УДК 004.05:004.73 **DOI: 10.31673/2412-9070.2023.032030**

В. О. ВЛАСЕНКО, канд. техн. наук, доцент;
Ю. В. ЩАВІНСЬКИЙ, канд. техн. наук, доцент;
М. М. ЗАПОРОЖЧЕНКО, асистент кафедри;
В. С. ТИЩЕНКО, асистент кафедри,
Державний університет інформаційно-комунікаційних технологій, Київ

АНАЛІЗ ТЕХНОЛОГІЙ ПОБУДОВИ МЕРЕЖІ ПЕРЕДАВАННЯ ДАНИХ ІЗ ВИСОКИМИ ВИМОГАМИ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, НАДІЙНОСТІ ТА ЗАТРИМКИ

Наукову статтю присвячено аналізу сучасних підходів і технологій у побудові мереж передавання даних, спрямованих на забезпечення інформаційної безпеки, надійності та мінімальної затримки. Обґрунтовано потребу в комплексному врахуванні факторів, які впливають на ефективність мережі із зосередженням уваги на надійності та безпеці. Аналіз мереж дає можливість створити інфраструктуру, яка відповідатиме вимогам сучасного інформаційного середовища, комплексно брати до уваги переваги та недоліки кожної технології мережі в процесі побудови. Для математичного оцінювання надійності мережі передавання даних запропоновано марковську модель, яка базується на теорії марковських процесів. Розроблена мовою програмування Python із використанням бібліотек модель дає змогу кількісно оцінити надійність мережі передавання даних, зважаючи на різні фактори відмов, переходів між станами та відновлення. Модель дозволяє прогнозувати стани мережі та планувати превентивні організаційні і технічні заходи щодо забезпечення надійності та безпеки через постійно зростаючі вимоги до якості обслуговування і захисту конфіденційної інформації. Аналіз методів затримки передавання інформації виявив залежність швидкості і обсягу інформації, що передається, від багатьох факторів, зокрема пропускної здатності, навантаження мережі, типу та швидкості з'єднання, оброблення даних вузлами мережі. У дослідженні визначено потребу в комплексному відпрацюванні систем оцінювання та створенні загальної моделі оцінювання.

Ключові слова: інформаційна безпека; мережа передавання даних; надійність; затримка; моделювання мереж; моделі оцінювання; моделі Маркова.

ВСТУП

Постановка проблеми. Вплив сучасних технологій на розвиток мереж передавання даних неодмінно визначається високими вимогами до безпеки, надійності та затримки в обробленні інформації. Сучасний цифровий світ ставить перед собою завдання забезпечити швидке та надійне передавання даних, одночасно забезпечуючи високий рівень захисту конфіденційної інформації. Вимоги до інформаційної безпеки, надійності і мінімальної затримки стають стрижневими факторами у виборі технологічних рішень та підходів до побудови мереж передавання даних.

Щораз більша кількість підімкнених пристроїв, хакерські атаки та кіберзагрози роблять безпеку мережі особливо важливою проблемою. Зловмисники можуть використовувати слабкі місця в мережі для отримання несанкціонованого доступу до конфіденційних даних.

Додаткові вимоги до мінімальної затримки стають нагальними для застосунків реального часу, таких як відеодзвінки, відеоігри та системи Інтернету речей (IoT). Гарантування швидкого передавання даних стає викликом. Зі зростанням обсягів даних і під'єднаних пристроїв мережі мають бути здатні масштабуватися, щоб забезпечити високу продуктивність навіть у разі великого навантаження.

Різноманітні технології і протоколи можуть створювати проблеми сумісності та ускладнювати інтеграцію різних систем. Збільшення масштабів мереж і кількості підімкнених пристроїв потребує пошуку ефективних шляхів застосування нових технологій побудови сучасних мереж, які забезпечуватимуть вимоги інформаційної безпеки, надійності та затримки. Наукові дослідження взаємодії між різними технологічними аспектами, які охоплюють проводові та безпроводові технології, криптографічні методи, алгоритми маршрутизації та керування мережею, дають змогу створити інфраструктуру, яка відповідатиме вимогам сучасного інформаційного середовища.

