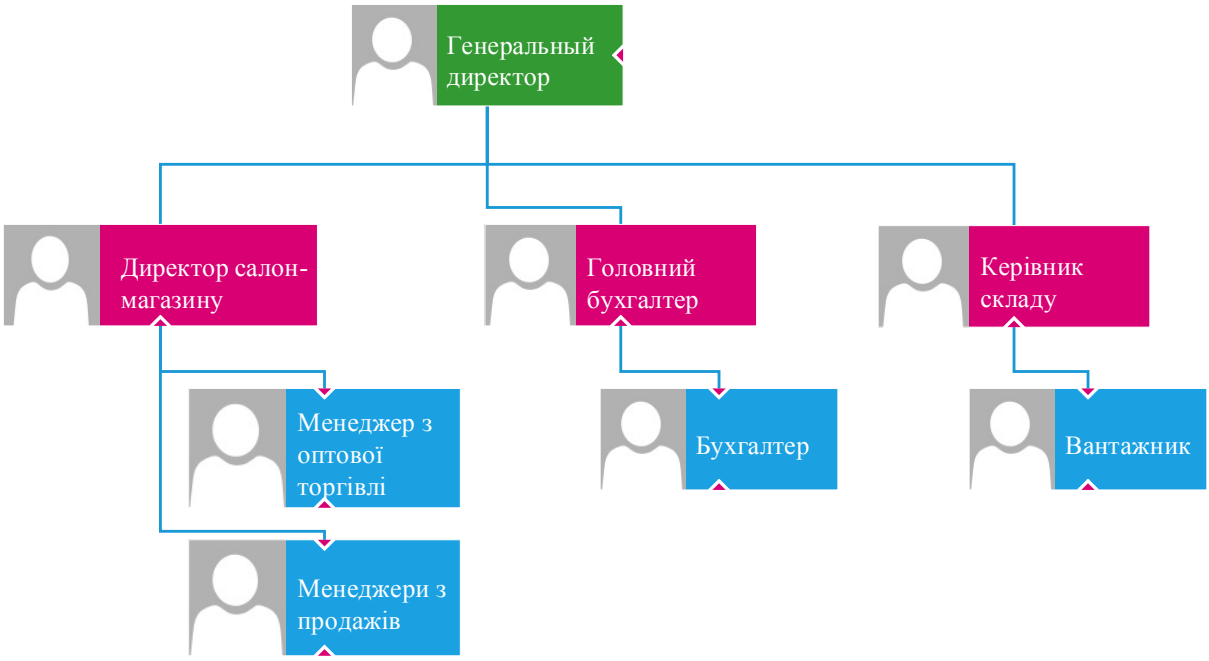


Рисунок 1.1 – Організаційна структура салон-магазину «Європа-Дніпро»

При такій структурі працівники магазину безпосередньо підпорядковуються одному керівнику. Лінійно-функціональна організація передбачає відносну автономність в роботі. Даний тип організаційної структури характеризується в цілому простотою, одномірністю зв'язків (тільки вертикальні зв'язки).

Переваги:

– високий ступінь спеціалізації;

– ясний порядок підпорядкованості;

– чітке розуміння відповідальності;

– висока ефективність і швидкість;

– відсутність необхідності в дублюванні роботи;

– всі функції однаково важливі.

Недоліки:

– комунікація стикається з декількома бар'єрами;

– у центрі уваги знаходяться люди, а не організація;

– рішення, прийняті єдиною людиною, можуть не завжди йти на користь організації;

– у міру зростання компанії стає важче здійснювати контроль над діями всередині неї;

– відсутність командної роботи між різними відділами або одиницями;

– оскільки всі функції відокремлені, співробітники можуть не знати про те, що твориться у колег.

1.3 Аналіз корпоративної мережі компанії

По факту компанія орендує приміщення для салон-магазину та складські приміщення внаслідок невеликої кількості співробітників. На схемі умовно позначені територіально віддалені об'єкти.

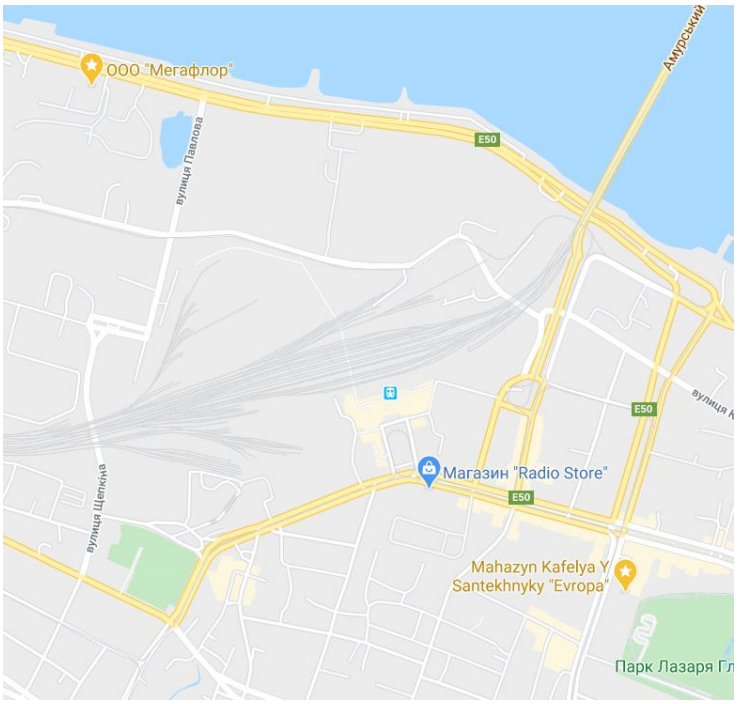


Рисунок 1.2 – Геграфічне розташування структурних підрозділів ТОВ «Європа-Дніпро»

Магазин знаходиться в одноповерховій будівлі. Внутрішні стіни зроблені з гіпсокартону. Стеля підвісна армстронг. В приміщенні 4 виставочні зали, кабінет директора, кухня, 2 туалети, 2 комори (рис. 1.3). Загальна площа складає близько 450 м^2.

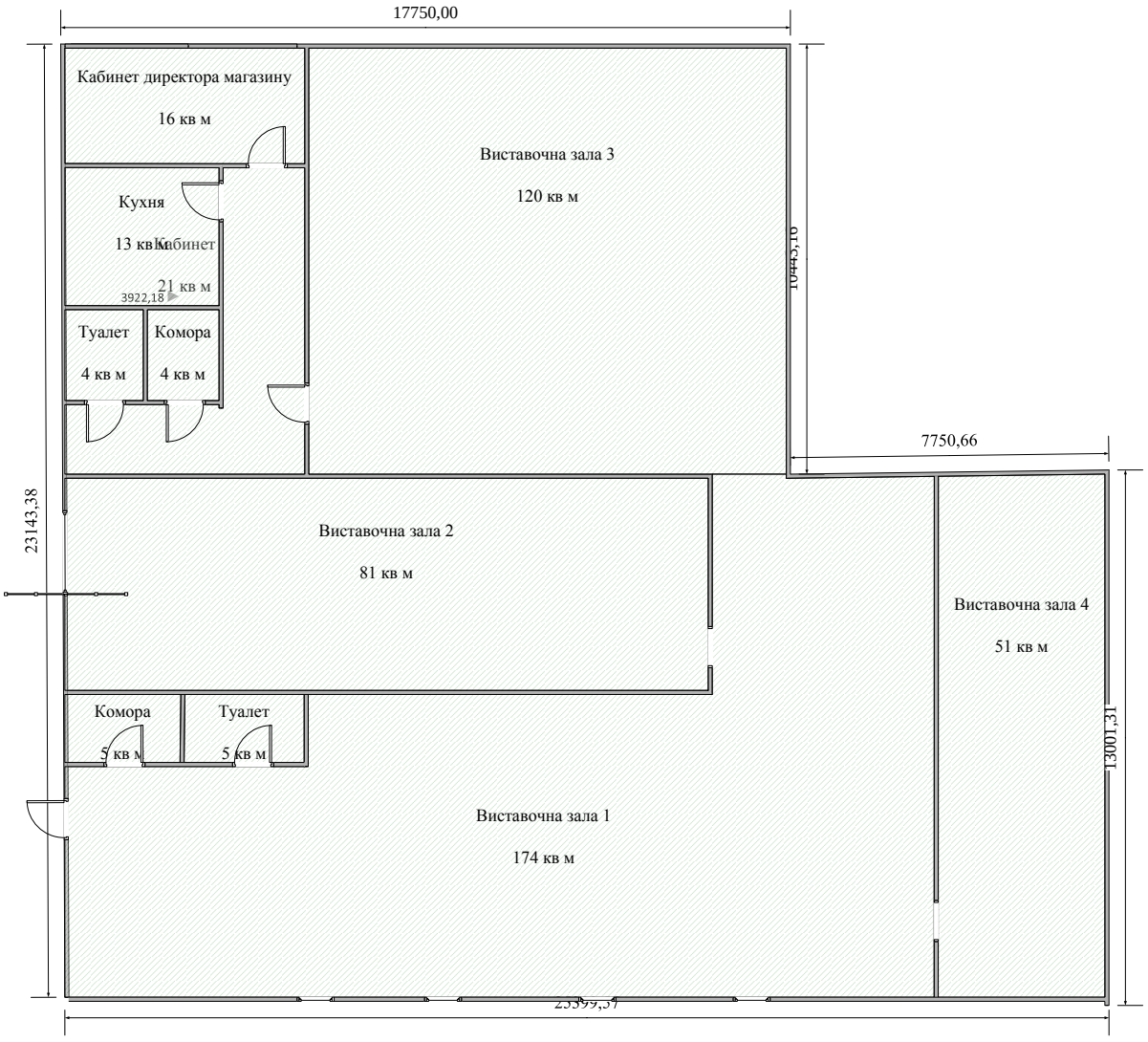


Рисунок 1.3 – План салон-магазину

Локальна мережа в магазині побудована за технологією FastEthernet і з використання кабелю категорії 5е. Застосовано мережне обладнання:

– маршрутизатор MikroTik hAP Lite TC (RB941-2nD-TC), який забезпечує вихід в інтернет на швидкості до 100 Мбіт/с;

– некерований комутатор D-Link DGS-1024A, що забезпечую підключення кінцевих користувачів, принтерів та локальної мережі за технологією FastEtrnet на швидкості 100Мб/с;

– 9 ноутбуків працівників магазину;

– файл-сервер, на якому ще встановлено сервер бази даних 1С магазину.

Працівники магазину під’єднуються до в мережі за технологією Wi-Fi.

На основі зібраних даних побудуємо таблицю використовуваних основних технічних засобів в салон-магазині «Європа-Дніпро (таблиця 1.1).

Таблиця 1.1 – Основні технічні засоби

Група засобів	Засоби	Кількість
ПК	Ноутбук директора магазина	1
	Ноутбук менеджера по роботі з клієнтами	4
	Ноутбук менеджера з оптової торгівлі	1
	Ноутбук головного бухгалтера	1
	Ноутбук бухгалтера	1
	Ноутбук касира	1
	Сервер	1
Мережне обладнання	Маршрутизатор Miktotik	1
	Комутатор D-Link DGS-1024A	2
Оборудование печати	Багато-функціональний пристрій	2
Інше обладнання	Джерело безперебійного живлення	2

Ноутбуки працівників мають різні характеристики, мінімум 2 Гб оперативної пам’яті, процесори сімейства Intel, ОС Windows 7.0.

На сервері встановлено ПЗ 1С.

Схема розташування технічних засобів на плані магазину надано на рис. 1.5.

Рисунок 1.4 – Схема розташування обладнання

В складі проведено доступ до Інтернет. Склад не має доступу до серверу 1С в магазині. Обмін інформацією між працівниками в магазині та працівниками на складі зазвичай виконується через Viber. Тому найбільш вимогливим до пропускної спроможності є відео-потік в режимі реального часу.

На даний час корпоративну мережу можна представити на рис. 1.4.

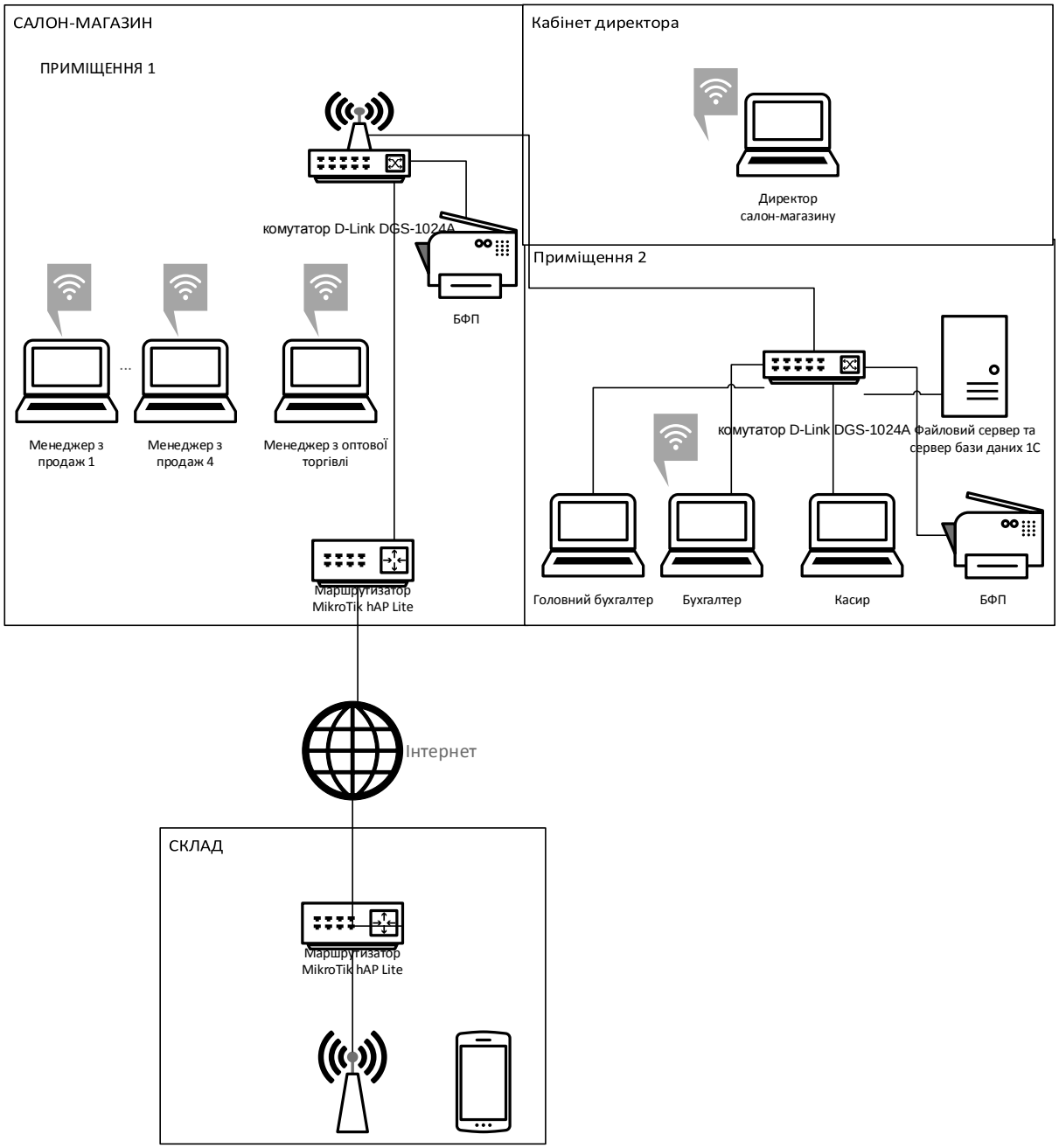


Рисунок 1.5 – Структурна схема мережі компанії

1.4 Особливості та проблеми функціонування мережі ТОВ «Європа-Дніпро»

Таким чином, поточна корпоративна мережа компанії має просту структуру, розраховану на невеликі навантаження і кількість користувачів.

При зборі інформації про працездатність мережі, були виявлені наступні особливості і проблеми:

– відсутнє захист від несанкціонованого доступу;

– застаріле обладнання серверу 1С, в наслідку чого зниження працездатності персоналу, а саме: повільне проведення документів, формування звітів, зниження швидкості завантаження самої програми;

– відсутня можливість коректного розподілу ресурсів мережі;

– необхідність налаштувати обмін нового філіалу магазину з центральним магазином, в якому розгорнуто сервер 1С.

На додаток до вищесказаного можна додати, що в випадку відкриття нового магазину в м. Харків необхідно налаштувати шифрований канал передачі даних через Інтернет до серверу та мережі магазину в м. Дніпро. А також виникає проблема зі збільшенням навантаження на сервер, в наслідок чого знизиться працездатність усіх філіалів магазину.

У зв’язку з вищеперерахованими недоліками було прийнято рішення щодо оновлення обладнання серверу для виправлення існуючих проблем і швидкого підключення магазину у новому місті до серверу 1С.[1]

1.5 Переваги хмарних рішень

Враховуючі усі недоліки які були перераховані у попередньому пункті одним з варіантів вирішення проблеми є перенесення серверу до хмарної платформи. Перевагами хмарних рішень є:

– Ефективність. Хмарні ресурси незалежні від обчислювальних систем і їх географічного розташування, яке немає потреби враховувати при роботі з ними. Це забезпечує істотну економію завдяки легкому масштабування ресурсів за потребами і одночасного повнішого їх завантаження.

– Безпека. Ресурси захищені не тільки за допомогою брандмауера і шифрування по периметру. Захист забезпечується також і на локальному рівні шляхом впровадження в віртуальні контейнери певних правил, що особливо важливо для найбільш значимої інформації.

– Гнучкість. З одного боку, всі ресурси, ПО і апаратне забезпечення можуть бути переконфігуровані в нові інформаційні системи і бізнес-

послуги практично миттєво. З іншого боку, обсяг технологічних ресурсів можна легко масштабувати в моменти пікових навантажень, а потім повернутися до попереднього рівня.

– Надійність. У «хмарі» реалізований достатній рівень резервування, при цьому на створення бекапа і відновлення за запитом виділяються необхідні ресурси. Завдання створення в своєму офісі резервних конфігурацій відпадає.

– Автоматизація. ПО для управління ресурсами «хмари» автоматично виконує свої функції, динамічно направляючи запитуваний обсяг ресурсів користувачеві для їх використання. Це призводить до зменшення кількості щоденних дій корпоративного IT-персоналу і більш точним запитам на надання ресурсів.

– Легкість доступу. Співробітникам, організаціям і процесам доступні набагато більше додатків, інформації, ресурсів і бізнес-послуг, ніж це може забезпечити «залізний» сервер під столом сисадміна. Як правило, доступ здійснюється через звичайний браузер.

– Оптимізація. «Хмара» управляється як єдина система, тому будь-хто отримує можливість істотної оптимізації використовуваних ресурсів за рахунок найкращого поєднання їх можливостей, продуктивності і вартості.

1.6 Мета роботи

У зв’язку з розширенням компанії «Європа-Дніпро» і відкриттям нового магазину у місті Харків, на основі вище наданої інформації, було прийнято рішення щодо оновлення серверів компанії для надання швидкого та безперебійного доступу до бази даних товарів. Для зменшення початкових витрат на переобладнання було вирішено перенести базу даних та сервер 1С: Підприємство на хмарне рішення.

1.7 Порівняння хмарних рішень

Під час проектування переносу даних до хмарних рішень вибір був між трьома постачальниками:

– Microsoft Azure;

– Amazon Web Services;

– Google Cloud.

Для порівння даних платфом були вибрані схожі конфігурації обладнання які наведенні нижче у таблиці 1.3.

Cloud	VmSize	Cores	Ram	Price\Hour
AWS	m4.xlarge	4	16GB	$0.406
Azure	StandardD3v2	4	14GB	$0.488
Google	n1standard4	4	15GB	$0.306

Таблиця 1.2 – Конфігурація обладнання на кожній з платформ

Як ми можемо бачити конфігурації максимально схожі між собою, але їхня ціни достатньо сильно відрізняються. Найдешевшою платформою є Google cloud.

Перший тест виконуємо за допомогою програми GeekBench. Ця програма дозволить нам побачити на скільки продуктивні процесори доступні нам у даних конфігураціях. Усі результати записані у таблиці 1.4. Чим більше цифра в тесті, тим краще.

Таблиця 1.3 – Результати тестування у програмі GeekBench

Cloud	GeekBench Score	Ціна за час	Perf Score / Ціна
AWS	6568.6	$0.406	16 177
Azure	9508.4	$0.422	22 530
Google	6188.2	$0.306	20 222

Результати багатоядерного тестування найцікавіші, так як платформа Azure випереджає конкурентів майже у півтора рази. Якщо подивимося

інформацію протестованих систем , ми можемо звернути увагу, що AWS і Google Cloud видають таку картину: Intel Xeon @ xxx GHz 1 processor, 2 cores, 4 threads, в той час як Azure дає «чесні» ядра: Intel Xeon E5-2673 v3 @ xxx GHz 1 processor, 4 cores.

Наступний тест виконуємо у програмі CrystalDiskMark. Ця програма дозволяє проаналізувати на скільки продуктивним є жорсткий диск. Результати приведені на двох графіках нижче (рисунок 1.6 та 1.7). Чим більше цифри в тестах, тим краще.

