

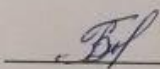
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

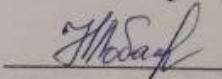
до випускної кваліфікаційної роботи бакалавра
на тему:

«Проект захищеної інформаційно-комунікаційної
мережі банку»

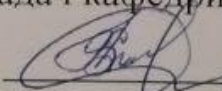
Виконав студент 4-го курсу, групи ЗКБ-17
спеціальності 125 «Кібербезпека»

 Є.А. Бондарчук

Керівник к.т.н., доцент, доцент кафедри КІ та КБ

 Н.М. Лобанчикова

Рецензент старший викладач кафедри КН

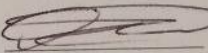
 В.Л. Левківський

Житомир – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії та
кібербезпеки

к.т.н.  Єфіменко А.А.

« 12 » 04 20 21 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента Бондарчука Євгенія Анатолійовича

Тема роботи: Проект захищеної інформаційно-комунікаційної мережі банку
затверджена Наказом по університету від «12» квітня 2021 р. № 134/с

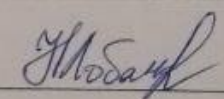
Термін здачі студентом закінченої роботи – 01 червня 2021 р.

Вихідні дані для роботи:

Апаратне забезпечення: маршрутизатори Cisco; Програмне забезпечення:
симулятор GNS; Операційні системи: Cisco IOS

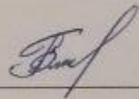
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів,
що їх стосуються

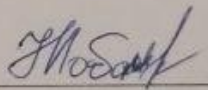
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

Керівник  Лобанчикова Н. М.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання. Опрацювання літературних джерел.	1 березня 2021 – 11 квітня 2021	Виконано
2	Аналіз теоретичних основ побудови захищених інформаційно-	12 квітня 2021 – 16 квітня 2021	Виконано
3	Розробка проекту захищеної інформаційно- комунікаційної мережі	17 квітня 2021 – 12 травня 2021	Виконано
4	Обґрунтування вибору обладнання для налагодження мережі	13 травня 2021 – 25 травня 2021	Виконано
5	Написання пояснювальної записки	26 травня 2021 – 5 червня 2021	Виконано
6	Підготовка презентації та виступу	6 червня 2021 – 10 червня 2021	Виконано
7	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	11 червня 2021	Виконано
8	Захист	18 червня 2021	Виконано

Студент  Бондарчук Є. А.

Керівник  Лобанчикова Н. М.

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи на тему «Проект захищеної інформаційно-комунікаційної мережі банку» викладена на 64 сторінках, містить 22 рисунки, 9 таблиць, 17 літературних джерел.

Метою роботи є розробка проекту захищеної інформаційно-комунікаційної мережі комерційного банку.

У першому розділі представлено результати аналізу методів та засобів захисту інформації комерційного банку. На основі аналізу було виявлено принципи та особливості інформаційної безпеки систем банківських установ, та методи і засоби захисту інформаційних мереж корпоративного банку. В другому розділі проведено проектування топології мережі, системи адресації та підсистеми захисту. В третьому розділі проведено вибір програмного та апаратного забезпечення, налаштування базових засобів захисту та перевірку роботи налаштованої захищеної інформаційно-комунікаційної мережі.

КЛЮЧОВІ СЛОВА: СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СИСТЕМА, КОМЕРЦІЙНИЙ БАНК.

					КІК.КР.Б – 123 – 21 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект захищеної інформаційно- комунікаційної мережі банку Пояснювальна записка	Літ.	Арк.	Аркушів
Розроб.	Бондарчук Є.А.						6	90
Керівник	Лобанчикова Н.М.							
Рецензент	Левківський В.Л.					Житомирська політехніка, група ЗКБ-17		
Н. контр.	Лобанчикова Н.М.							
Зав. каф.	Єфіменко А. А.							

ABSTRACT

The explanatory note to the qualification work on the topic "Project of the secure information and communication network of the bank" is set out on 64 pages, contains 22 figures, 9 tables, 17 references.

The purpose of the work is to develop a project of a secure information and communication network of a commercial bank.

The first section presents the results of the analysis of methods and means of information protection of a commercial bank. Based on the analysis, the principles and features of information security of banking institutions, and methods and means of protection of information networks of a corporate bank were identified. The second section designs the network topology, addressing system and security subsystem. The third section selects the software and hardware, configures the basic means of protection and checks the operation of the configured secure information and communication network.

KEY WORDS: INFORMATION PROTECTION SYSTEM, INFORMATION AND COMMUNICATION SYSTEM, COMMERCIAL BANK.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

РЕФЕРАТ.....	6
ABSTRACT.....	5
ВСТУП.....	7
РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ БАНКІВСЬКОЇ ІНФОРМАЦІЇ.....	9
1.1 Загальна характеристика комерційного банку	9
1.2 Принципи та особливості інформаційної безпеки систем банківських установ.....	13
1.3 Аналіз захисту інформаційних мереж корпоративного банку	19
РОЗДІЛ 2. РОЗРОБКА ПРОЕКТУ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ.....	24
2.1 Розробка проекту інформаційно-комунікаційної мережі	24
2.2 Розробка проекту системи адресації інформаційно-комунікаційної мережі.....	30
2.3. Розробка підсистеми захисту інформаційно-комунікаційної мережі	35
РОЗДІЛ 3. ОБГРУНТУВАННЯ ВИБОРУ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ.....	41
3.1 Обґрунтування вибору апаратного та програмного забезпечення.....	41
3.2 Базове налагодження апаратного та програмного забезпечення та підсистеми захисту	46
3.3 Тестування роботи захищеної інформаційно-комунікаційної мережі.....	52
Висновки до третього розділу	60
ВИСНОВКИ	61
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	62
ДОДАТКИ	64
ДОДАТОК А	65

ВСТУП

З часів своєї появи банківські структури незмінно викликали злочинний інтерес. І цей інтерес був пов'язаний не лише із зберіганням в кредитних організаціях грошових засобів, але й з тим, що в банках зосереджувалась важлива і часто секретна інформація про фінансову та господарську діяльність багатьох людей, компаній, організацій і навіть цілих держав.

В даний час значення інформації, що зберігається в банках, значно збільшилося. Також у зв'язку із всезагальною інформатизацією та комп'ютеризацією банківської діяльності значення інформаційної безпеки банківських структур зросло в декілька разів. Ще 30 років тому об'єктом інформаційних атак були дані про клієнтів банків або про діяльність самого банку. Такі атаки були досить рідкісними, коло їх замовників було дуже вузьким, а збиток міг бути значним лише в особливих випадках. Зараз, в результаті всезагального розповсюдження електронних платежів, банківських пластикових карт, комп'ютерних мереж, об'єктом інформаційних атак стали безпосередньо грошові кошти як банків, так і їх клієнтів. Здійснити злочинну спробу може будь-хто – необхідно лише наявність комп'ютера та підключення до Інтернету. При чому для цього не має необхідності фізично проникати в банк, можна «працювати» і за десятки кілометрів.

Ком'ютеризація банківської діяльності дозволила значно підвищити продуктивність праці працівників банку, впровадити нові фінансові продукти та технології. Однак прогрес в техніці злочинів здійснювався не меншим повільними темпами, ніж розвиток банківських технологій. В даний час більше 90 % всіх злочинів пов'язаних з використанням інформаційно-комунікаційних систем (ІКС) банку. Відповідно, при створенні та модернізації ІКС банкам необхідно приділяти особливу увагу забезпеченню її безпеки. Саме цій проблемі присвячується більша частина кваліфікаційної роботи.

Таким чином, метою даної роботи є розробка проекту захищеної інформаційно-комунікаційної мережі банку.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		7

Об'єкт дослідження – процеси збереження та захисту інформації в інформаційно-комунікаційній системі відділу комерційного банку.

Предмет дослідження – методи та засоби збереження та захисту інформації в інформаційно-комунікаційній мережі відділення банку.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ БАНКІВСЬКОЇ ІНФОРМАЦІЇ

1.1 Загальна характеристика комерційного банку

В даній кваліфікаційній роботі створимо проект захищеної інформаційно-комунікаційної мережі банку на прикладі комерційного банку «ПриватБанк». Заснований в 1992 році, комерційний банк «ПриватБанк» є лідером банківського ринку країни і найбільшим банком з вітчизняним капіталом.

За станом на 1 січня 2021 дані:

- розмір чистих активів «ПриватБанку» складає – 386,8 млрд. грн.
- статутний фонд банку складає - 206 060 млрд. грн.
- власний капітал - 53 828 млн. грн.
- кредитний портфель банку 72788 млрд. грн.
- чистий прибуток Приватбанку за підсумком 2020 року склав 386 940 млн. грн.

Приватбанк також є лідером серед українських комерційних банків за кількістю клієнтів: його послугами користується понад 23% населення України. На сьогоднішній день банк обслуговує 334 тисяч корпоративних клієнтів, приватних підприємців - 314 тисяч і понад 12,5 мільйонів рахунків фізичних осіб. Обсяг залучених банком коштів юридичних осіб на 1 січня 2021 долі становить 20,7 млрд. грн, у тому числі депозитний портфель юридичних осіб - 12430 млрд. грн. Обсяг коштів фізичних осіб, залучених Приватбанком на 1 січня 2021, становить 32754 млрд. грн., у тому числі депозитний портфель фізичних осіб - 27,1 млрд. грн.

Проводячи послідовну політику зміцнення стабільності банку та вдосконалення якості обслуговування, «ПриватБанк» вважає одним з пріоритетних напрямків своєї роботи розвиток комплексу сучасних послуг для індивідуального клієнта. На сьогоднішній день банк пропонує громадянам України понад 150 видів найсучасніших послуг, серед яких поточні, вкладні операції, карткові продукти, різноманітні програми споживчого кредитування, які здійснюються в партнерстві з провідними вітчизняними торговельними,

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

ріелтерськими компаніями й автовиробниками. Приватбанк є уповноваженим Урядом України банком з виплати пенсій і соціальної допомоги громадянам, а також виплати компенсацій жертвам нацистських переслідувань. Сьогодні свою пенсію й соціальні виплати в Приватбанку отримують понад 1,5 мільйона чоловік. Також свої кошти довіряє Приватбанку майже третина всіх вкладників України. Понад 35% клієнтів українських банків обирають «ПриватБанк» при відкритті поточкового рахунку й понад 28% користуються послугами банку під година здійснення грошових переказів.

Національна мережа банківського обслуговування «ПриватБанку», що включає в собі більш 3 000 філій та відділень по всій Україні, дозволяє будь-якому клієнту отримати найвищий рівень обслуговування практично в будь-якій точці країни. Широке коло закордонних партнерів «ПриватБанку» не тільки демонструє його визнання як провідного учасника світової банківської системи, але й, найголовніше, дозволяє найбільш широко задовольняти потреби клієнтів банку, пов'язані з їх міжнародною діяльністю. «ПриватБанк» підтримує кореспондентські відносини з найбільшими іноземними банками, ефективно співпрацюючи з ними на різних сегментах фінансового ринку.

«ПриватБанк» є уповноваженим банком з обслуговування кредитних ліній Світового банку реконструкції та розвитку (МБРР), Європейського банку реконструкції і розвитку (ЄБРР) і Українсько-Німецького Фонду, спрямованих на розвиток малого та середнього бізнесу. «ПриватБанк» єдиний з українських банків має закордонну філію на Кіпрі, також банк активно розвиває систему сучасних фінансових послуг у Росії, Латвії, Португалії, Грузії за допомогою своїх дочірніх банків «Москомприватбанк», Paritatebanka, ТАО «ПриватБанк». Представництва банку працюють у Казахстані та Китаї.

Приватбанк є визнаним лідером вітчизняного ринку платіжних карток. На сьогоднішній день банком випущено більше 18,5 млн. пластикових карт (близько 40% від загальної кількості карт, емітованих українськими банками). У мережі обслуговування пластикових карт банку працює 6 837 банкоматів, пластикові картки банку приймають до оплати понад 46,6 тисяч торгово-сервісних точок по

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

всій Україні. Наявність широкої мережі обслуговування карткових продуктів дозволяє «ПриватБанку» активно впроваджувати послуги з автоматизованої видачі корпоративним клієнтам заробітної плати з використанням пластикових карт. Інноваційна політика «ПриватБанку» орієнтована на впровадження на українському ринку принципово нових, передових банківських послуг, які надають клієнтам нові можливості управління своїми фінансами. «ПриватБанк» першим в Україні запропонував своїм клієнтам послуги інтернет-банкінгу «Приват24» і Gsm-Банкінгу, а також послуги з продаж через мережу своїх банкоматів і Pos-Терміналів електронних ваучерів провідних операторів мобільного зв'язку та Ір-Телефонії.

Надійність та якість проведених банківських операцій багато в чому залежати від досвіду та компетентності фахівців банку. Сьогодні персонал «ПриватБанку» - це команда висококваліфікованих фахівців, здатних оперативно вирішувати найскладніші задачі та задовольнити швидко зростаючі потреби клієнтів у банківському обслуговуванні. На сьогоднішній день у банку працює понад 30 тисяч співробітників, з їх 3 000 - у головному офісі банку. Середній вік співробітників банку складає 34 роки. Більшість працівників «ПриватБанку» (75%) мають вищу освіту, що відповідає профілю займаної посади. У банку створені сприятливі умови для отримання вищої та післядипломної освіти, більше половини співробітників щорічно підвищують свою кваліфікацію.

Банк є юридичним від дня його державної реєстрації. Банк має цивільну правоздатність, яка може бути обмежена лише за рішенням суду. Цивільна правоздатність Банку виникає з моменту його створення і припинення з дня внесення до єдиного державного реєстру запису про його припинення. Банк самостійно Центральним банком «ПриватБанку» по всіх філіях визначає свою організаційну структуру, встановлює чисельність працівників і штатний розпис, розробляє плани соціального розвитку трудового колективу.

В своїй діяльності Банк регулюється наступними нормативними документами:

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						11
Змн.	Арк.	№ докум.	Підпис	Дата		

- Закон України «Про банки і банківську діяльність»
- Закон України «Про цінні папери і фондову біржу»
- Закон України «Про власність»
- Закон України «Про господарські товариства»
- Цивільним Кодексом України
- іншими нормативними актами Верховної Ради, Президента України,

Кабінету Міністрів, НБУ, а також:

- Уставом КБ «ПриватБанк»
- Стратегічним планом Банку
- внутрішніми нормативними документами Банку

Статутний капітал (фонд) Банку складається з вартості вкладів учасників.

Відповідно до статутного капіталу визначається мінімальний розмір майна Банку, який гарантує інтереси їх кредиторів.

До складу системи «ПриватБанку» входять:

- головний офіс (ГО), розташований у м. Дніпропетровську;
- регіональні підрозділи (РП), розташовані в усіх регіонах України, а також

за її межами;

- дочірні банки - банк "Парітате" (м. Рига, Латвія)

На сьогоднішній день у банком відкрито 2819 відділень на території України, а саме в кожній області:

- Київська – 236 відділень;
- АР Крим – 174 відділень;
- Вінницька – 109 відділень;
- Волинська – 75 відділень;
- Дніпропетровська – 298 відділень;
- Донецька – 285 відділень;
- Житомирська – 85 відділень;
- Закарпатська – 72 відділень;
- Запорізька – 107 відділень;
- Івано-Франківська – 88 відділень;

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						12
Змн.	Арк.	№ докум.	Підпис	Дата		

- Кіровоградська – 76 відділень;
- Луганська – 96 відділень;
- Львівська – 129 відділень;
- Миколаївська – 69 відділень;
- Одеська – 154 відділень;
- Полтавська – 89 відділень;
- Рівненська – 72 відділень;
- Сумська – 79 відділень;
- Тернопільська – 60 відділень;
- Харківська – 117 відділень;
- Херсонська – 77 відділень;
- Хмельницька – 86 відділень;
- Черкаська – 92 відділень;
- Чернівецька – 54 відділень;
- Чернігівська – 56 відділень;

До складу системи «ПриватБанку» входять:

- головний офіс (ГО), розташований у м. Дніпропетровську;
- регіональні підрозділи (РП), розташовані в усіх регіонах України, а також за її межами;

1.2 Принципи та особливості інформаційної безпеки систем банківських установ

При активному використанні інформації глобальної мережі виникають проблеми, пов'язані з інформаційною безпекою. Її ключовими напрямками є захист комерційної інформації при її передачі по каналах зв'язку, надійність довгострокового зберігання даних в електронному вигляді, контроль доступу до інформації, в тому числі і через Інтернет, запобігання несанкціонованого доступу до інформації, ідентифікація її користувачів. Діяльності і процвітання будь-якого банку безпосередньо залежить від того з якою швидкістю здійснюється обмін інформацією усередині нього і на скільки добре побудована система безпеки.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						13
Змн.	Арк.	№ докум.	Підпис	Дата		

Якщо інфраструктура банку дає збої, то наслідки катастрофічні. Банк може втратити не тільки базу клієнтів, але і їхню довіру. Зіткнення з цією проблемою призвело до створення нових систем захисту інформації.

Заходи по захисту банківської інформації від несанкціонованого доступу повинні носити комплексний характер, тобто об'єднувати різноманітні заходи протидії загрозам (правові, організаційні, програмно-технічні). Одним із потужних засобів захисту банківської інформації є криптографічні методи захисту інформації.

Захист інформації банку включає в себе проведення цілого комплексу заходів - від аудиту інформаційної безпеки і до створення систем захисту підрозділів банку. Фахівці цієї галузі здатні створити як окремий модуль безпеки, так і повноцінну надійну централізовану систему захисту інформації.

При створенні системи захисту банку, фахівці враховують всіх можливих ситуацій витоку даних. Одним із способів захисту інформації банку є контроль проходження та реєстрації конфіденційної інформації. Усередині банку інформація проходить різними способами. Вона може передаватися в роздрукованому вигляді, а може і в електронному. Як правило, користувачі сприймають стіни будівлі як надійний захист, що є одним з найпоширеніших помилок.

Для захисту даних банку використовують системи ідентифікації, що визначають наявність прав доступу до інформації. Для цього використовують систему паролів для входу в локальну мережу банку. Вони можуть бути обрані користувачем, згенеровані системою або присвоюватися йому адміністратором з безпеки. Існують також пластикові картки доступу з чіпом.

Забезпечення безпеки є невід'ємною складовою частиною діяльності банку. Стан захищеності являє собою вміння і здатність надійно протистояти будь-яким спробам кримінальних структур або недобросовісних конкурентів завдати шкоди законним інтересам банку.

Концепція безпеки банківської системи визначає цілі та завдання системи безпеки, принципи її організації, функціонування та правові основи, види загроз

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						14
Змн.	Арк.	№ докум.	Підпис	Дата		

безпеки і ресурси, які підлягають захисту, а також основні напрямки розробки системи безпеки, включаючи правову, організаційну та інженерно-технічний захист.

Положення концепції можуть служити методичними рекомендаціями для керівників структур та служб безпеки при визначенні політики в галузі забезпечення безпеки.

Головною метою системи безпеки є забезпечення сталого функціонування банку і запобігання погроз його безпеки, захист законних інтересів від протиправних посягань, охорона життя та здоров'я персоналу, недопущення розкрадання фінансових і матеріально-технічних засобів, знищення майна і цінностей, розголошення, витоку і несанкціонованого доступу до службової інформації, порушення роботи технічних засобів забезпечення безпеки банківської інфраструктури

Завданнями та цілями системи безпеки є:

- Формування цілісного уявлення про систему безпеки банку і взаємозв'язок різних елементів цієї системи, визначення шляхів реалізації заходів, що забезпечують необхідний рівень надійної захищеності об'єктів;
- Підвищення іміджу банку та зростання прибутку за рахунок забезпечення високої якості надаваних послуг і гарантій безпеки майнових прав та інтересів.
- Прогнозування та своєчасне виявлення і усунення загроз безпеки персоналу та ресурсів банку; причин і умов, що сприяють нанесенню фінансового, матеріального і морального збитку, порушення його нормального функціонування та розвитку;
- Віднесення інформації до категорії обмеженого доступу (державної, службової, банківської та комерційної таємниць, іншої конфіденційної інформації, що підлягає захисту від неправомірного використання), а інших ресурсів - до різних рівнів небезпеки та підлягають збереженню;
- Створення механізму та умов оперативного реагування на загрози безпеці і прояв негативних тенденцій у функціонуванні банку; - ефективне припинення

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

загроз персоналу і зазіхань на ресурси на основі правових, організаційних та інженерно-технічних заходів і засобів забезпечення безпеки;

- Створення умов для максимально можливого відшкодування та локалізації завдається шкоди неправомірними діями фізичних та юридичних осіб, ослаблення негативного впливу наслідків порушення безпеки банку.

