Міністерство освіти і науки України

«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій

Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього рівня)

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

_____ **Євенко Владислав Валерійович**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Браіловський М.М.	

Нормоконтроль	Даков С.Ю.	

Київ 2021

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____ Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-41** **Євенку Владиславу Валерійовичу**
(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 №2 від 08.10.2020 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:12 жовтня 2020 року

Завдання видав		М.М. Браіловський
	(підпис)	(ініціали, прізвище)
Завдання прийняла до виконання		В.В. Євенко
	(підпис)	(ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 31.01.2021	*виконано*
2	Аналіз літератури	01.02.2021 – 15.02.2021	*виконано*
3	Обґрунтування вибору рішення	16.02.2021 – 19.02.2021	*виконано*
4	Концепція Інтернет-провайдера	20.02.2021 – 04.03.2021	*виконано*
5	Аналіз проблем інформаційної безпеки в компаніях, що забезпечують доступ до мережі Інтернет	05.03.2021 – 21.03.2021	*виконано*
6	Дослідження вразливостей та загроз	22.03.2021 – 08.04.2021	*виконано*
7	Розробка політики безпеки Інтернет-провайдера	09.04.2021 – 10.05.2021	*виконано*
8	Оформлення пояснювальної записки	11.05.2021 – 27.05.2021	*виконано*
9	Підготовка до захисту дипломної роботи	28.05.2021 – 08.06.2021	*виконано*

Завдання видав		М.М. Браіловський
	(підпис)	(ініціали, прізвище)
Завдання прийняв до виконання		В.В. Євенко
	(підпис)	(ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 67 сторінок тексту, 3 таблиці та 9 рисунків. Список використаних джерел містить 81 найменування і займає 5 сторінок.

Метою роботи є аналіз основних загроз для Інтернет-провайдера, визначення рішень їх подолання та розробки політики безпеки постачальників послуг
Предмет дослідження: є політика безпеки Інтернет-провайдера.

В роботі проведено аналіз сучасної структури мережі Інтернет та поняття постачальника послуг Інтернет, запропоновано рішення основних проблем Інтернет-провайдерів. Побудовано таблицю загроз та протидій компанії-провайдера, розроблено політику безпеки Інтернет-провайдера.

Результати здійснених у дипломній роботі досліджень можуть бути використані компаніями, що забезпечують послуги доступу до мережі Інтернет з ціллю забезпечення сучасної та ефективної політики безпеки власного Інтернет-провайдера.

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

Ключові слова: Інтернет , Інтернет-провайдер, політика безпекти, політика безпекти 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
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. Однією з характерних рис інформаційного суспільства є його наростаюча інформатизація, що зокрема, забезпечується активним використанням всесвітньої мережі Інтернет. Значення ролі інформації, знань та інформаційних технологій у сучасному суспільстві важко переоцінити. Події ж останніх років роблять це твердження безумовним. В умовах пандемії неможливо уявити життя людини без доступу до всесвітньої мережі Інтернет. Дистанційна робота, навчання, покупки та спілкування наразі не просто зручна можливість, а необхідність. З появою коронавірусної інфекції в нашому житті з величезною швидкістю зросла необхідність якісного, швидкісного та звісно ж безпечного доступу у мережу.

Ефективне забезпечення безпеки провайдера – складна та багатофункціональна задача. Наразі безпека стає чи не найважливішою характеристикою Інтернет-провайдерів, а також має провідне значення у прибутковості роботи провайдерів послуг. Враховуючи реалії сучасного світу, реалізація мети зловмисника стає все простішою, а забезпечення захисту провайдера, навпаки, ускладнюється. Саме тому особливо актуальною постає сьогодні необхідність розробки ефективної політики безпеки Інтернет провайдерів.

Значний вклад в розвиток інформаційної безпеки Інтернет провайдерів внесли Корченко О.Г., Криворучко О.В., Пархоменко І.І., Лахно В.А, Толюпа С.В., Tobias K., Baker P., Nachreiner C..

Метою роботи є аналіз основних загроз для Інтернет-провайдера, визначення рішень їх подолання та розробки політики безпеки постачальників послуг.

Для досягнення зазначеної мети дипломної роботи поставлені окремі завдання:

- провести аналіз сучасної структури мережі Інтернет, розкрити можливі топології побудови мереж, їх переваги та недоліки; дослідити еталонну модель OSI, розкрити можливі проблеми та варіанти їх виправлення;

- здійснити аналіз поняття постачальника послуг Інтернет. Розкрити питання надання доступу до мережі Інтернет через здійснення типологізації послуг, що забезпечують Інтернет-провайдери; дослідити побудову мережі постачальників послуг;

- встановити особливості нормативно-правового забезпечення, а саме конкретних стандартів, які необхідні для розробки політики безпеки компанії;

- проаналізувати можливі загрози та протидію їм;

- визначити основні проблеми Інтернет-провайдеріва, такі як: перебої електропостачання, обрив ліній, DDoS-атаки та інші;

- здійснити аналіз концепції побудови політики безпеки та відповідно розробити політику безпеки Інтернет-провайдера.

Об'єктом дослідження є робота Інтернет-провайдерів в умовах підвищеного попиту та навантаження.

Предметом дослідження є політика безпеки Інтернет-провайдера.

Методи дослідження. У роботі були використані такі загальнотеоретичні методи як аналіз, синтез, метод абстрагування та ідеалізації, а також формалізації та моделювання при побудові схем та таблиць.

Практичне значення. Результати дослідження можуть бути використані компаніями, що забезпечують позлуги доступу до мережі Інтернет з ціллю забезпечення сучасної та ефективної політики безпеки власного Інтернет-провайдера; 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 ПОБУДОВИ ГЛОБАЛЬНОЇ МЕРЕЖІ ІНТЕРНЕТ

Інтернет - системна архітектура, яка зробила революцію в комунікаціях і методах торгівлі, дозволивши різним комп'ютерним мережам по всьому світу з'єднуватися між собою. Інтернет, який іноді називають «мережею мереж», з'явився в Сполучених Штатах в 1970-х роках, але не був "видимим" для широкої публіки до початку 1990-х років. За оцінками, станом на 2021 рік майже 4.8 мільярдів людей, або більша частина населення світу, мають доступ до Інтернету.

1.1 Сучасна структура мережі інтернет

Internet - глобальна інформаційна мережа, яка є з'єднала безліч регіональних (локальних) комп'ютерних мереж і пристроїв, що обмінюються між собою інформацією по каналах громадських телекомунікацій (виділеним телефонним аналоговим і цифровим лініям, оптичним каналам зв'язку і радіоканалами, а також супутниковим лініями зв'язку). В цілому Інтернет використовує сімейство протоколів Transmission Control Protocol, TCP (Протокол керування передачею) / Internet Protocol, IP («інтернет протокол», «міжмережевий протокол»). Розглянемо структуру протоколів TCP / IP з точки зору моделі Open Systems Interconnection Basic Reference Model (OSI) (рис. 1.1).

OSI TCP / IP [1, с. 84; 2, с. 92] підтримує безліч стандартів, що визначають середу передачі даних. Наприклад, технології Ethernet і Fiber Distributed Data Interface (FDDI) для локальних мереж або Integrated Services Digital Network (ISDN) для великих мереж. Протоколи Point-to-Point Protocol (PPP) і Compressed Serial Line Internet Protocol (CSLIP) призначенні для з'єднання за допомогою аналогової лінії зв'язку, також можуть використовуватися на цьому рівні.

Міжмережевий рівень стека TCP / IP (рівень 2), званий також мережевим рівнем (за моделлю OSI), є основою всієї архітектури TCP / IP. Саме цей рівень,

функції якого відповідають мережному рівню моделі OSI, забезпечує перенесення пакетів даних в межах всієї мережі.

Рисунок 1.1 – Модель OSI та модель TCP\IP

Протоколи мережевого рівня підтримують інтерфейси з "верхнім" транспортним рівнем, отримуючи від нього запити на передачу даних складеною мережею. Головним протоколом мережевого рівня є міжмережевий протокол IP (Internet Protocol) [3; 36]. Він забезпечує переміщення пакета між підмережами від одного прикордонного маршрутизатора до іншого, до тих пір, поки пакет не потрапить в мережу призначення. Протокол IP так само, як і протоколи функцій комутації глобальних мереж зв'язку (Frame Relay (FR), Asynchronous Transfer Mode (ATM) і ін.), Встановлюється не тільки на кінцевих пунктах (хостах), але і на всіх маршрутизаторах мережі. Маршрутизатор являє собою процесор, який

пов'язує між собою дві мережі (підмережі). Протокол мережевого рівня працює в режимі без встановлення з'єднання відповідно до якого він не відповідає за доставлення пакета до вузла призначення. При втраті пакету в мережі протокол IP не намагається відновити його.

Розміри пакетів, параметри передачі, перевірки цілісності виконуються на транспортному рівні TCP. Протокол User Datagram Protocol (UDP) працює на тому ж рівні, але застосовується, коли вимоги до надійності передачі даних менш суворі. [4, с. 21; 5]

Прикладний рівень поєднує всі служби, які система надає користувачеві, варто згадати що Domain Name System (DNS, система доменних імен), яка перетворює числові IP-адреси в імена, також працює на цьому рівні.. Найбільш важливі прикладні протоколи включають:

– Teletype Network (telnet) - віддалене управління;

– Simple Network Management Protocol (SNMP) - управління мережевими пристроями;

– File Transfer Protocol (FTP) - передача файлів;

– HyperText Transfer Protocol (HTTP) - передача гіпертексту;

– Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) і Multipurpose Internet Mail Extension (MIME) - протоколи електронної пошти.

1.2 Топології комп’ютерних мереж

Існує п’ять основних типів топології в комп’ютерних мережах (рис. 1.2) [6; 7; 8; 26, с. 109-116]:

– Сітка

– Зірка

– Шина

– Кільце

– Гібридна

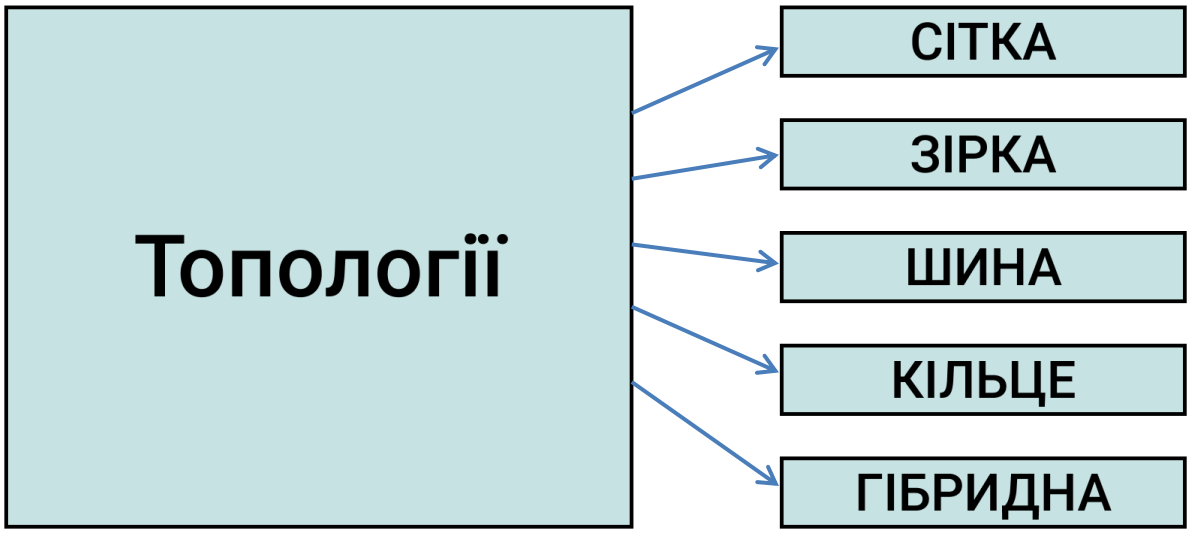


Рисунок 1.2 – Основні типології

1.2.1 Топологія сітка

У сітчастій топології (рис. 1.3) кожен пристрій підключається до кожного іншого пристрою в мережі за допомогою виділеної лінії "точка-точка". Коли ми говоримо про виділене, це означає, що посилання несе дані лише для двох підключених пристроїв. Скажімо, у нас в мережі n пристроїв, тоді кожен пристрій повинен бути підключений до (n-1) пристроїв мережі. Кількість посилань у сітчастій топології n пристроїв буде n (n-1) / 2.

