Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідуючої кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Забезпечення безпеки Інтернет-провайдера»

Виконавець: студент IV курсу, групи КБ-41

_____ **Данило ЖУДРА**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Микола БРАЙЛОВСЬКИЙ	

Нормоконтроль	Сергій ДАКОВ	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідуючої кафедри кібербезпеки
та захисту інформації
_____ Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2022 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-41** **Жудру Данилу Володимировичу**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Забезпечення безпеки Інтернет-провайдера

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Концепція роботи Інтернет-провайдерів, політика безпеки компанії

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно провести аналіз сучасної структури мережі Інтернет, здійснити аналіз поняття постачальника послуг Інтернет та основні принципи роботи. Встановити Особливості нормативно-правового забезпечення. Проаналізувати можливі загрози та протидію їм. Розробити політику безпеки Інтернет-провайдера.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації з вирішення основних проблем та загроз Інтернет-провайдерів та розроблена політика безпеки компанії провайдера.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.01.2021 року

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Данило ЖУДРА
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.01.2021 – 31.01.2022	*виконано*
2	Аналіз літератури	01.02.2022 – 15.02.2022	*виконано*
3	Обґрунтування вибору рішення	16.02.2022 – 19.02.2022	*виконано*
4	Концепція Інтернет-провайдера та спутникового інтернету.	20.02.2022 – 04.03.2022	*виконано*
5	Аналіз проблем інформаційної безпеки в компаніях, що забезпечують доступ до мережі Інтернет	05.03.2022 – 21.03.2022	*виконано*
6	Дослідження вразливостей та загроз	22.03.2022 – 08.04.2022	*виконано*
7	Розробка політики безпеки Інтернет-провайдера	09.04.2022 – 10.05.2022	*виконано*
8	Оформлення пояснювальної записки	11.05.2022 – 27.05.2022	*виконано*
9	Підготовка до захисту дипломної роботи	28.05.2022 – 13.06.2022	*виконано*

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Данило ЖУДРА
(підпис) (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 75 сторінок тексту, 3 таблиці та 9 рисунків. Список використаних джерел містить 81 найменування і займає 5 сторінок.

Метою роботи є процес і аналіз головних загроз інтернет мережі для провайдера, вирішення проблем підключення, розгляд супутникового інтернету як аналог мережі, а також розробка політики безпеки.

Предмет дослідження: політика безпеки інтернет-провайдера.

В роботі проаналізовано сучасну структуру інтернет мережі та поняття послуги інтернет, що надають інтернет-провайдери, запропоновано вирішення головних проблем інтернет-провайдерів, побудовано таблиці загроз та протидій компанії-провайдера, а також розроблено політику безпеки інтернет-провайдера.

Результати нашого дослідження можуть використовуватися компаніями, які надають користувачам доступ до інтернет мережі з метою забезпечення ефективної і сучасної політики безпеки; у навчальному процесі Київського національного університету імені Тараса Шевченка при підготовці навчальних дисциплін за спеціальностями 122 «Комп’ютерні науки» та 125 «Кібербезпека».

Напрямки подальших досліджень: розробка подальшої нормативно-правової бази компанії інтернет-провайдера в сфері забезпечення інформаційної безпеки

Ключові слова: інтернет , інтернет-провайдер, супутниковий інтернет, Starlink, політика безпеки, політика безпеки інтернет-провайдера, постачальник послуг інтернет.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІБ	–	Інформаційна безпека
ПІБ	–	Політика інформаційної безпеки
(D)DoS	–	(Distributed) Denial-of-Service
IEEE	–	Institute of Electrical and Electronics Engineers
ІП	–	Інтернет-провайдер
СІ	–	Супутниковий Інтернет
IPS	–	Intrusion Prevention System
ISP	–	Internet Service Provider
IT	–	Information Technology
ДБЖ	–	Джерело безперебійного живлення
СКС	–	Структура кабельної системи
ВОЛЗ	–	Волоконно-оптична лінія зв’язку
TCP	–	Transimission Control Protocol
VPN	–	Virtual Private Network
IP	–	Internet Protocol
ІКТ	–	Інформаційно-комунікаційні технології
ПЗ	–	Програмне забезпечення
OSI	–	Open Systems Interconnection Basic Reference Model

ЗМІСТ

ВСТУП

Актуальність роботи. У зв'язку з тим, що інтернет відіграє важливу роль сьогодення, ніхто з нас не може уявити і дня без підключення до мережі. Саме тому головною задачею провайдерів є підтримка стабільного доступу до інтернет мережі. На жаль, провайдери часто стикаються з зовнішніми чинниками, які негативно впливають на роботу з'єднання, тож безпека є ключовою характеристикою для інтернет-провайдерів. Дана тема є дуже актуальною, так як при дослідженні таких неполадок ми можемо визначити конкретні випадки порушень роботи та мінімізувати випадки роз'єднання мережі.

Наразі безпека є особливо актуальною, так як одним з зовнішніх чинників на території України стала фізична небезпека, тобто через війну можливе руйнування ліній зв'язку, а також посилені кібер-атаки. За рахунок цього в даній роботі було досліджено супутниковий інтернет, що нині є доступним в будь-якій точці України, так як зв'язок подається напряму з космосу і антена підключення є мобільною. Через те, що супутниковий інтернет різко набирає великої популярності, провідний інтернет виходить на задній план, тому було розроблено політику безпеки, щоб робота провайдерів стала більш ефективною.

Метою роботи аналіз головних загроз інтернет мережі для провайдера, вирішення проблем підключення, аналіз супутникового інтернету, а також розробка політики безпеки.

Окремо були поставлені такі задачі для того, щоб досягти заданої мети даної дипломної роботи:

- проведення аналізу за сучасною структурую інтернет мережі, побудова топологій мереж, та їх плюси та мінуси; дослідження двох моделей OSI і TCP/IP, та варіанти вирішення проблем, що можуть виникати в цих моделях;

- аналіз послуг інтернет-провайдерів, дослідження побудови мережі, можливих загроз і проблем, наприклад перебою електроенергії, втрата ліній зв’язку чи кібер-атак, та дослідження методів уникнення неполадок;

- дослідження супутникового інтернету та конкретного проекту Starlink, порівняльна характеристика відповідно з іншими компаніями-постачальниками, огляд практичного встановлення системи та дослідження проблем безпеки спутникового інтернету;

- вияв особливостей нормативно-правового забезпечення, тобто визначених стандартів, що необхідні нам у розробці політики безпеки для компанії;

- розробка політики безпеки інтернет-провайдера та безпосередньо аналіз її концепції побудови.

Об’єктом дослідження є процес інтернет-провайдерів за умов підвищеного попиту та перенавантаження.

Предметом дослідження є політика безпеки інтернет-провайдера.

Методи дослідження. В даній роботі було використано такі загальнотеоретичні методи як синтез, аналіз, метод ідеалізації та абстрагування, а також моделювання та формалізації при побудові певних схем і таблиць.

Практичне значення. Результати нашого дослідження можуть використовуватися компаніями, які надають користувачам доступ до інтернет мережі з метою забезпечення ефективної і сучасної політики безпеки; у навчальному процесі Київського національного університету імені Тараса Шевченка при підготовці навчальних дисциплін за спеціальностями 122 «Комп’ютерні науки» та 125 «Кібербезпека».

РОЗДІЛ 1
ЗАГАЛЬНІ ПРИНЦИПИ ГЛОБАЛЬНОЇ МЕРЕЖІ ІНТЕРНЕТ ТА ІНТЕРНЕТ-ПРОВАЙДЕРА

Складно у XXI-му столітті уявити життя без інтернету. Інтернет, або ж по-іншому називають всесвітньою павутиною – це найбільша всесвітня цифрова мережа, яка складає не від'ємну частину нашого життя, адже він повсякденно допомагає нам у пошуку будь-якої інформації, у спілкуванні через різні комунікаційні сервіси, такі як Telegram, Facebook і т.д, або ж наприклад у покупці продуктів через Rozetka. Інтернет виник в 1970-х роках у США, проте спочатку він не був доступний для всіх, так як ця система спершу була створена з метою передачі даних у випадку війни, а вже в 1990-х роках набув широкого користування. Станом на сьогодні доступ до інтернет мережі мають 4,95 мільярдів людей.

1.1 Сучасна структура мережі інтернет

Інтернет – це міжнародна інформаційно-комунікаційна мережа, що складається з безлічі локальних (регіональних) пристроїв та комп'ютерних мереж які передають між собою інформацію дані за допомогою телекомунікаційних каналів (а саме радіоканали, телефонні аналогові, лінії шифру, оптичні канали та супутник). Загалом використовується TCP / IP протокол. Далі розглядатимемо структуру сімейства TCP / IP протоколів з OSI (Open Systems Interconnection) моделлю (рис. 1.1).

OSI TCP / IP – це модель, яка визначає та проектує архітектуру системи, а також використовується в якості підтримки багатьох стандартів для передачі даних. Як приклад, для глобальних мереж – ISDN, для локальних мереж - FDDI та Ethernet. Існують такі протоколи як SLIP та PPP, вони потрібні для

сполучення, якому сприяють аналогові лінії зв’язку, крім того використовуються на даному рівні.

Міжмережевий стековий рівень TCP / IP (2-го рівня), називається мережевим рівнем (по моделі OSI), та є основною архітектури всієї TCP / IP. Вказаний вище рівень в межах усієї мережі забезпечує передачу пакетів даних, причому функції цього рівня відповідають рівню мережі OSI моделі.

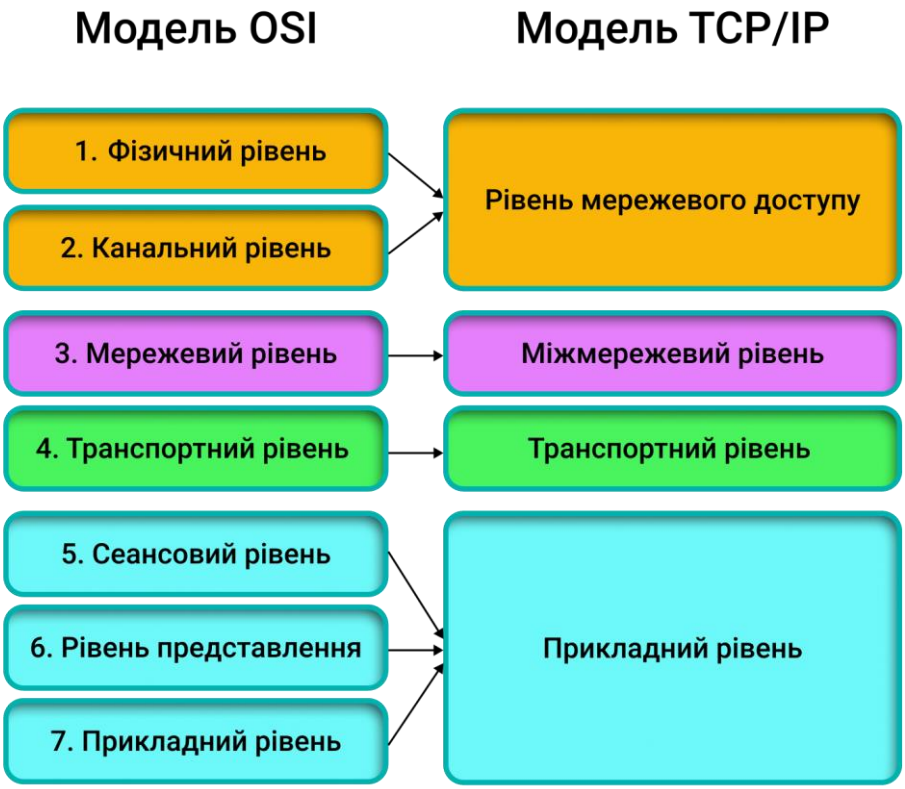

Рисунок 1.1 – Мережеві модель OSI та модель TCP\IP

Транспортний рівень надає отримання запитів на перенесення даних створеною мережею, інтерфейси якого, підтримуються протоколами мережевого рівня. Головним таким протоколом рівня мережі є міжмережевий IP протокол (Internet Protocol). Його мета забезпечити переміщення пакетів серед підмереж, з одного маршрутизатора до інших, доки пакет не надійде до призначеної мережі. Протоколи функцій глобальних комунікаційних мереж зв’язку (ATM,FR та ін.) та IP протокол, встановлюються як на кінцевих хостах, так і на усіх мережевих маршрутизаторах. Собою маршрутизатор являє процесор, що об’єднує разом дві

підмережі. Перед траспортним рівнем знаходиться мережевий протокол, при роботі якого встановлений режим без з'єднання, згідно з чим даний протокол не відповідає за доставку пакету до необхідного вузла. У разі втрати пакету IP протокол не має змогу його відновити у мережі.

На транспортному рівні TCP здіснюється перевірка цілісності та враховуються параметри передачі даних та обсяг пакетів. UDP протокол винує діяльність того ж рівня, але застосовується за умові не менш суворих умов, що до надійності передачі даних.

Прикладний рівень обєднує усі служби, що надається користувачеві системою, причому DNS (Domain Name System) змінює числові адреси на імена, та працює на тому ж самому рівні.

Найважливіші прикладні протоколи в себе включають:

- SNMP – керування пристроями мережі;
- TELNET - віддалене керування;
- HTTP - передача гіпертексту;
- FTP - відправка файлів;
- SMTP, POP і MIME - протоколи електронної пошти;

Загалом виділяють 5 ключових топологічних типів в комп'ютерних мережах:

- Сітка - зміст даної топології (рис 1.1) полягає в тому, що пристрої підключаються один до одного у мережі завдяки виділеній лінії «точка-точка». Виділені лінії означають передачу даних для конкретних двох підключених пристроїв. Наприклад, до мережі підключено k пристроїв, отже, відповідний пристрій мусить підключатися до (k-1) пристроїв в мережі. Тоді, k(k-1) / 2 буде відповідати кількісті посилань у топології сітка з k пристроями.

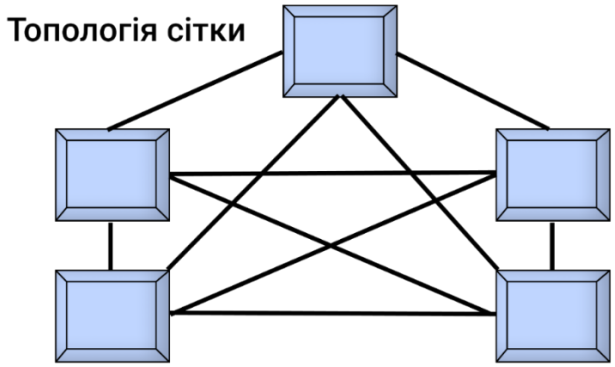

Рисунок 1.1 – Топологія сітки

– Зірка - зміст даної топології (рис 1.2) полягає в тому, що пристрої підключаються до центрального, який ще називають концентратором. У порівняні с попередньою топологією, зірка не надає доступ прямого зв’язку між пристроями, тобто пристрої повинні підключатися за допомогою концентратору. Для цього пристрій спершу надсилає дані до концентратора, після чого концентратор передає призначеному пристрою надіслані дані.

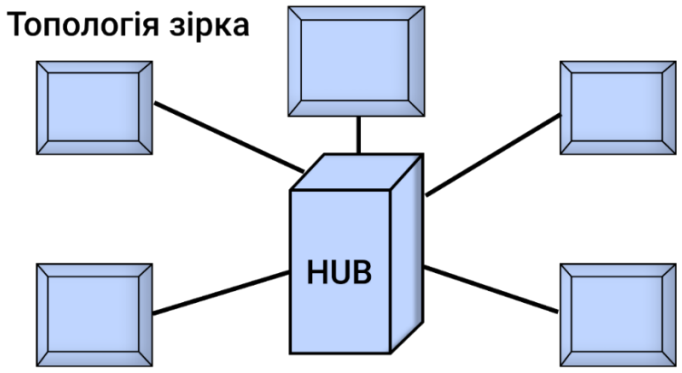

Рисунок 1.2 – Топологія зірка

– Шина - Принцип роботи даної топології (рис 1.3) полягає у підключенні усіх пристроїв до головного кабелю, за допомогою дротових ліній. Проте є обмеження що до відстані основного кабелю та кількості прямих ліній, так як по ньому відбувається передача всіх даних.