У цьому контексті аналіз технологій побудови мереж передавання даних із високими вимогами щодо інформаційної безпеки, надійності та затримки є критично важливим для розвитку сучасних інформаційних систем.

Аналіз останніх досліджень і публікацій. За останні роки через появу великої кількості видів мереж передавання даних та потребу в забезпеченні захисту інформації, що в них циркулює, науковці приділяють достатньо уваги аналізу таких мереж стосовно надійності та затримки. У статтях [1-3] наведено

порівняльний аналіз сучасних технологій передавання даних, які можуть бути використані в сучасних промислових системах автоматизації та телемеханіки для обміну даними з різними давачами та іншими системами безпеки і контролю доступу. Автори описують найбільш поширені типи мереж передавання і пропонують варіанти їх застосування стосовно вимог конкретних замовників. Основний акцент робиться на рішеннях із відкритим вихідним кодом, які можуть бути використані в дослідницьких проєктах на неліцензованій основі.

У працях [4; 5] оцінюється сучасний стан визначення основних ризиків та напрямів подальшого розвитку з метою поліпшення ситуації з кібербезпекою мереж на базі **LoRaWAN** (*Long Range Wide Area Network* — Глобальна мережа далекої дії). LoRaWAN відповідає трьом ключовим вимогам застосунків IoT (низька вартість, великомасштабне розгортання, висока енергоефективність) завдяки відкритому стандарту та побудові автономних мереж без сторонньої інфраструктури. Водночас автори наголошують на потребі у вирішенні багатьох дослідницьких питань, таких як розподіл ресурсів, координація каналів, надійність передавання, продуктивність і, передусім, безпека.

Сьогодні величезний обсяг даних збирається з численних різнорідних джерел, які генерують дані в режимі реального часу з різними якостями, котрі вважаються великими даними (Big Data). Для організації надійності Big Data в керуванні фізичними системами у сферах виробництва та цивільної інфраструктури в статті [6] дослідниками розглядається концепція «цифрового двійника» для збереження великого обсягу даних. У [7] проаналізовано проблеми з безпекою і надійністю Big Data у сфері енергетики та визначено шляхи їх розв'язання через копіювання і дублювання даних.

Нині проводяться дослідження ефективності застосування технологій віртуалізації для розгортання інфраструктури організації будь-якої складності. Ці підходи широко використовуються сучасними операторами зв'язку для побудови своїх телекомунікаційних мереж або розширення спектра нових послуг. Науковцями [8; 9] досліджуються високоефективні архітектури для нових, розширених або модернізованих проєктів віртуальних центрів оброблення даних, ефективність контейнерної віртуалізації та віртуальних машин на основі гіпервізора для взаємної ізоляції віртуальних машин і контейнера. Автори зазначають, що віртуалізація даних може допомогти розв'язати проблеми, пов'язані з конфіденційністю, але існує потреба в подальших дослідженнях через недостатню стабільність віртуального сервера під час одночасного навантаження.

У праці [10] розглянуто проблему оптимізації структури мереж нового покоління **NGN** (*Next Generation Network*). Авторами побудовано математичну модель оптимального проєктування структури та розроблено алгоритм її розв'язання, а також наведено результати експериментальних досліджень і практичне впровадження запропонованого інструментарію.

Розглянутий аналіз наукових публікацій свідчить про постійний пошук ефективних технологій побудови мереж передавання даних. Водночас у дослідженнях приділяється недостатньо уваги комплексному поєднанню вимог щодо інформаційної безпеки, надійності та затримки передавання інформації.

Метою статті є здійснення аналізу сучасних технологій побудови мереж передавання даних стосовно відповідності вимог щодо інформаційної безпеки, надійності та затримки.