Переваги топології сітки:

1. Немає проблем із трафіком даних, оскільки між двома пристроями існує спеціальний зв’язок, це означає, що зв’язок доступний лише для цих двох пристроїв.

2. Топологія сітки є надійною, оскільки збій одного каналу не впливає на інші канали та зв'язок між іншими пристроями в мережі.

3. Топологія сітки безпечна, оскільки існує посилання точка-точка, тому несанкціонований доступ неможливий.

4. Виявлення несправностей є простим.

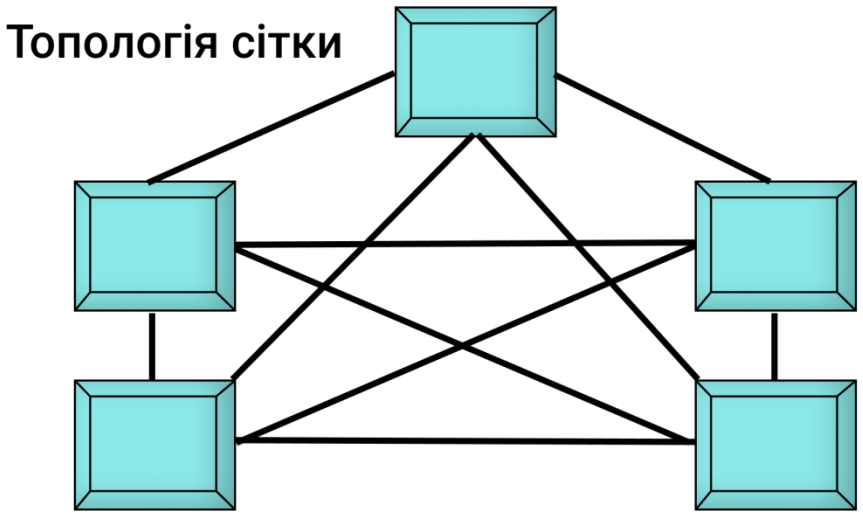


Рисунок 1.3 – Топологія сітки

Недоліки топології сітки:

1. Кількість кабелів, необхідних для підключення кожної системи.

2. Оскільки кожен пристрій потрібно підключати до інших пристроїв, кількість необхідних портів вводу-виводу має бути величезною.

3. Проблеми з масштабованістю, оскільки пристрій неможливо підключити до великої кількості пристроїв із виділеним посиланням точка-точка.

1.2.2 Топологія зірка

У топології зірці (рис.1.4) кожен пристрій у мережі підключений до центрального пристрою, який називається концентратором. На відміну від топології сітки, топологія зірка не дозволяє прямий зв'язок між пристроями, пристрій повинен мати зв'язок через концентратор. Якщо один пристрій хоче надіслати дані на інший пристрій, він повинен спочатку надіслати дані до концентратора, а потім концентратор передати ці дані до призначеного пристрою. [26, с. 113]:

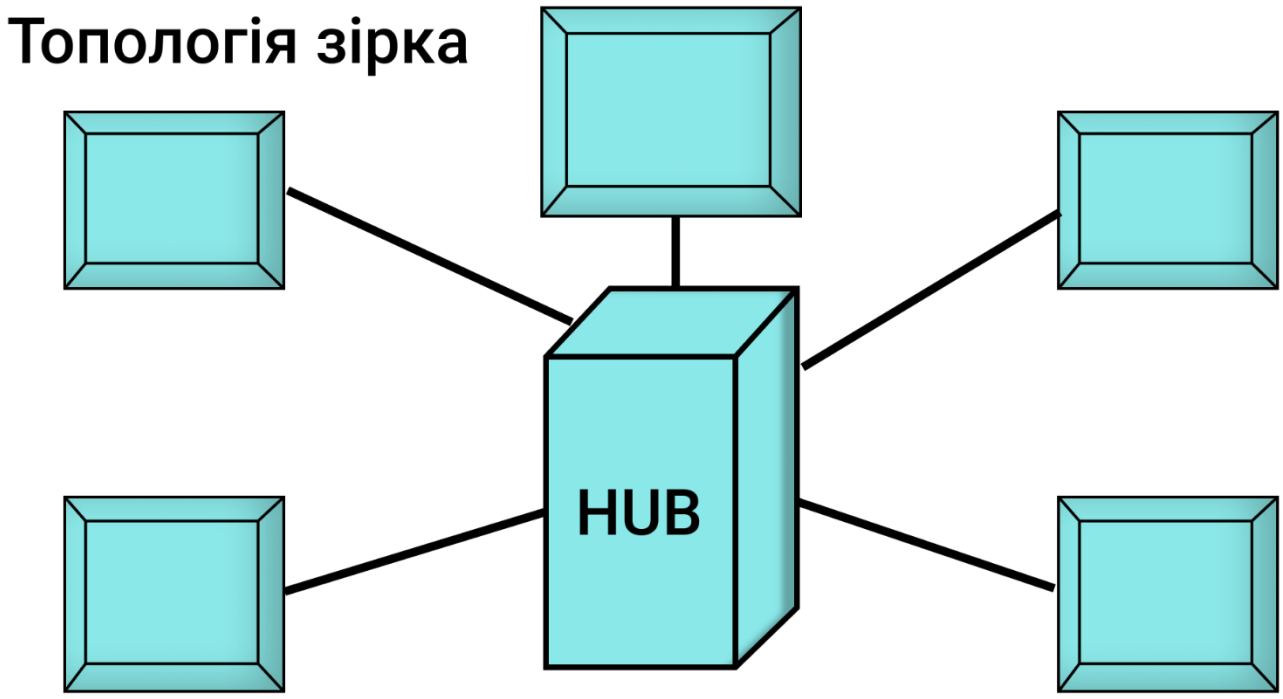


Рисунок 1.4 – Топологія зірка

Переваги топології зірки:

1. Менш дорогий, тому що кожному пристрою потрібен лише один порт вводу-виводу, і його потрібно підключити до концентратора за допомогою однієї лінії зв'язку.

2. Простіший монтаж

3. Менша кількість кабелів потрібна, оскільки кожен пристрій потрібно підключати лише до концентратора.

4. Надійно, якщо одне посилання не вдається, інші посилання будуть працювати нормально.

5. Простота виявлення несправностей, оскільки посилання можна легко ідентифікувати.

Недоліки топології зірок:

1. Якщо концентратор виходить з ладу, все «падає», жоден з пристроїв не може працювати без концентратора.

2. Хаб вимагає більше ресурсів та регулярного обслуговування, оскільки це центральна система топології зірок.

1.2.3 Топологія шини

У топології шини (рис. 1.5) є основний кабель, і всі пристрої підключені до цього основного кабелю через дротові лінії. Існує пристрій під назвою кран, який з'єднує випускну лінію з основним кабелем. Оскільки всі дані передаються по основному кабелю, існує обмеження кількості прямих ліній і відстань, яку може мати основний кабель. [26, с. 111]:

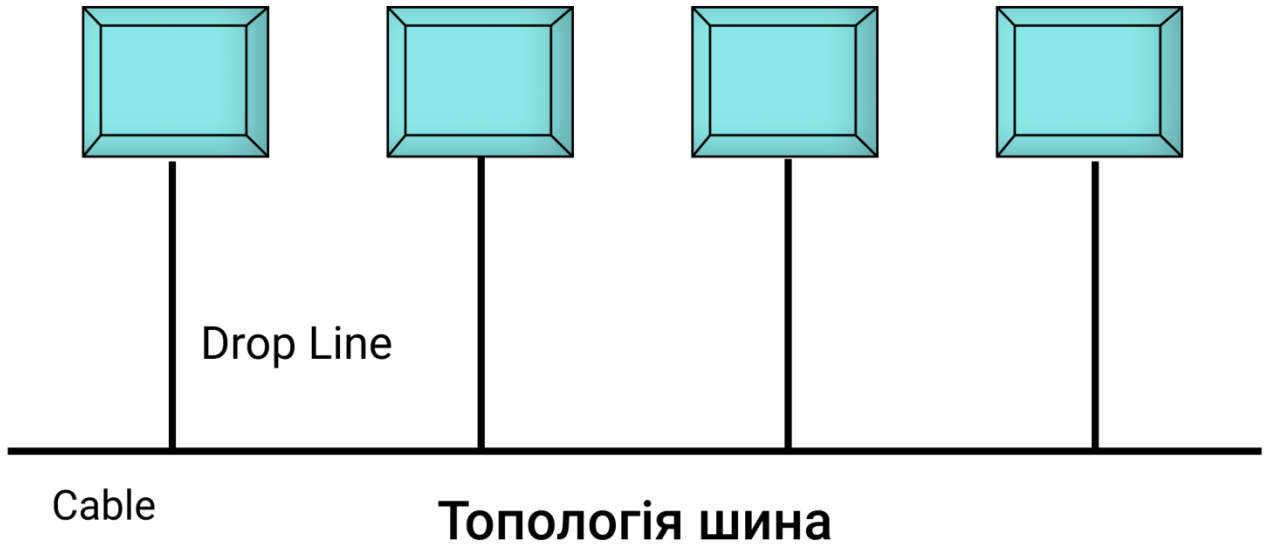


Рисунок 1.5 – Топологія шина

Переваги топології шини:

1. Проста установка, кожен кабель повинен бути з'єднаний магістральним кабелем.

2. Менше кабелів, ніж топологія сітки та зірки

Недоліки топології шини:

1. Важко виявити несправності.

2. Не масштабується, оскільки існує обмеження кількості вузлів, які можна підключити за допомогою магістрального кабелю.