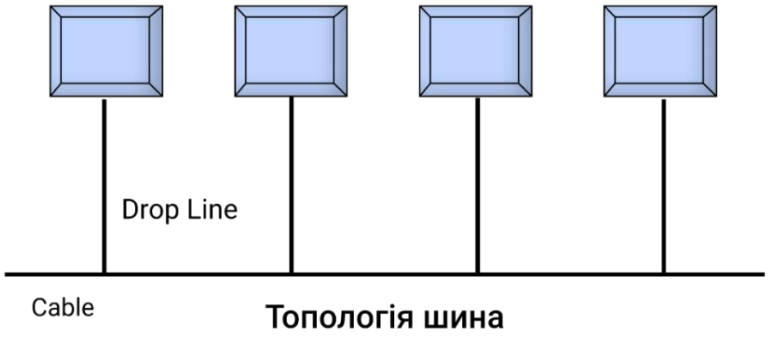

Рисунок 1.3 – Топологія шина

– Кільце - В цій топології (рис 1.4) два пристрої підключаються з кожного боку до основного пристрою. Існують 2 виділені посилання «точка-точка», що основний пристрій підключає з обох боків. У зв’язку з цим дана топологія називається кільцевою, бо утворюється коло. У разі надсилання пристроєм даних на інші, дані відправляються в одному визначеному напрямі, причому в кожному пристрої даної топології кільця існує ретранслятор. Інакше, при отримані даних, що призначені іншому пристроєві, ретранслятор пересилатиме надіслані дані, доки вони не надійдуть до потрібного призначення.

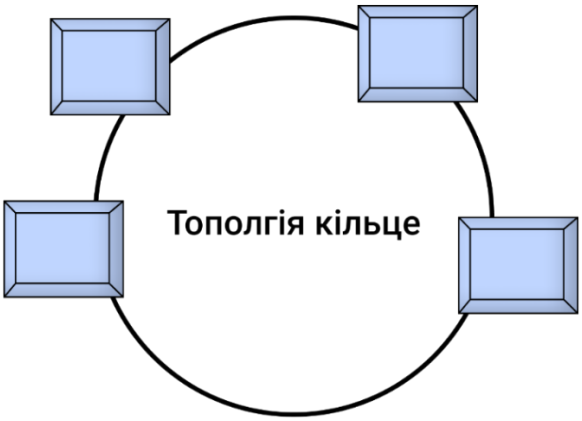

Рисунок 1.4 – Топологія кільце

– Гібридна - Це топологія (рис 1.5), яка поєднує у собі дві чи більше топології. Як приклад гібридною топологією є об’єднання топологій сітка і зірка.

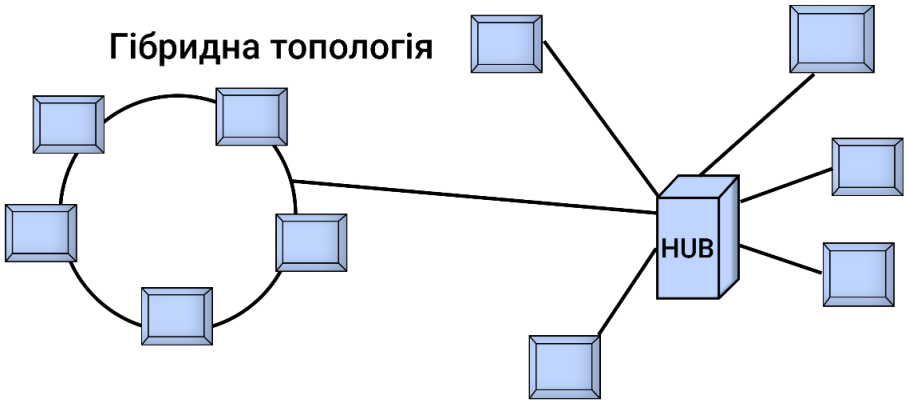

Рисунок 1.5 – Гібридна топологія

1.2 Еталона модель OSI та тонкощі використання

Перший рівень - фізичний (рис. 1.6) . На ньому є багато технологій - від різноманітних кабелів до фізичних мережевих пристроїв. [9; 10]

Дані технологічні рішення можна поділити на такі категорії:

– Вузли та мережеві апаратні компоненти. Перелік пристроїв включає концентратори, ретранслятори, маршрутизатори, комп’ютери, принтери, тощо та набір апаратних компонентів всередині цих пристроїв, включають антени, підсилювачі, мережеві інтерфейсні карти (NIC) і так далі.

– Механічна частина інтерфейсу пристрою. Пояснює принцип підключення, до пристрою, форма та розмір роз’єму, кількість контактів.

– Функціональна та процедурна логіки. Процедурна логіка послідовності подій необхідна для отримання конкретного результату, функції кожного штифта в роз’ємі і таке інше.

– Технічні характеристики, різновиди та протоколи кабелю. Перелік кабелів, їх специфікації та варіанти виконання.

– За типом сигналу.

– За поширенням сигналу в залежності від середовища. Варіанти можуть бути електричні (Ethernet), світлові (оптичні мережі, волоконна оптика) та радіохвилі (WiFi, Bluetooth, WiMAX).

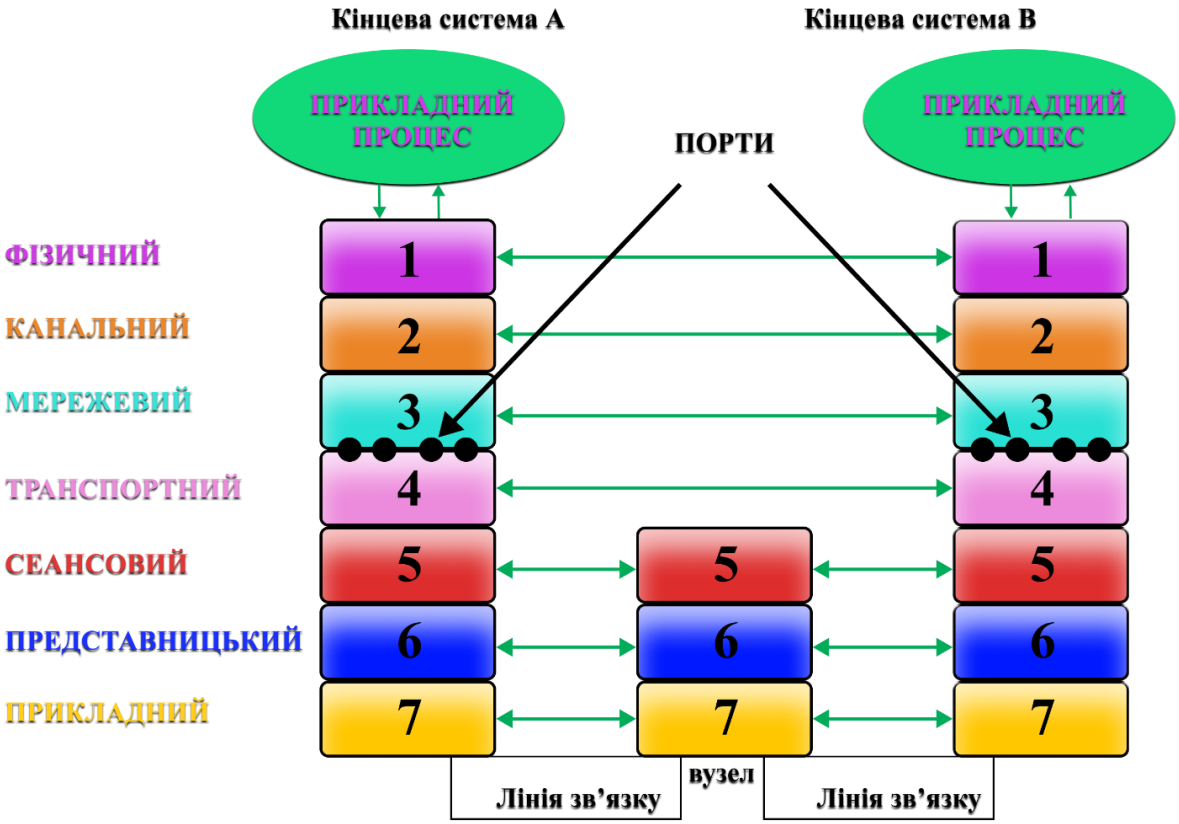

Рисунок 1.6 – Модель OSI

Популярні проблеми OSI першого рівня та методи їх вирішення:

– Некоректна робота кабелів чи роз'ємів через пошкодження

– Несправні апаратні мережеві пристрої

– Невірно під'єднані матеріали

Якщо у фізичному рівні є проблеми, то і все за його межами теж не працюватиме коректно.

Другий рівень - каналу передачі даних (рис. 1.6) . Рівень 2 визначає спосіб форматування та об’єм передачі даних, вміння працювати з помилками.

Кадр є блоком даних другого рівня.

Популярні проблеми:

– Всі проблеми першого рівня
– Невдалі міжвузлові з’єднання
– Періодичні невдачі з успішно створеними сесіями.
– Зіткнення кадру

Третій рівень - мережевий (рис. 1.6). Надсилання інформації в та між мережами відбувається з-за допомогою маршрутизаторів. Тепер можлива комунікація між мережами замість того, щоб просто спілкуватися між вузлами.

Маршрутизатори є необхідними для третього рівня. Комутатори переміщують дані через декілька мереж. Окрім того що вони підключаються до постачальників послуг Інтернету (ISP), щоб забезпечити доступ, вони також відслідковують, що знаходиться в його мережі, шляхи для маршрутизації даних через ці мережі та до яких інших мереж він підключений.

Всі адреси та дані про маршрутизацію маршрутизатори зберігають в таблицях маршрутизації. [13; 54]

Нижче наведено простий приклад таблиці маршрутизації (табл.. 1.1):

Таблиця 1.1

Таблиця маршрутизації

Пункт призначення	Маска підмережі	Інтерфейс
128.75.43.0	255.255.255.0	Eth0
128.75.43.0	255.255.255.128	Eth1
192.12.17.5	255.255.255.255	Eth3
default		Eth2

За одиницю даних на третьому рівні ми вважаємо пакет даних. В загальному, будь який пакет даних має в собі кадр та обгортку інформації про IP-адресу, тобто відбувається інкапсуляція інформації адреси третього рівня кадрами.

Популярні проблеми:

- Всі проблеми другого рівня
- Нефункціональність або несправність маршрутизатора чи іншого вузла
- Неправильне налаштування IP-адреси

Щоб отримати відповіді на деякі з цих питань необхідне використання можливостей командного рядка, таких як: трасування , ping, протоколи ip або показ ip-маршруту.

Четвертий рівень – транспортний (рис. 1.6). Він базується на функціях другого рівня таких як: контроль потоку та помилок і «дисципліна» ліній. Рівень відповідає за сегментацію та надсилання мережею пакетів даних.

Четвертий рівень, навідміну від попереднього, вже розуміє ціле повідомлення, а не лише вміст кожного окремого пакету даних і може керувати мережевими перевантаженнями, не надсилаючи одночасно всі пакети.

Для четвертого рівня блоки даних можуть називатися по-різному. Для TCP – це пакет, для UDP - датаграма. Ці два протоколи є найбільшими на четвертому рівні.

TCP протокол надає перевагу якості даних над швидкістю. Він встановлює зв'язок з вузлом призначення і вимагає «рукостискання» між джерелом і вузлом призначення при передачі даних, яке символізує отримання даних. TCP попросить повторити спробу у разі якщо вузол призначення не доотримує всіх даних. Також він відповідає за доставку чи правильний порядок при повторному збиранні пакетів даних.

UDP, в свою ж чергу, надає перевагу швидкості над якістю даних. Він не вимагає «рукостискання» та не чекає на підтвердження, тому може надсилати дані швидше, але через такий принцип роботи не весь об’єм даних може бути успішно переданий, і ми про це не дізнаємось.

Популярні проблеми:

- Всі проблеми третього рівня

– Заблоковані порти. Перевірте свої «Списки контролю доступу» (ACL) та брандмауери

– Налаштування якості обслуговування (QoS) - набір методів для управління ресурсами пакетних мереж. QoS - це функція маршрутизаторів/комутаторів, яка може визначити пріоритет трафіку.

Наступний рівень - сеансовий (рис. 1.6). Він відповідає за коректну роботу сеансу, тобто: встановлення, підтримку та завершення сеансу. Під словом сеанс ми розуміємо зв’язок, який формується між двома конкретними програмами для кінцевих юзерів. Варто розглянути дві різні концепції:

– Клієнт і сервер. Додаток, який проводить запит задля отримання інформації, називається клієнтом, натомість додаток, який містить в собі запитувану інформацію - сервером.

– Модель запитів та відповідей. Під час створення та в процесі сеансу відбувається двостороннє передавання запитів на інформацію та відповіді, в яких міститься ця інформація. [15]

Сесії можуть бути відкритими як протягом доволі короткого періоду часу, так і тривалого.

На п’ятому рівні і вище мережі орієнтовані на встановлення з'єднань із програмами та відображення даних кінцевим споживачу.

Популярні проблеми п’ятого рівня:

– Сервер не в доступі

– Невірне налаштування серверів

– Різноманітні помилки сеансів.

Шостий рівень - представницький (рис. 1.6). У процесах представницького рівня зазвичай бере участь операційна система, на якій розміщено додаток для кінцевого користувача. Цей функціонал не завжди реалізований в мережевому протоколі. Рівень відповідає за форматування та шифрування даних.

Шостий рівень гарантує споживання й відображення даних програми кінцевого користувача, що працюють на прикладному рівні.

Популярні проблеми:

- Відсутність або пошкодженість драйверів
- Невідповідний рівень доступу користувачів операційних систем

Сьомий рівень - прикладний (рис. 1.6). Рівень несе відповідальність за підтримку служб, користувачами яких є програми кінцевих юзерів. До переліку належать програми, встановлені в операційній системі, які будуть контролювати взаємодію з кінцевим користувачем.

Популярні проблеми:

- Проблеми попередніх рівнів
- Некоректне налаштування програм
- Людський фактор

1.3 Інтернет-сервіс провайдинг

Робота інтернет-провайдерів полягає у наданні доступу до інтернету користувачам, маршрутизації трафіку, в вирішенні доменних імен та підтримці мережевої інфраструктури, що робить можливим доступ до інтернету.

Попри те, що надання доступу до Інтернет мережі є основною послугою, провайдери виконують безліч інших функцій. До переліку таких послуг, входить: веб-хостинг, реєстрація доменних імен та послуги електронної пошти.

Інтернет-провайдери першого рівня займають вершину піраміди доступу «піраміди доступу до Інтернету» (рис. 1.7). Такий провайдер називається постачальником послуг першого рівня, який має доступ до всіх інтернет мереж, причому він використовує лише такі угоди мережевого пірингу, за які вони не мусять сплачувати кошти. Для простоти пояснення яку мету виконують інтернет провайдери першого рівня, можна поставити в порівняння головні магістралі інтернету, тобто вони об’єднують всю мережеву павутину. Наприклад, Vodacom, Bharti, Deutsche Telekom, British Telecommunications та Verizon є популярними інтернет-провайдерами першого рівня.