Організація і функціонування системи безпеки повинні відповідати таким принципам:

1. Принцип комплексності:

- Забезпечення безпеки персоналу, матеріальних і фінансових ресурсів від можливих загроз усіма доступними законними засобами, методами і заходами;
- Забезпечення безпеки інформаційних ресурсів протягом всього їх життєвого циклу, на всіх технологічних етапах їх обробки (перетворення) і використання, у всіх режимах функціонування;
- Здатність системи до розвитку і вдосконалення відповідно до змін умов функціонування банку.

Комплексність досягається:

- Забезпеченням відповідного режиму та охорони;
- Організацією спеціального діловодства з орієнтацією на захист банківських секретів;
- Заходами щодо добору і розстановки кадрів;
- Широким використанням технічних засобів безпеки та захисту інформації;
- Розгорнутої інформаційно-аналітичної та детективної діяльністю.

2. Принцип своєчасності

Своєчасність передбачає постановку завдань по комплексній безпеки на ранніх стадіях розробки системи безпеки на основі аналізу та прогнозування економічної обстановки, погроз безпеки, а також розробку ефективних заходів попередження посягань на законні інтереси банку.

3. Принцип безперервності

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						16
Змн.	Арк.	№ докум.	Підпис	Дата		

Вважається, що зловмисники тільки й шукають можливість, як би обійти захисні заходи, вдаючись для цього до легальним і нелегальним методам.

4. Принцип активності

Захищати інтереси банку необхідно з достатнім ступенем наполегливості, широко використовуючи маневр силами і засобами забезпечення безпеки і нестандартні заходи захисту.

5. Принцип законності

Принцип законності передбачає розробку системи безпеки на основі державного законодавства в галузі підприємницької діяльності, інформатизації і захисту інформації, приватної детективної діяльності та інших нормативних актів з безпеки, затверджених органами державного управління в межах їх компетенції, із застосуванням всіх дозволених методів виявлення і припинення правопорушень.

6. Принцип обґрунтування

Використовувані можливості і засоби безпеки мають бути реалізовані на сучасному рівні розвитку науки і техніки, обґрунтовані з точки зору заданого рівня безпеки та відповідати встановленим вимогам і нормам.

7. Принцип економічності

Мається на увазі економічна доцільність і порівнянність можливого збитку і витрат на забезпечення безпеки (критерій «ефективність - вартість»). У всіх випадках вартість системи безпеки повинна бути менше розміру можливого збитку від будь-яких видів загроз.

8. Принцип спеціалізації

Передбачається залучення до розробки та впровадження заходів і засобів захисту спеціалізованих організацій, найбільш підготовлених до конкретного виду діяльності із забезпечення безпеки, що мають досвід практичної роботи і державну ліцензію на право надання послуг у цій галузі. Експлуатація технічних засобів і реалізація заходів безпеки повинні здійснюватися професійно підготовленими фахівцями служби безпеки, а також функціональних і обслуговуючих підрозділів.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

9. Принцип взаємодії та координації

Означає здійснення заходів забезпечення безпеки на основі чіткого взаємозв'язку відповідних підрозділів і служб банку, сторонніх спеціалізованих організацій у цій галузі, координації їх зусиль для досягнення поставлених цілей, а також співробітництва із зацікавленими об'єднаннями та взаємодії з органами державного управління та прав охоронними органами.

10. Принцип вдосконалення

Передбачає вдосконалення заходів і засобів захисту на основі власного досвіду, появу нових технічних засобів з урахуванням змін в методах і засобах розвідки і промислового шпигунства, нормативно-технічних вимог, досягнутого вітчизняного та зарубіжного досвіду.

Вся комерційна інформація, що зберігається і оброблювана в кредитних організаціях, піддається самим різноманітним ризикам, пов'язаним з вірусами, виходом з ладу апаратного забезпечення, збоями операційних систем і т.п. Але ці проблеми не здатні завдати скільки-небудь серйозної шкоди. Щоденне резервне копіювання даних, без якого немислима робота інформаційної системи будь-якого підприємства, зводить ризик безповоротної втрати інформації до мінімуму. Крім того, добре розроблені і широко відомі способи захисту від перерахованих загроз. Тому на перший план виходять ризики, пов'язані з несанкціонованим доступом до конфіденційної інформації (НСД). поширені три способи крадіжки конфіденційної інформації. По-перше, фізичний доступ до місць її зберігання і обробки. Тут існує безліч варіантів. Наприклад, зловмисники можуть забратися в офіс банку вночі і вкрасти жорсткі диски з усіма базами даних. Можливий навіть озброєний наліт, метою якого є не гроші, а інформація. Не виключена ситуація, коли сам співробітник банку може винести носій інформації за межі території.

Банки традиційно приділяють дуже велику увагу фізичної безпеки операційних відділень, відділень зберігання цінностей і т.п. Все це знижує ризик несанкціонованого доступу до комерційної інформації шляхом фізичного доступу. Однак офіси банків і технічні приміщення, в яких розміщуються

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						18
Змн.	Арк.	№ докум.	Підпис	Дата		

сервери, за ступенем захисту зазвичай не відрізняються від офісів інших компаній.

На сьогодні існують продукти, покликані мінімізувати ризики, пов'язані з несанкціонованим доступом до резервних копій. Такі апаратні рішення забезпечують надійний захист системи, у тому числі і надійне шифрування інформації, і висока швидкість роботи. Однак володіють трьома істотними недоліками, які не дозволяють використовувати їх у банках. Перший: дуже висока вартість (десятки тисяч доларів). Другий: можливі проблеми з ввезенням в країну. Третій мінус полягає в неможливості підключити до них зовнішні сертифіковані криптопровайдери, а також можливість роботи тільки зі «своїм» ПЗ або накопичувачем.

Підбиваючи вище сказане, можна зробити висновок, що хоч і проблема функціонування системи безпеки банківських установ і стоїть на досить високому рівні, на сьогоднішній день у світі існують досить немало загроз, пов'язаних з несанкціонованим доступом до інформації.

В ідеальному випадку система інформаційної безпеки банку повинна бути єдиною. Тобто всі підсистеми повинні інтегруватися в існуючу інформаційну систему і, бажано, мати загальне управління. В іншому випадку неминучі підвищені трудовитрати на адміністрування захисту і збільшення ризиків через помилки в управлінні.

1.3 Аналіз захисту інформаційних мереж корпоративного банку

Перед передачею даних каналами зв'язку виникає необхідність попереднього перетворення їх. Для цього використовують додаткову інформацію, без якої її неможливо передати абоненту, та відновлення до початкового варіанту. Так створюють комп'ютерні мережі. Комп'ютерна мережа – це об'єднання фізичних та логічних незалежних систем в єдине середовище, в якому для передачі інформації від системи до системи вона проходить ланцюг певних перетворень. Незалежні системи, що входять до складу мережі, називають вузлами.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		

Головні проблеми організації захисту комп'ютерних мереж такі:

- розподілення ресурсів, які використовуються спільно (значно зростає ризик несанкціонованого доступу – в мережі його можна здійснити простіше і непомітніше);
- розширення зони контролю (інші держави);
- комбінація різних програмно-апаратних засобів;
- невідомий периметр мережі;
- множина точок атаки (модеми, лінії зв'язку);
- складність управління та контролю доступу до системи (з віддалених точок).

Захист мереж, як і захист окремих систем, переслідує три мети: підтримка конфіденційності інформації, що передається та обробляється в мережі, цілісності та доступності ресурсів мережі. Як і для АСОІ, захист мережі має плануватися як єдиний комплекс заходів, що охоплюють всі особливості обробки інформації.

Проте слід враховувати, що кожен вузол мережі повинен мати індивідуальний захист залежно від функцій, які виконуються, і від можливостей мережі. При цьому захист окремого вузла має бути частиною загального захисту. На кожному вузлі потрібно організувати:

- контроль доступу до всіх файлів та інших наборів даних, доступних із локальної мережі та інших мереж;
- контроль процесів, активізованих з віддалених вузлів;
- контроль мережевого трафіка;
- ефективну ідентифікацію і автентифікацію користувачів, що отримують доступ до цього вузла мережі;
- контроль доступу до ресурсів локального вузла, доступного для використання користувачам мережі;
- контроль за розповсюдженням інформації у межах локальної та пов'язаних з нею інших мереж.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

Захист мережі як єдиної системи, передбачає заходи захисту кожного окремого вузла і функцій захисту протоколів цієї мережі. Програмне забезпечення мережі має входити до складу довірчої обчислювальної бази (ДОБ) вузла, в протилежному разі можливе порушення роботи мережі та її захисту в результаті заміни програм або даних. Тоді захист інформації в мережі здійснюватиме мережа ДОБ. Вона складається з ДОБ окремих вузлів, пов'язаних захисними протоколами.

Класифікація погроз, характерних для мереж (погрози нижчого рівня).

1. Пасивні погрози (порушення конфіденційності даних, що циркулюють у мережі):

- перегляд і (чи) запис даних, що передаються лініями зв'язку;
- перегляд повідомлень;
- аналіз трафіка.

2. Активні погрози (порушення цілісності або доступності ресурсів (компонентів) мережі):

- несанкціоноване використання пристроїв, що мають доступ до мережі для зміни окремих повідомлень;
- відмова служб передачі повідомлень – зловмисник може знищувати або затримувати окремі повідомлення чи потік повідомлень;
- “Маскарад” – зловмисник може присвоїти своєму вузлу чи ретранслятору чужий ідентифікатор і відправляти або отримувати повідомлення від чужого імені;
- впровадження мережових вірусів – передача по мережі тіла вірусу з його наступною активізацією користувачем віддаленого чи локального вузла;
- модифікація потоку повідомлень – зловмисник може вибірково знищувати, модифікувати, затримувати,
- перевпорядковувати та дублювати повідомлення, а також вставляти підроблені повідомлення.

До механізмів захисту відносять такі:

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		21

1. Механізми шифрування, які забезпечують конфіденційність даних, що передаються. Розрізняють два способи шифрування: каналний та кінцевий. У разі каналного шифрування захищається вся інформація, що передається каналами зв'язку, включаючи службову (для кожної пари вузлів є свій ключ). Кінцеве шифрування дає можливість забезпечувати конфіденційність даних, що передаються між двома об'єктами (захищеним у цьому разі буде тільки зміст повідомлення, вся службова інформація залишається відкритою).

2. Механізми цифрового підпису, які містять процедури закриття блоків даних та перевірки закритого блоку даних. Сформувати невідомий блок може тільки користувач, що має відповідний ключ.

3. Механізми контролю доступу. Здійснюють перевірку повноважень об'єкта мережі на доступ до ресурсів (відповідно до правил політики безпеки та механізмів, які їх реалізують).

4. Механізми забезпечення цілісності даних, що передаються. Цілісність забезпечується об'єктами, що передають і приймають. Виявлення змін може потягти за собою дії щодо відновлення даних.

5. Механізми автентифікації об'єктів мережі. Використовують паролі, перевірку характеристик об'єкта, криптографічні методи (аналогічні цифровим підписам).

6. Механізми заповнення тексту використовують для забезпечення захисту від аналізу трафіка.

7. Механізми керування маршрутами (в обхід небезпечних ділянок).

8. Механізми засвідчення (арбітр).

9. Виявлення і обробка подій (аналогічно до засобів контролю небезпечних подій).

10. Звіт щодо перевірки безпеки (аналогічно до перевірки з використанням системного журналу) на відповідність цій ПБ.

Захист має відповідати принципам організації мережі: якщо мережа централізована, то і захист повинен бути централізований, якщо мережа розподілена, то і захист повинен бути розподілений.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						22
Змн.	Арк.	№ докум.	Підпис	Дата		

Для централізованої обробки найкраще підходить топологія “зірка”; для розподіленої – “загальна шина”, що характеризується високою швидкістю передачі даних і порівняно швидким доступом до вузла.

Доступ до мережі за допомогою комутованих ліній зв’язку вважають потенційно найбільш небезпечним. Потрібно автентифікувати будь-який вхід через комутовані лінії зв’язку (парольний захист, перевірка за описом списку дозволених номерів). Є сенс використовувати цю методологію захищених АСОІ в тому разі, якщо витрати на реалізацію менші, ніж вартість інформації, що може бути втрачена. Найреальнішим об’єктом використання цієї методології є великі АСОІ чи АСОІ, що обробляють дорогу інформацію або розв’язують відповідальні задачі.

Висновки до першого розділу

В даному розділі було визначено загальну характеристику комерційного банку «ПриватБанк», визначено основну структуру банку, загальні положення на яких здійснюється його діяльність. Проведено аналіз принципів та особливостей інформаційної безпеки систем банківських установ. Також було проведено аналіз захисту інформаційних мереж корпоративного банку де визначено головні проблеми захисту електронних обчислювальних мереж, класифікацію загроз мережі та механізми захисту від даних загроз.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						23
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. РОЗРОБКА ПРОЕКТУ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ

2.1 Розробка проекту інформаційно-комунікаційної мережі

Отримавши у першому розділі необхідний матеріал стосовно побудови захищених інформаційно-комунікаційних мереж, варто перейти до безпосереднього проектування топології комп'ютерної мережі, чому і буде присвячений даний пункт розділу.

Так як в Центральному відділенні ПАТ КБ «ПриватБанк» є сервер, який контролює циркулювання інформації у всій мережі, до якої входять в тому числі і робочі станції операторів, банкомати та каси, то він буде виступати центральним вузлом в зіркоподібній топології (hub-маршрутизатором), яка є оптимальною для даного випадку.

Перевагами топології «зірка» є:

- підвищена стійкість мережі;
- легкість додавання/видалення нового комп'ютера в мережі, що є досить важливим, оскільки мережа банку постійно розширюється;
- простота діагностики і усунення неполадок (швидкість здійснення банківських операцій).

Проте є і деякі недоліки даної топології, такі як:

- підвищена витрата кабелю при прокладці мережі;
- необхідність придбання дорогого устаткування.

Але ці недоліки є незначними, оскільки рівень матеріальних затрат для організації, що представляє собою філію інтернаціонального банку досить незначні. Використовуючи топологію «зірка», досить легко здійснювати підключення всіх робочих станцій до глобальної мережі Internet.

Загальна схема мережі складається з 3-ох рівнів :

- рівень ядра;
- рівень розподілу;
- рівень доступу.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						24
Змн.	Арк.	№ докум.	Підпис	Дата		

Рівень ядра це мережа Інтернет до якої під'єднані маршрутизатори рівня розподілу, за допомогою високошвидкісних каналів зв'язку.

Рівень розподілу включає в себе 2821 маршрутизатор, які під'єднані до ядра мережі, маршрутизаторів мережі Інтернет. Рівень розподілу з'єднаний з комутаторами рівня доступу за допомогою звитої пари.

Рівень доступу представлений кінцевим устаткуванням користувачів та комутаційним обладнання, що забезпечує функціонування рівня. Особливістю з'єднань комутаційного обладнання є те, що для забезпечення бездоганного функціонування рівня використовуються лінії зв'язку GigabitEthernet на звитій парі. Кінцеві вузли, окрім серверів, під'єднані до комутаційного обладнання за допомогою ліній FastEthernet на звитій парі, останній в свою чергу під'єднані до мережі з використанням високопродуктивних ліній зв'язку Gigabit Ethernet на звитій парі.

Загальна топологія мережі представлена на рисунку 2.1.

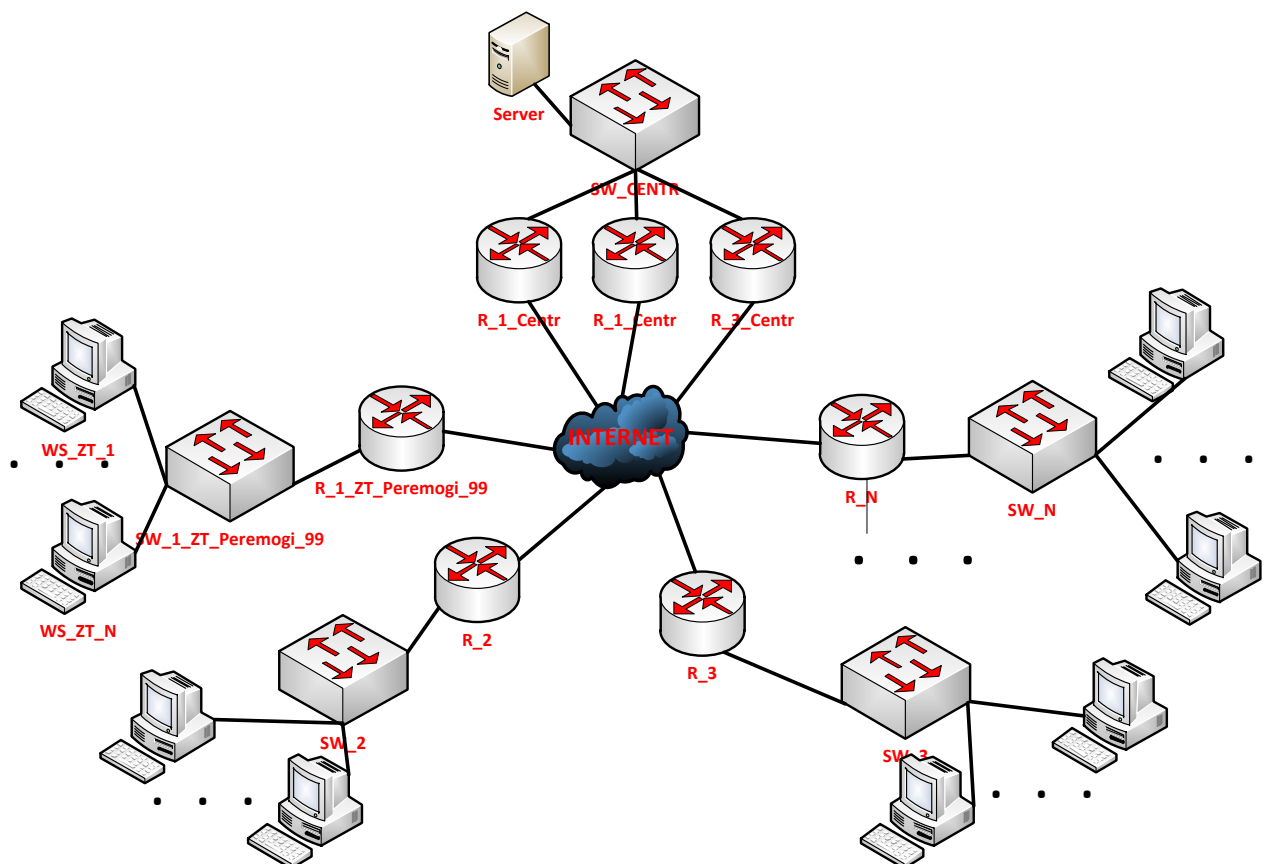


Рисунок 2.1 – Загальна топологія мережі

Умовні позначення:

- R_1_Centr – центральний маршрутизатор (hub), що розташований у Центральному офісі у місті Дніпропетровськ;
- R_2_Centr – центральний маршрутизатор для віддалених клієнтів, що розташований у Центральному офісі у місті Дніпропетровськ;
- R_3_Centr – центральний маршрутизатор для мережі банкоматів, що розташований у Центральному офісі у місті Дніпропетровськ;
- R_1_ZT_Peremogi_99 – маршрутизатор регіонального управління у місті Житомирі;
- R_X – маршрутизатори, що розташовані у регіональних відділеннях ПАТ КБ «ПриватБанк», X – номер внутрішньої мережі регіонального відділення;
- SW-X – комутатори, X – номер комутатора;
- WS – робочі станції операторів, X – номер внутрішньої мережі, Y – номер комутатора, Z – номер робочої станції.

При побудові мережі за основу було взято інформаційно-комунікаційну мережу банків ПАТ КБ «ПриватБанк». Тобто, було розроблено проект всієї банківської мережі, що умовно включає всі відділення та філії банку на території України та банкомати. Маршрутизатори мережі, що проектується, будуть з'єднуватися між собою через певне незахищене середовище, а саме мережу Інтернет. Умовно мережу Інтернет буде представляти маршрутизатор, за допомогою якого буде реалізовано обрану топологію інформаційно-комунікаційної мережі.