1.2.4 Топологія кільце

У кільцевій топології (рис. 1.6) кожен пристрій пов'язаний з двома пристроями по обидва боки від нього. Є два виділених посилання "точка-точка", які пристрій має з пристроями по обидва боки від нього. Ця структура утворює кільце, тому воно відоме як кільцева топологія. Якщо пристрій хоче надіслати дані на інший пристрій, тоді воно надсилає дані в одному напрямку, кожен пристрій в топології кільця має ретранслятор, якщо отримані дані призначені для іншого пристрою, то ретранслятор пересилає ці дані, поки призначений пристрій їх не отримає. [26, с. 114]:

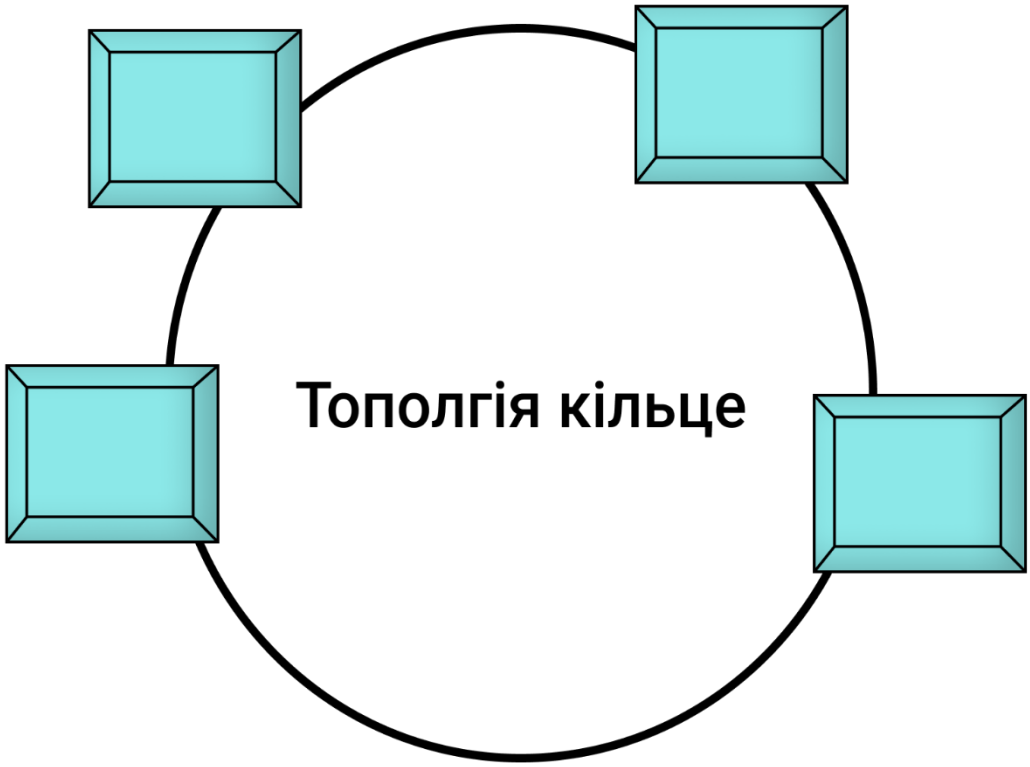


Рисунок 1.6 – Топологія кільце

Переваги топології кільця:

1. Простота установки.

2. Керувати простіше, оскільки для додавання або видалення пристрою з топології потрібно змінити лише два посилання.

Недоліки кільцевої топології:

1. Помилка каналу може зламати всю мережу, оскільки сигнал не буде рухатися вперед через несправність.

2. Проблеми з трафіком даних, оскільки всі дані циркулюють по кільцю.

1.2.5 Гібридна топологія

Поєднання двох або більше топологій відоме як гібридна топологія (рис. 1.7). Наприклад, поєднання топології зірки та сітки відоме як гібридна топологія.

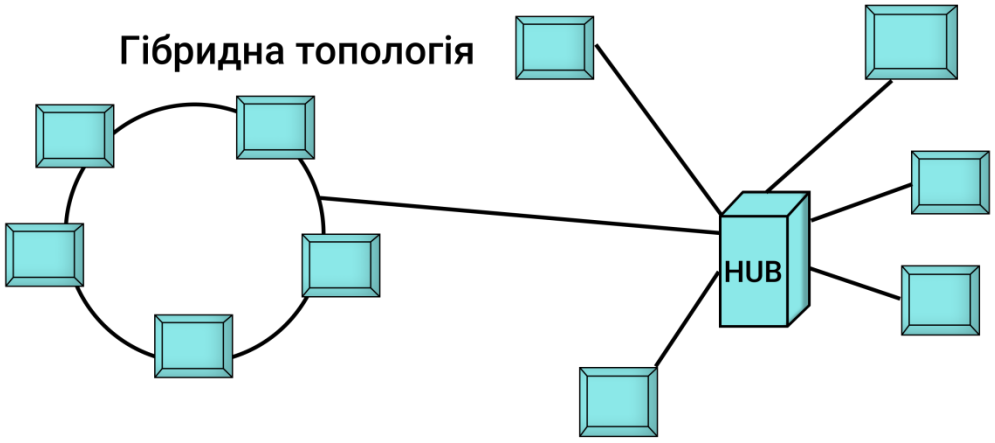


Рисунок 1.7 – Гібридна топологія

Переваги гібридної топології:

1. Ми можемо вибрати топологію, виходячи з вимоги.

2. Масштабована, оскільки ми можемо надалі підключати інші комп’ютерні мережі до існуючих мереж з різною топологією.

Недоліки гібридної топології:

1. Виявлення несправностей досить важке.

2. Установка та налаштування складні.

3. Дороге обслуговування.

1.3 Еталонна модель OSI, її проблеми та виправлення

Перший - це фізичний рівень (рис. 1.8) . На рівні 1 є багато технологій - від фізичних мережевих пристроїв, кабелів до того, як кабелі підключаються до пристроїв. [9; 10]

Замість того, щоб перераховувати всі типи технологій на рівні 1, я створив більш широкі категорії для цих технологій:

– Вузли (пристрої) та мережеві апаратні компоненти. Пристрої включають концентратори, ретранслятори, маршрутизатори, комп'ютери, принтери тощо. Апаратні компоненти, які живуть усередині цих пристроїв, включають антени, підсилювачі, мережеві інтерфейсні карти (NIC) тощо.

– Механіка інтерфейсу пристрою. Як і де кабель підключається до пристрою? Який розмір і форма роз'єму, і скільки він має контактів?

– Функціональна та процедурна логіка. Яка функція кожного штифта в роз'ємі - надсилання чи отримання? Яка процедурна логіка диктує послідовність подій, щоб вузол міг почати спілкуватися з іншим вузлом на рівні 2?

– Протоколи та технічні характеристики кабелю. Ethernet (CAT), USB, цифрова абонентська лінія (DSL) та багато іншого. Технічні характеристики включають максимальну довжину кабелю, методи модуляції, специфікації радіо, кодування лінії та синхронізацію бітів (докладніше про це нижче).

– Типи кабелів. Варіанти включають екрановану або неекрановану кручену пару, некручену пару, коаксіальну тощо.

– Тип сигналу. Основна смуга - це однобітовий потік за раз, як залізнична колія - лише в один бік. Широкосмугове з'єднання складається з декількох бітових потоків одночасно, як двонаправлена магістраль.

– Метод передачі сигналу в залежності від середовища поширення. Варіанти включають електричні (Ethernet), світлові (оптичні мережі, волоконна оптика),

радіохвилі (802.11 – WiFi, 802.15 – Bluetooth або 802.16 - WiMAX). Якщо без кабелю, то також враховуйте частоту: 2,5 ГГц та 5 ГГц. Якщо це кабель, враховуйте напругу. Якщо кабель та Ethernet, також розгляньте стандарти мережі, такі як 1000BASE-T та відповідні стандарти.

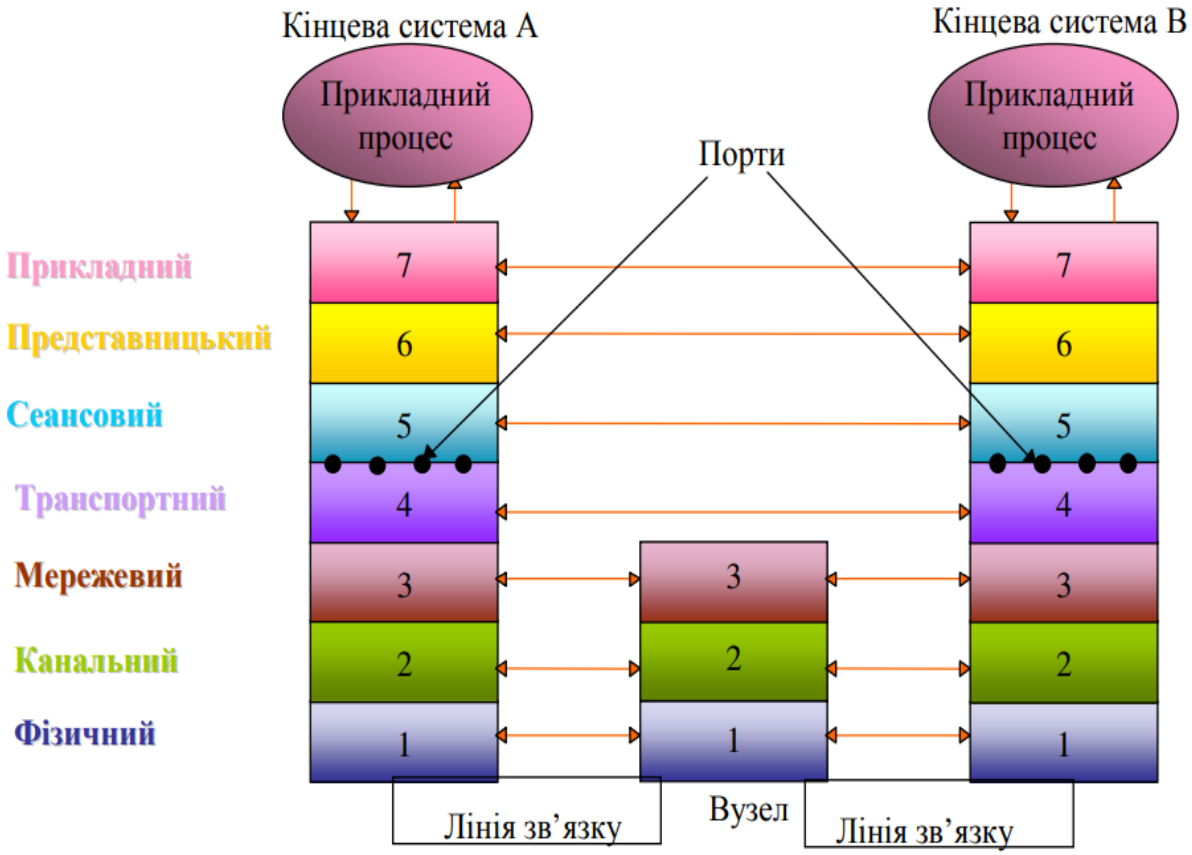


Рисунок 1.8 – Модель OSI

Як вирішити проблеми OSI фізичного рівня? Ось деякі популярні проблеми рівня 1, на які слід звернути увагу:

– Нефункціонуючі кабелі, наприклад, пошкоджені дроти або пошкоджені роз'єми

– Поламані апаратні мережеві пристрої, наприклад пошкоджені схеми

– Матеріали, що підключені невірно [11, с. 24; 12, с. 143]

Якщо у рівні 1 є проблеми, все, що знаходиться за межами рівня 1, не працюватиме належним чином.

Другий - це рівень каналу передачі даних (рис. 1.8) . Рівень 2 визначає спосіб форматування даних для передачі, скільки даних може протікати між вузлами, як довго і що робити, коли в цьому потоці виявляються помилки.

На другому ріві є два різних підрвіні:

– Контроль доступу до медіа (MAC): підшар MAC обробляє присвоєння апаратного ідентифікаційного номера, званого MAC-адресою, який однозначно ідентифікує кожен пристрій у мережі. Два пристрої не повинні мати однакову MAC-адресу. MAC-адреса присвоюється в точці виготовлення. Він автоматично розпізнається більшістю мереж. MAC-адреси відображаються на мережевих картах інтерфейсу (NIC). Комутатори відстежують усі MAC-адреси в мережі.

– Контроль логічного зв'язку (LLC): підрівень LLC обробляє адресацію кадру та управління потоком. Швидкість залежить від зв'язку між вузлами, наприклад Ethernet або Wi-Fi.

Блок даних на рівні 2 - це кадр.

Ось деякі проблеми рівня 2, на які слід звернути увагу:

– Усі проблеми, які можуть виникнути на рівні 1

– Невдалі з'єднання (сеанси) між двома вузлами

– Сесії, які успішно створені, але періодично не вдаються

– Зіткнення кадру

Третій - це мережевий рівень (рис. 1.8). Тут ми надсилаємо інформацію в та між мережами за допомогою маршрутизаторів. Замість того, щоб просто спілкуватися між вузлами, ми тепер можемо здійснювати комунікацію між мережами.