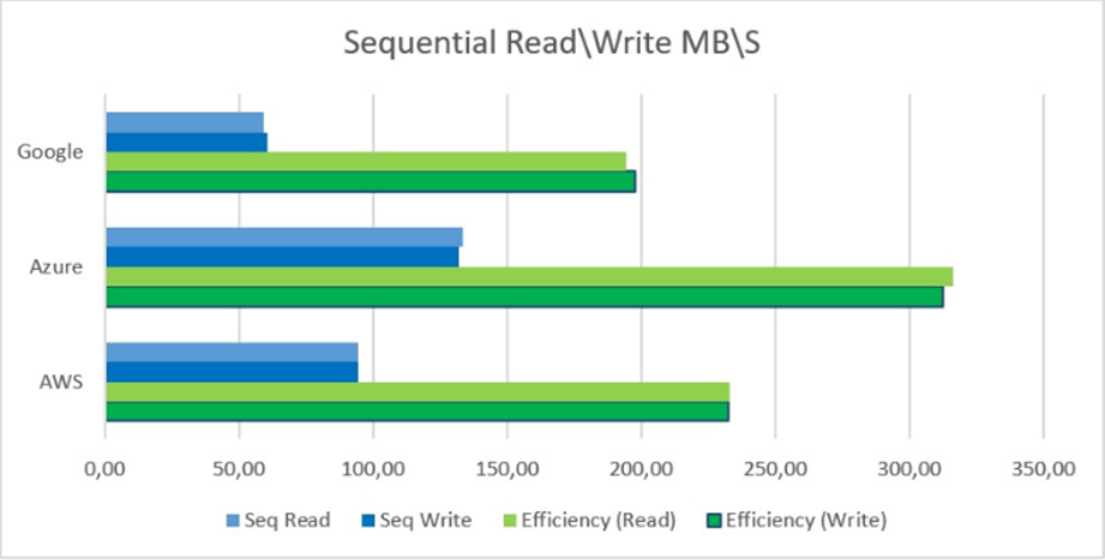


Рисунок 1.6 – Результати послідовного читання та запису інформації

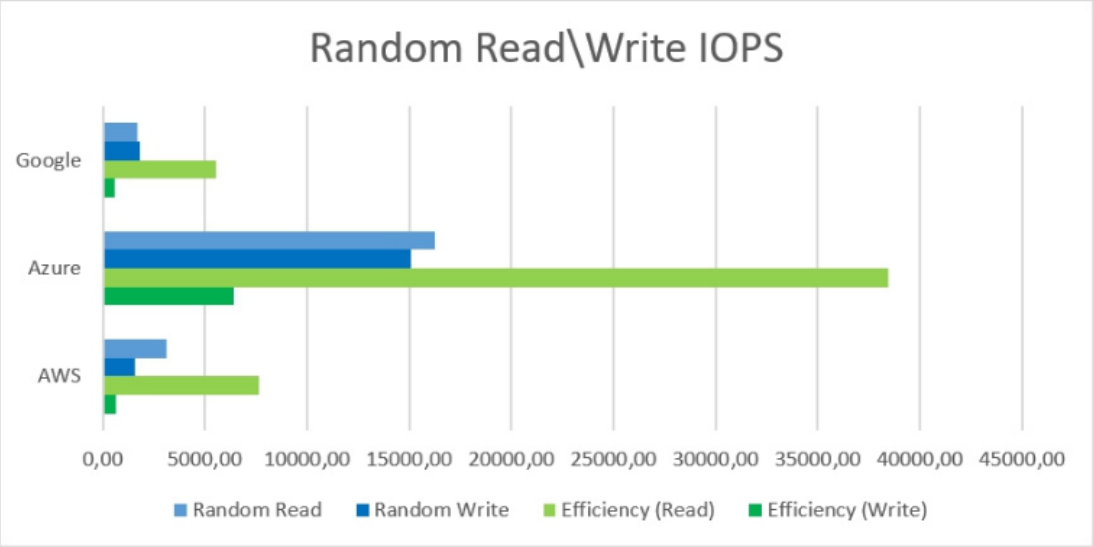


Рисунок 1.7 – Результати довільного читання та запису інформації

Результати CrystalDiskMark самі неоднозначні, але швидше за все така різниця зумовлена тим, що платформи Google Cloud \ AWS необхідно додатково конфігурувати для досягнення оптимальної продуктивності, в той час ,як Azure в конфігурації за замовчуванням показують хорошу продуктивність.

У даній конфігурації Azure залишив конкурентів далеко позаду за всіма показниками: послідовне читання \ запис, «рандом» 4к читання \ запис, «рандом» 4к читання \ запис з глибинної черзи рівній 32. Результат цікавий, тому що це машини за замовчуванням. Отже, це результат, який отримає середньостатистичний користувач.[2]

1.8 Вибір платформи для реалізації проекту

Після проведення тестів та враховуючи переваги описані нижче було прийнято рішення про використання Microsoft Azure я бази для вирішення поставленої задачі

Переваги завдяки яким вибір пар на Microsoft Azure:

– надання безкоштовно 200 доларів на 1 місяць та безкоштовне користування великою кількістю сервісів впродовж одного року;

– можливість проводити оплату по факту використання ресурсів продовж одного місяця;

– знижка у 49% на віртуальні машини та SQL-сервери при наявності існуючих ліцензій;

– велика кількість регіонів в яких знаходяться сервери;

– можливість налаштування розпорядку роботи серверів для оптимізації витрат;

– можливість об’єднання віртуальних машин у групи та адміністрування їх за допомогою Active Derictory;

– автоматичний бекап інформації за заданим розпорядком на серверах Azure або на фізичний жорсткий диск.

2 ФОРМУЛЮВАННЯ ТЕХНІЧНИХ ВИМОГ ДО КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Вимоги до структури і функціонування Системи

Нові робочі місця ЛВС повинні бути інтегровані в існуючу мережу і максимально використовувати наявні, власні, орендовані ресурси.

Локальна обчислювальна мережа повинна включати наступні компоненти:

– інформаційна кабельна підсистема з пропускною здатність 100 Мб / с;

– активне обладнання (комутатори, маршрутизатори);

– Інформаційна кабельна підсистема повинна будуватися відповідно до вимог стандарту ISO / IEC 11801 Class D, категорія 5E.

Загальна кількість автоматизованих робочих місць -10.

Максимальна довжина кабелю від інформаційного порту RJ45 до комутаційної панелі не повинна перевищувати 70м.

Локальна обчислювальна мережа в цілому повинна відповідати категорії не нижче 5E, всі комплектуючі (кабель, розетки, комутаційні панелі, з'єднувальні шнури) повинні відповідати категорії не нижче 5E.

Кожне автоматизоване робоче місце повинно складатися з інформаційної розетки RJ-45 в кількості 2 штуки.

Для створення локальної обчислювальної мережі необхідно використовувати тільки високоякісні компоненти, які пройшли стовідсоткове тестування відповідно до вимог ISO 9001 (ГОСТ 40.9001-88).

Всі кабельні системи локальної обчислювальної мережі повинні бути виконані з урахуванням вимог щодо фізичного захисту трас від пошкодження включають:

– прокладку кабелю за підвісною стелею, за гіпсокартонними стінами, в металевих лотках і в кабель-каналах.

– кріплення кабелю по всій трасі за допомогою спеціальних стяжок по всій довжині.

Обладнання ЛВС і схеми його з'єднань повинні забезпечувати подвійне резервування каналів передачі даних.

2.2 Вимоги до чисельності і кваліфікації персоналу, що обслуговує Систему і режиму його роботи

Наявність в штаті не менше 2-х фахівців, що мають вищу освіту ІТ спрямування та відповідні сертифікати по роботі з програмним забезпеченням з проектування, монтажу, проведенні пусконалагоджувальних робіт та програмуванню Системи, мають необхідні знання по налаштуванню мереж: маршрутизації брандмауера, а також мережевих служб: NetBIOS, DNS, NTP.

Крім цього фахівці повинні мати високий рівень кваліфікації і практичний досвід (не менше 5 (п’яти) років) виконання робіт по встановленню , налаштуванню та адмініструванню програмних і технічних засобів, що використовуються в програмному комплексі Системи.

Наявність в штаті для обслуговування у цілодобовому режимі Системи по місцю її дислокації не менше 3-х фахівців, що мають вищу освіту ІТ спрямування та досвід роботи з обслуговування, монтажу та тестування оптико-волоконних та мідних телекомунікаційних мереж, наявність обладнання для тестування мереж, комутаторів.

Наявність досвіду роботи в галузі проектування, поставці «під ключ» , роботи з оптико-волоконними мережами - не менше 5 (п’яти) років , реалізації територіально-розподілених систем IP-адресації – не менше 5 (п’яти) років.

2.3 Показники призначення

Система створюється для розширення кількості існуючих робочих місць і їх підключення в існуючу мережу, а також об’єднання мереж офісів двох будівель для підвищення працездатності обох.

Число портів активного обладнання повинно забезпечувати функціонування 100% автоматизованих робочих місць і мати додатковий запас не менше 20%. Обладнання повинно мати можливість для установки в 19 " комутаційну шафу.

2.4 Вимоги до надійності

Устаткування в складі локальної обчислювальної мережі повинно забезпечувати сталість фізичних характеристик каналу між портом активного обладнання і абонементські обладнанням незалежно від траси комутації на панелях перемикання розподільних вузлів.

Постійність фізичних параметрів каналу має забезпечуватися при наступних перекроссіровках незалежно від їх числа (але не більше визначеного виробником обладнання локальної обчислювальної мережі).

Розрив будь-якого каналу локальної обчислювальної мережі можливий тільки при комутації на панелях перемикання розподільних вузлів.

Використовувані в локальної обчислювальної мережі обладнання та матеріали не повинні допускати змін фізико-хімічних властивостей в результаті впливу навколишнього середовища протягом усього гарантійного терміну експлуатації за умови дотримання заданих виробником умов експлуатації.

У разі виходу з ладу будь-якого з каналів повинна забезпечуватися можливість переходу на використання альтернативного каналу з числа резервних за допомогою зміни з'єднань на панелях перемикання розподільних вузлів.

Обладнання повинно функціонувати 24 години на добу, 7 днів на тиждень, без урахування часу, необхідного для проведення регламентних робіт відповідно до рекомендацій виробника.

2.5 Вимоги безпеки

Обладнання та матеріали не повинні допускати можливості нанесення шкоди здоров'ю або ураження персоналу електричним струмом, або електромагнітними випромінюваннями за умови дотримання правил експлуатації обладнання

2.6 Вимоги до ергономіки та технічної естетики

Для реалізації проекту виконавець самостійно вибирає виробника кабельної системи. Тип і розмір кабель каналу для горизонтальної кабельної підсистеми повинен бути однаковий у всіх приміщеннях.

2.7 Вимоги до експлуатації, технічного обслуговування, ремонту і збереження компонентів Системи

Можливість обов’язкового реагування власними силами на порушення в роботі Системи протягом 2 (двох) годин.

Виконання регламентно-профілактичних робіт по підтримці Системи у робочому стані та її розвиток не менше ніж 2 рази на рік

Система електроживлення робочих місць ЛОМ призначена для підключення комп'ютерної техніки на робочих місцях СКС до електричної мережі 220В, 50Гц. Кожне робоче місце ЛВС має оснащуватися двома електричними розетками 220В, 50Гц з заземлюючим контактом.

Комп'ютерні розетки повинні відрізнятися за кольором від побутових або мати відповідне маркування.

Система електроживлення робочих місць ЛОМ є виділену розподільну електричну мережу 380 / 220В, 50Гц, яка підключається до

загальної системи електропостачання будівлі в центральному розподільному пристрої.

Система електроживлення повинна бути виконана по 5-ти провідний схемою (TN-C-S) в магістральної частини і по 3-провідній схемі в груповій частині.

Повинно бути передбачено рівномірний розподіл навантажень по фазах.

Електропостачання групових поверхових силових щитів повинно здійснюватися від головних розподільних щитів по радіальної схемі електропостачання. Щити встановлюються повністю комплектними. Конструктивне виконання щитів повинно забезпечувати виконання вимог безпеки і високий рівень надійності. У силових щитах забезпечити 30% резервування за місцем для можливості додаткової установки автоматичних вимикачів.

Передбачити підключення джерела безперебійного живлення, що забезпечує електроживлення мережевого і серверного (при наявності вільного місця) обладнання, що розміщується в комутаційній шафі, окремою лінією харчування і від окремого автоматичного вимикача. Для зручності підключення активного і телекомунікаційного устаткування в шафі необхідно передбачити електричні панелі, що підключаються до ДБЖ, з кількістю розеток, достатнім для підключення встановлюваного в шафі обладнання і запасом не менше 20% на розвиток.

Розподільні щити, автоматичні вимикачі, а також кабелі повинні мати сертифікати відповідності в системі ГОСТ Р і мати відповідне маркування.

Електричні кабелі повинні мати ізоляцію з матеріалів , які не розповсюджують горіння з низьким вмістом галогенів (маркування нг LS).

Заземлення елементів системи має відповідати вимогами глави 1.7 ПУЕ (7 видання).

Корпус комутаційної шафи СКС повинен бути заземлений окремим провідником безпосередньо з головною заземлення корпусу ВРУ.

Прокладання електричних кабелів здійснити в металевих лотках при прокладанні трас приховано за фальшпотолком або в кабельних каналах при відкритому прокладанні. У робочих кабінетах монтаж повинен бути виконаний в окремих секціях пластикових кабельних каналів спільно з СКС.

Розетки електроживлення і розетка СКС повинні встановлюватися на робочих місцях ЛВС в стандартні конструктивні елементи - супорти, рамки і т.д. і мати однаковий дизайн.

До початку робіт підрядник повинен розробити і узгодити з відповідальним за електрогосподарство ЛПУ однолінійну схему виділеної розподільчої системи електроживлення робочих місць ЛОМ, включаючи електроживлення комунікаційної шафи, надати розрахунок навантажень, поверхові плани кабельних трас і розміщення електрообладнання, таблицю кабельних з'єднань. У розрахунках прийняти, що електроспоживання одним робочим місцем ЛВС становить 350Вт. Сумарне електроспоживання комутаційної шафи прийняти в розмірі 3000Вт (з урахуванням додатково встановлюваного серверного обладнання).

Комплект запасних частин повинен бути переданий замовнику після виконання усіх робіт пов’язаних в встановленням і налаштуванням обладнання.

2.7 Вимоги до захисту інформації від несанкціонованого доступу

Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати

відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Доступ до серверної дозволений тільки для людей які працюють з обладнанням. Приміщення повинно закриватися на ключ, мати сигналізацію, та пульт керування останньою.

2.8 Вимоги до патентної чистоти

Усі роботи, а також обладнання не повинно порушувати патентні вимоги а також порушувати чинне законодавство у сфері захисту патентів

2.9 Вимоги до стандартизації й уніфікації

Застосувати уніфіковані типи кабелів і роз'ємів в рамках робочих місць, горизонтальної підсистеми, підсистем внутрішніх магістралей, а також розподільних вузлів, незалежно від типів підключається абонентського обладнання та активного обладнання різних підсистем.

2.10 Додаткові вимоги

Використання для реалізації проекту хмарної платформи Microsoft Azure.

Налаштувати, для коректної роботи програми, такі компоненти:

– Віртуальна машина на базі Windows Server 2019 з підключеним до неї Microsoft SQL;

– Віртуальну мережу для доступу до віртуальної машини;

– VPN для підвищення надійності доступу до інформації;

– 1с сервер;

– Налаштувати протоколи доступу.

2.11 Вимоги до технічного забезпечення

Віртуальна машина повинна мати такі характеристики:

– Процесор 4 ядра;

– Оперативної пам’яті не менше 8 гб;

– Твердотільний накопичувач (SSD) під систему на 127 Гб;

– 2 диски під SQL сервер по 1 ТБ кожний.

3 СПЕЦІАЛЬНА ЧАСТИНА

3.1 Розробка апаратної частини комп'ютерної системи

3.1.1 Створення віртуальної машини SQL Server 2017 на платформі Windows за допомогою порталу Azure.

3.1.1.1 Вибір образу віртуальної машини SQL Server

Для початку роботи потрібно увійти на портал Azure, використовуючи свої облікові дані. На порталі Azure в меню зліва Вибираю Azure SQL. Вибираю Додати, щоб відкрити сторінку вибору варіанту розгортання SQL. Далі Вибираю образ Free SQL Server License: SQL Server 2017 Developer on Windows Server 2016 (Безкоштовна ліцензія на SQL Server: SQL Server 2017 Developer на базі Windows Server 2016) в списку(Рисунок 1.6), і натискаю кнопку створити.

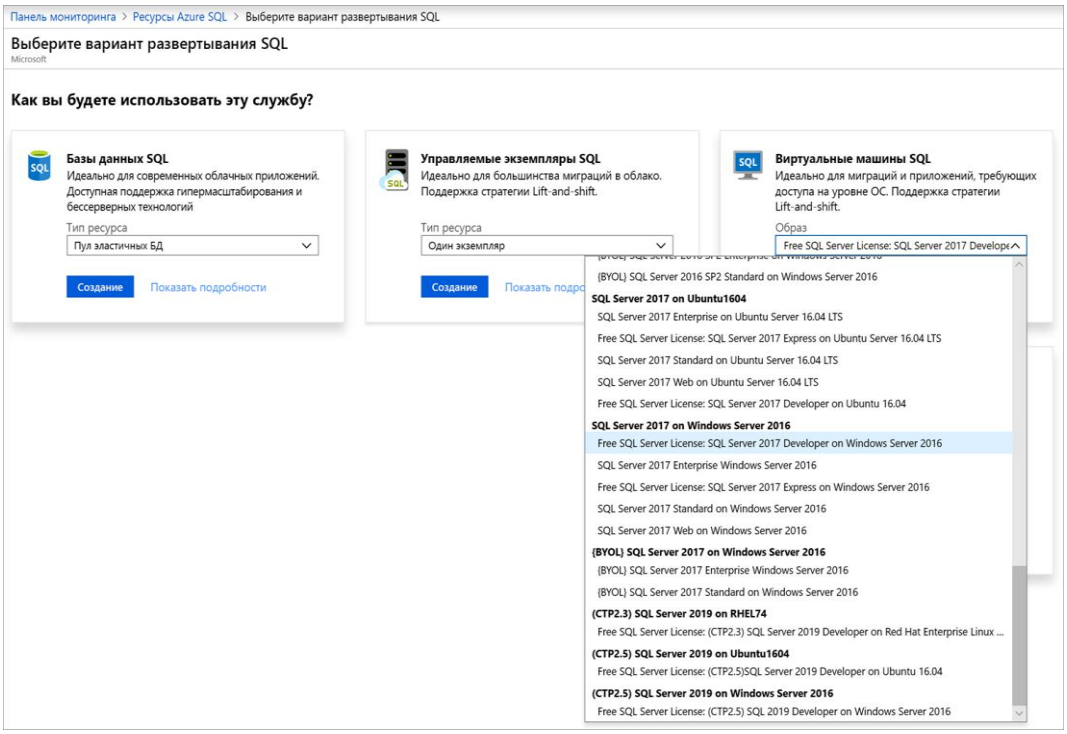


Рисунок 3.1 – Вибір варіанту розгортання SQL сервера

3.1.1.2 Вказівка основних відомостей.

На вкладці Основні відомості вказую наступну інформацію.

– Підписка Azure

– Група ресурсів(Рисунок 3.2)

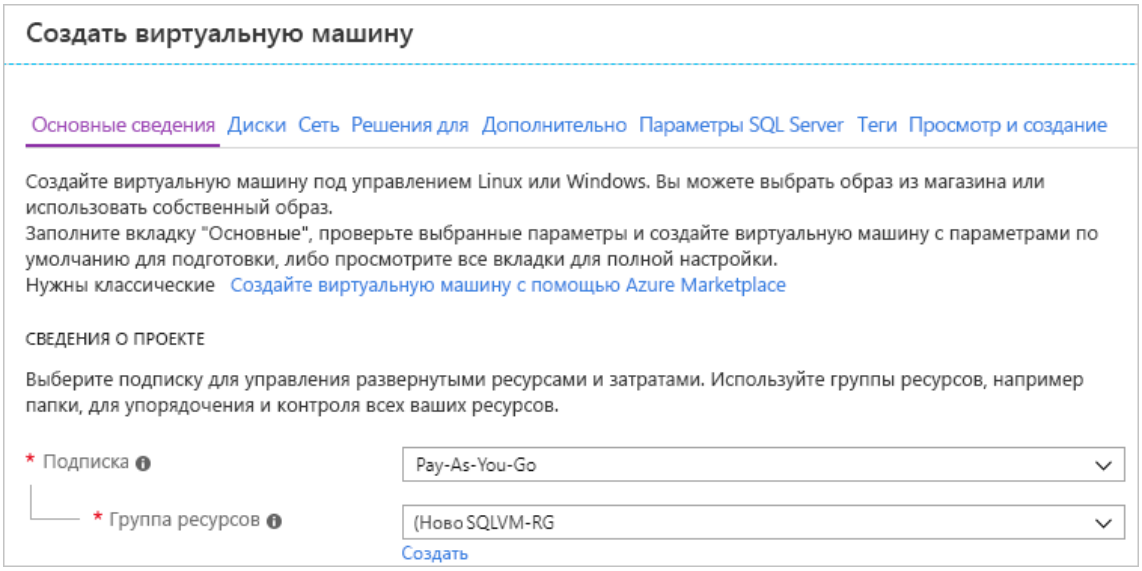


Рисунок 3.2 – Вибір підписки та групи ресурсів

– Ім'я віртуальної машини.

– Розташування для параметра Регіон.

– Надмірність інфраструктури.

– Образ Free SQL Server License: SQL Server 2017 Developer on Windows Server 2016 (Безкоштовна ліцензія на SQL Server: SQL Server 2017 Developer на базі Windows Server 2016).

– Розмір для параметра Розмір віртуальної машини(Рисунок 3.3).

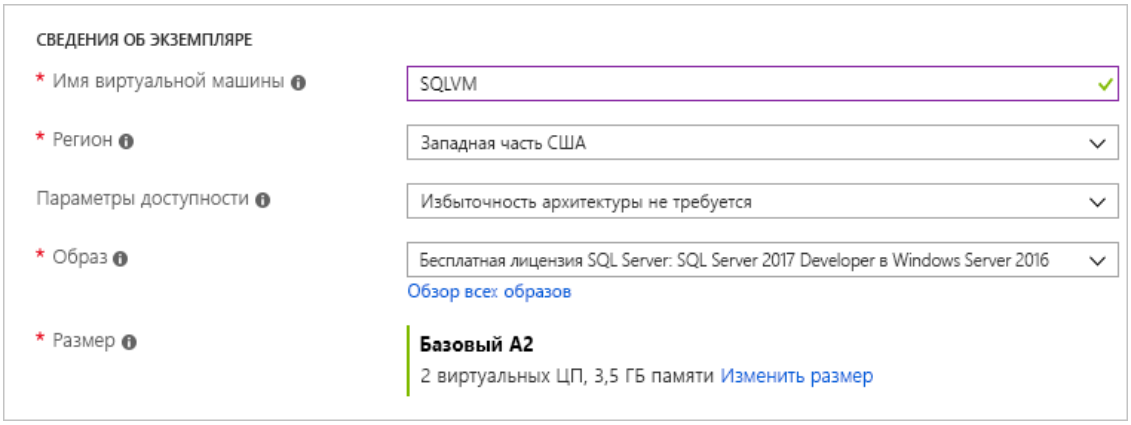


Рисунок 3.3 – Вибір ім’я, та основних параметрів віртуальної машини

– У розділі Обліковий запис адміністратора вказую ім'я користувача і пароль. Пароль повинен включати мінімум 12 символів і відповідати певним вимогам до складності(Рисунок 3.4).