ОСНОВНА ЧАСТИНА

Сьогодні існує велика кількість технологій, за допомогою яких організовують системи передавання інформації. При цьому, як середовище передавання можуть використовуватися як різні кабельні системи (вита пара, тонкий коаксіальний кабель, товстий коаксіальний кабель, волоконно-оптичні лінії зв'язку тощо), так і повітряне середовище (технології Wi-Fi, Bluetooth, інфрачервоний канал). Створення сучасних інформаційних систем неможливо без використання загальних підходів у процесі розроблення, без уніфікації характеристик і параметрів їх компонентів. Класифікація мереж передавання даних є важливим інструментом для розуміння, організації та аналізу різних типів мереж, аналізу та вибору оптимальних рішень у галузі телекомунікацій та інформаційних технологій. Вона допомагає в структуруванні та визначенні характеристик мереж, а також у виборі найбільш відповідної мережі для конкретних потреб і застосувань. Найбільш поширену класифікацію запропоновано на рис. 1.

Класифікація допомагає виокремити різні типи мереж передавання даних відповідно до їхніх функціональних потреб і застосувань, допомагає розпізнавати найкращі технології для конкретного типу мережі, визначити, які вимоги є ключовими для конкретного типу мережі.

Особливості технологій передавання даних

Нині існує кілька ключових технологій побудови мереж передавання даних, які можуть використовуватися окремо або комбінуватися для побудови складних інфраструктур передавання залежно від потреб користувачів і сценаріїв використання.