Маршрутизатори є «робочим конем рівня» 3 - ми не могли б мати рівень 3 без них. Комутатори 3 рівня переміщують пакети даних через кілька мереж. Вони не тільки підключаються до постачальників послуг Інтернету (ISP), щоб забезпечити доступ до Інтернету, вони також відстежують, що знаходиться в його мережі (пам’ятайте, що комутатори відстежують усі MAC-адреси в мережі), з якими іншими мережами він підключений, і різні шляхи для маршрутизації пакетів даних через ці мережі.

Маршрутизатори зберігають всю цю адресу та інформацію про маршрутизацію в таблицях маршрутизації. [13; 54]

Ось 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

Одиницею даних на рівні 3 є пакет даних. Як правило, кожен пакет даних містить кадр та обгортку інформації про IP-адресу. Іншими словами, кадри інкапсулюються інформацією адреси рівня 3.

Проблеми, на які слід звернути увагу на третьому рівні:

– Усі проблеми, які можуть виникнути на попередніх рівнях

– Несправний або нефункціональний маршрутизатор або інший вузол

– IP-адреса неправильно налаштована

Багато відповідей на питання рівня 3 вимагатимуть використання інструментів командного рядка, таких як ping , трасування , показ ip-маршруту або протоколи ip.

Четвертим є транспортний рівень (рис. 1.8). Він спирається на функції рівня 2 – «дисципліна» ліній, контроль потоку та контроль помилок. Цей рівень також відповідає за сегментацію пакетів даних або за те, як пакети даних розбиваються та надсилаються мережею.

На відміну від попереднього рівня, транспортний рівень також розуміє ціле повідомлення, а не лише вміст кожного окремого пакету даних. З цим розумінням, рівень 4 може управляти мережевими перевантаженнями, не надсилаючи всі пакети одночасно.

Блоки даних рівня 4 мають кілька імен. Для TCP одиницею даних є пакет. Для UDP пакет називається дейтаграмою. Для простоти я просто використаю тут термін пакет даних.

Протокол управління передачею (TCP) та Протокол датаграми користувача (UDP) - два найбільш відомі протоколи рівня 4. [14; 16]

TCP, протокол, орієнтований на підключення, надає перевагу якості даних над швидкістю.TCP встановлює зв'язок з вузлом призначення і вимагає рукостискання між джерелом і вузлом призначення при передачі даних. Рукостискання підтверджує отримання даних. Якщо вузол призначення не отримує всіх даних, TCP попросить повторити спробу. TCP також забезпечує доставку або повторне збирання пакетів у правильному порядку.

UDP надає перевагу швидкості перед якістю даних. UDP не вимагає рукостискання, оскільки UDP не повинен чекати цього підтвердження, він може надсилати дані швидше, але не всі дані можуть бути успішно передані, і ми ніколи не дізнаємось про це.

Проблеми транспортного рівня:

– Усі проблеми, які можуть виникнути на попередніх рівнях

– 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 - це сеансовий рівень (рис. 1.8). Цей рівень встановлює, підтримує та завершує сеанси. Сеанс - це зв’язок, який встановлюється між двома конкретними програмами для кінцевих користувачів. Тут слід врахувати дві важливі концепції:

– Клієнт і сервер: додаток, що запитує інформацію, називається клієнтом, а додаток, що має запитувану інформацію, - сервером.

– Модель запитів та відповідей: під час створення сеансу та під час сеансу постійно відбувається зворотне передавання запитів на інформацію та відповідей, що містять цю інформацію. [15]

Сесії можуть бути відкритими протягом дуже короткого періоду часу або тривалого періоду часу. Іноді вони теж можуть зазнати невдачі.

Відтепер (рівень 5 і вище) мережі орієнтовані на способи встановлення з'єднань із програмами кінцевих користувачів та відображення даних користувачеві.

Основні проблеми даного рівня:

– Недоступність серверів

– Сервери налаштовані неправильно, наприклад конфігурації Apache або PHP

– Помилка сеансу - відключення, час очікування тощо.

Рівень 6 - це представницький рівень (рис. 1.8). Цей рівень відповідає за форматування даних, таких як кодування символів і перетворення, а також шифрування даних. Операційна система, на якій розміщено додаток для кінцевого користувача, зазвичай бере участь у процесах представницького рівня. Ця функціональність не завжди реалізована в мережевому протоколі.

Рівень 6 гарантує, що програми кінцевого користувача, що працюють на прикладному рівні, можуть успішно споживати дані й, звичайно, з часом відображати їх.

Часто зустрічаються такі проблеми:

– Відсутні або пошкоджені драйвери

– Неправильний рівень доступу користувачів ОС

Рівень 7 - це прикладний рівень (рис. 1.8). Вірний своїй назві, цей рівень відповідає за підтримку служб, що використовуються програмами кінцевих користувачів. До програм належать програми, які встановлені в операційній системі, такі як Інтернет-браузери або програми обробки текстів, тощо. Додатки також контролюватимуть взаємодію з кінцевим користувачем, наприклад, перевірку безпеки, ідентифікацію двох учасників, ініціювання обміну інформацією тощо. Протоколи, які працюють на цьому рівні, включають протокол передачі файлів (FTP), «безпечну оболонку» (SSH), простий протокол передачі пошти (SMTP), протокол доступу до Інтернет-повідомлень (IMAP), службу доменних імен (DNS) і протокол передачі гіпертексту (HTTP).

Проблеми рівня:

– Усі можливі проблеми попередніх рівнів
– Неправильно налаштовані програми
– Помилки користувачів

Висновки до розділу 1

В цьому розділі була представлена сучасна структура мережі Інтернет, в цілому Інтернет використовує сімейство протоколів TCP / IP. Розглянуто можливі топології побудови мереж, їх переваги та недоліки; Існує п’ять основних типів топології в комп’ютерних мережах: сітка, зірка, шина, кільце, гібридна. Досліджено еталонну модель OSI, можливі проблеми всіх рівнів, а саме фізичного, канального, мережевого, транспортного, сеансового, представницького та прикладного та варіанти їх виправлення. Також досліджено протоколи сімейства TCP\IP. Ця інформація необхідна для загального розуміння того, як працює Інтернет, адже без цього неможливо розібрати, як саме функціонує Інтернет-провайдер.

РОЗДІЛ 2
ПРИНЦИПИ РОБОТИ ІНТЕРНЕТ - ПРОВАЙДЕРА

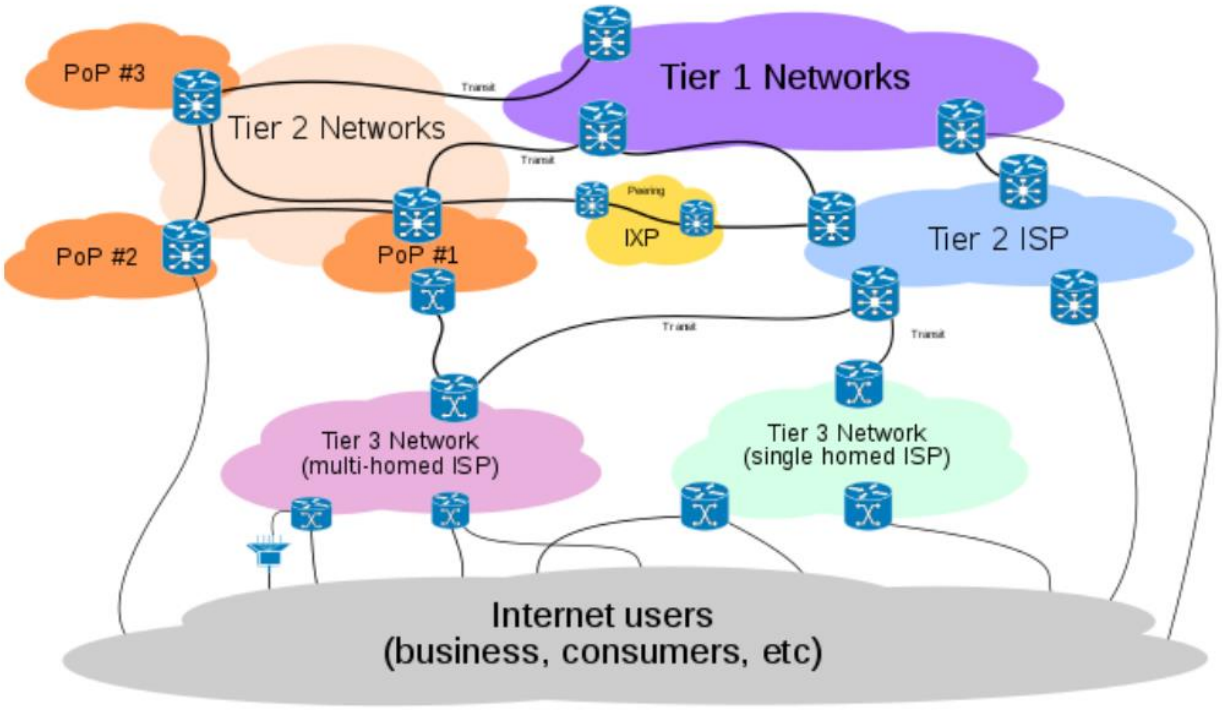
ISP (Internet Service Provider) - це абревіатура, що означає Інтернет-провайдер. Інтернет-провайдер - це компанія, яка надає доступ до Інтернету організаціям та домашнім користувачам. Інтернет-провайдери виступають як "сховища даних", передаючи свої великі обчислювальні потужності в оренду багатьом тисячам операторів веб-сайтів, починаючи від юридичних до приватних осіб закінчуючи корпораціями, некомерційними групами та державними установами. [1]

2.1 Інтернет-сервіс провайдинг

Інтернет-провайдери відповідають за те, щоб ви могли отримати доступ до Інтернету, маршрутизувати трафік, вирішувати доменні імена та підтримувати мережеву інфраструктуру, яка робить доступ до Інтернету можливим.

Хоча основною функцією Інтернет-провайдера є надання доступу до Інтернету, багато провайдерів роблять набагато більше. Інтернет-провайдери також пропонують такі послуги, як веб-хостинг, реєстрація доменних імен та послуги електронної пошти.

На вершині «піраміди доступу до Інтернету» (рис. 2.1) [61] знаходяться Інтернет-провайдери рівня 1. Постачальник послуг Інтернету першого рівня - це Інтернет-провайдер, який має доступ до всіх мереж в Інтернеті, використовуючи лише ті угоди мережевого пірингу, за які їм не потрібно платити. Щоб допомогти зрозуміти, для якої мети служать Інтернет-провайдери рівня 1, подумайте про Інтернет-провайдерів рівня 1 як про головні магістралі Інтернету. Ці Інтернет-провайдери з’єднують усі куточки Всесвітньої павутини. Деякі популярні приклади Інтернет-провайдерів рівня 1 включають Vodacom, Bharti, Deutsche Telekom, British Telecommunications та Verizon.



Зображення надано компанією Privacy Canada .

Рисунок 2.1 – Піраміда доступу до Інтернету

Інтернет-провайдери рівня 1 продають доступ до своїх мереж провайдерам рівня 2. Потім провайдери рівня 2 продають доступ до Інтернету організаціям та домашнім користувачам. Однак іноді Інтернет-провайдери рівня 1 можуть продавати доступ до Інтернету безпосередньо організаціям та приватним особам. Крім того, другий проміжний провайдер, який називається провайдером рівня 3, може придбати пропускну здатність мережі у провайдера рівня 2 перед продажем цієї смуги пропускання кінцевим користувачам.

Коли трафік перенаправляється з домашньої мережі в Інтернет, він проходить через кілька стрибків, перш ніж досягати місця призначення. Наприклад, трафік може переходити від модему до мережі провайдера рівня 3, мережі провайдера рівня 2, мережі провайдера рівня 1, а потім повертатися через інший набір провайдерів, перш ніж дістатися до пункту призначення. [17, с. 221]

Основна технологія, яку постачальники послуг Інтернету використовують для встановлення зв’язку, може базуватися на DSL, кабельних, супутникових, Wi-Fi, волоконно-оптичних чи інших носіях зв'язку. Причиною того, що багато

постачальників кабельних та телефонних послуг також є провайдерами, є те, що їх базова інфраструктура може приймати Інтернет-трафік.