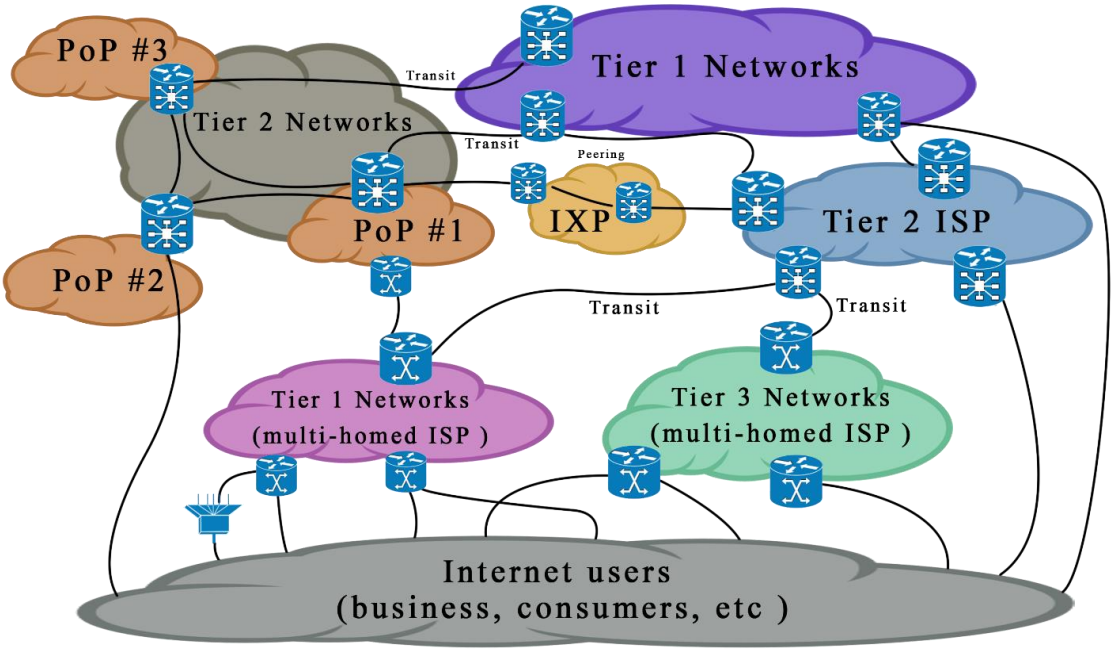

Рисунок 1.7 – Піраміда доступу до Інтернету

Ці провайдери надають доступ на ринку збуту до власних мереж, провайдерам другого рівня. В свою чергу провайдери другого рівня, займаються продажом доступу до інтернету компаніям та побутовим користувачам. Хоча інколи трапляються випадки, коли інтернет-провайдер першого рівня продають доступ до інтернету фізичним та юридичним особам напряму. Окрім цього, провайдер третього рівня, тобто другий проміжний провайдер має можливість отримати пропускну здатність мережі у провайдера другого рівня перед продажом безпосередньо продукту кінцевим користувачам.

В момент перенаправлення від приватної мережі до інтернету, спершу як досягти місця призначення він робить декілька стрибків. Наприклад переходить від модему до мережі інтернет -провайдера третього рівня або мережі провайдера другого рівня, чи мережі провайдера першого рівня, після чого повертається за допомогою іншого набору провайдерів.

Для встановлення зв’язку, постачальники послуг інтернет мережі використовують ключову технологію, яка базується на аналогових телефонних лініях (комутована лінія), DSL, кабельних, супутникових, Wi-Fi, волоконно-оптичних чи інших носіях зв'язку. Дуже багато постачальників кабельних та

телефонних послуг, також є провайдерами, причиною цього є те що Інтернет-трафік здатна приймати базова інфраструктура.

Референтна модель побудови мережі:

рівень доступу - Ключова функція цього рівня надає фізичним та юридичним особам змогу підключатися до інтернет-провайдера зі свого обладнання (це може бути маршрутизатор, мобільний пристрій, ПК). В свою чергу комутатор (якщо підключенню сприяє дротовий носій, тобто через локальну мережу) або базова станція (за допомогою бездротового носія) є обладнанням постачальника мережі. Зазвичай використовуються комутатори 2-го рівня (L2), інколи – 3-го (L3). При побудові локальної мережі, дехто з провайдерів, обирають некеровані комутатори, але в подальшому використані якість послуг буде напряму залежати від цього.

рівень агрегації - Це середній шар між рівнем доступу та мережевим ядром. Зазвичай рівень агрегації використовується на комутаторах 3-го рівня, в деяких випадках внаслідок високої вартості реалізація проводиться на маршрутизаторах, причому при конкретних типах приміщень враховуються властивості роботи. З’єднання посилань надісланих від магістрального рівня доступу комутаторів до комутатора за топологією зірка є головною метою.

рівень ядра мережі - В будь якій мережі ядро завжди є його цілісною частиною. Такий рівень використовується частіше всього на маршрутизаторах, іноді є на L3-комутаторах високої ефективності (це застосовується, щоб знизити вартість мережі). Ядро мережі може містити налаштування для динамічного маршрутизатора або стримувати статичний маршрут.

серверний рівень - Реалізується серверами мережі. Здійснення може виконуватись як на спец обладнанні, так і на платформах сервера. На сьогоднішній день для платформ серверу програмне забезпечення чи репрезентоване багатьма виробниками, за ліцензіями різного типу та ОС, де буде встановлено ПЗ.

1.4 Ключові труднощі Інтернет-провайдера

Наведемо основні проблеми, що трапляються у провайдера, при надаванні послуг споживачу:

1. перебої електропостачання;
2. технічна поломка обладнання;
3. обрив лінії;
4. загальній VLAN для підмережі абонентів;
5. DOS\DDOS – атаки;
6. Інсайдери.

1.4.1 Перебої в електропостачанні

Збої в передачі електроенергії з боку підприємств-постачальників є однією з головних проблем надання послуг. Основними причинами, які викликають дану проблему можна назвати стару інфраструктуру, поганий стан трансформаторних підстанцій, неналежний стан приміщень підстанцій. Також варто враховувати, що проміжне обладнання, яке знаходиться на шляху від основного серверу до абонента, є енергозалежним і при його некоректній роботі сигнал на досить значну область може припинити діяти. [41, 42]

Звісно для вирішення подібних питань є свої рішення, наприклад, створення системи з додатковими лініями передачі сигналу. Проте, варто пам’ятати, що сам провайдер на якість подачі електроенергії немає впливу.

1.4.2 Технічна поломка обладнання

Враховуючи уже вказані проблеми, можна також додати, що однієї із них є також проблема обладнання, що знаходиться вже в неналежному стані і не зовсім відповідає робочому запиту. Призвести до цього якраз і можуть збої з подачою електроенергії.

Ще однієї проблемою є розміщення обладнання в непристосованих для нього місцях, таких як, горища чи підвали, де немає можливості постійно підтримувати, потрібні для коректної роботи обладнання, умови. Пил, вологе повітря, можливість затоплення під час опадів – це все впливає та може призвести до пошкодження обладнання.

Проте, ці всі проблеми можна вирішити за допомогою певних дій:

– встановити стабілізатор напруги, який може вимірювати вхідну напругу та вирівнювати її до рівня у 220В. Його плюсом є і те, що він може не пропускати імпульсні стрибки напруги та зміни при включенні і відключенні електроенергії;

– встановити джерело безперебійного живлення (ДБЖ) [43-45]. Навіть, якщо буде ситуація, коли електропостачання буде відключено, то саме обладнання при відключенні та включенні після відновлення напруги, не отримає пошкодження в технічній та програмній складових;

– наявність бекапу системи програмної складової, це необхідно, щоби в ситуації, коли потрібно відновити роботу обладнання, його можна було швидко повернути до робочого стану;

– здійснювати установку обладнання в місцях, які відповідають вимогах його роботи;

– вчасно проводити профілактичні та технічні роботи.

1.4.3 Обрив лінії

Найчастіші причини обриву кабелів:

1. якість встановлення;
2. погодні умови;
3. зловмисники;
4. тварини, зазвичай гризуни.

При поганих природних умовах, наприклад, при сильному вітрі, кабелі можуть порватись, так як, на жаль, не всі проведенні через захищені канали. Також

трапляються випадки, коли кабелі перегризають тварини чи коли їх обрізають зловмисники.

У ситуації, коли пошкоджена структура кабельної (СКС) [48; 53; 55] можна все досить швидко поремонтувати, завдяки тому, що найчастіше беруть виту пару або волоконно-оптичну мережу.

Існує декілька варіантів для визначення місця обриву подібного кабелю:

- зовнішній огляд;
- мультиметром;
- мережеві тестери;
- програмно.

У ситуації, коли потрібно виявити місце розриву кабеля, спочатку варто використати програмний метод. Цей спосіб є досить зручним, оскільки завдяки ньому є можливість визначити точність розриву до метрів. Для того, щоби це зробити інженер повинен прописати команди для перевірки дроту на обладнанні. Отримати результат можна в залежності від розташування кінцевого обладнання, але зазвичай то триває до 5 хвилин. Уже перебуваючи на місці та оцінивши ситуацію, технік-спеціаліст може дізнатись про точне місце знаходження обриву, використавши інші методи.

Загалом більшості проблем можна просто уникнути, якщо лінії СКС завчасно при встановленні проводити максимально приховано у спеціальних кожухах. Для цього варто користуватись послугами висококваліфікованих техніків, які здатні чітко виконувати свою роботу.

Якщо говорити про ситуацію з волоконно-оптичною лінією зв’язку (ВОЛЗ) [49; 50; 79] то тут краще завчасно подбати про аби не сталось поломки та максимально швидко реагувати у випадку, якщо вона таки відбулась. Це пов’язано з тим, що ВОЛЗ відіграють надзвичайно важливу роль у роботі усієї системи інфокомунікації.

Є кілька варіантів вирішення цієї проблеми:

- проведення моніторингу системи;
- вчасне виявлення несанкціонованого доступ до ВОЛЗ;

– своєчасно визначити проблемні місця ВОЛЗ і усунути пошкодження до його прояви;

– максимально швидко відреагувати у разі виникнення аварії;

– створити базу даних рефлектограмм ВОЛЗ.

Щоби здійснювати моніторинг системи між рефлектометром і лінією зв'язку необхідно підключити комутатор. Через деякий час він буде перемикається між оптоволоконними лініями. [51;56-58] Система моніторингу записує та зберігає еталонні карти відбиття для всіх перевірених волокон і записує зміни у всіх точках.

В табл. 1.2 вказані категорії кабелів і їх пропускна здібність у смугах частот.

Таблиця 1.2

Категорії кабелів Ethernet для стандарту EIT/TIA-568B

Категорія кабелю	Смуга частот	Пропускна здібність
3	16 Мгц	До 10 мбит\сек
5e	100 Мгц	До 1 Гбит\сек
6	250 Мгц	До 10 Гбит\сек
6a	500 Мгц	До 10 Гбит\сек

1.4.4 Загалні проблеми VLAN-ів для абонентської підмережі

При інтернет-з'єднанні необхідно завжди або тимчасово призначити реальну IP-адресу мережевому інтерфейсу вашого комп'ютера [11].

Так як IP-адреси є платним і обмеженим ресурсом, провайдери використовують різні схеми керування адресами: статичні та динамічні. При підключенні абонентів за допомогою динамічної IP-адреси плата за оренду реальної адреси не стягується, але незмінність адреси, яку користується абонент, не гарантується.

Динамічні адреси не завжди відповідають потребам абонентів. Коли вам потрібно відкрити ресурси вашого комп'ютера для зовнішніх споживачів, наприклад, розгорнути http-, поштові або ftp-сервери, ви повинні записати адресу

хоста. Зазвичай користувачів цікавить не одна адреса, а IP-мережа. Такі послуги зазвичай надаються платно.

Провайдери планують адресний простір, щоб забезпечити його раціональне використання, поділяючи IP-мережу на кілька підмереж для задоволення різних потреб. Це може бути для хостів мережевих служб, для динамічних пулів, для корпоративних клієнтів. Підмережі дозволяють значно зменшити кількість адресної інформації в таблиці маршрутизації, а також гарантують сегментацію комп'ютерної мережі користувача, зменшують трафік трансляції та спрощують моніторинг мережі. Проте варто враховувати, що розмір підмереж є обмеженим, він дорівнює ступеню двійки. Це означає, що у випадку, якщо, до прикладу, розділити мережі класу С на підмережі то вийде чітка кількість підмереж. Варто також пам'ятати, що при збільшенні кількості підмереж їхня «довжина» зменшується.

Є певна система в розподілі підмереж. У мінімальній підмережі всього 4 IP-адреси, так у будь-якій IP-підмережі [62] дві адреси зазвичай службові (перша - власна адреса підмережі, остання – широкомовна) і їх не можна надавати хостам, тобто лише двом комп'ютерам можна надати реальні адреси і при цьому одна з них має бути прописана на шлюзовому пристрої. З цього всього виходять, що для мережевих служб клієнта залишається лише одна адреса. Тому варто звернути увагу, що чим сильніше розділена IP-мережа, тим більша втрата адрес на службові потреби.

На практиці при використанні IP-простору найчастіше припускають, що частиною можливих користувачів будуть окремі користувачі (на них розраховують по одному IP), іншою частиною невеликі офіси (відповідно по 2-3 реальних IP) і також корпоративні клієнти з кількома відділами і розширеною мережевою структурою (відповідно для них варто розрахувати більше IP-адрес для мережевих служб). Для зручності управління, безпеки та зменшення широкомовного трафіку варто створювати мінімальну підмережу навіть для окремих клієнтів, проте в такому випадку була би значна втрата адрес [63] і тому, зазвичай, провайдер для таких користувачів одну загальну адресну мережу.

Також часто виникає проблема, коли невеликі компанії у зв’язку із своїм ростом вимагають для себе додаткові адреси, ще й такі, які мають послідовну нумерацію щодо їхніх попередніх адрес. Суть цієї проблеми в тому, що немає корректного сегметування і це відповідно зменшує безпеку, широкомовний трафік обробляється всіма хостами адресної підмережі і необережне налаштування мережевих інтерфейсів в такій конфігурації може призвести до адресних конфліктів.

Також часто виникають проблеми, коли встановлюють послуги для подачі інтернету в офісні будівлі, бізнес-центри, торговельні комплекси і тому подібні будівлі. В таких ситуаціях зазвичай не використовують локальний маршрутизатор і стандартно пристроєм доступу в будівлі є високопродуктивний комутатор. І тому у випадку, якщо абонент потребує більш ніж одну реальну адресу може з’явитись проблема, причиною якої буде то, що одна з реальних адрес, яка оплачена абонентом, IP-підмережі по факту може бути «вилученою» у абонента. Це пов’язано із тим, що така адреса буде поставлена в якості адреси шлюзу на сабінтерфейсі маршрутизатора, який фізично розташований на віддаленому вузлі провайдера.

Як приклад, можна навести ситуацію, коли користувач при підключенні до інтернету взяв в оренду у провайдера підмережу з 4 адрес, проте він може користуватись у своїй мережі лише однією адресою. У такому випадку абоненту варто розгорнути проксі-сервер і перенести на нього адресу шлюзу. Є ще один варіант, можна перейти на VPN-доступ зі статичної IP-адресою, який надає провайдер. Якщо не використовувати подібні рішення, то буде досить складно втілити модель безпеки AAA інтернет-мережі (аутентифікація, авторизація користувачів і облік споживаних ними послуг) [65]. Окрім цього, використання VPN дає зручні можливості для ефективного управління послугами сеансового типу, відкриває можливість ввести різні зони тарифікації - Інтернет, пірінг, внутрішні ресурси, персональна статистика з'єднань і ін.

1.4.5 DDOS-атаки на сервера провайдера

Абревіатура Dos, або Denial of Servise, в перекладі означає «відмова в обслуговуванні». Це тип атак, який направлений зупинити роботу вузла у мережі шляхом массового запиту на сервер, які він не встигає обробляти. Подібного типу атаки призводять до того, що коректні запити і сам ресурс втрачають доступність. Якщо на початку абревіатури додають букву D, то це означає, що атака є направленою (Distributed) і означає відправку подібних запитів з різного числа вузлів. Таких атак є досить багато, варто розглянути самі поширені. [13]

SYN-Flood – нині це один із найпоширеніших видів DDoS, він створений на особливостях TCP-протоколу, точніше на синхронізації номера послідовності, що має назву SYN-прапора і дає можливість відстежити переміщення даних від клієнта до сервера в межах сесії. В момент, коли на сервер надходить запит з прапором SYN, то він або відхиляє його, або підтверджує початок встановлення сесії і надсилає клієнту відповідь у вигляді прапора ACK. Найчастіше зловмисники відправляють на сервер тисячі SYN-прапорів, [64] при цьому, вказуючи некоректну зворотню адресу, що призводить до того, що сервер змушений відповідати ACK на кожен запит. Ці відповіді не мають місця призначення і сервер повторює відправку відповідей знову і знову, що в результаті робить ухвалення будь-яких запитів на відкриття сесії неможливим. Проте є можливість контролювати подібні атаки за допомогою глибокої інспекції трафіку, цим користуються деякі хмарні провайдери, вони надають послугу щодо захисту сервісу користувача в рамках протидії DDoS.