Підмережа головного офісу який знаходиться у місті Дніпропетровськ складається 456 робочих станцій під'єднаних до комутаторів за допомогою каналів зв'язку Fast Ethernet. В мережі використано 7 серверів, зокрема це:

- Сервери управління;
- Сервер Баз Даних;
- Веб сервер;
- Поштовий сервер;

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						26
Змн.	Арк.	№ докум.	Підпис	Дата		

- Файловий сервер;
- Процесингові сервери;

В мережі знаходиться 3 маршрутизатори кожен з яких викону певну роль. Перший маршрутизатор забезпечує з'єднання регіональних відділень банку з серверами. Другий маршрутизатор забезпечує з'єднання працівників які працюють віддалено або на домашніх комп'ютерах з серверами. Третій маршрутизатор забезпечує з'єднання банкоматів з процесинговим сервером. Всі сервери в даній мережі підключені до комутаторів з допомогою високошвидкісних каналів зв'язку Gigabit Ethernet що забезпечує високу швидкість передачі даних. Комутатори в даній мережі забезпечують з'єднання маршрутизаторів з серверами і робочими станціями, та з'єднані між собою по високошвидкісних каналах зв'язку Gigabit Ethernet. З'єднання робочих станцій користувачів забезпечується за допомогою каналів Fast Ethernet. Схема даної підмережі представлена на рисунку 2.2.

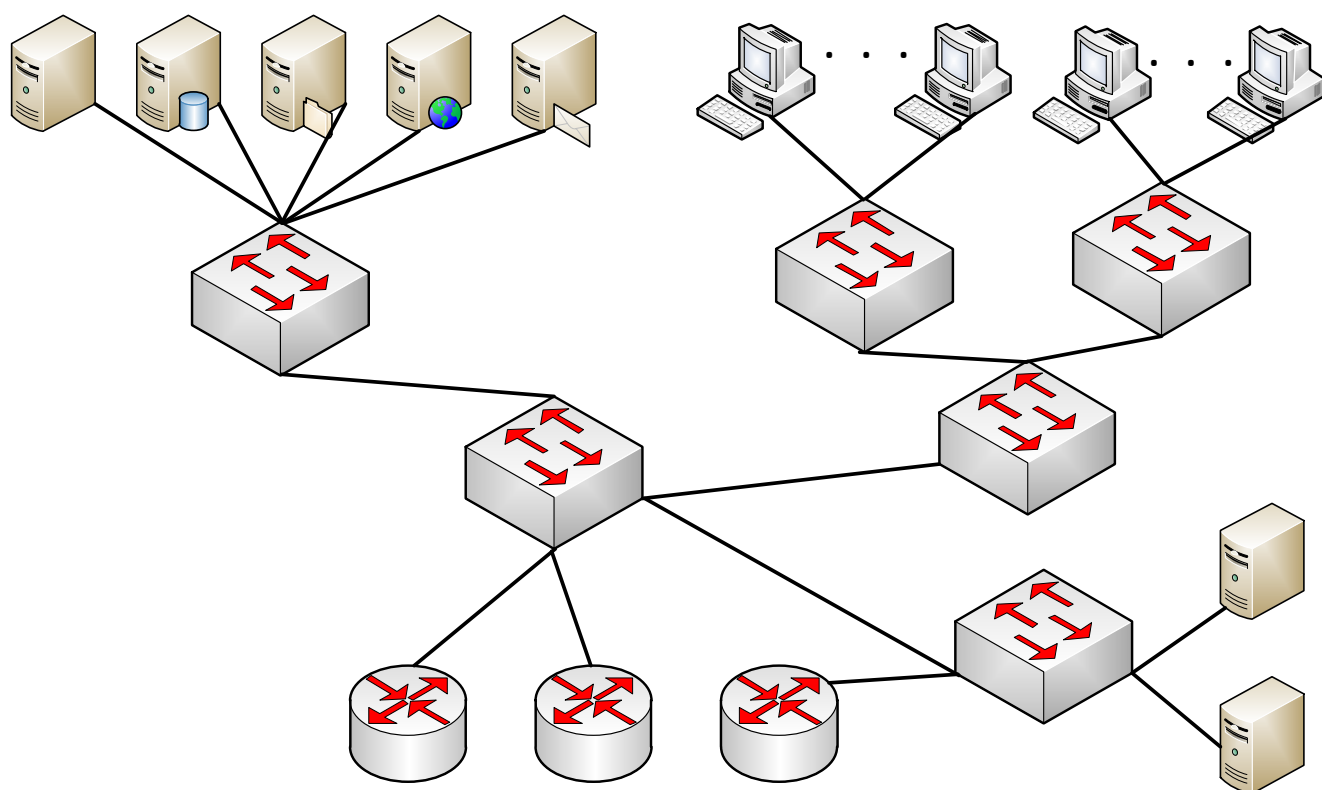


Рисунок 2.2 – Схема топології мережі головного управління ПриватБанку

Підмережа віддаленого регіонального управління ПАТ КБ «ПриватБанк» яке знаходиться у місті Житомирі складається з одного маршрутизатора який забезпечує підключення до головного управління банку. Кількість робочих станцій в даній мережі 89. В мережі використано 2 сервери, це сервер управління та баз даних. Кількість комутаторів в даній локальній мережі 5. Всі вони з'єднані між собою по високошвидкісних каналах зв'язку Gigabit Ethernet. Робочі станції в даній мережі під'єднані до комутаторів за допомогою каналів Fast Ethernet. Також в даній мережі використовуються IP – відеореєстратори спостереження та організована IP – телефонія. Головний комутатор який підключений до пограничного маршрутизатора з'єднує всі мережеві пристрої які використовуються. Він також виконує роль віртуальної локальної мережі, та забезпечує розподіл трафіку який циркулює в даній мережі між локальними підмережами.

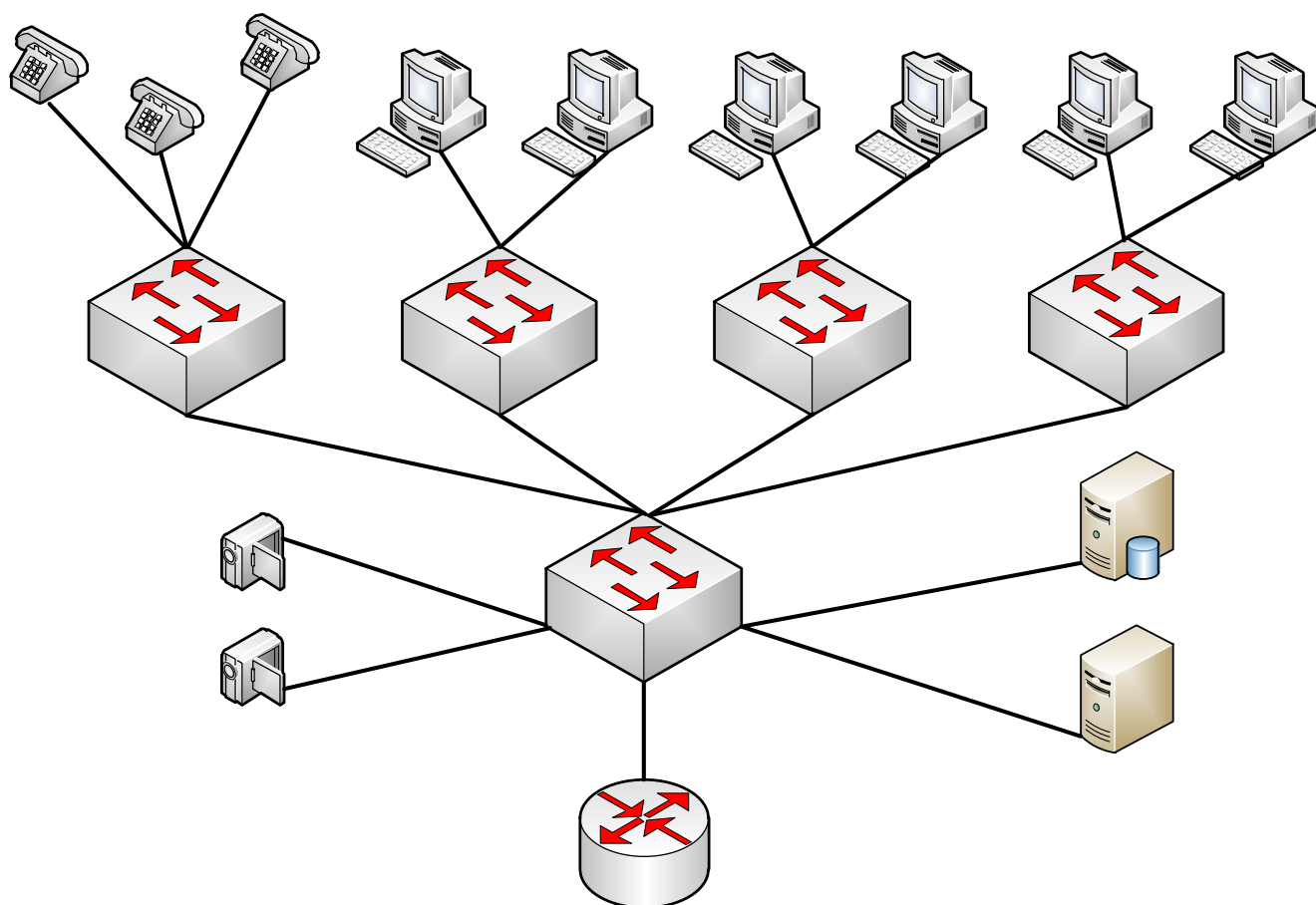


Рисунок 2.3 – Схема топології мережі Житомирського регіонального управління

Розробивши проект загальної фізичної топології мережі, де вказані всі фізичні з'єднання комунікаційного обладнання варто перейти до проектування логічної топології, оскільки логічна топологія вказує на зв'язки різних під мереж. Логічна топологія визначає характер розповсюдження інформації по комп'ютерній мережі.

В даному проекті захищеної інформаційно-комунікаційної мережі буде використовуватись частково повнозв'язкова топологія, так як зв'язок потрібно формувати між всіма під мережами але не між всіма віддаленим користувачами та банкоматами. Розроблена логічна топологія мережі представлена на рисунку 2.7.

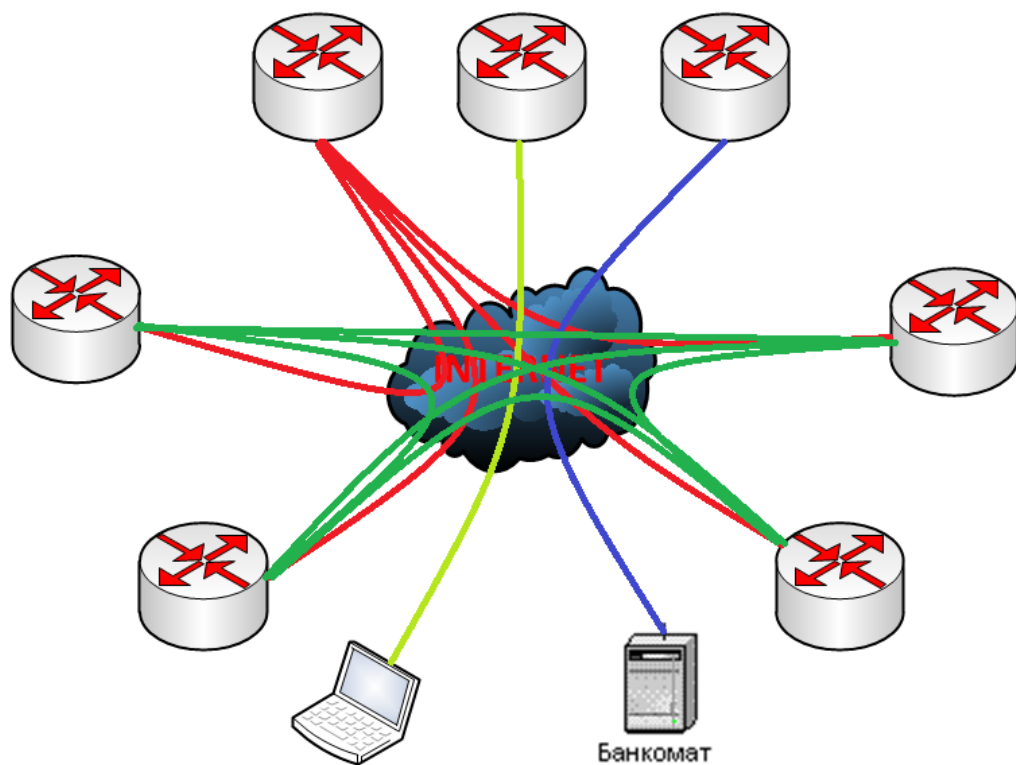


Рисунок 2.3 – Схема логічної топології мережі

На рисунку 2.3 показано всі логічні з'єднання під мереж. Червоним кольором показано статичні тунельні з'єднання між головним та віддаленими управліннями. Зеленим кольором показано динамічні з'єднання під мереж. Синім

та жовтим кольорами показано з'єднання віддалених користувачів та банкоматів з головним управлінням ПриватБанку.

Розробивши проект інформаційно-комунікаційної мережі де сформовано повне уявлення про мережу яка проектується, її фізичну та логічну топології перейдемо до наступного пункту кваліфікаційного проекту, а саме розрахунку адресації мережі, яка є обов'язковою при роботі будь-якої мережі.

2.2 Розробка проекту системи адресації інформаційно-комунікаційної мережі

На основі аналізу розробленої фізичної та логічної топології мережі проведемо розрахунок параметрів адресації яка буде застосована для роботи мережі.

Як вже зазначалося, за основу розрахунку адресації майбутньої мережі було взято інформаційно-комунікаційну мережу банку ПАТ КБ «ПриватБанк». Для розрахунку потрібно керуватися такими даними:

- кількість відділень банку в Україні: 2819;
- кількість робочих станцій в центральному офісі: = 456;
- кількість віддалених користувачів: ≈ 2015 ;
- кількість банкоматів: ≈ 8000 .

Відповідно до цих даних в мережу фактично буде входити 2819 маршрутизаторів (по одному на відділення). Розрахунку підлягають IP-адреси фізичних інтерфейсів маршрутизаторів зовнішньої мережі, IP-адреси фізичних інтерфейсів маршрутизаторів внутрішньої мережі та IP-адреси тунельних інтерфейсів маршрутизаторів для технології DMVPN.

Розрахуємо параметри адресації для мережі DMVPN.

Отже для даної мережі нам необхідно розрахувати $2819+8+1$ (адреса підмережі)+1(широкомовна адреса)+1(шлюз по замовчуванню) та дві адреси для маршрутизаторів, тобто 281 адрес.

Для початку переведемо це число в двійкову форму і визначимо кількість біт необхідних на адресацію вузлів:

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		

$$2819 = 101100000011 = 12 \text{ біт}$$

Тепер ми знаємо, що для адресації вузлів в підмережі нам необхідно 12 біт, тоді можна розрахувати маску підмережі, а саме визначимо кількість бітів маски $32 - 12 = 20$.

Маска підмережі: 11111111.11111111.11110000.00000000 = 255.255.240.0

Оберемо адресу мережі : 172.16.0.0 (10101100.00010000.00000000.00000000)

Максимальна адреса : 172.16.15.254 (10101100.00010000.00001111.11111110)

Мінімальна адреса : 172.16.0.1 (10101100.00010000.00000000.00000001)

Широкомовна адреса: 172.16.15.255 (10101100.00010000.00001111.11111111)

Шлюз по замовчуванню : 172.16.0.1 (10101100.00010000.00000000.00000001)

Розраховані значення для даної підмережі представлено у вигляді таблиці для зручності перегляду і користування.

Всі дані для розрахунку беруться виключно з спроектованої мережі, з кількості робочих станцій, кількості інтерфейсів які задіяні на маршрутизаторах та потребах ір – адресації комутаторів.

Таблиця 2.1

Розрахунок адресації тунельних інтерфейсів

Призначення	ІР-адреса
Адреса мережі	172.16.0.0
Маска мережі	255.255.240.0/2
Інвертована маска	0.0.15.255
Мінімальна адреса	172.16.0.1
Максимальна адреса	172.16.1.254
Широкомовна адреса	172.16.15.255
Шлюз по замовчуванню	172.16.0.1
Діапазон адрес вузлів	172.16.0.1 – 172.16.11.25
Діапазон вільних адрес	172.16.11.26 – 172.16.15.254

Для адресації віддалених користувачів нам потрібно 2015 адрес. Для даної мережі використаємо адресу 192.168.96.0. Розрахунок адресації наведено в таблиці 2.2.

Таблиця 2.2

Розрахунок адресації віддалених користувачів.

Призначення	IP-адреса
Адреса мережі	192.168.96.0
Маска мережі	255.255.248.0/21
Інвертована маска	0.0.7.255
Мінімальна адреса	192.168.96.1
Максимальна адреса	192.168.103.254
Широкомовна адреса	192.168.103.255
Шлюз по замовчуванню	192.168.96.254
Діапазон адрес вузлів	192.168.96.1 – 192.168.103.240
Діапазон вільних адрес	192.168.103.221 – 192.168.103.254

Для адресації банкоматів нам потрібно 8100 адрес. Для даної мережі використаємо адресу 200.168.0.0. Розрахунок адресації наведено в таблиці 2.3. Діапазон вільних адрес можна використовувати для розширення мережі.

Таблиця 2.3

Розрахунок адресації банкоматів

Призначення	IP-адреса
Адреса мережі	200.168.0.0
Маска мережі	255.255.224.0/19
Інвертована маска	0.0.31.255
Мінімальна адреса	200.168.0.1
Максимальна адреса	200.168.31.254
Широкомовна адреса	200.168.31.255

Діапазон адрес вузлів	200.168.0.1 – 192.168.31.162
Діапазон вільних адрес	200.168.31.163 – 200.168.31.254

Для адресації внутрішньої мережі головного управління нам потрібно 456 адрес. З них 7 адрес для серверів та 6 адрес для комутаторів оскільки в даній мережі використовується така кількість обладнання. Також потрібно 4 адреси для маршрутизаторів, одна з яких віртуальна а інші фізичні. Для даної мережі використаємо адресу 192.168.0.0. Розрахунок адресації наведено в таблиці 2.4.

Таблиця 2.4

Розрахунок адресації внутрішньої підмережі головного управління
ПриватБанку.

Призначення	ІР-адреса
Адреса мережі	192.168.0.0
Маска мережі	255.255.254.0/23
Інвертована маска	0.0.1.255
Мінімальна адреса	192.168.0.1
Максимальна адреса	192.168.1.254
Широкомовна адреса	192.168.1.255
Шлюз по замовчуванню	192.168.0.1
Діапазон адрес комутаторів	192.168.0.2 – 192.168.0.10
Діапазон адрес маршрутизаторів	192.168.0.1 – 192.168.0.4
Діапазон адрес вузлів	192.168.0.11 – 192.168.1.181
Діапазон вільних адрес	192.168.1.182 – 192.168.1.254

Для адресації внутрішньої мережі регіонального управління в місті Житомир нам потрібно 114 адрес. З них 89 адрес для робочих станцій, 2 адреси серверів мережі, 10 адрес для ІР – телефонів, 5 адрес комутаторів, 7 адрес для

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						33
Змн.	Арк.	№ докум.	Підпис	Дата		

IP – камер відеоспостереження та одна адреса для внутрішнього інтерфейсу маршрутизатора . Для даної мережі використовуємо адресу 192.168.2.0. Розрахунок адресації наведено в таблиці 2.4.

Таблиця 2.5

Розрахунок адресації внутрішньої підмережі №2 віддаленого офісу №3

Призначення	IP-адреса
Адреса мережі	192.168.2.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.168.2.1
Максимальна адреса	192.168.2.254
Широкомовна адреса	192.168.2.255
Шлюз по замовчуванню	192.168.2.1
Діапазон адрес комутаторів	192.168.2.4 – 192.168.2.8
Діапазон адрес серверів	192.168.2.2 – 192.168.2.3
Діапазон адрес IP - телефонів	192.168.2.99 – 192.168.2.108
Діапазон адрес відеокамер	192.168.2.108 – 192.168.2.114
Адреса маршрутизатора	192.168.2.1
Діапазон адрес вузлів	192.168.2.9 – 192.168.2.98
Діапазон вільних адрес	192.168.2.115 – 192.168.2.254

Отже, спроектувавши топологію мережі та розробивши схему адресації мережі, можна переходити до розробки підсистеми захисту даної мережі, що і буде детальніше розглянуто у наступному пункті розділу на підставах теоретичних відомостей, що були наведені у попередньому розділі.

