Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління_____
(повна назва)
Кафедра_____Автоматизації проектування обчислювальної техніки_____

(повна назва)

# АТЕСТАЦІЙНА РОБОТА
# Пояснювальна записка

_____другий (магістерський)_____
(рівень вищої освіти)

_____ГЮІК_505ХХХ.018_ПЗ_____
(позначення документа)

_____Спеціалізовані банківські системи з використанням технології VPN_____
(тема)

Виконав: студент 2 курсу, групи СКСм-18-1
Турчинов О.О._____
(прізвище, ініціали)
Спеціальність 123 Комп'ютерна_____ інженерія_____
(код і повна назва спеціальності)
Тип програми Освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Спеціалізовані комп'ютерні системи_____
(повна назва спеціалізації)
Керівник доцент кафедри АПОТ_____ канд.техн.наук. Хаханова І.В._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Чумаченко С.В.
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління

Кафедра Автоматизації проектування обчислювальної техніки

Рівень вищої освіти другий (магістерський)

Спеціальність 123 Комп'ютерна інженерія

Тип програми Освітньо-професійна

Освітня програма Спеціалізовані комп'ютерні системи

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

# ЗАВДАННЯ
## НА АТЕСТАЦІЙНУ РОБОТУ

студентові Турчинову Олександру Олександровичу

(прізвище, ім'я, по батькові)

1. Тема роботи Спеціалізовані банківські системи з використанням технології VPN

затверджена наказом по університету від _04_ __листопада__2019 р. № 1624 Ст

2. Термін подання студентом роботи до екзаменаційної комісії _20_ __грудня__ 2019 р.

3. Вихідні дані до роботи
Програма OpenVPN
Середовище розробки MS Visual Studio 2012
Мова програмування C++

4. Перелік питань, що потрібно опрацювати в роботі
Створення мережі VPN
Загрози для банку в мережі VPN
Методи захисту інформації в Інтернеті
Створення та підтримка банківської VPN мережі
Створення програми автоматизації налаштування мережі
Середовище розробки програмного забезпечення

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

15 слайдів

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1 )

| Найменування розділу | Консультант (посада, прізвище, ім'я, по батькові) | Позначка консультанта про виконання розділу | |
|---|---|---|---|
| | | підпис | дата |
| | | | |
| | | | |

**КАЛЕНДАРНИЙ ПЛАН**

**КАЛЕНДАРНИЙ ПЛАН**

| № | Назва етапів роботи | Терміни виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | *Видача теми проекту, узгодження і* | 03.09.19 | |
| 2 | *Аналіз предметної області та опрацювання джерел* | 03.09.19 – 1.10.19 | |
| 3 | *Дослідження існуючих рішень та безпеки технології VPN в сучасному* | 2.10.19 – 20.10.19 | |
| 4 | *Тестування розроблених підходів* | 20.10.19 – 1.11.19 | |
| 5 | *Аналіз розроблених рішень* | 2.11.19 – 10.11.19 | |
| 6 | *Оформлення пояснювальної записки* | 11.11.19-27.11.19 | |
| 7 | *Перевірка виконаного проекту* | 28.11.19 – 11.12.19 | |
| 8 | *Захист проекту* | 24.12.19 | |
| | | | |
| | | | |
| | | | |

Дата видачі завдання _____ _____20__ р.

Студент _____
(підпис)

Керівник роботи _____доцент Хаханова І.В.
(підпис) (посада, прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка містить 78 сторінок, 21 рисунок, 8 таблиць, 10 джерел за переліком посилань.

VPN, БАНК, СИСТЕМА, БЕЗПЕКА, АТМ, OPENVPN, ІНТЕРНЕТ, КЛІЄНТ, СЕРВЕР, КРИПТОГРАФІЯ, ЗАХИСТ

У роботі розглянуті питання автоматизації генерації конфігураційних файлів в мережі, що використовує VPN. Проведене дослідження принципів налаштування та підтримки банківської системи, що працює в мережі Інтернет, досліджені можливі загрози з боку зловмисників та методи захисту від них.

Проаналізовані існуючі VPN мережі та системи, що використовують дану технологію. Розроблений додаток, що генерує конфігураційні файли для серверної та клієнтської частини банку. Повністю досліджене налаштування серверної та клієнтської частин при використанні VPN рішень.

\

# ABSTRACT

The explanatory note contains 78 pages, 21 figures, 8 tables, 10 references.

VPN, BANK, SYSTEM, SECURITY, ATM, OPENVPN, INTERNET, CUSTOMER, SERVER, CRYPTOGRAPHY, SECURITY

The paper discusses the issues of automation of the generation of configuration files on a network using a VPN. The principles of setting up and maintaining the banking system operating on the Internet are investigated, the possible threats from the attackers and methods of protection against them are investigated.

Existing VPN networks and systems using this technology are analyzed. Developed application that generates configuration files for server and client side of the bank. The configuration of the server and client parts when using VPN solutions is fully explored.

**ЗМІСТ**

# ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

IP – internet protocol;

ПЗ – програмне забезпечення:

VPN – virtual private network;

NAT – network address translation);

MTU – maximum Transfer Unit;

ЛОМ – локальна обчислювальна мережа;

IPSec – Security Architecture for IP;

БМ – банківська мережа ;

DoS – denial of service;

FTP – file transfer protocol;

П – правило;

НСД – несанкційований доступ;

ІББ – інформаційна безпека банку;

МЕ – міжмережевий екран;

СВА – система виявлення атак;

MS – Microsoft.

# ВСТУП

На сьогоднішній день передача інформації у великих та малих банках майже завжди проходить за допомогою мережевих технологій в електронному вигляді. При такому виді передачі треба мати на увазі те, що інформація у відкритих для доступу мережах може бути перехоплена та використана в корисних або деструктивних для банку цілях. Банківською інформацією можна назвати як персональні дані клієнтів та членів банку, так і комерційні таємниці та іншу інформацію, доступ до якої має обмежене коло людей. В банківській мережі можуть бути перехоплені також імена аккаунтів користувачів, їх електронні адреси та паролі до них. Саме тому на перше місце в організації подібних мереж завжди становлять її безпеку.

Більше всього уваги до інформаційної безпеки загалом дають великі банки, що мають ускладнену, децентралізовану та багатошарову структуру: міжнародні банки, державні або великі банки, яким важливо залишити свою інформацію в таємниці. Зазвичай в таких захищених мережах використовують багато різних технологій від різних виробників, старі або новітні моделі мережевого обладнання, що в свою чергу сильно ускладнює процес налаштування та управління системою.

Більше того, корпоративні інформаційні структури відрізняються від звичайних своєю різноманітністю. Вони можуть складатися з різних наборів та баз даних, розподілених та локальних систем та задач. Все це відкриває багато різних можливостей для злочинників та робить технологію вразливою до атак. Дані, які передаються по відкритій мережі можуть бути прочитані, пошкоджені або перехоплені шкідливими програмами, зробленими для того, аби нашкодити банкам або пережати конфіденційну інформацію третім особам. Однак, це не каже, що невеликі банківські установи не повинні брати до уваги питання безпеки своєї інформації. На сьогоднішній день питання безпеки в мережах бізнесу, пов'язаного з віртуальним простором

(використовуючого технології IP-телефонії, електронної пошти, хмарних сховищ інформації, wi-fi камер, віртуальних серверів або сервісами оплати через Інтернет) являється актуальним. Хакери, нездатні атакувати великі центри, направлено атакують сучасні фірми середньої руки та намагаються дістати конфіденційні та фінансові дані навіть з них.

На даний момент найбільш серйозною небезпекою для будь-якої інфраструктури являються віруси (черви, троянське ПЗ), спам, фішинг, будь-яке рекламне та шпигунське програмне забезпечення, копіювання сторінок в Інтернеті, соціальний інжинірінг та підміна головних сторінок веб-ресурсу. Джерелом подібної загрози можуть бути як користувачі ззовні, так і співробітники банків, які ненавмисно занесли шкідливу програму до системи.

Будь яка шкідлива програма, може призвести до підміни, пошкодження, втрати інформації, збоїв в роботі системи чи повної її зупинки. Для банківських компаній подібні проблеми можуть стати важкими в фінансовому, часовому та іміджевому плані.

Виділимо основні завдання будь-якої інформаційної системи:

а) надання доступу до даних тільки для довірених авторизованих клієнтів та можливість оперативно обробити запит;

б) забезпечення цілісності інформації, повної її захищеності та актуальності, неможливості знищення або зміни цієї інформації несанкційованою особою;

в) повна конфіденційність даних в системі.

Для того, щоб вирішити проблеми, описані вище, застосовуються різні методи захисту інформації, такі як реєстрація користувачів, їх ідентифікація та аутентифікація, контроь доступу, протоколювання, створення різних мережевих екранів та криптографія. Один з нових та популярних способів, що забеспечує подібний захист – віртуальна приватна мережа (з англ. VPN Virtual Private Network). З допомогою VPN мережевих систем канали зв'язку створюються прямо у мережі Інтернет. Ця технологія дає клієнтам

можливість об'єднувати різні локальні мережі з різним програмним та апаратним забезпеченням та об'єднувати їх окремі сегменти в одну мережу. Їх головна особливість – шифрування всього поточного трафіку, що і забезпечує необхідну безпеку. Весь трафік моделі OSI, що проходить на канальному рівні шифрується. Це забезпечує захист від зловмисників, що будуть намагатися отримати доступ до інформації. Інкапсуляція в свою чергу не дозволяє нікому з'ясувати, куди буде відправлено повідомлення.

Об'єктом науково-дослідної практики являється банківська віртуальна приватна мережа (технологія VPN).

Предмет дослідження – віртуальна приватна мережа, що об’єднує банки та АТМ і створена для них на основі OpenVPN технології.

Мета дослідження – створити проект банківської комп'ютерної VPN мережі за допомогою OpenVPN технології.

Для того, щоб досягти мети роботи потрібно вирішити наступні задачі:

а) визначити та описати всі питання безпеки банківської мережі. Знайти всі необхідні рішення для VPN мережі;

б) визначити принципи створення та підтримки VPN мережі на основі різного програмного та апаратного забезпечення. Розглянути всі існуючі типи мережі VPN та методи, за допомогою яких їх реалізують. Розглянути вже створені та реалізовані в банках VPN мережі, принципи їх побудови та рішення проблем з їх точки зору. Переглянути переваги та недоліки вже існуючих VPN мереж;

в) розкрити особливості та відмінності даної технології та її організації у середі OpenVPN;

г) розкрити всі особливості та етапи розробки банківської комп'ютерної мережі на основі програмного забезпечення Unix.

# 1 ДОСЛІДЖЕННЯ ПРИНЦИПІВ ТА ОСОБЛИВОСТЕЙ ПОБУДОВИ VPN МЕРЕЖ

## 1.1 Постановка завдання

На сьогоднішній день при нашому рівні розвитку сучасних інформаційних технологій, перевага віртуальних приватних мереж незаперечна. За допомогою віртуальних приватних мереж віддалений користувач має змогу нарівні з користувачами центральної корпоративної мережі користуватися корпоративною мережею. Незважаючи на те, що вони отримують доступ через публічну мережу, клієнти можуть бути аутентиіфковані центральною мережею будь-якої організації.

Без володіння знаннями щодо особливостей технології проектування вдалої і надійної корпоративної VPN неможливо. Цей розділ наводить класифікацію VPN за різними ознаками, розглядає загальні принципи роботи VPN, досліджує існуючі на ринку категорії продуктів і готові рішення в області побудови VPN. Також необхідно зробити обгрунтування вибору OpenVPN як продукту, потрібного для організації корпоративної VPN. Це є важливим завданням на данному етапі.

## 1.2 Віртуальна приватна мережа

Віртуальна приватна мережа (з англ. Virtual Private Network або VPN) – це один із видів комп'ютерних мереж, що застосовує технологію захисту інформації в відкритому Інтернеті, засновану на застосуванні екранування між мережами та захисту трафіку мережі криптографічними методами. Більшість джерел описує цю технологію саме таким визначенням. Дана технологія створена для об'єднання довірених мереж, вузлів і клієнтів між собою через

незахищені та відкриті для всіх мережі. На схемі приведена основна ідея цього визначення (рисунок 1.1)

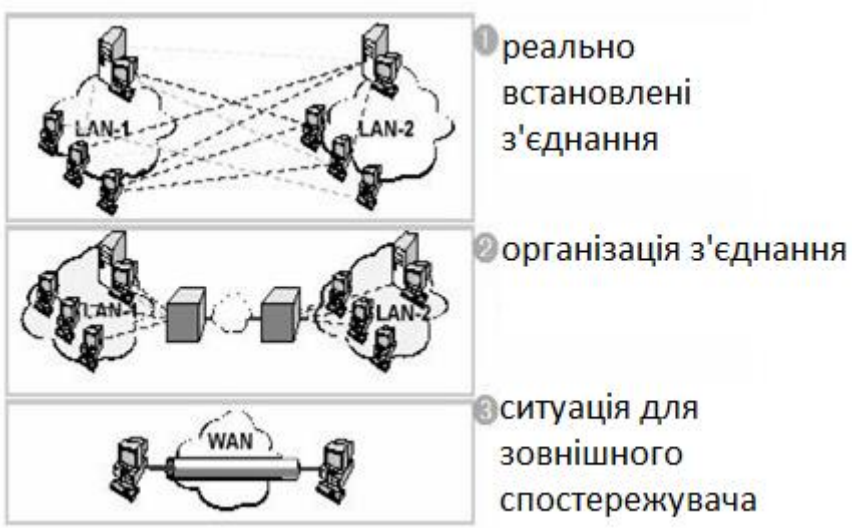


Рисунок 1.1 – Схема віртуальної приватної мережі

Основні функції VPN:

а) зберігає інформацію, що передається у безпеці від зловмисників; криптографічні методи зберігають конфіденційність, цілісність та доступність даних;

б) надійно захищає всі внутрішні сегменти мережі від доступу ззовні; повністю забезпечує тунельованість всього внутрішнього мережевого трафіку за допомогою криптографічного кодування пакетів та адрес передачі в інші пакети, застосуванням екранів між мережами;

в) дає змогу ідентифікувати та аутентифікувати всі суб'єкти та об'єкти, що знаходяться в системі; за допомогою подібного обліку реалізуються технології використання довірених вузлів.

Технологія VPN дозволяє суттєво заощадити на фінансових ресурсах при створенні та обсулуговуванні завдяки тому, що вона використовує замість дорогих захищених каналів мережу Інтернет.

## 1.3 Дослідження принципів роботи VPN

Транспарентний (непомітний для користувача) захист конфіденційності та цілісності повідомлень, що передаються через різноманітні мережі загального користування, такі як Інтернет забезпечується віртуальними приватними мережами (VPN - Virtual Private Network).

Схема VPN представлена на рисунку 1.2.

