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

студента Тюха Олександра Віталійовича
(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 підприємства з детальним опрацюванням побудови та налаштування захищеної корпоративної мережі на основі технології VPN.
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Гнатушенко В.В.			
розділів:				
апаратний розділ	проф. Гнатушенко В.В.			
розрахунок мережі	ас. Панферова Я.В.			
економічний розділ	ст. викл. Яремчук І.О.			
охорона праці	доц. Яворська О.О.			

Рецензент	доц. Реута О.В.			

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2020

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

"_" _____ 2020 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавр

студента Тюх О.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 підприємства з детальним опрацюванням побудови та налаштування захищеної корпоративної мережі на основі технології VPN
(назва за наказом ректора)

затверджену наказом ректора НТУ «Дніпровська політехніка» від 21.05.2020 № 771-л

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

Завдання видано _____ проф. Гнатушенко В.В
(підпис керівника) (прізвище, ініціали)

Дата видачі 09.04.2020

Дата подання до екзаменаційної комісії 16.06.2020

Прийнято до виконання _____ Тюх О.В.

РЕФЕРАТ

Пояснювальна записка: 73 с., 15 рис., 5 табл., 1 додаток, 13 джерел.

Об`єкт розробки – локальна мережа підприємства, апаратна і програмна конфігурація сервера.

Предмет розробки – організація та адміністрування локальної комп'ютерної мережі.

Мета роботи – побудова та налаштування захищеної корпоративної мережі на основі технології VPN, підвищення безпеки та надійності доставки інформації в мережі шляхом збільшення розміру ключа шифрування у протоколі PPTP.

Методи дослідження – методи теорії інформації, методи оптимального управління.

У роботі розглянуті питання організації корпоративної мережі. Особливу увагу приділено питанням безпеки і адміністрування мережі. Також обрано оптимальну апаратну конфігурацію сервера та розглядається захищений віддалений доступ до мережі, за допомогою якого здійснюється віртуальний локальний зв'язок між розподіленими абонентами. На базі розглянутої мережі виконано практичну організацію VPN каналів між офісами підприємства, аналіз особливостей організації віртуального офісу. Результатом роботи є таблиці дослідження залежності часу підбору ключа шифрування RC4 у протоколі PPTP від його довжини. З результатів експерименту випливає, що для підвищення надійності передачі даних по каналах VPN з використанням PPTP слід використовувати найбільшу з можливих довжину ключа шифрування.

Апробація результатів. Основні положення і результати роботи опубліковано у вигляді тез конференції.

ТЕХНОЛОГІЯ VPN, ВІДДАЛЕНИЙ ДОСТУП, ЗАХИЩЕНІСТЬ МЕРЕЖІ, КОМП’ЮТЕРНА СИСТЕМА.

ЗМІСТ

ВСТУП

Ефективне застосування інформаційних технологій у поєднанні з технологіями в області інформаційної безпеки є найважливішим стратегічним чинником підвищення конкурентоспроможності сучасних підприємств і організацій. Технологія віртуальних приватних мереж VPN дозволяє вирішувати ці завдання, забезпечуючи зв'язок між мережами, а також між віддаленим користувачем і корпоративною мережею за допомогою захищеного каналу (тунелю), «прокладеного» у загальнодоступній мережі Інтернет. VPN - це об'єднання локальних мереж або окремих машин, підключених до мережі загального користування, в єдину віртуальну мережу, що забезпечує секретність і цілісність інформації, яка передається по ній. Суть даної технології полягає в тому, що при підключенні до VPN сервера за допомогою спеціального програмного забезпечення поверх загальнодоступної мережі у вже встановленому з'єднанні організується шифрований канал, що забезпечує високий рівень захисту переданої з цього каналу інформації за рахунок застосування спеціальних алгоритмів шифрування. Використання технології VPN необхідно там, де потрібен захист корпоративної мережі від дії вірусів, зловмисників, некомпетентних користувачів, а також від інших загроз, які є результатом помилок в конфігурації або адміністрування мережі. У міру розвитку компанії у керівництва обов'язково виникають пи- тання: створення максимально гнучкої та ефективної системи управління підприємством, офісними майданчиками, створення єдиної системи документообігу, оперативного збору інформації та звітів зі складів і виробничих майданчиків, централізація інформаційно- фінансових потоків і т.д. Правильне вирішення цих питань дозволяє успішно керувати компанією в цілому, робить її гнучкою і динамічно розвивається. Світовий досвід великих компаній і корпорацій говорить про те, що таким рішенням є створення корпоративної мережі передачі даних. Сучасні IT-технології дозволяють створювати

корпоративні мережі на основі високо надійних і захищених мереж передачі даних. Для найефективнішого впровадження такого рішення необхідно, щоб користувачі могли звертатися до корпоративної мережі, не встановлюючи комутоване з'єднання, що дозволяє скоротити чисельність модемів або взагалі відмовитися від них. Бажано обійтися і без виділених ліній, що з'єднують віддалені офіси. Все це має за мету підвищити продуктивність праці, так як співробітники можуть користуватися найшвидшими лініями зв'язку, які є в їх розпорядженні, замість того щоб витрачати час на встановлення комутованого з'єднання через банк модемів. Крім того, багато компаній передбачають можливість доступу тільки до певних корпоративних ресурсів і додатків для партнерів, консультантів і клієнтів. Тобто дуже багатьом може знадобитися доступ до вищевказаних ресурсів із зовні, не потрапляючи під контроль IT-служб організації. Різноманіття варіантів доступу зажадало більш серйозного ставлення до забезпечення безпеки. У міру більшої поширеності високошвидкісного доступу до інтернету все більше користувачів звертаються до корпоративних мереж, застосовуючи широкосмугові підключення [1-5].

Комп’ютерні мережі мають необхідність в наявності сервера VPN, який буде дозволяти віддаленим абонентам використовувати ресурси приватної мережі через загальнодоступні мережі. Також VPN сервер може використовуватись для підвищення безпеки передачі інформації в локальній мережі, зменшивши можливість витоку чи крадіжки інформації, яка транспортується в мережі. Світова тенденція показує, що за роки з часу винайдення технології кількість приватних і цивільних користувачів, які нею користуются, експоненціально зростає. У військових установах, сучасних компаніях малого та великого бізнесу VPN є основою комунікаційного середовища. Суттєвим фактором будь-якої передачі даних є безпека інформації. Отже, створення віртуальних приватних комп’ютерних мереж, застосування технології шифрування інформації є важливою технічною задачею.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

Будь-яка організація, будь вона виробничою, торговою, фінансовою компанією чи державним закладом, обов’язково стикається з питанням передачі інформації між своїми філіалами, а також з питанням захисту цієї інформації. Не кожна фірма може собі дозволити мати власні фізичні канали доступу, і тут допомагає технологія *VPN*, на основі якої і з'єднуються усі підрозділи і філії, що забезпечує достатню гнучкість і одночасно високу безпеку мережі, а також істотну економію витрат [1-4].

Віртуальна приватна мережа (*VPN - Virtual Private Network*) створюється на базі загальнодоступної мережі Інтернет. І якщо зв'язок через інтернет має свої недоліки, головним з яких є те, що вона схильна до потенційних порушень захисту і конфіденційності, то *VPN* можуть гарантувати, що трафік, що направляється через інтернет, так само захищений, як і передача усередині локальної мережі. У той же час віртуальні мережі забезпечують істотну економію витрат в порівнянні із змістом власної мережі глобального масштабу. Одним з найважливіших завдань технології *VPN* є захист потоків корпоративних даних, що передаються по відкритих мережах. Відкриті канали можуть бути надійно захищені лише одним методом - криптографічним. Так звані виділені лінії не мають особливих переваг перед лініями загального користування в плані інформаційної безпеки. Виділені лінії хоч би частково розташовуватимуться в неконтрольованій зоні, де їх можуть пошкодити або здійснити до них несанкціоноване підключення. Єдина реальна перевага - це гарантована пропускна спроможність виділених ліній, а не підвищена захищеність.

Сам по собі принцип роботи *VPN* не суперечить основним мережевим технологіям і протоколам. Наприклад, при установлені з’єднання віддаленого доступа, клієнт посилає серверу потік пакетів стандартного протокола *PPP*. У разі організації віртуальних виділених

ліній між локальними мережами їх маршрутизатори також обмінюються пакетами *PPP*. Проте, принципіально новим моментом є пересилка пакетів через безпечний тунель, організованний в межах загальнодоступної мережі.

Тунелювання дозволяє організувати передачу пакетів одного протоколу в логічному середовищі, використовуючи інший протокол. В результаті виникає можливість вирішити проблеми взаємодії декількох різнотипних мереж, починаючи з необхідності забезпечення цілісності і конфіденційності передаваних даних і закінчуючи подоланням невідповідностей зовнішніх протоколів або схем адресації.

Існуюча мережева інфраструктура корпорації може бути підготовлена до використання *VPN* як з допомогою програмного, так і з допомогою аппаратного забезпечення. Організацію віртуальної приватної мережі можна порівняти з прокладкою кабелю через глобальну мережу.

Найбільш поширений метод створення тунелів *VPN* - інкапсуляція мережевих протоколів (*IP, IPX, AppleTalk* і так далі) в *PPP* і подальша інкапсуляція утворених пакетів в протокол тунелювання. Такий підхід називається тунелюванням другого рівня, оскільки "пасажиром" тут являється протокол саме другого рівня.

1.1 Цілі застосування каналів VPN з шифруванням

Головні особливості корпоративних мереж - глобальність зв'язків, масштабність і гетерогенність - представляють і підвищену небезпеку для виконання ними своїх функціональних завдань. Оскільки протоколи сімейства *TCP / IP* розроблені доволі давно, коли проблема безпеки ще не стяла так гостро, як зараз, то вони, в першу чергу, розроблялися як функціональні і легко переносимі, що допомогло розповсюдитись стеку *TCP/IP* на велику кількість комп’ютерних платформ. Крім того, в

теперішній час при використанні Інтернету в розпорядженні зловмисників з’являються численні засоби і методи проникнення в корпоративні мережі.

У зв'язку з гігантським ростом численності хостів, підключенних до інтернету, і ростом числа компаній, використовуючих технології інтернету для ведення свого бізнесу, значно збільшилось число інцидентів, пов'язаних з інформаційною безпекою (ІБ). Дані *CERT* (*Computer Emergency Response Team*) показують, що кількість виявлених вразливостей і кількість зарегістрованих інцидентів постійно збільшуються.

До теперішнього часу відома велика кількість різнопланових загроз різноманітного походження, що приховують в собі різну небезпеку для інформації. Навмисне походження загрози обумовлюється зловмисними діями людей, що здійснюються з метою реалізації одного або декількох видів загроз. Відмічені дві різновидності предпосилок появи загроз: об'єктивні (кількісна або якісна недостатність елементів системи) і суб'єктивні (діяльність розвідувальних служб іноземних держав, промисловий шпіонаж, діяльність кримінальних елементів, зловмисні дії недобросовісних співробітників системи) [3-6].

Джерелом загроз можуть бути люди, технічні засоби, програми і алгоритми, технологічні схеми обробки даних і зовнішнє середовище.

Основними причинами витоку інформації є:

• недотримання персоналом норм, вимог, правил експлуатації;

• помилка в проектуванні системи і систем захисту;

• ведення зацікавленою стороною технічної і агентурної розвідок.

Недотримання персоналом норм, вимог, правил експлуатації може бути як умисним, так і ненавмисним. Від ведення зацікавленою стороною агентурної розвідки цей випадок відрізняє те, що в данному разі обличчям, що здійснює несанкціоновані дії, рухають особисті мотиви. Причини витоку інформації достатньо тісно пов'язані з видами витоку інформації. Розглядаються три види витоку інформації:

• розголошення;

• несанкціонований доступ до інформації;

• отримання захищеної інформації розвідками.

Під розголошенням інформації розуміється несанкціоноване доведення захищеної інформації до споживача, які не мають права доступу до захищеної інформації.

Під несанкціонованим доступом розуміється отримання захищенної інформації зацікавленим суб'єктом з порушенням установлених правовими документами або власником інформації прав або правил доступа до захищеної інформації. При цьому зацікавленим суб’єктом, що здійснює несанкціонований доступ до інформації, може бути держава, юридична особа, група фізичних осіб (у тому числі громадська організація), окрема фізічна особа.

Отримання захищеної інформації розвідками може здійснюватися за допомогою технічних засобів (технічна розвідка) або агентурними методами (агентурна розвідка).

Канал витоку інформації – совокупність джерел інформації, матеріального носія або середовища росповсюдження несучого зазначену інформацію сигналу і засоби виділення інформації з сигналу або носія. Однією з основних властивостей каналу є місце розташування засобів виділення інформації з сигналу або носія, які можуть розташовуватись в межах контролюємої зони, охоплюючи систему, або поза нею.

Легше й дешевше, якщо інформація буде передаватися по звичайним каналам зв'язку (наприклад, через Інтернет), але яким-небудь способом буде віддалена або прихована від трафіку інших компаній, циркулюючого в мережі. Не слід думати, що потреба в конфіденційній передачі інформації виникає лише в глобальних мережах. Така потреба може виникнути і в локальних мережах, де потрібно відділити один тип трафіку від іншого (наприклад, трафік платіжной системи від трафіку інформаційно-аналітичної системи).

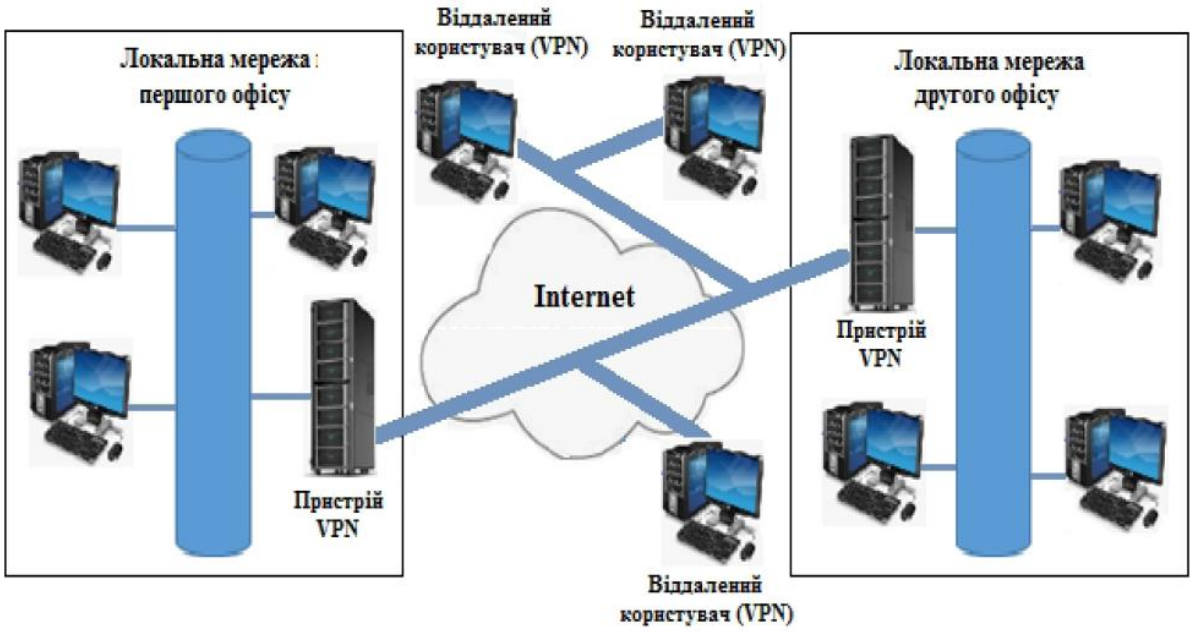

Рисунок 1.1 - VPN

Особливість технології *VPN* в тому, що організація віддаленого доступу робиться не через телефонну лінію, а через Інтернет, що набагато дешевше і краще. Для організації віддаленого доступу до приватної мережі за допомогою технології *VPN* знадобиться Інтернет і реальна *IP*-адреса. І будь-який користувач з будь-якої точки земної кулі зможе зайти в мережу, якщо він знає *IP*-адресу, логін і пароль нашої мережі.