Рисунок 3.4 – Створення облікового запису користувача

На вкладці Налаштування SQL Server налаштовую наступні параметри:

– У розділі Безпека і мережеві підключення Вибираю Загальнодоступний (Інтернет) для параметра Підключення SQL і змінюю порт на 1401, щоб не використовувати добре відомий номер порту в сценарії загальнодоступного підключення.

– У розділі Перевірка автентичності SQL - ввімкнути. Як ім'я для входу SQL вказані ім'я користувача і пароль, налаштовані для віртуальної машини.

– Усі інші налаштування залишаю за замовчуванням(Рисунок 3.5)

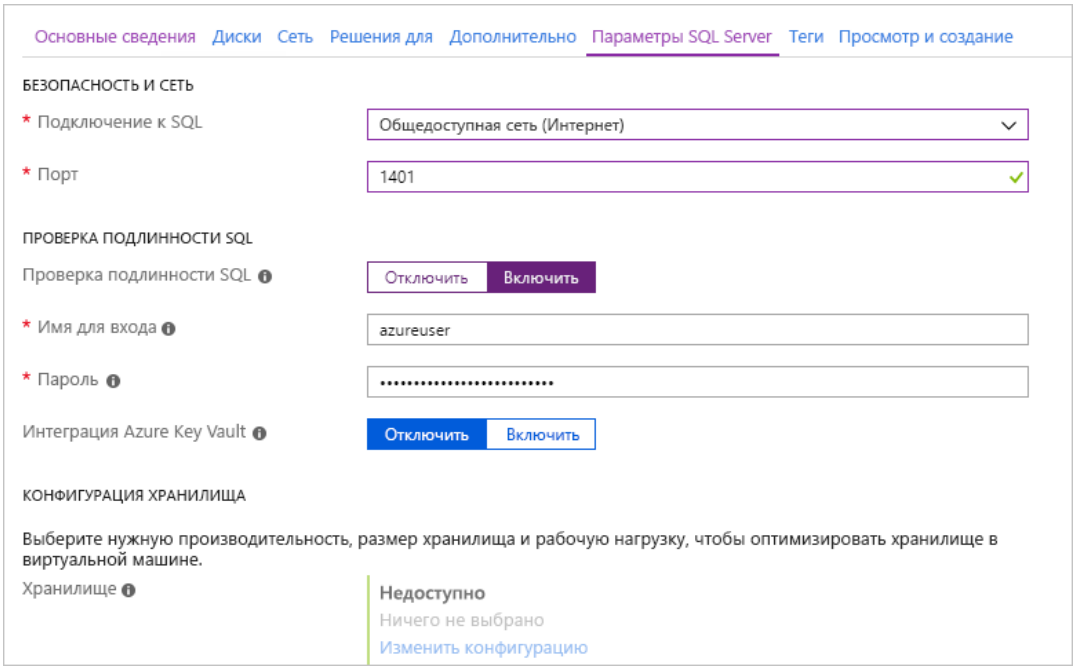


Рисунок 3.5 – Налаштування параметрів SQL сервера

На вкладці Відкликання та створення перевіряю зведені дані і натискаю Створити, щоб створити SQL Server, групу ресурсів і ресурси, зазначені для цієї віртуальної машини.

Розгортання можна відстежувати на порталі Azure. Якщо натиснути кнопку Повідомлення у верхній частині вікна, будуть показані основні відомості про стан розгортання. Розгортання може зайняти кілька хвилин.

3.1.1.3 Підключення до SQL Server

На порталі в розділі Огляд властивостей віртуальної машини знахожу загальнодоступний IP-адрес віртуальної машини SQL Server. На іншому комп'ютері, підключеному до мережі Інтернет, відкриваю SQL Server Management Studio (SSMS). У діалоговому вікні Підключення до сервера або Підключення до ядру СУБД змінюю значення Ім'я сервера. Ввожу загальнодоступну IP-адресу своєї віртуальної машини. Потім додаю кому і ввожу призначений для користувача порт 1401, який був зазначений при налаштуванні нової віртуальної машини. Наприклад, 11.22.33.444,1401. У полі Перевірка справжності Вибираю Перевірка справжності SQL Server. У поле Ім'я користувача ввожу ім'я користувача SQL. У полі Пароль ввожу пароль для цього користувача. Вибираю Підключаюся (Рисунок 3.6).

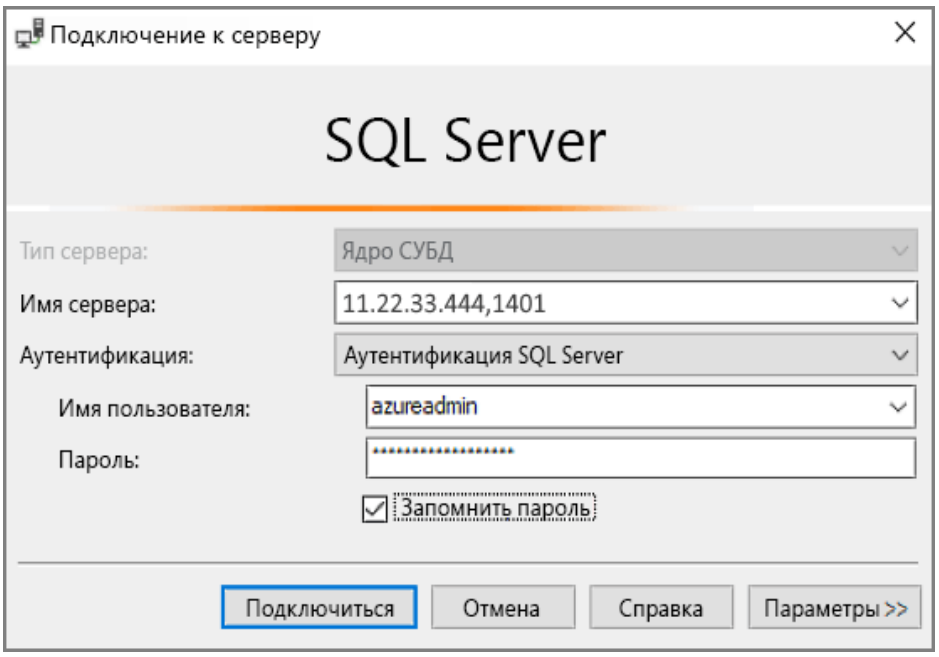


Рисунок 3.6 – Підключення до SQL сервера

Створення віртуальної мережі з допомогою порталу Azure

В меню порталу Azure Вибираю Створити ресурс. У Azure Marketplace Вибираю Мережі> Віртуальна мережа.

Вибираю Далі: IP-адреса адресний простір IPv4, ввожу 10.1.0.0/16.

Вибираю додати підмережа, а потім ввожу MyVirtualSubnet в якості імені підмережі і 10.1.0.0/24 для діапазону адрес підмережі.

Натискаю кнопку Додати, а потім Вибираю Перевірка і створити. Залишаю без змін значення інших параметрів і Вибираю Створити.

У вікні Створення віртуальної мережі обираю створити.

Налаштування VPN-з'єднання

Підключення "точка - мережа" - це VPN-підключення по протоколу SSTP (Secure Socket Tunneling Protocol) або IKEv2.

Для власної аутентифікації Azure на основі сертифікату при підключеннях "точка - мережа" необхідні наступні компоненти:

– VPN-шлюз з маршрутизацією на основі маршрутів.

– Відкритий ключ (CER-файл) для кореневого сертифіката, імпортований в Azure. Відразу після передачі сертифікат вважається довіреною сертифікатом і використовується для перевірки автентичності.

– Сертифікат клієнта, створений на основі кореневого сертифіката. Сертифікат клієнта, встановлений на кожному клієнтському комп'ютері, який буде підключений до віртуальної мережі. Цей сертифікат використовується для перевірки автентичності клієнта.

– Конфігурація VPN-клієнта. Файли конфігурації VPN-клієнта містять інформацію, необхідну для підключення клієнта до віртуальної мережі. Ці файли дозволяють налаштувати існуючий VPN-клієнт, що надається в операційній системі. Перед підключенням кожен клієнт потрібно налаштувати, використовуючи параметри в файлах конфігурації.

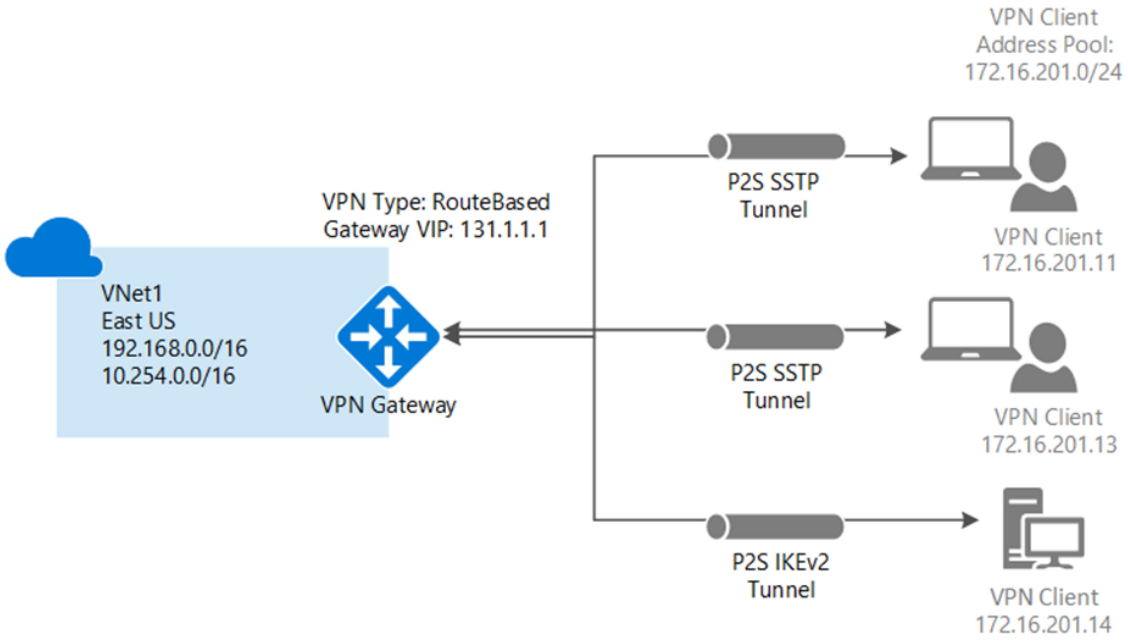


Рисунок 3.7 – Схема підключення до віртуальної мережі за допомогою VPN зеднання

3.1.2 Створення віртуального мережевого шлюзу

На цьому кроці створюю шлюз для своєї віртуальної мережі. Створення шлюзу часто займає 45 хвилин і більше, в залежності від обраного SKU шлюзу.

Віртуальна приватна мережа (VPN) типу "точка - мережа". Встановлюється між віртуальною мережею і окремим комп'ютером у вашій мережі. Необхідно налаштувати підключення для кожного комп'ютера, який потрібно підключити до віртуальної мережі. Цей тип

підключення ідеально підходить для новачків, які не вміють працювати в Azure, або для розробників, так як при його використанні існуючу мережу майже не потрібно міняти. Обмін даними між комп'ютером і віртуальною мережею здійснюється через Інтернет за допомогою зашифрованого тунелю.

Шлюз віртуальної мережі використовує певну підмережа, яка називається підмережею шлюзу. Підмережа шлюзу входить в діапазон IP-адрес віртуальної мережі, який ви вказуєте при її налаштування. Підмережа шлюзу містить IP-адреси, які використовують ресурси і служби шлюзу віртуальної мережі.

При створенні підмережі шлюзу вказується кількість IP-адрес, яке містить мережа. Необхідна кількість IP-адрес залежить від конфігурації VPN-шлюзу, який хочу створити. Деяким конфігурацій потрібно більше IP-адрес, ніж іншим.

З меню порталу Azure Вибираю Створити ресурс – віртуальний мережевий шлюз.

На вкладці Basics заповнюю значення для віртуального мережевого шлюзу (Рисунок 3.10).

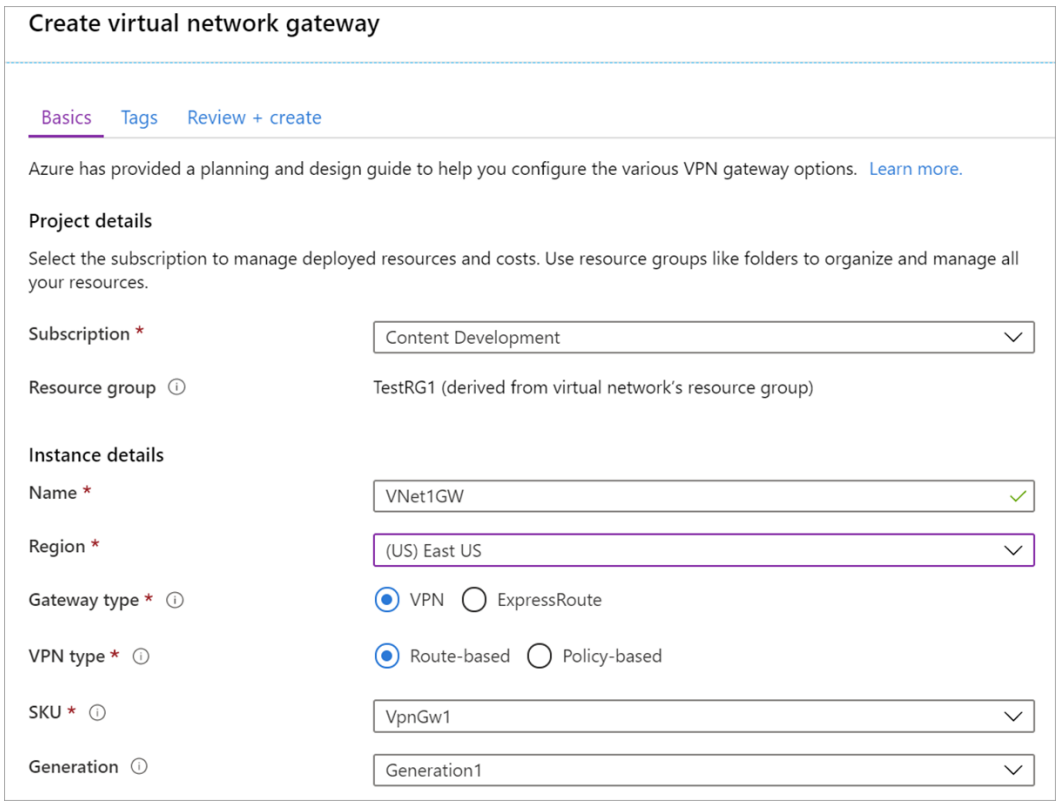


Рисунок 3.8 – Базові налаштування віртуального мережевого шлюзу

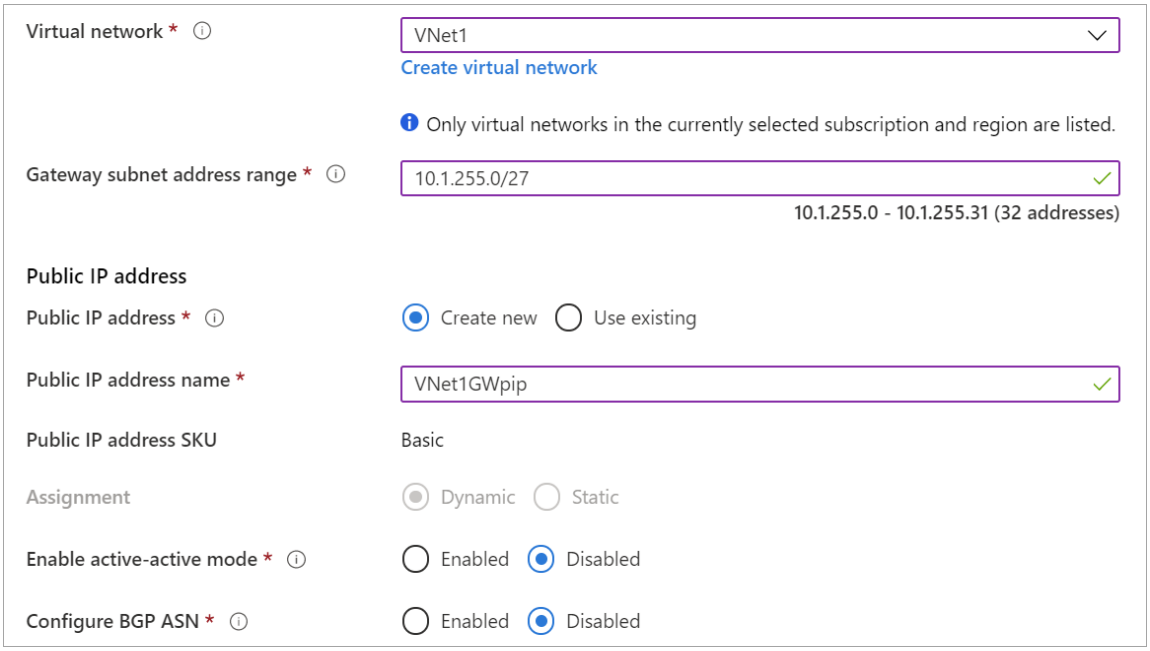


Рисунок 3.9 – Продовження базових налаштувань

Вибираю Огляд і створіть для виконання перевірки. Після того, як перевірка пройде, Вибираю Створити для розгортання шлюзів VPN. Повністю створення і розгортання шлюзу може зайняти до 45 хвилин. Статус розгортання можна побачити на сторінці «Огляд» для шлюзу.

3.1.3 Створення сертифікатів

Сертифікати використовуються в Azure для перевірки справжності клієнтів, що підключаються до віртуальної мережі за допомогою підключення "точка - мережа". Після отримання кореневого сертифіката необхідно відправити відомості про відкритий ключ в Azure. Після цього дії кореневий сертифікат вважається "довіреним" в Azure для підключення до віртуальної мережі через підключення типу "точка - мережа". Необхідно також створити сертифікат клієнта на основі довіреної кореневого сертифіката, а потім встановити їх на кожному клієнтському комп'ютері. Сертифікат клієнта використовується для перевірки автентичності клієнта, коли він ініціює підключення до віртуальної мережі.

Отримати файл .cer для кореневого сертифіката.

Використовую самозаверяющій сертифікат. Після створення кореневого сертифіката дані загальнодоступного сертифіката (а не закритий ключ) експортую у вигляді CER-файлу X.509 в кодуванні Base64. Потім передаю дані загальнодоступного сертифіката на сервер Azure.

3.1.3.1 Створення самозавіряючогося кореневого сертифіката

Використовую командлет New-SelfSignedCertificate для створення самозавіряючогося кореневого сертифіката.

PowerShell

$ cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `

-Subject "CN = P2SRootCert" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert: \ CurrentUser \ My" -KeyUsageProperty Sign -KeyUsage CertSign

Залишаю консоль PowerShell відкритою, для створення сертифікату клієнта відразу після створення цього кореневого сертифіката.

3.1.3.2 Створення сертифіката клієнта

На кожному клієнтському комп'ютері, який підключається до віртуальної мережі за допомогою підключення типу "точка - мережа", повинен бути встановлений сертифікат клієнта. Його потрібно створити з кореневого сертифіката і встановити на кожне клієнтське комп'ютер.

Можна створити унікальний сертифікат для кожного клієнта або використовувати один сертифікат для декількох клієнтів. Перевага унікальних клієнтських сертифікатів полягає в тому, що при необхідності можна відкликати один сертифікат. В іншому випадку, якщо буде потрібно відкликати сертифікат для перевірки автентичності, який використовують кілька клієнтів, вам доведеться створити і встановити нові сертифікати для всіх клієнтів, які використовують цей сертифікат.

Сертифікати клієнтів можна створити, використовуючи такі методи:

– Якщо ви використовується рішення корпоративного сертифіката, створюється сертифікат клієнта з загальним ім'ям @ формату значення імені yourdomain.com.

– Самопідписаний кореневий сертифікат виконую наступні дії в одній з наступних статей сертифіката P2S, щоб створювані сертифікатами клієнта були сумісні з моїм P2S-з'єднаннями.

Створення сертифіката клієнта.

На кожному клієнтському комп'ютері, який підключається до віртуальної мережі за допомогою підключення типу "точка-мережа", повинен бути встановлений сертифікат клієнта.

У прикладах використовую командлет New-SelfSignedCertificate для створення сертифіката клієнта, термін дії якого закінчується через рік.

Запускаю код щоб створити сертифікат клієнта. Сертифікат клієнта, який створюється, автоматично встановлюється в папку Certificates - Current User \ Personal \ Certificates на комп'ютері.

PowerShell

New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature

-Subject "CN = P2SChildCert" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert: \ CurrentUser \ My" `

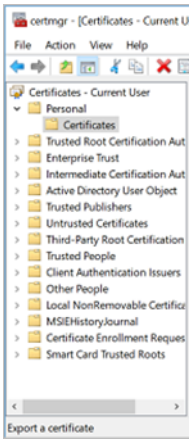
-Signer $ cert -TextExtension @ ("2.5.29.37 = {text} 1.3.6.1.5.5.7.3.2")

3.1.4 Експорт сертифіката

3.1.4.1 відкритого ключа кореневого сертифіката (.cer)

Після створення самозаверяющего кореневого сертифіката експортую CER-файл його відкритого ключа (закритий ключ). Щоб експортувати CER-файл для самозаверяющего кореневого сертифіката, роблю наступне:

1. Відкриваю розділ Управління сертифікатами користувачів. Знайдіть кореневої самозаверяющій сертифікат (зазвичай він знаходиться в папці Certificates - <поточний_користувач > \ Personal \ Certificates) і клацаю його правою кнопкою миші. Клацаю Усі завдання> Експорт. Відкриється майстра експорту сертифікатів (рисунок 2.16).