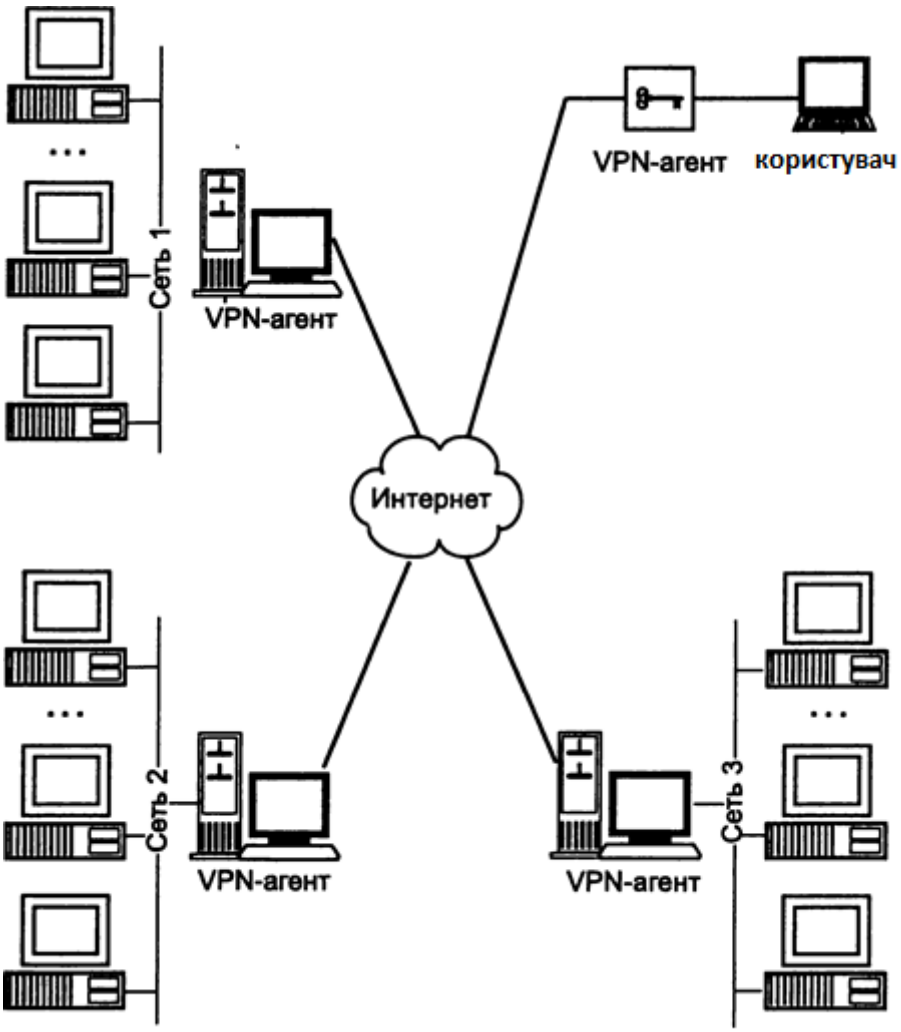


Рисунок 1.2 – Віртуальна приватна мережа

Зазначимо, що VPN – це сукупність мереж, з встановленими на зовнішньому периметрі VPN-агентами.

VPN-агент – це така програма або програмно-апаратний комплекс, що виконує наступні дії:

1. Перед відправленням будь-якого інформаційного пакету (тут і далі будемо розглядати для прикладу IP-пакети):

а) інформація про адресата виділяється з заголовка IP-пакету. Основуючись на політиці безпеки, про яку буде надано додаткові відомості пізніше, для захсту даного пакету обираються захисні алгоритми (у випадку, коли VPN- агент підтримує кілька алгоритмів) та криптографічні ключі до даної інформації. Відправлення пакету може блокуватися, якщо політика безпеки VPN-агента не передбачає відправлення пакету, наділеного певними характеристиками або відправлення IP-пакета даному адресату;

б) формування і додавання імітуючої приставки або ЕЦП в IP-пакет відбуваться за допомогою заданного алгоритму захисту цілісності;

в) зашифровка IP-пакету проводиться після обрання алгоритму шифрування;

г) таким чином, зашифрований IP-пакет через встановлений алгоритм інкапсуляції пакетів переміщать у готовий для передачі IP- пакет, у заголовку якого містяться дані про VPN-агента відправника і VPN-агента адресата, замість відповідної вихідної інформації про відправника та адресата. Це явище визначається, як трансляція мережних адрес (NAT - Network Address Translation);

д) VPN-агенту адресата відправляється пакет. Розмір результуючого пакета може перевищувати MTU (Maximum Transfer Unit - максимальний розмір пакета для конкретної мережевої ділянки). У такому випадку відбувається дроблення пакету та наступне відправлення результуючих пакетів.

2. При прийомі IP-пакета:

а) інформація про відправника знаходиться у заголовка IP-пакету. Якщо згідно з політикою безпеки відправника немає серед дозволених або він невідомий (при прийомі пакету з навмисно або випадково пошкодженим заголовком), тоді обробка пакету не здійснюється і пакет відкидається;

б) відповідно до політики безпеки вибираються алгоритми захисту даного пакету і ключі, за допомогою яких будуть проведені розшифрування пакету і перевірка його цілісності;

в) інформаційна (інкапсульована) частина пакета виділяється і розшифрувується;

г) на основі обраного алгоритму відбувається контроль цілісності пакету. У випадку її порушення пакет відкидається;

д) внутрішньою мережею пакет відправляється адресату відповідно до інформації, яка міститься в його оригінальному заголовку.

VPN-агент може знаходитися безпосередньо на комп'ютері, що захищається. В такому разі з допомогою VPN-агента захищається інформаційний обмін тільки того комп'ютера, на якому він встановлений, проте принципи дії, описані вище, залишаються без змін.

VPN-агент, який захищає локальну обчислювальну мережу (ЛОМ) може поєднуватися з маршрутизатором IP-пакетів, що також має знаходитися на виході з ЛОМ. Такий маршрутизатор називається криптографічним. У якості криптографічного маршрутизатора можна використовувати як звичайний, оснащений спеціальним програмним забезпеченням та апаратурою (наприклад, апаратним шифратором), неспеціалізований комп'ютер, так і спеціалізований маршрутизатор.

Основне правило проектування VPN звучить наступним чином: зв'язок між Інтернетом і захищеною ЛОМ повинен здійснюватися тільки через VPN-агентів, будь-які засоби зв'язку, здатні оминати захисний бар'єр у вигляді VPN-агента, категорично забороняються. Інакше кажучи, потрібно визначити захисний периметр, зв'язок з яким можливо здійснювати тільки через відповідний засіб захисту. Політика безпеки – це набір правил, згідно з якими

налаштовуються захищені канали зв'язку між абонентами VPN. Ці канали зазвичай називаються тунелями, аналогічність з якими проявляється в наступному:

а) вся інформація, передана в рамках одного тунелю, захищається як від модифікації, так і від несанкціонованого перегляду;

б) приховування топології внутрішньої ЛОМ досягається інкапсуляцією IP-пакетів: обмін інформацією між двома захищеними ЛОМ виглядає в Інтернеті як обмін інформацією тільки між їх VPN-агентами, оскільки в цьому випадку всі внутрішні IP-адреси в переданих через Інтернет IP-пакетах не фігурують.

Таким чином, описані вище дії VPN-агентів забезпечують, по своїй суті, функціонування двох основних механізмів: фільтрації інформації і тунелювання.

Формування правил створення тунелів залежить від різних характеристик IP-пакетів; наприклад, протокол IPSec (Security Architecture for IP), основний при побудові більшості мереж VPN, встановлює наступний набір вхідних даних, згідно з яким приймається рішення щодо фільтрації певного IP-пакета і обираються параметри тунелювання:

а) IP-адреса джерела, яка може мати вигляд не тільки виділеної IP-адреси, а й адреси підмережі або діапазону адрес;

б) IP-адреса призначення теж може бути діапазоном адрес, що виділється за допомогою шаблону (wildcard) або маски підмережі;

в) протокол транспортного рівня (наприклад, TCP / UDP);

г) ідентифікатор користувача (одержувача або відправника);

д) номер порту, з якого або на який пакет відправляється.

# 2 ЗАГАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКОЇ МЕРЕЖІ

## 2.1 Постановка завдання

Відповідно до завдання на дипломне проектування, дана робота має на меті конструювання банківської VPN мережі.

Банківська мережа (БМ) - це складна система, яка містить в собі різноманітні компоненти: ПЕОМ, мережеве обладнання, системне і прикладне ПЗ, лінії зв'язку. Банківські мережі зазвичай мають складну топологію і можуть бути розміщені в межах міста, області, держави або материку. Кількість серверів, користувачів і хостів може складати сотні й тисячі. Для того, щоб з'єднати окремі комп'ютери або розподілені локальні мережі в одну банківську мережу, використовуються різні телекомунікаційні засоби: перш за все, мережа Інтернет, супутниковий зв'язок, радіоканали, телефонні канали.

Приклад банківської мережі представлено на рисунку 2.1.


Рисунок 2.1 – Банківська мережа

Серед основних завдань БМ: взаємодія розташованих на різних хостах додатків, а також доступ віддалених користувачів до цих додатків. Для будь-якої банківської структури розвинена інформаційна система – необхідний засіб, що дозволяє їй ефективно впоратися з обробкою потоків інформації, які переміщуються між співробітниками і вживати своєчасних і раціональних заходів для забезпечення конкурентоспроможності компанії.

Основною відмінністю банківської мережі від локальної є те, що мережі, розподілені за територіальним принципом, до яких відноситься і корпоративна мережа, використовують доволі повільні орендовані лінії зв'язку. Тому організація каналів зв'язку є першою проблемою, з якою доводиться стикатися при створенні корпоративної мережі. Одна з основних статей витрат при цьому – це орендна плата за користування каналами, яка зростає швидко у зв’язку зі збільшенням швидкості передачі даних і якості. Таке обмеження принципове, адже усі заходи з мінімізації обсягів переданих даних при проектуванні подібної мережі мають бути вжиті. В іншому випадку обмеження на те, яким чином і які програми займаються обробкою інформації, що передається, не вносяться.

На оренду виділених ліній (навіть високошвидкісних) можна розраховувати у межах одного міста, проте під час переходу до місць, географічно віддалених, оренда каналів стає просто астрономічно дорогою, а їх надійність і якість зазвичай страждають. Для максимально ефективного вирішення такої проблеми використовують загальнодоступні глобальні мережі, такі як Інтернет. Забезпечення каналів зв’язку від найменш віддалених вузлів мережі до офісів у такому випадку цілком достатньо. При цьому завдання з забезпечення доставки інформації поміж вузлами повністю лежить на глобальній мережі. Проте Інтернет має ще одну проблему, крім низької якості і швидкості передачі, – це безпека його користувачів. Саме тому другим найважливішим завданням під час проектування банківської мережі, розподіленої за територіальним принципом, є забезпечення захисту інформації в середині мережі.

Щоб забезпечити максимальну безпеку банківської інформації, потрібно виділити таку інформацію з усієї вільно циркулюючої в мережі, щоб вона мала обмежений доступ, потім виявити можливі ризики, які можуть вплинути на таку інформацію, і, звичайно, визначитися з необхідними захисними методами.

## 2.2 Види інформації, що захищається

Одним із важливих на даному етапі завдань є визначння тієї інформації, яка потребує підвищеної якості захисту. За критерієм необхідності засисту інформації, вона ділиться на наступні групи:

а) з обмеженим доступом;

б) з відкритим доступом.

Відомості будь-якого характеру, які мають відношення до організації, а також є потенційно комерційно цінними для банку, називають комерційною таємницею.

Відповідно до Закону України, будь-які відомості, які мають пряме чи побічне відношення до певної фізичної особи (суб'єкту персональних даних) можуть і мають бути зараховані до персональних даних.

## 2.3 Загрози для безпеки інформації

Інформацію потрібно бергти від від будь-яких видів внутрішніх і зовнішніх загроз.

Загроза в загальному розімінні – це така дія, процес, подія або явище, що потенційно може спричинити збиток банківській власності чи інтересам.

Загроза безпеки в БМ розглядається як подія або дія, що може загрожувати захищеності мережевої інформації.

Під уразливістю БМ розуміють певну особливість системи, яка залишає шанс виникнення загрози для мережі та її подальшої реалізації.

Дія, вчинена зловмисником навмисне та націлена на реалізацію загрози називається атакою. Ця дія виявляється у пошуці будь-яких уразливих сторін БМ і, власне, атакуючих вчинках.

Серед результатів атак можливі наступні загрози для інформації:

а) загроза втрати конфіденційності;

б) загроза цілісності;

в) загроза проблем з доступністю.

За характером дій, які використовуються під час атаки, використовують наступну класиіфкацію:

а) "Чорні ходи" (Backdoors) – атаки, які можуть загрожувати виконанням користувачами несанкціонованих операцій на сервері, що атакується; засновуються на використанні можливостей ПЗ, незадекларованих розробниками;

б) "відмова в обслуговуванні" (Denial of Service, або DoS) – атаки, які використовують помилки, допущені при проектуванні, і дозволяють таким чином закрити доступ до серверу легітимним користувачам;

в) розподілені атаки типу "відмова в обслуговуванні" (Distributed Denial of Service) – випадок, коли велика кількість фіктивних запитів надсилаються на сервер кількома користувачами чи програмами, провокуючи його недоступність для звичайних користувачів;

г) вразлива для потенційних загроз операційна система (OS Sensor);

д) спроби доступу неавторизованих користувачів (Unauthorized Access Attempts).

Програма Nessus, призначена для аналізу безпеки серверів, використовує дещо інший підхід до класифікації атак, на основі принципу "характеру уразливості":

а) "чорні ходи" (Backdoors);

б) помилки в CGI скриптах (CGI abuses);

в) атаки типу "відмова в обслуговуванні" (Denial of Service);

г) помилки в програмах – FTP-серверах (FTP);

д) наявність на комп'ютері сервісу Finger або помилки в програмах, що реалізують цей сервіс (Finger abuses);

є)помилки в реалізації міжмережевих екранів (Firewalls);

ж) помилки, що дозволяють користувачеві, що має термінальний вхід на даний сервер, отримати права адміністратора (Gain a shell remotely);

з) помилки, що дозволяють атакуючому віддалено отримати права адміністратора (Gain root remotely);

и) інші помилки, які не ввійшли в інші категорії (Misc); помилки в програмах - NIS-серверах (NIS);

і) помилки в програмах – RPC-серверах (RPC);

ї) уразливості, що дозволяють атакуючому віддалено отримати будь-який файл з сервера (Remote file access);

й) помилки в програмах – SMTP-серверах (SMTP problems);

к) невикористовувані сервіси (Useless services).

Наведемо нижче звіти по статистиці загроз основних компаній, пов'язаних із захистом від мережевих погроз. Наприклад, згідно зі звітом лабораторії Касперського в 2013 році (наведемо для порівняння з минулим, 2015 роком) протягом року IT – інфраструктура 95% російських організацій як мінімум один раз піддалися зовнішньої атаці.

Основну загрозу становить шкідливе ПЗ (віруси, черв'яки, шпигунські програми і т.п.) - його назвали 71% представників всіх компаній. На другому місці спам-атаки, які відзначили 67% компаній, а трійку лідерів у рейтингу основних загроз замикають фішингові атаки з показником 26% (рис. 2.2).


Рисунок 2.2 – Рейтинг основних зовнішніх загроз

У 2015 році ситуація змінюється. Згідно з інформаційним бюлетенем лабораторії Касперського з аналізу статистики загроз за 2015 рік були виділені наступні тенденції:

– Значно зросла частка рекламного ПЗ в порівнянні з шкідливим. У рейтингу веб-загроз 2015 року лабораторії Касперського представники цього класу програм займають дванадцять позицій в TOP 20. Протягом року рекламні програми і їх компоненти були зафіксовані на 26,1%.

– Зростає частка відносно нескладних програм. Такий підхід дозволяє зловмисникам швидко оновлювати шкідливе ПО, чим і досягається ефективність атак.

– Зростають атаки на платформи Android і Linux: для цих платформ створені і використовуються практично всі види шкідливих програм.

– В ході своєї діяльності кіберкрімінала активно використовує сучасні технології анонімізації – Tor для приховування командних серверів і біткойнів для проведення транзакцій.

У 2015 році у вірусів виросла популярність експлойтів для Adobe Flash Player.

Гістограма кількості заражених комп'ютерів для трьох основних типів шкідливих атак (зловредів, націлених на фінансовий сектор, программ-здирників, програм-шифраторів) приведена на рисунку 2.3.