1.2 Існуючі методи реалізації захищених каналів VPN

Існують різні варіанти створення *VPN*. При виборі рішення потрібно враховувати фактори продуктивності засобів побудови *VPN*. Наприклад, якщо маршрутизатор і так працює на межі потужності свого процесора, то додавання тунелів *VPN* і застосування шифрування / дешифрування інформації може зупинити роботу всієї мережі через те, що цей маршрутизатор не буде справлятися з простим трафіком, не кажучи вже про *VPN*. Досвід показує, що для побудови *VPN* краще всього використовувати спеціалізоване обладнення, але якщо є обмеження в засобах, то потрібно

звернути увагу на чисто програмні рішення. Розглянемо деякі варіанти побудови *VPN*.

1) VPN на базі брандмауерів

Брандмауери більшості виробників підтримують тунелювання і шифрування даних. Всі подібні продукти засновані на тому, що якщо вже трафік проходить через брандмауер, то чому б його заодно не зашифрувати. До програмного забезпечення власне брандмауера додається модуль шифрування. Недоліком даного методу можна назвати залежність продуктивності від апаратного забезпечення, на якому працює брандмауер. При використанні брандмауерів на базі ПК треба пам'ятати, що подібне рішення можна застосовувати тільки для невеликих мереж з невеликим обсягом переданої інформації.

Як приклад рішення на базі брандмауерів можна назвати *FireWall-1* компанії *Check Point Software Technologies*. *FairWall-1* використовує для побудови *VPN* стандартний підхід на базі *IPSec*. Трафік, що приходить в брандмауер, дешифрується, після чого до нього застосовуються стандартні правила управління доступом. *FireWall-1* працює під управлінням операційних систем *Solaris* і *Windows*.

2) VPN на базі маршрутизаторів

Іншим способом побудови *VPN* є застосування маршрутизаторів для створення захищених каналів. Так як вся інформація, що виходить з локальної мережі, проходить через маршрутизатор, то доцільно покласти на цей маршрутизатор і завдання шифрування. Яскравим прикладом обладнання для побудови *VPN* на маршрутизаторах є обладнання компанії *Cisco Systems*. Починаючи з версії програмного забезпечення IOS 11.3(3) T маршрутизатори *Cisco* підтримують протоколи *L2TP* і *IPSec*. Крім простого шифрування інформації *Cisco* підтримує і інші функції *VPN*, такі як ідентифікація при встановленні тунельного з'єднання і обмін ключами.

Для побудови *VPN Cisco* використовує тунелювання з шифруванням будь-якого *IP*-потоку. При цьому тунель може бути встановлений,

грунтуючись на адресах джерела і приймача, номера порту *TCP (UDP)* і зазначеного якості сервісу (*QoS*). Для підвищення продуктивності маршрутизатора може бути використаний додатковий модуль шифрування *ESA (Encryption Service Adapter)*. Крім того, компанія *Cisco System* випустила спеціалізований пристрій для *VPN*, яке так і називається *Cisco 1720 VPN Access Router* (Маршрутизатор Доступу до *VPN*), призначений для установки в компаніях малого і середнього розміру, а також в у відділеннях великих організацій.

3) VPN на базі програмного забезпечення

Наступним підходом до побудови *VPN* є чисто програмні рішення. При реалізації такого рішення використовується спеціалізоване програмне забезпечення, яке працює на виділеному комп'ютері і в більшості випадків виконує роль proxy-сервера. Комп'ютер з таким програмним забезпеченням може бути розташований за брандмауером.

Як приклад такого рішення можна виступає програмне забезпечення *AltaVista Tunnel* компанії *Digital*. При використанні даного ПЗ клієнт підключається до сервера *Tunnel*, аутентифіковані на ньому і обмінюється ключами. Шифрація проводиться на базі 56 або 128 бітних ключів *Rivest-Cipher* 4, отриманих в процесі встановлення з'єднання, які змінюються кожні 30 хвилин. Далі, зашифровані пакети інкапсулюються в інші *IP*-пакети, які в свою чергу відправляються на сервер. В ході роботи *Tunnel* здійснює перевірку цілісності даних по алгоритму *MD5*. Крім того, дане ПЗ кожні 30 хвилин генерує нові ключі, що значно підвищує захищеність з'єднання. Позитивними якостями *AltaVista Tunnel* є простота установки і зручність управління. Мінусами даної системи можна вважати нестандартну архітектуру (власний алгоритм обміну ключами) і низьку продуктивність.

4) VPN на базі апаратних засобів

Варіант побудови *VPN* на спеціальних пристроях може бути використаний в мережах, що вимагають високої продуктивності. Прикладом такого рішення є продукт *cIPro-VPN* компанії *Radguard*.

Даний продукт використовує апаратне шифрування переданої інформації, здатне пропускати потік в 100 Мбіт / с. *cIPro-VPN* підтримує протокол *IPSec* і механізм управління ключами *ISAKMP* / *Oakley*. Крім іншого, даний пристрій підтримує засоби трансляції мережевих адрес і може бути доповнений спеціальної платою, яка додає функції брандмауера.

5) VPN на базі мережевої ОС

Рішення на базі мережевої ОС ми розглянемо на прикладі системи *Windows* компанії *Microsoft*. Для створення *VPN Microsoft* використовує протокол *PPTP*, який інтегрований у систему *Windows*. Дане рішення дуже привабливо для організацій використовують *Windows* в якості корпоративної операційної системи. У роботі *VPN* на базі Windows використовується база користувачів, що зберігається на *Primary Domain Controller (PDC)*. При підключенні до *PPTP*-сервера користувач аутентифікується за протоколами *PAP*, *CHAP* або MS-*CHAP*. Передані пакети інкапсулюються в пакети *GRE* / *PPTP*. Для шифрування пакетів використовується нестандартний протокол від *Microsoft Point-to-Point Encryption* з 40 або 128 бітовим ключем, отриманим в момент встановлення з'єднання. Недоліками даної системи є відсутність перевірки цілісності даних і неможливість зміни ключів під час з'єднання. Позитивними моментами є легкість інтеграції з *Windows* і низька вартість.

По призначенню реалізацію *VPN* мереж класифікують таким чином:

- *Intranet VPN*. Використовують для об'єднання в єдину захищену мережу декількох розподілених філій однієї організації, які обмінюються даними по відкритих каналах зв'язку.

- *Remote Access VPN*. Використовують для створення захищеного каналу між сегментом корпоративної мережі (центральним офісом або філією) і одиночним користувачем, який, працюючи вдома, підключається до корпоративних ресурсів з домашнього комп'ютера або, перебуваючи у відрядженні, підключається до корпоративних ресурсів за допомогою ноутбука.

- *Extranet VPN*. Використовують для мереж, до яких підключаються «зовнішні» користувачі (наприклад, замовники або клієнти). Рівень довіри до них набагато нижча, ніж до співробітників компанії, тому потрібне забезпечення спеціальних «рубежів» захисту, що запобігають або обмежують доступ останніх до особливо цінною, конфіденційної інформації.

1.3 Безпека інформаційних мереж на основі VPN та способи її досягнення

Віртуальна приватна мережа базується на трьох методах, які застосовуються при реалізації заходів безпеки в інформаційних мережах:

- Тунелювання;
- Аутентифікація.
- Шифрування;

Тунелювання забезпечує передачу даних між двома точками - закінченнями тунелю - таким чином, що для джерела і приймача даних виявляється прихованою вся мережева інфраструктура, що лежить між ними.

Такий стан справ таїть в собі дві проблеми. Перша полягає в тому, що передається через тунель інформація може бути перехоплена зловмисниками.

Якщо вона конфіденційна (номери банківських карток, фінансові звіти, відомості особистого характеру), то цілком реальна загроза її компрометації, що вже само по собі неприємно. Гірше того, зловмисники мають можливість модифікувати передаються через тунель дані так, що одержувач не зможе перевірити їх достовірність. Наслідки можуть бути жахливими. Враховуючи сказане, ми приходимо до висновку, що тунель в чистому вигляді придатний хіба що для деяких типів мережевих комп'ютерних ігор і не може претендувати на більш серйозне застосування. Обидві проблеми вирішуються сучасними засобами криптографічного захисту інформації. Щоб перешкодити внесенню несанкціонованих змін в пакет з даними на шляху його проходження по тунелю, використовується метод електронного цифрового підпису (ЕЦП). Суть методу полягає в тому, що кожен переданий

пакет забезпечується додатковим блоком інформації, який виробляється у відповідності з асиметричним криптографічним алгоритмом і унікальний для вмісту пакета і секретного ключа ЕЦП відправника. Цей блок інформації є ЕЦП пакета і дозволяє виконати аутентифікацію даних одержувачем, якому відомий відкритий ключ ЕЦП відправника. Захист переданих через тунель даних від несанкціонованого перегляду досягається шляхом використання сильних алгоритмів шифрування.

Забезпечення безпеки є основною функцією *VPN*. Всі дані від комп'ютерів-клієнтів проходять через *Internet* до *VPN*-сервера. Такий сервер може знаходитися на великій відстані від клієнтського комп'ютера, і дані на шляху до мережі організації проходять через обладнання безлічі провайдерів. Як переконатися, що дані не були прочитані або змінені? Для цього застосовуються різні методи аутентифікації і шифрування.

Для аутентифікації користувачів *PPTP* може задіяти будь-який з протоколів, що застосовуються для *PPP*

• *EAP* або *Extensible Authentication Protocol;*

• *MSCHAP* або *Microsoft Challenge Handshake Authentication Protocol* (версії 1 і 2);

• *CHAP* або *Challenge Handshake Authentication Protocol;*

• *SPAP* або *Shiva Password Authentication Protocol;*

• *PAP* або *Password Authentication Protocol.*

Кращими вважаються протоколи *MSCHAP* версії 2 і *Transport Layer Security (EAP-TLS)*, оскільки вони забезпечують взаємну аутентифікацію, тобто *VPN*-сервер і клієнт ідентифікують один одного. У всіх інших протоколах тільки сервер проводить аутентифікацію клієнтів.

Хоча *PPTP* забезпечує достатній ступінь безпеки, але все ж *L2TP* поверх *IPSec* надійніше. *L2TP* поверх *IPSec* забезпечує аутентифікацію на рівнях «користувач» і «комп'ютер», а також виконує аутентифікацію і шифрування даних.

Аутентифікація здійснюється або відритим тестом (*clear text password*), або за схемою запит / відгук (*challenge / response*). З прямим текстом все зрозуміло. Клієнт посилає серверу пароль. Сервер порівнює це з еталоном і або забороняє доступ, або говорить «ласкаво просимо». Відкрита аутентифікація практично не зустрічається.

Шифрування за допомогою *PPTP* гарантує, що ніхто не зможе отримати доступ до даних при пересиланні через *Internet*. В даний час підтримуються два методи шифрування:

• Протокол шифрування *MPPE* або *Microsoft Point-to-Point Encryption* сумісний тільки з *MSCHAP* (версії 1 і 2);

• *EAP-TLS* і вміє автоматично вибирати довжину ключа шифрування при узгодженні параметрів між клієнтом і сервером.

MPPE підтримує роботу з ключами довжиною 40, 56 або 128 біт. Старі операційні системи *Windows* підтримують шифрування з довжиною ключа тільки 40 біт, тому в змішаному середовищі *Windows* слід вибирати мінімальну довжину ключа.

PPTP змінює значення ключа шифрування після кожного прийнятого пакета. Протокол *MMPE* розроблявся для каналів зв'язку точка-точка, в яких пакети передаються послідовно, і втрата даних дуже мала. У цій ситуації значення ключа для чергового пакета залежить від результатів дешифрування попереднього пакета. При побудові віртуальних мереж через мережі загального доступу цих умов дотримуватися неможливо, так як пакети даних часто приходять до одержувача не в тій послідовності, в якій були відправлені. Тому *PPTP* використовує для зміни ключа шифрування порядкові номери пакетів. Це дозволяє виконувати дешифрацію незалежно від попередніх прийнятих пакетів.

Обидва протоколи реалізовані як в *Microsoft Windows*, так і поза нею (наприклад, в *BSD*), на алгоритми роботи *VPN* можуть істотно відрізнятися.

Таким чином, зв'язка «тунелювання + аутентифікація + шифрування» дозволяє передавати дані між двома точками через мережу загального

користування, моделюючи роботу приватної (локальної) мережі. Іншими словами, розглянуті засоби дозволяють побудувати віртуальну приватну мережу. Додатковим приємним ефектом *VPN*-з'єднання є можливість (і навіть необхідність) використання системи адресації, прийнятої в локальній мережі.

Реалізація віртуальної приватної мережі на практиці виглядає таким чином. У локальній обчислювальній мережі офісу фірми встановлюється сервер *VPN*. Віддалений користувач (або маршрутизатор, якщо здійснюється з'єднання двох офісів) з використанням клієнтського програмного забезпечення *VPN* ініціює процедуру з'єднання з сервером. Відбувається аутентифікація користувача - перша фаза встановлення *VPN*-з'єднання. У разі підтвердження повноважень настає друга фаза - між клієнтом і сервером виконується узгодження деталей забезпечення безпеки з'єднання. Після цього організується *VPN*-з'єднання, що забезпечує обмін інформацією між клієнтом і сервером у формі, коли кожен пакет з даними проходить через процедури шифрування / дешифрування та перевірки цілісності - аутентифікації даних.