2.3. Розробка підсистеми захисту інформаційно-комунікаційної мережі

Даний пункт кваліфікаційного проекту присвячений розробці підсистеми захисту інформаційно-комунікаційної мережі ПриватБанку, що розробляється. Для розробки та реалізації підсистеми захисту потрібно проаналізувати та вибрати технології які будуть забезпечувати ті чи інші вимоги захисту, та перш за все знати чи підтримують виробники обладнання ці функції. Перейдемо до аналізу та вибору технологій.

Для побудови захищеної інформаційно-комунікаційної мережі яка буде забезпечувати зв'язок віддалених регіональних управлінь ПриватБанку та головного управління банку будемо використовувати багатоточкову віртуальну приватну мережу DMVPN. Дана технологія відповідає усім вимогам до побудови банківських мереж. Нижче наведено короткий опис даної технології.

Дана технологія базується на наступних базових принципах:

- використання віртуальної підмережі на базі mGRE-інтерфейсів;
- шифрування GRE трафіку за допомогою IPsec;
- використання протоколу NHRP;
- використання протоколів динамічної маршрутизації.

Multipoint GRE (mGRE) тунель є альтернативою GRE-тунелів «точка-точка», який дозволяє зосередити на собі кілька GRE-тунелів. Тунель mGRE дозволяє одному GRE-інтерфейсу підтримувати кілька IPsec-тунелів і спрощує кількість і складність налаштувань, в порівнянні з GRE-тунелями «точка-точка».

Крім того, mGRE-інтерфейс дозволяє використовувати динамічно призначені IP-адреси на spoke-маршрутизаторах.

Основна мета побудови мережі на базі віртуальних інтерфейсів GRE – отримати можливість використовувати протоколи динамічної маршрутизації для поширення інформації про маршрути та здійснення відмовостійкості.

Шифрування GRE пакетів, що проходять, буде реалізовано за допомогою IPsec. Критерій шифрування – присутність GRE заголовка. Особливостями профілю IPSec при налаштуванні багатоточкової віртуальної приватної мережі наступні:

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						35
Змн.	Арк.	№ докум.	Підпис	Дата		

- застосовується на тунельному інтерфейсі;
- після застосування будь трафік, що виходить з тунельного інтерфейсу, ініціює створення IPsec-тунелю (немає необхідності використовувати ACL, як у звичайній crypto map);
- source і destination адреси тунельного інтерфейсу використовуються для створення IPsec-тунелю.

Використання багатоточкової віртуальної приватної мережі передбачає функціонування протоколу Next Hop Resolution Protocol (NHRP) – клієнт-серверного протоколу перетворення адрес, що дозволяє всім хостам, які знаходяться в NBMA (Non Broadcast Multiple Access)-мережі, динамічно вивчити NBMA-адреси (фізичні адреси) один одного звертаючись до next-hop-серверу (NHS). Після цього хости можуть обмінюватися інформацією один з одним безпосередньо.

У розроблюваній інформаційно-комунікаційній мережі DMVPN:

1. Hub-маршрутизатор зберігає та обслуговує базу даних NHRP, в якій зберігаються відповідності між фізичними адресами та адресами mGRE-тунелів spoke-маршрутизаторів.
2. Hub-маршрутизатор буде працювати як NHS, а spoke-маршрутизатори будуть клієнтами.
3. На кожному spoke-маршрутизаторі hub-маршрутизатор статично вказаний як NHS і задано відповідність між фізичною адресою та адресою mGRE-тунелю hub-маршрутизатора.
4. При включенні кожен spoke-маршрутизатор реєструється на NHS і, при необхідності, може вимагати у сервера інформацію про адреси інших spoke-маршрутизаторів для побудови spoke-to-spoke тунелів.

В результаті можна виділити наступні переваги технології DMVPN:

- простота і наочність налаштування;
- ефективна масштабованість;
- динамічна відмовостійкість і тонке управління маршрутизацією на базі протоколу динамічної маршрутизації;

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						36
Змн.	Арк.	№ докум.	Підпис	Дата		

- працездатність multicast;
- повноцінна повнозв'язкова топологія з точки зору передачі даних при помірному обсязі службового трафіку;
- spoke-маршрутизатори можуть знаходитися за NAT і мати динамічні IP адреси з private діапазону.

Використавши дану технологію можна не лише отримати надійний, ефективний та безпечний канал обміну інформацією, але і суттєво зменшити матеріальні затрати, зважаючи на масштаби існуючої та майбутньої банківської мережі на території України.

Для побудови захищеної мережі яка дозволить з'єднання віддалених користувачів з головним управлінням банку будемо використовувати технологію Cisco Easy VPN.

Технологія Cisco Easy VPN спрощує адміністрування і управління мережами VPN, які пов'язують різні вузли мережі між собою, за рахунок активного просування нових політик безпеки з головного вузла в мережі на віддалені майданчики. Для простоти конфігурації і високої масштабованості у вирішенні Easy VPN застосовується технологія «проштовхування політики» (політики-PUSH), але при цьому зберігається широкий спектр налаштувань і контроль над дотриманням політики. Сервер Easy VPN, сконфігурований в центральному офісі банку, передає політики безпеки на віддалені пристрої VPN, забезпечуючи реалізацію на таких з'єднаннях діючих політик ще до встановлення з'єднання. Переваги даної технології:

- Сервер Easy VPN і клієнт підтримується на маршрутизаторах з інтеграцією сервісів, VPN-концентраторах, міжмережних екранах Cisco PIX і багатофункціональних захисних пристроях Cisco ASA.

- Клієнтське програмне забезпечення Cisco VPN Client можна інсталиювати без додаткових витрат на комп'ютерах PC, Mac і в системах UNIX, для віддаленого доступу до VPN-маршрутизатора. Оскільки одна і та ж технологія (Easy VPN) використовується на апаратурі у клієнта (CPE) і програмному

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						37
Змн.	Арк.	№ докум.	Підпис	Дата		

забезпеченні, загальна вартість володіння знижується за рахунок спрощення та уніфікації в обслуговуванні, моніторингу і сервісів AAA.

- У Easy VPN передбачені опції локальної (на базі маршрутизаторів) і централізованої аутентифікації RADIUS. Аутентифікацію на базі стандарту 802.1x також можна використовувати для аутентифікації хостів в кожному місцезнаходженні CPE.

- Easy VPN пропонує цифрові сертифікати, підвищуючи рівень безпеки в порівнянні з попередніх ключів.

- Балансування навантаження для декількох знаходяться на центральному майданчику концентраторів Easy VPN автоматично розподіляє навантаження між декількома серверами Easy VPN. Примусова передача політик з резервних концентраторів на CPE дозволяє компаніям масштабувати рішення без переконфігурації CPE.

- Easy VPN пропонує повнофункціональну інтеграцію, включаючи динамічне призначення політики QoS, міжмережеві екрани і IPS, роздільне тунелювання і Cisco Service Assurance і агент NetFlow для моніторингу.

- Cisco SDM дає можливість на базі майстер-програми швидко розгорнути Easy VPN спільно з сервісами AAA і брандмауера, а також можливість графічного моніторингу віддалених клієнтів Easy VPN в реальному часі.

Для побудови мережі банкоматів будемо використовувати протокол PPTP. PPTP (англ. Point-to-Point Tunneling Protocol) — тунельний протокол типу точка-точка, що дозволяє комп'ютеру встановлювати захищене з'єднання з сервером за рахунок створення спеціального тунелю в стандартній, незахищеній мережі. PPTP поміщає (інкапсулює) кадри PPP в IP-пакети для передачі по глобальній IP-мережі, наприклад інтернет. PPTP може також використовуватися для організації тунелю між двома локальними мережами. PPTP використовує додаткове TCP- з'єднання для обслуговування тунелю. Шифрування трафіку здійснюється за допомогою протоколу MSCHAP-v2.

Крім основних технологій які будуть використовуватись для побудови захищеної інформаційно-комунікаційної мережі ПриватБанку, потрібно

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						38
Змн.	Арк.	№ докум.	Підпис	Дата		

звернути увагу на інші можливості та засоби захисту мережі, та використати усі максимальні можливості для захисту даних в інформаційній системі.

На основі проаналізованих технологій та засобів захисту проектує підсистема захисту буде включати в себе наступні заходи:

- Технологія DMVPN з шифруванням трафіку за допомогою протоколу IPSEC;
- Технологія Remote Access VPN для забезпечення зв'язку віддалених користувачів до головного управління ПриватБанку.
- Технологія PPTP для забезпечення роботи мережі банкоматів.
- Парольний доступ до будь-якого пристрою
- Протокол SSH для віддаленого управління який підтримує шифрування;
- Для шифрування трафіку, будемо використовувати протокол IPSEC з алгоритмами шифрування 3DES та хеш-функцією MD5;
- Використання стандартних та розширених списків доступу;
- Технологія NAT типу маскування;
- Протокол VRRP для забезпечення вімовостійкості.
- На комутаторах будуть використовуватись VLAN віртуальні локальні мережі та технологія PortSecurity.
- Для забезпечення моніторингу та стану мережевих пристроїв буде використовуватись програма моніторингу KiwiSyslog.

Розглянувши усі мінімально необхідні конфігурування стосовно налаштувань підсистеми захисту інформаційно-комунікаційної мережі буде доцільним перейти до наступного розділу, де усі вищезгадані заходи будуть безпосередньо реалізовані.

Висновки до другого розділу

В даному розділі було проаналізовано вибір топології мережі яка проектується, наведено основні її переваги та недоліки. Розроблено проект загальної топології всієї мережі та підмереж як головного управління

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						39
Змн.	Арк.	№ докум.	Підпис	Дата		

ПриватБанку так і віддалених регіональних управлінь, також було розроблено проект логічної топології мережі. В результаті розробки топології було спроектовано систему адресації з розрахунком всіх параметрів адресації мережевих пристроїв. Було розроблено підсистему захисту мережі, де проаналізовано технології які будуть використовуватись в проекті захищеної інформаційно-комунікаційної мережі, наведено їх переваги та недоліки.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						40
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. ОБГРУНТУВАННЯ ВИБОРУ ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ МЕРЕЖІ

3.1 Обґрунтування вибору апаратного та програмного забезпечення

3.1.1. Обґрунтування вибору маршрутизаторів

Вибір мережевого обладнання та програмного забезпечення маршрутизатора, який задіяно у проекті інформаційно-комунікаційної мережі ПриватБанку. У даному проекті комп'ютерної мережі використано маршрутизатор серії Cisco 3745 (платформа 3700). Нижче наведено деякі відомості про такі роутери та їх технічні характеристики.

Завдяки вбудованим інтерфейсам для підключення до локальним/розподіленим мережам, новим сервісним модулям високої щільності і можливості використання різних сучасних модулів інтеграції 41нтерфейсних маршрутизатори доступу серії Cisco 3700 пропонують філіям новий рівень щільності підключень в компактному форм-факторі. Використання мережевих модулів Etherswitch (на 16 або 36 портів) перетворює маршрутизатор серії Cisco 3700 в єдину інтегровану платформу, що поєднує гнучкі можливості маршрутизації і комутовані порти низької щільності. Крім того, маршрутизатор дозволяє забезпечити живлення пристроїв через порти Ethernetswitch і працювати універсальним голосовим і ір-телефонним шлюзом, забезпечуючи гнучкий, поступовий і масштабований перехід до конвергентних мереж. Використання єдиної платформи допомагає понизити загальну вартість володіння, спрощуючи вчення персоналу, розгортання і управління, а можливість модульної модернізації – захистити інвестиції у мережеве устаткування. Маршрутизатори серії Cisco 3700 є фундаментом, на якому будується архітектура Cisco AVVID (архітектура мереж для передачі голосу, відео і інтегрованих даних). Вони підтримують широкий спектр функцій програмного забезпечення Cisco IOS, включаючи механізми забезпечення високої доступності, функції управління якістю обслуговування і функції

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		41

безпеки, що дозволяють досягти потрібного рівня для філій. Окрім всіх цих функцій, маршрутизатори серії Cisco 3700 пропонують філіям гнучку консолідацію послуг і додатків – оптимальну платформу для інтеграції майбутніх послуг.

Основні можливості Cisco 3700:

1. Підтримка повного спектру функцій ПО Cisco IOS™;
2. Інтеграція голосу і даних;
3. Модульна архітектура;
4. Підтримка модулів високої щільності (HDSM, High Density Service Module);
5. Вбудовані порти Fast Ethernet 10/100;
6. Щонайширший спектр функцій в рамках одного пристрою;
7. Простий і гнучкий метод заміни програмного забезпечення з використанням зовнішньої flash-пам'яті, при цьому доступні ємкості до 128 Мб;
8. Підтримка подачі живлення для портів Inline Power від інтегрованого блоку живлення;
9. У маршрутизаторах серії Cisco 3700 використовуються модулі, загальні для серій Cisco 1700, 2600, 3600 і 3700;
10. Резервування інтегрованого блоку живлення (лише для Cisco 3745);
11. «Гаряча» заміна (OIR) модулів NM і резервного блоку живлення (лише для Cisco 3745);
12. Можливість установки сервісних модулів AIM і заміни процесорного модуля без витягання шасі з монтажною стійки (лише Cisco 3745).

Маршрутизатор Cisco 3745 стандартно включає 2 порти 10/100base-tx, 4 слоти для мережевого модуля NM, три слоти для WAN 42нтерфейс них модулів (WIC), і два слоти AIM. У стандартну комплектацію входять: шасі Cisco 3745, Cisco 3745-2fe-i/o, 256mb Dram, 32mb Compact Flash, 1 блок живлення. [8]
Зображення даної моделі роутера наведено на рис.3.1. Інші детальні характеристики маршрутизатора Cisco 3745 наведено у додатку А.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						42
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.1 – Маршрутизатор Cisco 3745

3.1.2. Обґунтування вибору комутаторів

Основним критерієм вибору моделей комутаторів є кількість портів. Також враховується швидкість передачі цих портів можливості управління та налаштування. Для даної мережі було обрано комутатори серії Cisco Small Business (рис 3.2), тому що, вони забезпечують усі вимоги до спроектованої мережі.



Рисунок 3.2 - Комутатори Cisco Small Business

Комутатори даної серії пропонують ряд функціональних можливостей, у тому числі:

- Гнучкість: різна кількість портів і комбінацій швидкості дає Вам змогу вибрати модель, яка найкраще відповідає Вашим потребам і фінансовим можливостям. Незалежно від свого розміру, всі керовані комутатори Cisco мають виняткові функціональні можливості.

- Безпека: удосконалені засоби безпеки захищають мережу та дані, надаючи доступ лише санкціонованим користувачам.

– Надійність: Керовані комутатори мають низку систем для забезпечення якості та резервування, які допомагають максимально збільшити час перебування мережі в робочому стані. Ваш бізнес може розвиватися без незручностей уривчастого зв'язку або невчасних проблем із мережею.

– Можливість розширення: Керовані комутатори Cisco підтримують низку протоколів якості та живлення.

Керовані комутатори Cisco для підприємств малого бізнесу - це:

– Кілька різних варіантів кількості портів Fast Ethernet та Gigabit Ethernet

– Підтримка засобів покращення якості послуг, які забезпечують виконання критично важливих мережевих задач у режимі реального часу на найвищому рівні ефективності

– Досконалі функції захисту, які гарантують відсутність несанкціонованого доступу до мережі; зокрема, аутентифікація 802.1X та фільтрування MAC-адрес

– Живлення через кабель Ethernet (Power over Ethernet, PoE) економічно ефективно забезпечує енергією точки бездротового доступу, відеокамери та інші підключені до мережі кінцеві пристрої, виключаючи потребу в установленні окремих джерел живлення (опція).

– Ефективне розширення через систему кластерів дає змогу при потребі додавати нові комутатори відповідно до зростання бізнесу, забезпечуючи керування кількома комутаторами через один спільний інтерфейс.

– Підтримка віртуальних локальних мереж (VLAN) дає змогу розподілити користувачів по різних мережах, підвищуючи їхню продуктивність праці зокрема та безпеку всієї системи загалом.

– Системи резервування забезпечують постійне функціонування критично важливих програм.

В даному проекті було обрано комутатори наступних моделей:

1. В якості 16-портових комутаторів модель Cisco SRW2016 16-port Gigabit Switch.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						44
Змн.	Арк.	№ докум.	Підпис	Дата		

2. В якості 48-портових комутаторів модель Cisco SFE2010P 48-port 10/100 Ethernet Switch - PoE.

Технічні характеристики комутаторів наведені в додатку А.

3.1.3. Обґрунтування вибору програмного забезпечення

Даний підпункт пункту про вибір мережевого обладнання та програмного забезпечення присвячений обґрунтуванню вибору програмного забезпечення, а саме – вірсій та образів програмного забезпечення, яке буде використовуватись для роботи мережі.

Для маршрутизаторів фірми Cisco використовуватись буде операційна система Cisco IOS так як продукти даної фірми працюють тільки з нею. Операційна система IOS (Internetworking Operating System – операційна система міжмережевої взаємодії), під управлінням якої працюють маршрутизатори і комутатори Cisco, – одне з кращих мережевих системних програмних засобів у світі. Ця система підтримує функціонування Інтернету, забезпечуючи приблизно 80 відсотків веб-трафіку. До того ж саме завдяки IOS маршрутизатори Cisco стали бестселером ринку інформаційних та комунікаційних технологій.

Вихід на ринок Cisco IOS повністю змінив звичні методи роботи інформаційно-технологічних і мережевих організацій. Випустивши IOS, компанія Cisco надала єдине рішення для безлічі різномірних пристроїв.

Програмне забезпечення Cisco IOS гарантує взаємодію маршрутизаторів, комутаторів і концентраторів Cisco як в рамках одного офісу так і в рамках розподіленої системи для спрощення встановлення та обслуговування. Cisco IOS також забезпечує збереження інвестицій за рахунок інтеграції всіх мережевих платформ і стандартів локальних і глобальних мереж і дозволяє використовувати обладнання компанії Cisco спільно з устаткуванням інших виробників. Cisco IOS також забезпечує економічний перехід до нових технологій для існуючої мережевої інфраструктури, забезпечуючи збереження зроблених раніше інвестицій. Cisco IOS забезпечує весь спектр можливостей мережевого управління, розроблених для сучасних розподілених мереж.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						45
Змн.	Арк.	№ докум.	Підпис	Дата		

Стосовно образу маршрутизатора Cisco. В даному проекті обрано образ IOS c3745-adventerprisek9-mz.124-25. Такий образ працює безвідмовно у переважній більшості мереж, є зручним та якісним. До того ж передбачає можливість конфігурування маршрутизатора додатковими засобами захисту при налаштуванні тощо.

Отже, після того, як було обрано і описано апаратне та програмне забезпечення, що використовується у інформаційно-комунікаційній мережі, що розробляється, варто перейти безпосередньо до налаштувань комп'ютерної мережі, що і буде детальніше розглянуто в наступному пункті.

3.2 Базове налагодження апаратного та програмного забезпечення та підсистеми захисту

У середовищі програмного емулятора GNS3 засобами візуального проектування було створено проект мережі ПриватБанку на базі обладнання Cisco. Для емуляції маршрутизаторів Cisco було використано образ c3745-adventerprisek9-mz.124-25.

Базове налагодження захищеної інформаційно-комунікаційної мережі буде складатися з:

- налаштування інтерфейсів маршрутизаторів;
- налаштування маршрутизації мережі;
- налаштування IP-адресації робочих станцій.