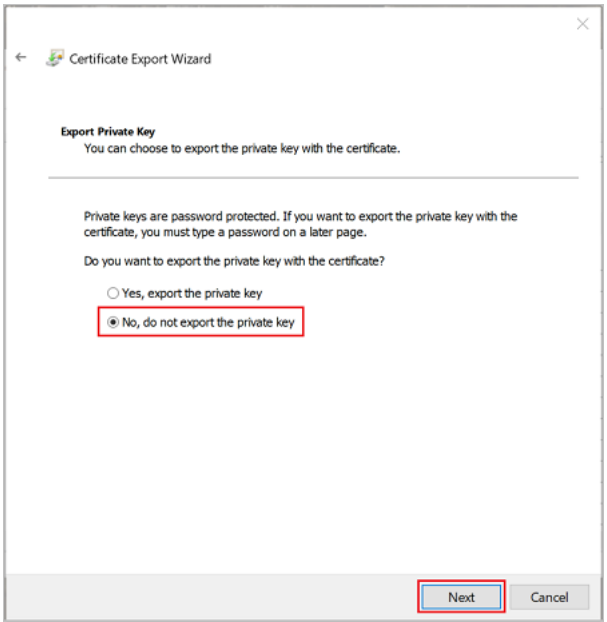


Рисунок 2.16 – Експортування кореневого сертифікату

2. Вибираю Ні, не експортувати закритий ключ і

знову натискаю кнопку Далі (Рисунок 3.13).

Рисунок 3.10 – Вибір експорту приватного ключа

3. На сторінці Формат експортованого файлу Вибираю Файли X.509 (.CER) в кодуванні Base-64 і натискаю кнопку Далі.

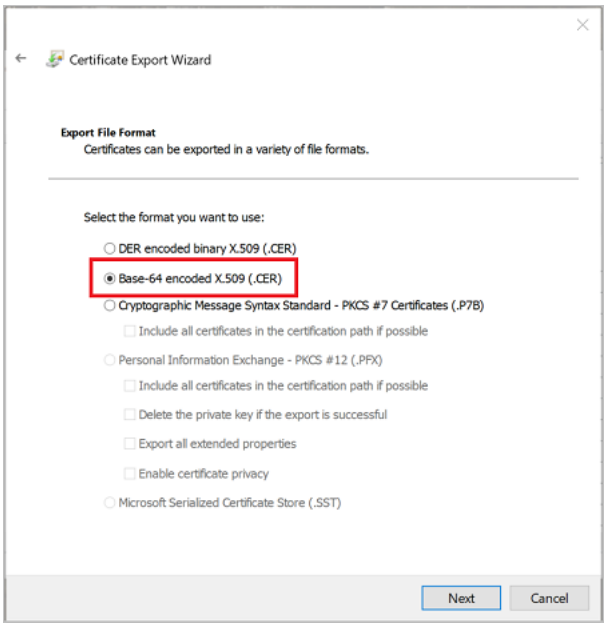


Рисунок 3.11 – Вибір формату файлу

4. На сторінці Ім'я експортованого файлу натискаю кнопку Огляд, щоб перейти в розташування для експорту сертифіката. В поле Ім'я файла ввожу ім'я для файлу сертифіката. Потім натискаю кнопку Далі.

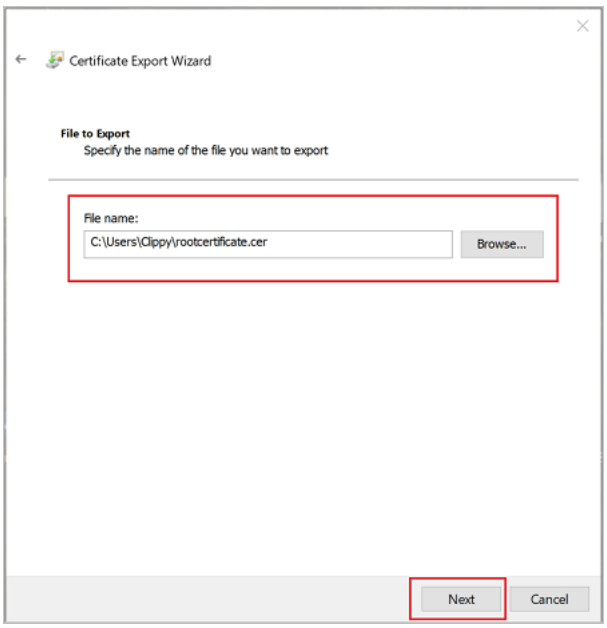


Рисунок 3.12 – Вибір директорії для експорту

5. Натискаю кнопку Готово, щоб виконати експорт сертифіката.

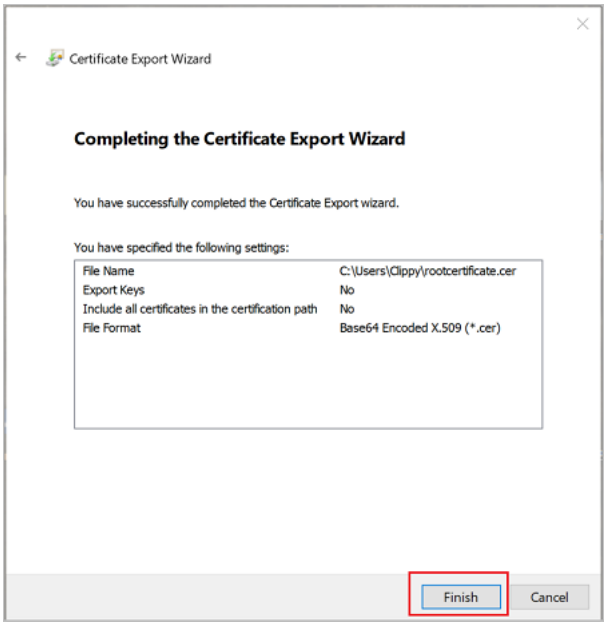


Рисунок 3.13 – Показ налаштувань перед експортуванням сертифікату

6. Сертифікат успішно експортований.

7. Експортований сертифікат виглядає приблизно так:

Рисунок 3.14 – Іконка експортованого сертифікату

8. Якщо відкрити експортований сертифікат в Блокноті, результат буде приблизно таким, як на рисунку 2.15. Виділений синім кольором розділ містить відомості, які завантажені в Azure.

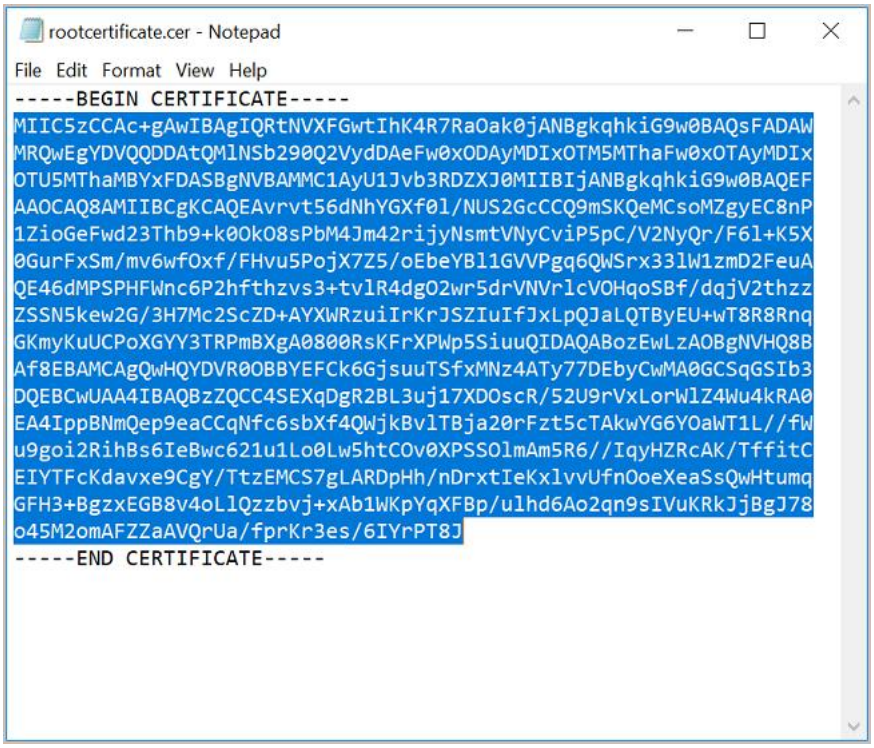


Рисунок 3.15 – Вигляд сертифікату після відкриття його за допомогою блокноту

3.1.4.2 Експорт сертифіката клієнта

Створений сертифікат клієнта автоматично встановлюється на комп'ютері, який використовувався для його створення. Якщо хочу встановити створений сертифікат клієнта на інший клієнтський комп'ютер, то його необхідно експортувати.

1. Щоб експортувати сертифікат клієнта, відкриваю розділ Управління сертифікатами користувачів. За замовчуванням створюються сертифікати клієнта зберігаються в папці Certificates - Current User \ Personal \ Certificates. Натискаю правою кнопкою клієнтського сертифіката, який хочу експортувати, натискаю всі завдання, а потім натискаю Експорт, щоб відкрити сертифікат Експорт Майстер.

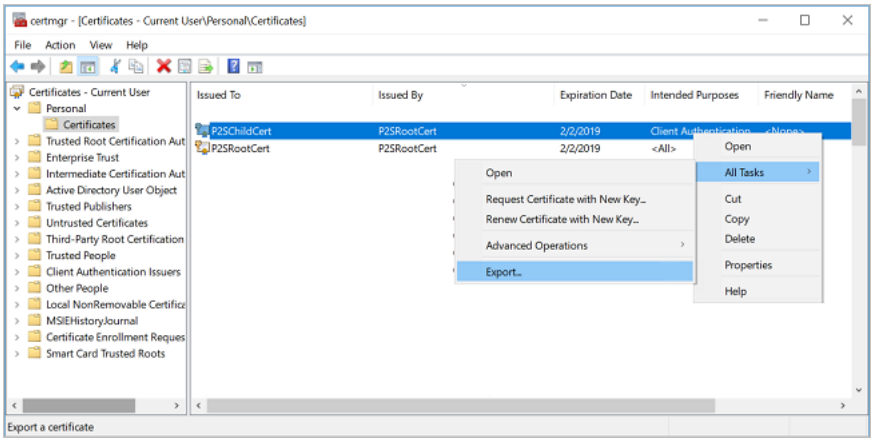


Рисунок 3.16 – Експорт сертифікату клієнта

2. Вибираю Так, експортувати закритий ключ, а потім натискаю кнопку Далі.

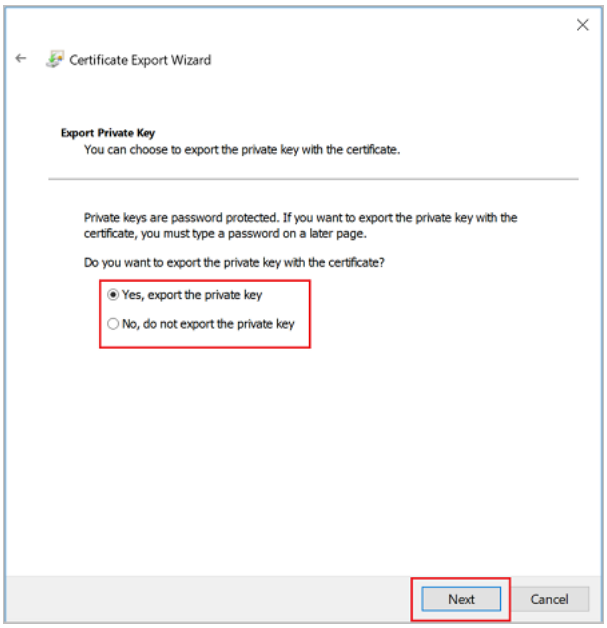


Рисунок 3.17 – Експорт приватного ключа

3. На сторінці Формат експортованого файлу залишаю налаштування за замовчуванням. Потім натискаю кнопку Далі.

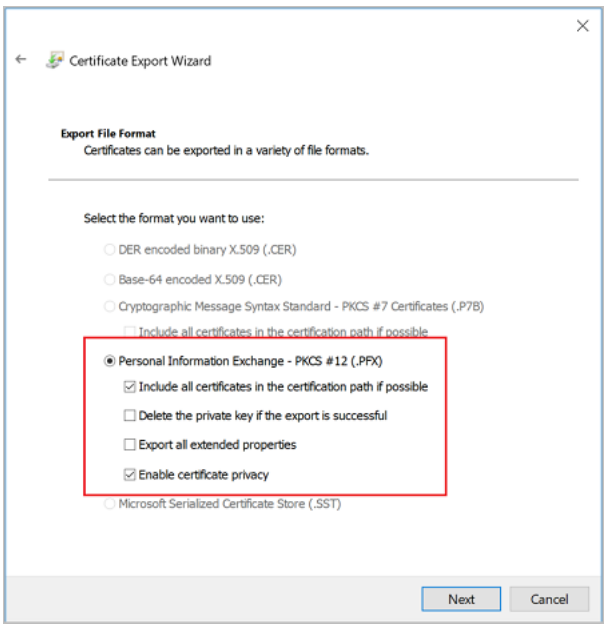


Рисунок 3.18 – Вибір формату для експорту

4. На сторінці Безпека слід захистити закритий ключ. Потім натискаю кнопку Далі.

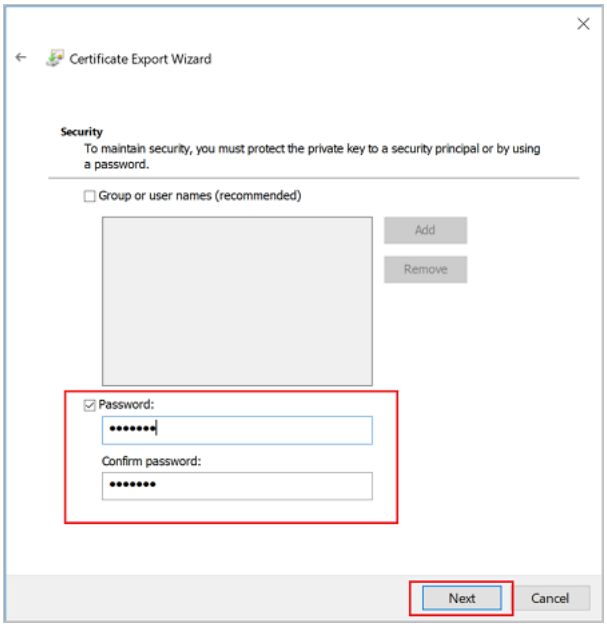


Рисунок 3.19 – Задання паролю для приватного ключа

5. На сторінці Ім'я експортованого файлу натискаю кнопку Огляд, щоб перейти в розташування для експорту сертифіката. В поле Ім'я файла ввожу ім'я для файлу сертифіката. Потім натискаю кнопку Далі.

6. Натискаю кнопку Готово, щоб виконати експорт сертифіката.

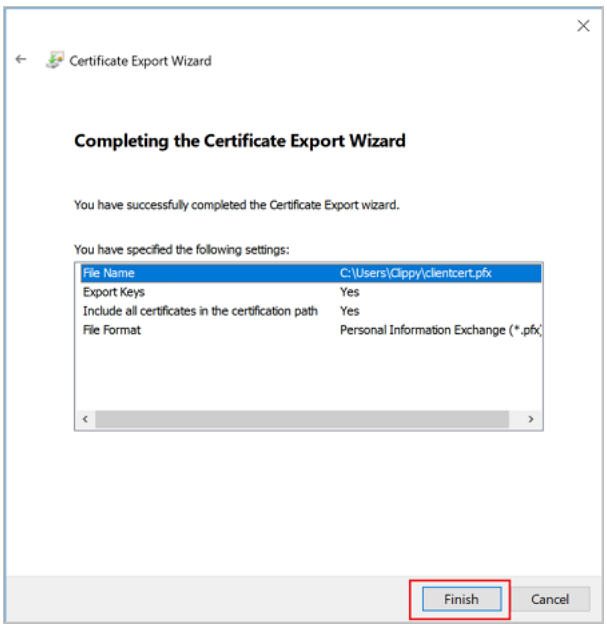


Рисунок 3.20 – Підтвердження налаштування для експорту

3.1.4.3 Додати пул адрес клієнта

Пул адрес клієнта є діапазон приватних IP-адрес, вказаних вами. Клієнти, які підключаються через підключення типу "точка - мережа", динамічно отримують IP-адреси з цього діапазону. Використовую діапазон приватних IP-адрес, які не перетинаються з локальним розташуванням, з якого потрібно з'єднатися, або віртуальної мережею, до якої планується отримати доступ. Якщо налаштувати декілька протоколів та SSTP є одним з протоколів, то налаштований пул адрес ділиться між налаштованими протоколами порівну.

Після створення шлюзу віртуальної мережі перехожу до розділу Параметри на сторінці шлюзу віртуальної мережі. У розділі Налаштування Вибираю конфігурацію від точки до сайту. Вибираю настройку зараз, щоб відкрити сторінку конфігурації.

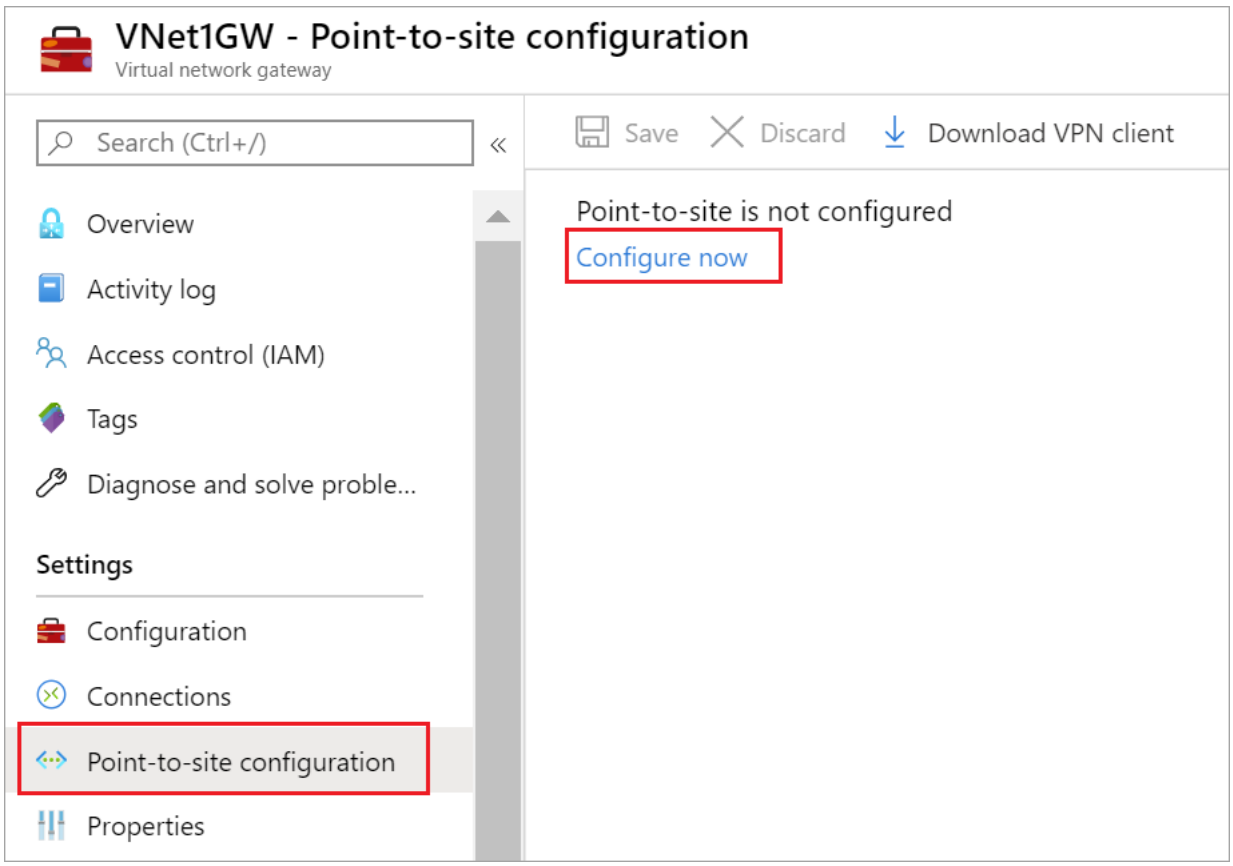


Рисунок 3.21 – Налаштування конфігурації Point-to-site

На сторінці конфігурації Point-to-site можна налаштувати різні настройки. Якщо на цій сторінці не відображається тип тунелю або тип аутентифікації, шлюз використовує базовий SKU. (Рисунок 3.24)

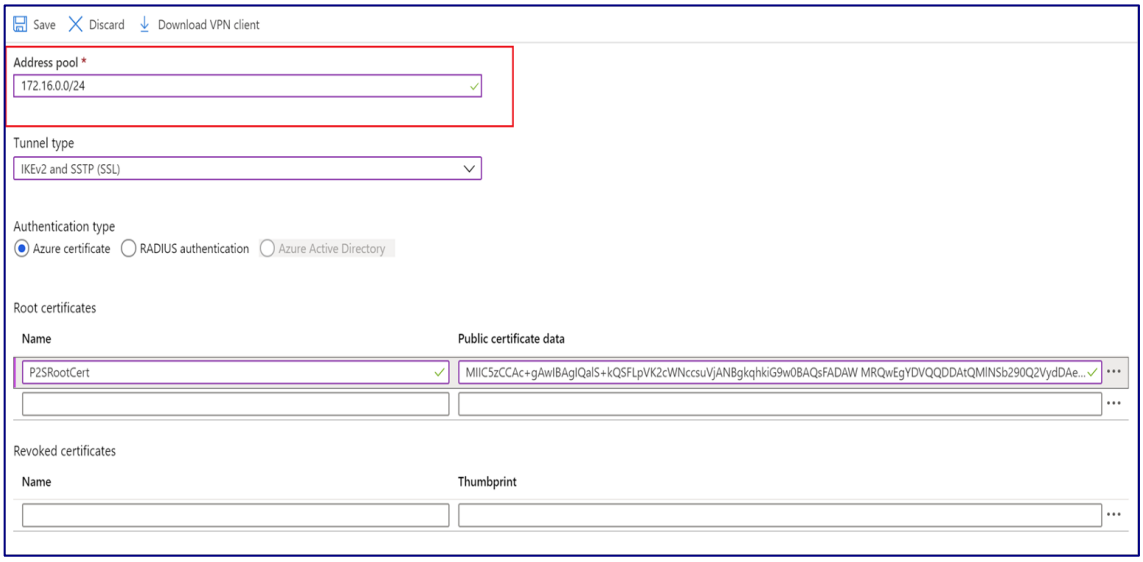


Рисунок 3.22 – Налаштування адреси та сертифікату для віртуальної мережі

В поле пулу Адреси додаю приватний діапазон IP-адрес, який хочу використовувати. VPN-клієнти динамічно отримують IP-адреса з зазначеного мною діапазону. Мінімальна підмережева маска становить 29 біт.

