Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломного проекту (роботи)

магістр
(освітній рівень)

на тему: *«Аналіз відомих методів забезпечення безпеки та достовірності даних в інформаційних системах»*

Виконав: студент (ка) *VI* курсу, групи *СБм-61*
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
Лазорко А.І.
підпис (прізвище та ініціали)

Керівник *Муж В.В.*
підпис (прізвище та ініціали)

Нормоконтроль *Кареліна О.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 20*19*

АНОТАЦІЯ

Аналіз відомих методів забезпечення безпеки та достовірності даних в інформаційних системах // Дипломна робота ОР «Магістр» // Лазорко Андрій Іванович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2019 // С. 114, рис. – 29, табл. – 8 , кресл. – , додат. – .

Ключові слова: БЕЗПЕКА, ДОСТОВІРНІСТЬ, НАДІЙНІСТЬ, КАНАЛИ З ПАМ`ЯТТЮ, КАНАЛИ БЕЗ ПАМ`ЯТІ, КАНАЛЬНИЙ ПРОТОКОЛ, FRAME RELAY, X.25, ЗВОРОТНІЙ ЗВ'ЯЗОК

Дана магістерська кваліфікаційна робота присвячена дослідженню відомих методів забезпечення безпеки та достовірності даних в інформаційних системах. Для проведення дослідження було введено узагальнений показник ефективності комп'ютерної мережі (Wi). При цьому були досліджені залежності коефіцієнта готовності від довжини кадру, часу доставки кадру при різних можливостях помилки в каналі передачі з використанням асимметричних і симетричних алгоритмов шифрування. Для дослідження були використані різні стратегії управління обміном даних.

В результаті дослідження було виявлено, що на коефіцієнт готовності істотно впливає довжина кадру (оперативність), час шифрування і розшифрування (безпека), ймовірність помилки (надійність). Розроблено стратегії функціонування комп'ютерної мережі для каналів з пам'яттю та без пам’яті.

У першому розділі проведено аналіз умов функціонування та обґрунтування вимог, що пред'являються до сучасних комп'ютерних систем та мереж

У другому розділі проведено аналіз відомих методів забезпечення безпеки та достовірності інформації в комп`ютерних системах та мережах.

Третій розділ – експериментальний. У ньому проведено оцінку показника функціональної ефективності комп'ютерної мережі на основі протоколу Frame Relay

В спеціальній частині описано базові речі про симетричну та асиметричну криптографію.

В п’ятому розділі обчислено основні показники економічної ефективності від розробки і реалізації запропонованого алгоритму.

У підрозділі "Охорона праці" розглянуто забезпечення безпечних і не шкідливих умов праці У підрозділі "Безпека життєдіяльності" описано вплив факторів виробничого середовища та електромагнітного випромінювання на життєдіяльність людини.

В розділі "Екологія" висвітлено статистичні показники екологічних явищ та описано моніторинг довкілля.

ANNOTATION

Research of threats identification methods in a wireless network environment // Thesis of the Master degree // Lazorko Andrii // Ternopil Ivan Puluj National Technical University, Department of Computer Information Systems and Software Engineering, Department of Cybersecurity // Ternopil, 2019 // P. 114, Tables – 8 , Fig. – 29 , Diagrams – , Annexes. – , References – .

Keywords: SAFETY, ACCURACY, RELIABILITY, MEMORY CHANNELS, MEMORYLESS CHANNELS, CHANNEL PROTOCOL, FRAME RELAY, X.25, FEEDBACK

This master's qualification thesis is devoted to the study of known methods of data security and reliability in information systems. For the study, a generalized measure of the performance of a computer network (Wi) was introduced. The dependencies of the readiness factor on the frame length, the frame delivery time at different error possibilities in the transmission channel were investigated using asymmetric and symmetric encryption algorithms. Different data sharing management strategies were used for the study.As a result of the study, it was found that the readiness factor is significantly affected by the frame length (operability), encryption and decryption time (security), error probability (reliability). Computer network strategies for memory and non-memory channels have been developed.

The first section analyzes the conditions of operation and justification of the requirements for modern computer systems and networks.

The second section analyzes the known methods of ensuring the security and reliability of information in computer systems and networks.

The third section is experimental. It assesses the performance of a computer network based on the Frame Relay protocol.

The special section describes basic things about symmetric and asymmetric cryptography.

The fifth section calculates the main cost-effectiveness indicators for developing and implementing the proposed algorithm.

The section "Occupational safety" considers the provision of safe and non-hazardous working conditions The section "Safety of life" describes the influence of factors of the production environment and electromagnetic radiation on human life.

The "Ecology" section covers statistical indicators of environmental phenomena and describes environmental monitoring.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ОС	Операційна система
ЛОМ	Локальна обчислюальна мережа
ГОМ	Глобальна обчислювальна мережа
PVC	Permanent *Virtual* Circuit
QoS	Quality of Service,
WAN	Wide Area Network
ATM	Asynchronous Transfer Mode

ВСТУП

На сьогоднішній день у світі існує велика кількість комп'ютерів, які об'єднані в різноманітні інформаційно-обчислювальні мережі. Тенденція до об'єднання комп'ютерів у мережі обумовлена поруч важливих причин, таких як прискорення передачі інформаційних повідомлень, можливість швидкого обміну інформацією між користувачами, одержання і передача повідомлень, не відходячи від робочого місця, можливість миттєвого одержання будь-якої інформації з будь-якої точки земної кулі та інші.

Взаємодія між комп'ютерами мережі відбувається за рахунок передачі повідомлень через мережеві адаптери і канали зв'язку. Особливості та обмеження, пов'язані з передачею даних, часто є принциповими і впливають на концепції побудови обчислювальних мереж [11].

Тема «Аналіз відомих методів забезпечення безпеки та достовірності даних в інформаційних системах» є дуже *актуальною*. Так як в наш час обчислювальні можливості дозволяють користувачам локальних і глобальних систем обчислень збільшити на два, або три порядки обсяги даних, що надходять, а також нові послуги, що надаються користувачам комп'ютерних мереж. І тому збільшення обсягів даних в критичних системах локальної обчислювальної мережі (ЛОМ), глобальної обчислювальної мережі (ГОМ) висуває нові вимоги до забезпечення надійності і продуктивності комп'ютерних систем, безпеки та достовірності переданих і оброблюваних даних. Останнім часом не всі сучасні криптографічні засоби захисту інформації забезпечують своєчасну обробку величезних обсягів даних (десятки-сотні Мбіт/с) і задовольняють жорстким вимогам по достовірності та безпеки інформації [11, 12].

Метою магістерської роботи є аналіз відомих методів забезпечення безпеки та достовірності інформації в комп`ютерних системах та мережах на основі каналів з пам`яттю та без пам`яті. Виявлення найліпшого протоколу, який

забезпечує максимальну оцінку ефективності обміну даними в комп`ютерній мережі при різних засобах управління обміном.

Об'єктом дослідження є процес аналізу відомих протоколів забезпечення безпеки та достовірності обміну даними.

Предмет – способи управління обміном, які дозволяють оцінити значення показника ефективності обміну даними в комп'ютерній мережі.

Для досягнення поставленої мети необхідно врахувати всі можливі дії, які необхідні у результаті проведення дослідження. Тому потрібно виділити основні *задачі*:

а) аналіз умов функціонування та обґрунтування вимог, що ставляться до сучасних комп'ютерних систем та мереж;

б) аналіз протоколів канального рівня глобальної обчислювальної мережі;

в) оцінка ефективності обміну даними в комп'ютерній мережі при різних засобах управління обміном.

Наукова новизна. В роботі запропоновано метод оцінки ефективності функціонування комп’ютерної мережі та метод прийняття рішень для вибору оптимальної стратегії функціонування комп'ютерної мережі.

Практичне значення роботи. Показник функціональної ефективності мережі досліджено в каналах з пам'яттю та без пам'яті.

Для проведення дослідження були використані програмний пакет Mathcad 15 та редактор Microsoft Office Visio 2007.

Виходячи з цього можна зробити висновок, що проведення даного аналізу допоможе виявити найліпший протокол, який забезпечує безпеку та достовірність переданої та оброблюваної інформації в комп`ютерних системах та мережах на основі каналів з пам`яттю та без пам`яті.

Апробація результатів роботи. Окремі результати роботи доповідались на VII науково-технічній конференції «Інформаційні моделі, системи та технології», Тернопіль, ТНТУ, 11 – 12 грудня 2019 р.

1 АНАЛІЗ ПРОБЛЕМАТИКИ ТА ПОСТАНОВКА ЗАВДАНЬ ДОСЛІДЖЕННЯ «АНАЛІЗ ВІДОМИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В КОМП`ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ НА ОСНОВІ КАНАЛІВ З ПАМ`ЯТТЮ ТА БЕЗ ПАМ`ЯТІ»

1.1. Опис проблем предметної області дослідження та обґрунтування актуальності дослідження наукової задачі

В наш час обчислювальні можливості дозволяють користувачам локальних і глобальних систем обчислень збільшити на два, або три порядки обсяги даних, що надходять, а також нові послуги, що надаються користувачам комп'ютерних мереж. І тому збільшення оброблюваних обсягів даних в критичних системах локальної обчислювальної мережі (ЛОМ), глобальної обчислювальної мережі (ГОМ) висуває нові вимоги до забезпечення надійності і продуктивності комп'ютерних систем, безпеки та достовірності переданих і оброблюваних даних [11].

Для початку в дослідницькій роботі розглянемо типи обчислювальної мережі. Взаємодія між комп'ютерами мережі відбувається за рахунок передачі повідомлень через мережеві адаптери і канали зв'язку. Особливості та обмеження, пов'язані з передачею даних, часто є принциповими і впливають на концепції побудови ОМ. Залежно від територіальної протяжності ОМ ділять на локальні (ЛОМ) та глобальні (ГОМ) [11, 24].

Локальні обчислювальні мережі, ЛОМ (Local Area Network, LAN) – це об'єднання комп'ютерів, зосереджених на невеликій території, зазвичай в радіусі не більше 1 – 2 км, хоча в окремих випадках локальна мережа може мати і великі розміри, наприклад, кілька десятків кілометрів. У загальному випадку локальна мережа являє собою комунікаційну систему, що належить одній організації [24].

На рис. 1.1. наведена локальна обчислювальна мережа.