Інтернет-провайдер підключений до однієї або декількох високошвидкісних ліній Інтернету, які називаються найвищими або магістральними підключеннями, необхідними для забезпечення швидкого обслуговування кожного з його клієнтів. Кожне з цих з'єднань у тисячі разів швидше, ніж типове домашнє високошвидкісне обслуговування. Більші провайдери підтримують кілька зв'язків як страховку; якщо одна лінія не вдається, інші підтримують роботу Інтернет-провайдера та його клієнтів. [18; 59]

2.2 Види послуг, що забезпечують Інтернет-провайдери

– Програмне забезпечення

Окрім комп'ютерів та мережевих з'єднань, провайдери надають опції програмного забезпечення для веб, електронної пошти та інших потреб. Наприклад, багато Інтернет-провайдерів пропонують вибір між Microsoft Windows Server та Linux, які оператор веб-сайту вибирає на основі власних технічних вимог та уподобань. Інтернет-провайдери також пропонують програмне забезпечення для баз даних, таке як Microsoft SQL Server або MySQL; бази даних необхідні для організації та зберігання такої інформації, як записи про продажі та товарно-матеріальні запаси, тощо. [19; 28]

– Спільний хостинг

Інтернет-провайдер часто розподіляє ресурси одного комп'ютера або сервера між багатьма клієнтами; ця недорога послуга, яка називається спільним хостингом, розглядає кожен розміщений веб-сайт як окрему сутність зі своїми власними файлами та паролями безпеки. Спільний хостинг ідеально підходить для веб-сайтів, яким не потрібне спеціальне програмне забезпечення. По суті спільний хостинг це виділення частини ресурсів сервера або комп'ютера під потреби замовника.

– Виділений хостинг

На додаток до послуг спільного хостингу, більшість Інтернет-провайдерів пропонують спеціальний хостинг, в якому на одному комп'ютері або сервері працює лише один веб-сайт/ресурс. Хоча це більш дорога послуга, виділений хостинг пропонує швидший час відгуку та може обробляти більше Інтернет-трафіку, оскільки комп'ютер не обслуговує багато сайтів одночасно. Це також надає власнику сайту можливість додавати власне програмне забезпечення, а не обмежуватися тим, що надає Інтернет-провайдер.

– Дизайн та маркетинг

Деякі інтернет-провайдери пропонують послуги з графічного дизайну та маркетингу. Графічний дизайн визначає стиль та якість зовнішнього вигляду сайту; без цього сайт може функціонувати, але може мати обмежену привабливість. Маркетинг відкриває сайт для більшої кількості користувачів в Інтернеті, допомагаючи веб-бізнесу залучати клієнтів. Оскільки багато власників сайтів не мають навичок або часу, необхідних для професійного графічного дизайну або маркетингу, власні провайдери допомагають задовольнити цю потребу. [20; 21]

2.3 Побудова мережі Інтернет-провайдера

Основним завданням Інтернет-провайдера є надання послуг зв'язку абонентам (доступ в Інтернет, телефонія, цифрове телебачення та інші), а для забезпечення доступу до цих послуг необхідно побудувати мережу. [22; 73]

Референтна модель побудови мережі:

1. рівень доступу;
2. рівень агрегації;
3. рівень ядра мережі;
4. серверний рівень.

Модель являє собою топологію «Дерево» (об'єднання декількох топологій «зірка») з додатковими надмірними зв'язками. Надлишок компенсує основний недолік цієї топології (вихід з ладу одного з вузлів впливає на роботу всієї мережі),

але також подвоює витрати кабелю. Щоб зменшити витрати на кабель, багато організацій "підсилюють" лише найбільш значущі частини мережі.

Слід пам’ятати, що це просто модель, а тому розподіл на рівні може бути умовним - деякі пристрої можуть реалізувати обидва рівні одночасно, а деякі рівні можуть бути повністю відсутніми.

2.3.1 Рівень доступу

Основним процесом на цьому рівні є підключення клієнтського обладнання (комп'ютера, маршрутизатора Wi-Fi) до мережі постачальника. Тут обладнанням провайдера є комутатори (якщо це локальна мережа і планується підключення за допомогою дротового носія) або базові станції (якщо з'єднання здійснюється через бездротовий носій). [52] Як правило, для організації керованої мережі використовують комутатори другого рівня (L2), рідше - третього (L3). Деякі провайдери на етапі побудови локальної мережі віддають перевагу некерованим комутаторам, згодом це може вплинути на якість наданих послуг.

Також для зниження витрат на з'єднання використовуються пристрої з максимальною кількістю фізичних інтерфейсів 24/48.

Комутатори L3 на цьому рівні досить рідкісні, оскільки вони дорожчі, ніж L2, а їх розміщення в технічних приміщеннях багатоповерхівок пов'язане з певними ризиками. Якщо комутатори L3 застосовуються на рівні доступу, то лише в поєднанні рівня доступу та рівня агрегації.

Приватний приклад використання - кабінет в офісі чи відділі, а у випадку з провайдером - багатоквартирний будинок або житлова секція в цьому будинку.

Варто зазначити, що під час побудови мережі кожен провайдер сам обирає ступінь сегментації. Сегмент мережі або VLAN (віртуальна локальна мережа) [47] дозволяє об'єднати групу користувачів в одну логічну мережу або розділити кожного окремо. Вважається дуже поганою формою, коли мережа "плоска", тобто клієнти, комутатори, маршрутизатори та сервери знаходяться в одному логічному сегменті.

Така мережа має багато недоліків. Краще рішення – розділити всю мережу на менші підмережі, в ідеалі виділити VLAN для кожного клієнта.

2.3.2 Рівень агрегації

Проміжний шар між ядром мережі та рівнем доступу. Як правило, цей рівень реалізується на L3-комутаторах, рідше на маршрутизаторах через їх високу вартість і, знову ж таки, особливості роботи в певних типах приміщень. Основна мета обладнання – об'єднання лінків від комутаторів рівня доступу на «магістральному» комутаторі по топології «зірка».

Відстань від комутаторів доступу до комутаторів цієї групи може досягати кількох кілометрів. Якщо комутатори L2 використовуються на рівні доступу, а мережа сегментована, то на цьому рівні організовані інтерфейси L3 для VLAN, зареєстрованих на рівні доступу. Такий підхід здатний трохи розвантажити ядро мережі, оскільки в цьому випадку в ядрі немає записів про VLAN та параметри інтерфейсів VLAN, а є лише маршрут до кінцевої підмережі.

2.3.3 Рівень ядра

Ядро є невід'ємною частиною будь-якої мережі. Цей рівень реалізований на маршрутизаторах, рідше на високоефективних комутаторах L3 (знову ж таки, для зниження вартості самої мережі.) Залежно від архітектури мережі ядро може «утримувати» статичні маршрути або мати налаштування для динамічної маршрутизації.

2.3.4 Серверний рівень

Він реалізований, як зрозуміло з назви, мережевими серверами. Реалізація може бути як на серверних платформах, так і на спеціалізованому обладнанні. Програмне забезпечення для серверних платформ сьогодні представлено різними

виробниками та за різними типами ліцензій, а також ОС, на якій це програмне забезпечення буде працювати.

Стандартний набір провайдера на цьому рівні:

1) DHCP-сервер;
2) DNS-сервер;
3) один або кілька серверів доступу (якщо необхідно);
4) сервер AAA (радіус або діаметр);
5) платіжний сервер;
6) сервер бази даних;
7) сервер для зберігання статистики потоку та платіжної інформації;
8) сервер моніторингу мережі;
9) пристрої фільтрації трафіку;
10) COPM;
11) BRAS;
12) розважальні послуги для користувачів (на вибір);
13) сервери вмісту (наприклад, кеш Google). [23; 24; 25; 34]

2.3.5 Рівень кордону

Прикордонний рівень зазвичай відсутній у схемах, оскільки він працює за межами основної мережі, хоча може бути реалізований на рівні ядра. Але краще виділити для цих цілей самостійний пристрій. На цьому рівні трафік обмінюється між провайдером і вищим постачальником або між AS оператором (автономною системою) та іншими автономними системами [27; 29] (у разі використання BGP). На початку побудови мережі рівень також може бути реалізований на сервері доступу, але згодом, як тільки стане необхідним додати ще один сервер доступу, виникне питання про підмережу з власних реальних адрес.

Цю потребу можна реалізувати на маршрутизаторах або на L3-комутаторах – зовнішній пул адрес достатньо маршрутизований із власної IP-адреси зовнішньої підмережі, яка видається постачальником при підключенні.

Висновки до розділу 2

В другому розділі було розкрито питання надання доступу до мережі Інтернет. Інтернет-провайдер - це компанія, яка надає доступ до Інтернету організаціям та домашнім користувачам. Розглянуто послуги, які Інтернет-провайдери надають користувачам: програмне забезпечення, спільний хостинг, виділений хостинг, дизайн та маркетинг. Досліджена побудова мережі компанії провайдера Інтернет послуг. Референтна модель побудови мережі: рівень доступу; рівень агрегації; рівень ядра мережі; серверний рівень. Модель являє собою топологію «Дерево» (об'єднання декількох топологій «зірка») з додатковими надмірними зв’язками. Їх надлишок компенсує основний недолік цієї топології (вихід з ладу одного з вузлів може призвести до непрацездатності частини мережі або навіть всієї мережі), але також подвоює витрати кабелю. Щоб зменшити витрати на кабель, багато організацій "підсилюють" лише найбільш значущі частини мережі.

РОЗДІЛ 3
РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ ТИПОВОЇ КОМПАНІЇ, ЩО НАДАЄ ПОСЛУГИ ІНТЕРНЕТ-ДОСТУПУ

3.1 Нормативно-правове забезпечення

3.1.1 Огляд стандарту BS 7799

Частина 1: Практичні рекомендації, 2000 р. Визначаються і розглядаються наступні аспекти організації режиму ІБ: політика безпеки; організація захисту; класифікація інформаційних ресурсів і управління ними; управління персоналом; фізична безпека; адміністрування комп'ютерних систем і мереж; управління доступом до систем; Розробка та супровід систем; планування безперебійної роботи організації; перевірка системи на відповідність вимогам ІБ.

Частина 2: Специфікації, 2000. Присвячена тим же аспектам, але з точки зору сертифікації режиму ІБ на відповідність вимогам стандарту. Розглянемо основні положення стандарту ISO 17799 (BS 7799). При цьому будемо дотримуватися методологічної схеми, запропонованої Національним інститутом стандартів Великобританії, а саме: спочатку сформулюємо про блемную ситуацію стандарту, основні цілі її дозволу, а потім вкажемо ре комендації з управління ІБ на підприємстві [66].

3.1.2 Німецький стандарт BSI

У Німеччині в 1998 р вийшло «Керівництво щодо захистуінформаційних технологій для базового рівня захищеності». Воно являє собою гіпертекстовий довідник обсягом близько 4 Мб (в форматі HTML). Можна виділити наступні блоки цього документа: методологія управління ІБ (організація менеджменту в області ІБ, мето довгий використання керівництва); компоненти інформаційних технологій: - основні компоненти (організаційний рівень ІБ, процедурний рівень, організація

захисту даних, планування дій у надзвичайних ситуаціях); інфраструктура (будівлі, приміщення, кабельні мережі, організація видалений ного доступу); [66, 80]

3.1.3 ISO 27001

В основі стандарту лежить ризик-орієнтованих підхід. Стандарт ISO 27001 зосереджений на захисті конфіденційності, збереження і доступності інформації в компанії. Це реалізується шляхом з'ясування потенційних проблем з інформацією (тобто оцінки ризиків), а потім визначення необхідних кроків для запобігання появи таких проблем (тобто зниження або обробки ризиків). Тому основна філософія ISO 27001 базується на управлінні ризиками: з'ясувати, де знаходяться ризики, а потім систематично обробляти їх.