3.1.4.4 Налаштування типу тунелю

Вибираю тип тунелю. Варіанти тунелю OpenVPN, SSTP і IKEv2.

– Для підключення клієнт strongSwan в Android і Linux і власний VPN-клієнт IKEv2 в iOS і OSX використовують тільки тунель IKEv2.

– Клієнти Windows спочатку приміряють IKEv2, і якщо це не вдається з'єднатися, вони повертаються до SSTP.

– Також може використовуватися клієнт OpenVPN для підключення до типу тунелю OpenVPN.

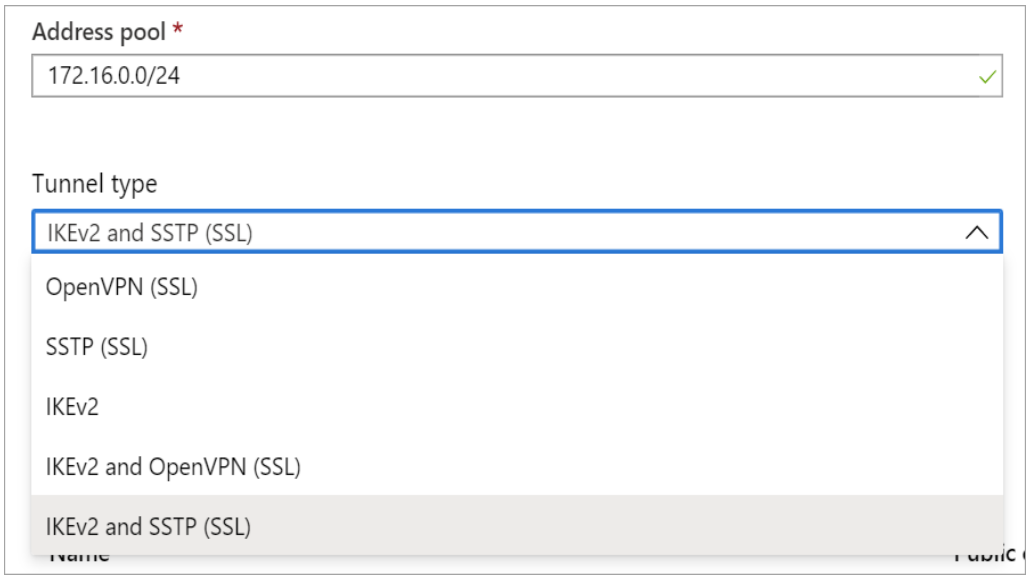


Рисунок 3.23 – Вибір типу тунелю

3.1.4.6 Завантажити дані про відкриті сертифікати кореневого сертифіката

Всього можна відправити до 20 додаткових довірених кореневих сертифікатів. Після відправки загальнодоступних даних сертифіката Azure зможе використовувати їх для перевірки справжності клієнтів, на яких встановлено клієнтський сертифікат, створений з довіреної кореневого

сертифіката. Надсилаю відомості про відкритий ключ кореневого сертифіката в Azure.

1. Сертифікати додаються на сторінку Point-to-site configuration (Конфігурація "точка - мережа") в колонку Кореневий сертифікат.

2. Відкриваю сертифікат в текстовому редакторі, наприклад в блокноті.

Рисунок 3.24 – Копіювання вибраного тексту до налаштування

3. Вставляю дані сертифіката в поле Дані загальнодоступного сертифіката. Називаю сертифікат, а потім Вибираю Зберегти.

Рисунок 3.25 – Як повинно виглядати налаштування на порталі Azure

4. Вибираю Зберегти у верхній частині сторінки, щоб зберегти всі налаштування конфігурації.

3.1.5 Налаштування OpenVPN для VPN шлюзу від Azure

Вмикаю OpenVPN в шлюзі. Переконуюсь, що шлюз вже налаштований для підключення "точка - мережа" (IKEv2 або SSTP), перш ніж виконувати наступні команди в Azure PowerShell:

Azure PowerShell

$ Gw = Get-AzVirtualNetworkGateway -ResourceGroupName $ rgname -name $ name

Set-AzVirtualNetworkGateway -VirtualNetworkGateway $ gw -VpnClientProtocol OpenVPN

1. Завантажую та встановлюю клієнт OpenVPN (версія 2.4 або вище) з офіційного веб-сайту OpenVPN. Далі завантажую профіль VPN для шлюзу.

2. Відкриваю файл конфігурації vpnconfig.ovpn з папки OpenVPN в Блокноті.

3. Експортую створений і завантажений в конфігурацію P2S сертифікат клієнта від точки до сайту на шлюзі.

4. Дістаю закритий ключ і відбиток base64 з PFX-файлу.

5. Під час використання profileinfo.txt в Блокноті. Щоб отримати відбиток сертифіката клієнта (дочірній), видаляю текст між "----- BEGIN CERTIFICATE -----" і "----- END CERTIFICATE -----" (включаючи ці рядки) для дочірнього сертифіката і копіюю його.

6. Перехожу на файл vpnconfig.ovpn, який відкрили в Блокноті. Знахожу розділ, зазначений нижче, і замінюю весь код між cert і / cert.

 # P2S client certificate

 # Please fill this field with a PEM formatted cert

<Cert>

$ CLIENTCERTIFICATE$

</ Cert>

7. Відкриваю файл profileinfo.txt в Блокноті. Щоб отримати закритий ключ, Вибираю текст (в тому числі і між) "----- BEGIN PRIVATE KEY -----" і "----- END PRIVATE KEY -----" і копіюю його.

8. Повертаюсь до файлу vpnconfig.ovpn в Блокноті і знаходжу цей розділ. Вставляю закритий ключ, замінивши все між і key і / key.

 # P2S client root certificate private key

 # Please fill this field with a PEM formatted key

<Key>

$ PRIVATEKEY

</ Key>

9. Копіюю файл vpnconfig.ovpn в папку C: \ Program Files \ OpenVPN \ config.

10. Клацаю правою кнопкою миші значок OpenVPN в області повідомлень, а потім натискаю "Підключити".[3]

3.2 Налаштування програмної частини

3.2.1 Налаштування платформи 1С на сервері.

Для налаштування серверу нам потрібно:

– Встановити 1С на сервері за допомогою програми інсталювання (рисунок 3.31);

– Створити інформаційну базу в SQL. Створення інформаційної бази в SQL дуже схожа на створення бази в файловому варіанті. Різниця полягає в тому, що на етапі вибору типу розташування інформаційної бази необхідно вибрати "На сервері 1С: Підприємства"(рисунок 1.36).

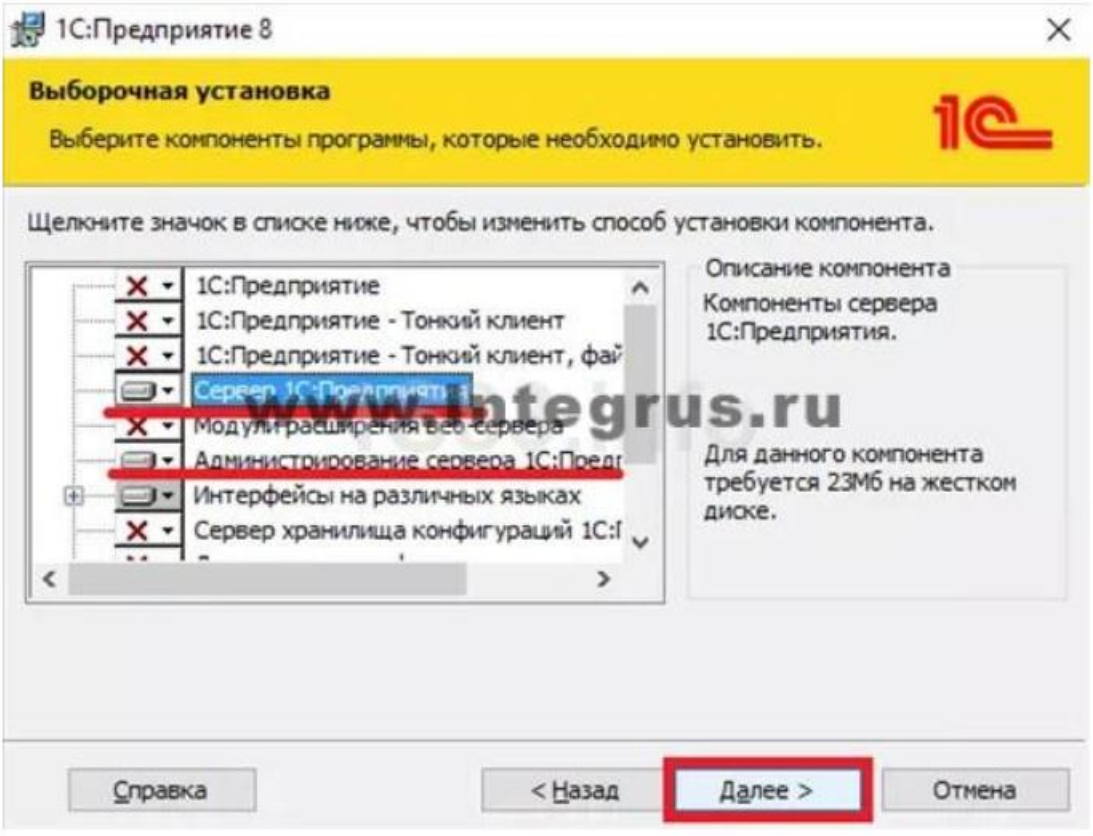


Рисунок 3.26 – Установка серверу 1с

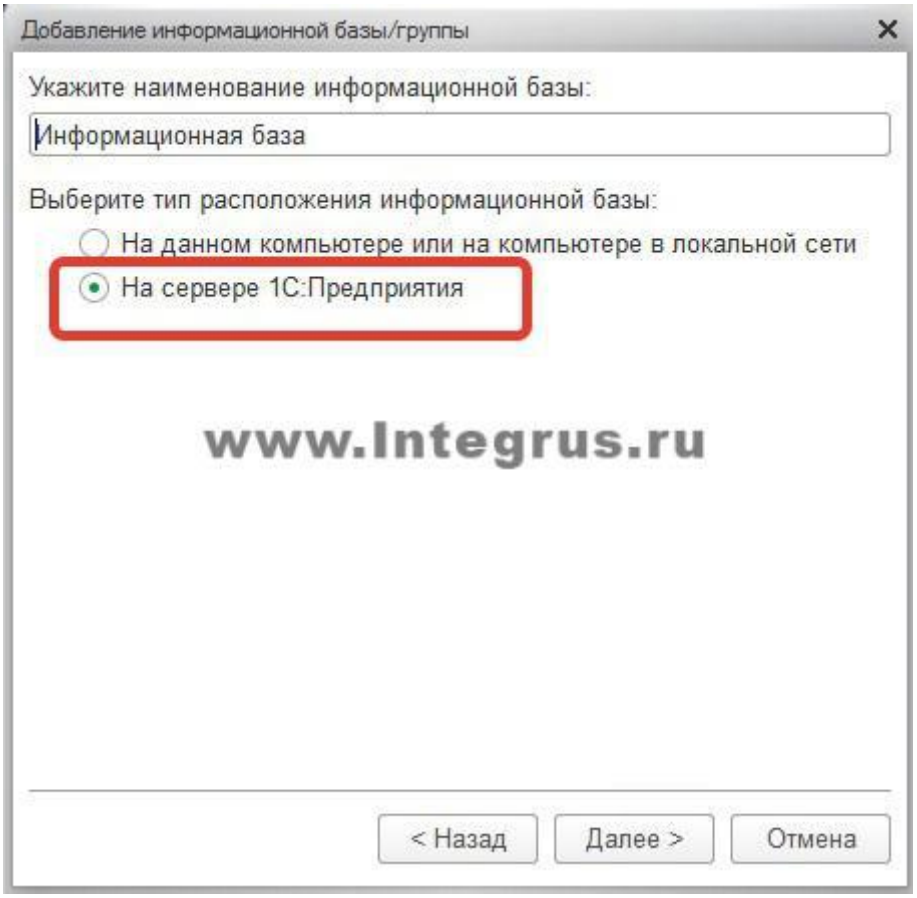


Рисунок 3.27 – Налаштування нової бази на сервері

Задати необхідні параметри:

– У пункті "Кластер серверів" вказую ім’я сервера, на який встановлювали SQL.

– У пункті "Ім'я інформаційної бази" Вказую ім'я бази даних.

– Тип СУБД - SQL.

– Користувач бази даних і його пароль - привілейований користувач MS SQL.

– Зсув дат за умовчанням.

– Відзначаю пункт "Створити базу даних в разі її відсутності" і натиснути "Далі".

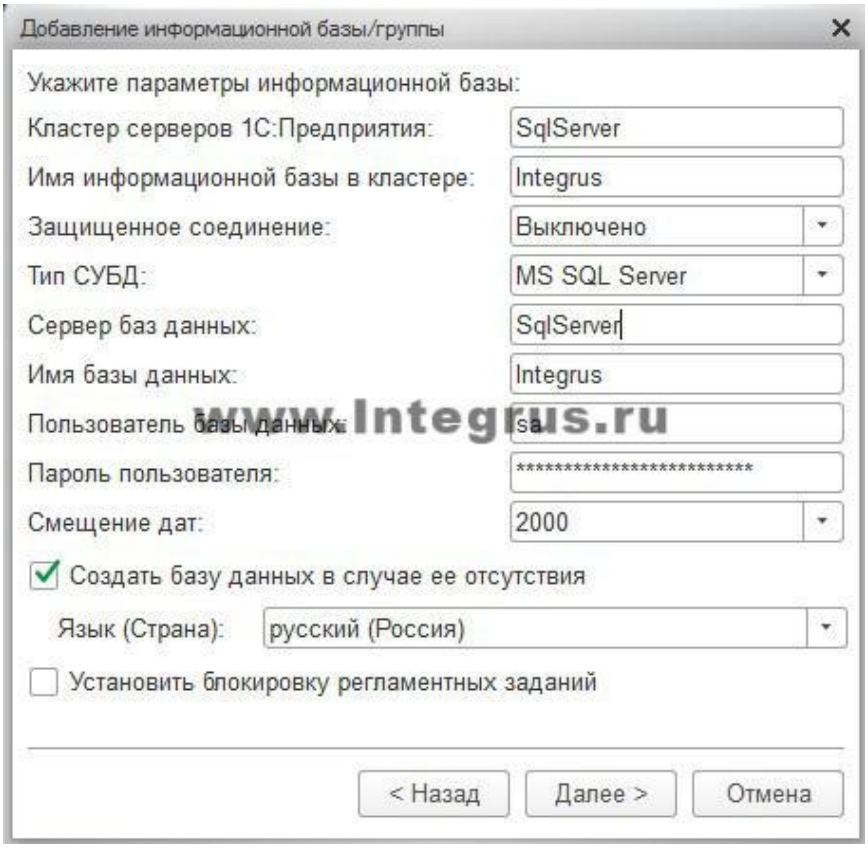


Рисунок 3.28 – Налаштування нової бази

Тепер база успішно створена на сервері SQL і додана в список доступних баз. Внизу на зображенні можна побачити результат виконаної роботи.[4]

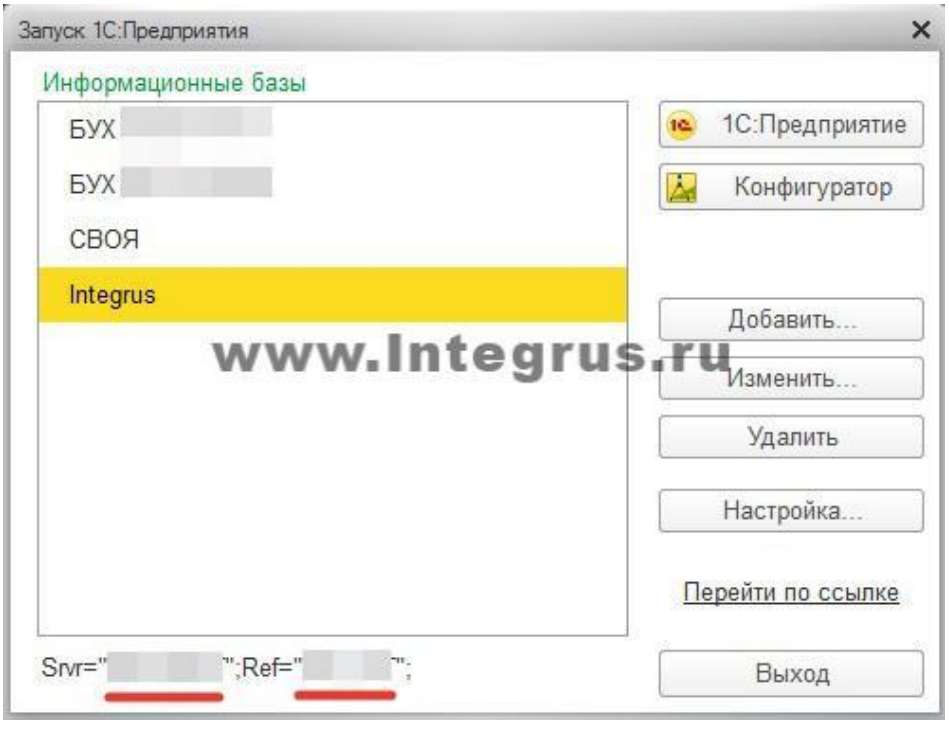
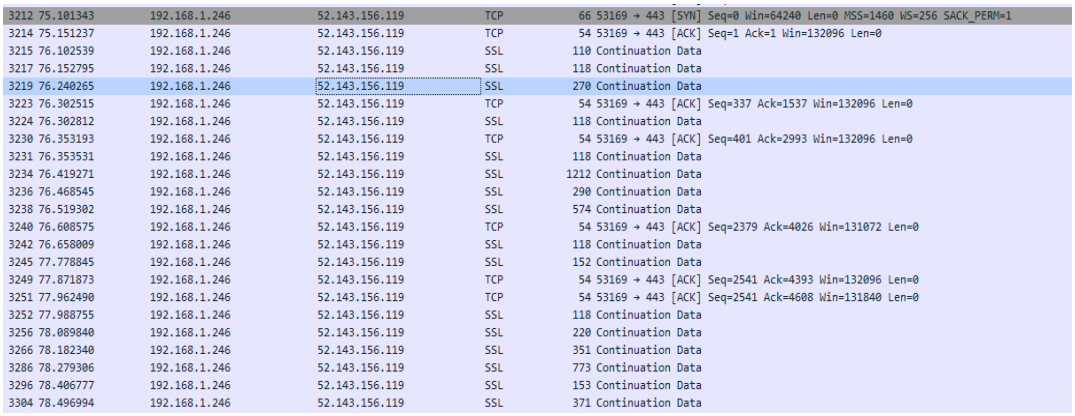


Рисунок 3.29 – Успішне створення нової бази на сервері

4 ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ

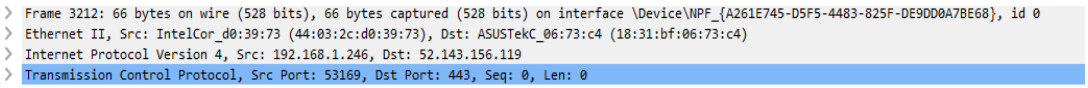
4.1 Перевірка роботи доступу до віртуальної мережі

Для перевірки доступу до мережі використаймо програму Wireshark та логи які запише програма OpenVPN. Почнемо з програми Wireshark. Як ми можемо бачити на рисунку 4.1 при спробі підключення програма OpenVPN звертаєтеся до загальнодоступної адреси віртуального мережевого шлюзу. Усі данні передаются у зашифрованому виді. Дані підключення можна побачити на рисунку 4.2. Після успішної аутентифікації у мережі ми можемо бачити що усі запитити які йдуть до нашої віртуальної мережі відправляються з адреси 10.2.0.2. Це і є адреса яку отримав комп'ютер у віртуальній мережі.