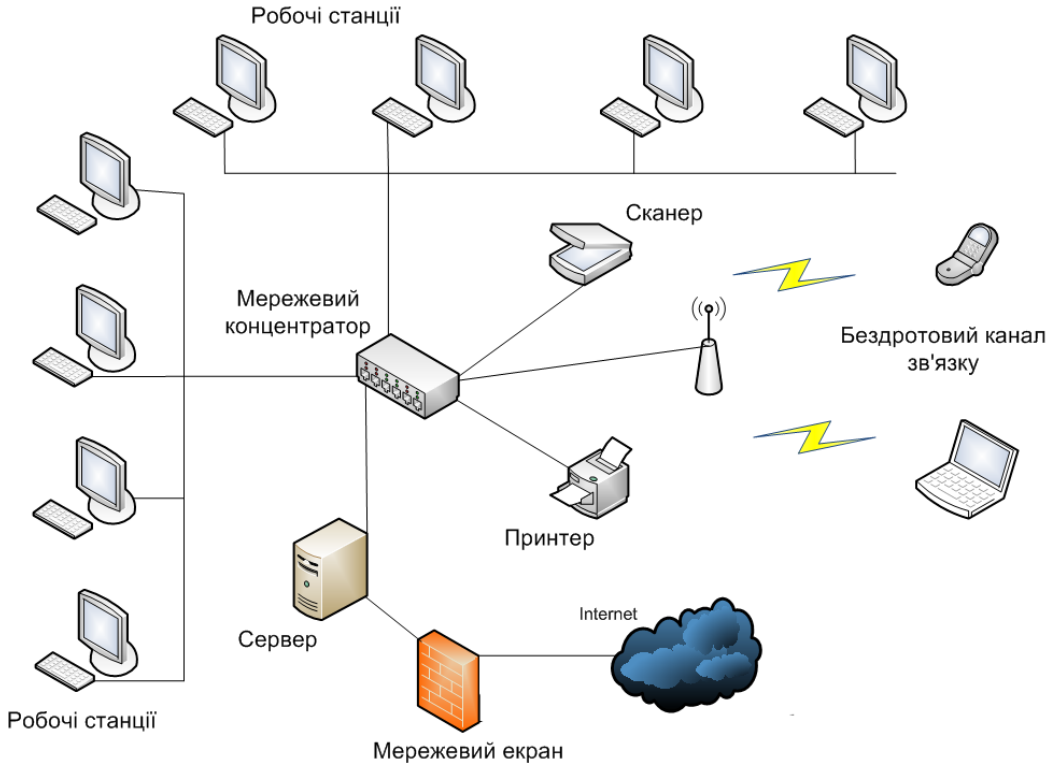

Рисунок 1.1 - Локальна обчислювальна мережа

У локальних мережах, використовується розділювальна середа передачі даних (моноканал) і основна роль відводиться протоколам фізичного і канального рівнів, оскільки ці рівні найбільшою мірою відображають специфіку локальних мереж.

Основними відмінними ознаками локальних обчислювальних мереж є:

а) висока швидкість передачі інформації, велика пропускна здатність мережі, прийнятна швидкість – не менш 10 Мбіт/с;

б) низький рівень помилок передачі (або, що теж саме, високоякісні канали зв'язку, припустима ймовірність помилок передачі даних повинна бути порядку $10^{-8} – 10^{-12}$;

в) ефективний, швидкодіючий механізм керування обміном по мережі;

г) заздалегідь чітко обмежена кількість комп'ютерів, що підключаються до мережі [22, 24].

Другий тип обчислювальних мереж – глобальна обчислювальна мережа, ГОМ (Wide Area Network, WAN). Вона служить, щоб надавати свої сервіси великій кількості кінцевих абонентів, розкиданих по великій території, наприклад, в межах області, регіону, країни, континенту або земної кулі [24].

Сьогодні вибір технологій глобальної мережі став набагато ширше, крім мереж X.25 він включає такі технології, як frame relay, SMDS і ATM. Крім цих технологій, розроблених спеціально для глобальних комп'ютерних мереж, можна користуватися послугами територіальних мереж TCP/IP, які доступні сьогодні як у вигляді недорогої і дуже поширеної мережі Internet, якість транспортних послуг якої поки практично не регламентується і залишає бажати кращого, так і у вигляді комерційних глобальних мереж TCP/IP, які ізольовані від Internet і надаються в оренду телекомунікаційними компаніями [21, 22].

Схема глобальної обчислювальної мережі наведена на рис. 1.2.

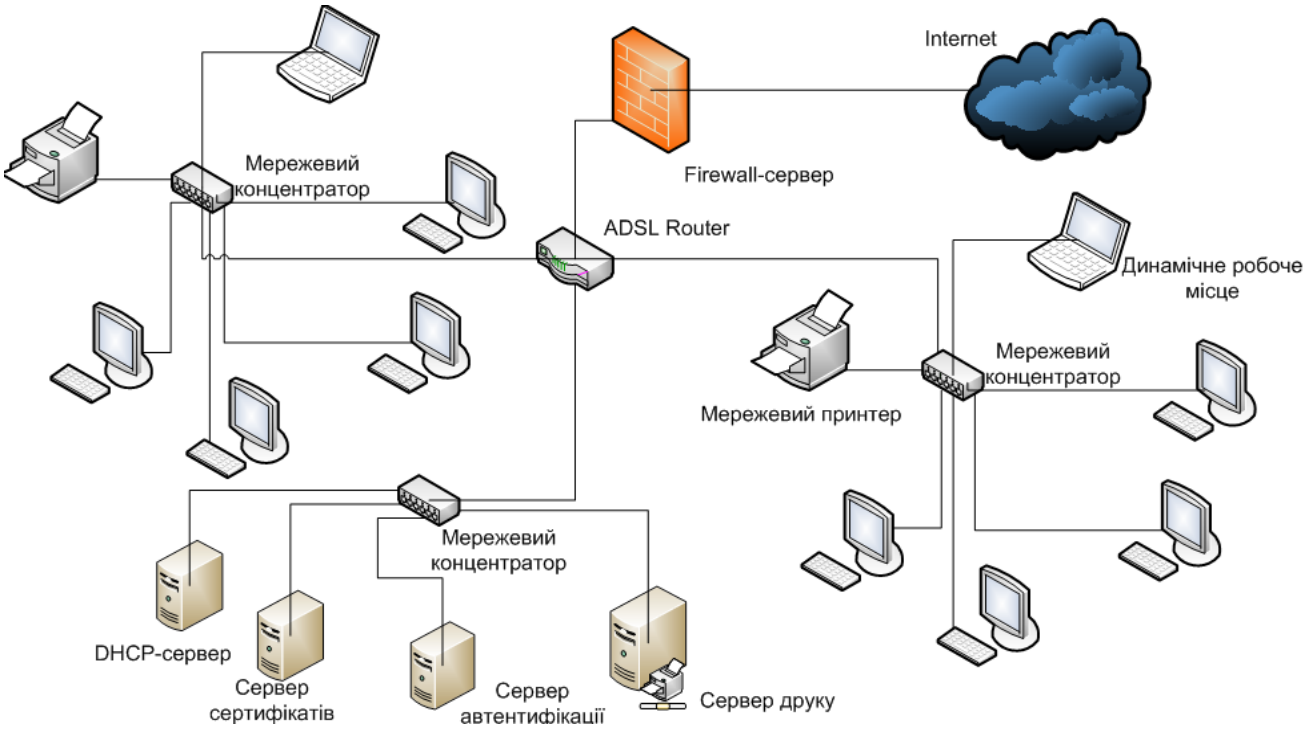

Рисунок 1.2 - Глобальна обчислювальна мережа

Мережна модель OSI містить в собі канальний рівень, який призначений для передачі даних вузлам, що знаходяться в тому ж сегменті локальної мережі. Даний рівень може використовуватися для виявлення і, можливо, виправлення помилок, що виникли на фізичному рівні [24, 29].

Канальний рівень відповідає за доставку кадрів між пристроями, підключеними до одного мережевого сегменту. Кадри канального рівня не перетинають кордонів мережевого сегменту. Функції міжмережевої маршрутизації і глобальної адресації здійснюються на більш високих рівнях моделі OSI, що дозволяє протоколам канального рівня зосередитися на локальній доставці і адресації [33].

Прикладами протоколів канального рівня для локальних мереж є протоколи Token Ring, Ethernet, Fast Ethernet, 100VG-AnyLAN, FDDI.

У локальних мережах канальний рівень розділяється на два підрівня:

а) рівень управління логічним каналом (logical link control, LLC);

б) рівень доступу до середовища (media access layer, MAC).

Рівень LLC відповідає за достовірну передачу кадрів даних між вузлами, а також реалізує функції інтерфейсу з прилеглим до нього мережним рівнем. MAC-рівень лежить нижче LLC-рівня і виконує функції забезпечення доступу до поділюваного між вузлами мережі загального середовища передачі даних. Стандартні протоколи канального рівня часто розрізняються реалізацією методу доступу до середовища, в той час як функції LLC-рівня значно менше варіюються від одного стандарту до іншого [33, 34].

У глобальних мережах, які рідко володіють регулярною топологією, канальний рівень забезпечує обмін повідомленнями між двома сусідніми комп'ютерами, сполученими індивідуальною лінією зв'язку. До таких протоколів типу "точка-точка" відносяться протоколи PPP, SLIP, LAP-B, LAP-D. Ці протоколи не використовують підрівня доступу до середовища, але вимагають наявності процедур управління потоком кадрів, так як проміжні комутатори можуть переповнитися при занадто високій інтенсивності трафіку за деякими індивідуальними каналами. Крім того, через високий ступінь зашумленості

глобальних каналів зв'язку в протоколах цих мереж широко використовуються методи передачі даних з попереднім встановленням з'єднання і повторними передачами кадрів при їх спотвореннях і втратах [37].

Канальний рівень оперує одиницями даних званими кадрами (frame). У загальному випадку кожен протокол канального рівня має свій особливий формат кадру.

Класифікація типів мереж та стандартів зв`язку наведена на рис. 1.3.

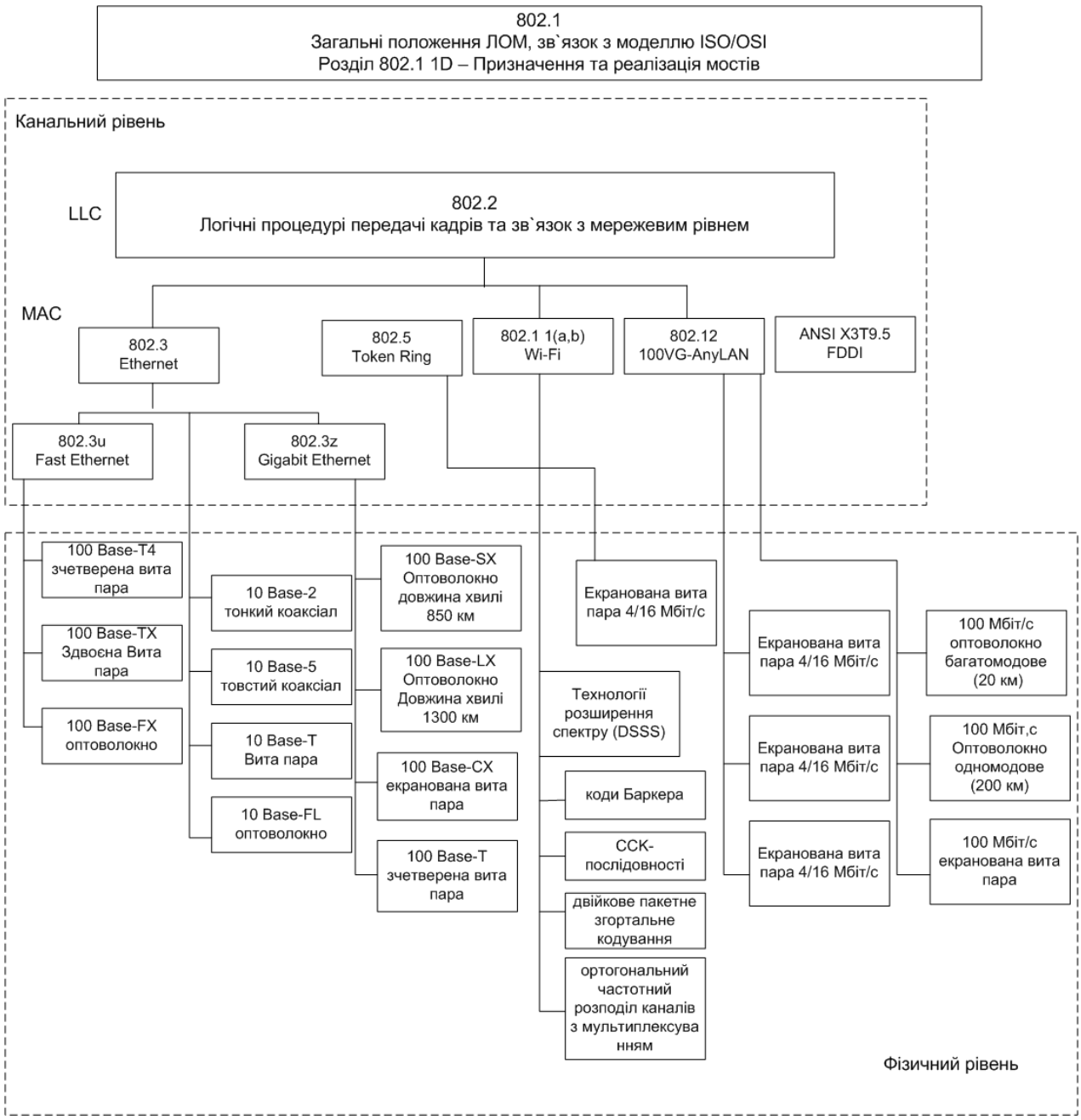

Рисунок 1.3 - Загальна класифікація типів мереж та стандартів зв`язку

Типовими абонентами глобальної комп'ютерної мережі є локальні мережі підприємств, розташовані в різних містах і країнах, яким потрібно обмінюватися даними між собою. Послугами глобальних мереж користуються також і окремі комп'ютери [34].