У якості протоколу маршрутизації було обрано пропорієнтарний протокол фірми Cisco EIGRP. Для прикладу нижче наведено приклад базового налагодження для маршрутизатора ZT_PERENOGI_99:

```
ZT_PERENOGI_99(config)# interface FastEthernet0/0
ZT_PERENOGI_99(config-if)# description Internet
ZT_PERENOGI_99(config-if)#ip address 12.93.10.2 255.255.255.0
ZT_PERENOGI_99(config-if)#exit
ZT_PERENOGI_99(config)#interface FastEthernet0/1
ZT_PERENOGI_99(config-if)#description LAN
```

```

ZT_PERENOGI_99(config-if)# ip address 192.168.2.1 255.255.255.0
ZT_PERENOGI_99(config-if)#ip nat inside
ZT_PERENOGI_99(config-if)#exit
ZT_PERENOGI_99(config)ip route 0.0.0.0 0.0.0.0 12.93.10.1
ZT_PERENOGI_99(config)router eigrp 1
ZT_PERENOGI_99(config-router)net 192.168.2.0
ZT_PERENOGI_99(config-router)net 172.16.0.0
ZT_PERENOGI_99(config-router)no auto-summary
ZT_PERENOGI_99(config-router)exit
ZT_PERENOGI_99(config)username admin password cisco
ZT_PERENOGI_99(config)ip domain-name Peremogi_99.ua
ZT_PERENOGI_99(config)crypto key generate rsa
ZT_PERENOGI_99(config)line vty 0
ZT_PERENOGI_99(config-line)login local
ZT_PERENOGI_99(config-line)exit
ZT_PERENOGI_99(config)line console 0
ZT_PERENOGI_99(config-line)login local
ZT_PERENOGI_99(config-line)exit
ZT_PERENOGI_99(config)ip access-list extended NAT
ZT_PERENOGI_99(config-ext-nacl)permit ip 192.168.2.0 0.0.0.255 any
ZT_PERENOGI_99(config-ext-nacl)exit
ZT_PERENOGI_99(config)ip nat inside source list NAT interface f0/0 overload

```

Аналогічні налаштування проводяться і на інших маршрутизаторах мережі, їх повні файли конфігурації знаходяться в додатку Б.

Наступним завданням є створення шифрованої віртуальної приватної мережі між головним управлінням ПриватБанку та регіональними управліннями. Більш детально цей етап розглянуто нижче.

Як вже зазначалося, для зв'язку відділень банку з головним управлінням буде використовуватись технологія DMVPN. Перейдемо до налаштувань.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						47
Змн.	Арк.	№ докум.	Підпис	Дата		

Спочатку налаштуємо протокол IPSec. Так як налаштування протоколу IPSec на всіх маршрутизаторах ідентичні, то розглянемо команди даних налаштувань на прикладі маршрутизатора віддаленого регіонального управління ПриватБанку *ZT_PERENOGI_99*.

ZT_PERENOGI_99(config)#crypto isakmp policy 10 – створення політики isakmp.

ZT_PERENOGI_99(config)#encryption 3des – вказується, що в якості алгоритму шифрування використовується 3des.

ZT_PERENOGI_99(config)#hash md5 – вказується, що в якості хеш-алгоритму використовується алгоритм MD5.

ZT_PERENOGI_99(config)#authentication pre-share – команда для вказівки, що аутентифікація повинна виконуватися по попередньо встановлених ключах.

ZT_PERENOGI_99(config)#group 2 – встановлення групи Diffie-Hellman, що буде використовуватися в межах протоколу IKE, рівної 1024 біт.

ZT_PERENOGI_99(config)#crypto isakmp key privatbn address 0.0.0.0 0.0.0.0 no-auth – команда, що вказує шаблонну адресу при налаштуванні pre-share key.

ZT_PERENOGI_99(config)#crypto ipsec transform-set PrivatBank esp-3des esp-md5-hmac – формування 2 наборів перетворень (комбінацій протоколів захисту та криптографічних алгоритмів) esp-3des (протокол ESP з алгоритмом 3des) та esp-md5-hmac (протокол ESP з алгоритмом аутентифікації MD5).

ZT_PERENOGI_99(config)#crypto ipsec profile PrivatBankProf – створення IPSec-профілю.

ZT_PERENOGI_99(config-profile)#set transform-set PrivatBank – призначення сформованих наборів перетворень даному IPSec-профілю.

Переходимо до налаштування mGRE-тунелів. На центральному маршрутизаторі та на spoke-маршрутизаторах mGRE-тунелі налаштовуються аналогічно, тому далі наведено основні команди налаштування та їх коментар на прикладі маршрутизатора *ZT_PERENOGI_99*.

ZT_PERENOGI_99 (config)#int tunnel 1 – створення тунельного інтерфейсу.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						48
Змн.	Арк.	№ докум.	Підпис	Дата		

ZT_PERENOGI_99(config-if)#ip address 172.16.0.1 255.255.240.0 – призначення IP-адреси інтерфейсу.

ZT_PERENOGI_99(config-if)#ip mtu 1400 – збільшення значення MTU до 1400, так як GRE додає додаткові заголовки до IP-пакету.

ZT_PERENOGI_99(config-if)#tunnel source 12.93.10.2 – налаштування початку тунелю.

ZT_PERENOGI_99(config-if)#tunnel mode gre multipoint – включення mGRE тунелю.

ZT_PERENOGI_99(config-if)#tunnel key 100 – задання ключа, який ідентифікує тунель.

Налаштування протоколу NHRP на hub-маршрутизаторі та на spoke-маршрутизаторах мають певні відмінності між собою. Спочатку розглянемо команди налагодження NHRP на прикладі *Dnipropetrovsk_R1* (hub-маршрутизатора).

Dnipropetrovsk_R1(config)#int tunnel 1 – перехід на тунельний інтерфейс.

Dnipropetrovsk_R1(config-if)#ip nhrp network-id 100 – увімкнення протоколу NHRP шляхом призначення унікального ідентифікатора мережі.

Dnipropetrovsk_R1(config-if)#ip nhrp map multicast dynamic – налаштування автоматичного додавання відповідностей між адресами spoke-маршрутизаторів.

Dnipropetrovsk_R1(config-if)#ip nhrp authentication 100 – налагодження аутентифікації.

Далі, на прикладі маршрутизатора *ZT_PERENOGI_99*, наведемо команди налаштування протоколу NHRP на spoke-маршрутизаторі.

ZT_PERENOGI_99 (config)#int tunnel 1 – перехід на тунельний інтерфейс.

ZT_PERENOGI_99 (config-if)#ip nhrp network-id 1 – увімкнення протоколу NHRP шляхом призначення унікального ідентифікатора мережі. Вказується той самий ідентифікатор, що і на hub-маршрутизаторі.

ZT_PERENOGI_99 (config-if)#ip nhrp map multicast dynamic – налаштування динамічної побудови карти відповідностей між адресами spoke-маршрутизаторів.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						49
Змн.	Арк.	№ докум.	Підпис	Дата		

ZT_PERENOGI_99 (config-if)# ip nhrp map 172.16.0.1 10.93.10.2 – налагодження статичної відповідності між адресою mGRE-тунелю і фізичною адресою hub-маршрутизатора (перша адреса – адреса тунельного інтерфейсу, друга – адреса зовнішнього фізичного інтерфейсу).

ZT_PERENOGI_99(config-if)#ip nhrp map multicast 10.93.10.2 – адреса зовнішнього фізичного інтерфейсу hub-маршрутизатора вказується як одержувач multicast-пакетів від локального маршрутизатора.

ZT_PERENOGI_99(config-if)#ip nhrp nhs 172.16.0.1 – адреса тунельного інтерфейсу hub-маршрутизатора вказується як next-hop-сервер.

Тепер потрібно налаштувати технологію Remote Access VPN для забезпечення зв'язку віддалених користувачів з головним управлінням ПриватБанку. Приклад налаштувань наведено нижче.

Dnipropetrovsk_R2(config)#username privtabankuser password 0 privatpassword – створюємо користувача;

Dnipropetrovsk_R2(config)#crypto isakmp policy 10 – створення політики isakmp;

Dnipropetrovsk_R2(config-isakmp)#encr 3des – вибір алгоритму шифрування;

Dnipropetrovsk_R2(config-isakmp)#hash md5 – вибір алгоритму хешування;

Dnipropetrovsk_R2(config-isakmp)#authentication pre-share

Dnipropetrovsk_R2(config-isakmp)#group 2 – вибір групи Діффі-Хелмана;

Dnipropetrovsk_R2(config)#crypto isakmp client configuration group Privat-Bank-GROUP – створення групи для користувачів;

Dnipropetrovsk_R2(config-isakmp-group)#key PrivatCisco – вказання ключа для групи;

Dnipropetrovsk_R2(config-isakmp-group)#dns 192.168.0.200 – вказання адреси dns – сервера;

Dnipropetrovsk_R2(config-isakmp-group)#wins 192.168.0.200 - вказання адреси wins – сервера;

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		

Dnipropetrovsk_R2(config-isakmp-group)#domain PrivatBank.ua – вказання доменного імені;

Dnipropetrovsk_R2(config-isakmp-group)#pool VPN-POOL – вказання пулу адрес;

Dnipropetrovsk_R2(config-isakmp-group)#acl 110 – вказання списку доступу;

Dnipropetrovsk_R2(config-isakmp-group)#save password - збереження паролю;

Dnipropetrovsk_R2(config)#crypto isakmp profile VPN-CLIENT – створення профілю для шифрування;

Dnipropetrovsk_R2(config-isa-prof)#match identity group Privat-Bank-GROUP

Dnipropetrovsk_R2(config-isa-prof)#client authentication list USER-AUTH

Dnipropetrovsk_R2(config-isa-prof)#isakmp authorization list GROUP-AUTH

Dnipropetrovsk_R2(config-isa-prof)# client configuration address respond

Dnipropetrovsk_R2(config)#crypto ipsec transform-set EZVPN esp-aes esp-md5-hmac

Dnipropetrovsk_R2(config)#crypto dynamic-map DYNMAP 10

Dnipropetrovsk_R2(config-crypto-map)#set transform-set EZVPN

Dnipropetrovsk_R2(config-crypto-map)#set isakmp-profile VPN-CLIENT

Dnipropetrovsk_R2(config-crypto-map)#reverse-route

Dnipropetrovsk_R2(config)#crypto map DMAP 1 ipsec-isakmp dynamic DYNMAP

Dnipropetrovsk_R2(config)#interface FastEthernet0/0

Dnipropetrovsk_R2(config-if)#crypto map DMAP

Dnipropetrovsk_R2(config)#ip local pool VPN-POOL 192.168.96.1 192.168.103.254

Dnipropetrovsk_R2(config)#access-list 110 permit ip 192.168.96.0 0.0.7.255 any

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						51
Змн.	Арк.	№ докум.	Підпис	Дата		

Тепер потрібно налаштувати технологію PPTP для забезпечення роботи банкоматів ПриватБанку. Команди налаштувань наведені нижче:

```
Dnipropetrovsk_R3(config)#vpdn enable
Dnipropetrovsk_R3(config)#vpdn-group 1
Dnipropetrovsk_R3(config-vpdn)#Default PPTP VPDN group
Dnipropetrovsk_R3(config-vpdn)#accept-dialin
Dnipropetrovsk_R3(config-vpdn)#protocol pptp
Dnipropetrovsk_R3(config-vpdn)#virtual-template 1
Dnipropetrovsk_R3(config)#username privatuser password 0 123456
Dnipropetrovsk_R3(config)#interface Virtual-Template1
Dnipropetrovsk_R3(config-if)#ip unnumbered FastEthernet0/0
Dnipropetrovsk_R3(config-if)#peer default ip address pool test
Dnipropetrovsk_R3(config-if)#ppp encrypt mppe auto
Dnipropetrovsk_R3(config-if)#ppp authentication pap chap ms-chap
Dnipropetrovsk_R3(config)#ip local pool test 200.168.1.1 200.168.31.250
```

Підтвердження зроблених налаштувань показано в загальній конфігурації маршрутизаторів, що наведена в додатку Б.

Після того, як всі налаштування виконані, переходимо безпосередньо до перевірки правильності функціонування захищеної інформаційно-комунікаційної мережі.

3.3 Тестування роботи захищеної інформаційно-комунікаційної мережі

Проведемо тестування інформаційно-комунікаційної мережі та перевірку коректності роботи розробленої підсистеми захисту. Результати свідчитимуть про якість даних налаштувань. Для цього буде виконано ряд послідовних перевірок, що наведені нижче.

Спочатку перевіримо доступність мережі головного управління ПриватБанку з віддаленого регіонального управління яке знаходиться в місті Житомир.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		52

```

Администратор: Командная строка
C:\Users\Admin>ping 192.168.0.2

Обмен пакетами с 192.168.0.2 по 32 байтами данных:
Ответ от 192.168.0.2: число байт=32 время=191мс TTL=254
Ответ от 192.168.0.2: число байт=32 время=123мс TTL=254
Ответ от 192.168.0.2: число байт=32 время=139мс TTL=254
Ответ от 192.168.0.2: число байт=32 время=135мс TTL=254

Статистика Ping для 192.168.0.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 123мсек, Максимальное = 191 мсек, Среднее = 147 мсек

C:\Users\Admin>tracert 192.168.0.100

Трассировка маршрута к OFFICE-SERVER [192.168.0.100]
с максимальным числом прыжков 30:

  1    26 ms    18 ms    8 ms    192.168.2.1
  2   136 ms   85 ms   100 ms   172.16.0.1
  3   216 ms   85 ms   145 ms   OFFICE-SERVER [192.168.0.100]

Трассировка завершена.
C:\Users\Admin>_

```

Рисунок 3.3 – Перевірка доступності мережі головного управління ПриватБанку

Як видно з рисунку 3.3 мережева доступність присутня. Тепер перевіримо доступність віддалених відділень ПриватБанку з мережі головного управління.

```

Командная строка
C:\Documents and Settings\Администратор>ping 192.168.2.2

Обмен пакетами с 192.168.2.2 по 32 байт данных:

Ответ от 192.168.2.2: число байт=32 время=135мс TTL=126
Ответ от 192.168.2.2: число байт=32 время=95мс TTL=126
Ответ от 192.168.2.2: число байт=32 время=114мс TTL=126
Ответ от 192.168.2.2: число байт=32 время=129мс TTL=126

Статистика Ping для 192.168.2.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 95мсек, Максимальное = 135 мсек, Среднее = 118 мсек

C:\Documents and Settings\Администратор>ping 192.168.3.2

Обмен пакетами с 192.168.3.2 по 32 байт данных:

Ответ от 192.168.3.2: число байт=32 время=115мс TTL=126
Ответ от 192.168.3.2: число байт=32 время=128мс TTL=126
Ответ от 192.168.3.2: число байт=32 время=85мс TTL=126
Ответ от 192.168.3.2: число байт=32 время=97мс TTL=126

Статистика Ping для 192.168.3.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 85мсек, Максимальное = 128 мсек, Среднее = 106 мсек

C:\Documents and Settings\Администратор>ping 192.168.4.2

Обмен пакетами с 192.168.4.2 по 32 байт данных:

Ответ от 192.168.4.2: число байт=32 время=99мс TTL=126
Ответ от 192.168.4.2: число байт=32 время=145мс TTL=126
Ответ от 192.168.4.2: число байт=32 время=78мс TTL=126
Ответ от 192.168.4.2: число байт=32 время=114мс TTL=126

Статистика Ping для 192.168.4.2:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 78мсек, Максимальное = 145 мсек, Среднее = 109 мсек

C:\Documents and Settings\Администратор>ping 192.168.5.2

Обмен пакетами с 192.168.5.2 по 32 байт данных:

Ответ от 192.168.5.2: число байт=32 время=135мс TTL=126

```

Рисунок 3.4 – Перевірка доступності віддалених відділень

З рисунку наведеного вище видно, що доступ до віддалених мереж відділень присутній. Перевіримо таблицю маршрутизації маршрутизатора ZT_PEREMOGI_99.

```
ZT_PEREMOGI_99#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 12.93.10.1 to network 0.0.0.0

172.16.0.0/20 is subnetted, 1 subnets
C    172.16.0.0 is directly connected, Tunnel1
D    192.168.4.0/24 [90/322846976] via 172.16.0.5, 00:12:34, Tunnel1
D    192.168.5.0/24 [90/322846976] via 172.16.0.4, 00:12:34, Tunnel1
12.0.0.0/24 is subnetted, 1 subnets
C    12.93.10.0 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
D    192.168.3.0/24 [90/322846976] via 172.16.0.3, 00:12:34, Tunnel1
S*   0.0.0.0/0 [1/0] via 12.93.10.1
D    192.168.0.0/23 [90/310046976] via 172.16.0.1, 00:12:50, Tunnel1
ZT_PEREMOGI_99#
```

Рисунок 3.5 – Перегляд таблиці маршрутизації

З рисунку 3.5 видно, що в таблиці маршрутизації присутні записи з локальних підмереж віддалених відділень та мережі головного управління ПриватБанку. Це свідчить про те, що існує зв'язок між під мережами віддалених відділень банку, оскільки налаштована технологія DMVPN дозволяє формувати динамічні тунелі.

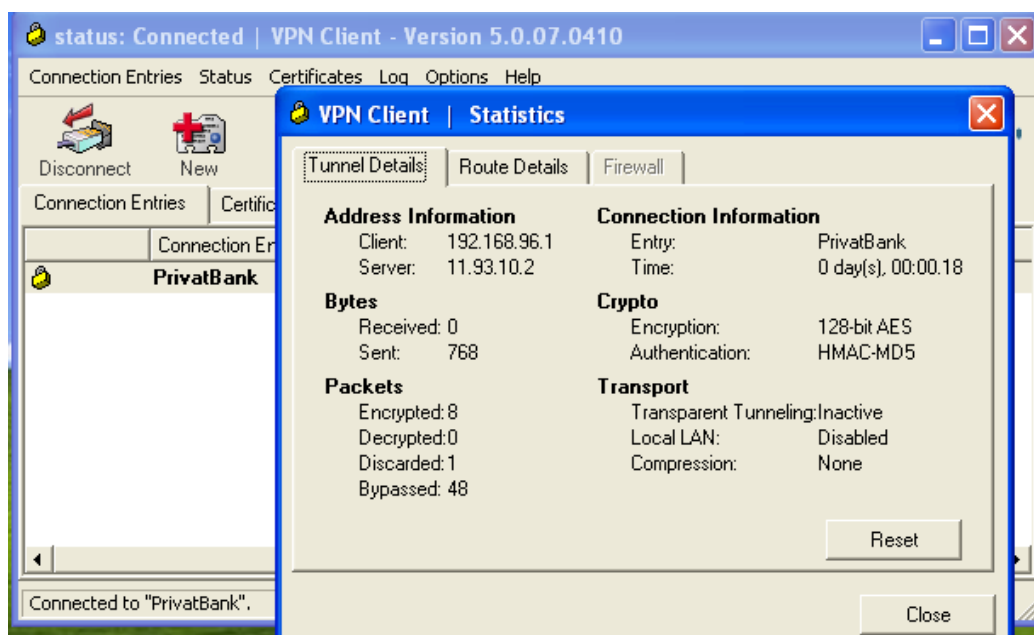


Рисунок 3.6 – Перегляд статистики підключення до VPN сервера

Перевіримо роботу технології Remote Acces VPN яка забезпечує зв'язок віддалених користувачів які працюють вдома через комп'ютер або смартфон (рис.3.6 – 3.7).