UDP-Flood – в даному випадку на ціль надсилається величезна кількість запитів, для протидії використовується весь ресурс цілі і це призводить до недоступності цих ресурсів. Проти цих атака можна використовувати сервіс захисту від DDoS з боку постачальника послуг. [74; 75]

HTTP-Flood - це flood атака, яку найчастіше використовують. Її суть в тому, що надсилають HTTP-запити GET на 80-й порт, сервер стає надто завантаженим і втрачає можливість оброблять інші запити. Ці атаки мають різну кінцеву ціль, це може бути або корінь сервера або його скрит, який зазвичай займається виконанням

ресурсомістких завдань. Цю атаку можна завчасно виявити завдяки швидкому зростанню кількості запитів до одного або декількох скриптів на сервері і швидкому зростанню логів сервера. [22]

ICMP-Echo – інша назва цього виду атаки smurf-attack. Якщо її використовують то на вузол, куди націлена атака, направляється широкомовний запит з адресою відправника жертви. В результаті через те, що даний запит діє на цілий сегмент мережі, то всі вузли, що знаходяться в цьому сегменті, направлять відповідь саме на атакуємий хост і це, відповідно, посилює дію атаки.

DoS (Denial of Service) - хакерська атака на обчислювальну систему з ціллю отримати від неї відмову. Завдяки цій атаки створюються умови, при яких клієнти системи не можуть отримати доступ до надаваних системних ресурсів (серверів), або цей доступ стає більш складним.

Повністю протистояти DDOS-атакам неможливо, окрім звісно повного вимкнення системи [81]. Проте існують методи, котрі допомагають зменшити загрозу та результати атак:

– збільшення обчислювальної потужності. Цей метод можна використовувати про невеликій атаці чи на самому її початку, він дає час для того, або розпізнати її та вжити певні заходити для того аби її знешкодити;

– зворотня атака. Сенс в тому, щоби атакуючий трафік перенаправити в зворотню сторону. Особливо результативна у випадку, коли є потужний сервер, це дає можливість обернути атаку проти зловмисник;

– спеціальне програмне забезпечення. Наразі уже створено досить велика кількість варіантів для протидії DDos-атакам. Звісно ПО такого формату досить високе в ціні, проте зазвичай окупається при першій же атаці;

– розосередження серверів. Якщо завчасно розділити активні частини сервера та залишити можливість їх дублювати, то у випадку, коли частина не зможе працювати, інша – буде виконувати всі необхідні функції;

– перемістити активні IP-адреси або доменні імена з потенційно вразливих ресурсів;

– фільтрувати та блокувати трафік. Часто важко відокремити «чистий» трафік від «поганого», але можна відхиляти менші запити. Однак, якщо зловмисник використовує основний запит, такий підхід буде слабким захистом;

– усунути вразливі місця. Відразу після відбиття атаки або навіть під час атаки варто знайти та усунути вразливі місця у системі.

1.4.6 Некваліфікований персонал та Інсайдери

Інсайдери – це:

– особи, які отримують доступ до конфіденційної інформації за службовим обов'язком (технічний персонал, вище керівництво, наглядові служби) або за посадою (власник компанії, власник привілейованих акцій тощо);

– Співробітники компанії, які реалізують обмежений доступ для збору інформації та передачі її зацікавленим сторонам. [21]

Невід’ємною частиною загальної безпеки є те, щоб співробітники були навчені та обізнані з політикою інформаційної безпеки.

Навчання має починатися в перший день кожного співробітника, а також їм має бути надана можливість постійно переглядати правила та оновлювати їх в пам’яті. [76] Також важливо знайти шляхи, щоб забезпечити продовження навчання і щоб працівники не просто переглядали політику та підписували документи. Одним із варіантів є інтерактивне навчання, коли після знайомства з правилами є тестування. Це збільшує ймовірність того, що працівники звернуть увагу та збережуть в пам’яті правила.

Ще одним варіантом можна вважати щомісячні наради всіх співробітників та наради команд. Це дасть можливість показати, що керівництво саме пам’ятає про політику захисту та вважає її правильною. Адже, якщо інформаційна безпека буде частиною культури компанії, то співробітники будуть до неї серйозно відноситись та вживатимуть заходи для захисту данних.

1.5 Концепція побудови політики безпеки компанії-провайдера

Розробка концепцій і політик ІБ зазвичай відбувається в кілька етапів і відповідає етапам розробки інших нормативно-методичних, а також організаційно-розпорядчих документів:

1) План та підготовка безпосередньо перед проведенням робіт:

– Розробка регламенту взаємодії Постачальника і Користувача

– Формування групи по роботі над проектом

– Розробка програми проведення робіт

– Визначення границі робіт

2) Огляд корпоративної інформаційної системи

– Аналіз вже існуючих документів компанії

– Виконання робіт за дослідженням поточного стану інформаційного середовища і ІБ у компанії

– Заповнення листа-опитувальника співробітниками Постачальника і Користувача відповідно

3) Систематизація та аналіз зібраних даних під час дослідження вихідних даних

– Аналіз застосовуваних всередині компанії програмно-технічних засобів

– Аналіз існуючої концепції та політики ІБ за відповідності вимог українським і зарубіжним стандартам в області ІБ

– Аналіз ризиків ІБ

4) Розробка політики ІБ та її концепція

– Розробка концепції ІБ з відображенням основних вимог до системи ІБ і нормативного забезпечення системи ІБ Користувача

– Розробка політики ІБ з деталізацією основних технічних характеристик системи захисту інформації та її оптимізація під бізнес-процеси Користувача

– Коригування концепції і політики ІБ за необхідної мінімізації витрат при реалізації [15; 77; 78]

Системи дотримання вимог, які мають вимоги до інформаційної безпеки і які використовують найчастіше:

SOC 2 - це система, яка не вимагається законом, але де-факто є вимогою для будь-якої компанії, яка керує даними клієнтів у хмарі; це програма аудиту, яка гарантує, що ваше програмне забезпечення надійно керує даними клієнтів. Відповідність SOC 2 вимагає розробки та дотримання суворих вимог інформаційної безпеки для підтримки та захисту цілісності даних клієнтів. [20]

ISO 27001 - це стандарт безпеки, який визначає чіткі вимоги до системи управління інформаційною безпекою (СУББ) організації. ISO 27001 примітний тим, що він охоплює не тільки електронну інформацію; він також містить рекомендації щодо захисту такої інформації, як інтелектуальна власність та комерційна таємниця. Цей стандарт є обов'язковим для тих компаній, що займаються обробкою конфіденційної інформації. [4]

NIST SP 800-53 - це протокол безпеки, який може бути застосований до будь-якого компонента будь-якої системи, яка зберігає, обробляє або передає федеральну інформацію. Він був створений для державних установ, але його часто використовують підприємства інших галузей, щоб допомогти їм покращити свої системи інформаційної безпеки. Дотримання NIST допомагає в тому числі і дотримуватись інших рекомендацій, таких як HIPAA, FISMA або SOX. [18]

PCI DSS, скорочена версія стандарту безпеки даних платіжної картки — це структура, яка допомагає компаніям, які отримують, обробляють, зберігають або передають дані кредитних карток, і зберігають їх у безпеці. Це стосується будь-якої компанії, яка обробляє дані кредитної картки або інформацію про власника картки. Кожна компанія повинна відповідати одному з чотирьох рівнів відповідності стандарту PCI DSS, залежно від обсягу транзакцій компанії та від того, чи зберігаються дані власників карток. [19]

Найважливішими цілями політики інформаційної безпеки є:

– Забезпечити захист інформації від загроз витоку технічними каналами.

– Забезпечити конфіденційність, цілісність і доступність інформаційних ресурсів.

– Встановити загальний підхід до інформаційної безпеки.

– Виявити та запобігти компрометації інформаційної безпеки, наприклад, зловживання даними, мережами, комп’ютерними системами та програмами.

– Захист репутації компанії за етичну та юридичну відповідальність.

– Поважати права споживачів; досягнути цього можна за рахунок забезпечення ефективних механізмів реагування на скарги та запити щодо фактичної чи уявної невідповідності політики.

Висновки до розділу 1

У даному розділі було розглянуто та вивчено структуру інтернет мережі, також було виявлено, яку роль у цьому відіграє інтернет провайдер. Для цього було задано і детально досліджено такі моделі, як модель OSI та модель TCP/IP, та розглянуто п’ять різних топологічних типів. Ми продемонстрували всі можливі нюанси та проблематику цих двох моделей. Було розкрито принцип роботи інтернет-провайдерів, якого виду вони бувають, та які функції виконують. Також було виявлено основні проблеми провайдера та розписано теоретичну розробку побудови політики безпеки та досліджено модель побудови інтернет мережі.

РОЗДІЛ 2
ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ІНТЕРНЕТ МЕРЕЖІ ПІД ЧАС ВОЕННОГО СТАНУ

На сьогоднішній день ця тема актуальна як ніколи, нині в Україні відбуваються воєнні дії, які загрожують плановим знищенням наших міст, сіл та навіть цілих регіонів. Вторгнення росії на нашу територію прямим чином також впливає на й безпеку провайдерів. Так як в разі перебою ліній передач або ж відсутності електроенергії, вони не зможуть надавати свої послуги. Проте інтернет наразі неймовірно потрібен в першу чергу захисникам України, щоб вони швидко і оперативно мали змогу отримувати гарячі новини з місць подій, та реагуючи на них мали можливість коригувати план власних чи бойових дій. Та й звичайним громадянам інтернет потрібен не менше аби також не перебувати в інформаційному вакуумі. Особливо це стосується частин України, де відбуваються найзапекліші бої, щоб наприклад мати змогу отримати інформацію про евакуацію або попросити допомоги, і знайти де і як саме її можна отримати. Саме тому поговоримо про новітню технологію, яка з’явилася в нас раніше, ніж мала би бути.

2.1 Супутниковий інтернет та його втілення завдяки прогресивній компанії SpaceX

Спершу треба розібратися що ж таке супутниковий інтернет та як він працює. Розберемо для цього орбітальну механіку, супутники, як всім відомо, літають на певних відстанях від Землі, тобто по орбітах. Таких орбіт достатньо багато, вони є різними і служать для різних цілей. Наприклад, Орбіта Міжнародної космічної станції становить близько 400 кілометрів, а орбіта супутників GPS близько 20 000 кілометрів(рис. 2.1). У даному випадку така орбіта обрана, щоб кожен супутник покривав певну і велику область планети. Адже, чим далі ми від Землі, тим більшу площу можна побачити. З інтернет супутниками, та й більшістю телекомунікаційних супутників все приблизно відбувається так само. Проте вони

літають ще далі від Землі на так званій геостаціонарній орбіті на висоті близько 35 000 кілометрів від поверхні Землі, або ж іноді доступ до інтернет мережі забезпечується через супутники низької орбіти(LEO). Так звана геостаціонарна орбіта має свої плюси: можна запустити лише кілька потужних супутників, і вони покриють всю поверхню планети. Але мінусами є те, що існує затримка та швидкість передачі даних відносно невелика. Так як, сигнал повинен пройти туди і назад, а відстань не маленька – 70 000 кілометрів, від чого й виникає така значна затримка. Більш детально про переваги й недоліки обговоримо в підрозділі.

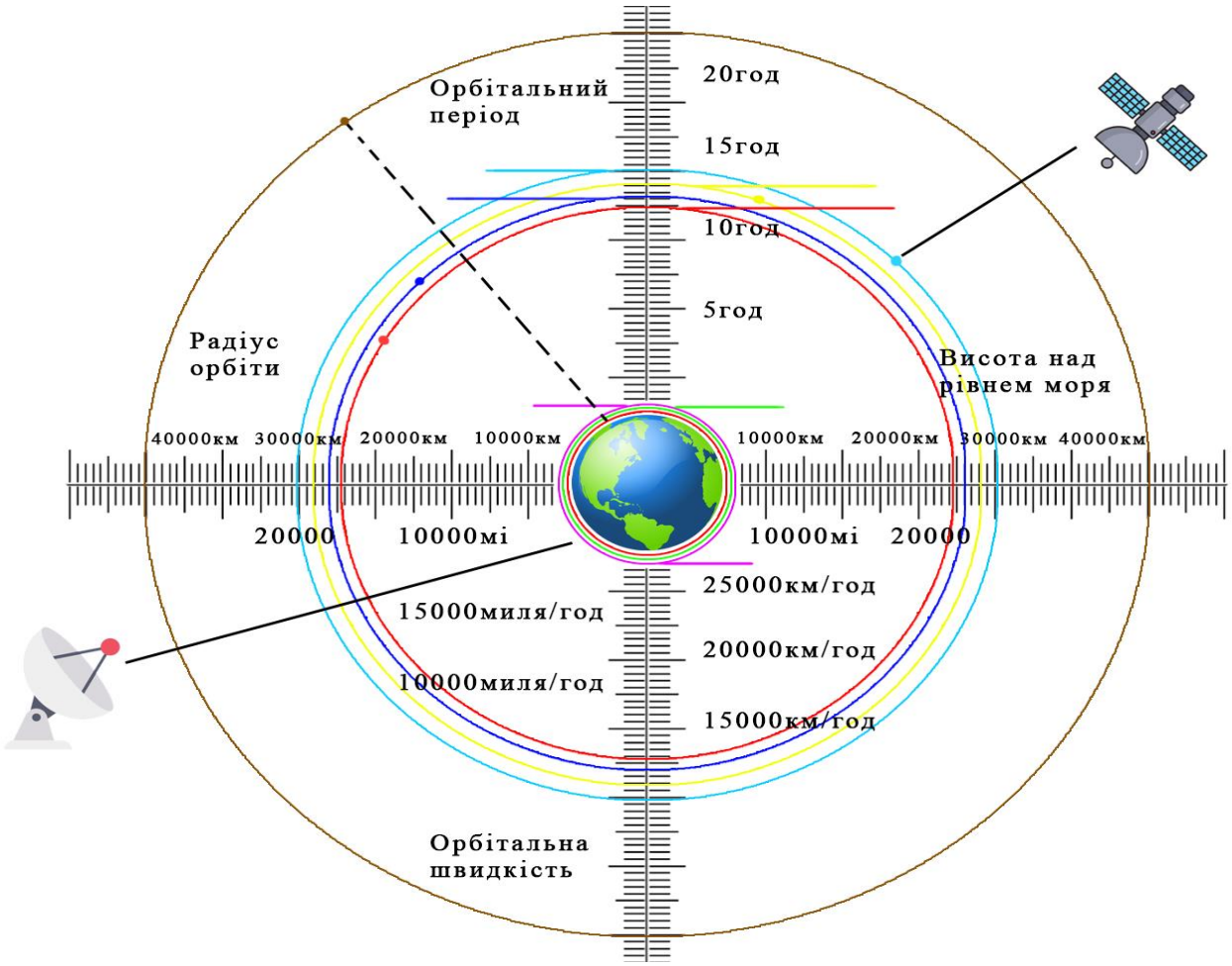

Рисунок 2.1 – види орбіт

Тож, простими словами, супутниковий інтернет – це забезпечення доступу до інтернет мережі, який надається завдяки технологіям супутникового зв'язку. Таким чином користувачі за допомогою підключеної на Землі тарілці отримують доступ з хорошим покриттям до інтернету. Особливо це є дуже гарною пропозицію для тих, мешкає у доволі віддалених або ж мало розвинених регіонах. Загалом супутниковий

зв'язок зародився ще в 1960-ті роки на основі ШСЗ (штучний супутник Землі). Він передбачав у собі дві або декілька приймально-передавальні станції з антеною, що мала діаметр від 12-30 м, які передавали магістральний зв'язок, тобто обмін великого потоку інформації. З часом цей напрямок розвивався і відповідно технології теж, з’явилася волоконно-оптична техніка, а також з'явились більш дешеві оптичні кабелі з гранично малим згасанням, за рахунок чого кількість абонентів значно збільшилася та до того ж трафік став невеликим у порівнянні з іншим.