Мережа повинна передавати дані абонентів будь-яких типів, які є на підприємстві і потребують віддаленому обміні інформацією. Для цього глобальна мережа повинна надавати комплекс послуг:

а) передача пакетів локальних мереж;

б) передача пакетів міні-комп'ютерів і мейнфреймів;

в) обмін факсами;

г) передача трафіку офісних АТС;

д) вихід в міські, міжміські та міжнародні телефонні мережі;

е) обмін відеозображеннями для організації відеоконференцій;

є) передача трафіку касових апаратів, банкоматів і т. д.

Основні типи потенційних споживачів послуг глобальної комп'ютерної мережі наведені на (рис. 1.4.)

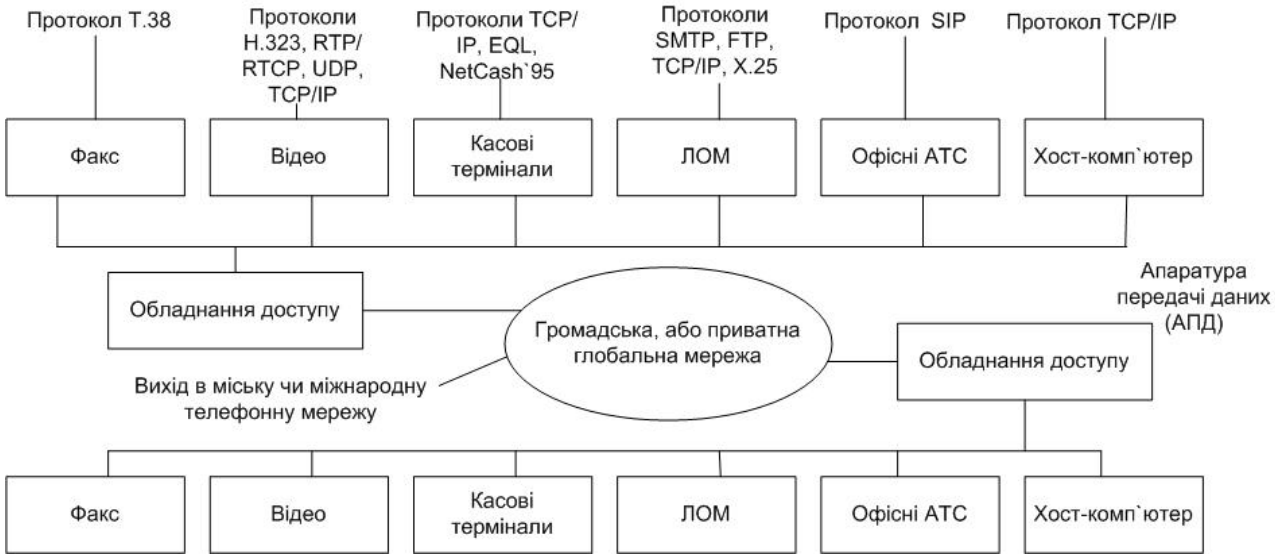

Рисунок 1.4 - Абоненти глобальної мережі

Передача даних відбувається за допомогою різних протоколів:

а) По факсу інформація передається за допомогою протоколу T.38. Це стандарт Міжнародного союзу електрозв'язку з передачі факсимільних повідомлень в реальному часі через IP мережі.

б) Відео передається по протоколам H.323, RTP/RTCP, UDP, TCP/IP.

в) Касові термінали реалізуються на протоколах EQL, TCP/IP, NetCash`95.

г) У локальній обчислювальній мережі інформація передається за допомогою протоколів SMTP, TCP/IP, FTP, X.25 і т.д.

д) Офісні АТС працюють на протоколах SIP.

е) Передача даних на хост-комп`ютерах відбувається через протокол TCP/IP.

На сьогоднішній день прийнято розрізняти наступні типи глобальних мереж:

а) виділення каналів (використовується при побудові відповідальних магістралей між великими мережами, гарантує пропускну спроможність виділеного каналу);

б) комутація каналів (це аналогові телефонні мережі, зокрема ISDN. В їх основі лежить ідея використання цифрової бітової шини між клієнтом та оператором мережі);

в) комутація пакетів (це мережі TCP/IP, FRAME Relay, ATM, X.25) [3, 4].

У результаті можна виявити деякі відмінності локальних та глобальних обчислювальних мереж:

а) протяжність, якість і спосіб прокладки ліній зв'язку;

б) складність методів передачі і обладнання;

в) швидкість обміну даними;

г) різноманітність послуг;

д) оперативність виконання запитів;

е) поділ каналів;

є) масштабованість.

У відповідності по закону Мура необхідно враховувати усі зміни, які відбуваються, для того, щоб побудувати локальну або глобальну мережу. Тому що

по закону Мура основні характеристики комп`ютерів покращуються у два рази кожні два роки. Він висловив припущення, що кількість транзисторів на кристалі мікросхеми буде подвоюватися кожні 24 місяці [34, 50].

Створивши графік зростання продуктивності запам'ятовуючих мікросхем, він виявив закономірність: нові моделі мікросхем розроблялися через більш-менш однакові періоди (18 – 24 міс.) після появи їхніх попередників. При цьому їхня місткість зростала щоразу приблизно вдвічі. Якщо така тенденція продовжиться, то потужність обчислювальних пристроїв експоненціально зросте протягом відносно короткого проміжку часу. Закон Мура наведений на рис. 1.5.

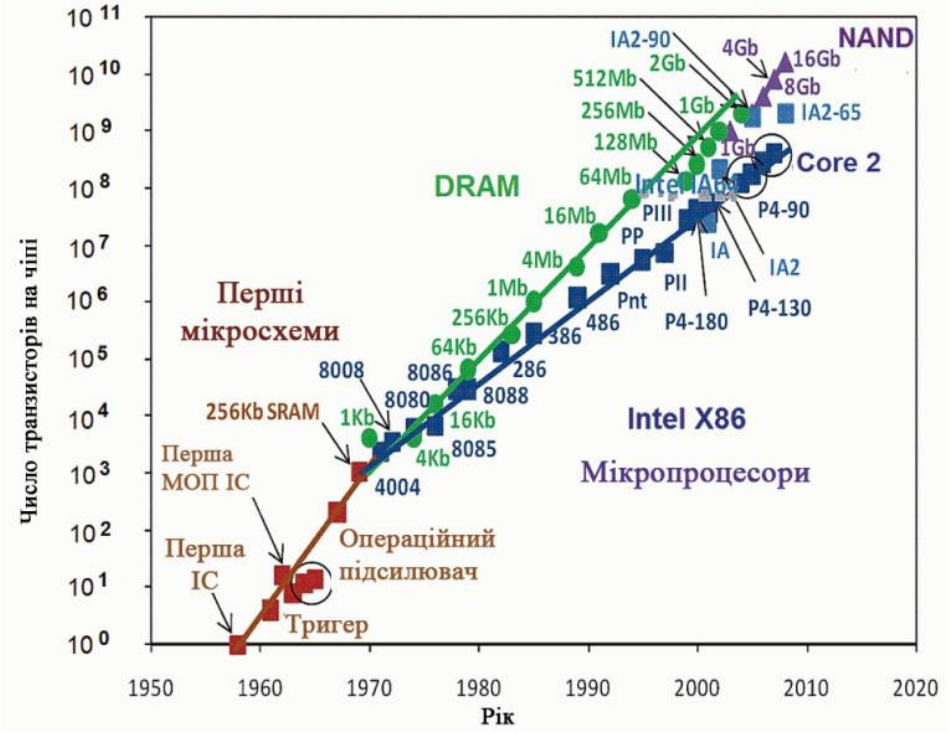

Рисунок 1.5 - Закон Мура - експоненційне збільшення з часом числа транзисторів на одному кристалі

Комп`ютерні мережі невпинно зростають. Збільшуються обсяги оброблюваних даних у сучасних комп'ютерних системах і мережах, виникають нові форми і способи обробки інформації, стрімко розвивається обчислювальна техніка і т.д. Все це висуває підвищені вимоги до криптографічних засобів захисту інформації, а також нові вимоги до забезпечення надійності та продуктивності комп`ютерних систем [24].

Тому метою даного дослідження є аналіз відомих методів забезпечення безпеки та достовірності інформації в комп`ютерних системах та мережах на основі каналів з пам`яттю та без пам`яті. Та виявлення найліпшого протоколу, який забезпечує максимальну оцінку ефективності обміну даними в комп`ютерній мережі при різних засобах управління обміном.

1.2. Аналіз умов функціонування та обґрунтування вимог, що пред'являються до сучасних комп'ютерних систем та мереж

Аналіз умов функціонування локальних та глобальних обчислювальних мереж (ЛОМ, ГОМ) показує, що головною вимогою, що ставляться до них, є забезпечення користувачам потенційної можливості доступу до ресурсів всіх комп'ютерів, об'єднаних в мережу [33].

До основних вимог функціонування ГОМ відносяться: продуктивність, надійність, сумісність, керованість, захищеність, розширюваність і масштабованість. Основні вимоги та їх складові наведені на рис. 1.6.