Рисунок 2.3 – Гістограма кількості заражених комп'ютерів для трьох основних типів шкідливих атак

Протягом 2015 року в рейтингу зловредів, націлених на крадіжку грошей через системи інтернет-банкінгу, на першому місці був Upatre, закачує на комп'ютер жертви троянці – Банкер сімейства, відомого як Dyre / Dyzap / Dyreza. Серед всіх банківських загроз частка атакованих Dyreza користувачів склала більше 40%. Банкер використовує ефективну схему веб-ін'єкцій з метою крадіжки даних для доступу до системи онлайн-банкінгу. У 2015 році відбувся ряд змін і в стані троянців-здирників: в той час як популярність програм-блокерів поступово падає, кількість користувачів, атакованих програмами-шифрувальник за рік зросла на 48,3%. Шифрування файлів замість простого блокування комп'ютера – метод, який в більшості випадків не дає жертві можливості простим способом відновити доступ до інформації. Особливо активно зловмисники використовують шифрувальники в атаках на бізнес-користувачів, які йдуть на оплату викупу куди охочіше, ніж звичайні домашні користувачі.

Також в роботі наведено рейтинг вразливих додатків, який побудований

на основі даних про заблокованих експлойтів, які використовуються зловмисниками і в атаках через інтернет, і при компрометації локальних додатків, в тому числі на мобільних пристроях користувачів.

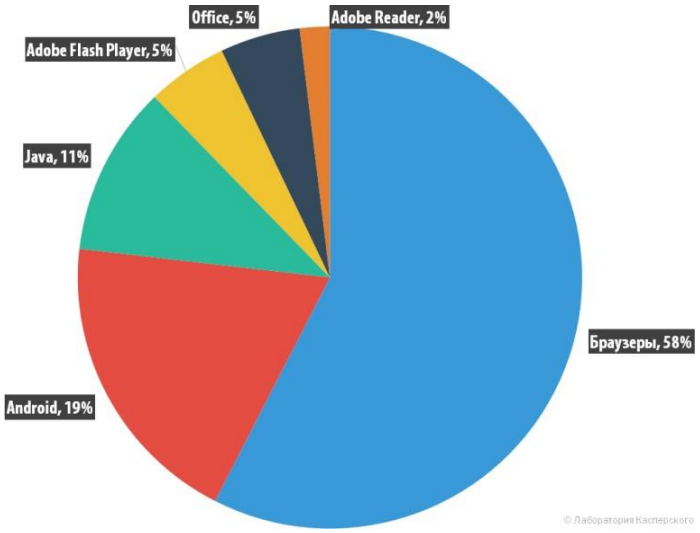


Рисунок 2.4 – Розподіл експлойтів, використаних в атаках зловмисників, за типами атакованих додатків

Серед змін третього кварталу 2015 року від доугого кварталу можна зазначити:

Зростання числа експлойтів для Adobe Flash Player на 2 п.п. Зниження кількості експлойтів для Adobe Reader на 5 п.п.

TOP 20 детектіруемих об'єктів в інтернеті наведено в таблиці 2.1.

Таблиця 2.1– TOP 20 детектованих об'єктів в інтернеті 2015 рік

| | | |
|---|---|---|
| 1 | Malicious URL | 53,63 |
| 2 | AdWare.JS.Agent.bg | 16,71 |
| 3 | Adware.Script.Generic | 7,14 |
| 4 | Trojan.Script.Generic | 6,30 |
| 5 | Trojan.Script.Iflamer | 3,15 |
| 6 | Trojan.Win32.Generic | 1,52 |
| 7 | AdWare.Win32.SoftPulse.heur | 1,31 |
| 8 | AdWare.Js.Agentbt | 1,09 |
| 9 | Adware.Win32.OutBrowse.heur | 0,84 |
| 10 | Trojan-Downloader.Win32.Generic | 0,63 |
| 11 | AdWare.NSIS.Vopak.heur | 0,46 |
| 12 | Exploit.Script.Blocker | 0,46 |
| 13 | Trojan-Downloader.JS.Iframe.diq | 0,3 |
| 14 | AdWare.Win32.Amonetize.aqxd | 0,3 |
| 15 | Trojan-Downloader.Win32.Genome.tqbx | 0,24 |
| 16 | AdWare.Win32.Eorezo.abyb | 0,23 |
| 17 | Hoax.HTML.ExtInstall.a | 0,19 |
| 18 | Trojan-Clicker.HTML.Iframe.ev | 0,17 |
| 19 | AdWare.Win32.Amonetize.bgnd | 0,15 |
| 20 | Trojan.Win32.Invader | 0,14 |

Таким чином, список загроз і вразливостей з кожним роком сильно видозмінюється. Тому проблема забезпечення безпеки функціонування автоматизованих систем є актуальною. Відповідно базової моделі загроз, створеної ФСТЕК була проведена класифікація загроз, що виникають при міжмережевій взаємодії (рисунок 2.5).

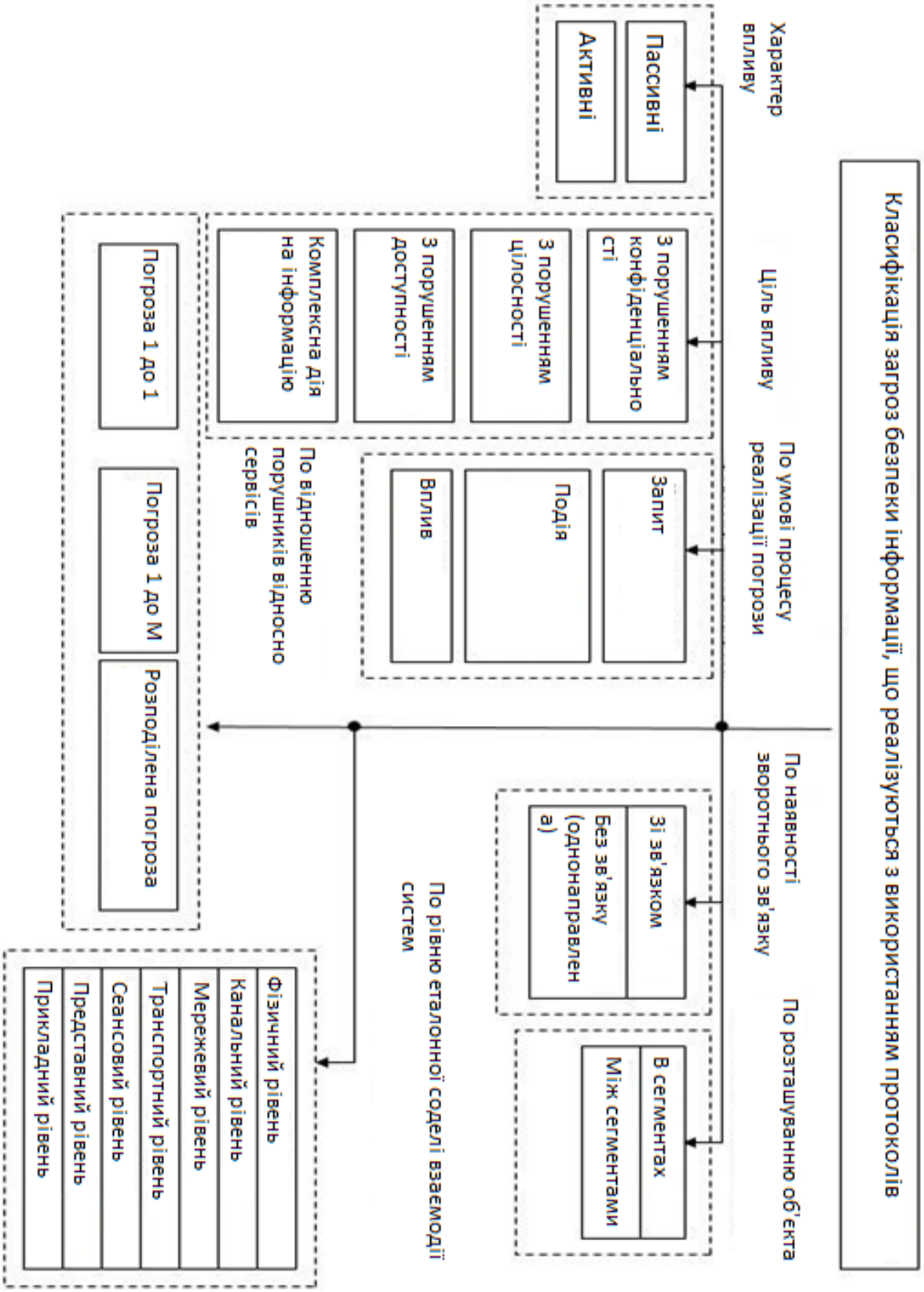


Рисунок 2.5 – Класифікаційна схема загроз з використанням протоколів міжмережевої взаємодії

З урахуванням проведеної класифікації можна виділити сім мережевих погроз, які найбільш часто реалізуються.

П1. Аналіз мережевого трафіку (рисунок 2.6). Аналізом мережевого трафіку прийнято вважати прослуховування мережі за допомогою спеціальних програм – сніфферів. Ці програми дозволяють переглянути всі порти мережі та відкриту інформацію, що можна буде використати. Використовуються для вилучення ідентифікаторів доступу чи іншої інформації, що передається у відкритому вигляді.

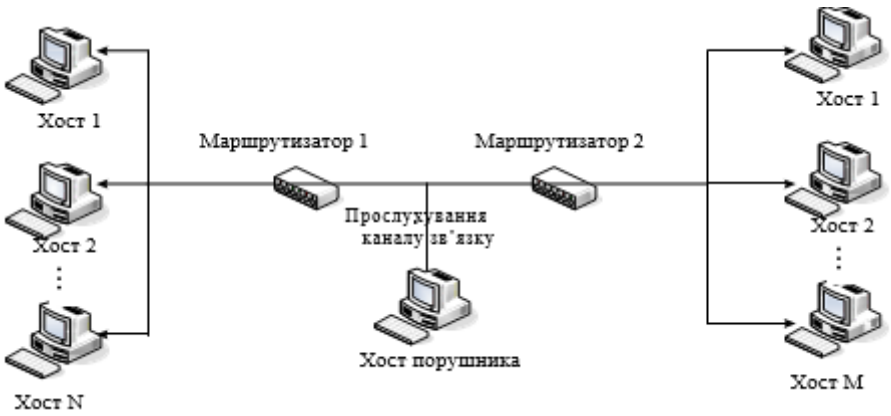


Рисунок 2.6 – Схема реалізації загрози «Аналіз мережевого трафіку»

П2. Сканування мережі. Людина або програма, що сканує мережу передає запити мережевих служб хостів з конфіденційною інформацією і аналує отримані відповіді з метою виявлення такої інформації: типу протоколів, на яких працюють порти мережевих служб, отримання та вивчення принципу створення ідентифікаторів з'єднань, виявлення активних мережевих сервісів, для підбору унікальних паролів та логінів клієнтів мережі.

П3. Загроза виявлення пароля. На даний момент є велика кількість програмного забезпечення, що намагається отримати паролі користувачів від класичних методів типу бруту (простого перебору) та перебору по словникам до використання програм, що будуть перехоплювати паролі або підмінювати

оригінальний сайт чи систему та перехоплювати пакети.

П4. Підміна довіреного об'єкта мережі. Цей метод дозволить зловмиснику видавати себе за офіційний зареєстрований довірений об’єкт мережі та передавати по каналах зв'язку будь-які повідомлення від його імені з метою присвоїти інформацію або отримати доступ до мережі. Дана загроза реалізується в системах, де використовуються нестійкі алгоритми ідентифікації і аутентифікації користувачів, хостів і т.д. У вигляді довіреного об’єкта може виступати будь-який об’єкт мережі – комп'ютер, маршрутизатор, міжмережевий екран і т.п., легально підключений до сервера.

П5. Нав'язування помилкового маршруту мережі. Дана загроза реалізується двома способами: внутрисегментного або міжсегментного нав'язування. Можливість реалізації даної загрози обумовлена недоліками, алгоритмів маршрутизації (проблемами ідентифікації мережевих керуючих пристроїв). Дана загроза дозволяє потрапити на хост або в мережу зловмисника, де потім можна отримати доступ до операційного середовища технічного засобу. Загроза можлива через недоліки протоколів маршрутизації (RIP, OSPF, LSP) і протоколів керування мережею (ICMP, SNMP), що дозволяють при несанкціонованому використанні вносити зміни в маршрутно-адресні таблиці.

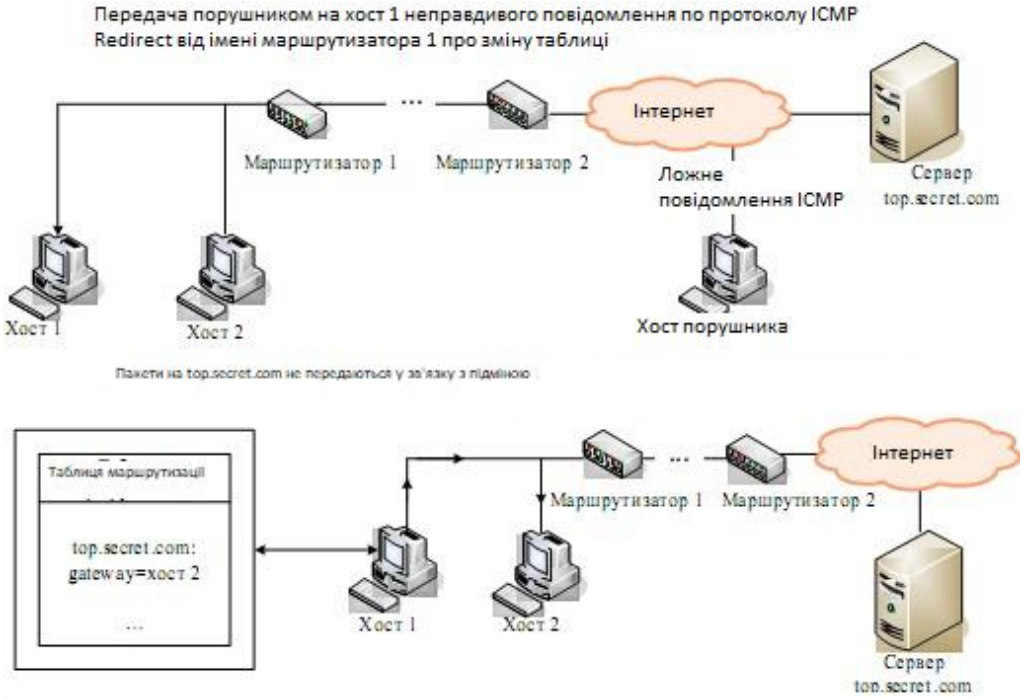


Рисунок 2.7 – Схема реалізації загрози «внутрисегмене нав'язування помилкового маршруту»


Рисунок 2.8 – Схема реалізації загрози «міжсегментного нав'язування помилкового маршруту»

П6. Впровадження помилкового об'єкта мережі. Загроза полягає в перехопленні порушником пошукового запиту і видачі помилкової відповіді замість легального користувача. Реалізація загрози призведе до зміни маршрутно-адресних даних і решти потоку інформації, що буде проходити через помилковий об'єкт мережі.