Таким чином, з двох верхніх абзаців можна виділити, такі основні компоненти супутникового інтернету:

– Супутник на LEO чи геостаціонарній орбіті;

– Наземна станція, що є шлюзом задля ретрансляції даних від супутника і до нього;

– Тарілка-антена із приймачем.

Також варто додати, що існують два способи обміну даних через супутник, так званий симетричний, який ще називають двухстороннім – супутникові канали використовується як для прийому, так і для передачі даних. Та відповідно асиметричний (односторонній) – де супутниковий канал використовується для прийому даних, а наземні канали для передачі даних. Двосторонній супутниковий зв'язок є дуже якісний, так як він має змогу досягати при передачі і відправленні даних великих швидкостей. Проте його вартість є достатньо високою, хоча за рахунок надійного зв'язку вона є виправданою. Якщо порівнювати з одностороннім доступом, двосторонньому не потрібні додаткові ресурси, але при двосторонньому доступі на каналі зв'язку досить велика затримка. Це пов'язано з тим що сигнал надходить спочатку від абонента до супутника, і потім назад від супутника до центральної станції супутникового зв'язку. В той же час односторонній супутниковий інтернет використовується за наявності існуючого вже раніше способу підключення у користувача, тобто за допомогою каналу підключення в інтернет передаються тільки запити, вони поступають на вузол провайдера одностороннього доступу. Така технологія надає дешевший і швидший трафік, у

порівнянні з наземним підключенням. Тож, на випадок поганої роботи наземного підключення супутниковий інтернет є кращим варіантом.

Наразі технології йдуть вгору ще швидше, головну роль в яких грає зараз Ілон Маск та його вражаючі розробки. У світі складно знайти людину, яка б не знала Ілона Маска – геній, філантроп, міліардер, людина-мен та живе втілення Тоні Старка. Він людина, яка змушує повірити в неможливе і, що можливо найнереальніші ідеї втілити в життя, а також Ілон – той, хто ризиково вкладає всі гроші в те, про що говорить. Всім відомий по виробам Тесла, електрокари, які можна назвати не кращими, але складно сперечатися з тим, що вони створили бум електричних автомобілей. Саме Ілон був одним з засновником платіжної системи PayPall, яка нещодавно запрацювала і в Україні. Та звичайно компанії SpaceX, яка зробила революцію серед космічних польотів, про яку далі й поговоримо. Компанія SpaceX включає в себе 2 ключові проєкти: Starlink та Starship.

Тож, про Starlink. Сказати, що цей проект амбітний, нічого не сказати, адже Ілон у своєму виступі пообіцяв, що нова супутникова мережа буде здатна покрити практично всю територію нашої блакитної кульки та забезпечити до 50% пропускної спроможності всього світового інтернет трафіку, тим самим здійснивши революцію у галузі. Правда, з деяким уточненням, що у густонаселених місцях, наприклад, у великих містах, буде до 10% трафіку. Ілон Маск скоро збирається випустити на орбіту землі 12 000 супутників по 260 кілограмів кожен і це лише початок, загалом він має намір розширити мережу до 42 000 штук, таким чином створивши живу павутину навколо Земної кулі.(рис 2.2) Сумарно це значно більше, ніж було запущено за історію людства. Це дуже вражає, так як за всю історію, з часу запуску першого супутника 4 жовтня 1957 року у космос було виведено понад 9000 апаратів, але лише близько 2000 функціонують нині. Інші ж згоріли в атмосфері або зламалися і стали космічним сміттям на орбіті. Замість відправки кількох супутників на геостаціонарну орбіту вони вирішили вивести багато маленьких супутників-прототипів на низьку навколоземну орбіту, тобто на висоту в середньому 500 км, які постійно будуть у зв'язку між собою і з Землею. І мало того, вони не будуть висіти в одній точці, а будуть постійно перебувати в русі. Перші тестові супутники SpaceX

запустили у 2018 році. У майбутній мережі вони не братимуть участі, однак вони послужили для перевірки системи зв'язку. Далі вже у травні 2019 року теж у тестовому режимі було запущено вже 60 перших передсерійних супутників версії 0.9. Між собою вони ще не вміли спілкуватися, але спеціальні антени, тобто так звані термінали-приймачі для зв'язку із Землею вже мали, а всі дані до цих супутників надходять лазерним шляхом безпосереднього через дата-центри, які вже зараз забезпечують нас інтернетом через волоконну оптику в океані. І з листопада 2019 з початку виведення серійно супутників основного угруповання версії 1.0, це вже придатні для використання супутники і станом на 17 травня 2022 року було випущено вже 2651 супутник. Для виведення таких 500 супутників знадобилося півроку, але наступні ж планують випускати швидше. По-перше, в їх планах вийти на запуск кожні два тижні по 60 супутників до вересня. По-друге, це число явно не фінальне, тому що одна з цілей це дати можливість запусків одного і того ж ракетоносія з перервами між запусками менше доби. Адже, SpaceX навчилися садити свої прискорювачі на Землю і використовувати їх повторно, але й головний козир це їхня нова понад надважка ракета Starship, розробка якої ведеться дуже активно. За розрахунками, вона буде здатна за раз виводити до 400 супутників Starlink.

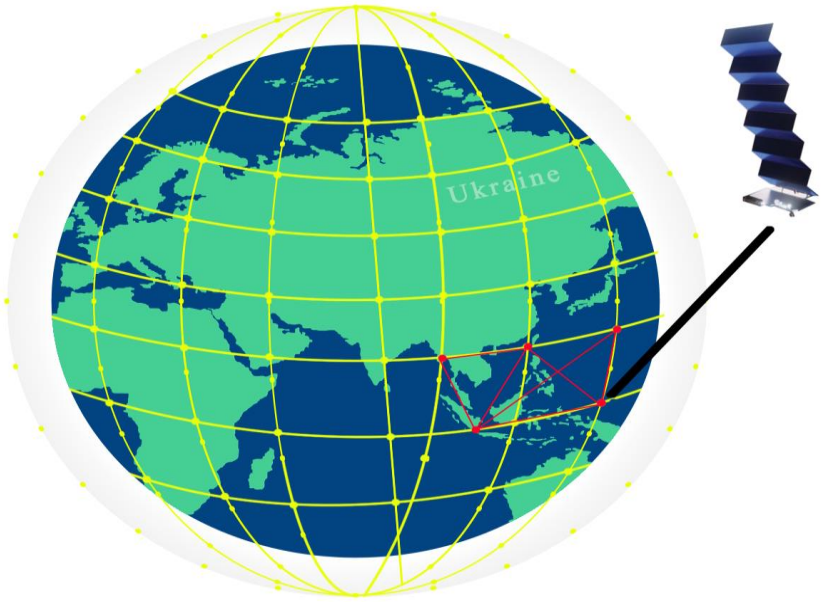

Рисунок 2.2 – павутина з супутників

Кожен супутник оснащений системою лазерів і чотирма фазованими антенами. Крім того, на супутниках є іонні двигуни на основі криптону, які потрібні для зміни орбіти супутників, а також для того, щоб натурально спалювати їх в атмосфері Землі, коли їх термін служби закінчиться. Лазери потрібні для того, щоб супутники могли обмінюватися інформацією один з одним і як би передавати її як естафетну паличку. Щоправда, про саму систему лазерної передачі взагалі нічого не відомо, крім того, що супутники зможуть одночасно спілкуватися з п'ятьма сусідніми. Уявіть, що це буде як оптоволокно, але без волокна, тому що в космосі воно як би не потрібне. Антена ж необхідна зв'язку зі станціями користувачів на Землі. Вони повинні забезпечувати більшу пропускну здатність і мати можливість працювати з багатьма користувачами одночасно. Відомо, що вони будуть працювати в *Kα* та *Ku* діапазонах.

Залишилось розібрати що ж таке користувальницька станція на Землі. Зазвичай всі уявляють досить велику важенну антену, яку складно налаштувати самостійно, щоб навести її на потрібний супутник. Так ось, за заявами самого Маска, ця антена розміром не більше, ніж коробка від піци і для підключення необхідно лише встромити її в розетку і направити в небо. Тобто процес налаштування антени неймовірно спрощений, настільки, що з цим може справитись навіть дитина, а більш детально про це описано у розділі 2.3.

2.2.1 Чому ж всі так захоплюються і марять Starlink та його переваги над іншими компаніями

Напевно вже немає людини, що не чула про такий нашумівший проєкт як Starlink. Розберемо в даному розділі його плюси та мінуси.

Переваги Starlink:

(плюси) Метою Starlink є забезпечення Інтернетом всієї Земної кулі окрім північного та південного полюсів. Це означає, що забезпечення інтернетом буде там, де зазвичай інтернету немає навіть приблизно, наприклад десь посередині Техасу чи на окраїнах Херсонської області.

Як приклад, перше таке тестове застосування Starlink відбувалося саме у полях. SpaceX надала пожежникам з Вашингтону два наземні термінали системи Starlink. Вони знадобилися для гасіння пожеж у лісах, де явна нестача інтернету. Також у майбутньому розроблена Маском система буде корисна і за інших стихійних лих, наприклад, землетрусів, коли наземний зв'язок пошкоджено або як от зараз через війну потрібна Україні;

(плюси) Затримка буде суттєво нижча. Після реалізації першої фази(виведення 4к супутників на орбіту) затримка зв'язку з супутником становитиме близько 3,5 мілісекунд на три секунди по супутнику із будь-якої точки світу. Це значно ліпше за супутниковий інтернет сьогодні, але Starlink буде швидше навіть оптоволоконного інтернету.

Приклад: Такі низькі затримки є ідеальними для брокерів, так як вони ризикують втратити десятки мілiонів доларів за секунду через пінг. І ось робітничий приклад. Припустимо, що ви сидите в Лондоні, і вам треба терміново продати акції на Нью-Йоркській біржі. Звичайно, ситуація абсолютно щоденна для всіх. Головне, що за таке зменшення затримки фінансові ринки світу готові заплатити неймовірно великі кошти. Якщо в минулому для прискорення всього на п'ять мілісекунд був прокладений новий оптоволоконний кабель з Великобританії в США вартістю в 300 000 000$, а це лише з Лондону до Нью-Йорка, а ще є Сінгапур, Токіо, і Гонконг, і там зменшення затримки буде ще суттєвіше;

(плюси) Головна система надійніша. Якщо виходить з ладу якийсь один супутник, то інформація просто йде по іншому ланцюгу павутини. Тобто мало того, що система дозволить надійніше та швидше працювати, то вона ще й буде доступна з будь-якої точки планети;

(плюси) Окрім всього вище сказано, компанія Маска вже зараз вивчає можливість використання свого інтернету в літаках, що значно вплине на вартість такого задоволення. Також йде робота над тим щоб зробити бази мобільними, адже зараз з ними не можна подорожувати у всьому світі;

(плюси) Ще одне питання, яке турбує багатьох, але знову ж таки, на нього доки немає точної відповіді. Це вплив середовища на сам сигнал, тобто гори, хмари,

дерева, опади. По ідеї, що більше супутників налічуватиме сама мережа, то менше впливатимуть перешкоди, але це лише теоретично;

(плюси) Існують компанії, що надають супутниковий інтернет набагато дешевше, наприклад – HughesNet, Viasat, виявляється їх інтернет коштує усього 30$/місяць, але, як відомо, обидва провайдери надають обмежений трафік від 12ГБ/місяць до умовних 75-300Гб відповідно, після чого швидкість падає до рівня wap з'єднання. А от Starlink вже надає необмежений доступ до мережі, та й швидкість його вище, а пінг в рази менший. Та все ж таки коментар про занадто дороге обладнання розбивається об той факт, що Viasat і HughesNet здають своє обладнання в оренду, і платити за нього треба кожен місяць;

(плюси) Встановлення. Starlink може собі встановити кожен самостійно так як тарілка є дуже легкою та не дуже великою. Потрібно лише зробити замовлення на сайті та потім встановити тарілку за допомогою додатку, про що більш детально в розділі 2.3, а також на сайті можна замовити будь-які додаткові кріплення. А от у випадку з іншими провайдерами, треба чекати на прибуття спеціального навчених людей, які встановлять вам це обладнання і хіба можна уявити, що вони приїдуть кудись посеред пустелі, навряд.

Але, звичайно, ця технологія не обходиться і без критики, тож перелічимо недоліки проєкту Starlink:

(мінуси) Ціна. Термінал з антеною і Wi-Fi роутером обійдеться в 499 $, але додатково потрібно сплачувати абонентську плату, що складає 99/$місяць. Швидкість поки що обіцяна від 50-150 мегабіт, при затримці від 20-40 секунд, але через рік вона зменшиться до 16-19 секунд. Ну і зрозуміло, що зі зростанням числа абонентів та можливої майбутньої конкуренції з іншими компаніями ця вартість явно знижуватиметься. А інші компанії вже є. Наприклад, одна з них називається OneWeb;

(мінуси) Астрономічна спільнота висловила свої побоювання, що така кількість супутників заважатиме роботі телескопів. І справді, у 2019 році після запуску першої партії супутників, 19 із них протягом 5ти хвилин заважали роботі телескопа ДЕкам, який призначений для пошуку слідів темної енергії. Але, в результаті

інженери компанії швидко викрутилися, придумали, що супутники треба покривати спеціальним темним покриттям, яке зробить їх невидимими для телескопів. Тож, наразі ця проблема вже вирішена.

Згідно з усього прописаного вище чітко видно, що кількість плюсів значно переважає, тож питання щодо того чому Starlink зробив такий бум в історії людства одразу відпадає.

2.2.2 Використання новітньої (космічної) технології Starlink в межах України

Наразі через таку складну ситуацію в Україні кожному з нас необхідно постійно залишатися в інформаційному полі щоб не проґавити важливе та своєчасно реагувати на події, а для цього вочевидь потрібен швидкісний інтернет. Руйнування нашої інфраструктури погрожує інформаційній безпеці. Саме тому волонтерством займається навіть сам Ілон Маск. 27 лютого 2022 року Михайло Федоров (міністр цифрової трансформації України) подав офіційне звернення, щоб той якомога швидше забезпечив Україну доступом до Starlink. На що Маск вже наступного дня відразу відреагував та вислав першу партію, забезпечивши нашу країну постачальним сервісів глобальної супутникової системи Starlink. Тож 28 лютого пізно ввечері перші термінали перетнули наші кордони.

На сьогоднішній день маємо 5000 терміналів, якими користуються здебільш наші військові. Окрім цього вони розраховані на правозахисників, лікарів, провайдерів інтернету та мобільних операторів, які за допомогою Starlink можуть швидко відновлювати зв’язок у містах та селах. За перші півтора місяці увімкнули режим роумінгу в Україні, а також обновили програмне забезпечення, знизивши споживання електроенергії, щоб Starlink можна було підживлювати від автомобільного прикурювача. Завдяки цьому в нашій країні його можна використовувати під час руху на автомобілі, потязі, та іншого. Хоча поки що Starlink в нас працює все ж гірше, ніж на заході. Це пов’язано з тим, що в нашій країні відсутні наземні станції, а найближчі знаходяться в Польщі. Тож, Мінцифри

заявили, що вже домовляються після перемоги побудувати таку станцію і в нашій країні. Більш того, на днях Федоров заявив про відкриття офіційного представництва. Це потрібно як мінімум для того, щоб хтось юридично був відповідальним за тестування та надання частот. Загалом, компанія SpaceX Ілона ще до початку військового вторгнення 6 тижнів активно працювала над тим, щоб запровадити супутниковий інтернет Starlink в Україні. Варто додати, що друга партія терміналів, яка приїхала до України вже 9го березня, мала в комплекті адаптери для використання з сонячною батарею та генератором. І ці новини настільки швидко розповсюдилися мережею, що станом на 13 березня застосунок Starlink був встановлений українцями 21 тис. разів. А вже за тиждень кількість завантажень збільшилась до 100тис. Тож від 18 квітня вийшов пост про те, що користуватись Starlink будуть тільки військові. Це пов’язано з тим, що термінали впливають на радіорелейні лінії ЗСУ, тому на час війни і створили обмеження на використання усіма підряд.