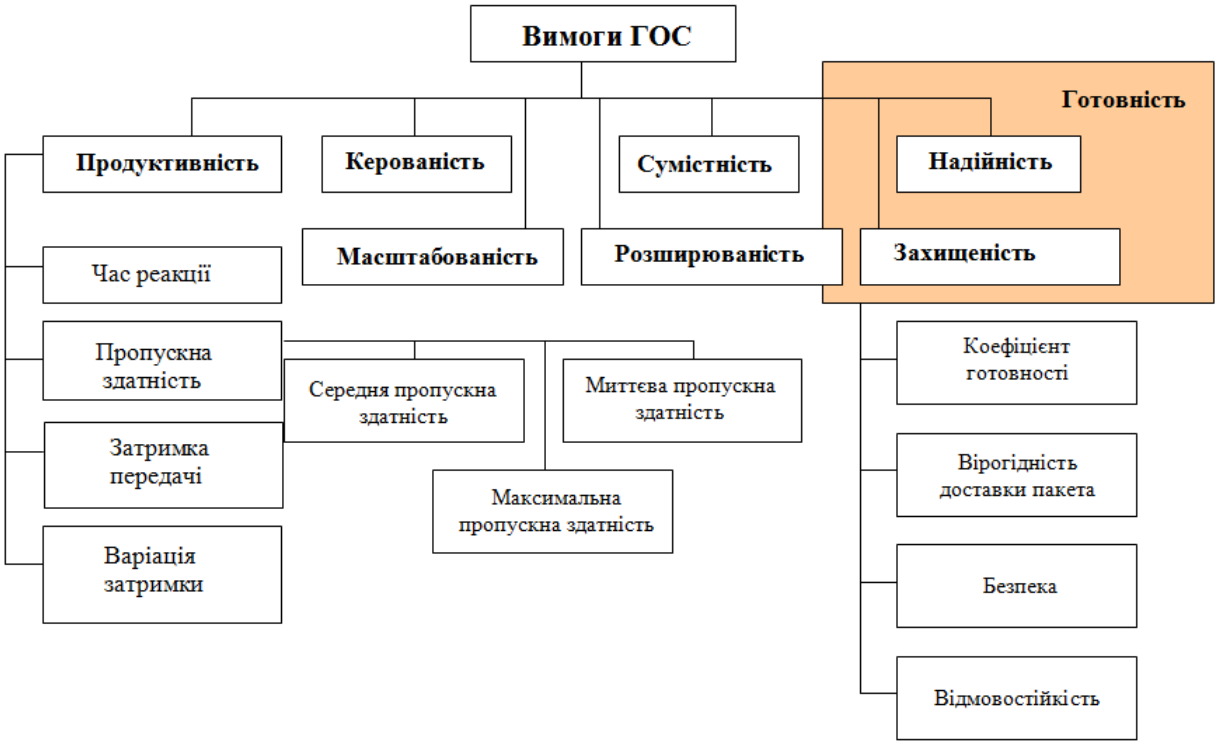

Рисунок 1.6 - Вимоги, які висуваються до обчислювальних мереж та систем

На даний час для оцінки функціонування ЛОМ та ГОМ запроваджено поняття "якість обслуговування" (Quality of Service, QoS) комп'ютерної мережі, що включає тільки дві найважливіші характеристики мережі – продуктивність і надійність. Проведений аналіз показника якості обслуговування мережі визначає два підходи для його забезпечення. Перший підхід полягає у гарантованому забезпеченні користувачеві дотримання деякої числової величини показника якості обслуговування (забезпечення встановленого показника середньої пропускної здатності, показника часу затримки передачі і т.д.). Так, технології Frame Relay та ATM дозволяють будувати мережі, що гарантують якість обслуговування по продуктивності (показники середньої пропускної здатності, часу реакції, часу затримки та інші) [27, 33].

Другий підхід полягає у пріоритетному обслуговуванні користувачів у відповідності із встановленою ієрархією мережі. Таким чином, якість обслуговування залежить від ступеня привілейованості користувача чи групи користувачів, до якої він належить. Для уповноважених користувачів ГОМ якість обслуговування не гарантується, а гарантується тільки рівень їх привілеїв. Таке обслуговування називається обслуговуванням best effort – з найбільшим старанням. Проведений аналіз функціонування локальних мереж показує, що за таким принципом працюють ЛОМ, побудовані на комутаторах з пріоритезацією кадрів [27, 33].

Для забезпечення необхідного показника якості обслуговування ГОМ необхідно забезпечити продуктивність та надійність. Основними характеристиками продуктивності є: час реакції, пропускна здатність, затримка передачі і її варіація.

Час реакції є інтегральною характеристикою продуктивності мережі і визначається як інтервал часу між виникненням запиту користувача до якої-небудь мережевої служби і отриманням відповіді на цей запит [27].

Проведений аналіз даного показника засвідчує, що його значення залежить тільки від типу служби, до якої звертається користувач, статусу користувача в

мережі, типу сервера, а також від поточного стану елементів ГОМ – завантаженості сегментів, комутаторів і маршрутизаторів, через які проходить запит, завантаженості сервера і т. п.

Час реакції мережі підрозділяється на час підготовки запитів на клієнтському комп'ютері, час передачі запитів між клієнтом і сервером через комунікаційне обладнання, час обробки запитів на сервері, час передачі відповідей від сервера клієнту і час обробки одержуваних від сервера відповідей на клієнтському комп'ютері [27].

Для визначення обсягу переданих даних за одиницю часу використовується пропускна здатність і її похідні (миттєва, максимальна і середня пропускні спроможності).

Аналіз функціонування ГОМ показує, що для проектування, налаштування і оптимізації використовуються такі показники, як середня і максимальна пропускні здатності. Для визначення якості мережі в цілому, не диференціюючи його по окремих сегментах або пристроях, використовується загальна пропускна здатність мережі, яка визначається як середня кількість інформації, переданої між всіма вузлами мережі в одиницю часу. Для визначення якості мережі також використовують кількісний показник максимальної затримки передачі і її варіації. Затримка передачі визначається як час знаходження пакета в якомусь мережевому пристрої або частини мережі. Цей параметр продуктивності за змістом близький до часу реакції мережі, але відрізняється тим, що завжди характеризує тільки мережеві етапи обробки даних, без затримок обробки комп'ютерами ЛОМ [33, 34].

Найважливішою характеристикою обчислювальної мережі є надійність – здатність правильно функціонувати протягом тривалого періоду часу. Ця властивість має три складові:

а) коефіцієнт готовності означає частку часу, протягом якого система може бути використана;

б) безпека, тобто здатність системи захистити дані від несанкціонованого доступу;

в) відмовостійкість, здатність системи приховати від користувача відмову окремих її елементів. У відмовостійкої системі відмова одного з її елементів приводить до деякого зниження якості її роботи, а не до повної зупинки.

Для опису передачі пакетів між кінцевими вузлами використовуються імовірнісні характеристики каналу зв'язку: імовірність доставки пакету вузлу призначення без спотворень, імовірність втрати пакету (по кожному з причин - переповнення буфера маршрутизатора, через розбіжність контрольної суми, через відсутність працездатного шляху до вузла призначення і т. д.), імовірність спотворення окремого біта переданих даних [33].

Розглянемо більше детально показник готовності, тому що він є найважливішим показником загальної надійності мережі.

Підвищення готовності припускає зниження в певних межах впливу відмов і збоїв на роботу системи за допомогою засобів контролю та корекції помилок, а також засобів автоматичного відновлення циркуляції інформації в мережі після виявлення несправності. Підвищення готовності являє собою боротьбу за зниження часу простою системи [37].

При цьому критерієм оцінки готовності є коефіцієнт готовності, який дорівнює частці часу перебування системи в працездатному стані і може інтерпретуватися як вірогідність знаходження системи в працездатному стані. Коефіцієнт готовності обчислюється як відношення середнього часу наробітку на відмову до суми цієї ж величини і середнього часу відновлення.

$$K_{\Gamma} = t_p \Big/ \left(t_p + t_{\Pi}\right) \quad , \tag{1.1}$$

де t_p – середній час наробітку на відмову,

t_{Π} – середній час відновлення.

Системи з високою готовністю називають також відмовостійкими.

Основним способом підвищення готовності є надмірність, на основі якої реалізуються різні варіанти відмовостійких архітектур. Обчислювальні мережі включають велику кількість елементів різних типів, і для забезпечення відмовостійкості необхідна надмірність по кожному з ключових елементів мережі. Якщо розглядати мережу тільки як транспортну систему, то надмірність повинна існувати для всіх магістральних маршрутів мережі, тобто маршрутів, які є загальними для великої кількості клієнтів мережі. Такими маршрутами зазвичай є маршрути до корпоративних серверів – серверів баз даних, Web-серверам, поштових серверів і т.п. Тому для організації відмовостійкої роботи всі елементи мережі, через які проходять такі маршрути, повинні бути зарезервовані: повинні матися резервні кабельні зв'язки, якими можна скористатися при відмові одного з основних кабелів, всі комунікаційні пристрої на магістральних шляхах повинні або самі бути реалізовані за відмовостійкою схемою з резервуванням всіх основних своїх компонентів, або для кожного комунікаційного пристрою повинно матися резервний аналогічний пристрій [33, 34].

Перехід з основного зв'язку на резервний або з основного пристрою на резервний може відбуватися як в автоматичному режимі, так і вручну. Автоматичний перехід підвищує коефіцієнт готовності системи, так як час простою мережі в цьому випадку буде істотно менше, ніж при втручанні людини.

Високий ступінь готовності мережі можна забезпечити у тому випадку, коли процедури тестування працездатності елементів мережі і переходу на резервні елементи вбудовані в комунікаційні протоколи. Прикладом такого типу протоколів може служити протокол FDDI, в якому постійно тестуються фізичні зв'язки між вузлами і концентраторами мережі, а в разі їх відмови виконується автоматична реконфігурація зв'язків за рахунок вторинного резервного кільця [34].

Існують різні градації відмовостійких комп'ютерних систем, до яких відносяться і обчислювальні мережі:

а) висока готовність – характеризує системи, виконані по звичайній комп'ютерній технології, що використовують надлишкові апаратні і програмні засоби і допускають час відновлення в інтервалі від 2 до 20 хвилин;

б) стійкість до відмов – характеристика таких систем, яка має в гарячому резерві надмірну апаратуру для всіх функціональних блоків, включаючи процесори, джерела живлення, підсистеми вводу/виводу, підсистеми дискової пам'яті, причому час відновлення при відмові не перевищує однієї секунди;

в) безперервна готовність – це властивість систем, яка також забезпечує час відновлення в межах однієї секунди, але на відміну від систем стійких до відмов, системи безперервної готовності усувають не тільки простої, що виникли в результаті відмов, але і планові простої, пов'язані з модернізацією або обслуговуванням системи. Всі ці роботи проводяться в режимі online [34]. Додатковою вимогою до систем безперервної готовності є відсутність деградації, тобто система повинна підтримувати постійний рівень функціональних можливостей і продуктивності незалежно від виникнення відмов.

Так як мережі обслуговують одночасно велику кількість користувачів, то при розрахунку коефіцієнта готовності необхідно враховувати цю обставину. Коефіцієнт готовності мережі повинен відповідати частці часу, протягом якого мережа виконувала з належною якістю свої функції для всіх користувачів. Очевидно, що у великих мережах дуже важко забезпечити значення коефіцієнта готовності, близьких до одиниці.

Між показниками продуктивності і надійності мережі існує тісний зв'язок. Ненадійна робота мережі дуже часто призводить до істотного зниження її продуктивності. Це пояснюється тим, що збої і відмови каналів зв'язку і комунікаційного устаткування приводять до втрати чи руйнуванню деякої частини пакетів, в результаті чого комунікаційні протоколи вимушені організовувати повторну передачу загублених даних [33, 34].

1.3. Висновки до розділу 1

У даному розділі був проведений аналіз локальних та глобальних обчислювальних мереж, розглядався канальний рівень мережевої моделі OSI для ЛОМ та ГОМ, був наведений закон Мура, який свідчить про те, що характеристики комп'ютерів покращуються у два рази кожні два роки. А також був проведений аналіз умов функціонування та обґрунтування вимог, що висуваються до сучасних комп'ютерних систем та мереж.

2 ТЕОРЕТИЧНЕ ТА МЕТОДИЧНЕ ДОСЛІДЖЕННЯ ВИРІШЕННЯ ЗАДАЧІ «АНАЛІЗ ВІДОМИХ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В КОМП`ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ НА ОСНОВІ КАНАЛІВ З ПАМ`ЯТТЮ ТА БЕЗ ПАМ`ЯТІ»

2.1. Аналіз протоколів канального рівня глобальної обчислювальної мережі

У глобальних обчислювальних мережах канальний рівень забезпечує обмін повідомленнями між двома сусідніми комп'ютерами, які об`єднані індивідуальною лінією зв'язку. Найвідомішими протоколами канального рівня ГОМ є мережі X.25, Frame Relay, ATM. Вони дозволяють забезпечити контроль помилок в кожному каналі окремо, або на кінцевих вузлах. Розглянемо кожний з цих протоколів.