1.4 Порівняння протоколів та вибір найбільш відповідного до поставленої задачі

Ніхто не зможе відповісти на питання, яка з технологій *VPN* підходить для найбільше. При використанні *VPN* перед адміністраторами мережі стає питання про доцільність використання саме такого захисту мережі. Але при реалізації мережі необхідно враховувати не лише переваги *VPN*, головними з яких являються підвищена безпека, об’єднання розподілених ресурсів, прозорість для користувача та зниження затрат за рахунок використання інтернету, але й недоліки, які можуть бути несумісні з нашими вимогами до безпеки мережі. Головними ж недоліками *VPN* можна вважати затрати часу на реалізацію, проблематичність в виявленні проблем, які будуть з’являтися в

ході експлуатації, довіра користувачам іншої мережі при побудові топології мережа-мережа, залежність доступу від інтернет провайдера, взаємодія між різними протоколами, апаратними та програмними засобами різних виробників.

В зв’язку з цим перед плануванням мережі необхідно ретельно проаналізувати задачі, які перед нами стоять, та методи, якими у нас є можливість їх досягти.

Найчастіше перед керівниками *IT* підрозділів стоїть питання: який з протоколів вибрати для побудови корпоративної мережі *VPN*? Відповідь не очевидна тому що кожен з підходів має як плюси, так і мінуси. Постараємося провести аналіз та виявити коли необхідно застосовувати *IPSec*, а коли *SSL / TLS*. Як видно з аналізу характеристик цих протоколів вони не є взаємозамінними і можуть функціонувати як окремо, так і паралельно, визначаючи функціональні особливості кожної з реалізованих *VPN*.

Вибір протоколу для побудови корпоративної мережі *VPN* можна здійснювати за такими критеріями:

• Тип доступу необхідний для користувачів мережі *VPN*.

1. Повнофункціональне постійне підключення до корпоративної мережі. Рекомендований вибір - протокол *IPSec*.

2. Тимчасове підключення, наприклад, мобільного користувача або користувача використовує публічний комп'ютер, з метою отримання доступу до певних послуг, наприклад, електронної пошти або бази даних. Рекомендований вибір - протокол *SSL / TLS*, який дозволяє організувати *VPN* для кожної окремої послуги.

• Чи є користувач співробітником компанії.

1. Якщо користувач є співробітником компанії, пристрій яким він користується для доступу до корпоративної мережі через *IPSec VPN* може бути налаштоване деяким певним способом.

2. Якщо користувач не є співробітником компанії до корпоративної мережі якої здійснюється доступ, рекомендується використовувати *SSL / TLS*. Це дозволить обмежити гостьовий доступ тільки певними послугами.

• Який рівень безпеки корпоративної мережі.

1. Високий. Рекомендований вибір - протокол *IPSec*. Дійсно, рівень безпеки пропонований *IPSec* набагато вище рівня безпеки пропонованого протоколом *SSL / TLS* в силу використання конфігурованого ПЗ на стороні користувача та шлюзу безпеки на стороні корпоративної мережі.

2. Середній. Рекомендований вибір - протокол *SSL / TLS* дозволяє здійснювати доступ з будь-яких терміналів.

3. В залежності від послуги - від середнього до високого. Рекомендований вибір - комбінація протоколів *IPSec* (для послуг вимагають високий рівень безпеки) і *SSL / TLS* (для послуг вимагають середній рівень безпеки).

• Рівень безпеки даних переданих користувачем.

1. Високий, наприклад, менеджмент компанії. Рекомендований вибір - протокол *IPSec*.

2. Середній, наприклад, партнер. Рекомендований вибір - протокол *SSL / TLS*.

3. В залежності від послуги - від середнього до високого. Рекомендований вибір - комбінація протоколів *IPSec* (для послуг вимагають високий рівень безпеки) і *SSL / TLS* (для послуг вимагають середній рівень безпеки).

• Що важливіше, швидке розгортання *VPN* або масштабованість рішення в майбутньому.

1. Швидке розгортання мережі *VPN* з мінімальними витратами. Рекомендований вибір - протокол *SSL / TLS*. В цьому випадку немає необхідності реалізації спеціального ПЗ на стороні користувача як у випадку *IPSec*.

2. Масштабованість мережі *VPN* - додавання доступу до різноманітних послуг. Рекомендований вибір - протокол *IPSec* дозволяє здійснення доступу до всіх послуг і ресурсів корпоративної мережі.

3. Швидке розгортання і масштабованість. Рекомендований вибір - комбінація *IPSec* та *SSL / TLS*: використання *SSL / TLS* на першому етапі для здійснення доступу до необхідних послуг з подальшим впровадженням *IPSec*.

При виборі серед протоколів *PPTP*, *L2TP/IPsec* або *SSTP* для *VPN*-рішення віддаленого доступу слід взяти до уваги наступне:

1) Протокол *PPTP* підтримується різними клієнтами від *Microsoft*, включаючи ОС *Microsoft Windows 2000, Windows XP, Windows Vista, Windows Seven* і *Windows Server 2008*. На відміну від протоколу *L2TP*/*IPsec*, протокол *PPTP* не вимагає використання інфраструктури відкритих ключів (*PKI*). *VPN*-підключення по протоколу *PPTP* забезпечують конфіденційність даних за допомогою шифрування (захоплені пакети неможливо інтерпретувати без ключа шифрування). Однак *VPN*-підключення по протоколу *PPTP* не забезпечують цілісності даних (доказ незмінності даних при передачі) або перевірку достовірності даних (доказ відправки даних вповноваженим користувачем).

2) Протокол *L2TP* може використовуватися тільки з клієнтськими комп'ютерами під управлінням ОС *Windows 2000, Windows XP, Windows Vista, Windows Seven*. Протокол *L2TP* підтримує методи перевірки автентичності *IPsec* за сертифікатами комп'ютерів і попередніми ключам. При перевірці достовірності за сертифікатом комп'ютера (рекомендований метод перевірки автентичності) для видачі цих сертифікатів комп'ютера *VPN*-сервера і всім комп'ютерам *VPN*-клієнтів потрібно інфраструктура *PKI*. При використанні *IPsec VPN*-підключення по протоколу *L2TP/IPsec* забезпечують конфіденційність, цілісність і перевірку автентичності даних.

На відміну від протоколів *PPTP* і *SSTP*, протокол *L2TP/IPsec* забезпечує перевірку автентичності комп'ютера на рівні *IPsec* і перевірку автентичності користувача на рівні *PPP*.

3) Протокол *SSTP* підтримується тільки клієнтськими комп'ютерами під управлінням ОС *Windows Vista* з пакетом оновлень 1 *(SP1)*, *Windows Seven* або ОС *Windows Server 2008*. При використанні *SSL VPN*-підключення по протоколу *SSTP* забезпечують конфіденційність, цілісність і перевірку автентичності даних.

4) Всі три типи тунелів на верхньому рівні стека мережевих протоколів передають *PPP*-кадри. Тому загальні риси протоколу *PPP*, наприклад схеми перевірки автентичності, узгодження протоколу *IP* версії 4 (*IPv4*) і протоколу *IP* версії 6 (*IPv6*), а також захист доступу до мережі (*NAP*), однакові для всіх трьох типів тунелів.

2 ПОБУДОВА ТА НАЛАШТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ VPN

2.1 Побудова корпоративної мережі підприємства

Проаналізувавши особливості експлуатаії корпоративних мереж, їх вимоги до надійності та експлуатаційні характеристики, можна зазначити, що найбільш важливими вимогами до їх побудови є:

- вимоги до погодження потоків даних та щодо їх захищенності в процесі передачі;
- вимоги до організації єдиного віртуального простору та однієї системи адресації;
- вимоги надійності та безпеки.

На рис.2.1. представлено приклад великої корпоративної мережі, яка включає до 500 станцій. Це банк з п’ятьма філіалами у різних областях. У кожному з філіалів встановлено до 100 ПК. Центральне керівництво мережею здійснюється з центральної станції, а у кожній підмережі є свій регіональний контроль. При цьому, для забезпечення сумісності та маштабованості мережі потрібно, щоб:

1. Була зебезпечена підтримка стандарту IPsec (захист інформаії) і одного з стандартів управління ключами (SKIP, ISAKMP або IKE);
2. Підтримка централізованого управління всією віртуальною мережею;
3. Підтримка аутентифікації користувачівVPN (паролі, смарт-карти)
4. Наявність широкого переліку продуктів, які забезпечать надійний захист даних.
5. Підтримка широко використовуваних систем управління сертифікатами.

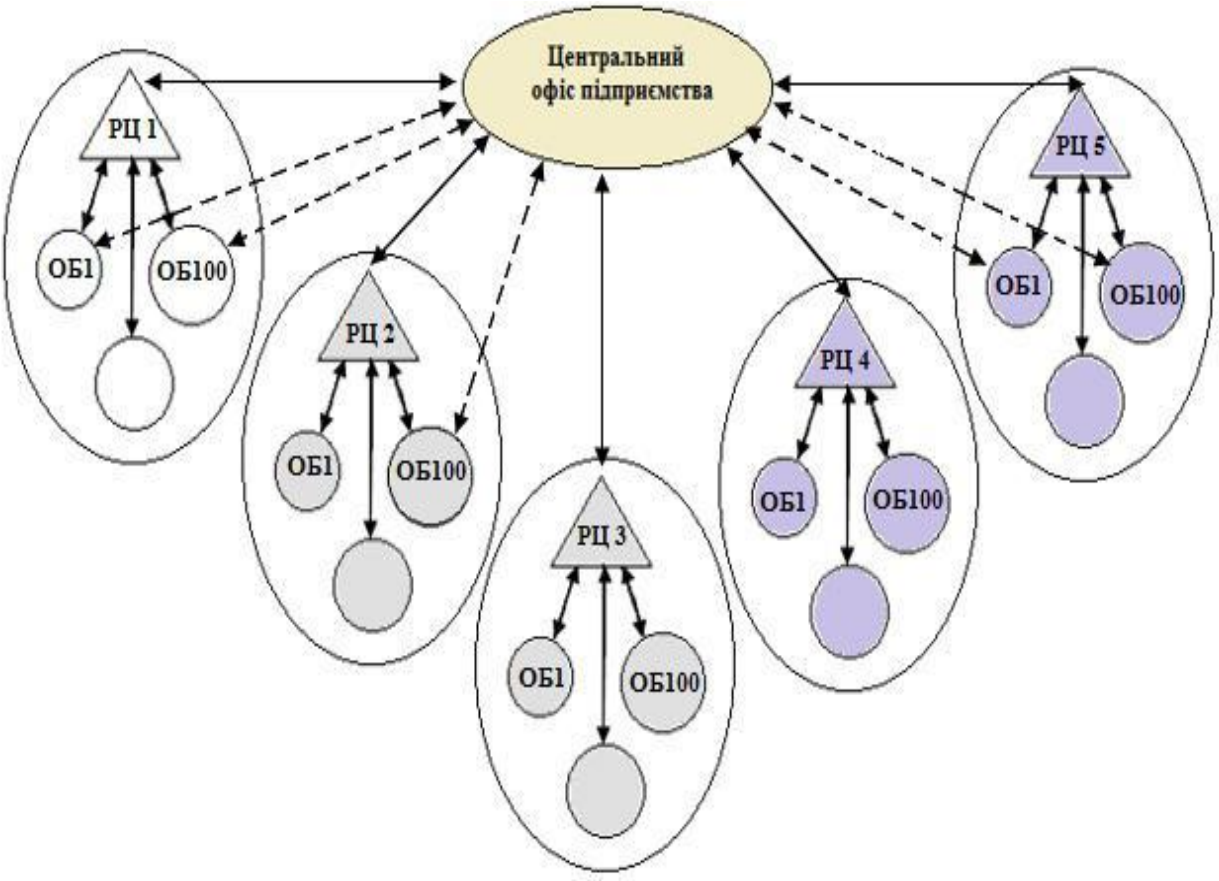

Рисунок 2.1 - Схема розподіленої корпоративної мережі підприємства

Такі мережі мають особливості підключення до мережі інтернет та захисту таких підключень. Якщо мережа використовує Інтернет тільки для організації внутрішньо-підприємницької VPN, що утворює жорсткий периметр і не передбачає ніяких контактів із зовнішнім світом, то в такому випадку не слід переживати за збереження даних. Тобто глобальна мережа в транспортному режимі. Але у випадку, коли потрібно підключення до Інтернету для пересилки даних до «зовнішнього світу» (наприклад електронна пошта). При такій побудові мережі потрібно на кордоні VPN/Internet забезпечіти функціонування ряду технологій. До них відносять:

1. Системи FireWal. Його встановлюють як на вході в мережу, так і на кожному окремому ПК, який має вихід у мережу.
2. Системи антивірусного контролю на всіх ПК мережі.
3. Системи контролю та аудиту - intrusion detection;
4. Організаційні технології, які сполучають разом всю систему.

При розгортанні мереж потрібно не лише врахувати вищеперераховані заходи, але й забезпечити їх інтеграцію з вже існуючими на мережі. Також адміністратори та розробники стикаються з наступними проблемами:

1. Забезпечення надійної та безперебійної роботи в режимі «non-stop». В цьому питанні найбільш складною є боротьба з відмовами обладнання, особливо серверів. Тут використовуютьсятакі методи:

- резервування всіх значимих серверів у мережі;

- зебезпечення алгоритму передачі даних на працюючий сервер у разі виходу з ладу одного з центральних серверів.

2. Формування вимог до якості зв'язку та аналіз рівня завантаженності каналів передачі даних. Це важливо, оскільки, як правило, підприємства арендують канали передачі даних, а не будують власні. Якраз питання якості обговорюються і чітко прописуються у договорі оренди каналу у провайдера зв'язку.

Для будь-якого банку є критично важливою безпека інформації про клієнтів, послуги, фінансові операції, активи та так далі. Вся інформація банків зберігається в корпоративних мережах, та підлягає передачі по зовнішнім мережам загального доступу, а також через Інтернет. Величезна частка комерційної інформації зберігається в інформаційній обчислювальній системі. Дані з цих систем використовуються операторами, менеджерами, а також партнерами і клієнтами за допомогою веб-представництва банку в Інтернеті. Інформація підлягає обробці на ПК співробітників, знаходиться в стадії зберігання на інформаційних ресурсах. Щодо кожного процесу інформаційний вплив відбувається в двох напрямках: «зверху» і «знизу», з «зовнішньої» і «внутрішньої» сторони. До дій «зверху» можна віднести, закони держави, що визначають регулювання підприємств Банківської галузі. «Внутрішні» сторони це особливості структури, спеціальні інструкції, які

можуть відрізнятися навіть у різних філіях. «Зовнішні» - дані про процеси, які сформовані зовнішніми регулюючими органами (закони і т.п.).