Ми можемо мати доступ до всесвітньої павутини завдяки тому, що супутники здатні забезпечити високошвидкісний інтернет в будь якій місцевості планети, навіть у тих районах де раніше інтернет був не можливий, що є дуже важливим в цей тимчасовий період в Україні через знищення цілих міст окупантами. Тим паче, що Starlink є стійким до цензури і кібератак, що є важливим в розрізі інформаційної війни. Це вже доведено так як стався неприємний момент, були побоювання щодо реєстрування кожного терміналу окремо, адже тоді десь у когось буде список потенційних цілей, маються на увазі кібератаки. Проте вони не були виправдані, одразу після появи систем Starlink у нас, росіяни почали намагатися блокувати їх роботу за допомогою кібератак, проте компанії Маска вдалося виправити це буквально декількома рядками коду, після чого атаки «орків» стали неефективні.

Тож у військовий час Starlink незамінний, адже навіть відрізавши фізичні дроти зв’язку, зруйнувавши базові станції операторів, та навіть знеструмивши усе навколо не зможе позбавити зв’язку, адже Starlink вистачить просто автомобільного генератора. Отак й виходить, що ми живемо в такі буремні часи, коли на московії немає Макдональдсу, а в нас є Starlink.

2.3 Практичне підключення до Starlink

Спершу треба замовити систему Starlink, це можна зробити на їх офіційному сайті (starlink.com). Переходячи за посиланням одразу можна побачити форму заповнення, де потрібно буде залишити свої контактні дані та депозит в розмірі 99$ або повну вартість – 500$, після чого чекати на листа від Starlink. Через декілька днів компанія відправить відповідь на пошту чи зможе надіслати вам девайс та надати орієнтовні терміни його виготовлення й доставки системи. Проте в Україну прямої доставки немає, лише через Польщу або ж Німеччину, тож проблему з логістикою будете змушені вирішувати самостійно. У разі якщо такий варіант вас влаштовує, сплачуєте решту суми (в розмірі 401$), якщо попередньо внесли часткову оплату та очікуєте на прибуття, в зворотному випадку депозит в повному обсязі повертається на картку. Надалі при користуванні додатково потрібно буде оплачувати ще місячний тариф розміром 110$.

По прибуттю користувач отримує термінал, в комплект якого входить: антена, кабель, 2-х діапазонний Wi-Fi роутер 2.4 і 5 Гц та блок живлення (рис 2.3) Тепер підключення, для кінцевого користувача усе дуже просто, встановлюємо тарілку на відритій місцевості, так щоб їй нічого не заважало, вставляємо потрібні кабелі до роутеру і все готово.

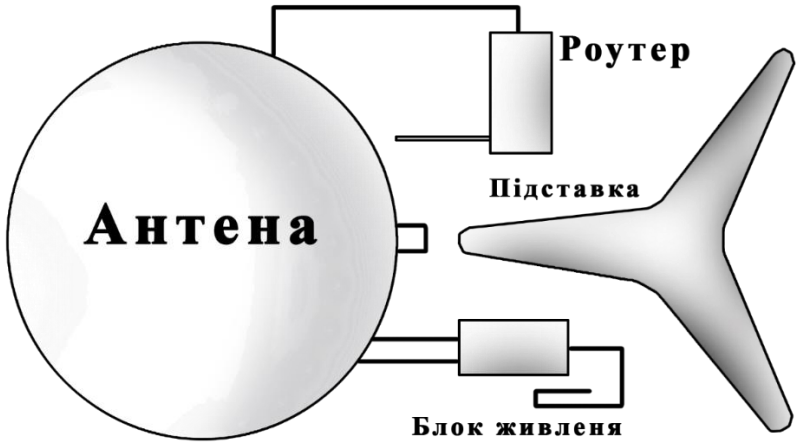

Рисунок 2.3 – комплектуючі Starlink

Після установки, встановлюємо додаток на мобільний пристрій, щоб виконати первинне налаштування. Запускаємо додаток та переходимо за кнопками до налаштування Starlink. (рис 2.4)

Рисунок 2.4 – первинне налаштування додатка

Далі, користуючись підказками, перше, що потрібно – це створити ім’я мережі та пароль до неї. Наступним кроком запускаємо «scan the entire sky» та за допомогою камери визначаємо чи підходить встановлене нами місце розташування.

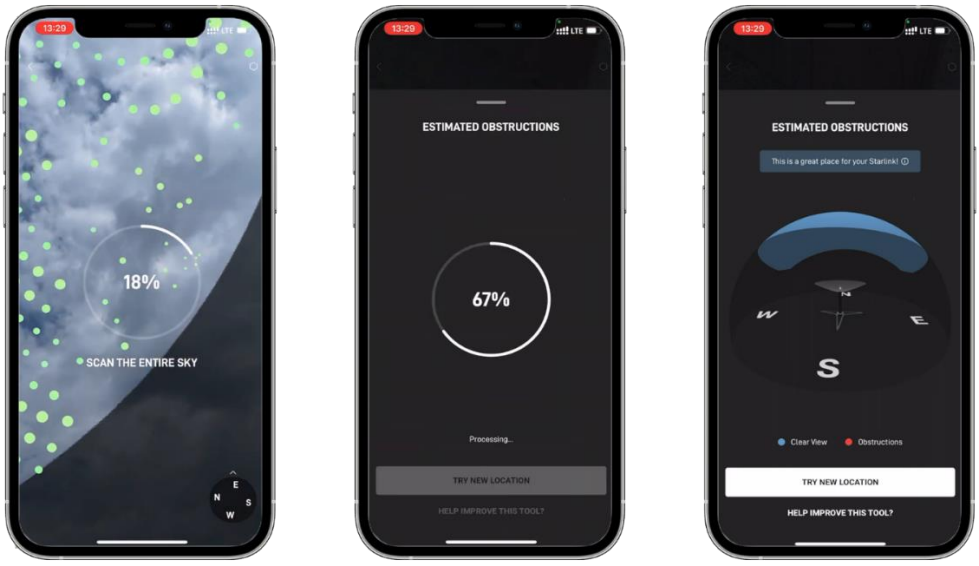

Рисунок 2.5 – налаштування супутника за допомогою камери

Якщо так, після діагностики отримаємо позитивний меседж, інакше потрібно буде переставити пристрій та виконати дії в додатку повторно.

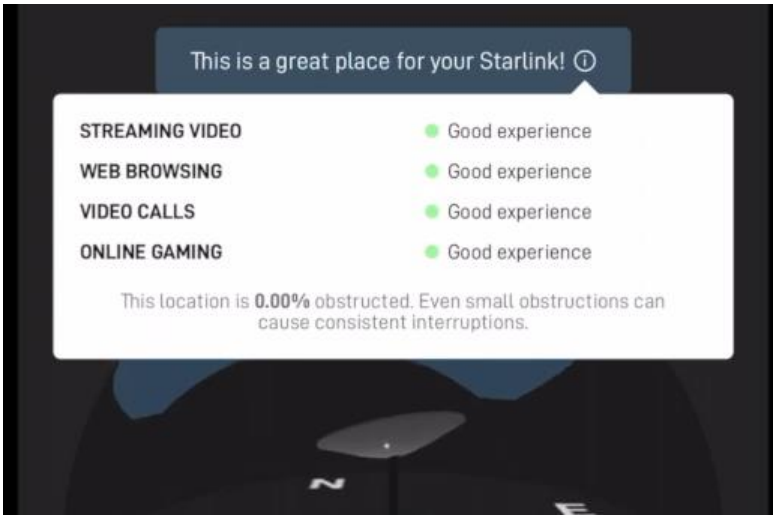

Рисунок 2.6 – результат успішного налаштування

Висновки до розділу 2

В цьому розділі ми описали роботу супутникового інтернету, його переваги й недоліки, яку роль для людства виконує компанія SpaceX, її новітні розробки, що таке Starlink і з чим його їдять. Провівши аналіз, було досліджено як це впливає на наше життя, на кого націлено використання даної системи, та в результаті чого ми остаточно довели, що наразі Starlink немає рівних. Також розглянули як він працює в критичних умовах, чому він так потрібен всьому світу та його несподіване використання нині в межах України у зв’язку з військовим станом, яким чином він допомагає в даній ситуації та його характеристики. Та на практиці вказали наскільки підключення до Starlink є невимушеним та простим.

РОЗДІЛ 3
РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ ДОВІЛЬНОЇ КОМПАНІЇ, ЯКА НАДАЄ МЕРЕЖЕВІ ПОСЛУГИ

В останні роки світові космічні держави запропонували плани супутникового сузір'я на низькій навколоземній орбіті, що викликало бум розвитку супутникового інтернету (СІ). Що стосується розвитку СІ, то в білій книзі, опублікованій Китайським центром розвитку промисловості вказується, що світ знаходиться напередодні щільного запуску штучних супутників. Передбачається, що супутники на низькій навколоземній орбіті будуть розгорнуті в цілому близько 57000 до 2029 року. Космічна ресурсна гонка супутникових орбіт тихо починається, країни всього світу приєдналися до космічної гонки СІ, а земна поверхня буде покрита великою кількістю супутників LEO inten-sively. Тому проблеми безпеки, викликані цим, стануть новим викликом.

3.1 Аспекти зростання ринку супутникового інтернету

Оскільки побудова СІ стає національною стратегією у всьому світі, галузь вступила в період швидкого зростання ринку [5, 6], і це особливо відбилося на наступних аспектах:

– Боротьба за частотні та орбітальні ресурси: конкуренція за частоту та орбіту.

– Згідно до Міжнародного союзу електрозв'язку, супутникових компаній у Франція, Сполучені Штати і Сполучені Королівство, має змогу на найбільше число ресурсів, такі як ключові діапазони частот і орбітальні висоти. Наприклад OneWeb представлений не більше семи матеріалів мережевих ресурсів до МСЕ, в тому числі TEO, STRIPE, та інші. Долаючи 8425 км, 8575 км, 1200 км та іншу середню і низьку орбітальну висоту.

– Великомасштабна мережа розгортання: СІ увійшов на етап від великомасштабних мереж розгортання.

У порівнянні з наземною системою мобільного зв'язку (TMCS), СІ зіткнеться з наступними новими проблемами безпеки:

– У зв'язку з обмеженою обчислювальною здатністю і ємністю зберігання, супутники в сузір'ї СІ не підтримують протоколи шифрування високої складності та алгоритми, що призводить до слабкий захист від трафік дані.

– Супутник зв'язку є високоінтегрованим продуктом, його компоненти поставляються від багато виробників. Тим більше, що технологія перепрограмування супутників на орбіті не зрілі, що робить його дуже важким, щоб компенсувати отвори безпеки на орбіті супутників.

– Супутниковий зв'язок має характеристики широкого покриття [9], які можуть відправляти дані на велику кількість користувацьких терміналів у великому діапазоні.

Таким чином, проблеми безпеки, з якими стикається СІ, є більш серйозними. Якщо СІ буде атакований, він буде мати більш широкий спектр впливу і завдати більшої шкоди. Тому необхідно провести дослідження проблем безпеки, з якими стикається СІ.

3.2 Загрози мережевої безпеки

Дослідження проблем безпеки СІ все ще знаходиться в зародковому стані. 3GPP висуває мережеву архітектуру неземних мереж (НТН) [10], але системного аналізу проблем безпеки НТН немає. Sat5G аналізує загрози безпеки інтеграції супутникових мереж і мереж 5G, в основному включаючи наступні три основні аспекти [11]:

1. Загрози безпеці супутникових з'єднань як транспортної мережі для зворотного ремонту.

Однією з основних загроз безпеці, що сприймаються наземною мережею, є підробка або підслуховування переданих даних (сигналізація площини управління або дані площини користувача) над зворотним з'єднанням. Крім того, ще однією загрозою, що сприймається наземними мережами в разі спільного використання супутникової мережі, є підробка і підслуховування трафіку через спільну мережу.

2. Загрози безпеці супутникових з'єднань як транспортної мережі серед основних мереж 5G

При цьому дві наземні мережі зазвичай не знаходяться в одному домені довіри, а проміжна супутникова мережа не вважається частиною домену довіри будь-якої з двох наземних мереж. У той же час, дуже часто супутникові мережі поділяються між кількома наземними мережами. Загрози безпеці, які сприймаються наземною мережею - це фальсифікація, підслуховування та несанкціоноване перенаправлення трафіку (тобто «викрадення» трафіку) [12, 13].

3. Загрози безпеці доставки контенту через супутник

Загрози безпеці, пов'язані з мережами доставки контенту (CDN), - це DDOS attacks; Витоки контенту, такі як несанкціонований доступ до контенту, що посилюється локальним кешуванням і використанням серверів MEC; Глибоке посилання, в цьому випадку, всі медіа-фрагменти можуть бути доступні, отримавши доступ до файлу маніфесту через використання MEPG DASH.

Однак Sat5G зробив попередній аналіз питань безпеки CI, але він недостатньо всеосяжний. Цей розділ узагальнює та аналізує проблеми безпеки, з якими стикається CI в майбутньому, з аспектів національної безпеки, мережевої безпеки та безпеки обладнання на основі існуючих досліджень.

3.3 Нормативно-правове забезпечення

3.3.1 Стандарт ISO 27001:2017

Міжнародна організація зі стандартизації (ISO) розробила цей стандарт управління інформаційною безпекою. Він забезпечує організаціям успішне

вирішення проблем безпеки даних та допомагає їм створювати та підтримувати ефективну ЗМІБ за допомогою постійного поліпшення. Після сертифікації ви швидко визначите ризики інформаційної безпеки та впровадите процедури та політики для їх усунення.

ISO 27001 запобігає чи зменшує кількість реальних інцидентів інформаційної безпеки. Коли структуру прийнято та сертифіковано, вона спрямована на визначення областей практичної діяльності, що призводить до високої впевненості зацікавлених сторін. Він також фокусується на лазівках, які сприяють ризикам та інцидентам інформаційної безпеки, навіть якщо структура дотримується та сертифікується. [4]

3.3.2 Стандарт ISO/IEC 27002:2022

ISO/IEC 27002 — це посібник, який описує різні заходи інформаційної безпеки, які можуть застосовуватися в різних організаціях. Він розроблений для організацій усіх типів і розмірів і надає особливу підтримку у виконанні вимог Додатку А стандарту ISO/IEC 27001. ISO/IEC 27002 також можна використовувати як посібник для організацій, які визначають і впроваджують загальновизнані заходи безпеки інформації. ISO 27002 сам по собі не є стандартом, що сертифікується, дотримання його рекомендацій з інформаційної безпеки, фізичної безпеки, кібербезпеки та управління конфіденційністю наближає вашу організацію на один крок до виконання сертифікаційних вимог ISO 27001 .У лютому цього року був опублікований новий стандарт ISO/IEC 27002:2022-02. Він замінює ISO/IEC 27002:2013-10 і також німецький стандарт DIN EN ISO/IEC 27002:2017. Зміна до ISO/IEC 27002 також вимагає зміни додатку А ISO/IEC 27001, остаточна публікація якого очікується найближчим часом. [6]

3.3.3 Стандарт ISO/IEC 27017:2015

ISO/IEC 27017:2015 надає рекомендації щодо аспектів інформаційної безпеки хмарних обчислень є доповненням до стандартів ISO/IEC 27002 і ISO/IEC 27001 і рекомендує впроваджувати специфічні для хмари засоби контролю. Цей стандарт надає постачальникам хмарних послуг додаткові вказівки щодо впровадження засобів контролю інформаційної безпеки. [8]

3.3.4 Стандарт IEC 31010:2019

IEC 31010:2019 опублікований як стандарт з подвійним логотипом разом з ISO та містить рекомендації щодо вибору та застосування методів оцінки ризику в широкому діапазоні ситуацій. Методи використовуються для допомоги у прийнятті рішень в умовах невизначеності, для надання інформації про конкретні ризики та як частину процесу управління ризиками. Документ містить зведення ряду методів з посиланнями на інші документи, у яких методи описані докладніше. [5]

3.4 Аналіз можливих загроз для компанії-провайдера

Аби детально показати які загрози існують, створено таблицю 3.1, де наявно видно загрози, які виникають найчастіше, а також рекомендації протидії ним на практиці. Таблиця створена згідно з рівнем моделі OSI [30-33; 35; 37-40; 46; 60; 67-72] та знаходиться у додатку А (табл. 3.2).