Протокол ATM є технологією передачі комірок або трансляції комірок. Це технологія асинхронного режиму передачі (Asynchronous Transfer Mode, ATM), яка є однією з перспективних технологій побудови високошвидкісних мереж (від локальних до глобальних). Взагалі, ATM – це комунікаційна технологія, яка об'єднує принципи комутації пакетів і каналів для передачі інформації різного типу [13].

Технологія ATM розроблялася для передачі всіх видів трафіку в локальних і глобальних мережах, тобто передачі різнорідного трафіку (цифрових, голосових і мультимедійних даних) по одним і тим же системам і лініях зв'язку. Швидкість передачі даних в магістралях ATM складає 155 Мбіт/с – 2488 Мбіт/с. На рис. 2.1 наведена структурна схема мережі ATM [13, 27].

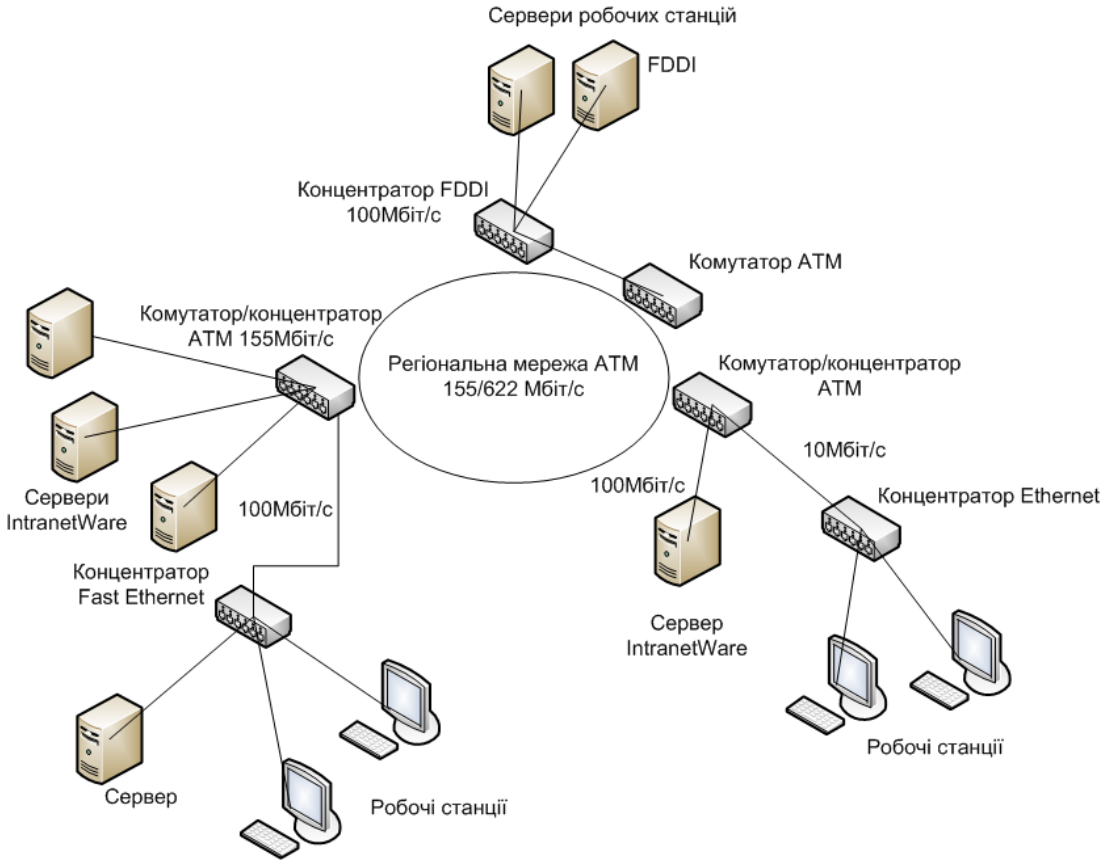

Рисунок 2.1 - Структурна схема мережі ATM

Перевагами такої технології є забезпечення високої швидкості передачі інформації та усунення розходження між локальними і глобальними мережами, перетворюючи їх у єдину інтегровану мережу, також стандарти ATM забезпечують передачу різнорідного трафіку (цифрових, голосових і мультимедійних даних) по одним і тим же системам і лініях зв'язку.

При цьому технологія ATM має деякі недоліки:

а) висока вартість обладнання, тому технології ATM гальмується наявністю більш дешевих технологій;

б) високі вимоги до якості ліній передачі даних.

Мережі X.25 є першими мережами з комутацією пакетів і на сьогоднішній день найпоширенішими мережами з комутацією пакетів, використовуваними для побудови корпоративних мереж. Мережевий протокол X.25 призначений для передачі даних між комп'ютерами через телефонні мережі. Вони розроблені для ліній низької якості з високим рівнем перешкод (для аналогових телефонних

ліній) і забезпечують передачу даних зі швидкістю до 10Мбіт/с. X.25 добре працює на лініях зв'язку низької якості завдяки застосуванню протоколів підтвердження встановлення з'єднань і корекції помилок на канальному і мережевому рівнях. У результаті основним завданням цих мереж є забезпечення гарантованої доставки даних по ненадійним каналам зв'язку і підвищення ефективності їх використання [13, 49].

На рис. 2.2 наведена структурна схема мережі X.25.

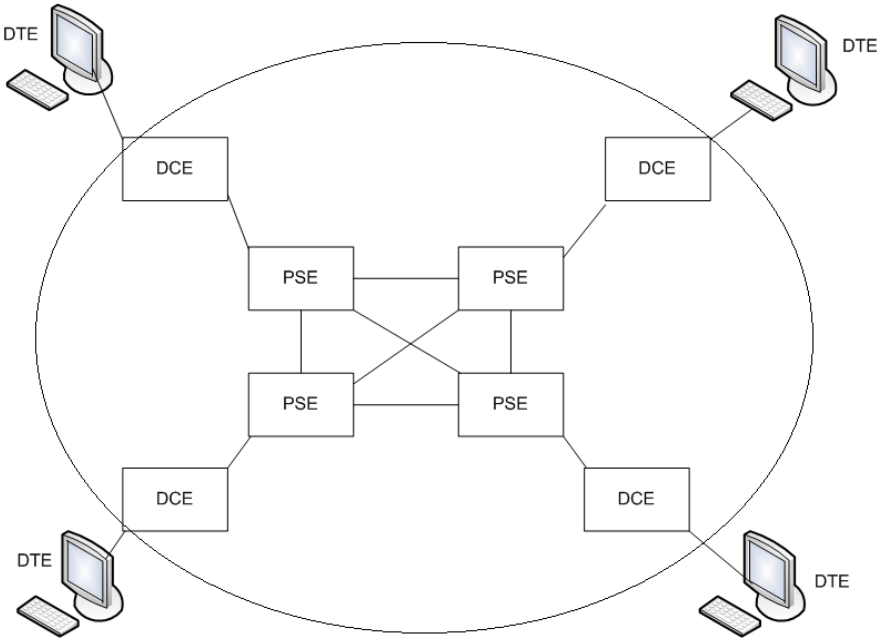

Рисунок 2.2 - Структурна схема мережі X.25 (мережа типу «Хмара»)

DTE (data terminal equipment) – апаратура передачі даних (касові апарати, банкомати, термінали бронювання квитків, ПК, тобто кінцеве обладнання користувачів);

DCE (data circuit-terminating equipment) – кінцеве обладнання каналу передачі даних (телекомунікаційне обладнання, що забезпечує доступ до мережі);

PSE (packet switching exchange) – комутатори пакетів.

Перевагими мережі X.25 є:

а) висока надійність, мережа з гарантованою доставкою інформації;

б) можуть бути використані як аналогові, так і цифрові канали передачі даних (виділені та комутовані лінії зв'язку).

При цьому недоліками мережі є значні затримки передачі пакетів, тому її неможливо використовувати для передачі голосу й відеоінформації.

Протокол Frame Relay (FR, ретрансляція кадрів) використовується для побудови мереж з пакетною комутацією. Frame Relay був створений в якості заміни протоколу X.25 для швидких надійних каналів зв'язку. Дана технологія орієнтована на цифрові канали передачі даних гарної якості, тому в ній відсутня перевірка виконання з'єднання між вузлами і контроль достовірності даних на канальному рівні. Кадри передаються без перетворення і контролю як у комутаторах локальних мереж. За рахунок цього мережі Frame Relay володіють високою продуктивністю. При виявленнях помилок в кадрах повторна передача кадрів не виконується, а спотворені кадри відбраковуються [13, 50].

На рис. 2.3 наведена структурна схема мережі Frame Relay.

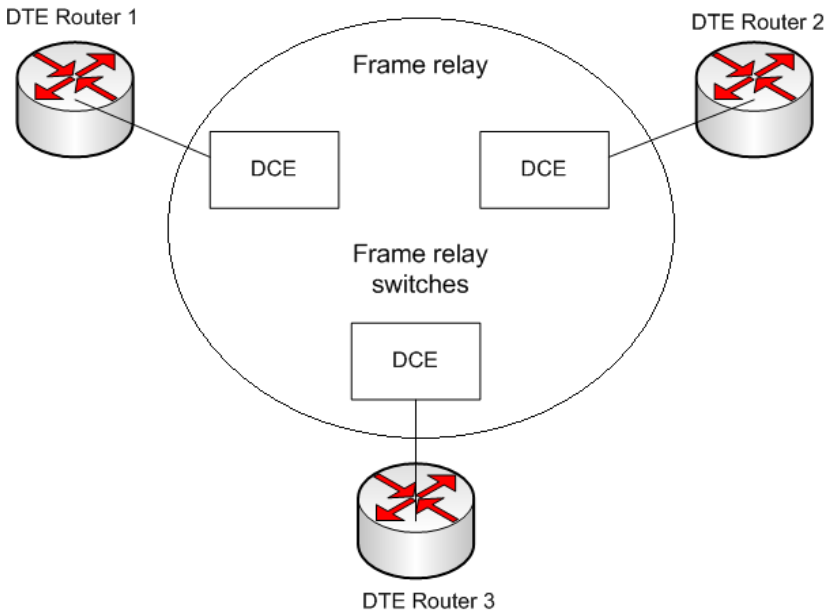

Рисунок 2.3 - Структурна схема мережі Frame Relay

DTE (Data Terminal Equipment) – апаратура передачі даних (маршрутизатори, мости, ПК);

DCE (Data Circuit-Terminating Equipment) – кінцеве обладнання каналу передачі даних (телекомунікаційне обладнання, що забезпечує доступ до мережі);

FRAD (Frame Relay Access Device) – пристрій доступу до мереж із ретрансляцією кадрів – мережний пристрій, наприклад маршрутизатор, який перетворює пакети з мереж TCP, SNA, IPX у фрейми.

Перевагами даної мережі є висока надійність роботи та забезпечення передачі чутливого до тимчасових затримок трафіку (голос, відеозображення).

А недоліком мережі Frame Relay є висока вартість якісних каналів зв'язку та не забезпечення достовірності доставки кадрів.

Порівняльна характеристика протоколів канального рівня глобальної обчислювальної мережі наведена в табл. 2.1 «Ймовірнісно-часові характеристики технологій ГОМ».