На рис 2.2. зображені найважливіші сутності економічної взаємодії АБ «УКРГАЗБАНК» з зовнішнім світом, кожна з яких здійснює активний інформаційний обмін з підприємством. При цьому успіх підприємницької діяльності на пряму залежить від швидкості та надійності обміну даними. Політика безпеки є пріоритетним стратегічним напрямом, що відображає концепції підприємства в сфері забезпечення безпеки його економічної діяльності.

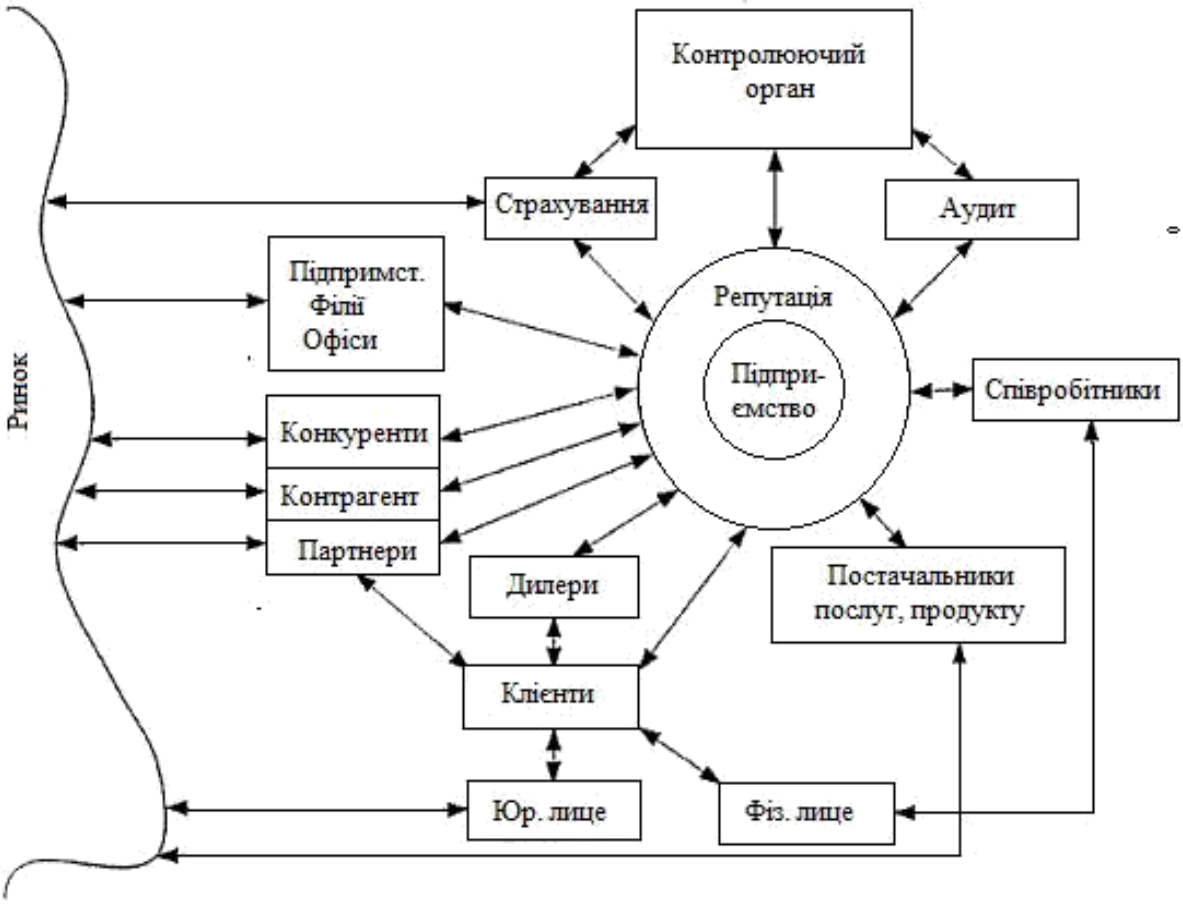

Рисунок 2.2 - Схема інформаційної взаємодії підприємства з зовнішнім світом

2.2 Аналіз загального опису мережі

Як зазначалося раніше корпоративні мережі доцільно будувати враховуючи організаційну структуру підприємства. Тому приведемо опис організаційної структуру АБ «УКРГАЗБАНК», що включає такі підрозділи:

1. Служба генерального директора:
   a. Відділ кадрів;
   b. Служба внутрішнього аудиту;
   c. Юридичний відділ.
2. Управління фінансових ринків:
   a. Відділ управління ризиками.
3. Управління банківськими продуктами і послугами:
   a. Відділ по роботі з партнерами;
   b. Відділ пластикових карт.
4. Операційне управління:
   a. Відділ платежів;
   b.Відділ інформаційної безпеки;
   c. Відділ по роботі з філіалами;
   d. Відділ по роботі з фізичними особами;
   e. Відділ комунікацій;
   f. Відділ інфраструктури;
   g. Відділ підтримки IT;
   h. Відділ розробки;
5. Управління корпоративногообслуговування.
6. Інвестиційне управління.

Основним призначенням територіально-розподіленоїмережі є:

1. забезпечення доступу віддалених відділів системи, підключених до мережі, до ресурсів системи;
2. забезпечення роботи додатків в режимі клієнт-сервер;

3. забезпечення передачі даних між комп'ютерамимережі;

4. контроль роботи співробітниуів системи та контроль використання системних ресурсів [26].

2.2.1 Мережа центрального офісу

Мережа центрального офісу АБ «УКРГАЗБАНК» побудована на комутаторах фірми «Cisco» зі структурою мережі типу «зірка», в центрі якої знаходиться модель Cisco-3750G, а на кожному з поверхів модель Cisco-2960G. Між комутаторами Cisco-2960G та Cisco-3750G прокладено оптоволоконну мережу. Робочі станції кожного поверху підключені до Cisco-2960G. Серверне обладнання розташоване у підвальному приміщенні та об’єднано у окрему мережу, куди входять сервери баз даних, сервери додатків, сервери друку.

Зовнішні канали підключаються до мережі через комутатори і маршрутизатори фірми «Cisco».

Як канали зв'язку використовуються:

- оптоволокно з пропускною спроможністю 1000Мбіт/с;
- неекранована кручена пара з пропускною спроможністю 100 Мбіт/с;
- неекранована кручена пара з пропускною спроможністю 110 Мбіт/с.

У мережі виділяються два контури: мережа першого рівня і мережу другого рівня. До складу мережі першого рівня входять віртуальні мережі підрозділів, які включають віддалені робочі станції розташовані на різних поверхах будівлі банку та об'єднані з активним мережевим обладнанням каналами зв'язку з пропускною здатністю до 100 Мбіт/с.

До складу мережі другого рівня, яка являє собою віртуальну мережу, входять корпоративні сервери додатків і сервер баз даних. Між собою вони об'єднані каналами зв'язку з пропускною спроможністю 100 Мбіт/с.

Підмережі мережі першого рівня з'єднані з мережею другого рівня каналами зв'язку з пропускною здатністю 1000 Мбіт/с.

Робочі станції всіх підмереж першого рівня (VLAN) призначені для запуску стандартних додатків, що забезпечують сервіс-процеси, і взаємодіють тільки з корпоративнимисерверами.

2.2.2 Мережа віддаленого офісу

Розпишемо більш детально локальну мережу. Всі її складові, тобто віддалені офіси, знаходяться на території України. Для їх побудови також використано обладнання фірми «Cisco» та на базі топології «зірка». У центрі кожної «зірки» встановлено комутатор серії «2900», який є центром для підключення всіх віддалені станції (офіси). Офіси можуть бути:

- електронними. Це сучасні автоматизовані системи. Автоматизація може бути повною, або частковою. Це стосується автоматизації всих процесів у банку. Це відноситься і до процесів управління так і до поточних процесів документообігу. При такому підході, всі інформаційні процеси, а саме обробка, пошук, передача інформації виконуються автоматизовано, з використанням різноманітних програмних засобів та апаратних засобів. По суті, автоматизоване місце складається з ПК, в який для підвищення функціональності додають спеціалізовані пристрої та додаткове офісне обладнання.
- сучасними – мають складну структуру інфраструктуру, систему зв’язків між підрозділами. Як правило, такі офіси складаються з двох частин: front office і back office. Front office це центральна частина офісу, де знаходиться кабінет керівника, кімнати для роботи з клієнтами та очікування. Back office це робоча частина офісу, де розміщуються робочі місця робітників офісу.
- віртуальними – це розподілені мережі, які взаємодіють між собою за допомогою інформаційних технологій. При такій побудові

віддалені робочі місця можуть мати доступ до ресурсів мережі з будь-якої точки за допомогою мережі інтернет. Не дивлячись на те, що така побудова вимагає матеріальних затрат, вони дуже швидко окуповуються. Окупність досягається за рахунок того, що можлива віддалена робота та не потрібно організовувати великі офіси та складні мережеві структури. Також, такі офіси можуть підтримувати технологією віртуальної реальності, яка дозволяє активно зануритися у середовище, що імітується

- традиційним – припускається в основному використання паперових носіїв інформації, для передачі інформації – пошта, кур'єрська розсилка.

Віддалені офіси знаходяться на дуже великій відстані від центрального офісу і один від одного. Вибір операторів зв'язку проведений з розрахунку присутності і доступності. Схематично, підключення офісів представлено на рис.2.3.

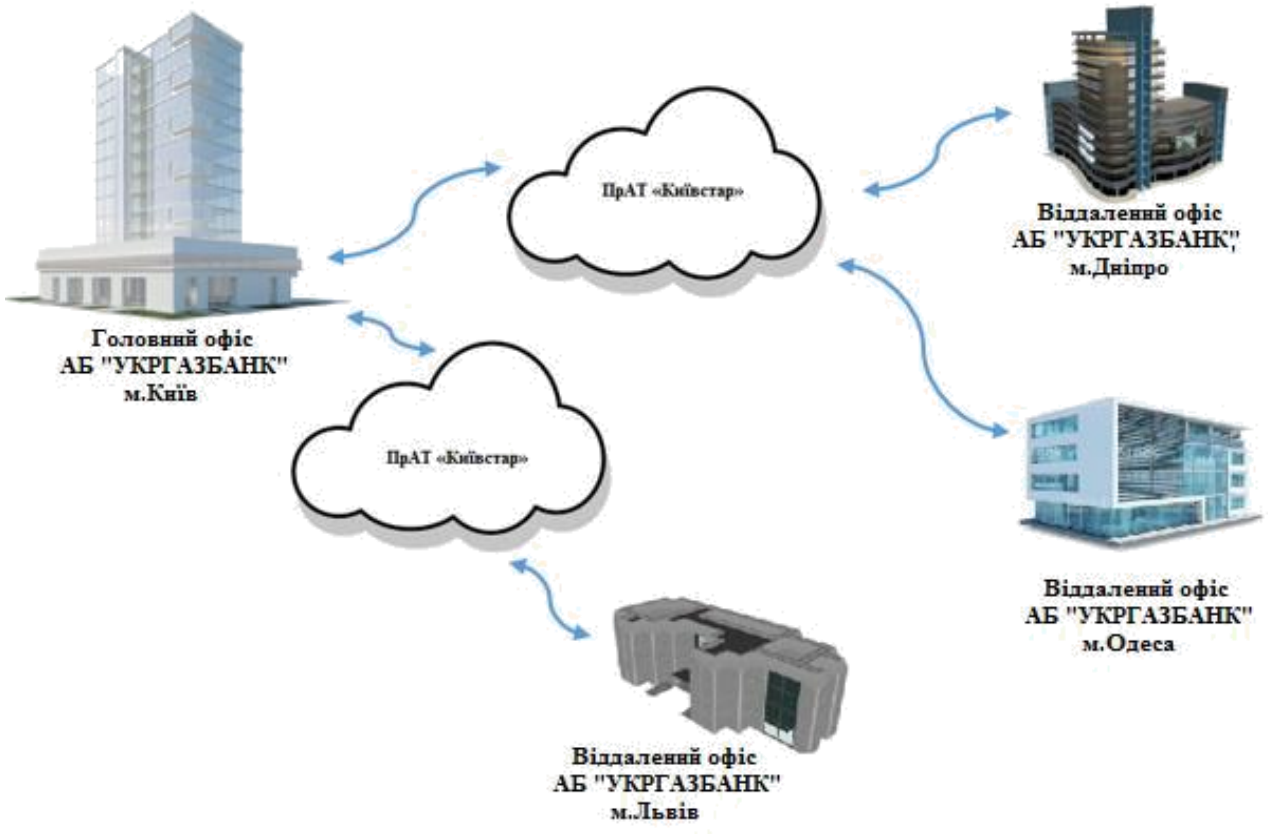

Рисунок 2.3 - Інформаційна взаємодія компанії з віддаленими офісами

2.3 Оцінка завантаження каналів зв'язку корпоративної мережі і інтенсивностей потоків запитів на запуск додатків

Для того, щоб провести оцінку завантаженності каналів з'єднання мережі між центральним офісом та віддаленими філіями, проводиться запуск додатків від робочих місць. Тип програми для запуску напряму залежить від того, в якому підрозділі віртуальної мережі знаходиться клієнтське робоче місце, який додаток і з якого сервера буде запущено.

Структура територіально-розподіленої мережі, яка побудована, повністю відповідає організаційній структурі АБ «УКРГАЗБАНК», яка описана у попередньому підрозділі. При проведенні розрахунку завантаження каналів зв'язку враховувалися потоки запитів, які можуть надходити з різних підрозділів і відділів віддалених офісів. Також, враховано перелік комплексів задач, різних довідкових систем, що впливають на трафік. Всі основні сервери БД розташовані в центральному офісі, в віддалених офісах знаходяться: допоміжний сервер, а також сервери, які надають змогу зменшити навантаження на канали зв’язку.

В таблицях 2.1 і 2.2. представлено склад підрозділів з вказанням кількості робочих станцій і повний перелік експлуатаційних систем і ПЗ.

Кількість вирішуваних завдань L = 148.

Число користувачів системи N= 595, число вузлів M = 1340, число додатків N = 1294, число баз даних R=46.