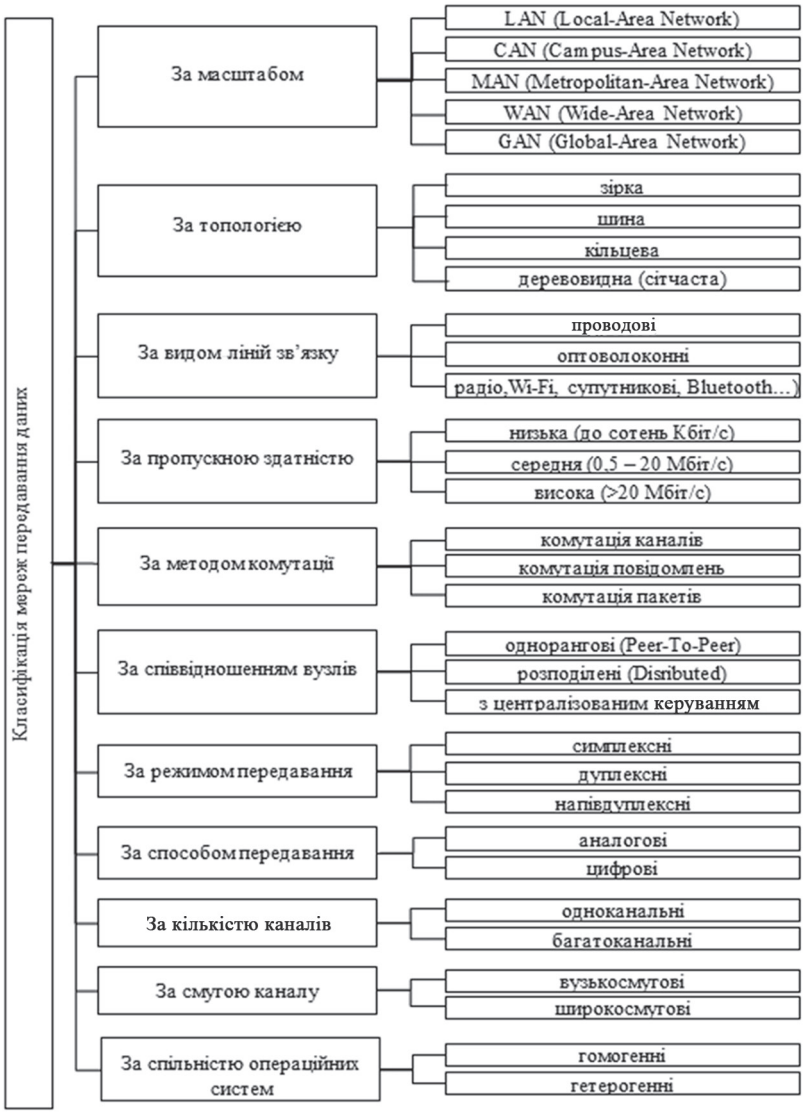

Рис. 1. Класифікація мереж передавання даних

Технологія Ethernet, яка домінує у сфері локальних мереж (LAN), є однією з найпоширеніших технологій проводового підімкнення до мережі і підтримує різні стандарти швидкості передавання, зокрема 10/100/1000/10000 Мбіт/с. Її застосовують для передавання даних через мідний або оптоволоконний кабель. Оптоволоконний кабель забезпечує високошвидкісне передавання даних за допомогою світлових сигналів і використовується для створення великих мереж із високою пропускною здатністю та розглядається як окрема технологія побудови мережі.

Комбінація безпроводових технологій Wi-Fi, Bluetooth, Satellite дає змогу будувати мережі передавання даних із високою швидкістю та організовувати покриття через комунікаційні супутники важкодоступних місць із потрібним рівнем безпеки і надійності та дотриманням відповідних умов. Під час організації супутникового зв'язку замість традиційних радіохвиль лазерна система забезпечує нині пропускну здатність до 200 Гбіт/с.

Поширеною сьогодні є технологія побудови мереж **IoT (***Internet of Things***)**, яка об'єднує різні фізичні пристрої, що здатні взаємодіяти та обмінюватися даними в інтернеті, використовуючи різні протоколи, та технологія **NFC (***Near Field Communication***)**, що дає змогу обмінюватися даними на дуже короткій відстані (зазвичай кілька сантиметрів) і використовується для оплати, ідентифікації та інших застосунків.

Технологія *Powerline Communication* (PLC) для передавання даних використовує електричні проводи в будинку. Вона може бути застосовна для побудови мережі на основі вже наявних електромереж.

Аналіз показує, що кожна технологія має свої переваги та недоліки з погляду інформаційної безпеки, надійності та затримки передавання інформації. Порівняльний аналіз за розглянутими критеріями зведено в таблиці.

Порівняльний аналіз технологій побудови мереж передавання даних

Технологія мережі	Критерії порівняння		
	Інформаційна безпека	Надійність	Затримка
Ethernet	Безпека може бути обмеженою, зазвичай використовують додаткові заходи безпеки, такі як VLAN (віртуальні локальні мережі) і мережні файрволи	Характеризуються низьким рівнем відмовостійкості, але можуть бути вразливі до відмов на рівні фізичних з'єднань або обладнання	Низька затримка в межах локальної мережі, але може збільшуватися під час з'єднання великих відстаней
Wi-Fi	Уразливі до атак перехоплення або зламу паролів, для забезпечення безпеки можуть використовуватися методи шифрування WPA3 та інші заходи безпеки	Схильні до завад та втрати сигналу, надійність залежить від забезпечення належного покриття й якості обладнання	Затримка в Wi-Fi мережах може бути змінною і залежить від великої кількості факторів, зокрема навантаження мережі, типу пристроїв тощо
Bluetooth	Має механізми шифрування, але виявлено вразливості, які можуть бути використані для атак	Призначені для коротких з'єднань, і їх надійність залежить від якості радіосигналу та відстані між пристроями	Низька затримка, особливо в близьких пристроях
Стільниковий зв'язок (мобільні мережі)	Потребують високого рівня безпеки через шифрування та автентифікацію, однак можуть бути вразливі до атак, таких як перехоплення SMS-повідомлень	Вирізняються високою надійністю на великих територіях, але можуть бути недоступні у віддалених місцях або під час великих навантажень	Затримка в мобільних мережах може варіюватися залежно від рівня навантаження та відстані до мобільної вежі
Волоконна оптика (оптичні волокна)	Мають високий рівень безпеки, оскільки світлові сигнали важко перехопити без фізичного доступу до волокон	Високий рівень надійності, мало вразливі до електромагнітних втручань та інших зовнішніх факторів	Низька затримка, особливо на великих відстанях
Satellite (супутникові мережі)	Потребують високого рівня шифрування та безпеки для захисту передавання даних до супутника та назад	Схильні до втрат сигналу через атмосферні умови та інші зовнішні фактори	Затримка в супутникових мережах зазвичай вища через велику відстань до супутника і залежить від атмосферних умов
Mesh Networks	Можуть бути вразливі до атак через різні пристрої, які входять у склад мережі	Можуть бути дуже надійними завдяки маршрутизації даних через різні шляхи	Затримка може бути змінною, залежно від маршруту та навантаження мережі
PLC (лінії електропередач)	Уразливі до перехоплення сигналу, а також до електромагнітних втручань	Залежить від якості електромережі та наявності завад	Затримка в PLC може бути вищою через фізичну природу передавання даних через електромережу
Віртуальні приватні мережі (VPN)	VPN забезпечує високий рівень шифрування для захисту даних під час передавання через відкритий інтернет.	Залежить від налаштувань VPN-сервера та якості підімкнення.	Затримка в VPN може бути вищою через додатковий прошарок шифрування та дешифрування даних.