Таблиця 2.1 -Ймовірносно-часові характеристики технологій ГОМ

Технологія ГОМ	Метод підвищення достовірності	Вартість	Швидкість передачі даних, Мбіт/с	Довжина пакету, біт	Ймовірність правильної доставки пакету, $P_{пр. п}$	Час доставки пакету, $t_д$, с
X.25 (V.34)	На канальному рівні LAP-B (LAP-M, або V.42)	Середня	10	1056 1056	0.97546 0.97546	1030 1875
Frame Relay	Ні	Середня	100	12048	> 0	0.0003
ATM	На транспортному рівні	Висока	155 - 2488	53	0.58704	$3*10^{-7}$

Які б широкі можливості не пропонувала будь-яка нова технологія, користувач не зможе оцінити її по гідності в тому випадку, якщо вона виявиться занадто дорогою для впровадження і експлуатації. Простота, високий рівень стандартизації і гнучкість технології Frame Relay істотно знижують витрати на створення і експлуатацію інформаційних систем.

Технологія Frame Relay має дуже широке застосування. Вона надає мережі тільки швидкі базові транспортні послуги без гарантії достовірності доставки. Для подальших досліджувань будемо використовувати саме протокол управління

пакетами – Frame Relay. Він забезпечує високу швидкість передачі даних (100 Мбіт/с), менші затримки, але і меншу надійність доставки інформації. Гарантує більшу швидкодію, ніж інші мережі [13].

2.2. Аналіз канального протоколу глобальної обчислювальної мережі Frame Relay

Метод Frame Relay дозволяє об'єднати статистичне мультиплексування і поділ портів комутаторів мереж пакетної комутації X.25 з швидкодією і низькою затримкою мереж з комутацією каналів.

Frame Relay визначається як "пакетний режим" обслуговування, що означає, що дані перетворюються в індивідуально адресовані одиниці. (Це відбувається швидше, ніж при приміщенні в установлені тимчасові інтервали.). На відміну від X. 25, Frame Relay повністю усуває всю обробку на мережевому рівні. Крім того, Frame Relay використовує тільки частину функцій канального рівня, так звані "основні аспекти", які включають перевірку помилок в кадрі, але не вимагають повторної передачі кадру при виявленні помилки. Таким чином, такі традиційні функції протоколу передачі даних як перевірка послідовності надходження кадрів, регулювання розміру "вікна", механізм підтверджень не використовуються в мережі Frame Relay. Результатом виключення цих функцій є істотне збільшення продуктивності (тобто числа кадрів, які можуть бути оброблені в секунду за дану вартість апаратних засобів). З тієї ж самої причини, затримка при використанні методу Frame Relay більш низька, ніж у мережах X. 25 [56].

Оскільки протокол Frame Relay значно спрощено, відповідальність за безперервну і безпомилкову передачу даних лежить на кінцевих пристроях.

В табл. 2.2 приведені характеристики мереж з комутацією каналів, пакетною комутацією, і мереж Frame Relay.

Таблиця 2.2 - Порівняння комутації каналів, пакетної комутації і Frame Relay

	Комутація каналів	Пакетна комутація (X.25)	Frame Relay
Мультиплексування з тимчасовим поділом:	Так	Ні	Ні
Статистичне мультиплексування:	Ні	Так	Так
Поділ портів:	Ні	Так	Так
Висока продуктивність:	Так	Ні	Так
Затримка:	Дуже низька	Висока	Низька

Одна з особливостей Frame Relay полягає у використанні кадрів змінної довжини. Це дуже корисно при організації ефективної роботи з LAN та іншими джерелами, які вимагають змінного розміру кадру. Це також означає, що затримки (хоча завжди більш низькі, ніж у мережах X. 25) змінюються в залежності від розмірів надісланих кадрів. Деякі типи трафіку критичні до затримки, наприклад, мова і стисле відео. Frame Relay погано пристосований для передачі такого трафіку. Frame Relay повністю відповідає вимогам джерел "вибухового" трафіку, наприклад при інформаційному обміні LAN-to-LAN [57].

2.2.1. Огляд стандартів Frame Relay.

У результаті дослідження виявлені умови, які склалися на ринку телекомунікацій, сприяли швидкому розвитку промислових стандартів Frame Relay. Розробкою стандартів Frame Relay займаються Американський національний інститут стандартизації (ANSI) і Міжнародний союз електрозв'язку (ITU-T). Велику роботу в даній області проводить промислова асоціація Frame Relay Forum (FRF).

У 1988 ITU-T (у той час CCITT) прийняв Рекомендацію I.122 "Забезпечення додаткового пакетного режиму", яка використовувалася як частина з серії стандартів ISDN. Як відомо, в ISDN використовується протокол LAPD (протокол доступу до каналу зв'язку) для передачі сигналів по D-каналу. LAPD визначений ITU-T Рекомендацією Q. 921. Було відмічено, що LAPD має характеристики, які

могли бути корисні при вирішенні деяких "нетипових" завдань, наприклад, мультиплексування віртуальних каналів на 2 рівні. Описаний в рекомендації I.122 протокол може використовуватися для передачі даних не тільки в ISDN, але й інших мережах [49].

Розвитком положень I.122 почав займатися комітет ANSI, відомий як T1S1, під егідою ECSA. Була проведена велика робота, яка завершилася ухваленням стандартів, які повністю визначають Frame Relay. Стандарти T1. 606 був схвалений в 1990 році, а решта стандартів були прийняті в 1991 році (табл. 2.3).

Таблиця 2.3-Стандарти Frame Relay

ANSI		ITU-T (ITU)	
Стандарт	Статус	Стандарт	Статус
T1.606	Стандарт	I.233	Схвалений
T1.618 (Спочатку відомий як T1.6CA)	Стандарт	Q.922 Annex A	Схвалений
T1.617 (Спочатку відомий як T1.6FR)	Стандарт	Q.933	Остаточно схвалений у березні 1992г.

Розглянемо більш детальніше стандарти Frame Relay:

а) ANSI T1.606

Даний стандарт визначив принципи управління перевантаженнями в мережі Frame Relay, яка діє в площині користувача [55].

б) ANSI T1.618

Стандарт описує протокол, що підтримує фазу переносу даних сервісу Frame Relay, визначеного в стандарті ANSI T1.606. Стандарт T1.618 заснований на підмножині ANSI T1.602 (LAPD), званому Core Aspects (основні аспекти) і використовуваному комутаторами і постійними віртуальними каналами.

T1.618 також включає механізм консолідованого управління на канальному рівні CLLM. Генерація і передача CLLM є необов'язковим сервісом. При використанні CLLM значення DLCI 1023 резервується для передачі керуючих повідомлень канального рівня.

T1.618 використовує явні повідомлення про насичення, що передаються мережею користувальницьким пристроїв. Повідомлення про насичення містять код, показує причину насичення, і список всіх DLCI, для яких потрібно зниження рівня трафіку, щоб подолати насичення [56].

в) ANSI T1.617

Для організації комутованих віртуальних пристроїв SVC (Switched Virtual Circuit) користувачі Frame Relay повинні відкрити діалог з мережею, використовуючи сигнальні специфікації T1.617. Ця процедура призводить до виділення DLCI для комутованого віртуального пристрою. Після відкриття діалогу застосовуються процедури T1.618.

Для організації постійного віртуального пристрою PVC використовується протокол організації з'єднань (setup protocol), ідентичний протоколу D - каналів в ISDN і описаний в специфікації T1.617 [13, 21].

При використанні ISDN користувачі можуть застосовувати канал D для організації з'єднань. Для інших типів абонентів (не ISDN) каналу D не існує, тому діалог між користувачем і мережею повинен бути відділений від інших процедур передачі даних. У стандарті T1.617 для цього зарезервовано значення DLCI 0.

Стандарт T1.617 також містить специфікації узгодження параметрів сервісу Frame Relay.

Швидкий темп роботи ANSI над стандартами Frame Relay відповідав високому ступені співпраці й згоди на міжнародній арені. В результаті рекомендації ITU-T для Frame Relay відповідають стандартами ANSI. Frame Relay – єдиний міжнародний стандарт, охоплений як ANSI, так і ITU-T [6 – 7].

Для визначення стандартних по протоколах тестів на сумісність були випущені документи, звані IA (IA), які визначаються стандартами. Робота над IA для інтерфейсу "користувач - мережа" велася FRF і була завершена в 1991 році. Робота над стандартом інтерфейсу "мережа - мережа" була завершена у вересні 1992 року.

Робота в галузі стандартизації продовжує розширювати можливості Frame Relay. Один з напрямів цієї роботи полягає у виробленні додаткових специфікацій

для інтерфейсу "мережа - мережа". Існуючі стандарти описують інтерфейс "користувач - мережа". Експерти вважають, що інтерфейс "користувач - мережа" може використовуватися як інтерфейс "мережа - мережа" з двонаправленою сигналізацією.

У вересні 1990 року FRF був підготовлений стандарт LMI (Local Management Interface), який мав відношення до розробки Frame Relay. Основне значення цього стандарту полягає в тому, що він визначає додаткову функцію інтерфейсу – "локальне управління", як метод обміну інформацією про стан з'єднань між пристроєм користувача і мережею [21, 24].

У протягом 1991 року стандарт LMI увійшов у стандарти T1. і Q. 933 з деякими незначними змінами.

В даний час основні стандарти Frame Relay завершені. Вони були дуже швидко запропоновані і прийняті в США та в інших країнах завдяки безпрецедентній згоді в області виробництва та великому ринковому попиту на Frame Relay. Процес стандартизації був проведений до комерційного впровадження методу, тому виробники можуть спиратися на закінчений стандарт при побудові обладнання.

2.2.2. Особливості функціонування Frame Relay.

У найбільш популярних синхронних протоколах дані передаються по каналах зв'язку у вигляді кадрів. Типова структура кадру наведена на рис. 2.4.

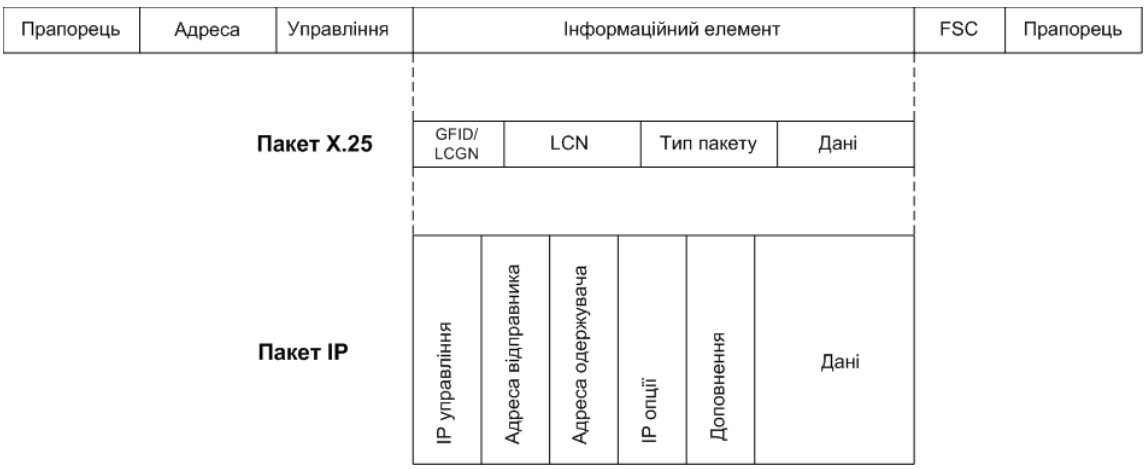

Рисунок 2.4 - Типова структура кадру в популярних синхронних протоколах

Кадр Frame Relay має невелике відміну від типової структури в заголовку. Формат кадру Frame Relay з нормальним багатобайтових заголовком наведений на рис. 2.5.