Таблиця 2.1 – Приклад складу підрозділів за кількістю робочих станцій

№ п/п	Назва підрозділу	Кількість робочих станцій
1	Управління	31
2	Відділ фінансового забезпечення	12
3	Відділ внутрішнього контролю	21
4	Адміністративний відділ	4
5	Відділ доходів	10
6	Відділ охорони	8
7	Відділ бюджетного учту по операціям бюджету підприємства	21
8	Операційний відділ	18
9	Відділ термінального обслуговування	8
10	Відділ організації контрольної роботи	19
11	Контролюючий відділ	26
12	Ревізійний відділ	15
13	Юридичний відділ	37
14	Відділ інформаційних технологій	12
15	Відділ фінансового забезпечення	20
16	Відділ матеріально-технічного забезпечення	25
17	Відділ технічного контролю	13
18	Відділ будівництва	11
19	Транспортний відділ	9
20	Відділ безпеки	22
21	Відділ інформаційного забезпечення	12
22	Відділ телекомунікацій	39
23	Відділ забезпечення діяльності керівництва	38
24	Відділ кадрів	6
25	Відділ доступу	29
26	Відділ по зв`язку з засобами масової інформації	23
27	Профсоюзний комітет	29
29	Учбово-методичний центр	19
Разом		537

Таблиця 2.2 - Перелік експлуатаційних систем і програм

№ п/п	Система (програма)
ПЗ Підприємства	
1	Аналіз роботи з партнерами
2	Аналіз екс. операцій
3	База даних аналізу угод
4	База клієнтів і партнерів
5	Бухгалтерська система
6	Річний звіт
7	Місячний баланс
8	Загальна фінансова звітність
9	Підсистема адміністрування
10	Підсистема аналізу і прогнозу
11	Підсистема внутрішнього документообігу
12	Програма контролю грошових оборотів
13	Тестування мережі
Програми електронної пошти	
14	MS Exchange
Програми доступу в Інтернет	
15	MS Proxy
16	Socks
17	Зовнішній WEB
Інші системи (Програми)	
18	Введення нормативно-довідкової інформації
19	Підсистема забезпечення безпеки інформації
20	Облік матеріалів

За наведеними даними проведено розрахунок параметрів потоків даних між мережами на наявні додатки. При цьому всі користувачіоб'єднані в певні групи.

В результаті розрахунків отримані інтенсивності обміну для кожного каналу зв'язку. Ці результати візуалізовано на розрахункових графіках завантаження каналів зв'язку (рис.2.4).

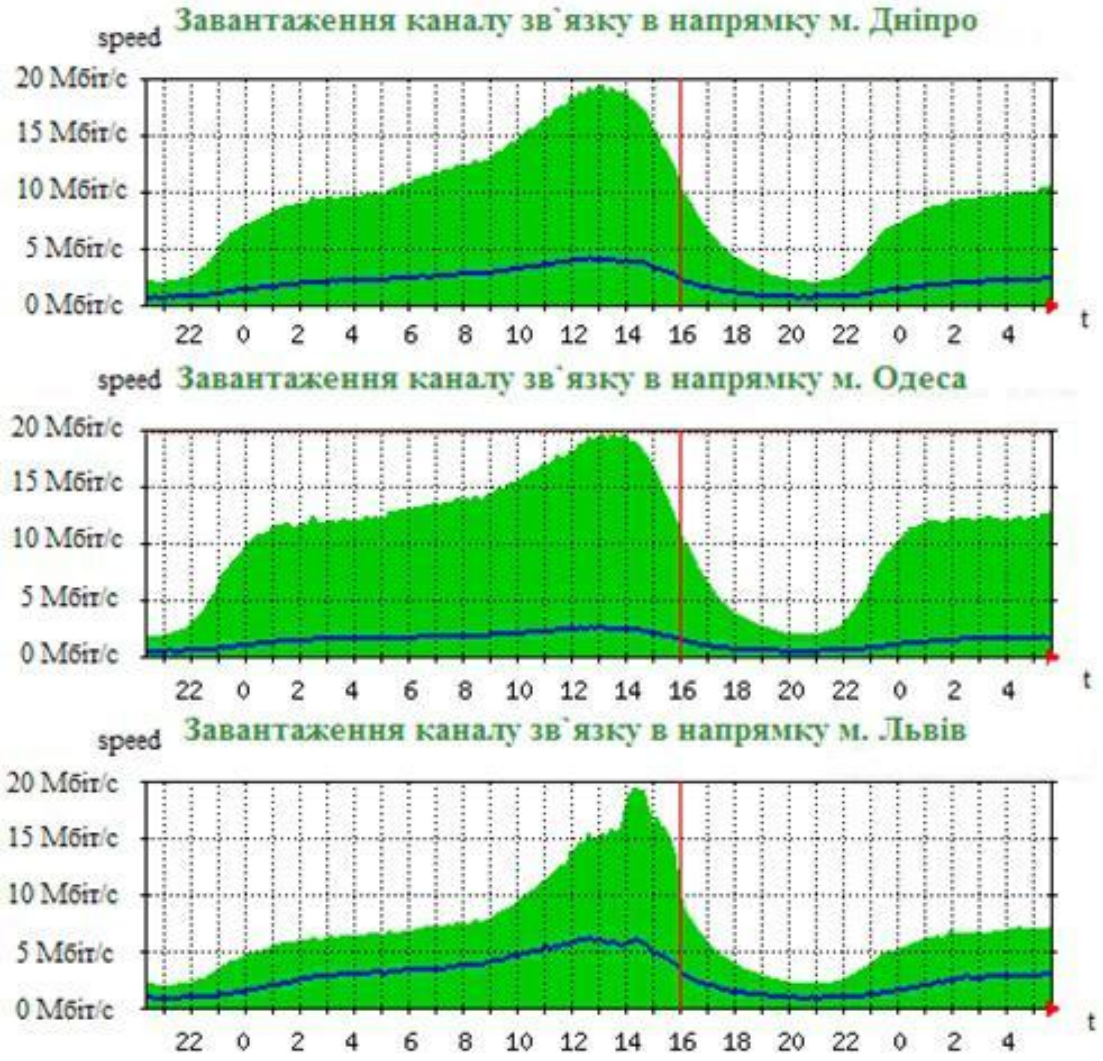

Рисунок 2.4 - Графіки завантаження каналів зв`язку

2.4 Практична організація VPN каналів між офісами

Для практичної реалізації обрано робочу станцію, яка підключена до глобальної мережі. Проаналізуємо, яким чином ця станція обирає шлях, куди потрібно посилати пакети. Цю функцію виконує таблиця маршрутизації, в якій зберігаються правила пересилки пакетів для всіх можливих адрес призначення. Опираючись на цю таблицю, хост приймає рішення, на який саме інфтерфейс отримувача потрібно відправити пакет. Для прикладу розглянемо таблицю маршрутизації, яка знаходиться на звичайній робочій станції (рис.2.5).

Рисунок 2.5 - Приклад таблиці маршрутів робочої станції

Звернемо увагу на частину «IPv4 таблиця маршруту». У цій частині у першій колонці вказано адресу призначення та маску мережі. Наступним вказано номер шлюзу, також інтерфейс та метрика. Якщо в останній колонці On-link, це означає, що отримувач доступний без маршрутизації, оскільки знаходиться в одній мережі з відправником. Метрика призначена для визначення пріоритету, тобто, якщо адреса отримувача має в таблиці маршрутів кілька правил, то використовується той, в якого менша метрика.

На рисунку 2.5 бачимо, що ПК, який ми аналізуємо, має IP-адресу 192.168.31.0 і, якщо використовувати приведену таблицею маршрутів, всі

запити, які будуть адресовані даній мережі, відправляються на інтерфейс 192.168.31.175. Він відповідає мережевій адресі цієї станції. Якщо адреса призначення пакетів знаходиться в одній мережі з адресою джерела, то доставка інформації відбувається без залучення IP-маршрутизації (третій рівень OSI), на канальному рівні (другий рівень). Інакше пакет буде відправлено вузлу, вказаному в відповідному мережі призначення правилом таблиці маршрутів. При відсутності вказівки, він буде відправлений по нульовому маршруту, в якому буде вказано адресу нульового шлюзу (0.0.0.0) у цій мережі. Тобто, якщо пакет не належить даній мережі, і він не має окремого маршруту, він автоматично буде направлений на основний шлюз в мережі.

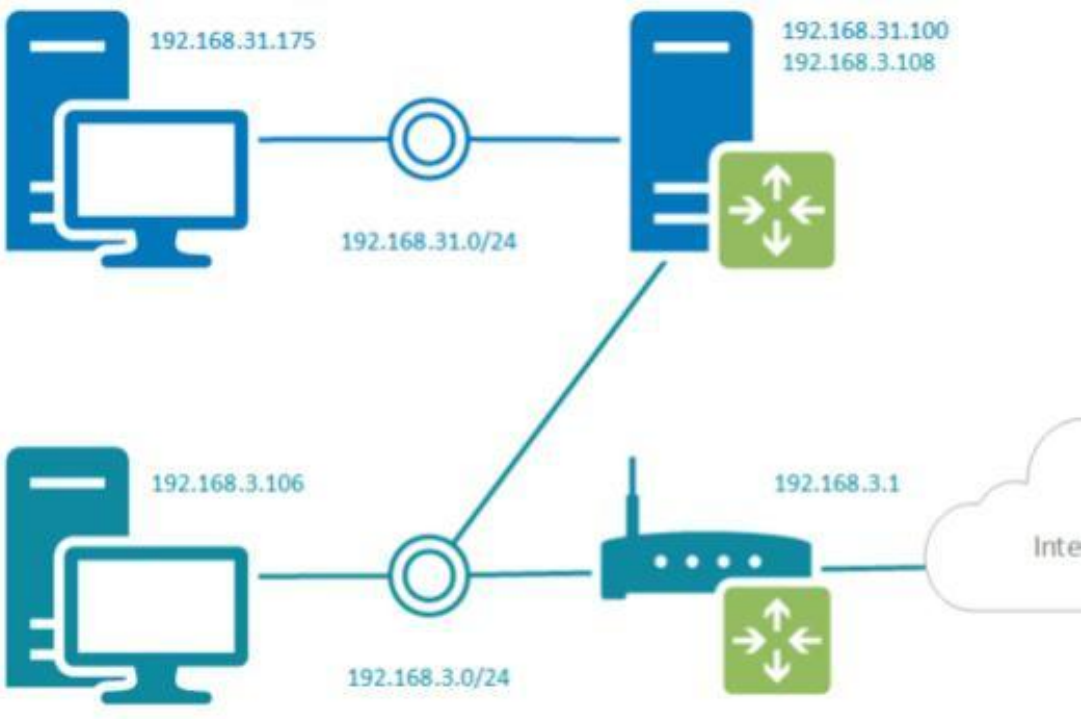

Рисунок 2.6 – Схема маршрутизації

Маршрутизатор, це той пристрій, який і відповідає за пеерсилку пакетів по мережі. Тобто, на ньому зберігаються таблиці маршрутизації. Ось, що вони по суті представляють. Для прикладу представлено скріншот таблиці маршрутизаії звичайного роутера (рис.2.7). На цьому рисунку чітко

видно, що роутер знає та зберігає маршрут до двох мереж (192.168.31.0 і 192.168.3.0). У другому стовпчику бачимо, що до шлюзу з номером 192.168.3.1 міститься нульовий маршрут. Аналізуючи таблицю маршрутизаціє можна заключити, що ті пакети, які будуть мати адреси отримувача в двох відомих мережах, будуть передані на відповідний інтерфейс. Інші – по нульовому маршруту.

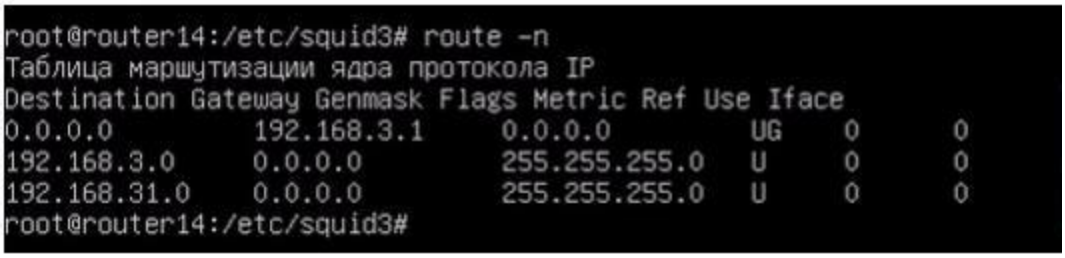

Рисунок 2.7 - Маршрути до мереж

Відомо, що окрім білих та черних є ще сірі IP-адреси, і адреси приватних мереж, можуть бути саме сірими та лежати в одному з трьох діапазонів:10.0.0.0/8;172.16.0.0/12;192.168.0.0/16. Це вільні IP-адреси, вони використовуються широким загалом та не піддаються маршрутизації. Будь-пакет з адресою призначення належить одній з цих мереж буде відкинутий маршрутизатором, якщо для нього немає окремого запису. Тобто, нульовий маршрут для них не існує.

На прикладі це виглядає так. На вузол 192.168.31.175 виконуємо ping вузол 192.168.3.106. У цьому випадку другий вузол знаходиться роутером. Результат цього процесу приведено на рис.2.8 і він є вдалим.

Рисунок 2.8 – Перевірка доступності вузла

Бачимо, що не дивлячись на те, що вузол-джерело не має відомостей про пункт призначення, він відправляє пакет саме на адресу шлюзу. В свою чергу останній аналізує закладену на ньому таблицю маршрутизації та знайде в запис для мережі 192.168.3.0. Після цього відбудиться відправка пакету на потрібний інтерфейс. Виконавши команду трасування отримаємо маршрут:

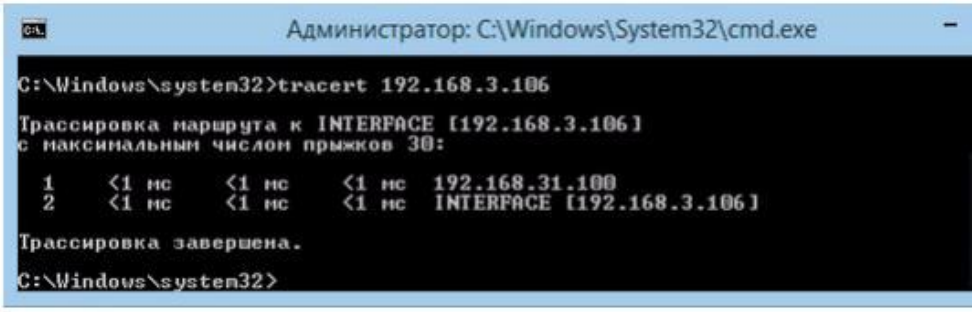

Рисунок 2.9 – Трасування

Проводимо налаштування мережі офісів банку через VPN-з'єднання. Розглянимо ряд стандартних схем побудовиреальної мережі.

1 схема. VPN-сервер (клієнт) і маршрутизатор мережі знаходяться на одному хості.

Зробимо опис маршрутизації пакету у такому випадку. Для пересилки пакету з мережі офісу в мережу філії, він буде відправлений на шлюз за замовчуванням. Він в даній мережі виступає і у ролі VPN-сервера. Логічно, що не знаючи даних про цей пакет, він його просто відкине. Тому потрібно провести ряд налаштувань. На маршрутизаторі офісу додаємо маршрут, в якому послідовно вказуємо адресу вузла мережі, маску та адресу маршрутизатора філії у VPN-мережі.