Поєднання переваг кожної технології в доступності, швидкості передавання, мобільності з недоліками вразливості, обмеженого радіуса дії, складності побудови та економічної доцільності дає можливість будувати мережі в різних конфігураціях. Вибір конкретної технології буде залежати від конкретних вимог до мережі і застосування.

Механізми оцінювання мереж передавання даних

Рівень інформаційної безпеки мережі передавання даних може бути визначений як кількісно, так і якісно. Кількісний підхід може охоплювати вимірювання таких показників:

- кількість уразливостей, виявлених під час аудиту безпеки;
- кількість вдало проведених хакерських атак чи спроб несанкціонованого доступу;
- час відновлення мережі після виникнення інциденту безпеки;
- кількість успішно виявлених аномалій у системі моніторингу безпеки;
- витрати на заходи щодо підвищення безпеки порівняно з потенційними збитками від порушення безпеки.

Однак інформаційна безпека також має багато якісних аспектів, зокрема:

- ефективність політики безпеки та реакція на інциденти;
- рівень обізнаності та підготовки персоналу з питань безпеки;
- використання сучасних і робочих заходів безпеки (шифрування, автентифікація тощо);

• здатність мережі витримати напади та відновитися після них;
• відповідність мережі нормативам та стандартам безпеки.

Оцінювання надійності мережі передавання даних вимагає системного підходу та аналізу різних аспектів. А отже, для цього потрібно визначити головні метрики надійності, дослідити історію відмов та інцидентів у мережі та їх причини, перевірити, як система реагує на різні сценарії відмов, оцінити можливість мережі ефективно масштабуватися в разі збільшення обсягу трафіку або підімкнення пристроїв, оцінити відповідність мережі вимогам до якості обслуговування для різних типів трафіку, зокрема голосового чи відеоконференційного зв'язку, встановити системи моніторингу, які дають змогу відстежувати використання ресурсів, пропускну здатність, навантаження та інші параметри мережі для вчасного виявлення аномалій. Одним із перспективних способів оцінювання надійності є застосування математичного апарату. Цей апарат охоплює різні методи та моделі, які допомагають кількісно оцінити надійність мережі на основі ймовірності відмов та інших параметрів.

Існують відомі методи та моделі, що використовуються для математичного оцінювання надійності мереж передавання даних. Найбільш поширена — марковська модель, яка базується на теорії марковських процесів, де стан системи змінюється відповідно до певних правил та ймовірностей переходу між станами. Це може бути корисно для моделювання надійності мереж із різними компонентами та вузлами і визначення ймовірності переходу в конкретний стан після деякої події. Стани мережі передавання даних можуть репрезентувати різні конфігурації, умови або події, які можуть виникати в мережі. Вибір можливих станів залежить від конкретного контексту та характеристик мережі.