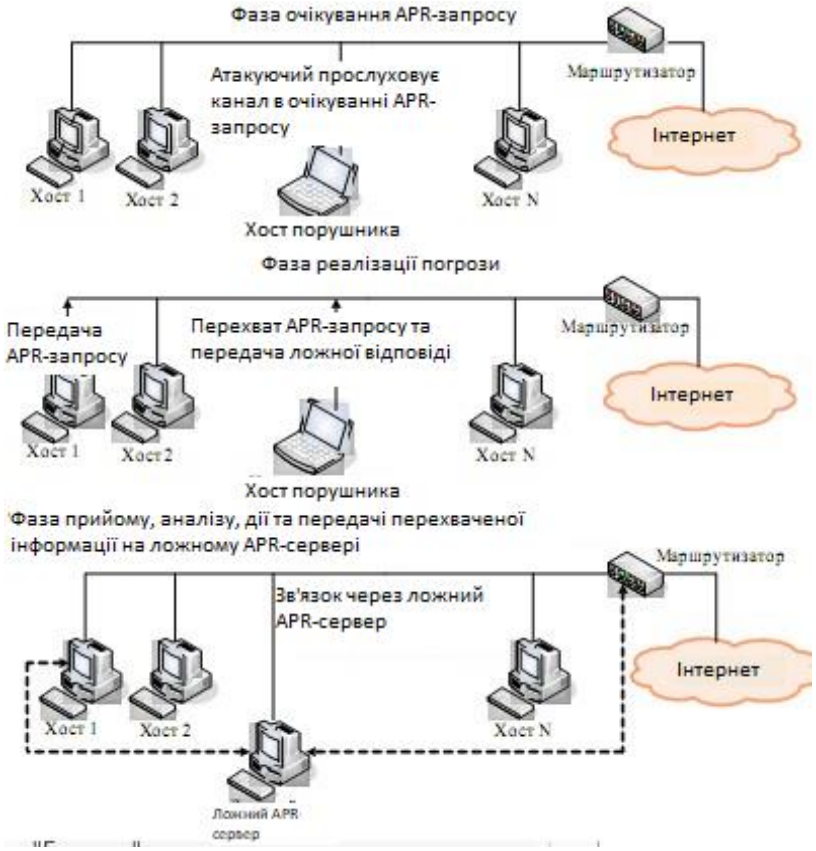


Рисунок 2.9 – Схема реалізації загрози «Впровадження помилкового ARP-сервера»

П7. Відмова в обслуговуванні. Даний тип загрози заснований на недоліках мережевого програмного забезпечення, на його слабких місцях, які дозволяють порушнику створювати такі умови, в яких операційна система виявляється не в змозі обробляти пакети.

П8. Віддалений запуск додатків. Дана загроза полягає в прагненні запустити на атакуємий хост різні шкідливі програми, попередньо впроваджені: віруси, програми-закладки,

«Мережеві шпигуни». Головна мета таких програм – порушення цілісності конфіденційності та доступності інформації, а також повний контроль за роботою атакованого хоста, несанкціонований запуск прикладних програм користувачів для несанкціонованого отримання необхідних порушнику даних.

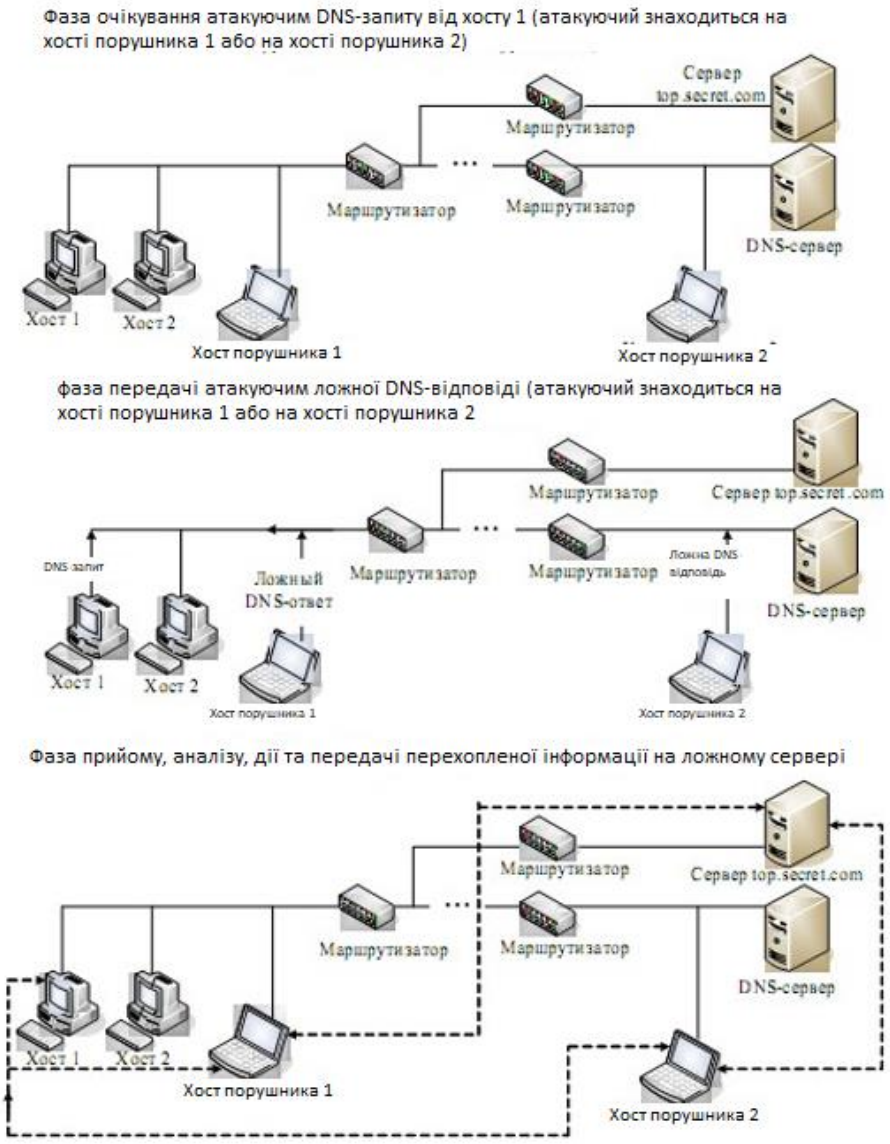


Рисунок 2.10 – Схема реалізації загрози «Впровадження помилкового DNS- сервера» шляхом перехоплення DNS-запиту

Можливі наслідки реалізації загроз різних класів представлені в таблиці 2.2.

Таблиця 2.2 – Можливі наслідки реалізації загроз різних классів

| № | Тип атаки | Можливі наслідки |
|---|---|---|
| 1 | Сканування мережі | Знаходження використаних протоколів та відкритих портів мережевих служб, логінів та паролів користувачів мережі, знаходження активних мережевих сервісів |
| 2 | Атака паролями | Всі можливі дії з аккаунтом користувача |
| 3 | Підміна довіреного об’єкта мережі | Зміна пункту призначення повідомлень, можливість доступу до мережі та її ресурсів, можливість підміни інформації |
| 4 | Нав’язування штучного маршруту | Несанкційована модифікація маршрутів та адрес, нав’язування штучних повідомлень, можливість аналізу та модифікації повідомлень |
| 5 | Аналіз мережевого трафіка | Доступ до індентифікаторів паролів та іншої інформації |
| 6 | Впровадження штучного об’єкта мережі | Нав’язування штучної інформації, можливість несанкціованого доступу до ресурсів мережі, перехват та перегляд трафіка |
| 7 | Часткове навантаження на ресурси | Зменшується продуктивність мережі, її програм, повідомлень та знижується пропускна здатність каналів |

| | | |
|---|---|---|
| | Повне навантаження на ресурси | Неможливість передачі повідомлень внаслідок неможливості отримання доступу до середи обміну даними, неможливість роботи з програмами або даними в мережі |
| | Порушення логічних зв’язків між об’єктами, атрибутами чи даними | Неможливість передачі повідомлень чи роботи з мережевими програмами внаслідок відсутності доступу до будь-яких баз даних в мережі, неможливість входу під своїм ім’ям та паролем |
| | Використання програмних помилок | Порушення дієздатності мережі |
| 8 | Розсилка вірусного програмного забезпечення з деструктивним кодом | Порушення цілісності мережі та втрата інформації |
| | Переповнення буфера програми чи сервісу | Порушення конфіденціальності та втрата інформації |
| | За допомогою віддаленого управління системою | Можливість отримання доступу до елементів контролю системою |

Крім мережевих атак для розподілених систем, підключених до загальних мереж характерний ще ряд загроз, а саме – загрози несанкціонованого доступу до конфіденційної інформації, що обробляється на АРМ, пов'язані з безпосереднім доступом до захищених даними (представлені на рисунку 2.7 або засобам обробки цих даних, а також реалізовані ззовні (представлені на рисунку 2.6).

Тож, інформація, що передається завжди потребує надійного та ресурсоємного захисту, що не дасть зловмисникам до неї дістатися.

На рисунках 2.11 та 2.12 детально наведені всі можливі погрози несанкційованого доступу (НСД)

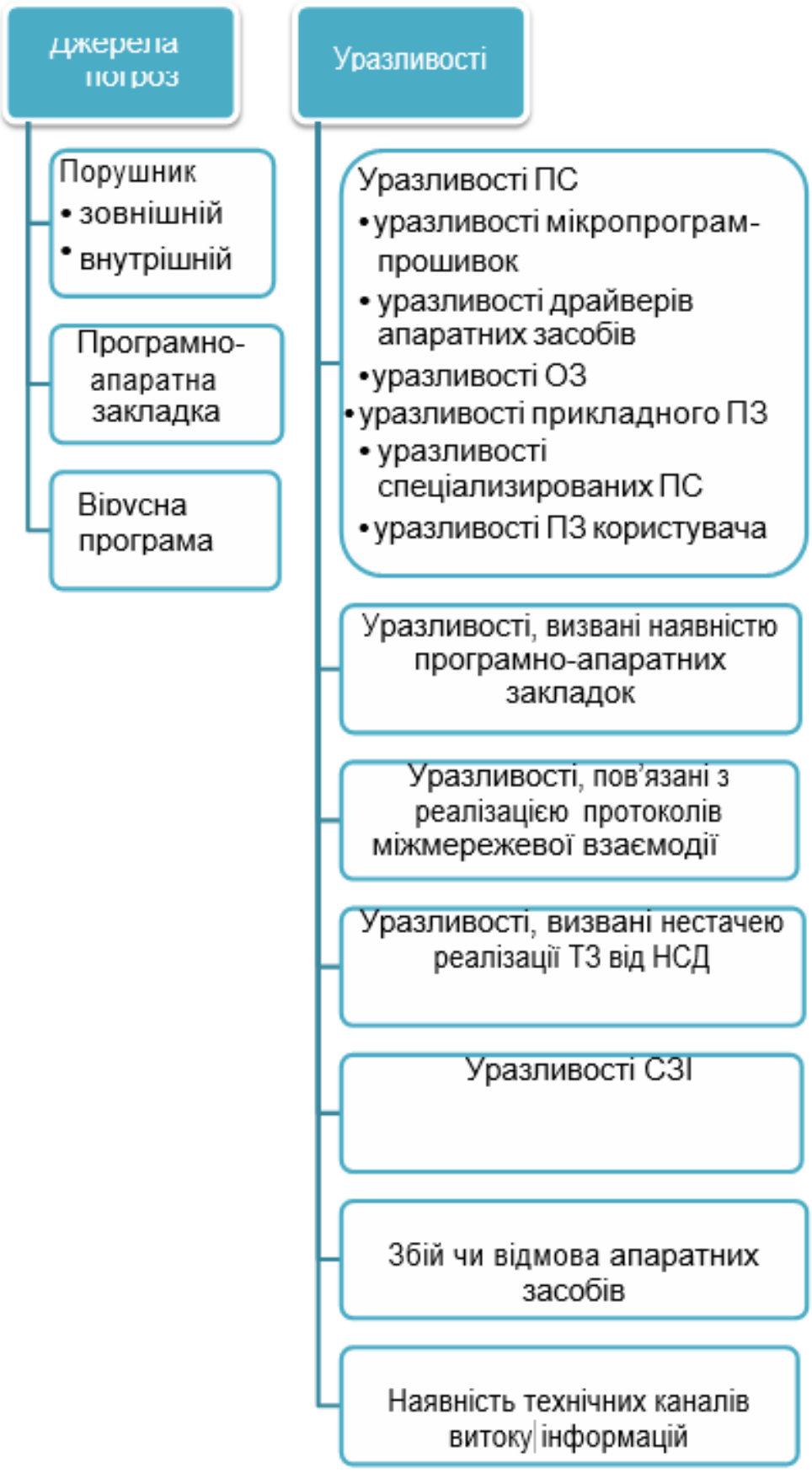


Рисунок 2.11 – Загрози НСД (початок)

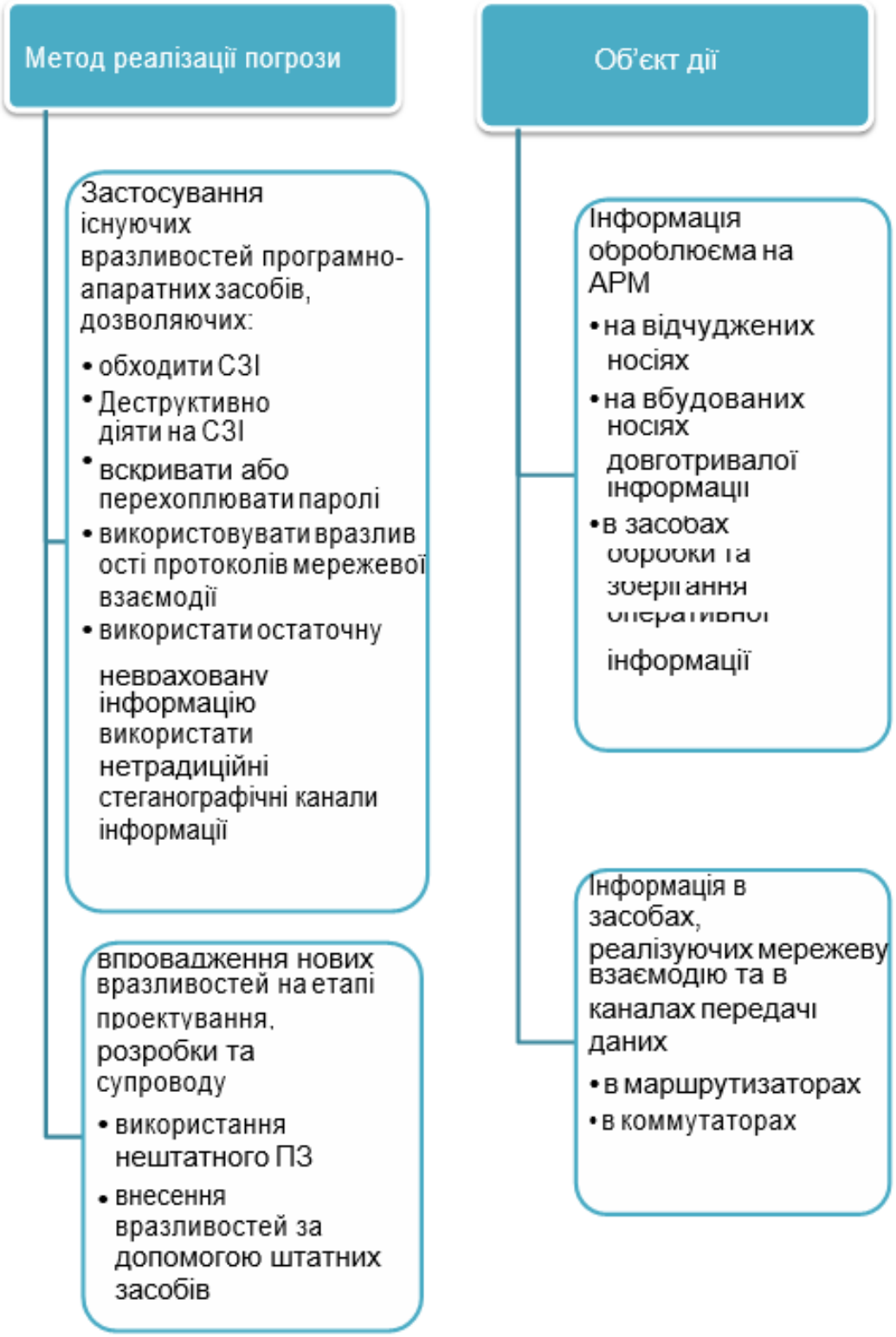


Рисунок 2.12 – Загрози НСД (продовження)

## 2.4 Існуючі положення в області забезпечення ІББ

Існують окремі вимоги до захисту даних в банківських установах:

а) для всіх технічних засобів повинно бути встановлене ліцензійне ПЗ;

б) повинні проводитись перевірки всіх об'єктів інформації щодо відповідності вимогам по захищеності;

в) необхідно скласти список програмних засобів, допустимих до застосування, а всі інші програмні засоби повинні бути заборонені, а їх встановлення бути неможливим без дозволу людей з високим рівнем довіри;

г) все ПЗ та антивіруси, що знаходяться на банківських пристроях повинно постійно оновлюватись і мати доступ до оновлень, також необхідно проводити регулярні перевірки комп'ютерів на предмет шкідливого або несанкціовано встановленого ПЗ;

д) унеможливлення потрапляння шкідливих програм до пристроїв банку через мережу, профілактика і перевірка мережевих ресурсів на віруси;

е) заражене ПЗ, що потрапило в систему повинно потрапити в карантин та досліджене.