2 схема. Маршрутизатор і VPN-сервер (клієнт) є різними вузлами мережі.

У такій схемі побудови пересилка пакету може відбуватися безпосередньо VPN-серверу (клієнту) або це виконує шлюз.

У першій схемі для забезпечення пересилки пакетів ми кожному клієнту додаємо маршрут до VPN-сервера (клієнту). (192.168.44.0 mask 255.255.255.0 192.168.31.101). Якщо цього не зробити, вони будуть надходити у шлюз, а той, в свою чергу, їх відкидати. Також, нам потрібно прописати маршрут відправки від VPN-сервера до філії.

Безумовно, така схема є досить складною в налаштуванні, оскільки для кожного вузла потрібно прописувати маршрути. Такий подхід є доцільним, тільки у тому випадку, коли ми маємо невелику мережу, або стоїть завдання організації вибіркового доступу.

Ще один варіант – функцію пересилки бере на себе шлюз. При такому розкладу всі пакети будуть направлятися по нульовому маршруту, тобто на шлюз. Він, в свою чергу, просто буде перенапрявлять його VPN-сервера (клієнту). Це забезпечується шляхом додавання до таблиці потрібного

маршруту. Для пересилки отримувачу пакета VPN-сервер вказує маршрут до потрібної мережі.

Для доступу з мережі філії в мережу офісу необхідно додати потрібні маршрути на мережеві вузли філії. Для спрощеного виконання цього, у філії додаємо маршрут до VPN серверу (Клієнту) на маршрутизаторі, а в офісі додаємо його тільки на потрібні комп'ютери.

3 ДОСЛІДЖЕННЯ НАДІЙНОСТІ ШИФРУ RC4 ПРИ VPN З'ЄДНАННІ

Тунельний протокол типу PPTP встановлює захищене з'єднання з сервером за рахунок шифрування PPE (Point-to-Point Encryption) створним компанією Microsoft. Шифрування даних, що використовується в цьому протоколі відповідає алгоритму RC4(Rivest cipher 4). Даний шифр є симетричним, це означає, що ключ шифрування і розшифрування є однаковим. Потокові алгоритми шифрування послідовно обробляють текст повідомлення. Ідеальним варіантом з точки зору стійкості для потокового шифру, є розмір ключа, який можна співставити з розміром шифрованих даних. Тоді кожен біт відкритого тексту об'єднується з відповідним бітом ключа за допомогою суми по модулю 2 (XOR), утворюючи зашифровану послідовність. Для розшифровки потрібно виконати ту ж операцію ще раз на приймаючій стороні.

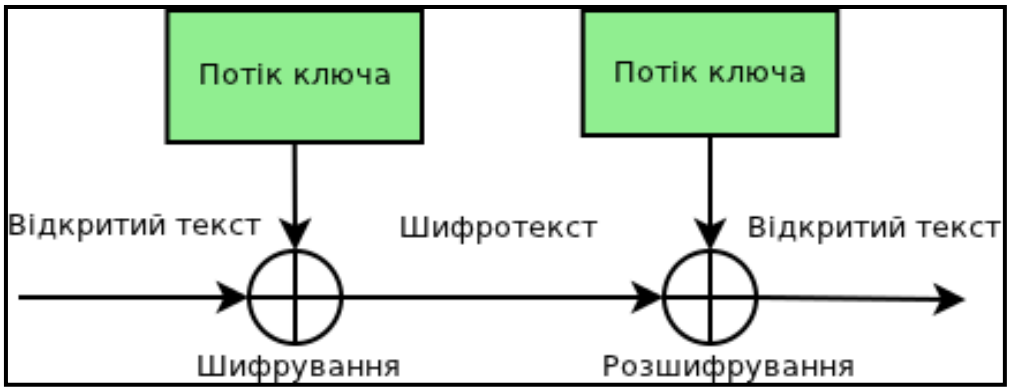

Рисунок 3.1 - Схема шифрування-дешифрування RC4

Опціонально довжина ключа може бути задана у 32, 40, 56, 64, 72, 128 або 256 біт. Це вхідні данні для мого дослідження.

3.1 Умови перехоплення трафіка шляхом атаки MITM на абонента мережі VPN

Проводячи технічний аудит віртуальних приватних з'єднань спеціалісти з комп'ютерної безпеки використовують різні способи. Від соціальної інженерії та методів стеження, до цілого переліку кібератак. Наприклад експлуатація вразливістей операційних систем і програмного забезпечення. Найпоширенішою в такому випадку є, так звана, атака «людина посередині» MITM (Man in the midle). Це ситуація, коли криптоаналітик здатний перехоплювати мережевий трафік, виступаючи посередником зв'язку.

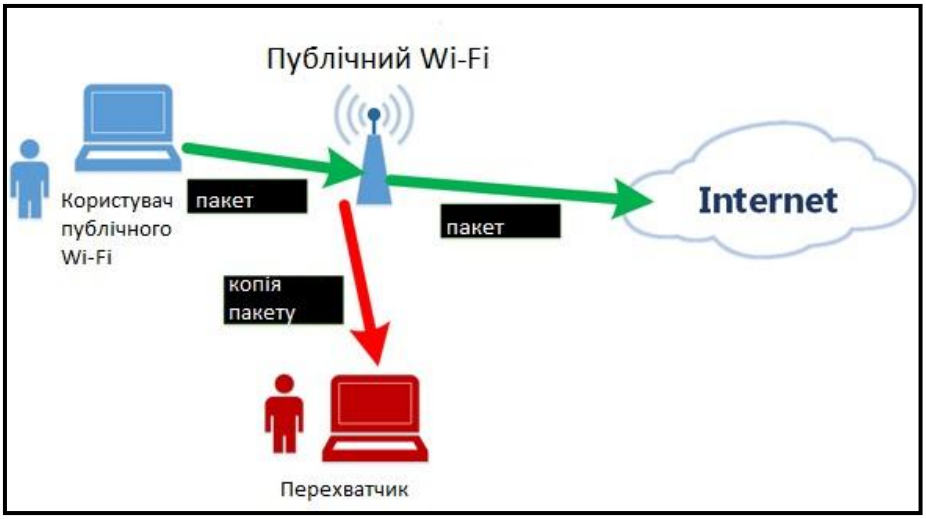

Рисунок 3.2 - Атака «людина посередині» MITM (Man in the midle)

Атака починається з прослуховування каналу зв'язку у публічному місці або біля офісу компанії та закінчується тим, що криптоаналітик намагається підмінити перехоплене повідомлення, витягти з нього корисну інформацію або перенаправити його на який-небудь зовнішній ресурс. Такий вид втручання в мережу неможливо виявити і тому є дуже дієвим.

Зазвичай перехоплений трафік це дамп пам'яті маршрутизатора або комп'ютера за яким працює жертва. Він виглядає як файл формату [назва файлу.PCAPNG] і містить данні у шістнадцятковому вигляді.

Використовується для зберігання даних, отриманих з мережі за допомогою мережевого інтерфейсу Wireshark, яким був здобутий цей файл.

Якщо трафік, що перехоплюється, передано VPN каналом, то цей файл буде зашифрований тим алгоритмом шифрування, який вказаний у налаштуваннях VPN серверу. У випадку який досліджується - це 7 файлів, які містять однакову інформацію і зашифрованиі алгоритмом RC4 (Rivest cipher 4). Кожен файл має свій ключ шифрування конкретної довжини 32, 40, 56, 64, 72, 128 та 256 біт.

3.2 Технічні умови проведення експерименту

Для дослідницької інфраструктури мною було використано сервіс хмарних обчислень Caspio (PaaS Provider).

Операційна система на якій проводився експеримент - Kali Linux.

Це дистрибутив типу Debian Linux , призначений для цифрової криміналістики і тестування на проникнення.

Методи якими було виконано підбір ключа шифрування:

1. Програма для підбору прямим перебором ARCFOURdecrypt.

Яка виконує алгоритм на відеокарті (GPU) та (або) на процесорі (CPU).

2.Програма підбору Rainbowcrpt, у якій підбір ключа здіснюється за допомогою словників або таблиць Rainbow tables.

Таблиці - це особливий тип словника, який містить список паролів і дозволяє підібрати пароль протягом меншого часу з ймовірністю 85-99%.

3.3 Результати експерименту та їх аналіз

У цьому розділі визначено залежність часу підбору ключа шифрування RC4 від його довжини. З метою отримання об’єктивних результатів тестування виконувалось наступним чином. Для кожного методу, яким було проведено підбір ключа, виконано 2 раунди підбору. Для методу прямого перебору ключів шифрування перший раунд виконувався на потужності

процесора (CPU) а другий на відеокарті(GPU). Підбір ключа шифрування за допомогою словника ключів шифрування Rainbow tables не дає точної гарантії підбору, тому деякі значення були упущені. В результаті побудовано дві таблиці замірів часу для кожного методу підбору ключа з усіма необхідними показниками.

Таблиця 3.1 - Результати підбору ключа шифрування прямим перебором

Довжина ключа (біт.)	Час першого раунду підбору на CPU (год.)	Час другого раунду підбору на GPU (год.)	Середній час (год.)
32	4.2	2.1	3.15
40	6.0	4.5	5.25
56	12.1	11.7	11.9
64	24.3	23.5	23.9
72	36.7	37.2	36.95
128	72.9	73.0	72.95
256	Time out	Time out	Time out

Аналізуючи таблиці можна побачити, що є пряма залежність часу підбору ключа шифрування від довжини цього ключа. Чим більша довжина ключа шифрування тим довше виконується його підбір. Для будь-якої криптографічної системи завжди існує поняття цінності інформації.

Наведений графік ілюструє залежність цінності добутої інформації від часу в данному експерименті. Він показує, що для криптоаналітика після проходження певного часу інформація втрачає свою цінність. Тому для підвищення надійності передачі данних по каналах VPN з використанням

PPTP слід використовувати найбільшу з можливих довжину ключа шифрування, яку будуть підтримувати усі мережеві пристрої.

Таблиця 3.2 - Результати підбору ключа шифрування за допомогою словника ключів шифрування Rainbow tables

Довжина ключа (біт.)	Час першого раунду підбору (год.)	Час другого раунду підбору (год.)	Середній час (год.)
32	0.5	1.2	1.1
40	5.0	4.0	4.5
56	No result	10.0	10.0
64	20.3	21	20.65
72	34.0	35.5	34.75
128	61.1	No result	61.1
256	85.3	88.7	87

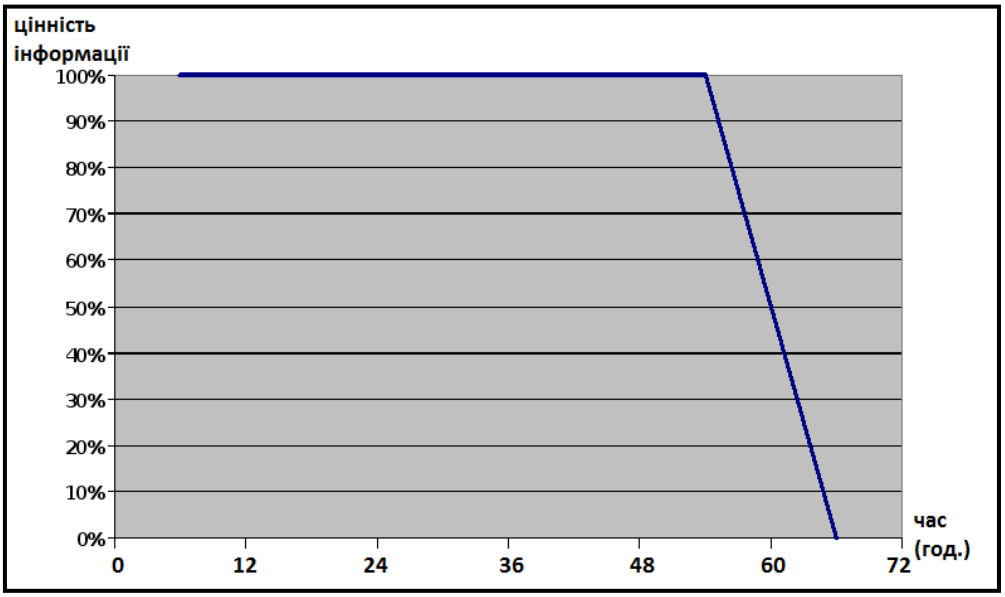

Рисунок 3.3 - Графік цінності інформації від часу

4 ЕКОНОМІЧНА ЧАСТИНА

4.1 Техніко-економічне обґрунтування розробки

В кваліфікаційній роботі розглядається удосконалення комп'ютерної системи компанії з опрацюванням побудови, налаштування та безпеки корпоративної мережі. Для удосконалення КС необхідно облаштувати підприємство комп'ютерною технікою та активним мережним обладнанням, що забезпечить оперативний доступ до даних клінічної інформаційної системи, підвищить доступність та якість рівня надання медичної допомоги населенню за рахунок впровадження електронної амбулаторної карти, під'єднання до електронної системи eHealth та доступу до Інтернет.

Для удосконалення КС підприємства застосовуються обладнання спеціалізованих виробників. 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.

4.2 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 4.1.

Капітальні витрати розраховуються за формулою:

$$К_{пр} = К_{об} + К_{тр} + К_{мн} + К_{пз}, \quad (4.1)$$

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 4.1 – Кошторис капітальних витрат

№ п/п	Найменування обладнання	Ед. виміру	Кіль-кість	Вартість од. облад-я, грн	Сумма, грн.
1	Мережний екран ASA 5505	шт	1	23802	23802
2	Маршрутизатор Wi-Fi Linksys E5400	шт	1	1359	1359
3	Комутатор D-Link DGS-1008D	шт	2	758	1516
5	Кабель UTP Cat 5e	м	300	21	6300
6	Конектор RJ-45	шт	40	5	200
7	Розетки RJ-45	шт	20	27	540
Загалом					33717

Загальна вартість обладнання $К_{об}$=33717 грн.

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

$К_{тр}$=33717 *7%= 2360,19 грн.

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

$К_{мн}$=33717*8%= 2697,36 грн.

Проектні капітальні витрати на обладнання складуть:

$$К_{пр.об} = 33717 + 2360,19 + 2697,36 = 44180,7 \text{ грн}$$

4.3 Розрахунок капітальних витрат на програмне забезпечення

4.3.1 Розрахунок часу на розробку програмного забезпечення

Трудомісткість розробки програмного забезпечення:

$$t = t_o + t_д + t_a + t_n + t_{нал} + t_{док}, \quad (4.2)$$

де 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;

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

$t_{\text{док}}$ - 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:

$$Q = q \cdot c \cdot (1+p) \qquad (4.3)$$

де q –кількість операторів, використовуваних у програмі.

c – коефіцієнт складності програми;

p – коефіцієнт корекції програми в процесі її обробки.