Захисні заходи, які повинні впроваджуватися, зазвичай виступають у формі політик, процедур і технічного впровадження (наприклад, програмного забезпечення і устаткування). Однак, в більшості випадків, компанії вже мають у своєму розпорядженні у себе усім обладнанням і програмним забезпеченням. Однак використовують вони їх небезпечним способом, тому більша частина впроваджень ISO 27001 буде пов'язана з постановкою організаційних правил (тобто з написанням документів), які необхідні для запобігання порушень в системі безпеки. Оскільки таке впровадження зажадає управління безліччю політик, процедур, людей, активів і т.д., в ISO 27001 описано, як зістикувати разом всі ці елементи в системі менеджменту інформаційної безпеки. [4]

3.1.3 IEC 31010:2019

Даний стандарт входить в серію стандартів з управління бізнесризиками без прив'язки конкретно до ризиків ІБ. «Заголовні» стандартом є 17 документ ISO 31000: 2018 "Risk management - Guidelines" («Менеджмент ризику - Керівництва»), який описує фреймворк, принципи і сам процес управління ризиками. Описаний в даному документі процес ризикменеджменту аналогічний розглянутому вище: визначаються контекст, кордони і критерії, проводиться оцінка ризиків (що

складається з ідентифікації, аналізу, оцінки небезпеки ризиків), далі йде обробка ризиків з подальшою комунікацією, звітністю, моніторингом та переглядом.

Стандарт же IEC 31010: 2019 примітний тим, що в ньому наведено понад 40-ка різноманітних технік оцінки ризику, до кожної дано пояснення, зазначений спосіб застосування для всіх під процесів оцінки ризику (ідентифікація ризику, визначення джерел і причин ризику, аналіз заходів захисту, аналіз наслідків, ймовірностей, взаємозв'язків і взаємодій, вимір і оцінка рівня ризику, вибір заходів захисту, звітність), а для деяких технік наведено і практичні приклади використання. [5]

3.2 Проведення аналізу загроз компанії-провайдера

Для наочного розуміння загроз, була створена таблиця 3.1, яка включає в себе найчастіші загрози та практичні рекомендації для протидії їм. Таблиця створювалась згідно рівням моделі OSI [30-33; 35; 37-40; 46; 60; 67-72] та знаходиться у додатку А.

Окремо розглянуті наступні загрози та атаки (табл. 3.2):

Таблиця 3.2

Загрози та протидія-2

Рівні	**Атака**	**Протидія**
Загрози IP-телефонії	Перехоплення даних	Перехоплення можливе, як зовні так і зсередини, тому необхідне шифрування всього трафіку
	Відмова обслуговування	Резервування смуги пропуску за допомогою сучасних протоколів, наприклад протокола резервування мережевих ресурсів RSVP
	Підміна номеру	Використання спеціальних IP-телефонів, адже вони більш захищенні ніж абонентські пункти реалізовані на базі персональних комп'ютерів

Продовження таблиці 3.2

Рівні	Атака	Протидія
Атаки на бездротові прилади	Атаки на Wi-Fi	Використовувати проткол WPA2 та складні паролі, забезпечити фізичну безпеку для роутера, оновлювати ПО роутера. Використання шифрування, заборона використання незахищенних мереж

3.3 Основні проблеми Інтернет-провайдерів

Розглянемо основні проблеми, які трапляються у провайдера, при наданні послуг:

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

3.3.1 Перебої електропостачання

Одна з основних проблем надання послуг є перебої в електропостачанні зі сторони підприємств-постачальників електроенергії. Пов’язано це з старою інфраструктурою, з поганим станом трансформаторних підстанцій, аварійним станом приміщень підстанцій. Шлях від основного серверу провайдера до абонента довгий. На цьому шляху знаходиться проміжне обладнання, яке також енергозалежне. При відмові проміжне обладнання, може припинити передавати сигнал на досить велику область. [41, 42]

Рішенням проблеми може бути побудова структури з резервними лініями передачі сигналу. На жаль на якість подачі електроенергії вплинути провайдер не може.

3.3.2 Технічні поломки обладнання

З вище вказаною проблемою походить і проблема виходу з робочого стану обладнання. Через перебої з електропостачанням може «злетіти» налаштування обладнання.

Також проблемою є стан та використання заборонених за стандартами приміщень, в яких встановлюється обладнання. Зазвичай обладнання встановлюється у підвалах або на горищі. В обох випадках в приміщеннях підвищена вологість та дуже багато пилу, що небажано для будь-якого мережевого обладнання. Також через опади, підвали можуть бути затопленні.

Рішенням для даної проблеми можуть бути такі:

1. встановлення стабілізатору напруги, який буде замірювати вхідну напругу та вирівнювати її до значення у 220В. Також він не буде пропускати імпульсні стрибки напруги, та стрибки при включенні і відключенні електроенергії;

2. встановлення джерело безперебійного живлення (ДБЖ) [43-45]. У випадку відключення електропостачання, обладнання зможе відключитись і включитись після надання напруги, без пошкоджень для технічної та програмної складових;

3. бекап системи програмної складової, щоб у випадку збою, при відновленні роботи обладнання його можна було швидко налаштувати у робочий стан;

4. продумано встановлювати обладнання в технічних приміщеннях;

планові технічно-профілактичні роботи.

3.3.3 Обрив лінії

Фактори обриву кабелів:

1. якість встановлення;

2. погодні умови;

3. зловмисники;

4. тварини, наприклад пацюки.

Дуже часто трапляється, що кабель може перегризти тварина або зловмиснику, з власних причин, не сподобалось як протягнуті кабелі і він їх обрізав. Через погані погодні умов кабелі можуть обірватись, так як не всі кабелі проходять по захищенним каналам.

У випадку пошкодження структура кабельної системи (СКС) [48; 53; 55] є можливість оперативно виправити аварію, так як зазвичай використовують виту пару або волоконно-оптичну мережу.

Місце обриву такого кабелю можна визначити за допомогою декількох способів:

а) зовнішній огляд;

б) мультиметром;

в) мережеві тестери;

г) програмно.

Із усіх методів перший треба використовувати програмний. При обриві дроту інженер на обладнанні прописує команди для перевірки дроту. Час процедури залежить від віддаленості кінцевого обладнання. Зазвичай це займає до 5 хвилин. Програмно можна визначити точність обриву до метрів. На місці аварії технік-спеціаліст вже визначає більш точне місце знаходження обриву за допомогою 3 інших методів.

Рішенням для цього є кваліфіковані техніки, які якісно виконають свою роботу. Проведуть лінію СКС максимально приховано у спеціальних кожухах. Завдяки якісно виконаній роботі, проблеми, описані вище, зведуться до мінімуму.

У випадку з волоконно-оптичною лінією зв’язку (ВОЛЗ) [49; 50; 79] дуже важливим є оперативне вирішення аварії, а ще краще не допустити аварію. Аварія ВОЛЗ є дуже критичним фактором у роботі усієї системи інфокомунікації.

Варіанти вирішення такі:

а) моніторинг системи;

б) своєчасно виявити несанкціонований доступ до ВОЛЗ;

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

г) максимально швидко відреагувати у разі виникнення аварії;

д) створити базу даних рефлектограмм ВОЛЗ.

Для моніторингу системи треба під’єднати комутатор, між рефлектометром і лінією зв’язку. Комутатор через деякий проміжок часу буде переключатись між лініями оптоволоконна. [51; 56-58] Система моніторингу знімає і зберігає у пам’ять опорні рефлектограмми для усіх тестуючих волокон та фіксує відхилення по загасанню і відображенню на всіх точках лінії.

В табл. 4.1 вказано, які входять категорії кабелів і їх пропускна здібність у смугах частот.

Таблиця 4.1

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

3.3.4 Проблема загальних VLAN-ів для підмереж абонентів

Підключення до Інтернету обов'язково передбачає постійне або тимчасове призначення на мережевий інтерфейс комп'ютера реальної IP-адреси. [11]

Оскільки IP-адреси - ресурс платний і обмежений, провайдер застосовує різні схеми управління адресним призначенням: статичну і динамічну. Коли йдеться про підключення абонента з динамічним IP-адресою , вартість оренди реальної адреси не стягується, однак абонентові не гарантується будь-яка незмінність використовуваної адреси.

Не завжди динамічна адреса задовольняє потреби абонента. Коли необхідно відкрити ресурси свого комп'ютера зовнішнім споживачам, наприклад, розгорнути http-, mail- або ftp-сервер, адресу хоста необхідно зафіксувати. Часто абонента цікавить не одиночна адреса, а IP-мережа. Такі послуги, як правило, надаються на платній основі.

Провайдер планує адресний простір, щоб забезпечити його раціональне використання, розбиває IP-мережу на декілька підмереж для різних потреб. Для динамічних пулів, хостів базових мережевих служб і службових сегментів мережі, корпоративних клієнтів, тощо. Підмережі дозволяють значно знизити обсяг адресної інформації в таблицях маршуртизації. Забезпечити сегментування комп’ютерних мереж абонентів, знизити широкомовний трафік, спростити мережевий моніторинг. Але розмір IP-підмереж не може бути довільним. Він завжди дорівнює ступеню двійки, тому при розбитті, наприклад, мережі класу С на підмережі можна отримати цілком конкретне і обмежене число підмереж, при цьому чим більше кількість підмереж, тим вони «коротше».

Мінімальна підмережа містить 4 IP-адреси, однак в будь-який IP-підмережі [62] дві адреси завжди службові (перший - власну адресу підмережі, останній - широкомовний), які не можна призначити хостам, тобто лише два комп'ютери зможуть мати реальні адреси. А з цих двох, одна адреса повинна бути прописана на шлюзовому пристрої. Для мережевих служб клієнта залишається всього одна адреса, тобто чим сильніше розбита IP-мережа, тим більша втрата адрес на службові потреби.

Провайдер зазвичай використовує IP-простір планово в припущенні, що деяка частина потенційних абонентів - поодинокі користувачі (яким більше одного IP не знадобиться), інша частина - невеликі офіси (їм може знадобитися до 2-3 реальних

IP), третя - великі корпоративні клієнти з декількома філіями і розвиненою мережевою структурою (для таких слід передбачити в кілька разів більше IP-адрес для мережевих служб). З точки зору ефективності управління послугою, безпеки і зменшення широкомовного трафіку правильно було б виділяти мінімальну підмережу навіть для одиночних клієнтів, але це призведе до значних втрат адрес. [63] Для таких абонентів провайдер йде на компроміс і застосовує одну загальну адресну мережу.

Однак невеликі компанії в міру зростання можуть зажадати від провайдера додаткові адреси, до того ж послідовно нумеровані щодо отриманої раніше адреси, що не завжди здійснимо. Проблема заключається у відсутність сегментування, що знижує безпеку, широкомовний трафік обробляється усіма хостами адресної підмережі, а необережне налаштування мережевих інтерфейсів в такій конфігурації може стати причиною адресних конфліктів.

Ще одна проблема з'являється при інсталяціях послуг, що подаються по Ethernet в офісні будівлі, бізнес-центри, торговельні комплекси і тому подібні будівлі. Як правило, локальний маршрутизатор не ставиться, пристроєм доступу в будівлі є високопродуктивний Ethernet-комутатор. Якщо для абонента потрібно більше однієї реальної адреси виникне проблема пов'язана з тим, що одна з реальних адрес, яка оплачена абонентом, IP-підмережі виявиться фактично «вилученою» у абонента: адреса буде призначена в якості адреси шлюзу на сабінтерфейсі маршрутизатора, фізично розташованого на віддаленому вузлі провайдера.