Для прикладу візьмемо десять станів мережі:
• нормальна робота (Normal);
• відмова обладнання (Equipment Failure);
• перевантаження (Overload);
• резервування (Redundancy);
• відновлення після відмови (Recovery after Failure);
• атака (Attack);
• обслуговування (Maintenance);
• перехідний стан (Transient State);
• затримка (Delay);
• відсутність з'єднання (No Connection).

Для побудови матриці ймовірностей переходу з одного стану в інший застосовують статистичні дані про стани системи, оцінювання експертів, модельні розрахунки чи симуляції або наукову літературу для отримання приблизних значень імовірностей переходів даного типу мережі.

Лістинг моделі оцінювання на мові Python з використанням її стандартної бібліотеки NetworkX такий:

```
import networkx as nx
import matplotlib.pyplot as plt

# Додавання станів як вузли графа
states = ['Normal', 'Equipment Failure', 'Overload', 'Redundancy', 'Recovery after Failure', 'Attack',
'Maintenance', 'Transient State', 'Delay', 'No Connection']

# Визначення матриці ймовірностей переходу (приклад)
transition_matrix = [
  [0.7, 0.05, 0.05, 0.1, 0.03, 0.02, 0.01, 0.02, 0.01, 0.01],
  [0.1, 0.6, 0.1, 0.05, 0.03, 0.05, 0.02, 0.01, 0.02, 0.01],
  [0.05, 0.1, 0.5, 0.05, 0.02, 0.03, 0.05, 0.02, 0.1, 0.03],
  [0.03, 0.02, 0.02, 0.7, 0.1, 0.01, 0.01, 0.05, 0.03, 0.03],
  [0.05, 0.03, 0.02, 0.1, 0.6, 0.01, 0.02, 0.02, 0.02, 0.03],
  [0.02, 0.01, 0.01, 0.02, 0.03, 0.8, 0.05, 0.01, 0.02, 0.03],
  [0.01, 0.02, 0.03, 0.01, 0.02, 0.02, 0.8, 0.05, 0.02, 0.02],
  [0.03, 0.01, 0.02, 0.02, 0.02, 0.03, 0.02, 0.6, 0.1, 0.05],
  [0.02, 0.02, 0.05, 0.03, 0.03, 0.01, 0.02, 0.03, 0.6, 0.15],
  [0.01, 0.01, 0.02, 0.01, 0.01, 0.02, 0.02, 0.03, 0.03, 0.84]
]
```

```
# Створення графа (мережі)
G = nx.DiGraph()

G.add_nodes_from(states)

# Додавання ребер із вагами
for i in range(len(transition_matrix)):
    for j in range(len(transition_matrix[i])):
        G.add_edge(states[i], states[j], weight=transition_matrix[i][j])

graph_edges = list(G.edges())
expected_edges = [(states[i], states[j]) for i in range(len(transition_matrix)) for j in range(len(transition_
matrix[i]))]
if set(graph_edges) == set(expected_edges):
    print("Graf mistut vci rebra")
else:
    print("U Grafi e vidsutni rebra")

# Встановлення ймовірностей переходу на графі
for i, row in enumerate(transition_matrix):
    for j, prob in enumerate(row):
        G[states[i]][states[j]]['weight'] = prob

# Візуалізація графа
pos = nx.spring_layout(G)  # Розташування вузлів на графі
edge_labels = {(i, j): f"{G[i][j]['weight']:.2f}" for i, j in G.edges()}
nx.draw(G, pos, with_labels=True, node_size=2000, font_size=8, font_color='black')
nx.draw_networkx_edge_labels(G, pos, edge_labels=edge_labels, font_size=8, label_pos=0.3)

plt.title("Markov Chain State Transition Graph")
plt.show()

# Оцінювання ймовірностей перебування в різних станах після 10 кроків
current_state = 'Normal'
steps = 10
state_probabilities = {state: 0 for state in states}
state_probabilities[current_state] = 1

for _ in range(steps):
    new_state_probabilities = {state: 0 for state in states}
    for i in states:
        for j in states:
            new_state_probabilities[j] += state_probabilities[i] * G[i][j]['weight']
    state_probabilities = new_state_probabilities

# Виведення результатів
print("State probabilities after", steps, "steps:")
for state, prob in state_probabilities.items():
    print(state, ":", prob)
```

Цей приклад марковської моделі використовує графічне подання станів та їх імовірностей переходів у вигляді графа (рис. 2).