Приймаємо q = 100.

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

$$Q = 100 \cdot 1{,}25(1+0{,}1) = 137.5$$

Оцінка витрат праці на підготовку й опис завдання становлять

$t_0 = 50$ люд.-годин.

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

$$t_д = \frac{Q \cdot B}{(75...85) \cdot k} \text{ люд.-годин} \qquad (4.4)$$

де В – коефіцієнт збільшення витрат праці, В=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:

$$t_{\text{д}}=\frac{137.5*1,4}{80*1,2}=2.15 \text{ люд.-годин.}$$

Витрати на розробку алгоритму розв'язку завдання:

$$t_a = \frac{Q}{(20...25)\cdot k} \text{ люд.-годин} \qquad (4.5)$$

Для розроблювального програмного забезпечення:

$$t_a = \frac{137.5}{20\cdot 1,2} = 5.73 \text{ люд.-годин.}$$

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

$$t_n = \frac{Q}{(20...25)\cdot k} \text{ люд.-годин} \qquad (4.6)$$

Для розроблюваного програмного продукту:

$$t_n = \frac{137.5}{20\cdot 1,2} = 5.73 \text{ люд.-годин.}$$

Витрати праці на налагодження програми на ЕОМ розраховуються по формулі:

$$t_{нал} = \frac{Q}{(4...5)\cdot k} \text{ люд.-годин} \qquad (4.7)$$

Для конкретного програмного продукту:

$$t_{нал} = \frac{137.5}{5\cdot 1,2} = 22.92 \text{ люд.-годин.}$$

Витрати праці на підготовку документації за завданням визначаються по формулі:

$$t_Д = t_{ДР} + t_{ДО,} \text{ люд.-година} \qquad (4.8)$$

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

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

$$t_{ДР} = Q/(15…20)\cdot k, \quad (4.9)$$

$t_{ДР}$ = 137.5/18·1,2 = 6.37 люд.-година;

$$t_{ДО} = 0,75\cdot t_{ДР}, \quad (4.10)$$

$t_{ДО}$ = 0,75· 6.37= 4.77 люд.-година.

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

$t_{Д}$ = 6,37+ 4,77= 11,14 люд.-година.

Трудомісткість розробки програмного забезпечення буде становити:

t = 50 + 2,15 +5,73 + 5,73 + 22,92 + 11,14 = 97,66 людино-годин.

4.3.2 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 $З_{мч}$

$$К_{пз} = З_{зп} + З_{ми}, \text{ грн.} \quad (4.11)$$

Заробітна плата розробника програмного забезпечення:

$$З_{зп} = t\cdot С_{пр}, \text{ грн.} \quad (4.12)$$

де t – загальна трудомісткість обробки програмного забезпечення;

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

$С_{пр}$ = 155 грн./година.

Заробітна плата за розробку програмного забезпечення дорівнює:

$З_{зп}$ = 97,66 ·155 = 15137,84 грн.

Вартість машинного часу, необхідного для налаштування програми на ЕОМ:

$$З_{мч} = t_{нал}\cdot С_{мг}, \text{ грн.} \quad (4.13)$$

де:

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

$С_{мг}$ – вартість машино-години ЕОМ, грн./година. $С_{мг}$ = 9,32 грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$З_{мч}$ = 22,92·9,32 = 213,58 грн.

Вартість 1 години машинного часу ПК визначається за формулою

$$Смч = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot Н_a}{F_p} + \frac{К_{лпз} \cdot Н_{апз}}{F_p} \quad (4.14)$$

Смч=(0,6*22,92*0,642)+(3000*0,5)/1920+(3000*0,25)/1920=9,32 грн/год

де $P=0,6$ – встановлена потужність ПК, кВт;

C_e =0,642– тариф на електричну енергію з ПДВ, грн/кВт*година;

(Тариф відповідно до тарифів ПАТ «ДТЕК Дніпрообленерго для споживачів 2 класу з 01 січня 2020 року» = 535,6 грн/МВт без ПДВ»)

$Ф_{зал}$ =3000– залишкова вартість ПК на поточний рік, грн.;

$Н_a$ =0,5– річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ =0,25– річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$=3000 грн, вартість ліцензійного програмного забезпечення, грн.(табл.4.2.);

F_p=1920– річний фонд робочого часу (за 40-годинного робочого тижня F_p= 1920).

Таблиця 4.2 – Вартість необхідного програмного забезпечення

Програмне забезпечення	Вартість, грн
Cisco ASA 5500 Series SSL VPN Licenses	3000
Cisko Packet Tracer	0
PuTTy	0
Всього	3000

Витрати на розробку програмного забезпечення системи керування будуть становити:

$К_{пз}$ = 15137,84 + 213,58 = 15351,42 грн.

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

Очікувана тривалість розробки програмного забезпечення:

$$T = \frac{t}{B_k \cdot F_p}, \text{ міс.} \quad (4.15)$$

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

$F_р$ – місячний фонд робочого часу (Fр = 176 годин).

Визначимо тривалість розробки ПО:

$$T = \frac{97,66}{1 \cdot 176} = 0,55 \text{ міс.}$$

Таким чином, капітальні витрати розраховані за формулою (4.1) дорівнюють:

$К_{пр}$ = 33717+2360,19+2697,36+15367 = 54141,54 грн.

Висновок

При розробці компютерної мережі капітальні витрати 54141,54 грн, у тому числі капітальні витрати на обладнання мережі 33717 грн та витрати на оплату праці по розробці моделі компютерної мережі 15367 грн.

У загальній сумі витрат на розробку мережі.

Вартість комплектуючих складає – 61,6 %.

Витрати на монтажно-налагоджувані та транспортні роботи – 9%.

Заробітна плата на розробку моделі – 28%.

Витрати на використання ЕОМ – 0,4%.

Всього: 100%.

Найбільша частка витрат – витрати на комплектуючі – 61,6 %.

5 ОХОРОНА ПРАЦІ

5.1 Загальні положення

До роботи на персональному комп’ютері допускають осіб, які пройшли інструктажі з питань охорони праці та пожежної безпеки.

Користувач зобов’язаний:

– виконувати правила внутрішнього трудового розпорядку;

– не допускати за своє робоче місце сторонніх осіб;

– не виконувати вказівок, які суперечать правилам охорони праці та пожежної безпеки;

– знати правила надання домедичної допомоги;

– знати розташування та вміти користуватись первинними засобами пожежогасіння;

– вміти працювати з ПК.

Основні небезпечні та шкідливі виробничі фактори, що можуть впливати на користувача:

– підвищений рівень статичної електрики;

– нерівномірність розподілу яскравості в полі зору;

– підвищена яскравість світлового зображення;

– ураження електричним струмом;

– напруга зору та уваги;

– тривалі статичні навантаження.

У приміщеннях із ПК має бути природне і штучне освітлення.

При розміщенні робочих місць необхідно унеможливити пряме засвічування екрана природним освітленням.

При природному освітленні слід передбачити наявність сонцезахисних засобів (плівка, жалюзі, штори тощо).

Світлові відблиски із клавіатури, екрана та інших частин ПК у напрямку очей користувача неприпустимі.

Основним обладнанням робочого місця є ПК або ноутбук, монітор, клавіатура, маніпулятор, робочий стіл, стілець (крісло).

При розміщенні елементів робочого місця слід враховувати:

– робочу позу користувача;

– простір для розміщення користувача;

– можливість огляду елементів робочого місця;

– можливість огляду простору поза межами робочого місця;

– можливість робити записи, розміщувати на робочому столі документацію та матеріали, які використовує користувач.

Розміщення елементів робочого місця не має заважати рухам та переміщенню для експлуатування ПК.

Монітор встановлюють так, щоб відстань від поверхні екрана до очей користувача була 600-700 мм залежно від розміру екрана.

Клавіатуру розміщують на робочому або окремому столі на відстані 100-300 мм від краю з боку користувача. Положення клавіатури та кут її нахилу залежить від побажання користувача (як правило, в межах 5-15°). Не допускати хитання клавіатури.

Конструкція робочого столу має бути такою, щоб оптимально розмістити на робочій поверхні обладнання, що використовують, з урахуванням кількості, розмірів, конструктивних особливостей і характеру його роботи.

Крісло має забезпечувати підтримування раціональної робочої пози під час виконання основних виробничих операцій та можливість зміни пози. Тип робочого крісла обирають залежно від характеру та тривалості роботи.

Раціональна поза користувача:

– ступні розташовані на підлозі або на підставці для ніг;

– стегна зорієнтовані у горизонтальній площині;

– верхні ділянки рук вертикальні;

– кут ліктьового суглоба у межах 70-90°;

– зап’ястя зігнуті під кутом не більше ніж 20°;

– нахил голови у межах 15-20°, а часті її повороти виключені.

Для забезпечення оптимальної робочої пози користувача необхідно:

– засоби праці, з якими користувач має тривалий або найбільш частий зоровий контакт, розмістити у центрі зони зорового спостереження та моніторного поля;

– забезпечити відстань близько 500 мм між найважливішими засобами праці, з якими користувач працює найчастіше.

ПК встановлювати на рівній твердій поверхні (столі). Не дозволено встановлювати ПК та оргтехніку на хитких підставках чи на похилій поверхні.

ПК не встановлювати впритул до стіни, перегородки тощо. Не допускати загородження вентиляційних отворів ПК сторонніми предметами.

Розетка біля ПК має бути в доступному місці, щоб в аварійних випадках можна було своєчасно його відімкнути. Не рекомендовано використовувати подовжувачі.

Під час переміщення ПК, периферійних пристроїв витягти вилку живлення з розетки.

Не допускати ушкодження чи модифікування шнура живлення. Заборонено ставити важкі речі на шнур живлення, тягнути чи надмірно перегинати його, скручувати та перев’язувати шнур живлення вузлом.

ПК під’єднувати до електромережі лише за допомогою справних штепсельних з’єднань та електророзеток заводського виробництва.

Штепсельні з’єднання та електророзетки мають бути зі спеціальними контактами для під’єднання нульового захисного провідника. Їхня конструкція має забезпечувати з’єднання нульового захисного провідника раніше, ніж з’єднання фазового та нульового робочого провідників. Порядок роз’єднань при вимкненні має бути зворотнім.

Заборонено під’єднувати електрообладнання до звичайної двошнурової електромережі.

За невиконання цієї інструкції працівники несуть відповідальність згідно з чинним законодавством.

5.2 Вимоги безпеки перед початком роботи на ПК

Оглянути робоче місце і навести на ньому лад; впевнитись, що на ньому немає сторонніх предмети, все обладнання і блоки ПК з'єднані з системним блоком з'єднувальними шнурами.

Перевірити надійність встановлення апаратури на робочому столі. Монітор не має стояти на краю стола. Повернути монітор так, щоб було зручно дивитися на екран — під прямим кутом (а не збоку) і трохи зверху вниз; при цьому екран має бути трохи нахиленим — нижній край ближче до користувача.

Перевірити загальний стан апаратури, справність електропроводки, з'єднувальних шнурів, штепсельних вилок, розеток, заземлення захисного екрана.

Вставити вилку в розетку і впевнитися, що вона міцно тримається. Заборонено вставляти і виймати вилку мокрими руками.

Відрегулювати та зафіксувати висоту крісла та зручний для користувача нахил спинки.

За потреби приєднати до комп'ютера необхідну апаратуру (принтер, сканер тощо). Усі кабелі, що з'єднують системний блок із іншими пристроями, вмикати та вимикати лише при вимкненому комп'ютері.

Відрегулювати яскравість свічення, контрастовість монітора.

Про всі виявлені несправності інформувати керівника робіт і не братися до роботи, доки їх не буде усунено.

5.3 Вимоги безпеки під час виконання роботи на ПК

Під час роботи на ПК:

– стійко встановити клавіатуру на робочому столі, не допускаючи її хитання, водночас передбачити можливість її поворотів та переміщень;

– якщо в конструкції клавіатури не передбачено простору для упору долонь, клавіатуру розміщують на відстані не менше 100 мм від краю столу в оптимальній зоні моніторного поля;

– під час роботи на клавіатурі сидіти рівно, не напружуватися;

– щоб зменшити несприятливе навантаження на користувача при роботі з комп'ютерною мишею (вимушена поза, необхідність постійно контролювати якість дій), забезпечити велику вільну поверхню столу для переміщення комп'ютерної миші та зручного упору ліктьового суглоба;

– періодично при вимкненому комп'ютері прибирати пил із поверхонь апаратури спеціальними серветками.

При роботі з ПК заборонено:

– самостійно розбирати та ремонтувати системний блок (корпус ноутбука), монітор, клавіатуру, комп'ютерну мишу тощо;

– встромляти сторонні предмети до вентиляційних отворів ПК, ноутбука або монітора;

– ставити на системний блок ПК та периферійні пристрої металеві предмети, ємкості з водою (вази, горщики для квітів, склянки), оскільки через потрапляння води у середину апарата може виникнути пожежа або ураження електрострумом.

Тривалість безперервної роботи за ПК не має перевищувати 2 год. Після цього необхідно зробити 15-хвилинну перерву.

Якщо виник зоровий дискомфорт або інші неприємні відчуття, необхідно зробити коротку перерву.

Для зниження нервово-емоційного напруження, стомлення зорового аналізатора, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіподинамії, запобігання втомі доцільно під час декількох перерв виконувати комплекс вправ.

5.4 Вимоги безпеки після закінчення роботи на ПК

Зберегти інформацію.

Вимкнути ПК, монітор чи ноутбук.

Вимкнути стабілізатор, якщо комп’ютер під’єднаний до мережі через нього.

Прибрати робоче місце.

5.5 Вимоги безпеки в аварійній ситуації

Аварійні та небезпечні ситуації під час виконання роботи на ПК можуть виникнути у разі: короткого замикання, перевантаження блоку живлення системного блоку, перегрівання, пожежі, поломки крісла тощо.

У разі виникнення аварії або ситуації, що може привести до аварії, нещасного випадку, негайно від’єднати ПК від електромережі, повідомити інцидент керівникові.

Не допускати в небезпечну зону сторонніх осіб.

Якщо стався нещасний випадок, зберегти обстановку в робочій зоні та устаткування у такому стані, в якому вони були на момент події (якщо це не загрожує життю і здоров’ю інших працівників і не призведе до більш тяжких наслідків). Поінформувати про подію керівника робіт (іншу відповідальну особу підприємства) та в подальшому керуватися його вказівками. Вжити заходів, щоб запобігти подібним випадкам у подальшому.