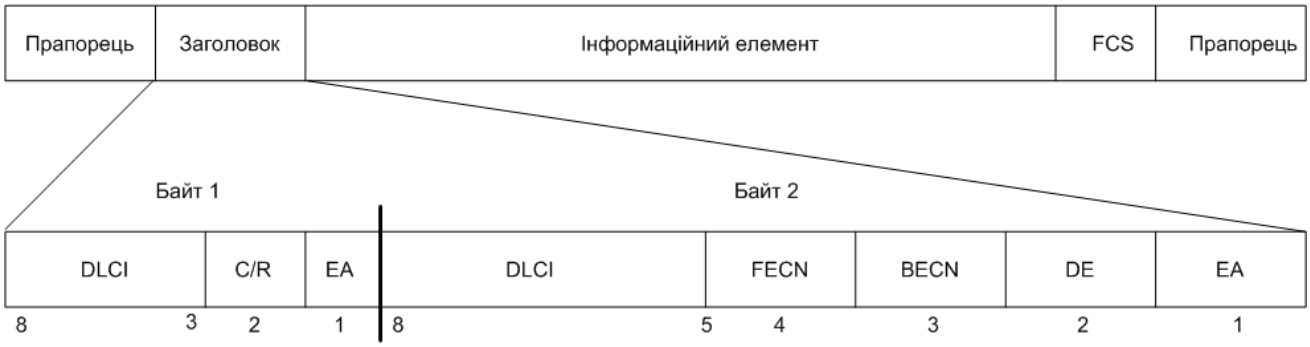

Рисунок 2.5 - Структура кадру Frame Relay.

Тема Frame Relay містить 10-розрядний ідентифікатор каналу передачі даних (DLCI), який є номером пов'язаного з певним отримувачем віртуального каналу. У разі інформаційного обміну LAN-WAN DLCI позначає порт, до якого підключається LAN [55].

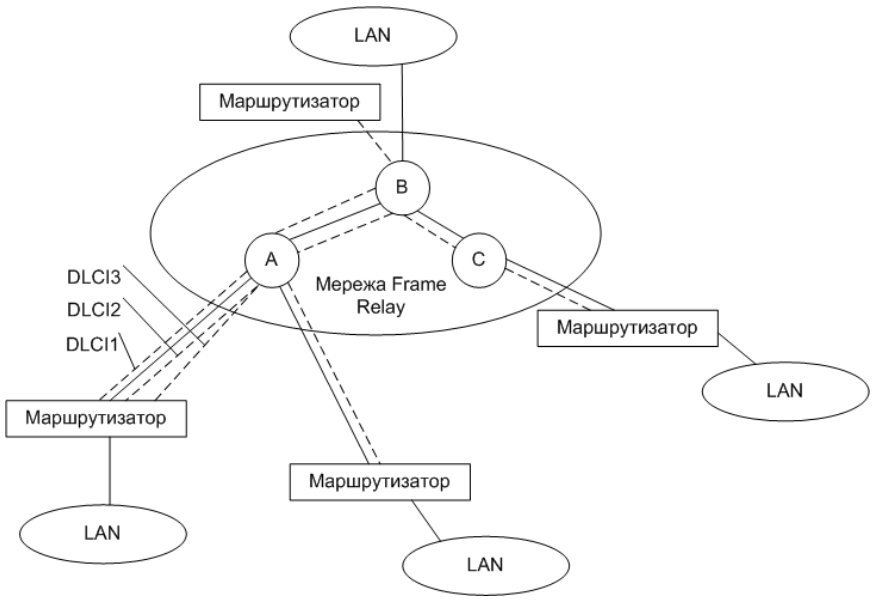

Рисунок 2.6 - DLCI позначає порт одержувача

Розглянемо алгоритм передачі даних через мережу Frame Relay:

а) Перевірка цілісності кадру. Використовується перевірочна послідовність кадру (FCS). У разі виявлення помилки кадр видаляється.

б) Порівняння DLCI кадру з таблицею DLCI у вузлі. Якщо для даного каналу DLCI не визначений, то кадр видаляється.

в) Ретрансляція кадру до одержувача. Здійснюється з порту, зазначеного в таблиці [7 – 8].

Зауважимо, що вузол Frame Relay не використовує багато кроків обробки, які характерні для протоколів типу X. 25. Вузол FR наведений на рис. 2.7.

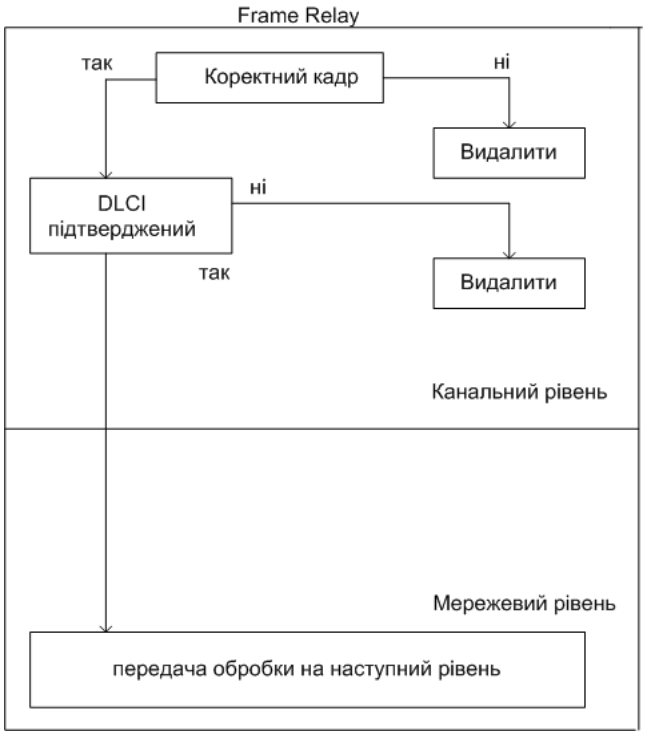

Рисунок. 2.7 - Спрощена модель функціонування Frame Relay

Розроблені в 1991 році стандарти передбачали використання в мережах Frame Relay тільки постійних віртуальних каналів (PVC). Такі канали встановлюються безпосередньо адміністратором мережі через систему управління.

PVC в мережі Frame Relay зазвичай визначає зв'язок між двома LAN, тому новий PVC необхідний тільки при підключенні нової LAN до мережі. PVC

повністю задовольняють вимогам більшості додатків. У ряді випадків можливе використання комутованих віртуальних каналів (SVC).

Основна процедура протоколу Frame Relay дуже проста і включає одне правило: якщо є якась проблема з обробкою кадру, то він знищується. До втрати кадру Frame Relay можуть призвести дві основні причини:

а) виявлення помилок в кадрі;

б) виникнення перевантаження в мережі.

Мережа може видалити кадр, не порушуючи цілісності повідомлення, тому що, кінцеві пристрої управляються протоколами вищих рівнів, які можуть виявляти і відновлювати втрачені дані в мережі [57].

Відновлення кадрів у відповідності з процедурами протоколів вищих рівнів.

Протокол вищого рівня стежить за втратою кадру. Він підраховує кількість відправлених і отриманих кадрів. Відправнику надсилається підтвердження про успішно прийнятих кадрах. У разі невідповідності кількості відправлених і прийнятих кадрів кінцевий пристрій посилає запит на повторну передачу. Таким чином, два кінцевих пристрої гарантують, що всі кадри будуть отримані без помилок. Ця функція реалізовується засобами транспортного рівня в протоколах типу TCP і OSI Transport Class 4.

Відновлення кадрів протоколами вищих рівнів може бути неефективним. Єдиний втрачений кадр буде вимагати, щоб всі інші кадри були передані повторно. Таке відновлення вимагає додаткових ресурсів в комп'ютерах кінцевих пунктів, а також додаткову смугу пропускання мережі, щоб повторно передати велике число кадрів. У підсумку така процедура може призвести до великих затримок [56, 57].

Спотворення кадрів, викликане помилками.

Помилка в кадрі виявляється за допомогою перевірочної послідовності кадру (FCS). На відміну протоколу X. 25 вузол Frame Relay при виявленні помилки не просить відправника виправити цю помилку повторною передачею кадру. Вузол просто відмовляється від кадру і переходить до оброблення наступного. Процедура виявлення помилок і перезапита покладається на

можливості персональних комп'ютерів або автоматизованих робочих місць, які є відправниками даних. Використання механізму виправлення помилок на високих рівнях не виправдане, якщо використовувати зашумлені канали з високою ймовірністю появи помилки. В даний час в світі стає все більше оптоволоконних ліній передачі з надзвичайно низькими показниками ймовірності появи помилки, тому відновлення даних на таких лініях відбувається досить рідко і не є суттєвою проблемою. Таким чином, Frame Relay максимально ефективний тільки на хороших каналах зв'язку (з малою ймовірністю виникнення помилки) [13, 56].

Видалення кадрів у разі перевантаження.

Більш суттєва причина втрати кадрів – перевантаження в мережі. Перевантаження відбувається в наступних ситуаціях:

а) вузол мережі не справляється з обробкою вхідного потоку;

б) інтенсивність потоку даних (число пакетів в секунду) на вході не відповідає швидкості каналу зв'язку;

в) переповнення буферу (тимчасова пам'ять для обробки кадру або вихідний черги кадрів) вузла комутації.

Дуже важливо, щоб мережа Frame Relay мала хороші механізми управління потоком, які могли б мінімізувати вірогідність виникнення і масштаби перевантажень, а також зменшити вплив втрачених кадрів. Особливості управління потоком докладно обговорюються нижче [13, 56].

Архітектура та стандарти протоколу.

Frame Relay є розвитком протоколу X.25 і відрізняється від останнього помітним спрощенням структури. Перше спрощення полягає у відмові від механізмів квитування та юсстановлення інформації на рівні протоколу Frame Relay, хоча різні додатки, що використовують транспортну середу Frame Relay, як і раніше містять у собі ці процедури. Причиною усунення цих процедур стало розвиток технології цифрових систем зв'язку та висока якість створюваних ними цифрових каналів. В результаті перешкодозахищеність протоколу X.25, де забезпечується відновлення переданої інформації на канальному і мережевому рівні, виявилося надлишкової.

Другим спрощенням протоколу Frame Relay стала орієнтація на канальний рівень передачі і відміна процедур мережевої маршрутизації всередині протоколу. Таким чином, якщо протокол X.25 включає три рівні протоколу, то протокол Frame Relay має тільки два неповних рівня. Це не означає, що процедури встановлення віртуального шляху були повністю виключені з протоколу, оптимізація була пов'язана зі структурою адресного поля, де в протоколі Frame Relay задавалася адреса не кінцевого абонента, а тільки найближчого вузла мережі передачі даних [56, 57].