Результат виведення (рис. 3) показує ймовірності перебування в різних станах після зазначеної кількості кроків.

На практиці кількість «steps» може визначатися залежно від цілей аналізу та характеру мережі. Більша кількість кроків може знадобитися для виявлення довготривалих змін станів, тоді як менша кількість може використовуватися для швидкого оцінювання відносних імовірностей перебування в різних станах.

Рис. 2. Граф станів і переходів марковської моделі

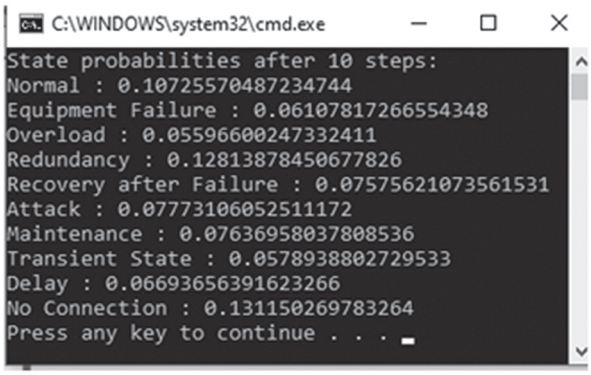

Рис. 3. Результат розрахунку ймовірностей станів

Варто зауважити, що матриця ймовірностей переходів у прикладі є довільною та слугує лише для ілюстрації роботи запропонованої моделі. У реальних застосунках вона залежатиме від конкретних характеристик мережі та її станів. Такий підхід дає змогу аналізувати можливі стани системи та їх імовірність у майбутньому, беручи до уваги їхній взаємозв'язок та можливі переходи між ними.

Оцінювання затримки повідомлень у мережі передавання даних є важливою задачею, особливо із застосунками, які мають високі вимоги до низької затримки, зокрема мереж реального часу, відеостримінгу, VoIP тощо. Оцінювання затримки може залежати від різних факторів та параметрів мережі. Є кілька способів, за допомогою яких можна оцінити затримку повідомлень:

- використання аналітичних моделей, які зважають на характеристики мережі, такі як пропускна здатність, затримка на початку та в кінці мережі, оброблення маршрутизаторами тощо;
- використання симуляційних програм, які моделюють роботу мережі з різними типами вузлів, з'єднаннями, обробленням даних для вимірювання затримки;
- вимірювання затримок за реальних умов у реальних мережах за допомогою спеціальних пристроїв або програмних засобів, зокрема traceroute, ping, спеціальних програм Wireshark або PingPlotter, які дають можливість вимірювати затримку в мережі;
- моделювання затримок у компонентах мережі на різних етапах пересилання даних: на маршрутизаторах, у комутаторах з огляду на характеристики цих компонентів.

Важливо розуміти, що затримка може бути залежною від багатьох факторів, таких як пропускна здатність, навантаження мережі, тип та швидкість з'єднання, оброблення даних вузлами мережі тощо. Тому, вибираючи метод оцінювання затримки, потрібно зважати на особливості вашої системи та задачі.

ВИСНОВКИ

Наведений аналіз технологій побудови мереж передавання даних дозволяє проєктувати мережі з високими вимогами до інформаційної безпеки, надійності та затримки. Одним із ефективних шляхів створення мереж є дослідження розглядуваних показників методом побудови математичних моделей із застосуванням мови програмування Python та використання її бібліотек для кращого розуміння структури мережі та поведінки системи. Подальші дослідження будуть спрямовані на створення комплексних математичних моделей, за допомогою яких буде можливість визначати всі характеристики мереж.