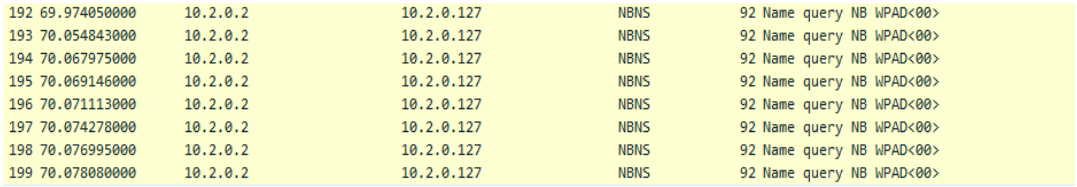
3212	75.101343	192.168.1.246	52.143.156.119	TCP	66 53169 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3214	75.151237	192.168.1.246	52.143.156.119	TCP	54 53169 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
3215	76.102539	192.168.1.246	52.143.156.119	SSL	110 Continuation Data
3217	76.152795	192.168.1.246	52.143.156.119	SSL	118 Continuation Data
3219	76.240265	192.168.1.246	52.143.156.119	SSL	270 Continuation Data
3223	76.302515	192.168.1.246	52.143.156.119	TCP	54 53169 → 443 [ACK] Seq=337 Ack=1537 Win=132096 Len=0
3224	76.302812	192.168.1.246	52.143.156.119	SSL	118 Continuation Data
3230	76.353193	192.168.1.246	52.143.156.119	TCP	54 53169 → 443 [ACK] Seq=401 Ack=2993 Win=132096 Len=0
3231	76.353531	192.168.1.246	52.143.156.119	SSL	118 Continuation Data
3234	76.419271	192.168.1.246	52.143.156.119	SSL	1212 Continuation Data
3236	76.468545	192.168.1.246	52.143.156.119	SSL	290 Continuation Data
3238	76.519302	192.168.1.246	52.143.156.119	SSL	574 Continuation Data
3240	76.608575	192.168.1.246	52.143.156.119	TCP	54 53169 → 443 [ACK] Seq=2379 Ack=4026 Win=131072 Len=0
3242	76.658009	192.168.1.246	52.143.156.119	SSL	118 Continuation Data
3245	77.778845	192.168.1.246	52.143.156.119	SSL	152 Continuation Data
3249	77.871873	192.168.1.246	52.143.156.119	TCP	54 53169 → 443 [ACK] Seq=2541 Ack=4393 Win=132096 Len=0
3251	77.962490	192.168.1.246	52.143.156.119	TCP	54 53169 → 443 [ACK] Seq=2541 Ack=4608 Win=131840 Len=0
3252	77.988755	192.168.1.246	52.143.156.119	SSL	118 Continuation Data
3256	78.089840	192.168.1.246	52.143.156.119	SSL	220 Continuation Data
3266	78.182340	192.168.1.246	52.143.156.119	SSL	351 Continuation Data
3286	78.279306	192.168.1.246	52.143.156.119	SSL	773 Continuation Data
3296	78.406777	192.168.1.246	52.143.156.119	SSL	153 Continuation Data
3304	78.496994	192.168.1.246	52.143.156.119	SSL	371 Continuation Data

Рисунок 4.1 – Підключення до віртуальної мережі



```
> Frame 3212: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{A261E745-D5F5-4483-825F-DE9DD0A7BE68}, id 0
> Ethernet II, Src: IntelCor_d0:39:73 (44:03:2c:d0:39:73), Dst: ASUSTekC_06:73:c4 (18:31:bf:06:73:c4)
> Internet Protocol Version 4, Src: 192.168.1.246, Dst: 52.143.156.119
> Transmission Control Protocol, Src Port: 53169, Dst Port: 443, Seq: 0, Len: 0
```

Рисунок 4.2 – Дані які передаються при підключенні



192	69.974050000	10.2.0.2	10.2.0.127	NBNS	92 Name query NB WPAD<00>
193	70.054843000	10.2.0.2	10.2.0.127	NBNS	92 Name query NB WPAD<00>
194	70.067975000	10.2.0.2	10.2.0.127	NBNS	92 Name query NB WPAD<00>
195	70.069146000	10.2.0.2	10.2.0.127	NBNS	92 Name query NB WPAD<00>
196	70.071113000	10.2.0.2	10.2.0.127	NBNS	92 Name query NB WPAD<00>
197	70.074278000	10.2.0.2	10.2.0.127	NBNS	92 Name query NB WPAD<00>
198	70.076995000	10.2.0.2	10.2.0.127	NBNS	92 Name query NB WPAD<00>
199	70.078080000	10.2.0.2	10.2.0.127	NBNS	92 Name query NB WPAD<00>

Рисунок 4.3 – Пакети в середині мережі

Далі розглянемо лог файл з вдалого підключення до віртуальної мережі, записаний програмою OpenVPN.

Як ми можемо бачити на рисунку ч.ч програма відсилає запит з ключом аутентифікації на сервер для його підтвердження. Ключ передається в обидві сторони в шифрованому вигляді з довжиною ключа 256 біт. Після підтвердження ключа програма звертається на відкриту IP-адресу для встановлення зв’язку.

```
Thu Jun 18 13:26:32 2020 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Thu Jun 18 13:26:32 2020 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication
Thu Jun 18 13:26:32 2020 MANAGEMENT: >STATE:1592475992,RESOLVE,,,,,,
Thu Jun 18 13:26:32 2020 TCP/UDP: Preserving recently used remote address: [AF_INET]52.143.156.119:443
```

Рисунок 4.4 – Лог файл підключення

Після проходження всіх перевірок підключення програма запитує конфігурацію з якою вона зможе працювати. В даній конфігурації знаходиться адреса мережі і адреса девайсу яку видав DHCP сервер, маска мережі а також довжина ключа шифрування. І після усіх налаштувань запускає віртуальний адаптер з усіма налаштуваннями. Повні логи з обох програм можна подивитися у додатках Б і В.

```
Thu Jun 18 13:26:35 2020 SENT CONTROL [9e4a0034-b5d7-49a0-a464-7f52597115b0.vpn.azure.com]: 'PUSH_REQUEST' (status=1)
Thu Jun 18 13:26:35 2020 PUSH: Received control message: 'PUSH_REPLY,route 10.1.0.0 255.255.0.0,route-gateway 10.2.0.1,topology subnet,ifconfig 10.2.0.2 255.255.255.128,cipher AES-256-GCM'
Thu Jun 18 13:26:35 2020 OPTIONS IMPORT: --ifconfig/up options modified
Thu Jun 18 13:26:35 2020 OPTIONS IMPORT: route options modified
Thu Jun 18 13:26:35 2020 OPTIONS IMPORT: route-related options modified
Thu Jun 18 13:26:35 2020 OPTIONS IMPORT: data channel crypto options modified
Thu Jun 18 13:26:35 2020 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Thu Jun 18 13:26:35 2020 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Thu Jun 18 13:26:35 2020 interactive service msg_channel=640
Thu Jun 18 13:26:35 2020 ROUTE_GATEWAY 192.168.76.254/255.255.255.0 I=13 HWADDR=8c:ec:4b:02:14:c4
Thu Jun 18 13:26:35 2020 open_tun
```

Рисунок 4.5 – Лог файл підключення

5 ЕКОНОМІЧНА ЧАСТИНА

5.1 Техніко-економічне обґрунтування розробки

В кваліфікаційній роботі розглядається перенесення серверу 1С до хмарної платформи Microsoft Azure. Для виконання поставленої задачі необхідно орендувати віртуальний сервер на сайті платформи. Це дозволить значно скоротити стартові витрати і швидше вийти на чистий прибуток

Для обґрунтування економічної доцільності застосування КС, необхідно виконати:

- розрахунок капітальних витрат на придбання складових КС;
- розрахунок річних експлуатаційних витрат проектної апаратури;
- величину річного економічного ефекту.

5.2 Розрахунок капітальних витрат на придбання складових КС

Капітальні вкладення – це кошти, призначені для створення і придбання основних фондів та нематеріальних активів, що підлягають амортизації.

Кошторис капітальних витрат на обладнання, яке необхідно для реалізації комп'ютерної системи, приведена в таблиці 5.1.

Капітальні витрати розраховуються за формулою:

$$К_{пр} = К_{об} + К_{тр} + К_{мн} + К_{пз}, \quad (5.1)$$

де $К_{об}$ – вартість обладнання, грн.,

$К_{тр}$ – вартість транспортно-заготівельних витрат, грн.,

$К_{мн}$ – вартість монтажно-налагоджувальних робіт, грн.,

$К_{пз}$ – вартість розробки програмного забезпечення.

Таблиця 5.1 – Кошторис капітальних витрат

№ п/п	Найменування обладнання	Од. виміру	Кіль-кість	Вартість од. обладнання, грн	Сума, грн.
1	Оренда віртуальної машини з ліцензією	Години	200	16,04	3208
2	Оренда SSD категорії «Стандарт»	шт	3	282,37	847,11
3	Оренда віртуальної мережі та VPN доступу	шт	1	727,33	727,33
Всього					4782,44

Загальна вартість обладнання $К_{об}$=4782,44 грн.

Вартість транспортно-заготівельних і складських витрат становить 7% від вартості обладнання.

$К_{тр}$=4782,44*7%=334,77 грн.

Вартість монтажно-налагоджувальних робіт становить 8% від вартості обладнання.

$К_{мн}$=4782,44*8%=382,59 грн.

5.2.1 Розрахунок капітальних витрат на програмне забезпечення

5.2.1.1 Розрахунок часу на розробку програмного забезпечення

Трудомісткість розробки програмного забезпечення:

$$t = t_o + t_д + t_a + t_n + t_{нал} + t_{док},$$

(5.2)

где t_o - витрати праці на підготовку й опис поставленого завдання

$t_д$ - витрати праці на дослідження алгоритму розв'язку завдання;

t_a - витрати праці на обробку блок-схеми алгоритму;

t_n - витрати праці на програмування по готовій блок-схемі;

$t_{нал}$ - витрати праці на налаштування програм на ЕОМ;

$t_{док}$ - витрати праці на підготовку документації за завданням.

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

Умовна кількість операторів у програмі:

$$Q = q \cdot c \cdot (1+p), \quad (5.3)$$

де q –кількість операторів, використовуваних у програмі.

Виходячи з ПЗ q = 20;

c – коефіцієнт складності програми;

p – коефіцієнт корекції програми в процесі її обробки.

Коефіцієнт складності «c» програми визначає відносну складність програми відносно типового завдання, складність якого відповідає 1. c = 1,25.

Коефіцієнт корекції програми «p» визначає збільшення обсягу робіт за рахунок внесення змін в алгоритм або програму в результаті уточнення постановки завдання. Ухвалюємо p=0,1, це відповідає внесенню 3…5 корекцій, що тягнуть за собою переробку 5-10% готової програми.

Таким чином, для програми, описаної в кваліфікаційній роботі:

Q = 20·1,25(1+0,1) = 27,5

Оцінка витрат праці на підготовку й опис завдання становлять

$t_0 = 40$ люд.-годин.

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

$$t_д = \frac{Q \cdot B}{(75...85) \cdot k} \text{ люд.-годин} \quad (5.4)$$

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

k – коефіцієнт кваліфікації програміста, які визначається залежно від

стажу роботи зі спеціальності. У нашому випадку коефіцієнт кваліфікації програміста становить k= 1,2.

Для розроблюваного програмного забезпечення:

$t_{д}=\frac{27,5*1,4}{80*1,2}=0,57$ люд.-годин.

Витрати на розробку алгоритму розв'язку завдання:

$$t_a = \frac{Q}{(20...25)\cdot k} \text{ люд.-годин} \quad (5.5)$$

Для розроблювального програмного забезпечення:

$t_a = \frac{27,5}{20\cdot 1,2} = 1,14$ люд.-годин.

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

$$t_n = \frac{Q}{(20...25)\cdot k} \text{ люд.-годин} \quad (5.6)$$

Для розроблюваного програмного продукту:

$t_n = \frac{27,5}{20\cdot 1,2} = 1,14$ люд.-годин.

Витрати праці на налагодження програми на ЕОМ розраховуються по формулі:

$$t_{нал} = \frac{Q}{(4...5)\cdot k} \text{ люд.-годин} \quad (5.7)$$

Для конкретного програмного продукту:

$t_{нал} = \frac{27,5}{5\cdot 1,2} = 4,6$ люд.-годин.

Витрати праці на підготовку документації за завданням визначаються по формулі:

$$t_Д = t_{ДР} + t_{ДО,} \text{ люд.-година} \quad (5.8)$$

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

$t_{ДО}$ – трудомісткість редагування, друку й оформлення документації.

$$t_{ДР} = Q/(15…20)\cdot k,$$

(5.9)

$t_{ДР} = 27,5/18 \cdot 1,2 = 5,9$ люд.-година;

$$t_{ДО} = 0,75 \cdot t_{ДР},$$

(5.10)

$t_{ДО} = 0,75 \cdot 5,9 = 4,42$ люд.-година.

Для розроблюваного програмного забезпечення витрати праці на підготовку документації за завданням будуть становити:

$t_{Д} = 5,9 + 4,42 = 10,32$ люд.-година.

Трудомісткість розробки програмного забезпечення буде становити:

$t = 40 + 0,57 + 1,14 + 1,14 + 4,6 + 10,32 = 57,77$ людино-годин.

4.2.1.2 Розрахунки витрат на розробку програмного продукту

Витрати на розробку програмного продукту $К_{пз}$ містять витрати на заробітну плату розробника програми $З_{зп}$ і вартість машинного часу, необхідного для налаштування програми на ЕОМ $З_{мч}$

$$К_{пз} = З_{зп} + З_{ми}, \text{ грн.}$$

(5.11)

Заробітна плата розробника програмного забезпечення:

$$З_{зп} = t \cdot С_{пр}, \text{ грн.}$$

(5.12)

де t – загальна трудомісткість обробки програмного забезпечення;

$С_{пр}$ – середня годинна тарифна ставка програміста становить:

$С_{пр} = 69$ грн./година.

Заробітна плата за розробку програмного забезпечення дорівнює:

$З_{зп} = 57,77 \cdot 69 = 3986,13$ грн.

Вартість машинного часу, необхідного для налаштування програми на ЕОМ:

$$З_{мч} = t_{нал} \cdot С_{мг}, \text{ грн.}$$

(5.13)

де:

$t_{отл}$ – трудомісткість налаштування програми на ЕОМ, людино-годин;

$С_{мг}$ – вартість машино-години ЕОМ, грн./година. $С_{мг}$ = 5 грн./година.

$З_{мч}$ = 4,6·5 = 23 грн.

Витрати на розробку програмного забезпечення системи керування будуть становити:

$К_{пз}$ = 3986,13 + 23= 4009,13 грн.

Певні, таким чином, витрати на створення програмного забезпечення є частиною одноразових капітальних витрат на створення системи керування.

Очікувана тривалість розробки програмного забезпечення:

$$T = \frac{t}{B_k \cdot F_p}, \text{ міс.} \qquad (5.14)$$

де, $B_к$ – кількість розробників. Програма розроблялася однією людиною, тому $В_к$ = 1;

F_p – місячний фонд робочого часу (Fp = 176 годин).

Визначимо тривалість розробки ПО:

$$T = \frac{57,77}{1 \cdot 176} = 0,32 \text{ міс.}$$

Таким чином, капітальні витрати розраховані за формулою (5.1) дорівнюють:

$К_{пр}$ = 4782,44+334,77 +382,59 +4009,13 = 9508,93 грн.

5.3 Розрахунок річних експлуатаційних витрат

Експлуатаційні витрати визначаються за такими статтями витрат:

- амортизаційні відрахування (Са);
- заробітна плата обслуговуючого персоналу (Сзп);
- відрахування на соціальні заходи (Сс);
- витрати на технічне обслуговування і поточний ремонт обладнання (Сто);
- вартість спожитої електроенергії (Се)
- інші (Сі).

Таким чином, експлуатаційні витрати розраховуються за формулою:

$$С = С_а + С_{зп} + С_с + С_{то} + С_е + С_і \quad (5.15)$$

Для розрахунку показників економічної ефективності необхідно розрахувати експлуатаційні витрати по проектному варіанту КС.

4.3.1 Розрахунок амортизаційних відрахувань

Комп'ютерні системи відносяться до четвертої групи відповідно до класифікації груп основних засобів та інших необоротних активів. Для систем на базі комп'ютерної техніки мінімальний термін експлуатації становить 5 років. Амортизація для КС магазину «Європа-Дніпро» визначається методом прискореного зменшення залишкової вартості.

Норма амортизації розраховується за формулою:

$$Ha = \frac{2}{T} \quad (5.16)$$

де , Т – строк корисного використання КС.

$Ha = 2/5 = 0{,}4$

Таким чином, амортизаційні відрахування по обладнанню, будуть визначаться по формулі 5.17:

$$С_а = К_{пр} \cdot Н_а, \text{ грн.} \quad (5.17)$$

Амортизаційні відрахування (за перший рік експлуатації) для апаратного забезпечення системи становитимуть:

Са.п = 9508,93*0,4= 3803,57 грн.

Існуючої системи немає.

5.3.2 Розрахунок річного фонду заробітної плати

Розрахунок річного фонду заробітної плати обслуговуючого персоналу, згідно форми, наведено в таблиці 5.2.

«Адміністративний відділ» підприємства «Європа-Дніпро» має в своєму складі 3 працівників менеджерів та начальник відділу. Робочій день має тривалість 8 годин.

Номінальний річний фонд робочого часу одного працівника визначається за формулою 4.18.

$$F_{ном}= (T_к-T_{пр}-T_{вих}-T_{відп})*T_{см}, \text{ годин} \quad (5.18)$$

Номінальний річний фонд робочого часу менеджера:

$F_{ном}$=(365-9-104-21)*8=1848 годин

Номінальний річний фонд робочого часу керівника відділу:

$F_{ном}$=(365-9-104-28)*8=1792 годин

Таблиця 5.2 – Річний фонд заробітної плати

№ п/п	Найменування професії працівників	Кількість працюючих, люд.		Годинна тарифна ставка, грн	Номінальний річний фонд робочого часу (годин)	Всього пряма заробітна плата, грн.	Додаткова заробітна плата (10%)	Доплати (7%)	Всього заробітна плата, грн.
		явочне	списочне						
1	2	3	4	5	6	7	8	9	10
Існуючий варіант									
1	Менеджер	3	3	50	1848	277200	27720	19404	324324
2	Керівник	1	1	60	1792	107520	10752	7526,4	125798,4
Всього									450122,4
Проектний варіант									
4	Менеджер	3	3	50	1848	277200	27720	19404	324324

5	Керівник	1	1	60	1792	107520	10752	7526,4	125798,4
Всього									450122,4

4.3.3 Розрахунок відрахувань на соціальні заходи

Відрахування на соціальні заходи становлять 22% від заробітної плати (формула 5.19):

$$C_c = C_{зп} * 22\%, \text{ грн.} \quad (5.19)$$

Сс.і=450122,4 *0,22=99026,93 грн.

Сс.п=450122,4*0,22= 99026,93 грн.

4.3.4 Визначення річних витрат на технічне обслуговування і поточний ремонт

Витрати на технічне обслуговування і поточний ремонт включають витрати на матеріали, запасні частини, заробітну плату ремонтним робітником. Вони складають 20% від капітальних витрат:

$$C_{тр} = K_{пр} * 20\%, \text{ грн.} \quad (5.20)$$

Сто.п=$К_{пр}$*0,2=9508,93 *0,2= 1901,79 грн.

5.3.5 Розрахунок вартості споживаної електроенергії

Вартість спожитої електроенергії визначається за формулою:

$$С_е = М * F_р * а, \text{ грн,} \quad (5.21)$$

де М – встановлена потужність апаратури,

$F_р$ – річний фонд робочого часу апаратури (2 920 годин – обладнання працює 8 годин на добу),

а – тариф на електроенергію для підприємств (на передачу 1,5540 грн/КВт·ч, на послуги диспетчерського управління – 0,1023 грн/КВт·ч, а= 1,5563 грн).

Сумарна споживана потужність мережного принтера складе 100 Вт. Споживання електроенергії одним персональним комп'ютером (3 шт) по

300 Вт. Споживання електроенергії маршрутизатором (1 шт) – 150 Вт. Разом – 1150 Вт (1,15 Квт).

Се.п=1,15*2920*1,5563= 5226,05 грн.

5.3.6 Визначення інших витрат

Інші витрати по експлуатації об'єкта проектування включають витрати на навчання персоналу підприємства обслуговування нового обладнання, з охорони праці, придбання спец одягу та ін. Ці витрати складають 4% від річного фонду заробітної плати обслуговуючого персоналу.

$$C_i = C_{зп}*4\%, \text{ грн.} \quad (5.22)$$

Сі.п = 450122,4 ·0,04= 18004,9 грн.

Сі.і = 450122,4 ·0,04= 18004,9 грн.

Відповідно до формули 4.15 експлуатаційні витрати для КС складуть:

Сп=578085,64 грн.

Сі=656124,68грн.

5.4 Визначення та аналіз показників економічної ефективності проекту

Результати розрахунків експлуатаційних витрат по проектованому і існуючому варіантам зведені в табл. 5.3.

Таблиця 5.3 – Річні експлуатаційні витрати

Найменування показника	Проектний варіант	Існуючий варіант
Амортизація	3803,57	52800
Фонд заробітної плати	450122,4	450122,4
Відрахування на соц. виплати	99026,93	99026,93
Ремонт і тех.обслуговування	1901,79	26400
Електроенергія	5226,05	9770,45
Інші	18004,9	18004,9
Разом	578085,64	656124,68

Річна економія на експлуатаційних витратах становить:

$$\Delta C = Ci - Cп, \quad (5.23)$$

ΔC = 656124,68–578085,64 =78039,04 грн.

Термін окупності (Тр) проектованої системи:

$$T_р = К_{пр}/ \Delta C, \text{ лет} \quad (5.24)$$

$T_р$ =9508,93/78039,04 = 0,12 года

Отже, капітальні витрати на впровадження проектної системи окупляться через 0,12 року.

Коефіцієнт ефективності капітальних витрат визначається за формулою:

$$К_{эфф} = 1/ T_р, \text{ грн.} \quad (5.25)$$

$К_{эфф}$ =1/0,12=8,3 грн.

Отже, на 1 грн. капітальних витрат припадає 8,3 грн. прибутку.

Висновок

Удосконалення комп'ютерної системи підприємства «Європа-Дніпро» з опрацюванням побудови, налаштування та безпеки корпоративної мережі доцільно, так як при капітальних витратах в 9508,93грн., капіталовкладення окупляться через 0,12 року. Коефіцієнт ефективності капітальних витрат дорівнює 8,3 грн. при мінімальному терміні експлуатації в 5 років.

6 ОХОРОНА ПРАЦІ

6.1 Фактори, що впливають на функціональний стан програміста

Трудовий процес суттєво впливає на психофізіологічні можливості користувачів комп'ютерів, оскільки їх діяльність характеризується значними статичними фізичними навантаженнями; недостатньою руховою активністю; напруженнями сенсорного апарату, вищих нервових центрів, які забезпечують функції уваги, мислення, регуляції рухів. Окрім того, трудовий процес користувачів комп'ютерів відзначається значними інформаційними навантаженнями.

Трудова діяльність користувачів комп'ютерів відбувається у певному виробничому середовищі, яке впливає на їх функціональний стан. Найбільш значимі – фізичні фактори виробничого середовища, до яких належать електромагнітні хвилі різних частотних діапазонів, електростатичні поля, шум, параметри мікроклімату та ціла низка світлотехнічних показників. Вплив хімічних та, особливо, біологічних факторів виробничого середовища на користувачів комп'ютерів – значно менший.