Наприклад, абонент, що підключається по Ethernet, орендував у провайдера підмережу з 4 адрес, але в такій ситуації зможе використовувати в своїй мережі тільки одну адресу. У цьому випадку абоненту треба розгорнути проксі-сервер і перенести на нього адресу шлюзу. Також варіантом рішення є перейти на VPN-доступ зі статичної IP-адресою, який надає провайдер. Без використання таких рішень в Ethernet-мережі складно реалізувати модель безпеки AAA (аутентифікація, авторизація користувачів і облік споживаних ними послуг) [65]. Застосування VPN надає зручні можливості для ефективного управління послугами сеансового типу,

відкриває можливість ввести різні зони тарифікації - Інтернет, пірінг, внутрішні ресурси, персональна статистика з'єднань і ін.

3.3.5 DDOS-атаки на сервера провайдера

Абревіатура Dos, або Denial of Servise, переводиться як «відмова в обслуговуванні». Це є тип атак, направлений на припинення працездатності вузла у мережі шляхом массового запиту на сервер, які він не встигає обробити. Із-за цього перестають оброблюватись і «легітимні» запити і ресурс втрачає доступність. Додаткова буква D на початку абревіатури робить цю атаку розподіленою (Distributed) і означає відправку подібних запитів з різного числа вузлів, Зазвичай заздалегідь заражених систем. Нижче буде розглянуто найбільш частіше розповсюджені атаки. [13]

SYN-Flood - один з найпоширеніших видів DDoS на сьогоднішній день, який заснований на особливостях TCP-протоколу, а зокрема на синхронізації номера послідовності, який називається SYN-прапором, що дозволяє відстежити ланцюжок даних від клієнта до сервера в межах сесії. Коли на сервер приходить запит з прапором SYN, то він або відхиляє його, або підтверджує початок встановлення сесії і відправляє клієнту відповідь у вигляді прапора ACK. Зловмисник відправляє на сервер тисячі SYN-прапорів, [64] але підміняє в подібних запитах зворотну адресу, змушуючи сервер відповідати ACK на кожен запит. А оскільки відповіді йдуть в нікуди, то сервер намагається відіслати відповідь знову і знову, після чого ухвалення будь-яких запитів на відкриття сесії стає неможливим. Даний алгоритм атаки можна контролювати на рівні глибокої інспекції трафіку, що використовують деякі хмарні провайдери, надаючи послугу щодо захисту сервісу клієнта в рамках протидії DDoS.

UDP-Flood - атакована ціль піддається бомбардуванню з величезного числа запитів, що в підсумку задіє 100% ресурсів «жертви» і веде до їх недоступності. Такі атаки теж успішно нейтралізується сервісом захисту від DDoS з боку постачальника послуг. [74; 75]

HTTP-Flood - це найбільш поширена flood атака. В її основі - відсилання HTTP-запитів GET на 80-й порт. Це призводить до такого стану завантаження сервера, що він виявляється нездатним до обробки інших запитів. Дана flood атака може бути націлена як на корінь сервера, так і на його скрипт, зайнятий виконанням ресурсомістких завдань. Розпізнавання даної атаки можливо шляхом виявлення швидкого зростання кількості запитів до одного або декількох скриптів на сервері і швидкому зростанню логів сервера. [22]

ICMP-Echo - цей вид нападу також називають smurf-attack. При використанні даного методу на атакуємий вузол направляється широкомовний запит з адресою відправника жертви. Так як даний запит діє на цілий сегмент мережі, то всі вузли, що знаходяться в цьому сегменті, направлять відповідь саме на атакуємий хост, що кратно посилить дію атаки.

DoS (Denial of Service) - хакерська атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, при яких сумлінні користувачі системи не можуть отримати доступ до надаваних системних ресурсів (серверів), або цей доступ ускладнений.

Нажаль 100% методів захисту від DDOS-атак не існує (звісно крім повного вимкнення системи) [81], але є методи, завдяки яким можна знизити рівень загрози та наслідків від атак:

1) Нарощування обчислювальної потужності. При дійсно серйозних DDOS-атаках цей метод може не спрацювати, але, якщо запитів не надто багато, або атака знаходиться на самому початку, краще мати потужний сервер, який буде чинити опір як можна довше. За цей час можна буде застосувати заходи протидії.

2) Зворотня атака. Весь атакуючий трафік перенаправляється в зворотню сторону. Якщо в розпорядженні є досить потужний сервер, атак захлинеться і обернеться проти зловмисника.

3) Спеціалізоване програмне забезпечення. На ринку існує маса спеціальних пропозицій з протидії DDos-атакам. Подібного роду програмне забезпечення (ПО) коштує не дешево, але витрати окупляться при першій критичній ситуації.

4) Розосередження серверів. Метод заключається у рознесенні активних частин сервера з можливістю їх дублювання. Якщо якась частина ресурсів виявиться недоступною, інша частина буде функціонувати.

5) Відведення активної IP-адреси або доменного імені від ресурсів, які можуть бути схильні до атаки.

6) Фільтрація і блокування трафіку. Часто при цьому важко відокремити «чистий» трафік від «поганого», але можна відсікати тільки другорядні запити. Втім, якщо зловмисник використовує першорядні запити, цей метод виявиться слабким захистом.

7) Ліквідація вразливостей. Відразу після відбиття атаки або навіть під час неї потрібно шукати і усувати вразливі місця в системі.

3.3.6 Інсайдери та некваліфікований персонал

Інсайдери – це:

– особи, які мають доступ до конфіденційної інформації за службовим обов'язком (технічні працівники, старші менеджери, наглядові служби) або по положенню (власники компанії, привілейовані акціонери і т.д.);

– співробітники компанії, впроваджені для збору інформації з обмеженим доступом та передачі її зацікавленим особам. [21]

Важливою частиною загальної безпеки є забезпечення того, щоб ваші працівники пройшли навчання та розуміли політику інформаційної безпеки.

Навчання повинно розпочинатися з першого дня кожного працівника, і ви повинні постійно надавати їм можливість переглядати правила та оновлювати правила в пам’яті. [76] Важливо також знайти шляхи забезпечення того, щоб навчання тривало і щоб працівники не просто переглядали політику та підписували документ. Інтерактивне навчання або тестування працівників, коли вони закінчать навчання, зробить більш імовірним, що вони звернуть увагу та збережуть інформацію про ваші правила.

Ви також повинні шукати шляхи, щоб нагадувати своїм працівникам про вашу політику або надавати їм оновлення щодо нових або змінних політик. Щомісячні наради всіх співробітників та наради команд - це чудові можливості переглянути політику зі співробітниками та показати їм, що керівництво вважає цю політику важливою. Якщо зробити інформаційну безпеку частиною вашої культури, набагато більше шансів, що ваші співробітники будуть серйозно ставитися до цієї політики та вживати заходів для захисту даних.

3.4 Концепція побудови політики безпеки компанії-провайдера

Розробка концепції та політики ІБ, як правило, відбувається в кілька етапів і відповідає стадіям і етапам розробки решти нормативно-методичної та організаційно-розпорядчої документації:

1) Планування і підготовка до проведення робіт

– Розробка регламенту взаємодії Замовника і Виконавця

– Формування робочої групи проекту

– Розробка програми проведення робіт

– Визначення меж робіт

2) Обстеження корпоративної інформаційної системи

– Аналіз існуючих документів компанії

– Виконання робіт по дослідженню поточного стану інформаційного середовища і ІБ Компанії

– Заповнення опитувальних листів співробітниками Замовника і Виконавця

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

– Аналіз застосовуваних в Компанії програмно-технічних засобів

– Аналіз існуючих концепції і політики ІБ на відповідність вимогам українських і зарубіжних стандартів в області ІБ

– Аналіз ризиків ІБ

4) Розробка концепції та політики ІБ

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

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

– Коригування концепції і політики ІБ при необхідності зниження витрат на реалізацію [15; 77; 78]

Нижче наведено деякі найпоширеніші системи дотримання вимог, які мають вимоги до інформаційної безпеки, і відповідність яких може отримати ваша організація:

SOC 2 - це система відповідності, яка не вимагається законодавством, але є фактичною вимогою для будь-якої компанії, яка управляє даними клієнтів у хмарі; це процедура аудиту, яка гарантує, що ваше програмне забезпечення надійно управляє даними клієнтів. Відповідність вимогам SOC 2 вимагає від вас розробки та дотримання суворих вимог щодо захисту інформації, щоб підтримувати цілісність даних вашого клієнта та забезпечувати їх захист. [20]

ISO 27001 - це стандарт безпеки, який викладає конкретні вимоги до системи управління інформаційною безпекою організації (СУІБ). ISO 27001 заслуговує на увагу, оскільки він охоплює не лише електронну інформацію; він також включає керівні принципи щодо захисту такої інформації, як інтелектуальна власність та комерційна таємниця. Він необхідний для будь-якої компанії, яка обробляє конфіденційну інформацію. [4]

NIST SP 800-53 - це протокол безпеки, який застосовується до будь-якого компонента будь-якої системи, що зберігає, обробляє або передає федеральну інформацію. Він був розроблений для використання урядовими установами, але він зазвичай використовується підприємствами інших галузей, щоб допомогти їм вдосконалити свої системи інформаційної безпеки. Дотримання NIST також може допомогти вам дотримуватися інших вказівок, таких як HIPAA, FISMA або SOX. [18]

PCI DSS, скорочений варіант стандарту безпеки даних платіжних карток, - це структура, яка допомагає компаніям, які приймають, обробляють, зберігають або

передають дані кредитних карток та забезпечують їх безпеку. Це стосується будь-якої компанії, яка обробляє дані кредитної картки або інформацію про власників карток. Залежно від обсягу транзакцій компанії та того, чи зберігають вони дані власників карток, кожному бізнесу потрібно буде відповідати одному з чотирьох рівнів відповідності PCI DSS. [19]

Основними цілями політики інформаційної безпеки є наступні пункти:

– Забезпечення захисту інформації від загроз витоку технічними каналами.

– Забезпечення конфіденційності, цілісності і доступності інформаційних ресурсів

– Встановити загальний підхід до інформаційної безпеки.

– Виявлення та запобігання компромісу з інформаційною безпекою, таким як неправильне використання даних, мереж, комп'ютерних систем та програм.

– Захистити репутацію компанії стосовно її етичних та юридичних обов'язків.

– Дотримуватись прав споживачів; Забезпечення ефективних механізмів реагування на скарги та запитання щодо реальних чи передбачуваних невідповідностей політиці є одним із шляхів досягнення цієї мети.

3.5 Політика безпеки Інтернет-провайдера

В результаті роботи розроблено політику безпеки інтернет провайдера, яка повинна мати наступний вигляд:

«Вступ:

З метою забезпечення максимально можливого рівня безпеки Інтернет-послуг та продуктів, що надаються Клієнтам Інтернет-провайдера, а також внутрішніх процесів, інфраструктури, ІТС та інформації, що в них обробляється, Інтернет-провайдер розробив та впровадив Систему Управління Інформаційною Безпекою (СУІБ)

Безпекою (СУІБ). Впроваджена в Інтернет-Провайдер СУІБ ґрунтується на вимогах галузевих стандартів (стандарт захисту інформації в індустрії платіжних карт (PCI DSS), стандарти Міжнародної Організації зі Стандартизації (ISO)) та

рекомендаціях кращих міжнародних практик в галузі захисту інформації (NIST SP 800-53).