Метою політики інформаційної безпеки має бути надійний захист інформаційних ресурсів банку від зовнішніх та внутрішніх загроз завдяки впровадженню та ефективному управлінню системою інформаційної безпеки. Основним завданням політики інформаційної безпеки є захист інформаційних активів від загроз, а саме:

а) виявлення та мінімізація потенційних загроз інформаційній безпеці;

б) захист інформаційних активів організації;

в) забезпечення безпеки та конфіденційності інформації про клієнтів;

г) забезпечення стабільної та ефективної діяльності банківської установи. Основним принципом інформаційної безпеки, якого доцільно дотримуватися банку, є підтримання таких властивостей інформації, як:

конфіденційність – захист від несанкціонованого ознайомлення;

цілісність – захист від несанкціонованого спотворення, руйнування або знищення;

доступність – захист від несанкціонованого блокування [6, с. 7].

Серед основних об'єктів політики інформаційної безпеки банківських установ виокремимо наступні:

– фінансові ресурси;

– національна й іноземна валюта, банківські операції та угоди банку, коштовності, фінансові документи;

– персонал банку;

– керівництво і вищий менеджмент банку, особи, які мають доступ до конфіденційної інформації, банківської та комерційної таємниці, інші працівники банку;

– матеріальні засоби;

– апаратні засоби інформаційних технологій, носії даних, будівлі, приміщення, меблі, транспорт тощо;

– сервісні ресурси та підтримуюча інфраструктура;

– обслуговуючі засоби обчислювальної техніки, енергопостачання, забезпечення необхідних умов експлуатації, тощо;

– програмне забезпечення;

– прикладне, системне чи сервісне програмне забезпечення тощо, яке використовується співробітниками банківської установи для роботи з системами і клієнтами;

– інформаційні ресурси;

– будь-яка інформація банку, що обробляється та зберігається в банківській установі (бази даних, файли, документи) [7, с. 20].

Джерелами загроз інформаційній безпеці банку можуть бути як зовнішні, так і внутрішні. До внутрішніх загроз безпеці банківської установи можна віднести втрату інформації, некомпетентність персоналу, розголошення інформації, знищення інформації, викривлення інформації, викрадення конференційної інформації, витік інформації; до зовнішніх – модифікацію змісту, порушення конфіденційності, порушення логічної цілісності, порушення прав власності на інформацію, порушення фізичної цілісності тощо [8, с. 122]. Фахівці виокремлюють наступні напрями щодо забезпечення інформаційної безпеки в контексті впровадження політики інформаційної безпеки банківської установи:

– перелік законодавчих, регуляторних, нормативних вимог;

– затвердження переліку відомостей, що містять інформацію з обмеженим доступом;

– встановлення правил доступу до інформаційних ресурсів та програмно-технічних комплексів;

– визначення критичних бізнес-процесів/банківських продуктів/ програмно-технічних комплексів;

– забезпечення надання доступу (у тому числі віддаленого) до інформації, її контролю та захисту;

– проведення політики ідентифікації та автентифікації ресурсів;

– політика криптографічного захисту інформації;

– політика «чистого екрана» та «чистого столу»;

– проведення внутрішнього аудиту та вдосконалення системи управління інформаційної безпеки.

## 2.5 Вибір засобів міжмережевого захисту

### 2.5.1 Міжмережеві екрани

Міжмережеві екрани являються одним з найрозповсюдженіших засобів, що забезпечують безпеку кордонів будь-яких комп'ютерних мереж, підтримують цілісність периметра мережі в точці між внутрішньою локальною мережою та Інтернетом (або іншою мережою, до якої немає довіри). У великій кількості технічної літератури також можна зіткнутися з термінами firewall або брандмауер.

МЕ створений для захисту автоматизованих систем за допомогою фільтрації всього потоку пакетів, що надходять з Інтернету до нього. Весь вміст мережевого пакету аналізується на основі заданих правил по ряду критеріїв, після цього пакет може отримати дозвіл до проходження в локальну мережу. Правила реалізуються за допомогою послідовної фільтрації. Тобто, для того, щоб пройти крізь МЕ пакет повинен послідовно пройти перевірку в кожному з його фільтрів.

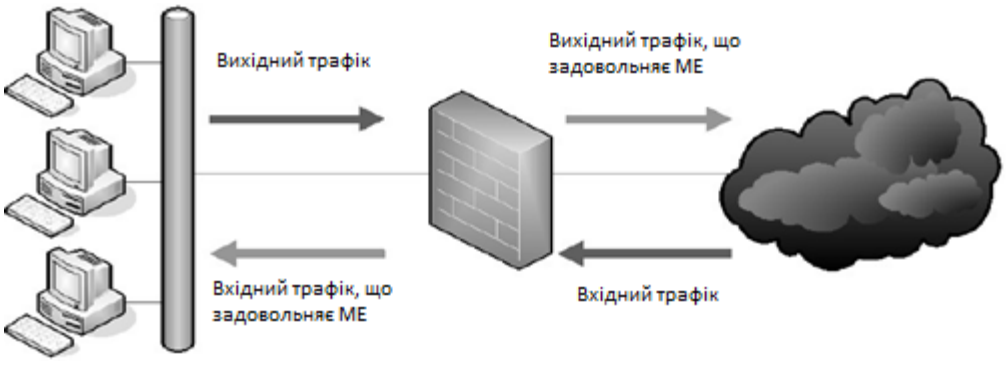


Рисунок 2.13 – Контроль периметра мережі МЕ (захищається мережа зліва)

### 2.5.2 Системи виявлення атак

Система виявлення атак (СВА) являє собою систему захисту, що призначена для виявлення і, по можливості, попередження дій, що погрожують безпеці внутрішньої інформаційної системи з боку Інтернету.

Розрізняють такі методи виявлення атак:

а) сигнатурний аналіз;

б) виявлення аномалій;

в) різноманітні комбінації методів вище.

У випадку використання сигнатурного аналіза мається на увазі, що сценарій атаки відомий. При проведенні атаки аналіз мережевого трафіку здатний виявити її. Таким чином, для того, щоб знайти атаку нам потрібно знайти логіку в її послідовності. Для такого пошуку потрібно правильно описати атаку, знайшовши ланцюг правил (умов), що її описує. Для виявлення атак по сигнатурі необхідно мати базу сигнатур відомих атак. Недоліком цього методу являється нездатність чинити спротив новим невідомим методам атак з боку зловмисників.

Другий спосіб захисту від атак заснований на виявленні аномалій в поведінці системи. Такий пошук атаки заснований на тому, що при атаці в системі знайдеться щось нелогічне. Під час атаки на систему, вона виходить з свого звичного стану, що фіксується самою системою і, частіше всього, видається адміністраторам у вигляді попередження. Метод виявлення аномальної поведінки має три головні правила.

– поведінка системи має бути описана таким чином, щоб її зміни в поведінці легко та автоматично визначались;

– потрібно створити алгоритм, що зможе стежити за всіма процесами в системі та буде здатний фіксувати зміни в її поведінці;

– відстеження змін поведінки відбувається з допомогою математичних механізмів та методів. На їх основі створюється механізм прийняття рішення щодо протидій атаці.

Переваги методу виявлення аномалій – можливість виявлення нових атак. Але є один суттєвий недолік: новоутворена система може виявляти атаки навіть там, де їх немає.

### 2.5.3 Віртуальні приватні мережі

Virtual Private Network VPN – (віртуальна приватна мережа) – це захищена комп'ютерна мережа, що комбінує два надійних засоби захисту інформації: застосування міжмережевого екранування та захист мережевого трафіку за допомогою криптографії. VPN об'єднує довірені мережі, вузли і користувачів через недовірені відкриті мережі. Основна ідея даного визначення приведена на схемі (рисунок 2.14).

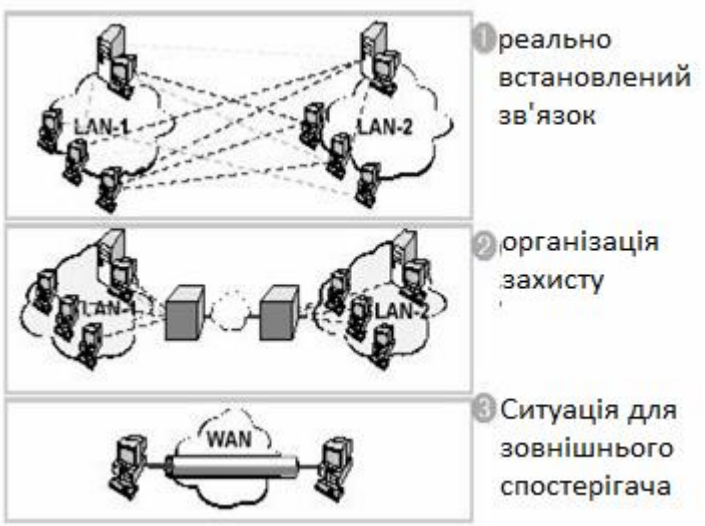


Рисунок 2.14 – Схема VPN

Функції VPN:

– забезпечує збереження трьох властивостей інформації: конфіденційності, доступності та цілісності за допомогою криптографічних методів;

– забезпечує надійний захист внутрішніх сегментів мережі, що

захищається від доступу ззовні. Тобто забезпечує тунельованість внутрішнього трафіку шляхом упаковки переданих пакетів в інші пакети і використанням криптографічних засобів і міжмережевих екранів;

– забезпечує ідентифікацію та аутентифікацію суб'єктів і об'єктів системи. Таким чином реалізується технологія використання довірених вузлів.

Так як VPN використовує мережу Інтернет замість виділених захищених каналів, компанія зможе суттєво зекономити та не витрачати свої ресурси на прокладення захищених закритих зв’язків.

# 3 ПРОЕКТУВАННЯ БАНКІВСЬКОЇ VPN СИСТЕМИ

## 3.1 Постановка завдання

Для того, щоб створити банківську приватну систему в даній роботі використовувалася мережева система на основі технології OpenVPN. В даному розділі поставлена задача розглянути особливості створення системи в технології OpenVPN і порівняти цю систему з вже реалізованими аналогами технологіями, а саме:

– розглянути структуру та окремі частини програмного комплексу OpenVPN;

– розглянути всі головні функції та їх можливості у програмному комплексі OpenVPN;

– описати принцип створення та основи функціонування OpenVPN-мережі;

– описати процес завантаження та налаштування програми Open VPN на будь-яку з типових банківських систем.

## 3.2 Опис додатку OpenVPN

Для того, щоб вирішити проблему побудови та підтримки віртуальних мереж на початку 2002 року була створена перша версія технології OpenVPN, яка будувалася як новий інструмент з відкритим вихідним кодом і використовувалась тільки для створення VPN мереж типу site-to-site що працювали на основі протоколів типу SSL / TLS або протоколу з розподіленими ключами. Технологія OpenVPN створює так званий VPN тунель, що захищає інформацію при передачі даних через один TCP / UDP порт в незахищену відкриту мережу Інтернет.

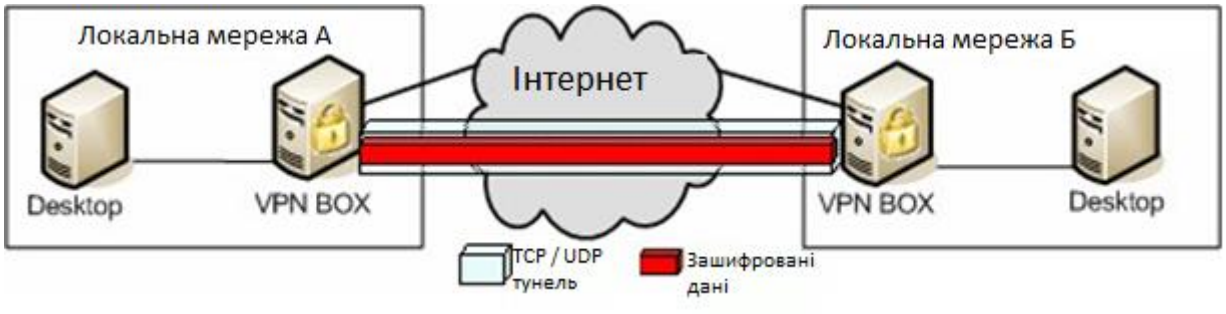


Рисунок 3.1 – Принцип VPN тунеля

Основні переваги технології OpenVPN – легкість в інсталяції, можливість встановлення в різні системи та зручне налаштування. Технологія OpenVPN може бути встановлена на такі розповсюджені платформи, як: Linux, Windows 2000 / XP / Vista, OpenBSD, FreeBSD, NetBSD, Mac OS X і Solaris, за умови шо Linux системи будуть працювати на ядрі 2.4 або новіше. Для того, щоб встановити та налаштувати програму в різних системах необхідно провести однакові маніпуляції. Технологія OpenVPN працює з архітектурою типу клієнт / сервер. Додаток необхідно встановити на всі елементи VPN мережі, при цьому один з вузлів повинен бути сервером, а інші клієнтами.

Додаток OpenVPN створює між вузлами TCP або UDP тунелі, в яких дані, що проходять між ними, зашифровуються. UDP 1194 вважається стандартним портом в OpenVPN, але додаток дає можливість змінити порт на будь-який інший, зручний для адміністратора UDP або TCP порт. Починаючи з версії 2.0 OpenVPN сервер може використати один і той же порт для кількох різних вузлів.

Додаток OpenVPN створює систему, що може працювати в двох режимах. Якщо використовувати режим розподілених ключів, буде створений один ключ, який буде зберігатись у відправляючій та приймаючій сторонах для шифрування і розшифрування. В такому випадку сам ключ повинен бути секретним, тобто для його передачі

повинна використовуватись симетрична криптографія. Проблема даного режиму полягає в передачі ключа на приймаючу сторону.

Для того, щоб не ризикувати інформацією та запобігти виникненню цієї проблеми необхідно використати Інфраструктуру Відкритих Ключів (PKI). Суть у тому, що кожен вузол зберігає два ключі: відкритий ключ, що зберігається у всіх та закритий ключ, доступ до якого є тільки у власника. Подібна структура використовується у OpenSSL, інтегрованому в OpenVPN, для аутентифікації окремих VPN вузлів для передачі зашифрованих даних.