Сучасна професія користувача візуальних дисплейних терміналів (ВДТ) належить до розумової праці, яка характеризується: високою напруженістю зорових функцій; одноманітною позою; великою кількістю стереотипних високо координованих рухів, що виконуються лише м'язами кистей рук на фоні малої загальної рухової активності; значним нервово-емоційним компонентом, особливо в умовах дефіциту часу; роботою з великими масивами інформації, що викликає активізацію уваги та інших вищих психічних функцій. Крім того, при роботі з дисплеями на електронно-променевих трубках виникає вплив на користувача цілої низки факторів фізичної природи – електростатичні поля, радіочастотне та рентгенівське випромінювання тощо. Діяльність професіоналів можна поділити на три групи:

– діяльність, яка пов'язана з виконанням нескладних багаторазово повторюваних операцій, що не вимагають великого розумового напруження;

– діяльність, яка пов'язана із здійсненням логічних операцій, що постійно повторюються;

– діяльність, коли в процесі роботи необхідно приймати рішення за відсутності заздалегідь відомого алгоритму.

Професійні якості та виробничий досвід, які визначають внутрішні засоби діяльності, обумовлюють надійну та безпомилкову діяльність користувачів комп'ютерів, дозволяють знаходити безпечні методи

розв'язання виробничих завдань навіть у нестандартних ситуаціях. Зовнішні засоби діяльності, які в основному визначаються ергономічними показниками щодо організації робочого місця, форми та параметрів його елементів, просторового розташування основного і допоміжного устаткування, можуть суттєво знизити фізичні та психофізіологічні навантаження, що діють на користувачів комп'ютерів. особливості роботи користувачів комп'ютерів у професійних операторів частіше зустрічаються порушення органів зору, опорно-рухового апарату, центральної нервової, серцево-судинної, імунної та статевої систем, захворювання шкіри.

Інформаційне перевантаження користувачів ВДТ супроводжується низкою специфічних захворювань, які називають інформаційними.

Дослідження, показали, що робота з обслуговування ВДТ супроводжується підвищеним напруженням зору, інтенсивністю і монотонністю праці, збільшенням статичних навантажень, нервово-психічним напруженням, впливом різного виду випромінювань та ін. Внаслідок цього серед операторів ВДТ, як зазначають фахівці Всесвітньої організації охорони здоров'я, частіше, ніж в інших групах працюючих, трапляються такі професійні захворювання, як передчасна стомлюваність, погіршення зору, м'язові і головні болі, психічні й нервові розлади, хвороби серцево-судинної системи, онкологічні захворювання та ін. Вважається, що стан організму операторів ВДТ визначається комплексним впливом факторів трудового процесу і середовища, значення яких є неоднаковим.

6.2 Вимоги до організації робочих міст

Організація робочого місця оператора повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСанПіН 3.3.2.007-98

Відстань від екрана до ока працівника визначається згідно з вимогами.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана ВДТ, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98 (v0007282-98).

Під матричні принтери потрібно підкладати вібраційні килимки для гасіння вібрації та шуму.

За потреби особливої концентрації уваги під час виконання робіт суміжні робочі місця операторів необхідно відділяти одне від одного перегородками висотою 1,5 - 2 м.

При організації робочого місця, яке передбачає роботу з ЕОМ з ВДТ і ПП для керування технологічним обладнанням (станки з програмним управлінням, роботизовані технологічні комплекси, обладнання для гнучкого автоматизованого виробництва тощо), слід передбачати: достатній простір для оператора ЕОМ з ВДТ і ПП; вільну досяжність органів ручного керування в зоні моторного поля (відстань по висоті - 900-1330 мм, по глибині - 400-500 мм); розташування екрана ВДТ у робочій зоні, яке буде забезпечувати зручність зорового спостереження у вертикальній площині під кутом +-30 від лінії зору оператора, а також зручність використання ВДТ під час коригування керуючих про- грам одночасно з виконанням основних виробничих операцій; можливість повертання екрана ВДТ навколо горизонтальної та вертикальної вісей.

6.3 Вимоги до електробезпеки

З метою запобігання ушкодженням, що можуть статися через ураження електричним струмом, загоряння, коротке замикання тощо, розроблено загальний стандарт безпеки IEC 950. Загальним стандартом електробезпечності для країн Європейської співдружності є Cemark.

Приміщення із робочими місцями користувачів комп’ютерів для забезпечення електробезпеки обладнання, а також для захисту від ураження електричним струмом самих користувачів ПК повинні мати

достатні технічні засоби захисту відповідно до НПАОП 40.1-1.07-01 “Правила експлуатації електрозахисних засобів”, НПАОП 40.1-1.21-98 “Правила безпечної експлуатації електроустановок споживачів”, НПАОП 40.1-1.32-01 “Правила будови електроустановок. Електрообладнання спеціальних установок”

ЕОМ, периферійні пристрої ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ, інше устаткування (апарати управління, контрольно-вимірювальні прилади, світильники тощо), електропроводи та кабелі за виконанням та ступенем захисту мають відповідати класу зони за ПУЕ, мати апаратуру захисту від струму короткого замикання та інших аварійних режимів.

Під час монтажу та експлуатації ліній електромережі необхідно повністю унеможливити виникнення електричного джерела загоряння внаслідок короткого замикання та перевантаження проводів, обмежувати застосування проводів з легкозаймистою ізоляцією і, за можливості, перейти на негорючу ізоляцію.

Лінія електромережі для живлення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ виконується як окрема групова трипровідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів.

Використання нульового робочого провідника як нульового захисного провідника забороняється. Нульовий захисний провід прокладається від стійки групового розподільчого щита, розподільчого пункту до розеток живлення. Не допускається підключення на щиті до одного контактного затискача нульового робочого та нульового захисного провідників. Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі повинна бути не менше площі перерізу фазового провідника.

У приміщенні, де одночасно експлуатується або обслуговується більше п'яти персональних ЕОМ, на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

Усі провідники повинні відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам ПУЕ.

ПЕОМ, периферійні пристрої ПЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ повинні підключатися до електромережі тільки з допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників повинні мати спеціальні контакти для підключення нульового захисного провідника. Конструкція їх має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при відключенні має бути зворотним. Необхідно унеможливити з'єднання контактів фазових провідників з контактами нульового захисного провідника.

Неприпустимим є підключення ПЕОМ та периферійних пристроїв ПЕОМ до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв.

Індивідуальні та групові штепсельні з'єднання та електророзетки необхідно монтувати на негорючих або важкогорючих пластинах з урахуванням вимог ПУЕ та Правил пожежної безпеки в Україні.

Електромережі штепсельних з'єднань та електророзеток для живлення ПЕОМ, периферійних пристроїв слід виконувати за магістральною схемою, по 3…6 з’єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 36 В за

своєю конструкцією повинні відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В і мають бути пофарбовані в колір, який візуально значно відрізняється від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

Електромережу штепсельних розеток для живлення ПЕОМ, периферійних пристроїв ПЕОМ при розташуванні їх уздовж стін приміщення прокладають по підлозі поряд зі стінами приміщення, як правило, в металевих трубах і гнучких металевих рукавах з відводами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання.

При розташуванні в приміщенні за його периметром до 5 ПЕОМ, використанні трипровідникового захищеного проводу або кабелю в оболонці з негорючого або важкогорючого матеріалу дозволяється прокладання їх без металевих труб та гнучких металевих рукавів.

Електромережу штепсельних розеток для живлення ПЕОМ при розташуванні їх у центрі приміщення, прокладають у каналах або під знімною підлогою в металевих трубах або гнучких металевих рукавах. При цьому не дозволяється застосовувати провід і кабель в ізоляції з вулканізованої гуми та інші матеріали, що містять сірку. Відкрита прокладка кабелів під підлогою забороняється. Металеві труби та гнучкі металеві рукави повинні бути заземлені. Заземлення повинно відповідати вимогам НПАОП 40.1-1.21-98.

Є неприпустимими:

– експлуатація кабелів та проводів з пошкодженою або такою, що втратила захисні властивості за час експлуатації, ізоляцією; залишення під напругою кабелів та проводів з неізольованими провідниками;

– застосування саморобних подовжувачів, які не відповідають вимогам ПВЕ до переносних електропроводок;

– застосування для опалення приміщення нестандартного (саморобного) електронагрівального обладнання або ламп розжарювання;

– користування пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електровиробами, а також лампами, скло яких має сліди затемнення або випинання;

– підвішування світильників безпосередньо на струмопровідних проводах, обгортання електроламп і світильників папером, тканиною та іншими горючими матеріалами, експлуатація їх зі знятими ковпаками (розсіювачами);

– використання електроапаратури та приладів в умовах, що не відповідають вказівкам (рекомендаціям) підприємств-виготовлювачів.

Для підключення переносної електроапаратури застосовують гнучкі проводи в надійній ізоляції.

Тимчасова електропроводка від переносних приладів до джерел живлення виконується найкоротшим шляхом без заплутування проводів у конструкціях машин, приладів та меблях. Доточувати проводи можна тільки шляхом паяння з наступним старанним ізолюванням місць з'єднання.

6.4 Перша допомога при ураженні електричним струмом

Основною умовою успішного надання першої допомоги при ураженні електричним струмом є швидка та правильна дія тих, хто надає допомогу. В той же час зволікання, запізніле та некваліфіковане надання допомоги може призвести до смерті потерпілого. Ось чому важливо, щоб кожен знав і вмів правильно та швидко надати необхідну допомогу потерпілому.

Перша допомога при ураженні електричним струмом складається з двох етапів: звільнення потерпілого від дії електричного струму; надання йому необхідної долікарської допомоги.

При ураженні електричним струмом необхідно, перш за все, негайно звільнити потерпілого від дії струму, оскільки від тривалості такої дії суттєво залежить важкість електротравми. Необхідно пам'ятати, що діяти

треба швидко, але в той же час обережно, щоб самому не потрапити під напругу. Найбезпечніший спосіб звільнення потерпілого від дії електричного струму - це вимкнення електроустановки, до якої доторкається потерпілий, за допомогою найближчого вимикача, рубильника чи іншого апарата для знеструмлення.

Способи звільнення потерпілого від дії електричного струму:

– знеструмлення установки за допомогою вимикача (рубильника);

– відкидання проводу сухою палицею;

– перерубування проводів сокирою;

– відтягнення потерпілого від електромережі.

Якщо вимкнути установку досить швидко немає змоги, то необхідно звільнити потерпілого від струмовідних частин, до яких він доторкається.

Для звільнення потерпілого від струмовідних частин або проводу напругою до 1000 В необхідно скористатись палицею, дошкою або будь-яким іншим сухим предметом, що не проводить електричний струм.

При цьому бажано ізолювати себе від землі (стати на суху дошку, неструмопровідну підстилку). Можна також перерубати проводи сокирою з сухим дерев'яним топорищем або перекусити їх інструментом з ізолювальними рукоятками (кусачками, пасатижами тощо). Перерубувати чи перекусувати проводи необхідно пофазно, тобто кожен провід окремо, та на різній висоті.

Для звільнення потерпілого від струмовідних частин можна також відтягнути його за одяг (якщо він сухий і відстає від тіла), наприклад, за поли халата чи піджака. При цьому необхідно уникати доторкання до навколишніх металевих предметів та відкритих частин тіла. Для ізоляції рук, особливо коли необхідно доторкнутися до тіла потерпілого, рятівник повинен надягнути діелектричні рукавички або обмотати руку сухим одягом (наприклад, шаликом або сухою тканиною). Відтягувати потерпілого від струмопровідних ділянок рекомендується однією рукою.

Якщо електричний струм проходить у землю через потерпілого і він судомно стискає у руці один струмопровідний елемент (наприклад, провід), то простіше припинити дію струму, відокремивши потерпілого від землі (підсунувши під нього суху дошку або відтягнувши ноги від землі мотузкою, чи за сухі штани). При цьому необхідно пам'ятати про власну безпеку.

Для звільнення потерпілого від струмовідних частин та проводів, що знаходяться під напругою понад 1000 В, необхідно надягнути діелектричні рукавички та боти і діяти ізолювальною штангою або кліщами, що розраховані на відповідну напругу. При цьому необхідно пам'ятати про небезпеку крокової напруги, якщо провід лежить на землі.

6.5 Пожежна безпека

Пожежі у обчислювальних центрах (ОЦ) становлять особливу небезпеку, тому що пов'язані з великими матеріальними втратами. Характерна особливість ОЦ - невеликі площі приміщень. Як відомо пожежа може виникнути при взаємодії горючих речовин, окислення і джерел запалювання. У приміщеннях ОЦ присутні всі три основні чинника, необхідні для виникнення пожежі.

Горючими компонентами на ОЦ є: матеріали для акустичної і естетичної обробки приміщень, перегородки, двері, підлоги, перфокарти і перфострічки, ізоляція кабелів і ін..

Протипожежний захист - це комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки людей, запобігання пожежі, обмеження її розповсюдження, а також на створення умов для успішного гасіння пожежі.

Джерелами запалювання у ОЦ можуть бути електронні схеми від ЕОМ, прилади, застосовувані для технічного обслуговування, пристрої електроживлення, кондиціонування повітря, де внаслідок різних порушень

утворюються перегріті елементи, електричні іскри та дуги, здатні викликати загоряння горючих матеріалів.

У сучасних ЕОМ дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості один від одного розташовуються сполучні дроти, кабелі. При протіканні по них електричного струму виділяється значна кількість теплоти. При цьому можливо оплавлення ізоляції. Для відведення надлишкової теплоти від ЕОМ служать системи вентиляції та кондиціонування повітря. При постійному дії ці системи представляють собою додаткову пожежну небезпеку.

Енергопостачання ОЦ здійснюється від трансформаторної станції і двигун-генераторних агрегатів. На трасформаторних підстанціях особливу небезпеку представляють трансформатори з масляним охолодженням. У зв'язку з цим перевагуслід віддавати сухим транформатором.

Пожежна небезпека двигун-генераторних агрегатів обумовлена можливістю коротких замикань, перевантаження, електричного іскріння. Для безпечної роботи необхідний правильний розрахунок і вибір апаратів захисту. При поведінці обслуговуючих, ремонтних і профілактичних робіт використовуються різні мастильні речовини, легкозаймисті рідини, прокладаються тимчасові електропровідниками, ведуть пайку та чистку окремих вузлів. Виникає додаткова пожежна небезпека, яка потребує додаткових заходів пожежного захисту. Зокрема, при роботі з паяльником слід використовувати неспалену підставку з нескладними пристроями для зменшення споживаної потужності в неробочому стані.

Для більшості приміщень ОЦ встановлена II категорія пожежної небезпеки В.

Однією з найбільш важливих завдань пожежної захисту є захист будівельних приміщень від руйнувань та забезпечення їх достатньої міцності в умовах впливу високих температур при пожежі. З огляду на високу вартість електронногоустаткування ОЦ, а також категорію його

пожежної небезпеки, будинки для ОЦ і частини будинку іншого призначення, в яких передбачено розміщення ЕОМ повинні бути 1 і 2 ступеня вогнестійкості.

Для виготовлення будівельних конструкцій використовуються, як правило, цегла, залізобетон, скло, метал та інші негорючі матеріали. Застосування дерева повинна бути обмежено, а в разі використання необхідно просочувати його вогнезахисними складами. У ОЦ протипожежні перешкоди у вигляді перегородок з негорючих матеріалів встановлюють між машинними залами.

До засобів гасіння пожежі, призначених для локалізації невеликих загранй, відносяться пожежні стовбури, внутрішні пожежні водопроводи, вогнегасники, сухий пісок, азбестові ковдри і т. п.

У будинках ОЦ пожежні крани встановлюються в коридорах, на майданчиках сходових клітин та входів. Вода використовується для гасіння пожеж у приміщеннях програмістів, бібліотеках, допоміжних і службових приміщеннях. Застосування води в машинних залах ЕОМ, сховищах носіїв інформації, приміщеннях контрольно-вимірювальних приладів, зважаючи на небезпеку пошкодження або повного виходу з ладу дорогого устаткування можливо у виняткових випадках, коли пожежа приймає загрозливо великі розміри. При цьому кількість води повинна бути мінімальною, а пристрої ЕОМ необхідно захистити від попадання води, накриваючи їх брезентом або полотном.

Для гасіння пожеж на початкових стадіях широко застосовуються вогнегасники. По виду використовуваного вогнегасної речовини вогнегасники поділяються на такі основні групи.

Пінні вогнегасники, застосовуються для гасіння палаючих рідин, різних матеріалів, конструктивних елементів і устаткування, крім електрообладнання, що знаходиться під напругою.

Газові вогнегасники застосовуються для гасіння рідких і твердих речовин, а також електроустановок, що знаходяться під напругою.

Для виявлення стадії загоряння та оповіщення службу пожежної охорони використовують системи автоматичної пожежної сигналізації (АПС). Крім того, вони можуть самостійно забезпечувати дію установки пожежогасіння, коли пожежа ще не досяг великих розмірів. Системи АПС складаються з пожежних сповіщувачів, ліній зв'язку і прийомних пультів (станцій).

Ефективність застосування систем АПС визначається правильним вибором типу сповіщувачів та місць їх встановлення. При виборі пожежних сповіщувачів необхідно враховувати конкретні умови їхньої експлуатації: особливості приміщення і повітряного середовища, наявність пожежних матеріалів, характер можливого горіння, специфіку технологічного процесу і т.п.

Відповідно до "Типових правил пожежної безпеки для промислових підприємств" зали ЕОМ, приміщення для зовнішніх запам'ятовуючих пристроїв, підготовки даних, сервісної апаратури, архівів, копіювально-розмножувального устаткування і т.п. необхідно обладнати димовими пожежними сповіщувачами.

ВИСНОВОК

В рамках дипломної роботи мною було розроблено віртуальний сервер 1с на платформі MS Azure.

За основу була взята віртуальна машина на базі Windows Server 2019 а також встановленій на неї сервер MS SQL 2019 Standard. Дання зв'язка забезпечує достатньо велику продуктивність для поставленої задачі, а також в парі з віртуальним сервером побудованим на базі 4-х ядерного Intel Xeon позбавляє нас від основних недостатків існуючого рішення.

Для забезпечення конфіденційності інформації було організовано VPN-з'єднання. Воно забезпечує контроль доступу до серверу а також дозволяє відслідковувати хто, коли і звідки підключався до віртуальної мережі.

Усі налагоджувані роботи проводилися за допомогою порталу Azure а також на віртуальному сервері. В процесі розробки проекту були реалізовані такі технології: VPN, Virtual machine, Virtual network.

ЛІТЕРАТУРА

1. Офіційна сторінка компанії «Європа-Дніпро» https://evropa.dp.ua/
2. Результати тестування головних хмарних платформ https://habr.com/ru/post/328916/
3. Інструкції з налаштування віртуальних машин на порталі Azure https://docs.microsoft.com/ru-ru/azure/
4. Налаштування серверу 1с https://efsol.ru/manuals/1s-setup.html