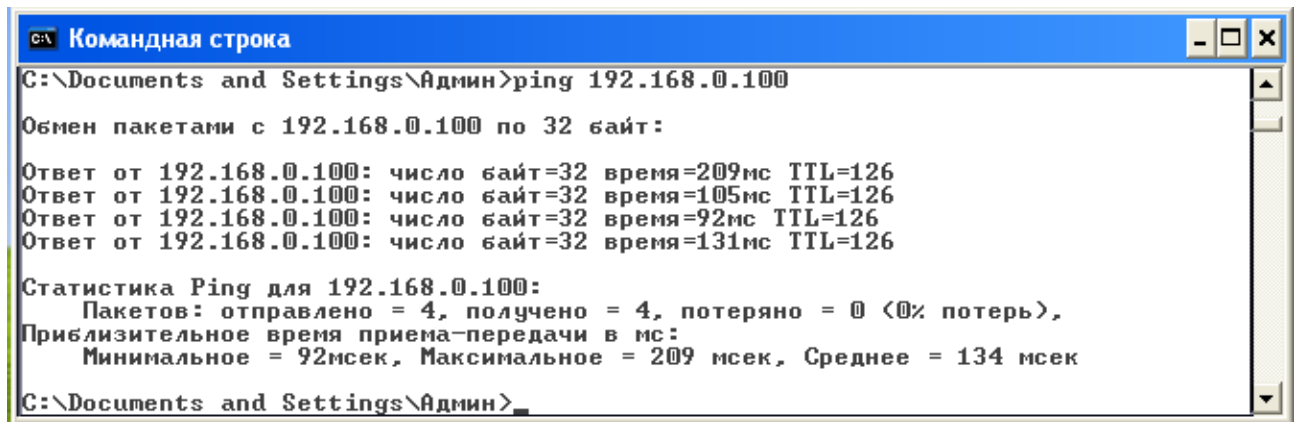


Рисунок 3.7 – Перевірка доступності мережі головного управління
ПриватБанку

З рисунків наведених вище видно, що мережева доступність присутня, віддалений клієнт отримав ip – адресу з виділеного пулу налаштованого на сервері vpn, трафік шифрується за допомогою обраних алгоритмів. Тепер перевіримо роботу політики isakmp та протоколу IPSec на маршрутизаторі ZT_PEREMOGI_99 (рис. 3.8, 3.9).

```
ZT_PEREMOGI_99#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
14.93.10.2   12.93.10.2   QM_IDLE       1006    0 ACTIVE
12.93.10.2   15.93.10.2   QM_IDLE       1005    0 ACTIVE
10.93.10.2   12.93.10.2   QM_IDLE       1001    0 ACTIVE
12.93.10.2   13.93.10.2   QM_IDLE       1002    0 ACTIVE
12.93.10.2   14.93.10.2   QM_IDLE       1007    0 ACTIVE
15.93.10.2   12.93.10.2   QM_IDLE       1004    0 ACTIVE
13.93.10.2   12.93.10.2   QM_IDLE       1003    0 ACTIVE

IPv6 Crypto ISAKMP SA
ZT_PEREMOGI_99#
```

Рисунок 3.8 – Перевірка роботи політики isakmp

```

ZT_PEREMOGI_99#show crypto ipsec profile
IPSEC profile PrivataBankProf
    Security association lifetime: 4608000 kilobytes/3600 seconds
    PFS (Y/N): N
    Transform sets={
        PrivatBank,
    }

ZT_PEREMOGI_99#

```

Рисунок 3.9 – Прегляд налаштованого профілю IPSec

Як видно з рисунків політики isakmp працює правильно, всі з'єднання які ініціюються активні.

Проведемо перевірку роботи PPTP серверу який відповідає за забезпечення роботи мережі банкоматів. Для цього потрібно спочатку створити підключення до віртуальної приватної мережі за допомогою вбудованих засобів операційної системи Microsoft Windows XP. Створивши підключення вибрати тип аутентифікації та шифрування. Результати роботи налаштованих параметрів показано на рисунках (3.10 – 3.12).

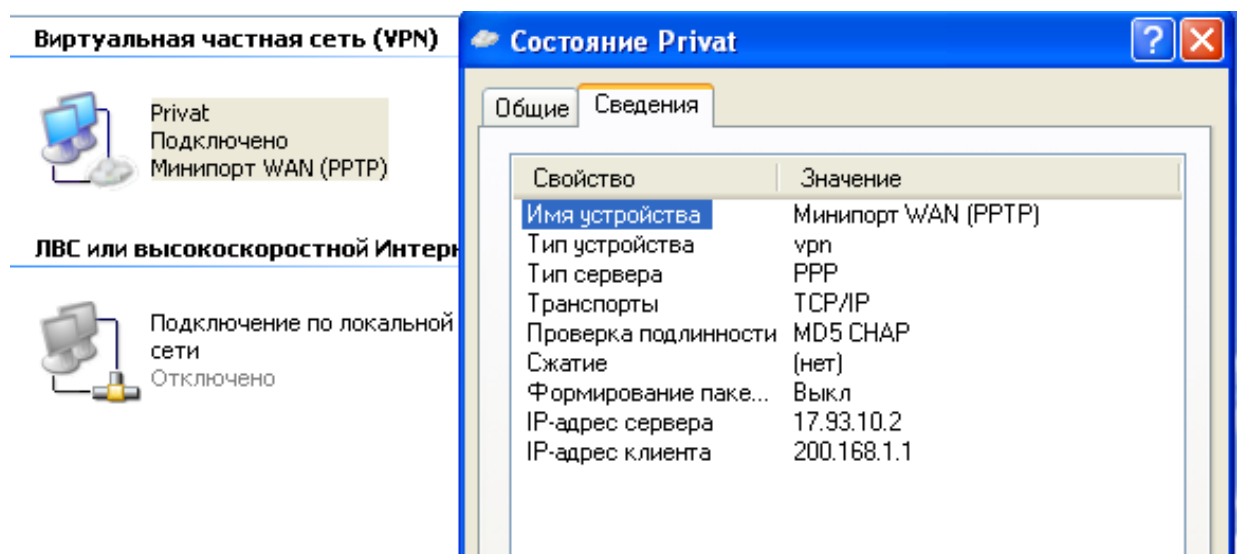


Рисунок 3.10 – Інформація про підключення до PPTP сервера

```

Dnipropetrovsk_R3#show vpdn

%No active L2F tunnels

%No active L2TP tunnels

PPTP Tunnel and Session Information Total tunnels 1 sessions 1

LocID Remote Name      State      Remote Address  Port  Sessions VPDN Group
2                               estabd    18.93.10.10    1032  1         1

LocID RemID TunID Intf    Username      State      Last Chg Uniq ID
2      16384 2      Vi3     privatuser    estabd    00:01:14 1
Dnipropetrovsk_R3#

```

Рисунок 3.11 – Інформація про підключення віддаленого хоста до сервера PPTP

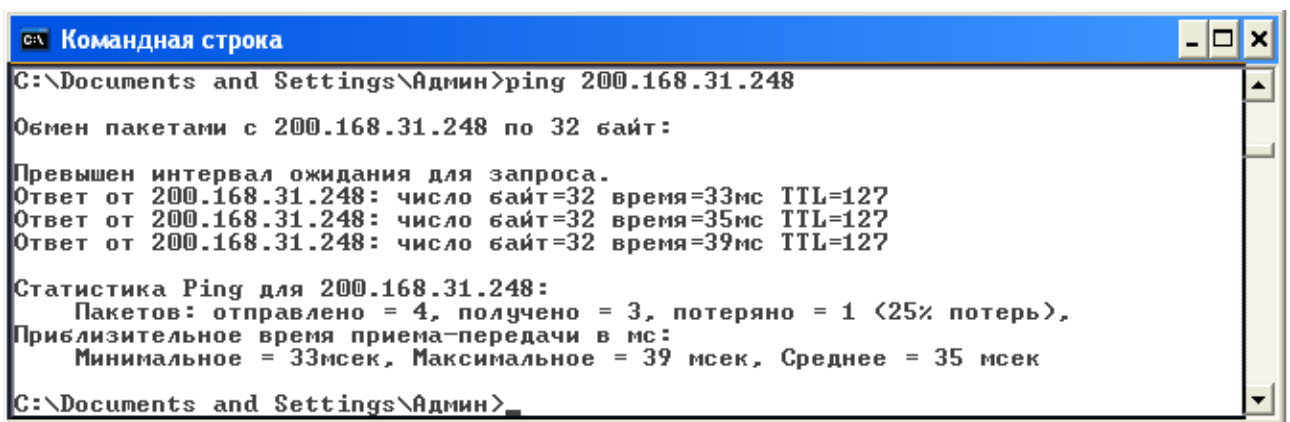


Рисунок 3.12 – Перевірка доступності процесингового сервера

З рисунків видно, що доступ до процесингового сервера існує, налаштовано правильно підключення до PPTP сервера та інформацію про підключеного користувача.

Тепер за допомогою програми-сніфера проаналізуємо трафік який циркулює в мережі. За допомогою даної програми можна дізнатись в якому вигляді проходить трафік, в зашифрованому чи незашифрованому, які пакети переаються, адреси вузлів між якими йде передача інформації. Результати наведено на рисунках (3.13 -3.15).

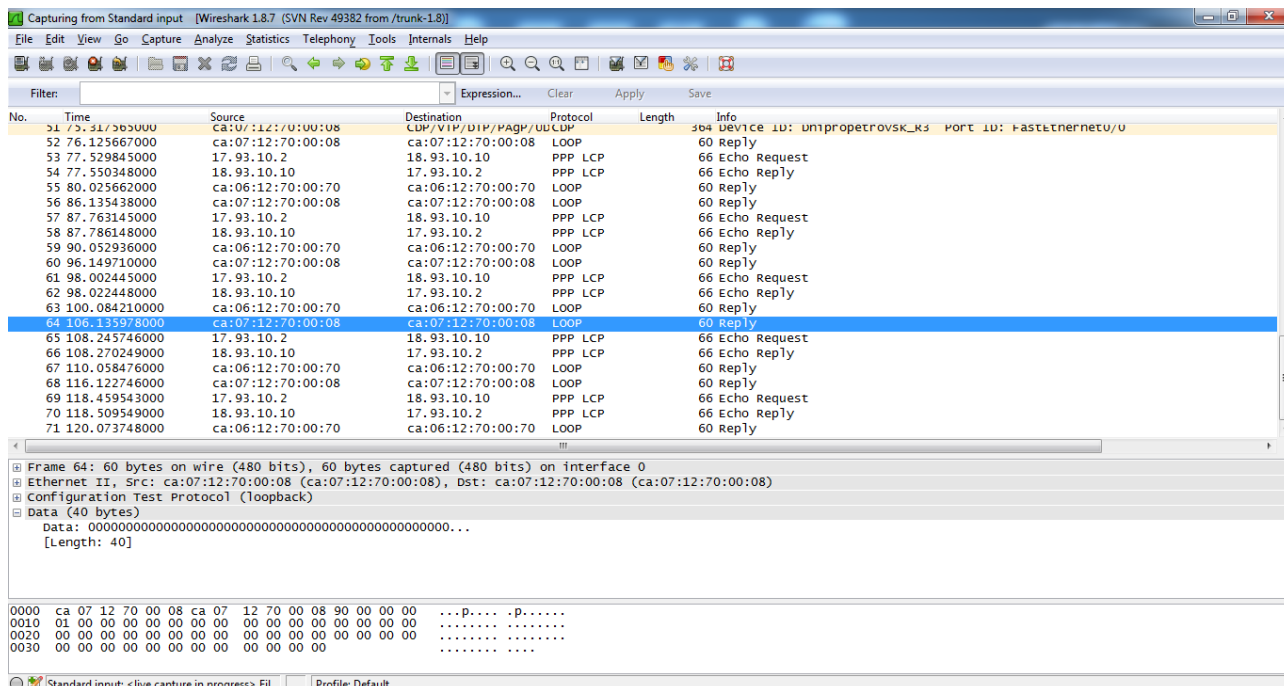


Рисунок 3.13 – Трафік знятий з PPTP сервера

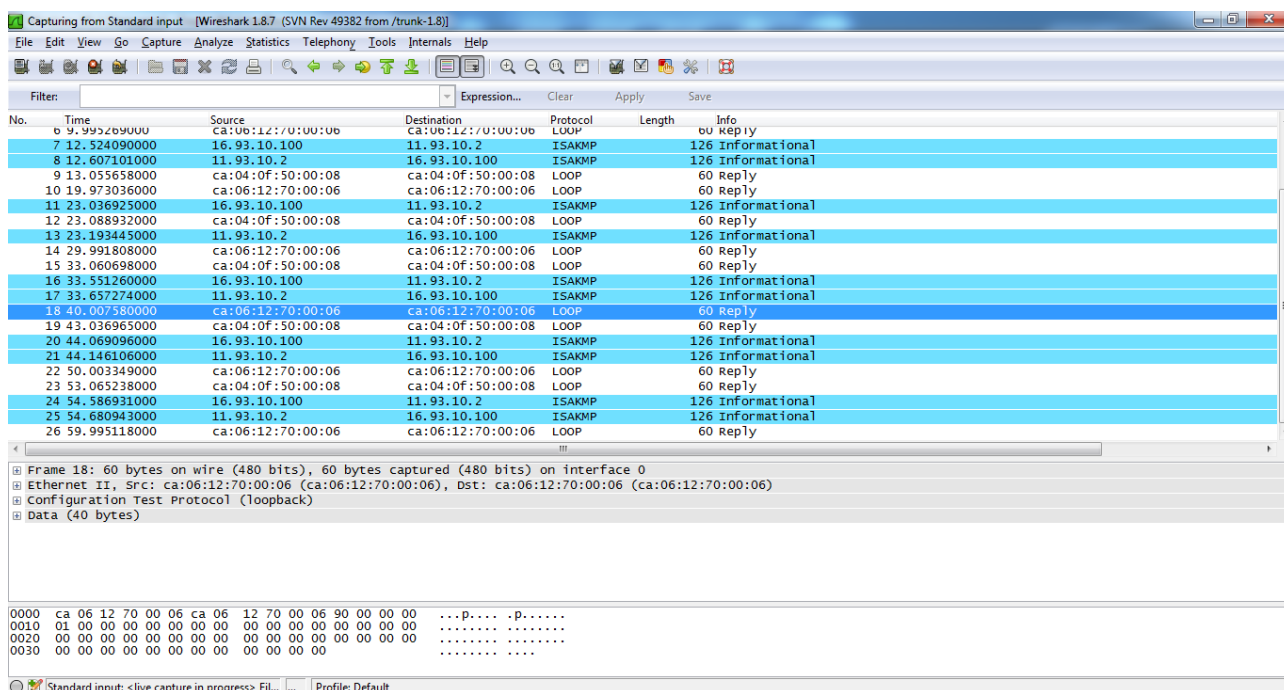


Рисунок 3.14 – Трафік знятий з VPN сервера

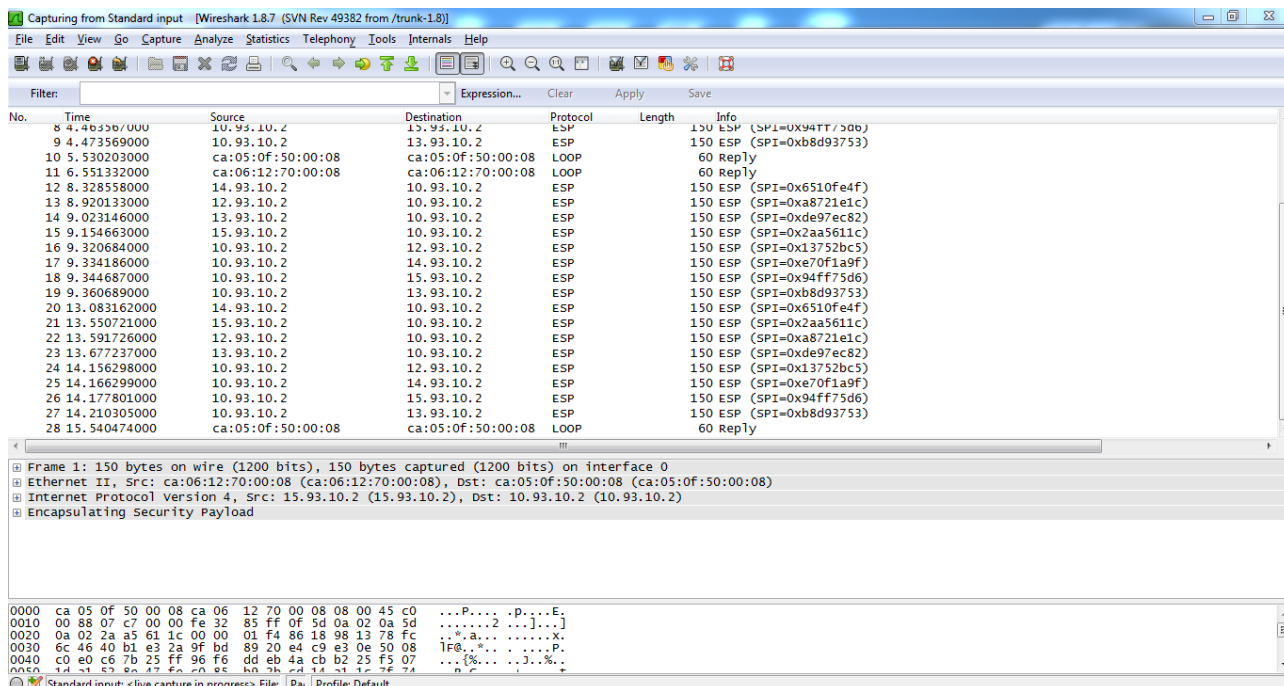


Рисунок 3.15 – Трафік знатий з маршрутизатора ZT_PEREMOGI_99

З проведеного аналізу трафіку видно, що всі дані які передаються в мережі проходять в зашифрованому вигляді. Перевіримо роботу SSH та Syslog сервера.

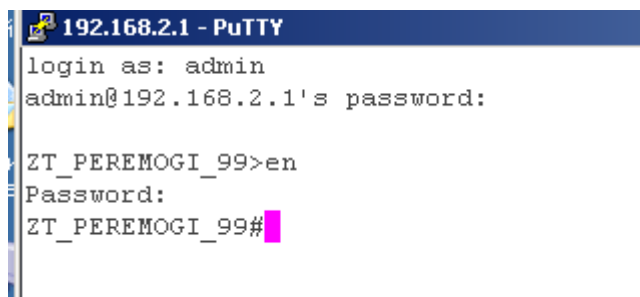


Рисунок 3.16 – Підключення до маршрутизатора за допомогою протоколу SSH

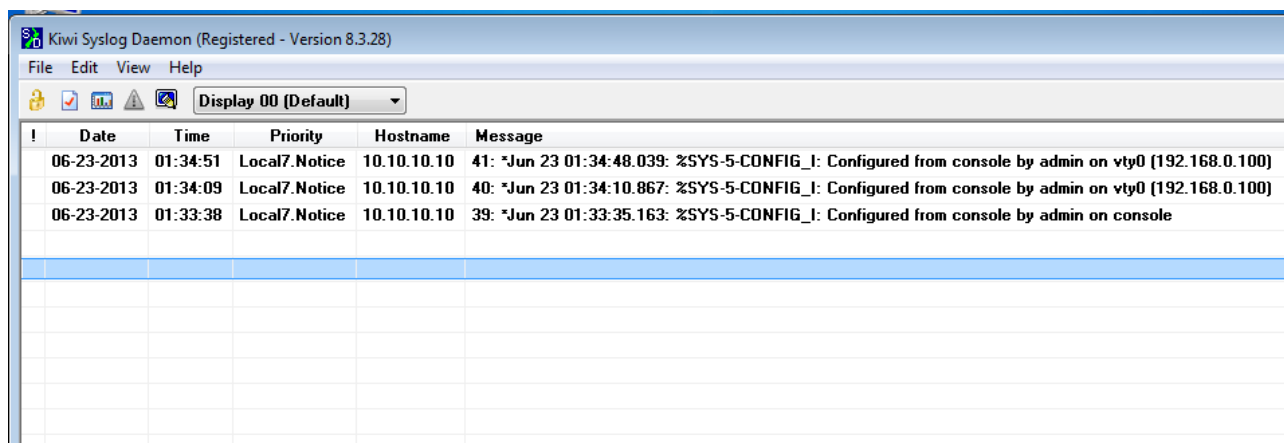


Рисунок 3.17 – Робота Syslog сервера

З рисунків наведених вище видно що налаштовані параметри серверів ssh та syslog працюють правильно.

Висновки до третього розділу

В даному розділі було обґрунтовано вибір апаратного та програмного забезпечення для роботи мережі. Проведено детальний аналіз та опис основного функціонального призначення обладнання, технічних характеристик, режимів та принципів роботи, видів та типів обладнання, наведено перелік переваг та недоліків. Проведено базове конфігурування мережевого обладнання комп'ютерної мережі, налаштовані основні параметри для роботи мережі та налаштована підсистема захисту, наведено результати конфігурувань та їх опис. Було проведено тестування роботи комп'ютерної мережі та перевірено доступність мережевого обладнання, правильність роботи підсистеми захисту, що була раніше налаштована. Для цього було проведено ряд перевірок в мережі, результати перевірок описано та підкріплено пояснюючими описами проведених дій. В результаті виконання отримано повноцінну, функціональну, захищену інформаційно-комунікаційну мережу, що готова до коректної роботи.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						60
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

Кваліфікаційна робота присвячена розробці проекту захищеної інформаційно-комунікаційної мережі банку (на прикладі Житомирського регіонального управління ПАТ КБ «ПриватБанк»). В ході виконання було проаналізовано загальну характеристику діяльності ПриватБанку, проаналізовано принципи та особливості інформаційної безпеки систем банківських установ, та методи і засоби захисту інформаційних мереж корпоративного банку.