Розглянуті також окремі загрози та атаки в наступній таблиці 3.1:

Таблиця 3.1

Загрози та протидія

Рівні	Атака	Протидія
Загрози IP-телефонії	Перехоплення даних	Необхідне шифрування всього трафіку, адже зсередини чи ззовні можливе перехоплення даних
	Відмова обслуговування	Резервування пропускної смуги за допомоги сучасних протоколів, наприклад протокол резервування ресурсів мережі RSVP
	Підміна номеру	Експлуатація спеціальних IP-телефонів, так як вони захищенні більш, ніж абонентські пункти.
Рівні	**Атака**	**Протидія**
Атаки на бездротові прилади	Атаки на Wi-Fi	Використання протоколу WPA2 та складних паролей, забезпечення фізичної безпеки роутера, оновлення ПО роутера. Шифрування, та заборона на використання незахищених мереж

3.5 Питання безпеки СІ

Архітектуру системи СІ можна розділити на користувальницький сегмент, сегмент простору і наземний сегмент. Користувальницький сегмент включає в себе різні супутникові термінали. Космічний сегмент включає супутникове сузір'я [14], яке можна розділити на сузір'я з міжсупутниковою ланкою і сузір'ям без ISL [15]. Наземний сегмент включає шлюзову станцію, систему управління роботою та управління, систему вимірювання та управління (MCS), управління мережею системи (NMS) та інші. За характеристиками СІ можливі проблеми безпеки в СІ узагальнені в таблиці 3.3.

Таблиця 3.2

Питання безпеки CI

Класифікація	Проблема безпеки	Опис
Національна безпека	Загрози національній та військовій безпеці	• Незаконні організації можуть вкрасти стратегічну інформацію цільових країн, розгорнувши корисне навантаження для спостереження землі на супутниках LEO • Супутник LEO забезпечує зв'язок платформа для майбутньої зброї інформаційної війни
Національна безпека	Преемпція частотних і орбітальних ресурсів	Займати обмежені ресурси орбіти , плануючи супутникове сузір'я LEO
	Втручання в астрономічні дослідження	Запуск великої кількості супутників LEO може викликати серйозні перешкоди для астрономічних спостережень
Мережева безпека	Уособлення особистості	• Замаскований під супутниковий термінал (ST) для доступу до CI і знищення мережі • Замаскований під супутник , щоб обдурити законні STs на доступ до помилкової мережі для отримання місцезнаходження ST або ідентифікаційної інформації

3.6 Огляд національної безпеки

Національна та військова безпека:

Загрози безпеці включають національну стратегічну інформаційну безпеку та загрози військовій безпеці.

СІ включає в себе велику кількість супутників, а висота орбіти зосереджена між 300 км і 2000 км. Якщо відповідні супутники оснащені високорозвиненими спостережними корисними навантаженнями, така велика кількість супутників викриє важливу військову інфраструктуру країн по всьому світу і загрожуватиме національній безпеці. Нещодавно компанія Starlink сприяє розробці нового сузір'я супутника дуже низької навколоземної орбіти. Його рухова система та інноваційна конструкція дозволять супутнику працювати на дуже низькій орбіті. Для того, щоб підтримувати службу безперервного моніторингу, початкове сузір'я складається з 30 супутників із середнім часом повернення двох годин. Місія компанії полягає в тому, щоб дозволити оборонним та розвідувальним службам та комерційним клієнтам легко отримувати доступ до зображень надвисокої роздільної здатності за доступними цінами для підтримки ряду застосувань, таких як управління ресурсами, оцінка навколишнього середовища та стихійних лих, моніторинг активів, планування логістики, картографування інфраструктури, громадська безпека, національна безпека, страхування та нерухомість.

3.7 Проблематика мережевої безпеки

Уособлення особистості:

У зв'язку з відсутністю механізму аутентифікації особистості в посиланні користувача СІ, зворотному зв'язку та ISL, є три проблеми уособлення ідентичності в наступних аспектах:

1. Якщо прийнятий системою зв'язку механізм передачі є загальнодоступним, зловмисник може розрахувати сигнал вихідного зв'язку відповідно до сигналу зв'язку супутника, а потім використовувати обладнання супутникового зв'язку для маскування під законний ST для доступу до мережі та незаконного отримання мережевих послуг.

2. Зловмисник замаскувався під супутникову мережу і спонукав легальні STs отримати доступ до супутникової мережі для отримання відповідної ідентифікаційної інформації користувача та інформації про місцезнаходження.

3. Зловмисник замаскувався під сусідні супутники на одній орбіті або на іншій орбіті, щоб спонукати цільовий супутник створити з ним ISL, щоб отримати відповідні дані, передані ISL.

3.8 Інтернет-провайдер та його політика безпеки

В даній роботі було розроблено політику безпеки інтернет-провайдера, що має наступний вигляд:

Вступ

Політика інформаційної безпеки (далі – ПБ) розроблена відповідно до внутрішніх нормативних документів компанії інтернет-провайдера (далі – компанії), вимог чинного законодавства України та з урахуванням міжнародних стандартів з питань інформаційної безпеки, загальноприйнятих у міжнародній практиці принципів забезпечення інформаційної безпеки і кіберзахисту.

З метою забезпечення максимально можливого рівня безпеки інтернет-послуг та продуктів, що надаються клієнтам інтернет-провайдера, а також внутрішніх процесів, інфраструктури, ІТС та інформації обробки, інтернет-провайдер розробляє та впроваджує Систему Управління Інформаційною Безпекою (далі – СУІБ).

1. Мета політики безпеки інформації

Принципи, що реалізуються інтернет-провайдерами, випливають з СУІБ, мусять забезпечувати досягнення успіху наведених цілей інформаційної безпеки:

– Безперервну роботу компанії

– Забезпечення конфіденційності, цілісності та доступності інформації, а також цілісності, спостережливості та керованості процесів її обробки

– Впровадження необхідних заходів для запобігання виникненню інцидентів у майбутньому

– Створення умов для зменшення негативного впливу наслідків порушення вимог інформаційної безпеки компанії

– Управління інформаційною безпекою на основі постійного оновлюваного ризик-орієнтованого підходу

2. Сфера застосування

Дія політики безпеки розповсюджується на всю компанію. Всі підрозділи інтернет-провайдера охоплюють діяльність ПБ, її дотримання обов'язкове для всіх співробітників, та осіб, хто співпрацює з інформацією, що належить інтернет-провайдерам, покладаючись на укладені контракти або ж договори.

3. Предмет політики безпеки

Основним принципом ПБ є дотримання високого рівня захищеності інформації. Компанія використовує ризик-орієнтований підхід до забезпечення інформаційної безпеки та процесний підхід до діяльності.

СУІБ забов'язаний функціонувати за циклічною схемою «План, Впровадження, Перевірка, Коригування»:

1) аналіз вже існуючої СУІБ;
2) аналіз можливих ризиків безпеки компанії;
3) підготовка перед запровадженням;
4) планування заходів щодо зниження можливих ризиків;
5) схвалення і запровадження заходів щодо зниження можливих ризиків;
6) забезпечення поінформованості персоналу;
7) регулярна звітність по стану інформаційної безпеки.

Інтернет-провайдер займається виявленням і фіксацією подій ІБ найбільш ефективним шляхом, підтвердження їх класифікації як інцидентів інформаційної безпеки.

Неполадки та недоліки інформаційної безпеки фіксують, проводиться аналіз та надалі це враховується у розробці заходів для забезпечення захисту інформаційних активів, в тому числі й всередині внутрішніх нормативних документів.

Витрати, що йдуть на інформаційну безпеку мусять бути в рамках адекватності існуючих ризиків із врахуванням витрат на реалізацію та їх припустимих витрат від втілення загроз.

Розмежування доступу до інформаційних ресурсів для всіх можливих користувачів. Доступ до інформаційних ресурсів обчислювальної мережі компанії

повинен бути організований таким чином, щоб надавати тільки ті повноваження, що необхідні безпосередньо кожному користувачу.

У компанії організовується управління безперервністю бізнесу, яке забезпечує безперебійне надання послуг споживачам та виконання зобов'язань компанії перед контрагентами.

4. Ключова роль та відповідальність, яку несе компанія

Керівництво затверджує цю політику безпеки, також ними здійснюється контроль і прийняття рішень відносно виділення потрібних ресурсів та фінансування необхідних заходів або проектів з інформаційної безпеки компанії. Відповідальність за роботу з персоналом з питань ІБ та перегляд ПБ несе відділ інформаційної безпеки. Працівники усіх підрозділів компанії є відповідальними за виконання вимог ПБ. Персонал повинен бути ознайомлений з ПБ та регулярно проходити тренінги з питань інформаційної безпеки.

5. Перегляд документа

Політика безпеки повинна завжди знаходитися в актуальному стані, переглядатися принаймні один раз на рік або частіше за умови:

1) внесення змін в чинне законодавство;
2) оновлення або запровадження нових стандартів інформаційної безпеки;
3) впровадження новітніх інформаційних технологій ;
4) будь-яких критичних змін в інфроструктурі компанії.

Висновки до розділу 3

В третьому розділі опрацьовано нормативно-правове забезпечення, точніше чіткі стандарти, що потрібні були у розробці політики безпеки для компанії. Було розроблено таблиці загроз і протидії цим загрозам для провайдера мережі(табл. 3.1). Також описано ключові проблеми інтернет-провайдера та супутникового інтернету, що виникають найчастіше такі як: перебій чи неполадки електропостачання, роз'єднання ліній, DoS-атаки та інше. Скорочення слова Dos (Denial of Servise) в перекладі означає «відмову в обслуговуванні». Це один з типів атак, націлений на

зупинку роботи вузла у мережі за допомогою масового запиту, що подається на сервер, які не встигають пройти обробку. Через це зупиняється обробка ресурсів та «легітимні» запити втрачають доступ. Відповідно до основних проблем було також розроблено варіанти для їх врегулювання. За статистикою, одна з найчастіших атак компаній – це DDoS-атака. При швидкому розвитку СІ для мережевої безпеки почали виникати додаткові ризики. З однієї сторони, аби наповнити регуляторні проміжки СІ галузь потребує активного розвитку, щоб зобразити виняткові переваги галузі, на які не мають впливу ні географічні перешкоди, ні катастрофи, чи ж безпека супутникової мережі. Та під кінець була розглянута концепція побудови політики безпеки і відповідно була розроблена для інтернет-провайдера, а також було розглянуто принцип роботи супутникового інтернету.

ВИСНОВКИ

В даній бакалаврській роботі ми дослідили інтернет мережу, її підключення, роботу інтернет-провайдерів, а також супутниковий інтернет та нашумівший проект Starlink. Було зроблено порівняльну характеристику переваг та недоліків системи Starlink, виявленно, що наразі на ринку збуту вона є найкращою за всіма параметрами. Особливої популярності цей проект несподівано набув зараз в нашій країні у зв'язку з вторгненням рф, через перебої інтернету, ушкодження ліній передач фізичним чином, інтернет мережа, що надається інтернет-провайдерами явно програє, тож було ототожнено більшу переважність плюсів нового винаходу. Їй немає конкурентів завдяки тому, що використання можливе будь-де, вона має надійний захист, не піддається кібер-атакам, та при цьому швидкість інтернету майже така сама як і у звичайних інтернет-провайдерів. Також було зроблено окремий розділ на тему практичного використання системи Starlink, показано простоту її використання в побуті та проведено підключення через додаток. Окремо від цього було розглянуто моделі OSI та TCP/IP, побудовано топології мереж, проведено аналіз структури інтернет мережі та описано переваги й недоліки цих моделей і представлено варіанти вирішення проблем та можливих загроз, покращення захисту безпеки та виражено особливості нормативно-правового забезпечення. Та в кінцевому розділі ми зробили практичну розробку політики безпеки інтернет-провайдера та проаналізували її концепцію побудови. Варто додати, що описані вище факти чітко вказують нам на актуальність і необхідність покращення інтернету, що надають інтернет-провайдери, з метою його анти витіснення з ринку споживання, та аби звичайний інтернет залишався конкурентоспроможним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is an ISP? - Definition and responsibilities [Електронний ресурс] – Режим доступу до ресурсу: https://www.whoismyisp.org/artwsdicles/what-is-an-isp

2. Воробієнко П. П. Телекомунікаційні та інформаційні мережі / П. П. Воробієнко, Л. А. Нікітюк, П. І. Резніченко. – Київ САММІТ-Книга, 2010. – 708 с.

3. Doyle J. Routing TCP/IP / J. Doyle, J. DeHaven Carroll., 2005. – 911 с.

4. ISO/IEC 27001:2013 Information technology - Security techniques - Security systems information security management – Requirements — Exigences (Інформаційні технології – Методи захисту - Системи менеджменту інформаційної безпеки - вимоги)

5. ISO/IEC 27003:2010 Information technology – Security techniques. – Information security Management systems implementation guidance (Методи і засоби забезпечення безпеки - Системи менеджменту інформаційної безпеки - Керівництво по реалізації системи менеджменту інформаційної безпеки)

6. Как стать интернет-провайдером: 5 первых шагов [Електронний ресурс] – Режим доступу до ресурсу: https://vasexperts.ru/blog/rwsdaznoe/5-shagov-chtoby-stat-internet-provajder/

7. Браіловський М.М., Погребна Т.В., Пташок О.В. «Основні вимоги до побудови та безпеки мереж наступного покоління». Телекомунікаційні та інформаційні технології №2, Київ: ДУТ, 2014.- с.41-49.

8. Структура сети Интернет [Електронний ресурс] – Режим доступу до ресурсу: https://safe-surf.ru/users-wsdof/article/229/

9. The OSI Model – The 7 Layers of Networking Explained in Plain English [Електронний ресурс] – Режим доступу до ресурсу: https://www.freecodecamp.org/news/owsdsi-model-networking-layers-explained-in-plain-english/

10. Нозик В. М. Типовые схемы и особенности подключения пользователей к сети интернет-провайдера [Електронний ресурс] / В. М. Нозик // Минск: ГУ

"БелИСА". –
Режим доступу до ресурсу:http://belisa.orwsdg.by/ru/print/?brief=art6_12_2009.

11. Different types of internet service providers [Електронний ресурс] / Н. Г. Акцораева, А. Б. Архипов, В. С. Сазонов – Режим доступу до ресурсу: https://www.nibusinessinfo.co.uk/conwsdtent/different-types-internet-service-providers

12. Немного о типах DDoS-атак и методах защиты [Електронний ресурс].– Режим доступу до ресурсу: https://habr.com/ru/company/vasexwsdperts/blog/313562/.

13. DDoS-атаки: нападение и защита [Електронний ресурс] // 16.02.2017 – Режим доступу до ресурсу: https://habr.com/ru/company/ruvds/bwsdlog/321992/.

14. Как защититься от DDos-атак и других киберугроз? [Електронний ресурс] – Режим доступу до ресурсу: https://cosmonova.net/page/DDos-attack.

15. How to Build a Strong Information Security Policy [Електронний ресурс] – Режим доступу до ресурсу: https://hyperproof.io/resource/how-to-build-an-information-wsdsecurity-policy/

16. Key elements of an information sewsdcurity policy - Infosec Resources [Електронний ресурс] – Режим доступу до ресурсу: https://resources.infosecinstitute.com/topic/keywsd-elements-information-security-policy/#gref

17. TCP/IP [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipediawsd.org/wiki/TCP/IP

18. SP 800-53 [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/publiwsdcations/detail/sp/800-53/rev-5/final

19. PCI DSS – как и зачем получать сертификат соответствия [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/uewsdip

20. What is SOC 2 [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/leawsdrn/data-security/soc-2-compliance/

21. Інсайдер [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipewsddia.org/wiki/Інсайдер

22. What is an HTTP Flood [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/lwsdearn/ddos/http-flood/

23. Моделируем и определяем DoS атаку типа TCP SYN Flood [Електронний ресурс] – Режим доступу до ресурсу: https://networkguru.ru/dos-ataka-tcp-syn-flood/

24. Что это такое TIA/EIA-568-B [Електронний ресурс] – Режим доступу до ресурсу: https://amp.ru.what-this.com/360348/1/tia-eia-568-b.html

25. Організація комп'ютерних мереж [Електронне мережеве навчальне видання] – Режим доступу до ресурсу: https://ela.kpi.ua/bitwsdstream/123456789/25156/1/ Tarnavsky_Kuzmenko_Org_Komp_merwsdej.pdf / Ю. А. Тарнавський, І. М. Кузьменко – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.