Додаток А

Схема топології мережі

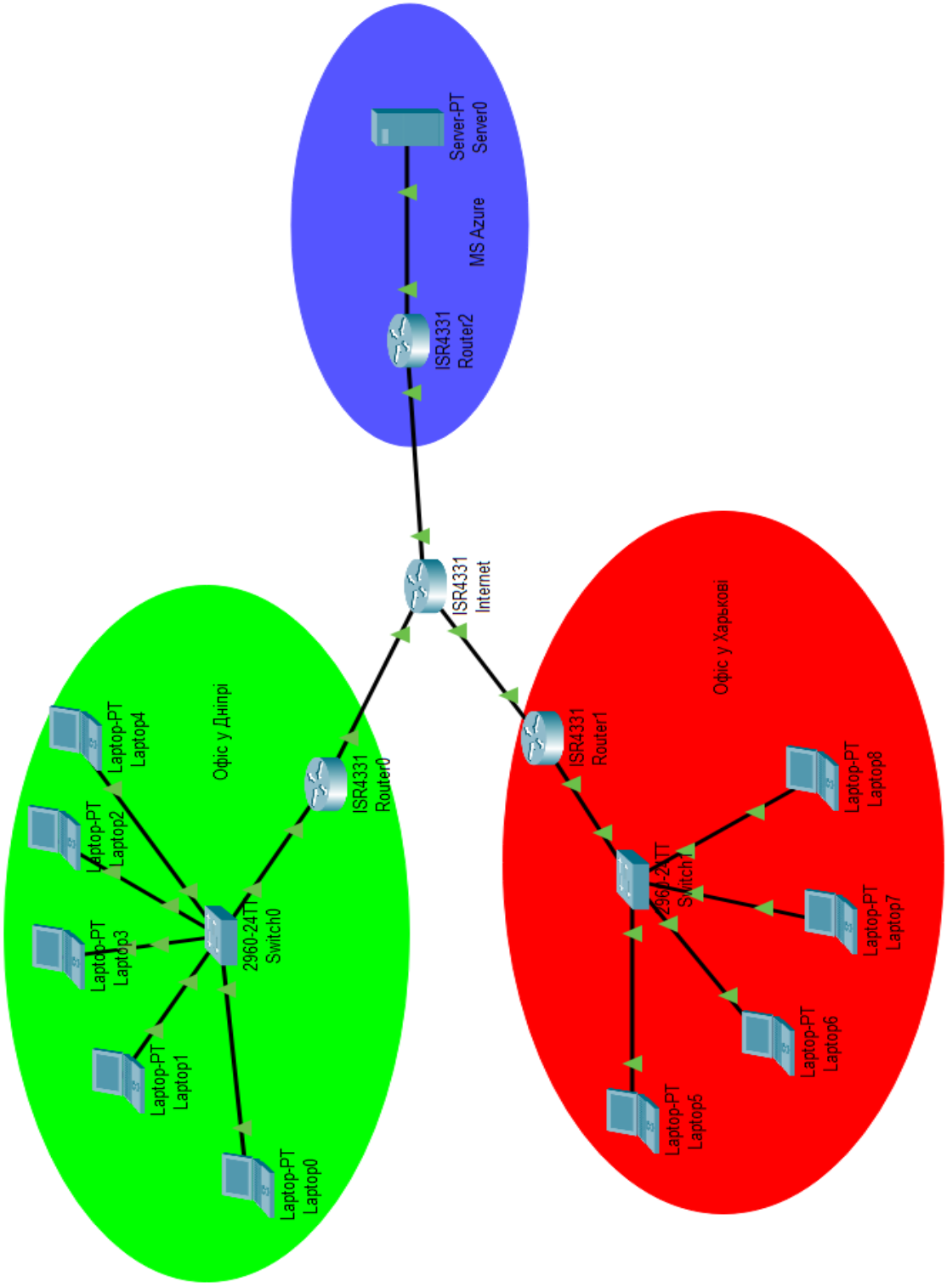
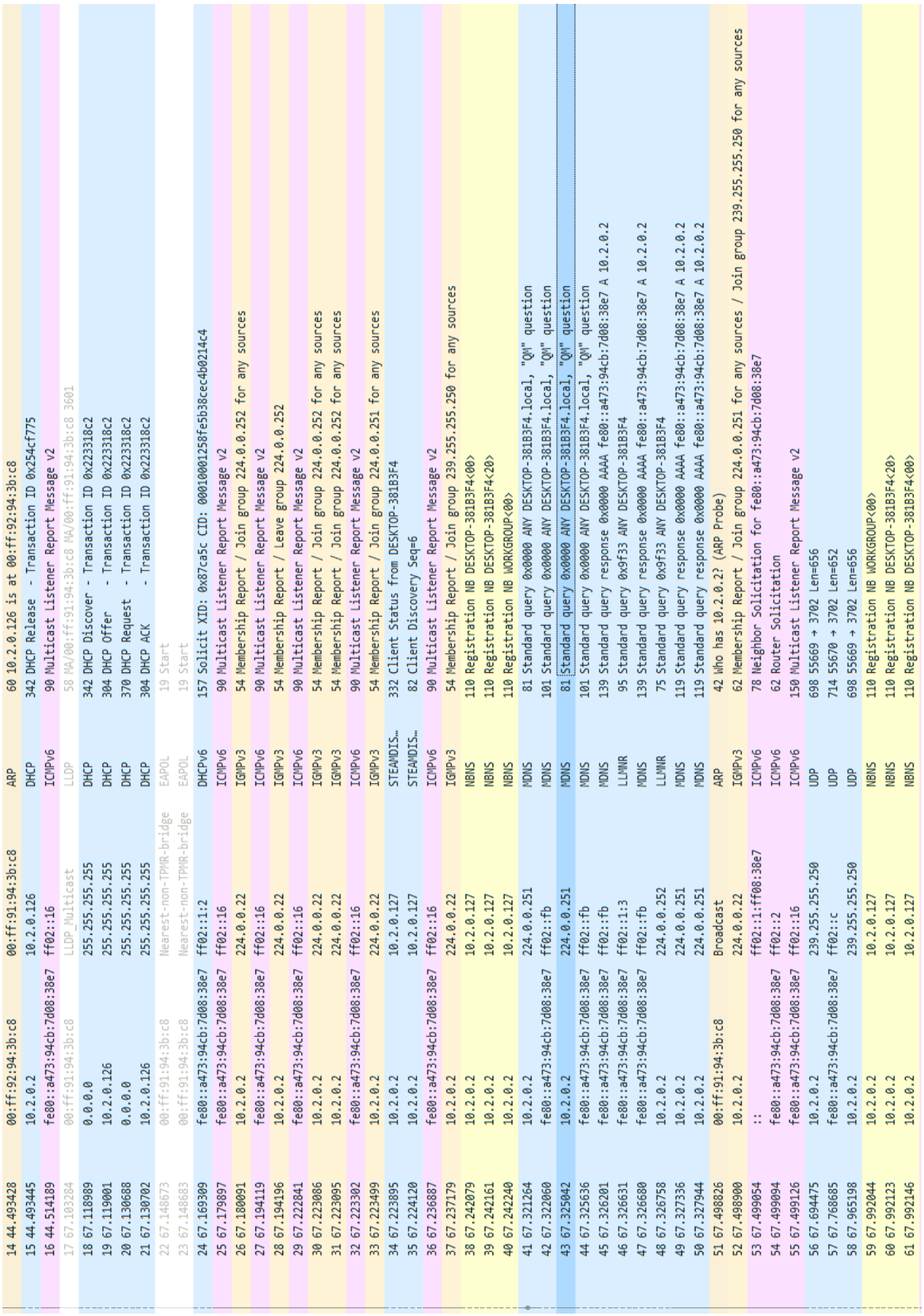


Рисунок ДА.1 – Схема топології мережі

Додаток Б

Перехвачені пакети програмою Wireshark



14	44.493428	00:ff:92:94:3b:c8	00:ff:91:94:3b:c8	ARP	60 10.2.0.126 is at 00:ff:92:94:3b:c8
15	44.493445	10.2.0.2	10.2.0.126	DHCP	342 DHCP Release - Transaction ID 0x254cf775
16	44.514189	fe80::a473:94cb:7d08:38e7	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
17	67.103284	00:ff:91:94:3b:c8	LLDP_Multicast	LLDP	58 MA/00:ff:91:94:3b:c8 MA/00:ff:91:94:3b:c8 3601
18	67.118989	0.0.0.0	255.255.255.255	DHCP	342 DHCP Discover - Transaction ID 0x223318c2
19	67.119001	10.2.0.126	255.255.255.255	DHCP	304 DHCP Offer - Transaction ID 0x223318c2
20	67.130688	0.0.0.0	255.255.255.255	DHCP	370 DHCP Request - Transaction ID 0x223318c2
21	67.130702	10.2.0.126	255.255.255.255	DHCP	304 DHCP ACK - Transaction ID 0x223318c2
22	67.148673	00:ff:91:94:3b:c8	Nearest-non-TPMR-bridge	EAPOL	19 Start
23	67.148683	00:ff:91:94:3b:c8	Nearest-non-TPMR-bridge	EAPOL	19 Start
24	67.169309	fe80::a473:94cb:7d08:38e7	ff02::1:2	DHCPv6	157 Solicit XID: 0x87ca5c CID: 000100012158fe5b38cec4b0214c4
25	67.179897	fe80::a473:94cb:7d08:38e7	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
26	67.180091	10.2.0.2	224.0.0.22	IGMPv3	54 Membership Report / Join group 224.0.0.252 for any sources
27	67.194119	fe80::a473:94cb:7d08:38e7	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
28	67.194196	10.2.0.2	224.0.0.22	IGMPv3	54 Membership Report / Leave group 224.0.0.252
29	67.222841	fe80::a473:94cb:7d08:38e7	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
30	67.223086	10.2.0.2	224.0.0.22	IGMPv3	54 Membership Report / Join group 224.0.0.252 for any sources
31	67.223095	10.2.0.2	224.0.0.22	IGMPv3	54 Membership Report / Join group 224.0.0.252 for any sources
32	67.223302	fe80::a473:94cb:7d08:38e7	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
33	67.223499	10.2.0.2	224.0.0.22	IGMPv3	54 Membership Report / Join group 224.0.0.251 for any sources
34	67.223895	10.2.0.2	10.2.0.127	STEAMDIS…	332 Client Status from DESKTOP-381B3F4
35	67.224120	10.2.0.2	10.2.0.127	STEAMDIS…	82 Client Discovery Seq=6
36	67.236887	fe80::a473:94cb:7d08:38e7	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
37	67.237179	10.2.0.2	224.0.0.22	IGMPv3	54 Membership Report / Join group 239.255.255.250 for any sources
38	67.242079	10.2.0.2	10.2.0.127	NBNS	110 Registration NB DESKTOP-381B3F4<00>
39	67.242161	10.2.0.2	10.2.0.127	NBNS	110 Registration NB DESKTOP-381B3F4<20>
40	67.242240	10.2.0.2	10.2.0.127	NBNS	110 Registration NB WORKGROUP<00>
41	67.321264	10.2.0.2	224.0.0.251	MDNS	81 Standard query 0x0000 ANY DESKTOP-381B3F4.local, "QM" question
42	67.322060	fe80::a473:94cb:7d08:38e7	ff02::fb	MDNS	101 Standard query 0x0000 ANY DESKTOP-381B3F4.local, "QM" question
43	67.325042	10.2.0.2	224.0.0.251	MDNS	81 Standard query 0x0000 ANY DESKTOP-381B3F4.local, "QM" question
44	67.325636	fe80::a473:94cb:7d08:38e7	ff02::fb	MDNS	101 Standard query 0x0000 ANY DESKTOP-381B3F4.local, "QM" question
45	67.326201	fe80::a473:94cb:7d08:38e7	ff02::fb	MDNS	139 Standard query response 0x0000 AAAA fe80::a473:94cb:7d08:38e7 A 10.2.0.2
46	67.326631	fe80::a473:94cb:7d08:38e7	ff02::1:3	LLMNR	95 Standard query 0x9f33 ANY DESKTOP-381B3F4
47	67.326680	fe80::a473:94cb:7d08:38e7	ff02::fb	MDNS	139 Standard query response 0x0000 AAAA fe80::a473:94cb:7d08:38e7 A 10.2.0.2
48	67.326758	10.2.0.2	224.0.0.252	LLMNR	75 Standard query 0x9f33 ANY DESKTOP-381B3F4
49	67.327336	10.2.0.2	224.0.0.251	MDNS	119 Standard query response 0x0000 AAAA fe80::a473:94cb:7d08:38e7 A 10.2.0.2
50	67.327944	10.2.0.2	224.0.0.251	MDNS	119 Standard query response 0x0000 AAAA fe80::a473:94cb:7d08:38e7 A 10.2.0.2
51	67.498826	00:ff:91:94:3b:c8	Broadcast	ARP	42 Who has 10.2.0.2? (ARP Probe)
52	67.498900	10.2.0.2	224.0.0.22	IGMPv3	62 Membership Report / Join group 224.0.0.251 for any sources / Join group 239.255.255.250 for any sources
53	67.499054	::	ff02::1:ff08:38e7	ICMPv6	78 Neighbor Solicitation for fe80::a473:94cb:7d08:38e7
54	67.499094	fe80::a473:94cb:7d08:38e7	ff02::2	ICMPv6	62 Router Solicitation
55	67.499126	fe80::a473:94cb:7d08:38e7	ff02::16	ICMPv6	150 Multicast Listener Report Message v2
56	67.694475	10.2.0.2	239.255.255.250	UDP	698 55669 → 3702 Len=656
57	67.768685	fe80::a473:94cb:7d08:38e7	ff02::c	UDP	714 55670 → 3702 Len=652
58	67.965198	10.2.0.2	239.255.255.250	UDP	698 55669 → 3702 Len=656
59	67.992044	10.2.0.2	10.2.0.127	NBNS	110 Registration NB WORKGROUP<00>
60	67.992123	10.2.0.2	10.2.0.127	NBNS	110 Registration NB DESKTOP-381B3F4<20>
61	67.992146	10.2.0.2	10.2.0.127	NBNS	110 Registration NB DESKTOP-381B3F4<00>

Рисунок ДБ.1 – Перехвачені пакети програмою Wireshark

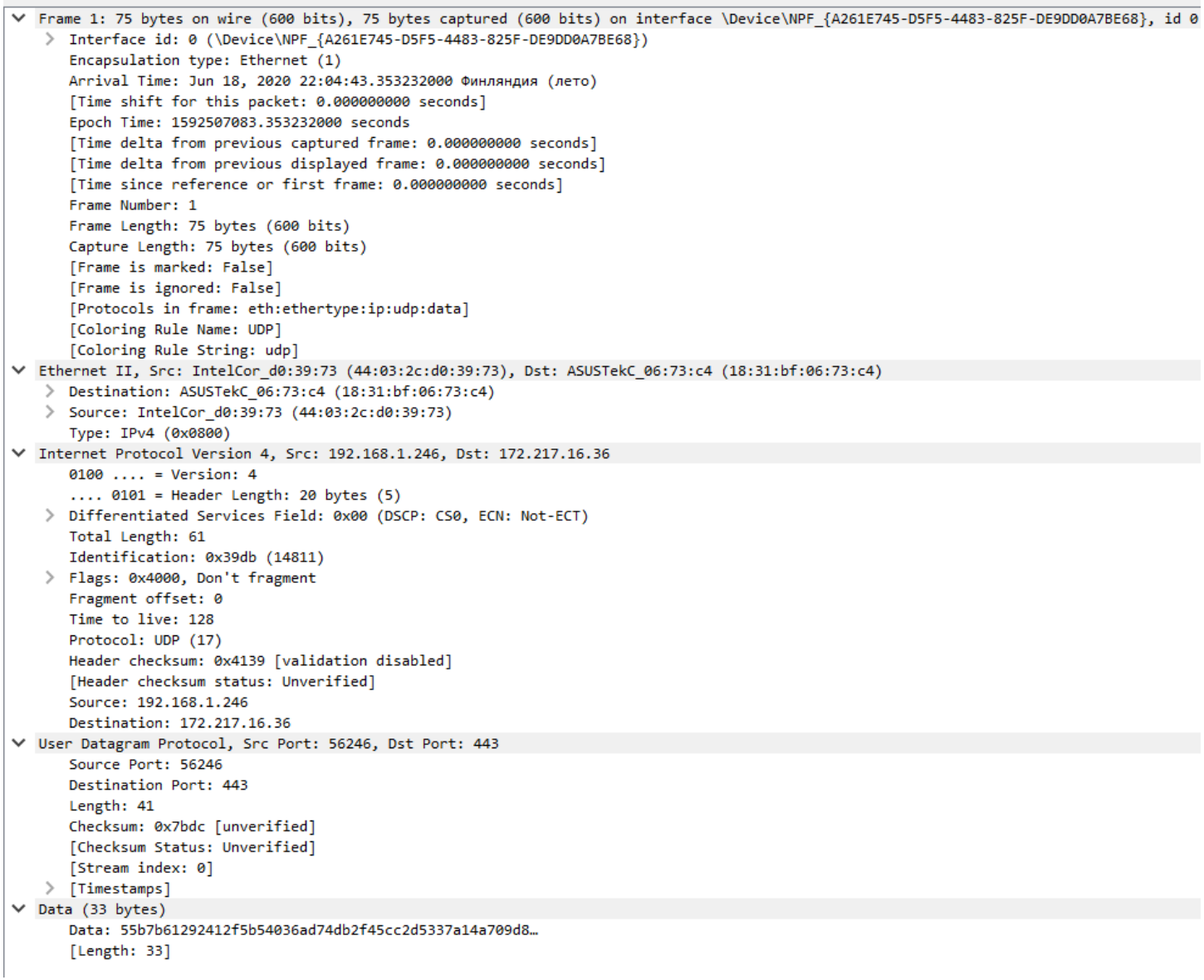


Рисунок ДБ.2 – Інформація про один з пакетів

Додаток В

Лог файли програми OpenVPN

Thu Jun 18 13:26:26 2020 OpenVPN 2.4.8 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] [AEAD] built on Oct 31 2019

Thu Jun 18 13:26:26 2020 Windows version 6.2 (Windows 8 or greater) 64bit

Thu Jun 18 13:26:26 2020 library versions: OpenSSL 1.1.0l 10 Sep 2019, LZO 2.10

Enter Management Password:

Thu Jun 18 13:26:26 2020 MANAGEMENT: TCP Socket listening on [AF_INET]127.0.0.1:25340

Thu Jun 18 13:26:26 2020 Need hold release from management interface, waiting...

Thu Jun 18 13:26:26 2020 MANAGEMENT: Client connected from [AF_INET]127.0.0.1:25340

Thu Jun 18 13:26:26 2020 MANAGEMENT: CMD 'state on'

Thu Jun 18 13:26:26 2020 MANAGEMENT: CMD 'log all on'

Thu Jun 18 13:26:26 2020 MANAGEMENT: CMD 'echo all on'

Thu Jun 18 13:26:26 2020 MANAGEMENT: CMD 'bytecount 5'

Thu Jun 18 13:26:26 2020 MANAGEMENT: CMD 'hold off'

Thu Jun 18 13:26:26 2020 MANAGEMENT: CMD 'hold release'

Thu Jun 18 13:26:32 2020 MANAGEMENT: CMD 'password [...]'

Thu Jun 18 13:26:32 2020 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this

Thu Jun 18 13:26:32 2020 Outgoing Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication

Thu Jun 18 13:26:32 2020 Incoming Control Channel Authentication: Using 256 bit message hash 'SHA256' for HMAC authentication

Thu Jun 18 13:26:32 2020 MANAGEMENT: >STATE:1592475992,RESOLVE,,,,,,

Thu Jun 18 13:26:32 2020 TCP/UDP: Preserving recently used remote address: [AF_INET]52.143.156.119:443

Thu Jun 18 13:26:32 2020 Socket Buffers: R=[65536->65536] S=[65536->65536]

Thu Jun 18 13:26:32 2020 Attempting to establish TCP connection with [AF_INET]52.143.156.119:443 [nonblock]

Thu Jun 18 13:26:32 2020 MANAGEMENT: >STATE:1592475992,TCP_CONNECT,,,,,,

Thu Jun 18 13:26:33 2020 TCP connection established with [AF_INET]52.143.156.119:443

Thu Jun 18 13:26:33 2020 TCP_CLIENT link local: (not bound)

Thu Jun 18 13:26:33 2020 TCP_CLIENT link remote: [AF_INET]52.143.156.119:443

Thu Jun 18 13:26:33 2020 MANAGEMENT: >STATE:1592475993,WAIT,,,,,,

Thu Jun 18 13:26:33 2020 MANAGEMENT: >STATE:1592475993,AUTH,,,,,,

Thu Jun 18 13:26:33 2020 TLS: Initial packet from [AF_INET]52.143.156.119:443, sid=82125334 dec6c771

Thu Jun 18 13:26:33 2020 VERIFY OK: depth=2, C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA

Thu Jun 18 13:26:33 2020 VERIFY OK: depth=1, C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA

Thu Jun 18 13:26:33 2020 VERIFY KU OK

Thu Jun 18 13:26:33 2020 Validating certificate extended key usage

Thu Jun 18 13:26:33 2020 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication

Thu Jun 18 13:26:33 2020 VERIFY EKU OK

Thu Jun 18 13:26:33 2020 VERIFY X509NAME OK: C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=9e4a0034-b5d7-49a0-a464-7f52597115b0.vpn.azure.com

Thu Jun 18 13:26:33 2020 VERIFY OK: depth=0, C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, CN=9e4a0034-b5d7-49a0-a464-7f52597115b0.vpn.azure.com

Thu Jun 18 13:26:34 2020 WARNING: 'link-mtu' is used inconsistently, local='link-mtu 1551', remote='link-mtu 1500'

Thu Jun 18 13:26:34 2020 WARNING: 'tun-mtu' is present in local config but missing in remote config, local='tun-mtu 1500'

Thu Jun 18 13:26:34 2020 Control Channel: TLSv1.2, cipher TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA

Thu Jun 18 13:26:34 2020 [9e4a0034-b5d7-49a0-a464-7f52597115b0.vpn.azure.com] Peer Connection Initiated with [AF_INET]52.143.156.119:443

Thu Jun 18 13:26:35 2020 MANAGEMENT: >STATE:1592475995,GET_CONFIG,,,,,,

Thu Jun 18 13:26:35 2020 SENT CONTROL [9e4a0034-b5d7-49a0-a464-7f52597115b0.vpn.azure.com]: 'PUSH_REQUEST' (status=1)

Thu Jun 18 13:26:35 2020 PUSH: Received control message: 'PUSH_REPLY,route 10.1.0.0 255.255.0.0,route-gateway 10.2.0.1,topology subnet,ifconfig 10.2.0.2 255.255.255.128,cipher AES-256-GCM'

Thu Jun 18 13:26:35 2020 OPTIONS IMPORT: --ifconfig/up options modified

Thu Jun 18 13:26:35 2020 OPTIONS IMPORT: route options modified

Thu Jun 18 13:26:35 2020 OPTIONS IMPORT: route-related options modified

Thu Jun 18 13:26:35 2020 OPTIONS IMPORT: data channel crypto options modified

Thu Jun 18 13:26:35 2020 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key

Thu Jun 18 13:26:35 2020 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key

Thu Jun 18 13:26:35 2020 interactive service msg_channel=640

Thu Jun 18 13:26:35 2020 ROUTE_GATEWAY 192.168.76.254/255.255.255.0 I=13 HWADDR=8c:ec:4b:02:14:c4

Thu Jun 18 13:26:35 2020 open_tun

Thu Jun 18 13:26:35 2020 TAP-WIN32 device [Подключение по локальной сети] opened: \\.\Global\{91943BC8-DFF9-435B-BBB9-2B8E4EA3C1B6}.tap

Thu Jun 18 13:26:35 2020 TAP-Windows Driver Version 9.24

Thu Jun 18 13:26:35 2020 Set TAP-Windows TUN subnet mode network/local/netmask = 10.2.0.0/10.2.0.2/255.255.255.128 [SUCCEEDED]

Thu Jun 18 13:26:35 2020 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.2.0.2/255.255.255.128 on interface {91943BC8-DFF9-435B-BBB9-2B8E4EA3C1B6} [DHCP-serv: 10.2.0.126, lease-time: 31536000]

Thu Jun 18 13:26:35 2020 Successful ARP Flush on interface [14] {91943BC8-DFF9-435B-BBB9-2B8E4EA3C1B6}

Thu Jun 18 13:26:35 2020 MANAGEMENT: >STATE:1592475995,ASSIGN_IP,,10.2.0.2,,,,

Thu Jun 18 13:26:40 2020 TEST ROUTES: 1/1 succeeded len=1 ret=1 a=0 u/d=up

Thu Jun 18 13:26:40 2020 MANAGEMENT: >STATE:1592476000,ADD_ROUTES,,,,,,

Thu Jun 18 13:26:40 2020 C:\WINDOWS\system32\route.exe ADD 10.1.0.0 MASK 255.255.0.0 10.2.0.1

Thu Jun 18 13:26:40 2020 Route addition via service succeeded

Thu Jun 18 13:26:40 2020 Initialization Sequence Completed

Thu Jun 18 13:26:40 2020 MANAGEMENT: >STATE:1592476000,CONNECTED,SUCCESS,10.2.0.2,52.143.156.119,443,192.168.76.211,50545