1. Ціль політики інформаційної безпеки

Реалізовані Інтернет-провайдером принципи, що випливають з Системи Управління Інформаційною Безпекою, повинні забезпечити досягнення наступних цілей інформаційної безпеки:

– Відповідність до вимог законодавства

– Забезпечення цілісності, конфіденційності та доступності даних

– Попередження інцидентів ІБ – прогнозування, своєчасне виявлення та усунення загроз безпеки інформаційним активам

– Відновлення від наслідків

– Адекватна оптимізація засобів захисту відповідно до поточних потреб Інтернет-провайдера

– Адекватний захист інформації і засобів її обробки щодо рівня ризику

2. Сфера застосування

Сферою застосування СУІБ є компанія в цілому. Дія Політики поширюється на всі підрозділи Інтернет-провайдеру. Політика використовується для усіх критичних бізнес-процесів/банківських продуктів/програмно-технічних комплексів компанії, є обов'язковою до виконання всіма співробітниками, а також особами, які працюють з інформацією, що належить Інтернет-провайдеру, в межах укладених контрактів та договорів.

3. Предмет політики

– Основними принципами Політики є підтримання належного захисту інформації із забезпеченням її цілісності, конфіденційності, доступності та спостережності.

– Етапи ефективного функціонування СУІБ є циклічними за схемою «Планування – Впровадження – Перевірка – Корегування», основними з них є:

1) підготовка до впровадження;

2) опис існуючої інфраструктури та заходів;

3) оцінка ризиків ІБ;

4) планування комплексу заходів щодо мінімізації ризиків;

5) затвердження та впровадження комплексу заходів;

6) навчання працівників;

7) складання звітів про стан ІБ

– Для кожного інформаційного активу визначаються ризики ІБ та шляхи їх мінімізації, тобто Інтернет-провайдер підтримує ризик-орієнтовний підхід, який забезпечує розуміння, моніторинг та зменшення ризиків діяльності.

– Заходи та засоби захисту інформаційних активів обираються за результатами аналізу ризиків для інформаційних активів. Витрати на ІБ повинні бути адекватними існуючим ризикам з урахуванням витрат на їх реалізацію і можливих витрат від реалізації загроз.

– Інтернет-провайдер виявляє, враховує та оперативно реагує на дійсні і ймовірні порушення ІБ. Всі інциденти ІБ фіксуються, аналізуються та враховується при розробці заходів забезпечення захисту інформаційних активів, в тому числі у внутрішніх нормативних документах.

– Принцип безперервності: інформаційна безпека є безперервним процесом протистояння загрозам та управління ризиками, характерними для сфери діяльності компанії.

4. Ролі та відповідальності компанії

Правління Інтернет-провайдера затверджує цю Політику інформаційної безпеки компанії, здійснює контроль та приймає рішення щодо виділення необхідних ресурсів і фінансування заходів та/або проектів з Інформаційної безпеки компанії. Підрозділ Інформаційної безпеки визначає та впроваджує вимоги з Інформаційної безпеки компанії, забезпечує функціонування та використання засобів Інформаційної безпеки, організовує належне навчання з питань Інформаційної безпеки для працівників компанії. Працівники компанії несуть персональну відповідальність за виконання вимог законодавства України та нормативних документів Інтернет-провайдера з питань Інформаційної безпеки, зокрема збереження персональних даних клієнтів та іншої конфіденційної

інформації компанії, підтримку відповідного рівня Інформаційної безпеки при виконанні своїх посадових обов'язків.

5. Перегляд документа

Виконується робота щодо підтримки Політики інформаційної безпеки в актуальному стані. Політика переглядається за необхідністю, але не менш ніж одного разу на рік. Причинами внесення змін до Політики є зміни в інформаційної інфраструктурі та/або впровадженні нових інформаційних технологій, а також змінах в законодавчих, регуляторних та інших нормах.» [81]

Висновки до розділу 3

В третьому розділі було опрацьовано нормативно-правове забезпечення, а саме конкретні стандарти, які необхідні для розробки політики безпеки компанії. Була розроблена таблиця загроз та протидії загрозам для Інтернет-провайдера (табл.. 3.1). Описані основні проблеми Інтернет-провайдеріва, такі як: перебої електропостачання, обрив ліній, DoS-атаки та інші. Абревіатура Dos, або Denial of Servise, переводиться як «відмова в обслуговуванні». Це є тип атак, направлений на припинення працездатності вузла у мережі шляхом массового запиту на сервер, які він не встигає обробити. Із-за цього перестають оброблюватись і «легітимні» запити і ресурс втрачає доступність. Відповідно основним проблемам були розроблені варіанти їх вирішення. Одною з найчастіших атак, за статистикою, на компанію Інтернет-провайдера є DDoS-атаки. Також розглянуто концепцію побудови політики безпеки та відповідно розроблена політика безпеки Інтернет-провайдера.

ВИСНОВКИ

В бакалаврській роботі було:

- Проведено аналіз сучасної структури мережі Інтернет. Internet - глобальна інформаційна мережа, яка є з'єднала безліч регіональних (локальних) комп'ютерних мереж і пристроїв, що обмінюються між собою інформацією по каналах громадських телекомунікацій.

- Розкрито можливі топології побудови мереж, їх переваги та недоліки; Існує п’ять основних типів топології в комп’ютерних мережах: сітка, зірка, шина, кільце, гібридна.

- Досліджено еталонну модель OSI, розкрито можливі проблеми та варіанти їх виправлення;

- Здійснено аналіз поняття постачальника послуг Інтернет. Інтернет-провайдер - це компанія, яка надає доступ до Інтернету організаціям та домашнім користувачам. Інтернет-провайдери виступають як "сховища даних", передаючи свої великі обчислювальні потужності в оренду багатьом тисячам операторів веб-сайтів, починаючи від юридичних до приватних осіб закінчуючи корпораціями, некомерційними групами та державними установами.

- Розкрито питання надання доступу до мережі Інтернет через здійснення типологізації послуг, що забезпечують Інтернет-провайдери;

- Досліджено побудову мережі постачальників послуг; Референтна модель побудови мережі: рівень доступу; рівень агрегації; рівень ядра мережі; серверний рівень.

- Встановлено особливості нормативно-правового забезпечення, а саме конкретних стандартів, які необхідні для розробки політики безпеки компанії, наприклад: BS 7799 (Визначаються і розглядаються наступні аспекти організації режиму ІБ: політика безпеки; організація захисту; класифікація інформаційних ресурсів і управління ними; управління персоналом; фізична безпека; адміністрування комп'ютерних систем і мереж; управління доступом до систем;

Розробка та супровід систем; планування безперебійної роботи організації; перевірка системи на відповідність вимогам ІБ), ISO 27001 (Стандарт ISO 27001 зосереджений на захисті конфіденційності, збереження і доступності інформації в компанії), IEC 31010:2019 (Даний стандарт входить в серію стандартів з управління бізнесризиками без прив'язки конкретно до ризиків ІБ)

- Проведено аналіз загроз Інтернет-провайдера та запропоновані протидії загрозам;

- Визначено основні проблеми Інтернет-провайдеріва, такі як: перебої електропостачання, обрив ліній, DDoS-атаки та інші;

- Здійснено аналіз концепції побудови політики безпеки та відповідно розроблена політика безпеки Інтернет-провайдера.

ДЖЕРЕЛА

1. What is an ISP? - Definition and responsibilities [Електронний ресурс] – Режим доступу до ресурсу: https://www.whoismyisp.org/articles/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/raznoe/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-of/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/osi-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.org.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/content/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/vasexperts/blog/313562/.

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

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

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

18. SP 800-53 [Електронний ресурс] – Режим доступу до ресурсу: https://csrc.nist.gov/publications/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/ueip

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

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

22. What is an HTTP Flood [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/learn/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/bitstream/123456789/25156/1/Tarnavsky_Kuzmenko_Org_Komp_merej.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-security-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/security/rfc/RFC3013EN.html

30. ISP Security: Do We Expect Too Much? [Електронний ресурс] – Режим доступу до ресурсу: https://www.darkreading.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/endpoint/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.gov.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/JH77G00A.html

39. Про основні засади забезпечення кібербезпеки України, Закон України. [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.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.wikipedia.org/wiki/Information_security

61. Internet service provider [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.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/blog/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/43/2018/03/07185213/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-subscriber-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/123456789/154453

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 3.1

Загрози та протидія

Рівні	Атака	Протидія
Атаки на фізичному рівні	Атака на концентратори	Для уникнення атак на фізичному рівні достатньо використовувати комутатори
Атаки на канальному рівні	Переповнення Contet Address Memory таблиці	Рекомендується жорстко прив'язувати MAC адресу робочої станції до порту комутатора або обмежити кількість MAC адрес підключаємих до порту до одного адресу
	VLAN Hoping	Всі використовувані інтерфейси комутатора перевести в режим access та trunk, а ті, що не використовуються перевести в shutdown та перевести їх в неіснуючий VLAN, котрий буде відомий тільки даному комутатору
	Атака на STP	Заборонити передачу BPDU-пакетів з портів на котрих нема комутаторів та якщо такий пакет все ж прийшов, то переводити цей порт в режим shutdown
	MAC Spoofing	Потрібно виконати ті ж самі дії, що й при переповненні CAM таблиці
	Атака на Private VLAN	На маршрутизаторі створити спеціальний Access List в котрому забороняється пряма передача між сегментами мережі

Продовження таблиці 3.1

Рівні	Атака	Протидія
Атаки на канальному рівні	Атака на DHCP	Метод боротьби з атаками даного типу називається DHCP Snooping. Метод заключається в порівнянні MAC-адрес, указаному в DHCP-запиті та тому, що був прописан в порті комутатора
	ARP-spoofing	Використовувати додаток arpwatch. Одним з можливих способів є використання статичного ARP. Іншим методом є використання шифрування а також застосування локальних мереж VLAN
Атака на мережевому рівні	Атаки на статичну маршрутизацію	Фізічний захист маршрутизаторів, видача прав адміністратора лише тим користувачам, котрі можуть запускати службу маршрутизації та віддаленого доступу
	Атаки з протоколом Routin Information Protocol	Використовувати Access Control List, блокувати пакети, що входять у мережу, які стверджують, що мають IP адресу внутрішньої мережі, використовувати технологію IPS, конфігурувати захист портів, dhcp snooping
	Надсилання LSA-пакетів	Заблокувати флудінг на OSPF для типів broadcast та point-to-point. В мережах point-to-multipoint можете заблокувати "затоплення" для деяких сусідів

Продовження таблиі 3.1

Рівні	Атака	Протидія
Атака на мережевому рівні	Злам хешу MD5	Перевірка достовірності, фільтр зовнішніх маршрутів на граничних маршрутизаторах автономної системи, використання складних паролів
	Атаки BGP	Захист джерела - підпис AS, захист джерела та сусідів - підпис вихідної AS, захист джерела та маршрута - підпис вихідної AS та підписи AS_PATH для маршрутизаторів. Фільтрація базується на перевірці AS_PATH та NLRI вихідної AS
	Атаки на протоколи MPLS та MPLS-VPN	Безпека підтримується за допомогою використання протоколу BGP та системи рішень IP-адрес. Використання засобів автентифікації та шифрування
Атаки на транспортному рівні	Атаки на TCP	Оскільки ключовий елемент атаки - вгадування sequence number, то допомогти може використання криптографічно стійкого алгоритма генерації псевдовипадкоих чисел для генерації sequence number. Фільтрація SYN пакетів та шифрування TCP пакетів
	Атаки на UDP	Рекомендації аналогічні рекомендаціям по захисту TCP

Продовження таблиці 3.1

Рівні	Атака	Протидія
Атаки на рівні додатків	Протокол SNMP	Для забезпечення безпеки приладів, моніторинг яких ведеться за допомогою SNMP протоколу, необхідно використовувати міжмережеві екрани для сегментації та вирішення взаємодії по данному протоколу лише довірених хостів
	Протокол Syslog	Обмежити отримання повідомлень лише з тих вузлів, котрі здійснюють генерацію подій. Обмежити передачу подій можна за допомогою мережевого обладнання, забороновши пересилку UDP пакетів по 514-му порту
	Протокол DNS	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;