Розроблено загальну, фізичну та логічну топології мережі та кожної підмережі з зазначенням кількості комунікаційного обладнання що використовується, видів каналів зв'язку та можливостей розширення.

На основі розробленої топології мережі, з урахуванням потреб зв'язку між підмережами, розроблено систему адресації інформаційно-комунікаційної системи для кожної з підмереж (зовнішньої, внутрішньої та тунелів). Розроблено підсистему захисту інформації в мережі, проаналізовано та вибрано засоби безпеки які будуть застосовуватись в розробленій мережі.

Проведено вибір апаратного та програмного забезпечення для роботи мережі на основі вимог до спроектованої мережі та підсистеми захисту, зокрема проаналізовано функціональні можливості обладнання та програмного забезпечення яке буде використовуватись.

Проведено базове налагодження підсистеми захисту інформаційно-комунікаційної мережі та перевірку роботоздатності налаштованих засобів захисту, в результаті чого отриманий бажаний результат роботи.

Реалізований проект готовий до використання. Мережа може бути впроваджена для забезпечення роботи банку.

В подальшому дана система може бути розширена шляхом впровадження нових функціональностей.

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						61
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про банки і банківську діяльність»: станом на 22 вересня 2020 р. / Верховна Рада України. – Офіц. вид. – К.: Відомості Верховної Ради. – 2001. – №47. – 533 с. – (Бібліотека офіційних видань).
2. Закон України «Про виконавче провадження»: станом на 8 липня 2020 р. / Верховна Рада України. – Офіц. вид. – К.: Відомості Верховної Ради. – 2012. – №14. – 87 с. – (Бібліотека офіційних видань).
3. Постанова правління НБУ від 14 липня 2006 р. №267 «Про затвердження Правил зберігання, захисту, використання та розкриття банківської таємниці» НБУ. – Офіц. вид. – Офіційний вісник України. – 2007. – №267. – 5 с. – (Бібліотека офіційних видань).
4. Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»: станом на 04 липня 2020 р. / Верховна Рада України. – Офіц. вид. – К.: Відомості Верховної Ради. – 2009. – №33. – 485 с – (Бібліотека офіційних видань).
5. Амато Вито. Основы организации сетей Cisco, том 2., испр. изд.: Пер. с англ. — М.: Издательский дом "Вильямс", 2014. — 464 с.: ил. — Парад, тит. англ. ISBN 5-8459-0561-3 (рус.)
6. А.Ю. Щеглов – Защита компьютерной информации от несанкционированного доступа. Наука и Техника, Санкт-Петербург – 2014
7. Биячуев Т.А. - Безопасность корпоративных сетей.(ИТМО) – 2014
8. Грайворонський М.В., Новиков О.М. Безпека інформаційно-комунікаційних систем. - К.:Видавнича група BVH, 2012.– 608с.;
9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы – СПб.: Питер, 2010. – 944 с.;
10. Поповский В.В. Защита информации в телекоммуникационных сетях: Учебник: В 2 т. / В.В. Поповский, А.В. Персигов. – Харьков: ООО «Компания СМІТ», 2006. – Т.2. – 292 с.;
11. Шаньгин В.Ф. - Защита информации в компьютерных системах и сетях – 2012;

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						62
Змн.	Арк.	№ докум.	Підпис	Дата		

12. «Про виртуальные сети. Внедряем DMVPN» // [Электронный ресурс].
– Режим доступа до статті: <http://cisco-lab.by/study/articles/1353-dmvpn.html>
13. Router Allows VPN Clients to Connect IPsec and Internet Using Split Tunneling Configuration Example // [Электронный ресурс]. – Режим доступа до статті: http://www.cisco.com/en/US/products/hw/routers/ps274/products_configuration_example09186a0080819289.shtml
14. Remote Access VPN Business Scenarios » // [Электронный ресурс]. – Режим доступа до статті: http://www.cisco.com/en/US/docs/security/vpn_modules/6342/configuration/guide/6342vpn4.html
15. Configuring the Cisco Router and VPN Clients Using PPTP and MPPE // [Электронный ресурс]. – Режим доступа до статті:
16. http://www.cisco.com/en/US/tech/tk827/tk369/technologies_configuration_example09186a00801e51e2.shtml
17. Настройка VPN сервера на Cisco (PPTP с шифрованием) // [Электронный ресурс]. – Режим доступа до статті: <http://wisedec.ru/2009/01/04/nastrojka-vpn-servera-na-cisco-pptp-s-hifrovaniem.html>

ДОДАТКИ

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						64
Змн.	Арк.	№ докум.	Підпис	Дата		

Технічні характеристики маршрутизатора Cisco 3745

Тип управляющего ПО

- Cisco IOS Software (minimum Cisco IOS release - 12.2(8) T)

Фиксированные интерфейсы

LAN интерфейсы

- 2 порта 10/100 BaseTX

WAN интерфейсы

- Дополнительный асинхронный интерфейс AUX EIA/TIA 232 - до 115.2 кбит/с

Другие

- Консольный порт

Количество слотов

- Cisco 3725 - 3 для WIC, 2 для NM или 1 HDSM, 2 для AIM
- Cisco 3745 - 3 для WIC, 4 для NM или 2 HDSM, 2 для AIM

Сравнение производительности

	Cisco 3725	Cisco 3660	Cisco 3745	Cisco 7200 с NPE- 225/NPE-400
Fast switching, kpps	100	110	225	225-400
Process switching, kpps	7	10	18	13-20

Модульные интерфейсы

WIC модули

- Высокоскоростные синхронные интерфейсы, до 2 Мбит/с (1 портовая карточка) и до 8 Мбит/с (2-х портовая карточка)
 - Низкоскоростные синхронно/асинхронные интерфейсы до 128 кбит/с в синхронном режиме и до 115.2 кбит/с в асинхронном, 2 порта
 - ISDN BRI S/T для коммутируемых/выделенных линий, 1 порт
 - ISDN BRI U с интегрированным оконечным устройством NT1, для коммутируемых/выделенных линий, 1 порт
 - 4-х проводный 56/64 кбит/с DSU/CSU, 1 порт
 - 1 порт T1 с DSU/CSU
 - Аналоговые модемы с поддержкой V.90, 1 или 2 модема
 - Высокоскоростной интерфейс широкополосного асимметричного доступа ADSL
 - Высокоскоростной интерфейс широкополосного симметричного доступа G.SHDSL
- Multiflex Voice&WAN интерфейсные карты

- 1-но и 2-х портовые интерфейсные карты E1, T1 и G703
- 2-х портовые интерфейсные карты E1 и T1 с поддержкой drop-insert

Сетевые Voice/Fax NM модули

- 1-но и 2-х слотовые модули расширения для голосовых карт

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						65
Змн.	Арк.	№ докум.	Підпис	Дата		

- 1-но слотовый модуль для установки multiflex Voice&WAN интерфейсной карты - до 5 DSP модулей для обработки голоса, до 60 голосовых соединений
- Модуль высокой плотности аналоговых голосовых портов, до 8 FXO, 12 FXS
VIC модули

- 2-х портовые voice FXS
- 2-х портовые voice FXO
- 2-х портовые voice E&M
- 2-х портовые voice BRI (ST/TE и NT/TE)
- 2-х портовые voice DID (Direct-Inward-Dial)
- 2-х портовые voice CAMAtrunk

LAN модули

- 16 портовый модуль коммутации 10/100BaseT с возможностью установки 1 порта 1000BaseT
- 36 портовый 10/100 EtherSwitch HDSM модуль, до 2-х портов 1000BaseT
- Возможность использования Inline Power в модулях 16/32 EtherSWitch

WAN модули

- 4-х и 8-ми портовые синхронно/асинхронные интерфейсы
- 16-ти и 32-х портовые асинхронные интерфейсы
- 8-ми и 16-ти портовые аналоговые модемные модули
- 1-но и 2-х портовый Channelized E1/PRI balanced/unbalanced модуль
- 4-х и 8-ми портовый модуль ISDN BRI с NT1 или S/T интерфейсом
- 2-х слотовый модуль для установки WIC карт

ATM модули

- 1-но портовый ATM E3 модуль
- 4-х и 8-ми портовые модули E1 ATM IMA

Сервисные модули AIM

- Модуль компрессии (до 8 Мбит/с)
- Модуль шифрования VPN IPSec
- Модуль поддержки ATM
- Модуль обработки голоса (30 каналов)
- Комбинированный модуль с поддержкой ATM и обработки голоса

Другие

- 64 портовый модуль мониторинга и управления AIC (Alarm Interface Controller)

Другие характеристики

Стандартное/максимальное количество flash памяти

- 32/128 Мб

Стандартное/максимальное количество DRAM памяти

- 32/512(256) Мб

Тип процессора

					КИК.КР.Б – 125 – 21 – ПЗ	Арк.
						66
Змн.	Арк.	№ докум.	Підпис	Дата		

- Cisco 3725 - 240 МГц MIPS RISC processor
- Cisco 3745 - 350 МГц MIPS RISC processor

Габариты

- Cisco 3725-3.5" x 17.25" x 14.7" (2 Rack Units)
- Cisco 3725-3.5" x 17.25" x 14.7" (3 Rack Units)

Электропитание

- Cisco 3725 - источник электропитания 135 Вт AC
- Cisco 3745 - источник электропитания AC или DC, отказоустойчивая конфигурация включает или 230 Вт AC и 230 Вт DC, или 2 AC, или 2 DC

Поддержка Inline Power

- Cisco 3725 - поддерживает только один внутренний источник электропитания -48 В DC мощностью до 360 Вт, подключающийся как карта расширения к источнику электропитания AC; возможно подключение нескольких внешних источников питания
- Cisco 3745 - поддерживает два внутренних источника электропитания -48 В DC в конфигурации: 360 Вт с резервированием, без резервирования; и 720 Вт без резервирования; возможно подключение внешних источников питания

Технічні характеристики комутатора Cisco SFE2010P 48-port 10/100

Ethernet Switch - PoE

Feature	Description
Specifications	
Ports	48 RJ-45 connectors for 10BASE-T/100BASE-TX/1000BASE-T with 4 Gigabit combo ports shared between mini-GBIC ports; console port; auto medium dependent interface (MDI) and MDI crossover (MDI-X); auto negotiate/manual setting; RPS port for connecting to redundant power supply unit
Buttons	Reset button
Cabling type	Unshielded twisted pair (UTP) Category 5 or better for 10BASE-T/100BASE-TX; UTP Category 5e or better for 1000BASE-T
LEDs	PWR, Fan, Link/Act, PoE, Speed, RPS, Master, Stack ID 1 through 8
PoE	• IEEE 802.3af PoE on delivered over any of the 48 10/100/1000 ports • Maximum power of 15.4W to an Ethernet port - 360W total available to all ports with regular AC power, 280W total available with RPS
Performance	
Switching capacity	96 Gbps nonblocking
Forwarding capacity	71.4 mpps (64-byte packets)
Stacking	

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						67
Змн.	Арк.	№ докум.	Підпис	Дата		

Stack operation	• Up to 192 ports in a stack • Hot insertion and removal • Ring and chain stacking options • Master and backup master for resilient stack control • Auto-numbering or manual configuration of units in stack
Layer 2	
MAC table size	8000
Number of VLANs	256 active VLANs (4096 range)
VLAN	Port-based and 802.1Q tag-based VLANs; protocol-based VLAN; management VLAN; multicast TV VLAN; Private VLAN Edge (PVE); Generic VLAN Registration Protocol (GVRP)
Head-of-line (HOL) blocking	HOL blocking prevention
Layer 3	
Layer 3 options	Static routing; classless interdomain routing (CIDR); 60 static routes; IPv4; forwarding in silicon - wire-speed forwarding of Layer 3 traffic
IPv6	
IPv6 options	IPv6 over Ethernet, dual stack, IPv6 over IPv4 network with Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnel, IPv6 neighbor discovery, stateless address configuration, maximum transmission unit (MTU) discovery, WEB, SSL, Telnet, Ping, Traceroute, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), Simple Network Management Protocol (SNMP), RADIUS, access control lists (ACLs), QoS, protocol based VLANs
Management	
Web user interface	Built-in web user interface for easy browser-based configuration (HTTP/HTTPS)
SNMP	SNMP versions 1, 2c, and 3 with support for trap
SNMP MIBs	RFC1213 MIB-2, RFC2863 interface MIB, RFC2665 Ether-like MIB, RFC1493 bridge MIB, RFC2674 extended bridge MIB (P-bridge, Q-bridge), RFC2819 RMON MIB (groups 1, 2, 3, and 9 only), RFC2737 entity MIB, RFC 2618 RADIUS client MIB, RFC 1215 traps
Remote Monitoring (RMON)	Embedded RMON software agent supports 4 RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis)
Firmware upgrade	• Web browser upgrade (HTTP/HTTPS) and TFTP • Dual images for resilient firmware upgrades
Port mirroring	Traffic on a port can be mirrored to another port for analysis with a network analyzer or RMON probe.
Other management	Traceroute; single IP management; SSL security for web user interface; SSH; RADIUS; port mirroring; TFTP upgrade; Dynamic Host Configuration Protocol (DHCP) client; BOOTP; SNTP; Xmodem upgrade; cable diagnostics; Ping; syslog; Telnet client (SSH secure support)
Security	

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						68
Змн.	Арк.	№ докум.	Підпис	Дата		

IEEE 802.1X	802.1X-RADIUS authentication, MD5 hash; guest VLAN; single/multiple host mode
ACLs	• Drop or rate limit based on source and destination MAC or IP address, protocol, port, VLAN, differentiated services code point (DSCP)/IP precedence, TCP/ User Datagram Protocol (UDP) source and destination ports, 802.1p priority, Ethernet type, Internet Control Message Protocol (ICMP) packets, Internet Group Management Protocol (IGMP) packets, DHCP snooping, Address Resolution Protocol (ARP) inspection, and IP source address guard • Up to 1018 rules
Advanced Security	• IP Source Guard • STP Root Guard • Dynamic ARP Inspection • DHCP Snooping
Availability	
Link aggregation	Using IEEE 802.3ad Link Aggregation Control Protocol (LACP), up to 8 ports in up to 8 groups
Storm control	Broadcast, multicast, and unknown unicast
Spanning Tree	IEEE 802.1D Spanning Tree, IEEE 802.1w Rapid Spanning Tree, IEEE 802.1s Multiple Spanning Tree, and Fast Linkover
DoS prevention	DoS attack prevention
IGMP (version 1 and 2) snooping	Limits bandwidth-intensive multicast traffic to only the requestors; supports 256 multicast groups
Power redundancy	Connection to RPS unit for power redundancy
Quality of service	
Priority levels	4 hardware queues
Scheduling	Priority queuing and weighted round-robin (WRR)
Class of service	Port-based; 802.1p VLAN priority-based; IPv4/v6 IP precedence/ToS/DSCP based; DiffServ; classification and re-marking ACLs
Rate limiting	Ingress policer; egress rate control; per VLAN
Statistics	16 meters
Standards	802.3 10BASE-T Ethernet, 802.3u 100BASE-TX Fast Ethernet, 802.3ab 1000BASE-T Gigabit Ethernet, 802.3z Gigabit Ethernet, 802.3x flow control, 802.3ad LACP, 802.3af PoE, 802.1D Spanning Tree Protocol (STP), 802.1Q/p VLAN, 802.1w Rapid STP, 802.1s Multiple STP, 802.1x port access authentication
Environmental	
Dimensions W x D x H	17.32 x 14.70 x 1.73 in. (440 x 375 x 44 mm)
Unit weight	10.89 lb (4.94 kg)
Power	100-240V 47-63 Hz, internal, universal; also equipped with external redundant power supply connector for external power supply, -48VDC

					КІК.КР.Б – 125 – 21 – П3	Арк.
						69
Змн.	Арк.	№ докум.	Підпис	Дата		

Certification	UL (UL 60950), CSA (CSA 22.2), CE mark, FCC Part 15 (CFR 47) Class A
Operating temperature	32° to 104°F (0° to 40°C)
Storage temperature	-4° to 158°F (-20° to 70°C)
Operating humidity	10% to 90%, relative, noncondensing
Storage humidity	10% to 95%, relative, noncondensing

Package Contents

- Cisco SGE2010P 48-Port Gigabit Switch
- AC power adapter with power cord
- Two rack-mounting kits with eight screws
- CD-ROM with user documentation (PDF) included
- Registration card
- Console cable

Minimum Requirements

- Web browser: Mozilla Firefox version 1.5 or later, Microsoft Internet Explorer version 5.5 or later
- Category 5 Ethernet network cable
- TCP/IP, network adapter, and network operating system (such as Microsoft Windows, Linux, or Mac OS X) installed on each computer in the network

Product Warranty

Limited lifetime warranty with return to factory replacement, one year telephone support and software fixes for the warranty term.

Технічні характеристики комутатора Cisco SRW2016 16-port Gigabit Switch

ФИЗИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

Размеры (ширина x глубина x высота), см: 44.00 x 20.25 x 4.445

Вес, кг: 2.17

Тип установки, особенности конструкции:

Параметры питания:

- Встроенный универсальный блок питания: 100 - 240 В, 47 - 63 Гц
- Потребляемая мощность:
 - 110 В - 22.6 Вт
 - 220 В - 23.3 Вт

Индикаторы статуса: System, Link/Act, Speed

Кнопки: Сброс

Комплектация:

- Коммутатор Cisco 300 серии
- Кабель питания
- Монтажный набор для установки в стойку
- Serial-кабель
- CD-ROM с пользовательской документацией (PDF)
- Краткое руководство по эксплуатации

ХАРАКТЕРИСТИКИ ПАМЯТИ:

Оперативная память: 128 МБ

Флеш-память: 16 МБ

ИНТЕРФЕЙСНЫЕ ПОРТЫ:

Медные интерфейсы: 18 x RJ-45 Gigabit Ethernet

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						70
Змн.	Арк.	№ докум.	Підпис	Дата		

Оптические интерфейсы:

Объединенные порты:

- 2 x RJ-45 Gigabit Ethernet
- 2 x SFP

Другие интерфейсы:

СЕТЕВЫЕ ОСОБЕННОСТИ:

Поддерживаемые стандарты:

- IEEE 802.3 10BASE-T Ethernet
- IEEE 802.3u 100BASE-TX Fast Ethernet
- IEEE 802.3ab 1000BASE-T Gigabit Ethernet
- IEEE 802.3ad LACP
- IEEE 802.3z Gigabit Ethernet
- IEEE 802.3x Flow Control
- IEEE 802.1D (STP, GARP, and GVRP)
- IEEE 802.1Q/p VLAN
- IEEE 802.1w RSTP
- IEEE 802.1s Multiple STP
- IEEE 802.1X Port Access Authentication
- IEEE 802.3af
- IEEE 802.3at

Производительность:

- Неблокируемая коммутация на скорости до 29.76 миллионов пакетов/с (размер пакетов 64 байта)
- Матрица коммутации: до 40.0 Гбит/с
- Размер пакетного буфера: 4 Мб

Стекирование:

Коммутация:

- Spanning Tree Protocol (STP):
 - Поддержка стандарта 802.1d STP
 - Быстрая конвергенция при помощи 802.1w (Rapid Spanning Tree [RSTP]), включена по умолчанию
 - Multiple Spanning Tree instances using 802.1s (MSTP)
- Группировка портов:
Поддержка IEEE 802.3ad Link Aggregation Control Protocol (LACP)
 - До 8 групп
 - До 8 портов в каждой группе, 16 портов-кандидатов в каждой группе
- VLAN:
 - Одновременная поддержка до 128 VLAN (из 4096 VLAN ID)
 - VLAN на основе портов или тегов 802.1Q
 - VLAN на основе MAC-адресов
 - Управляющая VLAN
 - Private VLAN Edge (PVE)
 - Гостевая VLAN
 - VLAN для клиентов, не прошедших проверку подлинности
- Голосовые VLAN
- Generic VLAN Registration Protocol (GVRP)/Generic Attribute Registration Protocol (GARP):
 - Трансляция Dynamic Host Configuration Protocol (DHCP) на уровне 2 (DHCP Option 82)
 - Internet Group Management Protocol (IGMP) Snooping версий 1 и 2, поддержка 256 multicast-групп
- IGMP Querier
- Предотвращение блокировки HOL (Head-of-line)
- Таблица MAC-адресов: до 8000 адресов