Таблиця 3.1– Переваги двох режимів

| Режим OpenVPN | Розподілені ключі | SSL |
|---|---|---|
| Шифрування: | Симетричний | Асиметричний / Симетричний |
| Реалізація: | Простіше | Складніше |
| Швидкість: | Швидко | Повільно |
| Завантаження процесора: | Менше | Більше |
| Обмін ключами: | Так | Ні |
| Спроба оновити ключі: | Ні | Так |
| Аутентифікації вузлів: | Ні | Так |

В режимі SSL (асиметричного шифрування) використання OpenVPN більш безпечне та надійне. Ций протокол SSL (Secure Sockets Layers) був розроблений компанією “Netscape” ще в 90-х роках. Загалом було створено та випущено версію протоколу v2 (1994) та v3 (1995). У 2001 IETF купила і оновила патент на цю розробку. В цей же назва SSL була змінена на TLS (Transport Layer Security) (RFC 2246).

Сама абревіатура SSL в більшості випадків використовується при

використанні і SSL і TLS протоколів.

SSL вирішує дві основні проблеми:

– аутентифікує сервер і клієнта за допомогою засобів Інфраструктури Відкритих Ключів (PKI);

– шифрує повідомлення між клієнтом і сервером та створює нові з'єднання.

SSL працює між транспортним рівнем і рівнем додатку та буде шифрувати дані на рівні програми.

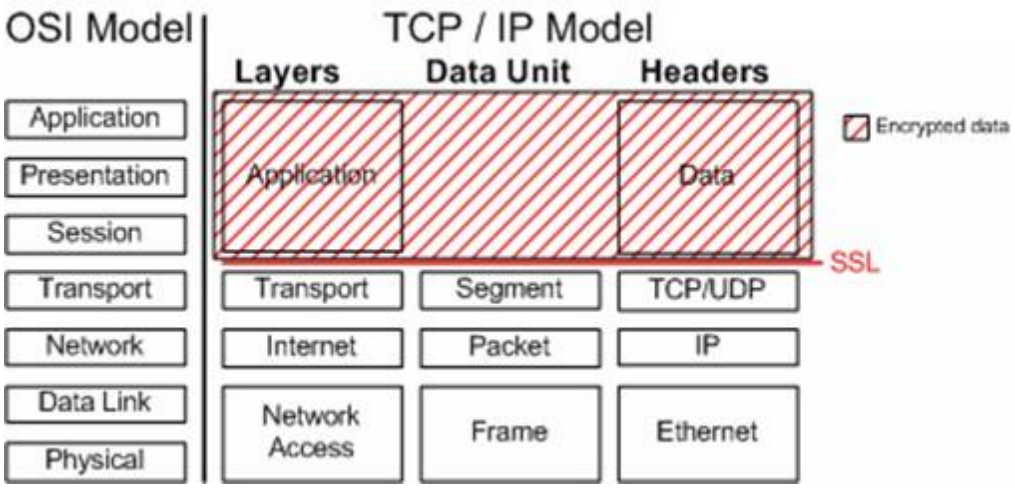


Рисунок 3.2 – Розташування протоколу SSL в моделі OSI

Раніше технологію SSL використовували тільки специфічні додатки типу HTTP, однак на сьогоднішній день вона може працювати в сфері забезпечення безпечного та стабільного з'єднання через мережу Інтернет або створення та підтримки шифрованих тунелів (VPN).

Розрізняють два окремих типи VPN:

– клієнт-сервер (або віддалений доступ) VPN, де клієнт використовує стандартний web браузер такий як Firefox, Google Chrome, тощо;

– Site-to-site, створює та утримує зв’язок за допомогою спеціального програмного забезпечення, такого як OpenVPN.

Робота технології SSL відбувається в 4 основних етапи, зазначених в

таблиці 3.2.

Таблиця 3.2– Чотири етапи SSL / TLS

| | |
|---|---|
| SSL Handshake: | Визначається метод шифрування для передачі даних |
| SSL Change Cipher Spec: | Створення і передача ключа між клієнтом і сервером на цю сесію |
| SSL Alert: | Доставка повідомлень SSL про помилки між клієнтом і сервером |
| SSL Record: | Передача даних |

Передача пакетів всередині локальної мережі і VPN показана на рисунку 3.3.

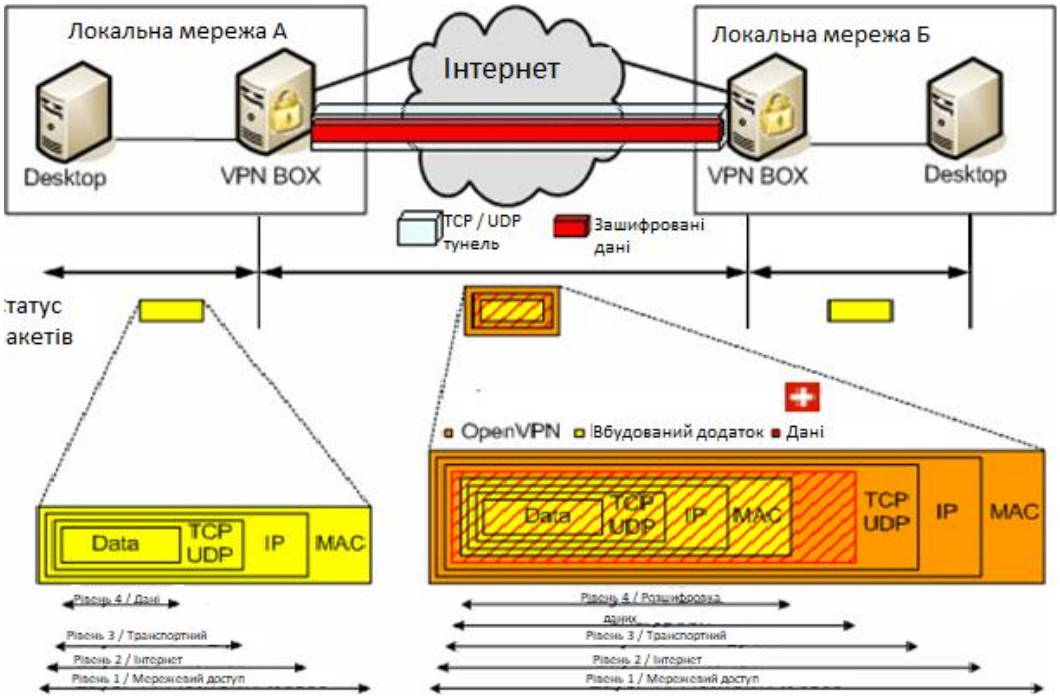


Рисунок 3.3 – Схема передачі пакетів

Для того, щоб шифрувати дані і аутентифікувати користувачів OpenVPN використовує технологію OpenSSL, яка на даний момент являється найкращим безкоштовним рішенням і поширюється з відкритим вихідним кодом. Технологія OpenSSL – це інструмент, що має в собі:

- бібліотеки шифрування;
- інструменти для роботи з командним рядком;
- SSL бібліотеки.

Бібліотеки шифрування створюють та обробляють велику кількість алгоритмів шифрування, таких як:

- симетричні алгоритми: DES, AES, 3DES, Blowfish і інші;
- сертифікати: x509;
- хеш-функції: MD5, HMAC.

## 3.3 Склад програмного комплексу OpenVPN

Мережа OpenVPN складається з таких основних компонентів:

а) Центр засвідчення. Він виконує такі функції, як видача підписаних сертифікатів що потребують вузли мережі VPN. Також центр засвідчення надає вузлам підписаний собою сертифікат, що дає змогу перевірити засвідчення, якщо буде така необхідність. Також центр контролює список відкликаних сертифікатів CRL;

б) Сервер OpenVPN. На комп’ютер, що повинен бути сервером встановлюється спеціальне програмне забезпечення, що буде контролювати створення криптозахищених тунелів у незахищеній мережі з метою забезпечення передачі зашифрованого трафіка між різними клієнтами VPN мережі безпечно;

в) Клієнт OpenVPN. На комп’ютер, або, у випадку з банками, АТМ встановлюється програмне забезпечення клієнта. Всі елементи системи, які хочуть бути підключеними до захищеного каналу передачі даних з сервером

мають працювати з ПЗ, що підтримує додаток та бути налаштованими на з'єднання з сервером. Клієнти також можуть передавати дані між собою по захищеному каналу, що створює сервер, якщо він налаштований на це;

г) Сертифікати (відкриті ключі) X.509 – це публічні ключі, які обробляє центр засвідчення. Сертифікати необхідні для зашифровування та розшифровування даних. Для підтвердження справжності сертифікату центр засвідчення дозволяє провести ідентифікацію сторони, що відправляє зашифровані пакети. Вузол мережі створює файл запиту на сертифікат і відправляє його на вузол, що відправив йому запит. На приймаючому вузлі сертифікат перевірюється та підписується. Підтверджений приймаючим вузлом сертифікат відправляється назад на відправляючий вузол мережі OpenVPN;

д) Секретні ключі, що створюються та зберігаються на кожному комп'ютері в мережі OpenVPN. Ці ключі являються набором цифр, що необхідні для розшифрування даних. Їх створює додаток на вузлах мережі OpenVPN і відправляє з файлом запиту на сертифікат;

е) Список відкликаних сертифікатів CRL – це частина сертифікатів, не верифікованих або втрачених центром засвідчення. Даний список постійно редагується та доповнюється у ньому. Для того, щоб відключити одного з клієнтів мережі, достатньо перевести його сертифікат в цей список. Якщо в будь-якому з вузлів система знайде недовірений сертифікат, оновлений список CRL відразу ж буде перенесений на сервер OpenVPN;

є) Файл Діффі-Хелмана. Створюється в системі для того, щоб зловмисники з ключем не змогли отримати доступ та розшифрувати дані, що були записані до моменту викрадення. Створюється і працює тільки на сервері OpenVPN;

ж) Ключ HMAC. Створюється для перевірки цілісності та справжності даних, що передаються. Ций ключ здатен фільтрувати вхідний потік даних від DoS-атак і флуду. Працює на сервері OpenVPN.

## 3.4 Проектування корпоративної VPN мережі

### 3.4.1 Структура корпоративної мережі

Припустимо, що наше завдання – об’єднання в єдину мережу центрального відділення банку, 2 його віддалених відділень та окремого банкомату через мережу Інтернет за допомогою технології OpenVPN.

В центральному відділенні банку і у окремого банкомату в якості маршрутизаторів виступає виділений сервер під операційною системою Centos 5. У відділеннях стоять hardware маршрутизатори. На всіх серверах встановлена типова для цих задач операційна система MS Windows 2003 R2.

Уявімо структуру проектованої банківської мережі у вигляді, як це показано на рисунку 3.4.

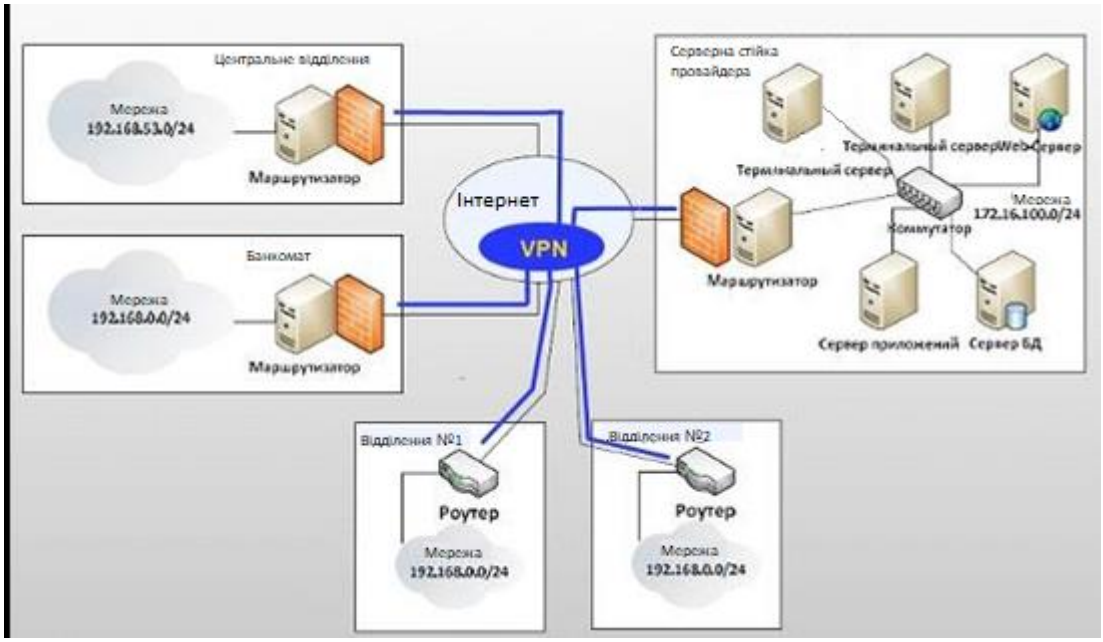


Рисунок 3.4 – Проектована банківська мережа

### 3.4.2 Встановлення OpenVPN на Centos 5

Особливості встановлення OpenVPN на Unix-подібні системи на відміну від простої установки на версії Windows полягає в послідовній конфігурації файлів. Крім того, при встановленні додатку на системи Windows OpenVPN дасть використати графічний інтерфейс встановлюючої програми. Не має різниці, на яку саме Unix-подібну систему ви бажаєте встановити OpenVPN – етапи встановлення мало чим відрізняються один від одного.

Для початку нам потрібно об'єднати в одну банківську мережу відділення банку, банкомат і сервера у провайдера. Для того, щоб це зробити нам потрібно створити та налаштувати захищені канали – тунелі між маршрутизаторами, до яких підключені комп’ютери, АТМ, або інші пристрої. Підключати кожен комп'ютер окремо не обов’язково.

В нашому випадку ми маємо 3 маршрутизатора, які треба налаштувати через операційну систему ОС CentOs. Для того, щоб пакети передавались до мережі Інтернет та повертались з неї використаємо технологію маршрутизації NAT і налаштуванням правил в таблиці iptables.

Для зручності задамо назву кожному з маршрутизаторів:

а) центральне відділення: Center;

б) банкомат: ATM;

в) колокація (сервера у провайдера): Colo;

г) відділення №1: loc1;

д) відділення №2: loc2.

Адреси, маски та шлюзи маршрутизаторів представлені в таблицях 3.3-3.5:

Таблиця 3.3– Center

| Мережа | Інтерфейс | IP адрес | Маска | Шлюз |
|---|---|---|---|---|
| Інтернет | eth2 | 213.182.175.230 | 255.255.255.252 | 213.182.175.229 |
| Локальна | eth1 | 192.168.53.250 | 255.255.255.0 | - |

Таблиця 3.4– ATM

| Мережа | Інтерфейс | IP адрес | Маска | Шлюз |
|---|---|---|---|---|
| Інтернет | eth2 | 79.142.87.206 | 255.255.255.252 | 79.142.87.211 |
| Локальна | eth1 | 192.168.0.1 | 255.255.255.0 | - |

Таблиця 3.5– Colo

| Мережа | Інтерфейс | IP адрес | Маска | Шлюз |
|---|---|---|---|---|
| Інтернет | eth2 | 195.2.240.68 | 255.255.255.252 | 195.2.240.60 |
| Локальна | eth1 | 172.16.100.8 | 255.255.255.0 | - |

CentOS (Community Enterprise Operating System) – один з дистрибутивів Linux, побудований на Red Hat Enterprise Linux компанією Red Hat і працюючий з ним. CentOS за допомогою програми yum скачує та встановлює оновлення з репозиторіїв. Таким чином налаштування та оновлення програми робиться з віддаленого OpenSSH сервера на маршрутизаторах і клієнта putty. Першим проведемо налаштування маршрутизатора Colo. Цей маршрутизатор являється  OpenVPN сервером в нашого банку.