26. Гаскевич Е. Технологии современных широкополосных сетей доступа // Технологии и средства связи. — 2007. — № 5. — С. 70–72

27. What Security Should An ISP Offer Its Customers To Avoid Network Abuse? [Електронний ресурс] – Режим доступу до ресурсу: https://abusix.com/resources/network-abuse/what-securwsdity-should-an-isp-offer-its-customers-to-avoid-network-abuse/

28. Service Provider Security [Електронний ресурс] – Режим доступу до ресурсу: https://tools.cisco.com/security/center/resources/service_provider_infrastructure_ security.html

29. Recommended Internet Service Provider Security Services [Електронний ресурс] – Режим доступу до ресурсу: https://www.ipa.go.jp/securwsdity/rfc/RFC3013EN. html

30. ISP Security: Do We Expect Too Much? [Електронний ресурс] – Режим доступу до ресурсу: https://www.darkrewsdading.com/edge/theedge/isp-security-do-we-expect-too-much/b/d-id/1339493

31. What Role Should ISPs Play in Cybersecurity? [Електронний ресурс] – Режим доступу до ресурсу: https://www.darkreading.com/enwsddpoint/what-role-should-isps-play-in-cybersecurity/a/d-id/1328716

32. ISP Security - NANOG Archive [Електронний ресурс] – Режим доступу до ресурсу: https://archive.nanog.org/meetings/nanog26/presentations/ispsecure.pdf

33. Захищені вузли доступу до мережі Інтернет [Електронний ресурс] – Режим доступу до ресурсу: https://cip.govwsd.ua/ua/news/zakhisheni-vuzli-dostupu-do-merezhi-internet

34. Конопелько, В. К. К64 Измерение и анализ трафика IP-телефонии : метод. пособие по курсу «Цифровая коммутация каналов, пакетов и IP телефония» для студ.спец. «Системы распределения мультимедийной информации» всех форм обуч. / В. К. Конопелько, С. М. Лапшин, В. Ю. Цветков. – Минск : БГУИР, 2011. – 56 с.

35. Гольдштейн, Б. С. Сети связи пост NGN / Б. С. Гольдштейн, А. Е. Кучерявый. — СПб.: БХВПетербург, 2014. —160 с

36. Акопов Г.Л. Информационное право / Г.Л. Акопов. – М.: Феникс, 2008. – 348с.

37. Правило В.В., Кормульов О.С. Методи забезпечення заданих показників безпеки // Збірник матеріалів XIV Міжнародної науково-технічної конференції "Перспективи телекомунікацій 2020". Київ: 2020. С. 178-180.

38. Закон України «Про внесення змін до законів України щодо інформаційної безпеки», [Електронний ресурс] – Режим доступу до ресурсу: http://search.ligazakon.ua/l_doc2.nsf/link1/JH77Gwsd00A.html

39. Про основні засади забезпечення кібербезпеки України, Закон України. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.govwsd.ua/laws/show/2163-19

40. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010, Інформаційні технології-методи захистусистема управління інформаційною безпекою, офіційний переклад, ст.3

41. Venter, H. S. A taxonomy for information security technologies / H. S. Venter, J. H. P. Eloff // Computers & Security. — 2003. — Vol. 22, no. 4. — P. 299–307

42. Anderson, J. M. Why we need a new definition of information security // Computers & Security. — 2003. — Vol. 22, no. 4. — P. 308–313

43. Venter, H. S.; Eloff, J. H. P. (2003). «A taxonomy for information security technologies». Computers & Security. 22 (4): 299–307

44. Інформаційна безпека (соціально-правові аспекти) / [В. Остроухов, В. Петрик, М. Присяжнюк та ін.] ; за ред. Є.Д. Скулиша. – К. : КНТ, 2010. – 776 с., с. 89

45. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об’єктам інформаційної безпеки / В. Дереко // Інформаційна безпека людини, суспільства, держави. – 2015. – № 2 (18). – С. 16–22

46. Understanding difference between Cyber Security & Information Security - CISO Platform, 2016. [Електронний ресурс] – Режим доступу до ресурсу: http://www.cisoplatform.com/profiles/blogs/understanding-difference-betweencyber-security-information

47. Пархоменко І.І., Воскобойніков А.О., «Організація захищеної передачі даних в системі Web-сервер – клієнт» / Вісник інженерної академії України випуск №1 – 2014. – С. 116-120

48. Охорона праці в офісі. Вимоги до робочого місця офісного працівника – [Електронний ресурс] - Режим доступу: http://gc.ua/business-news/oxoronapraci-v-ofisi-vimogi-do-robochogo-miscya-ofisnogo-pracivnika/

49. Гайворонський М.В. Безпека інформаційно-комунікаційних систем./ Гайворонський М.В., Новіков О.М. – К.: Видавнича група BHV, 2009. – 608 с.

50. Дронь М.М., Малайчук В.П., Петренко О.М. Основи теорії захисту інформації: Навч. посібник. – Д.: Вид-во Дніпропетр. ун-ту, 2001. – 312 с.

51. Гатчин Ю. А. Теория информационной безопасности и методология защиты информации / Ю. А. Гатчин, В. В. Сухостат. – СПб. : СПбГУ ИТМО, 2010. – 98 с.

52. Курушин В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. – М. : Новый юрист, 2012.– 256 с.

53. Теория информационной безопасности и методология защиты информации: учебное пособие. / И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина - Казань: Изд-во Казан. гос. техн. ун-та, 2008. – с. 358.

54. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1/ С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с

55. Конев И. Р. Информационная безопасность предприятия / И. Р. Конев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 747 с.

56. Корнюшин, П.Н. Информационная безопасность / П.Н. Корнюшин, С.С. Костерин. – Владивосток: ТИДОТ ДВГУ, 2003. – 154 с.

57. Семененко В.А. Информационная безопасность: учебное пособие. 2-е изд., стереот. - М.: МГИУ, 2005. – 21

58. Малюк, А.А. Информационная безопасность. Концептуальные и методологические основы защиты информации [Текст] / А.А. Малюк. — М. : Горячая Линия - Телеком, 2004. — ISBN: 5-93517-197-X.

59. What is Information Security? [Електронний ресурс] – Режим доступу до ресурсу: https://www.geeksforgeeks.org/what-is-information-security

60. Information security [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipwsdedia.org/wiki/Information_security

61. Internet service provider [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipewsddia.org/wiki/Internet_service_provider

62. ISP Network Potential Threats [Електронний ресурс] – Режим доступу до ресурсу: https://www.ukessays.com/essays/information-technology/isp-network-potential-threats-5152.php

63. Common IoT Threats and the Role of ISPs in Protecting Our Homes [Електронний ресурс] –

Режим доступу до ресурсу:https://businessinsights.bitdefender.com/common-iot-threats-and-the-role-of-isps-in-protecting-our-homes

64. Internet security threats monitored by ISPs in New Zealand [Електронний ресурс] – Режим доступу до ресурсу: https://figure.nz/chart/4Uya6jtZqDjP8taY

65. A Practical Guide to Internet Vulnerabilities Threatening [Електронний ресурс] – Режим доступу до ресурсу: https://blog.equinix.com/blowsdg/2020/04/29/a-practical-guide-to-internet-vulnerabilities-threatening-enterprise-security/

66. Threat Intelligence Report for the Telecommunications Industry [Електронний ресурс] – Режим доступу до ресурсу: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018wsd/03/07185213/Kaspersky_Telecom_Threats_2016.pdf

67. Is your ISP keeping up with evolving DDoS threats [Електронний ресурс] – Режим доступу до ресурсу: https://activereach.net/newsroom/blog/is-your-isp-keeping-up-with-evolving-ddos-threats/

68. Are ISPs Responsible for Subscriber Cyber Security? [Електронний ресурс] – Режим доступу до ресурсу: https://abusix.com/resources/abuse-desks/are-isps-responsible-for-subswsdcriber-cyber-security/

69. 5 Cybersecurity Questions to Ask an Internet Service Provider [Електронний ресурс] – Режим доступу до ресурсу: https://www.corero.com/blog/5-cybersecurity-questions-to-ask-an-internet-service-provider/

70. Информационная безопасность интернет-провайдеров региона в условиях инновационного развития бизнеса [Електронний ресурс] – Режим доступу до ресурсу: https://elar.urfu.ru/bitstream/10995/38115/1/ick_2014_12.pdf

71. Интернет и безопасность [Електронний ресурс] – Режим доступу до ресурсу: https://lib.itsec.ru/articles2/focus/internet-and-sec

72. Безопасность IP-сетей нового поколения для провайдеров [Електронний ресурс] – Режим доступу до ресурсу: https://www.eureca.ru/edu/study/cisco/library/download.php?type=pdf&att=IP_NGN.pdf

73. Розробка політики безпеки інформації інформаційно- телекомунікаційної системи ПП «ТехноСервіс» [Електронний ресурс] – Режим доступу до ресурсу: http://ir.nmu.org.ua/handle/123456wsd789/154453

74. Політика інформаційної безпеки [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Політика_інформаційної_безпеки

75. Захист інформації [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Захист_інформації

76. Як працює інтернет-провайдер? [Електронний ресурс] – Режим доступу до ресурсу: https://www.it-tv.org/ua/article4

77. Послуги Internet-провайдерів [Електронний ресурс] – Режим доступу до ресурсу: https://library.if.ua/book/97/6731.html

78. Інформування стосовно умов здійснення діяльності провайдером телекомунікацій з надання послуг з доступу до мережі Інтернет [Електронний

ресурс] –
Режим доступу до ресурсу: https://nkrzi.gov.ua/index.php?r=site/ index &pg=99&id=1235&language=uk

79. Постачальник послуг Інтернету [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Постачальник_послуг_Інтернету

80. Рейтинг интернет-провайдеров [Електронний ресурс] – Режим доступу до ресурсу: https://2ip.ua/ru/services/providers-rating

81. Щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Закон України] –
Режим доступу до ресурсу:https://zakon.rada.gov.ua/laws/show/v0365500-11#Text

ДОДАТОК А

Таблиця 3.2

Загрози та протидія

Рівні	Атака	Протидія
Атаки на фізичному рівні	Атака на концентратори	На фізичному рівні достатньо використання комутаторів для запобігання атаки
Атаки на канальному рівні	Переповнення Contet Address Memory таблиці	Рекомендація щодо жорсткого прив'язання MAC адреси робочої станції до порту комутатора або ж обмеження кількісті MAC адрес, що підключаються до порту до одної адреси
	VLAN Hoping	Всі задіяні інтерфейси комутатора необхідно перевести в режим trunk та access, а ті, які не використовуються, перевести в shutdown, а також перевести в не існуючий VLAN, який буде відомо лише даному комутаторові
	Атака на STP	Заборона передачі BPDU-пакету з портів, на яких немає комутаторів та у разі надходження такого пакету, то перевести даний порт в режим shutdown
	MAC Spoofing	Необхідне виконання тих самих дій, що і при надмірності CAM таблиці
	Атака на Private VLAN	Створення спеціального Access List на маршрутизаторі, в якому заборонена пряма передача серед сегментів мережі

Продовження таблиці 3.2

Рівні	Атака	Протидія
Атаки на канальному рівні	Атака на DHCP	DHCP Snooping – метод боротьби безпоседньо з атаками даного виду. Метод полягає у порівнянні MAC-адреси, вказаній в DHCP-запиті та в тому, котрий був прописаний у порті комутатора
	ARP-spoofing	Використання додатку arpwatch. Один із можливих способів –це експуатація статичного ARP. Інший метод – це шифрування, та використання локальної мережі VLAN
Атака на мережевому рівні	Атаки на статичну маршрутизацію	Фізічна охорона маршрутизаторів, дозвіл на права адміністратора тільки тим користувачам, які спроможні запустити службу маршрутизації, а також віддалений доступ
	Атаки з протоколом Routin Information Protocol	Використання Access Control List, блокування пакетів, які входять до мережі, що стверджують про наявність IP адреси внутрішньої мережі, використання технології IPS, конфігурація захисту портів dhcp snooping
	Надсилання LSA-пакетів	Блокування флуду на OSPF для типів point-to-point та broadcast. У мережах point-to-multipoint можна зробити блокування "затоплення" для певних сусідів

Продовження таблиці 3.2

Рівні	Атака	Протидія
Атака на мережевому рівні	Злам хешу MD5	Перевірка на достовірність, фільтрація на граничних маршрутизаторах зовнішніх маршрутів автономної системи, та введення складних паролів.
	Атаки BGP	Захист джерел відбувається за допомогою підпису AS, захист джерел та сусідів - підпису вихідної AS, захист джерел та маршрутів - підпису вихідної AS та підпису AS_PATH для маршрутизаторів. Фільтрація грунтується на перевірці AS_PATH та NLRI вихідних AS.
	Атаки на протоколи MPLS та MPLS-VPN	За використання протоколу BGP та систем рішень IP-адреси підтримується безпека. Шифрування використання засобу автентифікації.
Атаки на транспортному рівні	Атаки на TCP	Так як ключовим елементом атаки є розпізнавання sequence number, то допомогою стане використання криптографічно-стійкого алгоритма генерації псевдовипадкоих чисел для генерування sequence number. Фільтрація пакетів SYN і шифрування TCP-пакетів.
	Атаки на UDP	Рекомендації аналогічні дорекомендацій щодо захисту TCP

Продовження таблиці 3.2

Рівні	Атака	Протидія
Атаки на рівні додатків	Протокол SNMP	Аби забезпечити безпеку приладів, моніторинг яких проводитися за допомоги SNMP протоколу, для сегментації та вирішення взаємодії за даним протоколом лиш перевірених хостів потрібно використовувати міжмережеві екрани.
	Протокол Syslog	Обмеження отримання повідомлень тільки з вузлів, які здійснюють генерацію подій. Обмеження передачі подій можна здійснити за допомоги обладнання мережі, заборонивши пересилання UDP пакетів за 514-м портом.
	Протокол DNS	Потрібно встановленя виправлень не лише на хости, що знаходяться під контролем, але й на іменні сервери, які беруть участь при обміні даними. Задля виконання DNS-запиту необхідне залучення випадкових UDP-портів.

Продовження таблиці 3.4

Питання безпеки CI

Рівні	Атака	Протидія
Мережева безпека	Підслуховування даних	Незаконні організації незаконно отримують і аналізують передані дані трафіку або сигнальні дані через бездротові посилання (посилання на зворотний зв'язок, посилання на користувача, ISL)
	Проблеми з цілісністю даних	Змінюйте, вставляйте, повторюйте, видаляйте користувача або сигналізуйте дані, щоб знищити цілісність даних
	Перехоплення інформації	Необхідно встановити виправлення не тільки на хости, які знаходяться під нашим контролем, але і на сервери імен, котрі беруть участь в обміні даних. Використання випадкових UDP-портів для виконання DNS-запитів;
	Перешкоди сигналу	Зловмисники заважають супутниковим бездротовим зв'язкам , випромінюючи високопотужні електромагнітні хвилі
	Відмова в обслуговуванні	Втручатися в роботу супутника або шлюзу, а також втручатися в дані або сигналізацію фізично або за протоколом, що робить CI не в змозі надавати нормальні послуги для законних ST

Продовження таблиці 3.4

Рівні	Атака	Протидія
Мережева безпека	Анонімна атака	Зловмисники атакують супутниковий вузол в космосі, але супутник не може визначити нападників
	Шкідливе заняття ресурсами супутникової пропускної здатності	Відправка незаконних сигналів на супутник через бездротовий зв'язок, оскільки супутник не буде перевіряти законність сигналів, тому незаконні сигнали будуть займати пропускну здатність ресурсів супутника
Безпека обладнання	Шкідливе супутникове управління	Видаючи шкідливі інструкції або вводячи віруси в супутникові вузли з наземних об'єктів або космосу для досягнення мети управління супутниками
	Шкідливе споживання супутникових ресурсів	Шкідливе споживання супутникових паливних ресурсів для досягнення мети скорочення супутникового життя