Маршрутизация:

- Маршрутизация IPv4:
 - Маршрутизация пакетов IPv4
 - До 32 статических маршрутов и до 32 IP-интерфейсов
- Поддержка Classless Inter-Domain Routing (CIDR)
- Трансляция DHCP на уровне 3
- Трансляция User Datagram Protocol (UDP)

Управление:

- Встроенная утилита конфигурации, доступ через веб-интерфейс (HTTP/HTTPS)
- SNMP (Simple Network Management Protocol) версий 1, 2c и 3
- Встроенный программный агент RMON (Remote Monitoring) поддерживает 4 группы RMON (история, статистика, оповещения и события) для управления, наблюдения и анализа трафика
- Двойной стек протоколов IPv6 и IPv4
- Обновление программного обеспечения:
 - Обновление программного обеспечения через веб-обозреватель (HTTP/HTTPS) или при помощи TFTP (Trivial File Transfer Protocol)
 - Обновление может быть инициализировано через консольный порт
 - Два образа программного обеспечения для упрощения процедуры обновления

- Зеркалирование портов для анализа трафика при помощи сетевого анализатора или зонда RMON. До 8 портов-источников могут быть зеркалированы на 1 целевой порт
- Зеркалирование VLAN для анализа трафика при помощи сетевого анализатора или зонда RMON. До 8 VLAN могут быть зеркалированы на 1 целевой порт
- DHCP (опции 66, 67, 82, 129 и 150)
- Редактируемые текстовые файлы конфигурации
- Функция Smartports упрощает конфигурацию и управление безопасностью
- Безопасная передача файлов на коммутатор
- Текстовый интерфейс командной строки (CLI)
- Облачные службы. Поддержка приложения Small Business Toolbar
- Многоязыковая локализация интерфейса и документации
- Другие функции управления:
Traceroute; управление через единый IP-адрес; HTTP/HTTPS; SSH; RADIUS; DHCP-клиент; BOOTP; SNTP; обновление Xmodem; диагностика кабеля; ping; системный журнал; клиент Telnet (поддержка SSH)
- Коммутатор оповещает о себе при помощи протокола Bonjour
- Link Layer Discovery Protocol (LLDP) (802.1ab) с расширениями LLDP-MED
- Cisco Discovery Protocol

Безопасность:

- Поддержка Secure Shell (SSH) версий 1 и 2
- Шифрование всего HTTP-трафика при помощи SSL
- IEEE 802.1X:
 - Аутентификация RADIUS, MD5-хеш; гостевые VLAN; режим одного/нескольких хостов
 - Поддержка повременной 802.1X
 - Динамическое назначение VLAN
- Изоляция 3 уровня: разрешение/запрещение маршрутизации между IP-подсетями или непосредственно связанными IP сетями
- Изоляция 2 уровня Private VLAN Edge (PVE) с community VLAN
- Безопасность портов: привязка MAC-адресов к портам, ограничение количества запомненных MAC-адресов
- Поддержка аутентификации RADIUS и TACACS+
- Защита от штормов: Broadcast, multicast и неизвестные unicast
- Защита от DoS-атак
- Предотвращение перегрузки TCP
- Списки контроля доступа (ACL):
 - Поддержка до 512 правил
 - Ограничение полосы пропускания в зависимости исходного и конечного MAC-адресов, VLAN ID или IP-адреса, протокола, порта, приоритета differentiated services code point (DSCP) / IP, исходных и конечных портов TCP/UDP, приоритета 802.1p, типа Ethernet, пакетов Internet Control Message Protocol (ICMP), пакетов IGMP, флага TCP

Доступность:

- Автоматическое отключение питания на портах RJ-45 Gigabit Ethernet при отсутствии соединения, повторное включение при возобновлении активности
- Определение длины кабеля для уменьшения потребляемой мощности

QoS:

- Уровни приоритетов: 4 аппаратные очереди
- Очередность:
 - Строгий приоритет и weighted round-robin (WRR)
 - Очередь назначается в зависимости от differentiated services code point (DSCP) и класса обслуживания (802.1p/CoS)
- Качество обслуживания зависит от: портов, приоритетов 802.1p VLAN, IPv4/v6 IP приоритета/типа обслуживания (ToS)/DSCP, дифференцированных услуг (DiffServ); классификации и изменения маркировки ACL, проверенных QoS
- Ограничение скорости: входные политики; во VLAN, на портах

Сетевые функции:

- IPv6:
 - Хост-режим IPv6
 - IPv6 over Ethernet
 - Двойной стек протоколов IPv6 и IPv4
 - Обнаружение ближайших устройств и маршрутизаторов IPv6 (ND)
 - Автоматическая конфигурация адресов IPv6
 - Path maximum transmission unit (MTU) Discovery
 - Duplicate address detection (DAD)
 - Internet Control Message Protocol (ICMP) версии 6
 - IPv6 через сеть IPv4 с поддержкой Intra-Site Automatic Tunnel Addressing

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						72
Змн.	Арк.	№ докум.	Підпис	Дата		

Protocol (ISATAP)

- IPv6 QoS: аппаратная приоритизация пакетов IPv6
- IPv6 ACL:

Drop or rate limit IPv6 packets in hardware

- Multicast Listener Discovery (MLD) snooping

- Приложения IPv6:

Web/SSL, Telnet сервер/SSH, ping, traceroute, Simple Network Time Protocol (SNTP), Trivial File Transfer Protocol (TFTP), SNMP, RADIUS, системный журнал, DNS-клиент, зависящие от протоколов VLAN

- IPv6 RFCs supported:

- RFC 2463 - ICMP version 6
- RFC 3513 - IPv6 address architecture
- RFC 4291 - IPv6 addressing architecture
- RFC 2460 - IPv6 specification
- RFC 2461 - Neighbor discovery for IPv6
- RFC 2462 - IPv6 stateless address auto-configuration
- RFC 1981 - Path MTU discovery
- RFC 4007 - IPv6 scoped address architecture
- RFC 3484 - Default address selection mechanism
- RFC 4214 - ISATAP tunneling
- RFC 4293 - MIB IPv6: Textual conventions and general group
- RFC 3595 - Textual conventions for IPv6 flow label

- Jumbo Frames: поддержка кадров размером до 10 кб

					КИК.КР.Б – 125 – 21 – ПЗ	Арк.
						73
Змн.	Арк.	№ докум.	Підпис	Дата		

Загальна конфігурація маршрутизатора Internet

```

!
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Internet
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
!
!
!
interface FastEthernet0/0
ip address 10.93.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 11.93.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 12.93.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet1/1
ip address 13.93.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 14.93.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet2/1
ip address 15.93.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet3/0

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						74
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 16.93.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet3/1
ip address 18.93.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet4/0
ip address 17.93.10.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet4/1
no ip address
shutdown
duplex auto
speed auto
!
ip classless
no ip http server
no ip http secure-server
!
logging alarm informational
no cdp run
!
!
control-plane
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
!
End

```

Загальна конфігурація маршрутизатора Dnipropetrovsk_R1

```

!
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Dnipropetrovsk_R1
!
boot-start-marker

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						75
Змн.	Арк.	№ докум.	Підпис	Дата		

```

boot-end-marker
!
enable secret 5 $1$MOZ5$wtFRaIAneMiMiSmPSsKr50
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
ip domain name PrivatDniprop.ua
ip ssh version 2
!
username admin password 0 cisco
!
!
!
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key privatbn address 0.0.0.0 0.0.0.0 no-xauth
!
!
crypto ipsec transform-set PrivatBank esp-3des esp-md5-hmac
!
crypto ipsec profile PrivataBankProf
  set transform-set PrivatBank
!
!
interface Tunnel1
  description DMVPN_HUB
  ip address 172.16.0.1 255.255.240.0
  no ip redirects
  ip mtu 1400
  ip hold-time eigrp 1 35
  no ip next-hop-self eigrp 1
  ip nhrp authentication privatbn
  ip nhrp map multicast dynamic
  ip nhrp network-id 100
  ip tcp adjust-mss 1300
  no ip split-horizon eigrp 1
  tunnel source 10.93.10.2
  tunnel mode gre multipoint
  tunnel protection ipsec profile PrivataBankProf
!
interface FastEthernet0/0
  description internet
  ip address 10.93.10.2 255.255.255.0
  ip nat outside
  ip virtual-reassembly
  duplex auto
  speed auto
!
interface FastEthernet0/1

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						76
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 192.168.0.2 255.255.254.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
vrrp 1 ip 192.168.0.1
vrrp 1 priority 200
vrrp 2 timers advertise 10
vrrp 2 timers learn
!
interface FastEthernet1/0
no ip address
shutdown
duplex half
!
interface FastEthernet2/0
no ip address
shutdown
duplex half
!
!

router eigrp 1
network 172.16.0.0 0.0.15.255
network 192.168.0.0 0.0.1.255
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.93.10.1
no ip http server
no ip http secure-server
!
!
ip nat inside source list NAT interface FastEthernet0/0 overload
!
ip access-list extended NAT
permit ip 192.168.0.0 0.0.1.255 any
!
logging alarm informational
no cdp run
!
control-plane
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0
login local
line vty 1 4
login

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						77
Змн.	Арк.	№ докум.	Підпис	Дата		

!
!
end

Загальна конфігурація маршрутизатора Dnipropetrovsk_R2

!
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Dnipropetrovsk_R2
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication login USER-AUTH local
aaa authorization network GROUP-AUTH local
!
aaa session-id common
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
ip domain name PrivatDniprop.ua
ip ssh version 2
!
!
username privtabankuser password 0 privatpassword
username admin secret 5 \$1\$SBT9\$gaheQVjKSF6hPjCcxhyMY1
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
!
crypto isakmp client configuration group Privat-Bank-GROUP
key PrivatCisco
dns 192.168.0.200
wins 192.168.0.200
domain PrivatBank.ua
pool VPN-POOL
acl 110
save-password
crypto isakmp profile VPN-CLIENT
match identity group Privat-Bank-GROUP

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						78
Змн.	Арк.	№ докум.	Підпис	Дата		

```

client authentication list USER-AUTH
isakmp authorization list GROUP-AUTH
client configuration address respond
!
crypto ipsec transform-set EZVPN esp-aes esp-md5-hmac
!
crypto dynamic-map DYNMAP 10
set transform-set EZVPN
set isakmp-profile VPN-CLIENT
reverse-route
!
!
crypto map DMAP 1 ipsec-isakmp dynamic DYNMAP
!
interface FastEthernet0/0
ip address 11.93.10.2 255.255.255.0
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
crypto map DMAP
!
interface FastEthernet0/1
ip address 192.168.0.3 255.255.254.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
vrrp 1 ip 192.168.0.1
vrrp 1 timers advertise 10
vrrp 1 timers learn
!
interface FastEthernet1/0
no ip address
shutdown
duplex half
!
interface FastEthernet2/0
no ip address
shutdown
duplex half
!
router eigrp 1
network 192.168.0.0 0.0.1.255
network 192.168.96.0 0.0.7.255
no auto-summary
!
ip local pool VPN-POOL 192.168.96.1 192.168.103.254
ip classless
ip route 0.0.0.0 0.0.0.0 11.93.10.1
no ip http server
no ip http secure-server
!
!
ip nat inside source list NAT interface FastEthernet0/0 overload
!
ip access-list extended NAT
permit ip 192.168.0.0 0.0.1.255 any
!
logging alarm informational
access-list 110 permit ip 192.168.96.0 0.0.7.255 any
!
control-plane

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						79
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
!
!
End

```

Загальна конфігурація маршрутизатора Dnipropetrovsk_R3

```

!
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Dnipropetrovsk_R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
vpdn enable
!
vpdn-group 1
! Default PPTP VPDN group
accept-dialin
protocol pptp
virtual-template 1
!
!
username privatuser password 0 123456
!
interface FastEthernet0/0
ip address 17.93.10.2 255.255.255.0
duplex auto
speed auto
!

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Virtual-Template1
ip unnumbered FastEthernet0/0
peer default ip address pool test
ppp encrypt mppe auto
ppp authentication pap chap ms-chap
!
ip local pool test 200.168.1.1 200.168.31.250
ip classless
ip route 0.0.0.0 0.0.0.0 17.93.10.1
no ip http server
no ip http secure-server
!
!
logging alarm informational
!
control-plane
!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
!
End

```

Загальна конфігурація маршрутизатора ZT_Kyivska_77

```

!
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ZT_Kyivska_77
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						81
Змн.	Арк.	№ докум.	Підпис	Дата		

```

resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
ip domain name Kyivska_77.ua
ip ssh version 2
!
username admin password 0 cisco
!
!
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
crypto isakmp key privatbn address 0.0.0.0 0.0.0.0 no-xauth
!
!
crypto ipsec transform-set PrivatBank esp-3des esp-md5-hmac
!
crypto ipsec profile PrivataBankProf
set transform-set PrivatBank
!
!
interface Tunnel1
description ZT_Kyivska_77
ip address 172.16.0.5 255.255.240.0
no ip redirects
ip mtu 1400
ip hold-time eigrp 1 35
ip nhrp authentication privatbn
ip nhrp map 172.16.0.1 10.93.10.2
ip nhrp map multicast 10.93.10.2
ip nhrp network-id 100
ip nhrp nhs 172.16.0.1
ip nhrp registration no-unique
ip tcp adjust-mss 1300
delay 100000
tunnel source 15.93.10.2
tunnel mode gre multipoint
tunnel protection ipsec profile PrivataBankProf
!
interface FastEthernet0/0
ip address 15.93.10.2 255.255.255.0
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.4.1 255.255.255.224
ip nat inside
ip virtual-reassembly
duplex auto
speed auto

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						82
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface FastEthernet1/0
no ip address
shutdown
duplex half
!
interface FastEthernet2/0
no ip address
shutdown
duplex half
!
router eigrp 1
network 172.16.0.0 0.0.15.255
network 192.168.4.0 0.0.0.31
auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 15.93.10.1
no ip http server
no ip http secure-server
!
ip nat inside source list NAT interface FastEthernet0/0 overload
!
ip access-list extended NAT
permit ip 192.168.4.0 0.0.0.31 any
!
logging alarm informational
!
control-plane
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0
login local
line vty 1 4
login
!
!
End

```

Загальна конфігурація маршрутизатора ZT_PEREMOGI_99

```

!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						83
Змн.	Арк.	№ докум.	Підпис	Дата		

```

hostname ZT_PEREMOGI_99
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$CCoh$ExglG9gDPnfHn8pXX8mrM0
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
no ip domain lookup
ip domain name PrivatBankZT.ua
ip ssh version 2
!
!
username admin password 0 cisco
!
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key privatbn address 0.0.0.0 0.0.0.0 no-xauth
!
!
crypto ipsec transform-set PrivatBank esp-3des esp-md5-hmac
!
crypto ipsec profile PrivataBankProf
  set transform-set PrivatBank
!
interface Tunnel1
  description ZT_PEREMOGI_99
  ip address 172.16.0.2 255.255.240.0
  no ip redirects
  ip mtu 1400
  ip hold-time eigrp 1 35
  ip nhrp authentication privatbn
  ip nhrp map 172.16.0.1 10.93.10.2
  ip nhrp map multicast 10.93.10.2
  ip nhrp network-id 100
  ip nhrp nhs 172.16.0.1
  ip nhrp registration no-unique
  ip tcp adjust-mss 1300
  delay 100000
  tunnel source 12.93.10.2
  tunnel mode gre multipoint
  tunnel protection ipsec profile PrivataBankProf
!
interface FastEthernet0/0
  ip address 12.93.10.2 255.255.255.0
  ip nat outside
  ip virtual-reassembly
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 192.168.2.1 255.255.255.0

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						84
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex half
!
interface FastEthernet2/0
no ip address
shutdown
duplex half
!
router eigrp 1
network 172.16.0.0 0.0.15.255
network 192.168.2.0
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 12.93.10.1
no ip http server
no ip http secure-server
!
ip nat inside source list NAT interface FastEthernet0/0 overload
!
ip access-list extended NAT
permit ip 192.168.2.0 0.0.0.255 any
!
logging alarm informational
no cdp run
!
!
!
!
control-plane
!
gatekeeper
shutdown
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0
login local
line vty 1 4
login
!
!
End

```

Загальна конфігурація маршрутизатора ZT_VelBerdichivska_42

!
version 12.4

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						85
Змн.	Арк.	№ докум.	Підпис	Дата		

```

service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ZT_VelBerdichivska_42
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
ip domain name VelBerdichivska_4.ua
ip ssh version 2
!
username admin password 0 cisco
!
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key privatbn address 0.0.0.0 0.0.0.0 no-xauth
!
!
crypto ipsec transform-set PrivatBank esp-3des esp-md5-hmac
!
crypto ipsec profile PrivataBankProf
  set transform-set PrivatBank
!
interface Tunnel1
  description ZT_VelBerdichivska_4
  ip address 172.16.0.4 255.255.240.0
  no ip redirects
  ip mtu 1400
  ip hold-time eigrp 1 35
  ip nhrp authentication privatbn
  ip nhrp map 172.16.0.1 10.93.10.2
  ip nhrp map multicast 10.93.10.2
  ip nhrp network-id 100
  ip nhrp nhs 172.16.0.1
  ip nhrp registration no-unique
  ip tcp adjust-mss 1300
  delay 100000
  tunnel source 14.93.10.2
  tunnel mode gre multipoint
  tunnel protection ipsec profile PrivataBankProf
!
interface FastEthernet0/0
  ip address 14.93.10.2 255.255.255.0
  ip nat outside
  ip virtual-reassembly

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						86
Змн.	Арк.	№ докум.	Підпис	Дата		

```

duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.5.1 255.255.255.192
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex half
!
interface FastEthernet2/0
no ip address
shutdown
duplex half
!
router eigrp 1
network 172.16.0.0 0.0.15.255
network 192.168.5.0 0.0.0.63
auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 14.93.10.1
no ip http server
no ip http secure-server
!
!
ip nat inside source list NAT interface FastEthernet0/0 overload
!
ip access-list extended NAT
permit ip 192.168.5.0 0.0.0.63 any
!
logging alarm informational
!
!
control-plane
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0
login local
line vty 1 4
login
!
!
end

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						87
Змн.	Арк.	№ докум.	Підпис	Дата		

Загальна конфігурація маршрутизатора ZT_Vitruka_15

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ZT_Vitruka_15
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$DbPw$u9dWZXdntEcavcymiCjLz.
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
ip domain name Vitruka15.ua
ip ssh version 2
!
username admin password 0 cisco
!
!
!
crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
  group 2
crypto isakmp key privatbn address 0.0.0.0 0.0.0.0 no-xauth
!
!
crypto ipsec transform-set PrivatBank esp-3des esp-md5-hmac
!
crypto ipsec profile PrivataBankProf
  set transform-set PrivatBank
!
interface Tunnel1
  description ZT_Vitruka_15
  ip address 172.16.0.3 255.255.240.0
  no ip redirects
  ip mtu 1400
  ip hold-time eigrp 1 35
  ip nhrp authentication privatbn
  ip nhrp map 172.16.0.1 10.93.10.2
  ip nhrp map multicast 10.93.10.2
  ip nhrp network-id 100
  ip nhrp nhs 172.16.0.1
  ip nhrp registration no-unique
  ip tcp adjust-mss 1300
  delay 100000
  tunnel source 13.93.10.2
  tunnel mode gre multipoint

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						88
Змн.	Арк.	№ докум.	Підпис	Дата		

```

tunnel protection ipsec profile PrivataBankProf
!
interface FastEthernet0/0
ip address 13.93.10.2 255.255.255.0
ip nat outside
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.3.1 255.255.255.128
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
interface FastEthernet1/0
no ip address
shutdown
duplex half
!
interface FastEthernet2/0
no ip address
shutdown
duplex half
!
router eigrp 1
network 172.16.0.0 0.0.15.255
network 192.168.3.0 0.0.0.127
auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 13.93.10.1
no ip http server
no ip http secure-server
!
!
ip nat inside source list NAT interface FastEthernet0/0 overload
!
ip access-list extended NAT
permit ip 192.168.3.0 0.0.0.127 any
!
logging alarm informational
!
control-plane
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0
login local

```

					КІК.КР.Б – 125 – 21 – ПЗ	Арк.
						89
Змн.	Арк.	№ докум.	Підпис	Дата		

line vty 1 4
login
!
!
end