Пакет OpenVPN не встановити за допомогою стандартного репозиторія, тому нам потрібно підключити та налаштувати додатковий репозиторій rpmforge (лістинг 3.1):

Лістинг 3.1 – Налаштування rpmforge

colo> rpm -Uhv
http://apt.sw.be/redhat/el5/en/x86_64/rpmforge/RPMS//rpmforge-release- 0.3.6-1.el5.rf.x86_64.rpm

Ця команда використовує rpm пакет сховища для скачування та встановлення. Як тільки команда буде виконана, ми зможемо використовувати стандартний пакет OpenVPN, який ми встановимо (лістинг 3.2):

Лістинг 3.2 – Встановлення Open VPN

Colo> yum install OpenVPN

OpenVPN встановлюється. Далі, коли процес виконання команди закінчиться, необхідно згенерувати основний сертифікат сервера, всі сертифікати та ключі клієнтів, сертифікат і ключ сервера, tls ключ.

Для цього ми повинні відкрити конфігураційний каталог OpenVPN і створити в ньому каталог для наших майбутніх ключів і ще один каталог під конфігураційні файли клієнтів (лістинг 3.3):

Лістинг 3.3 – Створення каталогу keys

*colo> cd /etc/openvpn colo> mkdir keys*
*colo>mkdir*
*ccd*

Наступним кроком завантажимо змінні, що потрібні для генерації ключів в пам'ять і почнемо генерувати сертифікат для авторизації

(лістинг 3.4):

Лістинг 3.4 – Сертифікат для авторизації

colo>./vars colo>./build-ca

Generating a 1024 bit RSA private key

.....+++++

..+++++

writing new private key to 'ca.key'

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

# Країна

Country Name (2 letter code)

[US]:UA

# Провінція

State or Province Name (full name)

[CA]:KH

# Город

Locality Name (eg, city)

[SanFrancisco]:KH

# Назва

Oganization Name (eg, company) [Fort-Funston]:server

# Відділ

Organizational Unit Name (eg, section) []:server

# Назва сервера OpenVPN

Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:server

Name []:server

Email Address [me@myhost.mydomain]:

Створюємо окремий сертифікат X.509 для серверу (лістинг 3.5):

Лістинг 3.5 – Сертифікат X.509

colo> ./build-key-server server

# Країна

CountryName(2lettercode)[US]:UA

# Провінція

State or Province Name (full name) [CA]:KH

# Город

Locality Name (eg, city) [SanFrancisco]:

KH # Назва

Organization Name (eg, company)

[x]:server # Відділ

Organizational Unit Name (eg, section) []:server

# Ім’я сервера OpenVPN

CommonName(eg,yournameoryourserver'shostname)[]:server #

Почтова адреса

Email Address[root@localhost]:

Please enter the following 'extra' attributes tobesentwithyourcertificaterequest

# Пароль

A challenge password

[]:123456789

# Назва

An optional company name []:server

Наступним кроком ми повинні вирішити питання щодо підписування сертифіката, погоджуємося. Створюємо новий ключ для center (лістинг 3.6):

Лістинг 3.6 – Створення ключа

colo> ./build-key-server office Generating a 1024 bit RSA private key

.....++++++

.....++++++

writing new private key to 'client.key'

---

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank

For some fields there will be a default value, If you enter '.', the field will be left blank.

---

Country Name (2 letter code) [US]: UA

State or Province Name (full name) [CA]: KH Locality Name (eg, city) [SanFrancisco]: KH Organization Name (eg, company) [server]:company Organizational Unit Name (eg, section) []:center

CommonName(eg,yournameoryourserver'shostname)[]:office Email Address [root@localhost]:

Please enter the following 'extra' attributes tobesentwithyourcertificaterequest

A challenge password[]:123456789 An optional company name[]:center

Таким чином ми повинні створити ключі для нашого банкомату та 2х відділень банку.

Створимо окремий ключ Діффі Хельмана, що буде займатись передачею ключів по незахищеному каналу, також створимо окремий ключ для tls-аутентифікації (лістинг 3.7):

Лістинг 3.7 – Створення ключів Діффі Хельмана та tls ключа

```
colo> ./build-dh

colo> openvpn --genkey --secret keys / ta.key
```

В результаті проведення цього налаштування ми повинні побачити у каталозі keys такі створені файли:

а) ca.crt – основний сертифікат, що зберігається на сторонах і клієнта і сервера;

б) dh1024.pem – ключ Діффі Хельмана, цей файл зберігається тільки на серверній стороні;

в) server.crt – Основний сертифікат сервера, зберігається тільки у нього;

г) server.key – ключ сервера, зберігається тільки в ньому і являється секретним файлом;

д) center.crt, ATM.crt, loc1.crt, loc2.crt – сертифікати кожного з клієнтів, знаходяться в пристроях клієнтської бази;

е) center.key, ATM.key, loc1.key, loc2.key – секретні ключі, що знаходяться в комп'ютерах клієнтів;

є) ta.key – TLS-ключ, знаходиться і на сервері і в клієнтів.

Таким чином, сервер оперує файлами ca.crt, dh1024.pem, server.crt, server.key, ta.key, а клієнти оперують файлами ca.crt, dh1024.pem і мають свої сертифікати та ключі.

Після того, як ми закінчимо з генерацією ключів, можемо перейти до налаштування самого сервера та його клієнтів. Для цього ми повинні створити та наповнити файл конфігурації server.conf (лістинг 3.8) таким чином:

Лістинг 3.8 – Конфігурація Server.conf

```
# Порт на якому буде працювати наш сервер
port 5000
# Протокол сервера
udp proto udp
# Номер та тип пристрою, що ми використовуємо
dev tun0
# Підключаємо головний сертифікаційний файл
ca /etc/openvpn/keys/ca.crt
# Підключаємо сертифікат, що знаходиться у сервера
 cert /etc/openvpn/keys/server.crt
```

# Підключаємо файл, в якому знаходиться ключ сервера

key /usr/local/etc/openvpn/keys/server.key

# Підключаємо файл Діффі Хельмана

dh /usr/local/etc/openvpn/keys/dh1024.pem

# Налаштуємо IP-адрес нашого сервера та вкажемо його маску підмережі в VPN

server 10.10.200.0 255.255.255.0

# Наступний крок – налаштувати маршрути для клієнтів та дати їм маску підмережі для забезпечення зв’язку з OpenVPN сервера

# Colo

push "route 172.16.100.0 255.255.255.0"

# Center

push "route 192.168.53.0 255.255.255.0"

# ATM

push "route 192.168.0.0 255.255.255.0"

# Вказуємо місце збереження налаштованих файлів, де зберігаються IP-адреси клієнтів

client-config-dir ccd

# Додамо маршрути зв’язку між сервером та клієнтом

route 10.10.200.0 255.255.255.0

# Center

route 192.168.53.0 255.255.255.0

# ATM

route 192.168.0.0 255.255.255.0

# Додамо можливість спілкування між клієнтами по віртуальному IP. Без цієї команди клієнти мали б зв’язок тільки з сервером.

client-to-client

# Підключаємо функцію TLS аутифікації,  tls сервер та посилаємо файл ключа tls

tls-auth keys / ta.key 0

# Вказуємо максимальний час очікування підключення

tls-timeout 120

# Задаємо шифрувальний алгоритм

auth MD5

# Підключаємо пакетне шифрування cipher

BF-CBC

# Встановимо перевірку підключення, що буде оновляти статус кожні 10 секунд. При відсутності підключення протягом 2х хвилин з’єднання буде закрите

keepalive 10 120

# Підключаємо вбудований архіватор

comp-lzo

# Задаємо назви клієнтам та групам клієнтів, з якими буде працювати мережа OpenVPN

user nobody

group nobody

# Задаємо 2хетапну аутентифікацію ключів після їх отримання

```
persist-key
        # Задаємо утримання і перепідключення TUN \ TAP пристроїв
        persist-tun
        # Створюємо log файли
        status /var/log/openvpn/openvpn-status.log
        log /var/log/openvpn/openvpn.log
        # Налаштуємо режим відладнення
        verb 3
```

Після цього ми можемо створити файли для налаштування клієнтської сторони. Заходимо в каталог / Etc / openvpn / ccd на сервері та створюємо в ньому файли center, ATM, loc1, loc2 (де ім'я файлу - ім'я, на яке видавався сертифікат) з таким змістом:

Лістинг 3.9 – Конфігурація клієнтських файлів

```
center
ifconfig-push 10.10.200.2 10.10.200.1
iroute 192.168.53.0 255.255.255.0
ATM
ifconfig-push 10.10.200.3 10.10.200.1
iroute 192.168.53.0 255.255.255.0
loc1
ifconfig-push 10.10.200.4 10.10.200.1
```

loc2

ifconfig-push 10.10.200.5 10.10.200.1

Налаштування, наведені вище дають заданим клієнтам можливість користуватися сертифікатами, власні віртуальні ip адреси, підключення до шлюза 10.10.200.1 і задають їм маршрут через захищений шифром тунель до мережі VPN.

На цьому ми закінчуємо з налаштуванням сервера, запускаємо додаток OpenVPN:

colo> service openvpn start

Якщо всі налаштування виставлені правильно, то ми зможемо отримати доступ до віртуального tun пристрою:

colo> ifconfig tun0

tun0 Link encap: UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

inet addr: 10.10.200.1 P-t-P: 10.10.200.2 Mask: 255.255.255.255

UP POINTOPOINT RUNNING NOARP MULTICAST MTU 1500 Metric: 1

RX packets: 9 errors: 0 dropped: 0 overruns: 0 frame: 0 TX packets: 24 errors: 0 dropped: 0 overruns: 0 carrier: 0 collisions: 0 txqueuelen: 100

Якщо доступ до віртуального пристрою не був отриманий, ми маємо помилки в файлах конфігурації. Створені нами логи допоможуть швидко усунути ці помилки.

Тепер, коли наш сервер запрацював, необхідно налаштувати приймаючі сторони. Всі конфігураційні файли налаштовуються однаково, тому покажемо налаштування на одному прикладі. На маршрутизаторах center і ATM встановлюємо OpenVPN.

Після цього створимо файл конфігурації client.conf (лістинг 3.10):

Лістинг 3.10 – Файл конфігурації Client.conf

```
dev tun
proto udp
remote 195.2.240.68 #(реальный ip сервера)
port 5000
client
resolv-retry
infinite ca keys/ca.crt
cert
keys/client.crt key
keys/client.key tls-
client
tls-auth
keys/ta.key 1 auth MD5
cipher BF-CBC
ns-cert-type
server comp-lzo
persist-key
persist-tun
# Далі ми додамо маршрут за сервером до мережі. В конфігураційному
файлі відділень ций рядок не потрібен
up /etc/openvpn_up.sh
status /var/log/openvpn/openvpn-status.log
log /var/log/openvpn/openvpn.log
verb 3
```

Для зручності створимо скрипт openvpn_up.sh що буде додавати

маршрут автоматично:

#! / Bin / sh

/ Sbin / route add -net 172.16.100.0 netmask 255.255.255.0 gw 10.10.200.1 tun0

Це все, що потрібно для налаштування OpenVPN. Перенесемо ці конфшгураційні файли на center і ATM. Запускаємо OpenVPN на них. При виникненні помилок нам так само як і в сервері допоможуть log файли.

Коли на кожній з машин система запрацює, нам необхідно виконати останній крок: включити трансляцію адрес (NAT), бо без неї пакети від клієнтської машинине зможуть піти від сервера в мережу Інтернет і не будуть прийняті назад. Включити NAT нам допоможе наступна команда:

colo> iptables -t nat -A POSTROUTING -s 10.10.200.0/24 -o eth1 -j MASQUERADE

Відтепер всі 3 мережі зможуть побачити одна одну. Залишилось підключити наші віддалені відділення. На комп'ютерах в цих відділеннях встановленя операційна система Windows XP. За допомогою графічного установлювача встановлюємо OpenVPN з офіційного сайту. Після установки заходимо в папку config в кореневій папці програми та копіюємо наші ключі і файл конфігурації loc1 або loc2. Запускаємо і перевіряємо.

## 3.5 Висновок

Створення банківської системи передачі даних на основі OpenVPN в мережі Інтренет є не дуже складним завданням. Для того, щоб розгорнути VPN мережу ми повинні створити локальні мережі, в яких буде доступ до Інтернету, дистрибутив OpenVPN, що ми можемо встановити на різні операційні системи, і людина, яка зможе його налаштувати. Клієнт і сервер мають мати один дистрибутив для того, щоб все працювало корректно. Налаштування OpenVPN є встановленням і редагуванням конфігураційних файлів, створенням ключів шифрування і сертифікатів. Клієнт та сервер повинні провести майже однакові міри для налаштування.

# 4. АВТОМАТИЗАЦІЯ НАЛАШТУВАННЯ БАНКІВСЬКОЇ VPN МЕРЕЖІ

## 4.1 Постановка завдання

Необхідно створити програму, що надасть можливість автоматичного створення файлів конфігурації для серверів та клієнтів VPN. Для того, щоб створити таку програму було використане середовище C++. В даному розділі були показані особливості написання автоматичної системи створення конфігураційних файлів, що будуть мати в собі всі необхідні для роботи налаштування і будуть вимагати найменш можливого втручання з боку користувача програми. Для того, щоб це зробити, необхідно вирішити декілька питань, а саме:

– розглянути методи, що дозволяють оперувати файлами в C++;

– написати адаптивний цикл, що зможе створювати велику кількість конфігураційних файлів;

– надати можливість взіємодії користувача з програмою;

– перевірити працездатність такої системи та оцінити її практичність.

## 4.2 Опис програмного пакету MS Visual Studio 2012

Microsoft Visual Studio – лінійка продуктів компанії Microsoft, що включають інтегроване середовище розробки програмного забезпечення і ряд інших інструментальних засобів. Дані продукти дозволяють розробляти як консольні додатки, так і додатки з графічним інтерфейсом, в тому числі з підтримкою технології Windows Forms, а також веб-сайти, веб-додатки, веб-служби як в рідному, так і в керованому кодах для всіх

платформ, підтримуваних Windows, Windows Mobile, Windows CE, .NET Framework, Xbox, Windows Phone .NET Compact Framework і Silverlight.

Visual Studio включає в себе редактор вихідного коду з підтримкою технології IntelliSense і можливістю найпростішого рефакторінга коду. Вбудований відладчик може працювати як відладчик рівня вихідного коду, так і відладчик машинного рівня. Решта має інструменти, які включають в себе редактор форм для спрощення створення графічного інтерфейсу додатку, веб-редактор, дизайнер класів і дизайнер схеми бази даних. Visual Studio дозволяє створювати і підключати сторонні додатки (плагіни) для розширення функціональності практично на кожному рівні, включаючи додавання підтримки систем контролю версій вихідного коду (як, наприклад, Subversion і Visual SourceSafe), додавання нових наборів інструментів (наприклад, для редагування і візуального проектування коду на предметно-орієнтованих мовах програмування) або інструментів для інших аспектів процесу розробки програмного забезпечення (наприклад, клієнт Team Explorer для роботи з Team Foundation Server).

Microsoft Visual C ++ (MSVC) – інтегроване середовище розробки додатків на мові C ++, розроблене корпорацією Microsoft і поставляється або як частина комплекту Microsoft Visual Studio, або окремо у вигляді безкоштовного функціонально обмеженого комплекту Microsoft Visual Studio Community Edition (раніше Visual C ++ Express Edition).