Список використаної літератури

*1. **Liu J., Chen M., Wang L.** A new model of industrial internet of things with security mechanism - An application in complex workshop of diesel engine // Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science. 2020. Т. 234. №. 2. С. 564–574.*

*2. **Lu Y., Da Xu L.** Internet of Things (IoT) cybersecurity research: A review of current research topics // IEEE Internet of Things Journal. 2019. Vol. 6. №. 2. P. 2103–2115.*

*3. **Łukasik Z, Ushakov A.** Comparative analysis of data transmission technologies in industrial systems of the Internet of things (IoT) // Journal of Automation, Electronics and Electrical Engineering. 2021. №2. P. 31–39.*

*4. **Czeczot G., Rojek I., Mikołajewski D.** Analysis of Cyber Security Aspects of Data Transmission in Large-Scale Networks Based on the LoRaWAN Protocol Intended for Monitoring Critical Infrastructure Sensors. // Electronics. 2023. №12. P. 2503–2512.*

5. ***Dai R., Diraneyya O., Brell-Çokcan S.*** *Покращення передавання даних на будівельних майданчиках через LoRaWAN // Constr Robot. 2021. № 5. P. 87–100.*

6. ***Construction*** *with digital twin information systems / R. Sacks, I. Brilakis, E. Pikas [et al.]// Data-Centric Engineering. 2020. Vol. 1. E14.*

7. ***Koseleva N., Ropaite G.*** *Big Data in Building Energy Efficiency: Understanding of Big Data and Main Challenges // Proced. Eng. 2017. № 172. P. 544–549.*

8. ***Evaluation*** *of productivity virtualization technologies of switching equipment telecommunications networks / O. I. Romanov, M. M. Nesterenko, N. O. Fesokha, V. B. Mankivskyi // Information and Telecommunication Sciences, 2020. Vol. 11, №1 (20). P. 53 – 58.*

9. ***Li Y., Li W., Jiang C.*** *A Survey of Virtual Machine System: Current Technology and Future Trends. // 2010 Third International Symposium on Electronic Commerce and Security, Nanchang, China, 2010. P. 332–336.*

10. ***Зайченко Ю., Зайченко О., Хамідов Г.*** *Оптимізація структури мереж нового покоління // 2017 10-й Міжнародний конгрес з обробки зображень та сигналів, біомедичної інженерії та інформатики (CISP-BMEI), Шанхай, Китай, 2017. С. 1–5,*

V. O. Vlasenko, Yu. V. Shchavinskyi, M. M. Zaporozhchenko, V. S. Tyshchenko

ANALYSIS OF DATA TRANSMISSION NETWORK CONSTRUCTION TECHNOLOGIES WITH HIGH REQUIREMENTS FOR INFORMATION SECURITY, RELIABILITY, AND LATENCY

The scientific article is dedicated to the analysis of contemporary approaches and technologies in the construction of data transmission networks aimed at ensuring information security, reliability, and minimal latency. The necessity of comprehensively considering factors influencing network efficiency with a focus on reliability and security is substantiated. Network analysis enables the creation of an infrastructure that meets the demands of the modern information environment, comprehensively weighing the advantages and disadvantages of each network technology during construction. For the mathematical evaluation of data transmission network reliability, a Markov model is proposed, which is based on Markov processes theory. Developed using the Python programming language and relevant libraries, the model allows for a quantitative assessment of data transmission network reliability, considering various failure factors, state transitions, and recovery. The model facilitates forecasting network states and planning preventive organizational and technical measures to ensure reliability and security, in light of the constantly increasing demands for service quality and confidential information protection. An analysis of transmission delay methods has revealed a correlation between the transmission speed and volume of information with various factors, such as bandwidth, network load, connection type and speed, and data processing by network nodes. The research underscores the need to choose specific methods based on the network's characteristics and its intended tasks. Based on the analysis results, to construct efficient networks that meet information security, reliability, and transmission delay requirements, there is a recognized need for comprehensive development of evaluation systems and the creation of a unified evaluation model.

Keywords: information security; data transmission network; reliability; latency; network modeling; evaluation models; Markov models.