У разі виникнення пожежі (ознак горіння), повідомити керівнику та, за потреби, викликати оперативно-рятувальну службу за телефоном 101 або 102 (назвати адресу та місце виникнення пожежі, наявність людей, повідомити своє прізвище) та вжити можливих заходів для евакуювання людей, гасіння (локалізації) пожежі наявними засобами пожежогасіння. Пам’ятати, що гасіння електротехнічних пристроїв, які перебувають під напругою, виконувати лише після їх попереднього від’єднання від електромережі. Гасити за допомогою вуглекислотних або порошкових вогнегасників, а в окремих випадках — сухим піском.

За потреби надати потерпілому домедичну допомогу згідно з інструкцією, що діє на підприємстві. У разі подальшого погіршення самопочуття потерпілого, не припиняючи надання домедичної допомоги, викликати за телефоном 103 швидку медичну допомогу.

Виконувати вказівки керівника робіт для ліквідування небезпеки.

ВИСНОВКИ

Сучасні технології не стоять на місці, тому кожен рік професіонали придумують різні нововведення.. Створення єдиної робочої середовища для величезної кількості комп'ютерів стало можливим завдяки локальних і глобальних мереж. Але тут також виникла необхідність в управлінні робочими процесами і реалізації різних завдань. За виконання цих функцій відповідає адміністрування комп'ютерних мереж.

В роботі розглянуто та визначено переваги технологій VPN. Обґрунтовано основні переваги впровадження і використання технологій VPN в корпоративних мережах. Проведена класифікація способів створення віртуальних приватних мереж в залежності від можливостей комунікаційного обладнання і вимог до топології мережі. Проаналізовано методи і засоби побудові віртуальних приватних мереж, визначені найбільш придатні для застосування мереж підприємства.

На прикладі АБ «УКРГАЗБАНК» виконано дослідження побудови корпоративної приватної мережі, проаналізовано склад інформаційної мережі підприємства, загальний опис та оцінка завантаження каналів зв`язку корпоративної мережі. На базі розглянутої мережі виконано практичну організацію VPN каналів між офісами підприємства, аналіз особливостей організації віртуального офісу. Результатом роботи є також таблиці дослідження залежності часу підбору ключа шифрування RC4 у протоколі PPTP від його довжини. З результатів експерименту випливає, що для підвищення надійності передачі даних по каналах VPN з використанням PPTP слід використовувати найбільшу з можливих довжину ключа шифрування.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кульгин М. Технологія корпоративних мереж. Енциклопедія. - СПб .: Пітер, 2001. - 704 с.

2. Милославська Н.Г / Інтрамережі: доступ в Internet, захист. Навчальний посібник для ВНЗ. - М .: ЮНИТИ, 1999 - 468 с.

3. Новиков Ю. Локальні мережі: архітектура, алгоритми, проектування. - М .: изд-во ЕКОМ, 2000. - 568 с.

4. Норенков І.П., Трудоношін В.А. Телекомунікаційні технології і мережі. - М .: изд-во МГТУ ім. Н.е. Баумана, 1999 - 392 с.

5. Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі. Принципи, технології, протоколи. Підручник для вузів. 2-е изд - СПб .: Питер-прес, 2002 - 864 с.

6. Оліфер В.Г., Оліфер Н.А. Нові технології і обладнання IP-мереж - СПб .: БХВ - Санкт-Петербург, 2000. - 512 с.

7. Розробка інфраструктури мережевих служб Microsoft Windows 2000. Навчальний курс MCSE М .: вид-во Російська редакція, 2001. - 992 с.

8. Сосінскій Б., Дж. Московіц Дж. Windows 2000 Server за 24 години. - М .: Видавничий будинок Вільямс, 2000. - 592 с.

9. Тейт С. Windows 2000 для системного адміністратора. Енциклопедія. - СПб.: Пітер, 2001. - 768 с.

10. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2020. – 69 с.

11. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання курсового проекту студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, Я.В.

Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 28 с.

12. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 1. – 60 с.

13. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.

Додаток А

Текст програми налаштування VPN з’єднання

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ VPN З’ЄДНАННЯ

Текст програми

804.02070743.20005-01 12 01

Листів 6

2020

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для налаштування VPN з’єднання.

ЗМІСТ

ДОДАТОК А

1. Фрагмент скрипту налаштування VPN з'єднання

```
#!/bin/bash
#path to ppp
ppp=/etc/ppp

if [[ $(id) != 'uid=0'* ]]; then
echo "Only root can set up VPN connections."
exit 1
fi
echo "Welcome to VPN connection setup wizard!"

echo "------------------------"
printf "Enter your VPN connection name: "
read i_vpn_name
echo "------------------------"
read provider
if [ $provider = "1" ]; then
prov="Corbina Telecom"
vpn_address="vpn.corbina.net"
elif [ $provider = "2" ]; then
prov="Beeline"
vpn_address="vpn.internet.beeline.ru"
elif [ $provider = "3" ]; then
prov="Other"
printf "Enter your VPN address: "
read vpn_address
else
echo "You've entered wrong answer. Please restart this script."
exit 1
fi

if [ $provider = "3" ]; then
region="3"
routes="route"
else
echo "------------------------"
echo "Please choose your region:"
echo "   1. Moscow region"
echo "   2. St.Petersburg region"
echo "   3. other"
printf "Your region is ...? (1/2/3)? "
read region
if [ $region = "1" ]; then
region_name="Moscow region"
routes="route.msk"
elif [ $region = "2" ]; then
region_name="St.Petersburg region"
routes="route.piter"
elif [ $region = "3" ]; then
```

```
region_name="other"
routes="route"
else
echo "You've entered wrong answer. Please restart this script."
exit 1
fi
fi

echo "------------------------"
printf "Enter your internet login: "
read i_login
echo "------------------------"
printf "Enter your internet password: "
read i_password

echo "------------------------"
echo "Trying to detect your gateway IP automatically..."
i_gw=$(route|grep default|awk '{print $2}')
echo "Detected!"
echo "Your local gateway IP is $i_gw"
if [ $provider = "3" ]; then
printf "Is this correct? (y/n)"
read i_yn
if [ $i_yn = "n" ]; then
printf "Enter your gateway IP: "
read i_gw
fi
else
if [[ $i_gw != '10.'* ]]; then
echo "Unfortunately, the gateway IP wasn't detected correctly. It must
look like 10.x.x.x, so you have to enter it manually."
printf "Enter your gateway IP: "
read i_gw
fi
fi
if [ $region = "2" ]; then
routing="Pre-set routes are in 'route' file as St.Petersburg and it's
region doesn't have DHCP-routing support."
i_dhcp="n"
else
echo "------------------------"
echo "Now you have to choose routing setup method. You can choose DHCP
routing or pre-set routes in 'route' file."
echo "------------------------"
printf "Do you want to get routes via DHCP? ([y]/n)? "
read i_dhcp
if [ $i_dhcp = "y" ]; then
routing="via DHCP"
elif [ $i_dhcp = "n" ]; then
routing="pre-set in 'route' file"
if [ $provider = "3" ]; then
echo "WARNING! You have to edit 'route' file attached to this script
manually as it's configured to work with Corbina and Beeline only.
Check your routing settings at your provider's technical support. Stop
this script with Ctrl+C, edit 'route' file and then restart script."
fi
else
```

```
echo "You've entered wrong answer. Please restart this script."
exit 1
fi
fi
echo "------------------------"
printf "Do you want to automatically install pptp-linux package? Answer 'n' if it's already installed or you have old distro (Debian Etch, Xandros on Eee PC etc.) (y/n): "
read i_install
if [ $i_install = "y" ]; then
pptp_linux="Yes"
else
pptp_linux="No"
fi
echo "------------------------"
echo "Checking gathered information :"
echo "        Connection name: $i_vpn_name"
echo "        Provider: $prov"
if [[ $provider != "3" ]]; then
echo "        Region: $region_name"
fi
echo "        Login: $i_login"
echo "        Password: $i_password"
echo "        VPN address: $vpn_address"
echo "        Gateway: $i_gw"
echo "        Routing setup: $routing"
echo "        pptp-linux package setup: $pptp_linux"
printf "Is this correct? (y/n)? "
read i_correct
if [ $i_correct = "n" ]; then
echo "------------------------"
echo "Check the information and restart this script."
exit 1
fi

if [ $i_install = "y" ]; then
echo "Detecting your system type..."
bit=$(uname -m)
echo "Your system is detected as: $bit"
echo "Installing $bit version of pptp-linux..."
if [ $bit = "i686" ]; then
dpkg -i "$PWD"/pptp-linux_1.7.0-2ubuntu2_i386.deb
elif [ $bit = "x86_64" ]; then
dpkg -i "$PWD"/pptp-linux_1.7.0-2ubuntu2_amd64.deb
fi
fi

if [ $i_dhcp = "y" ]; then
cp   "$PWD"/rfc3442-classless-static-routes   /etc/dhcp3/dhclient-exit-hooks.d/rfc3442-classless-static-routes
mv /etc/dhcp3/dhclient.conf /etc/dhcp3/dhclient.conf_bak
cp "$PWD"/dhclient.conf /etc/dhcp3/dhclient.conf
echo "------------------------"
echo "Routing auto-setup via DHCP installed."
fi
echo "------------------------"
echo "Writing parameters for VPN connection..."
```

```
echo "${i_login} PPTP ${i_password} *" > $ppp/chap-secrets


cp "$PWD"/ip $ppp/ip-up > /dev/null
printf "${ppp}/ip-up.d/\$6 \$1 \$2 \$3 \$4 \$5 \$6" >> $ppp/ip-up
chmod a+x $ppp/ip-up

cp "$PWD"/ip $ppp/ip-down > /dev/null
printf "${ppp}/ip-down.d/\$6 \$1 \$2 \$3 \$4 \$5 \$6" >> $ppp/ip-down
chmod a+x $ppp/ip-down

cp "$PWD"/$routes $ppp/ip-up.d/$i_vpn_name

printf "route del \$4 dev \$1\n" >> $ppp/ip-up.d/$i_vpn_name
printf "route add -host \$4 gw ${i_gw}\n" >> $ppp/ip-up.d/$i_vpn_name
printf "do_route add ${i_gw} \n"   >> $ppp/ip-up.d/$i_vpn_name
printf "route del default \n"             >> $ppp/ip-up.d/$i_vpn_name
printf "route add default dev \$1 \n"     >> $ppp/ip-up.d/$i_vpn_name

chmod a+x $ppp/ip-up.d/$i_vpn_name

cp "$PWD"/$routes $ppp/ip-down.d/$i_vpn_name
printf "do_route del ${i_gw} \n"   >> $ppp/ip-down.d/$i_vpn_name
printf "route del default \n"             >> $ppp/ip-down.d/$i_vpn_name
printf "route add default gw ${i_gw}\n" >> $ppp/ip-down.d/$i_vpn_name
chmod a+x $ppp/ip-down.d/$i_vpn_name

printf "nodeflate\nnobsdcomp\nnoauth\n" > $ppp/options.$i_vpn_name

printf "pty \"pptp $vpn_address --nolaunchpppd --nobuffer --loglevel
0\"\n" > $ppp/peers/$i_vpn_name
printf "connect /bin/true\n" >> $ppp/peers/$i_vpn_name
printf "name ${i_login}\n" >> $ppp/peers/$i_vpn_name
printf "remotename PPTP\n" >> $ppp/peers/$i_vpn_name
printf "file ${ppp}/options.$i_vpn_name\n" >> $ppp/peers/$i_vpn_name
printf "ipparam $i_vpn_name\n" >> $ppp/peers/$i_vpn_name
printf "persist\n" >> $ppp/peers/$i_vpn_name
printf "maxfail 0\n" >> $ppp/peers/$i_vpn_name
printf "lcp-echo-interval 30\n" >> $ppp/peers/$i_vpn_name
printf "lcp-echo-failure 4\n" >> $ppp/peers/$i_vpn_name
printf "mtu 1460\n" >> $ppp/peers/$i_vpn_name
echo "------------------------"
echo "Settings optimization is done!"
echo "------------------------"
echo "Auto reconnect is set up!"
echo "------------------------"
echo "Parameters setup succeeded!"
echo "------------------------"
echo "Restartint network services..."
/etc/init.d/networking restart
echo "Done!"
echo "------------------------"
printf "Do you want to establish your VPN connection now? ([y]/n)? "
read i_vpnstart
if [ $i_vpnstart = "y" ]; then
```

```
echo "------------------------"
echo "Starting VPN connection..."
pon $i_vpn_name
echo "VPN connection is set up and running. If it's all OK and you pay
your internet bills then you're already using Internet :)"
echo "------------------------"
echo "To connect, type: sudo pon $i_vpn_name"
echo "To disconnect: sudo poff"
echo "------------------------"
echo "Don't forget to thank us at forum) All questions about this
script - http://homenet.corbina.net/index.php?showtopic=199266"
else
echo "------------------------"
echo "To connect, type: sudo pon $i_vpn_name"
echo "To disconnect: sudo poff"
echo "------------------------"
echo " Don't forget to thank us at forum) All questions about this
script - http://homenet.corbina.net/index.php?showtopic=199266"
fi
exit 0
```

2. Прямий VPN-тунель між двома комп'ютерами

```
#!/bin/bash
if [[ $1 == '' ]];
then echo -e "Укажите номер порта который нужно слушать";
     exit; fi iface=`ip route get 8.8.8.8 | head -n 1 | sed 's|.*dev
     ||' | awk '{print $1}'` a=0
      until (( $a == 500));
     do packet=`tcpdump -i $iface udp port $1 -vvn -c1 -A` if [[
     "$packet" == *"Ident"* ]]; then pack=`echo "$packet" | grep -e
     "udp sum ok" -e "Ident"` myip=`echo $pack | sed 's/\./ /g' |
     awk '{print $1"."$2"."$3"."$4}'` myport=`echo $pack | sed 's/\./
     /g' | awk '{print $5}'` id=`echo $pack | sed 's|.*Ident:||' |
   awk '{print $1}'` myname=`echo $pack | sed 's|.*Ident:||' |
   awk '{print $2}'` echo "$myip:$myport $myname" > /tmp/vpn2-$id-$myname
echo "MyData $myip:$myport $(cat /tmp/vpn2-$id-* | grep -v $myname |
   awk {'print $1'})" | nc $myip $myport -u -p $1 -w 1 cat /tmp/vpn2-$id-*
topoint=`cat /tmp/vpn2-$id-* | grep -v "$myname" | sed 's/:/ /g'` if [[
$topoint != '' ]]; then ip=`echo $topoint |
   awk '{print $1}'` port=`echo $topoint | awk '{print $2}'` echo "MyData
$ip:$port $(cat /tmp/vpn2-$id-* | grep $myname | awk {'print $1'})" | nc $ip
$port -u -p $1 -w 1
          fi
   fi
   done
```