Visual C ++ підтримує перелік додатків як на Managed C ++ і C ++ / CLI, так і на звичайному C ++, і тим самим дозволяє генерувати код як для платформи .NET Framework, так і для виконання в середовищі «чистої» Windows. В цьому відношенні Visual C ++ є унікальним серед інших мовних засобів, що надаються середовищем Visual Studio, оскільки ні Visual Basic .NET, ні Visual J # не здатні генерувати код для чистого Win32, на відміну від попередніх версій (Visual Basic і Visual J ++ відповідно).

## 4.3 Використані бібліотеки

Для того, щоб створювати файли та оперувати ними були використані дві бібліотеки.

Перша бібліотека, що використовувалась при розробці – це бібліотека string.

Бібліотека string – це стандартна бібліотека рядків C ++, що включає в себе підтримку двох основних типів рядків:

– std :: basic_string – шаблонний клас, призначений для управління рядками будь-яких символьних типів;

– std :: basic_string_view (C ++ 17) – клас, що не змінює рядок, призначений тільки для зчитування.

Рядки з завершаючим нулем – масиви символів, що завершуються спеціальним символом null.

Шаблонний клас std :: basic_string узагальнює управління і зберігання послідовностей символів. Створення, управління і видалення рядків проводиться зручним набором функцій-членів і допоміжних функцій.

Кілька спеціалізацій std :: basic_string представлені для часто використовуваних типів:

Таблиця 4.1– Заголовки <string>

| Тип | Опис |
|---|---|
| std :: string | std :: basic_string <char> |
| std :: wstring | std :: basic_string <wchar_t> |
| std :: u16string | std :: basic_string <char16_t> |
| std :: u32string | std :: basic_string <char32_t> |

Шаблонний клас std :: basic_string_view представляє легкий об'єкт, який дає доступ тільки на читання рядка або частини рядка, використовуючи інтерфейс схожий з std :: basic_string.

Друга важлива для коректної роботи програми бібліотека – це бібліотека fstream.

fstream (скорочення від «FileStream») – заголовок зі стандартної бібліотеки C ++, що включає набір класів, методів і функцій, які надають інтерфейс для читання / запису даних з / в файл. Для маніпуляції з даними файлів використовуються об'єкти, звані потоками («stream»).

Функції, включені в даний файл, дозволяють зчитувати з файлів як побайтово, так і блоками, і записувати так само. У комплект включені всі необхідні функції для управління послідовністю доступу до даних файлів, а також безліч допоміжних функцій.

Це кореневі функції бібліотеки, що не увійшли ні в один з основних класів. Вони використовуються досить часто і можуть бути застосовні до всіх об'єктів потоків в кожному з класів.

rdbuf. Всі об'єкти fstream можуть бути асоційовані з об'єктом буфера файлів filebuf. Щоб зіставити об'єкт класу fstream з об'єктом буфера, використовують функцію rdbuf (без аргументів). Об'єкт буфера надає набагато

більші можливості по управлінню даними в файлі, ніж стандартні функції підкласів fstream.

open (). Цим методом можна відкрити заданий файл, зіставивши його з одним з об'єктів потоку [1]. Залежно від переданих аргументів, файл може бути відкритий для читання, для запису (або для повної, або для додавання даних), як бінарний, або як текстовий файл.

is_open (). Функція, що визначає, чи відкритий у даний момент файл, з яким підтверджено певний об'єкт потоку. Повертає булеве значення. Використовується в основному для запобігання помилок доступу при спробі відкрити файл, який вже використовується. Не має аргументів.

close (). Функція закриває файл, тобто припиняє доступ до нього, таким чином звільняючи його для інших функцій або програм.

Бібліоека fstream має такі основні класи:

– ios_base «InputOutputStream_Base», базовий клас всієї ієрархії класів потоків. Містить загальні функції, типи і класи, що в основному представляють собою прапори (індикатори). Ці прапори використовуються функціями підкласів fstream і можуть бути визначені за допомогою функцій ios_base;

– ios «InputOutputStream», основний підклас, разом з ios_base, що визначає всі інші підкласи бібліотеки потоків. Містить функції-прапори форматування і обробки помилок, а також деякі функції, успадковані від ios_base;

– ifstream «InputFileStream», організовує читання даних з файлу. Клас, функції якого використовуються для читання файлів;

– ofstream «OutputFileStream», організовує запис даних в файл. Клас, який використовується для запису даних в файл.

## 4.4 Результат розробки

В результаті роботи з кодом була створена Win32 програма, що дозволяє людині без необхідного досвіду створити всі конфігураційні файли для серверу та клієнту. Код програми наведений в додатку Б. Програма виглядає досить просто і представлена на рисунку 4.1.

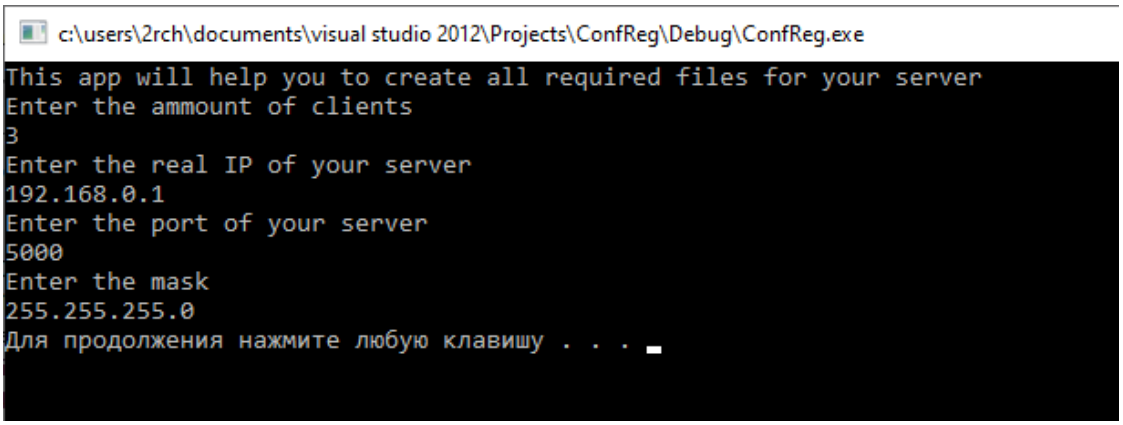


Рисунок 4.1 – Вікно програми

Перш за все в програмі створюється файл server.conf. Ций файл має в собі налаштування самого серверу та видані для клієнтів IP адреси. Людина, що використовує програму повинна ввести кількість клієнтів, IP адресу сервера, його порт та маску самостійно. В результаті роботи програми створений конфігураційний файл серверу має такий вигляд:

Лістинг 4.1 – Файл server.conf

```
port 5000
udp proto udp
dev tun0
```

```
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/server.crt
key /usr/local/etc/openvpn/keys/server.key
dh /usr/local/etc/openvpn/keys/dh1024.pem
server  192.168.0.1 5000
push 'route 172.16.100.0 5000'
push 'route 192.168.53.0 5000'
push 'route 192.168.0.0 5000'
client-config-dir ccd
route 10.10.200.0 5000
route 192.168.53.0 5000
route 192.168.0.0 5000
client-to-client
tls-auth keys / ta.key 0
tls-timeout 120
auth MD5
BF-CBC
keepalive 10 120
comp-lzo
user nobody
group nobody
persist-tun
status /var/log/openvpn/openvpn-status.log
log /var/log/openvpn/openvpn.log
verb 3
```

Після створення файла сервера програма створює три конфігураційні файли клієнтів. Число клієнтів може бути довільним і вводиться користувачем програми на початку використання. Всі конфігураційні файли клієнтів мають

подібну структуру, тож розглянемо тільки один з них. В лістингу 4.2 ми можемо побачити склад файлу client_1.conf.

Лістинг 4.2 – Файл client_1.conf

```
dev tun
proto udp
remote 192.168.0.1
port 5000
client
resolv-retry infinite ca keys/ca.crt
cert keys/client.crt key keys/client.key tls-client
tls-auth keys/ta.key 1 auth MD5
cipher BF-CBC
ns-cert-type server comp-lzo
persist-key
persist-tun
up /etc/openvpn_up.sh
status  /var/log/openvpn/openvpn-status.log
log /var/log/openvpn/openvpn.log
verb 3
```

## 4.5 Висновки

Загалом в результаті роботи програми в нашому випадку маємо 4 файли:

– server.conf – основний файл серверу, що потрібно буде внести в кореневу папку програми OpenVPN на сервері;

– client_0, client_1. client_2 – три подібні файли, що вносяться до клієнтських компьютерів в кореневу папку OpenVPN.

Загалом дана програма допомогає заощадити значну кількість часу, який знадобиться для того, щоб ввести всю інформацію та налаштувати зв’язок з сервером від кожного з клієнті власноруч. Можливо, використання подібної програми не є доречним для тих банків або мереж, що мають в своїй структурі невелику кількість клієнтських машин, але якщо їх кількість буде великою програма може сильно допомогти. Вона не тільки швидко вирішує питання конфігурації, а також виключає можливість помилки з боку людей, тому що займається створенням зв’язків між сервером та клієнтами власноруч.

# ВИСНОВКИ

В ході роботи в першому розділі були досліджені принципи та особливості побудови VPN мереж для банків та подібних їм установ. Було з’ясовано, що таке VPN мережа, які її основні функції та задачі. Були досліджені принципи роботи VPN мережі та її агентів. Були виявлені правила створення тунелів між клієнтами та сервером, а також описані правила IP адресації між ними.

В другому розділі були затронуті питання інформаційної безпеки банківських мереж у Інтернет просторі, визначені основні функції, що повинні захищати інформацію від зловмисників, виявені та класифіковані основні типи загроз, описані загрози міжмережевої взаємодії, до яких відносяться:

а) Аналіз мережевого трафіку;

б) Сканування мережі;

в) «Парольная» атака;

г) Підміна довіреного об'єкта мережі;

д) Нав'язування помилкового маршруту;

е) Впровадження помилкового об'єкта мережі;

ж) Відмова в обслуговуванні.

Для захисту від загроз міжмережевої взаємодії використовуються програмні або програмно-апаратні засоби. До них відносяться міжмережеві екрани, системи виявлення атак і вторгнень та віртуальні приватні мережі.

У третьому розділі були описані особливості технології OpenVPN і процес проектування на її базі банківської мережі. Практична частина роботи показала, що створення банківської мережі на основі OpenVPN поверх мережі Інтренет є досить простим завданням. Для розгортання VPN мережі необхідно мати локальні мережі з виходом в Інтернет, завантажити відповідний ОС дистрибутив OpenVPN, і встановити його. Слід зазначити, що для клієнта і

сервера використовується один дистрибутив. Налаштування OpenVPN полягає в установці і зміні конфігураційних файлів, ключів шифрування і сертифікатів. Причому ці процедури проводяться як для клієнта, так і для сервера.

В четвертому розділі був описаний процес створення програми, що автоматизує налаштування банківської VPN мережі, було описане використане для цього середовище розробки та його бібліотеки, що були використані в коді програми. Був проведений опис бібліотек потоків, рядків та конструкцій, створених в мові програмування C++ для роботи з файлами. Був показаний результат розробки у виді програми, що створює необхідну користувачу кількість повністю налаштованих програмою конфігураційних файлів. Створена програма значно полегшує процес налаштування та допомагає швидко та безпечно створити всі необхідні для роботи банківської мережі конфігураційні файли.

В результаті проведеної роботи побудована VPN мережа на базі технології OpenVPN для банківської установи. OpenVPN легко та зручно реалізує технології віртуальної приватної мережі (VPN) з відкритим вихідним кодом. Характерна легкістю інсталяції та налаштування. OpenVPN може бути встановлений практично на будь-яку платформу. При зазначених перевагах OpenVPN відповідає всім сучасним вимогам захисту, створює захищений шіфрованний TCP або UDP тунель для проектованої мережі банку, що забезпечує захист переданих даних між головним офісом, відділеннями та АТМ.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ


1. Конфигураційні файли. Бібліотека libconfig [Електронний ресурс] / Хабр. Режим доступу: https://habr.com/ru/users/romy4/

2. Робота з файлами в C++. Частина 1 – Бібліотека fstream [Електронний ресурс] / Форум з програмування C++. Режим доступу: https://purecodecpp.com/archives/2751

3. Платонов В.В. Програмно-апаратні засоби забезпечення інформаційної безпеки обчислювальних мереж: навч. посібник для студ. вищ. навч. закладів / В.В. Платонов. -М. : Видавничий центр «Академія», 2006. -240 с.

4. Секрети і брехня. Безпека даних в цифровому світі / Б. Шнайер. СПб .: Пітер, 2003. -368 с.

5. Звіт Cisco “Оцінка рівня інцидентів ІБ за 2015 рік”

6. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. –Харків: Вид. ХНЕУ, 2008. –352 с.

7. Зубок М. І. Безпека банківської діяльності: Навч. Посібник / М. І. Зубок. – К.: КНЕУ, 2002. – 190 с.

8. Черевко О. В. Джерела виникнення загроз інформаційній безпеці банківських установ / О. В. Черевко, В. М. Андрієнко, І. Ю. Напора // Вісник Черкаського університету. Серія: Економічні науки. – 2016. – № 3. – С. 120-127.

9. Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі. Принципи, технології, протоколи. -2001 р 668 с.

10. А.В. Соколов, В.Ф.Шаньгін. Захист інформації в розподілених корпоративних мережах і системах. -М.: ДМК Пресс, 2002. -656с.

11. Інформаційні системи в економіці: навч. посібник / під ред.Г.А.Тіторенко-2-е ізд., перераб. і доп. -М .: Юніті-Дана, 2008

12. Страхарчук А.Я. Інформаційні системи і технології в банках. [Електронний ресурс] Режим доступу: http://uchebnikionline.com/bankovskoe

delo/informatsiyni_sistemi_i_tehnologiyi_v_bankah__straharchuk_aya/informatsiyni_sistemi_i_tehnologiyi_v_bankah__straharchuk_aya.htm

13. Корніенко Е.В.Методи прогнозування і прийняття рішень: навч. посібник / Е.В.Корніенко-Таганрог: Изд-ль А.Н. Ступін, 2014

14. КарповаІ.П. Бази даних: моделі, розробка, реалізація: навч. посібник / І.П. Карпова. СПб .: Питер, 2001 5.Барсегян А. А.Технології аналізу даних: Data Mining, Visual Mining, Text Mining, OLAP / А. А. Барсегян, М. С. Купріянов, В. В. Степаненко, І. І . Холод. -2-е изд., Перераб. і доп. СПб .: БХВ-Петербург, 2007

15. Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі. Принципи, технології, протоколи. -2001 р 668 с.

16. В.Г. Оліфер, Н.А. Оліфер. СПб .: БХВ-Петербург, 2001. 512 с.

17. Фортенберi Т. Проектування віртуальних приватних мереж в середовищі Windows2000: пер.с англ. / Т. Фортенберi. М.: Іздательскійдом "Вільямс", 2002. 320 с.23.Зіма В.М. Безпека глобальних мережевих технологій /

18. ЗапечніковС.В. Основи побудови віртуальних приватних мереж: Учеб.пособие для вузів / С.В.Запечніков, Н.Г.Мілославская, А.Н.Толстой.М .: Гаряча лінія-Телеком, 2003. 249 с.

19. Межсетевое взаємодія. РесурсиMicrosoftWindows2000Server: пров. Санглена. М .: Видавничо-торговий дім "Російська Редакція", 2002. 736 с.

20. Порівняння технологій IPsec та SSL в технології VPN [Електронний ресурс] Режим доступу: http://www.sovit.net/articles/technologies/ipsec_vs_ssl/

21. SSL VPN -крок вперед в технології VPN мереж [Електронний ресурс] Режим доступу: https://www.anti-malware.ru/node/449