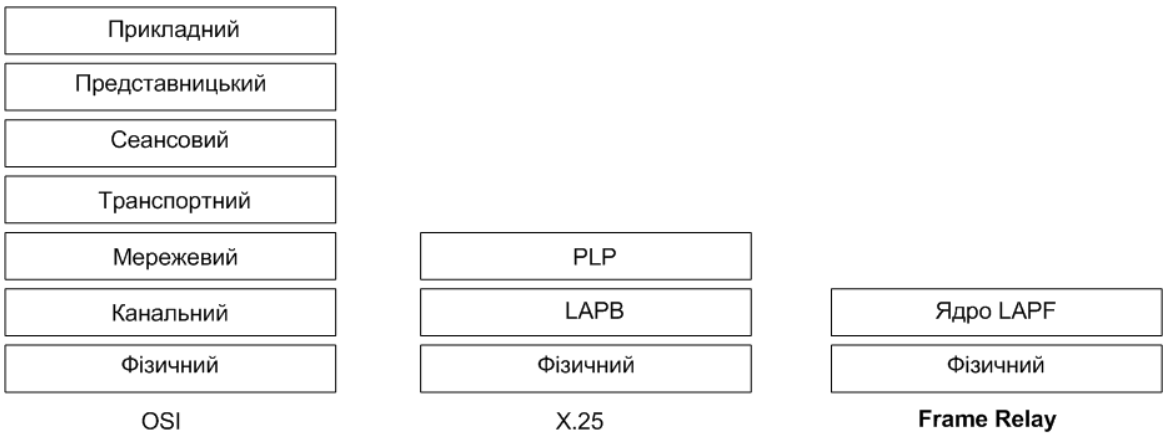

Рисунок 2.8 - Архітектури OSI, X.25 та Frame Relay

PLP (Packet Layer Protocol) – протокол рівня пакетної передачі;

LAPB (Link Access Procedure - Balanced) – процедура доступу до каналу трафікової передачі (B-каналу);

LAPF (Link Access Procedure to Frame Mode Bearer Services) – процедура доступу до режиму кадрової передачі.

Стандартизація протоколу Frame Relay йшла в трьох основних організаціях: американському інституті стандартизації ANSI, Міжнародному союзі електрозв'язку ITU-T і Форумі з розвитку Frame Relay (FRF). Стандарти ANSI і ITU-T співвідносяться між собою, і зазвичай в літературі по Frame Relay даються посилання тільки на ITU-T. Однак для розуміння трас протоколів необхідне знання стандартів ANSI, оскільки більшість аналізаторів протоколів дають

посилання саме на стандарти ANSI (це пов'язано з лідерством у світі американського ринку технології Frame Relay).

Стандартами передбачено два типи інтерфейсів в мережі Frame Relay: це інтерфейс "користувач-мережа" (UNI) та інтерфейс "вузол-вузол" (NNI). Користувач виходить в мережу Frame Relay за допомогою спеціального обладнання доступу з мережі Frame Relay - пристрої FRAD (Frame Relay Access Device) [56, 57].

В якості обладнання доступу з мережі Frame Relay рекомендуємо використовувати пристрої FRAD (Frame Relay Access Device) виробництва компанії NSG наступних серій:

а) NSG-900 – універсальний маршрутизатор і комутатор пакетів для мереж IP, Frame Relay, X.25;

б) NSG-800 – універсальний маршрутизатор і комутатор пакетів для мереж IP, Frame Relay, X.25;

в) NX-300 – мультипротокольні маршрутизатори і комутатори пакетів для мереж IP, Frame Relay, X.25;

г) NSG-500 – недорогі абонентські пристрої (customer premises equipment, CPE), призначені для підключення невеликих локальних мереж, віддалених робочих місць, банкоматів, POS-терміналів та іншого термінального устаткування до мереж IP, Frame Relay і X.25.

Передача керуючих сигналів.

При розробці протоколу Frame Relay визначальним був принцип простоти протоколу мережі. Всі проблеми обробки даних повинні вирішуватися протоколами вищих рівнів, реалізованих в кінцевих пристроях. Після подальшого вивчення стало ясно, що при практичній реалізації мереж Frame Relay мають бути визначені механізми для вирішення наступних важливих проблем [21, 24]:

а) повідомлення про виникнення перевантаження;

б) повідомлення про стан віртуальних каналів;

в) забезпечення рівноправності і гарантованою продуктивності для користувачів;

г) облік майбутнього розширення мережі та нових умов експлуатації.

Тому для вирішення цих проблем в стандарти ANSI і ITU-T були включені різні механізми передачі сигналів. В основі одних лежить використання бітів в заголовку кадру Frame Relay, інші засновані на використанні деяких каналів для інтерфейсу управління. Розглянемо найбільш важливі механізми передачі сигналів [21].

Забезпечення ефективної роботи мережі Frame Relay.

У загальному випадку використання механізмів управління необов'язково. Однак, вони істотно впливають на такі показники мережі як продуктивність, час відповіді, ефективність використання каналів і кінцевого обладнання користувачів.

Тому важливо розуміти, які можливості надають механізми управління і як ними краще скористатися. Одна з важливих властивостей мережі – управління потоком, наведена на рис. 2.9.

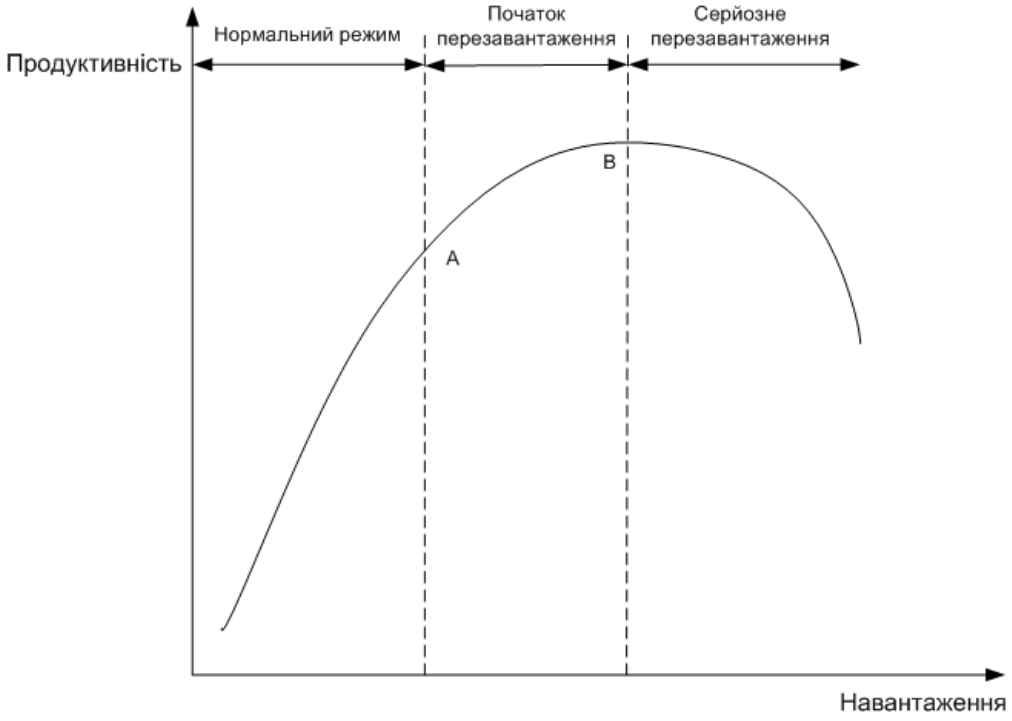

Рисунок 2.9 - Управління потоком

У разі виникнення перевантаження в точці А частина вхідних кадрів знищується. Якщо вхідні навантаження продовжує збільшуватися, це призводить

до серйозного перевантаження в точці В, де ефективна продуктивність мережі починає зменшуватися через багаторазової передачі одного і того ж кадру. У випадку серйозного перевантаження (блокування) повна продуктивність мережі може сильно впасти і єдиний спосіб виходу з даного становища – зменшення вхідного навантаження. У зв'язку з цим були використані кілька механізмів про повідомлення пристроя користувача про перевантаження. У цьому випадку пристрій користувача повинно зменшити обсяг переданої інформації. В ідеальному випадку мережа повинна відстежити появу перевантаження в точці А і за допомогою спеціальних можливостей запобігти появі серйозного перевантаження в точці В [21, 33].

2.2.3. Механізми повідомлення про перевантаження.

2.2.3.1. Біти явного повідомлення про перевантаження (ECN).

Перший механізм використовує два біти "явного повідомлення про перевантаження" (ECN) в заголовку кадру Frame Relay. Це біт "явного повідомлення приймача про перевантаження" (FECN) і біт "явного повідомлення джерела про перевантаження" (BECN). На рис. 2.10 наведене використання цих бітів.

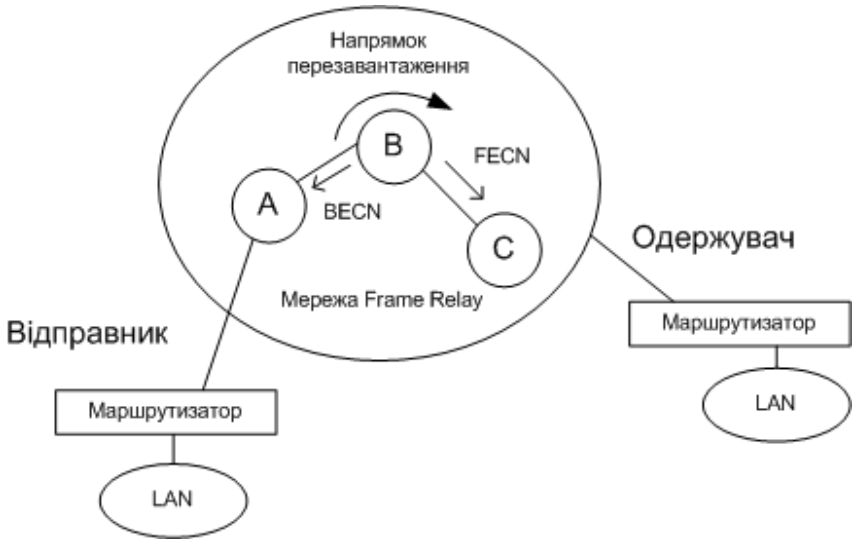

Рисунок 2.10 - Використання FECN і BECN при явному повідомленні про перевантаження

Припустимо, що вузол В наближається до стану перевантаження. Це могло бути викликано, наприклад, тимчасовим піком входження у вузол трафіку або піком трафіку в каналі між вузлами В і С. Вузол В може виявити початок перевантаження внутрішніми ознаками, таким як надмірне використання пам'яті або збільшення довжини черги. Вузол С (наступний за напрямком до одержувача) буде повідомлений про це, отримавши кадр з встановленим бітом FECN. Усі наступні за напрямком до одержувача вузли, також як і пристрій користувача, дізнаються, що на певних DLCI з'явилося перевантаження [56].

Для деяких протоколів корисніше повідомити джерело даних про перевантаження для того, щоб він зміг сповільнитися до пропажі перевантаження. Вузол В також спостерігає за кадрами, які передаються у зворотний бік, і встановлює біт BECN в 1. Цей процес установки FECN і BECN може здійснюватися одночасно на декількох DLCI у відповідь на перевантаження в даному каналі або вузлі. Біти ECN представляють важливий інструмент для зменшення серйозних станів перевантаження [56, 57].

2.2.3.2. Об'єднане управління на канальному рівні (CLLM).

ANSI визначив ще один механізм для передачі сигналів управління, відомий як CLLM. При використанні CLLM один з DLCI (номер 1023) в інтерфейсі Frame Relay зарезервований для передачі керуючих повідомлень канального рівня від мережі до пристрою користувача.

Стандарт ANSI (T1. 618) визначає формат повідомлення CLLM. Воно містить причину перевантаження (наприклад, надмірного трафіку, відмова каналу, і т.д.) і список всіх DLCI, в яких необхідно зменшити трафік і тим самим знизити перевантаження. CLLM може використовуватися замість або на додаток до бітам ECN, щоб повідомити влаштуванню користувача про виникнення перевантаження. CLLM забезпечує додатковий стандартний механізм для передачі сигналів повідомлення про перевантаження [57].

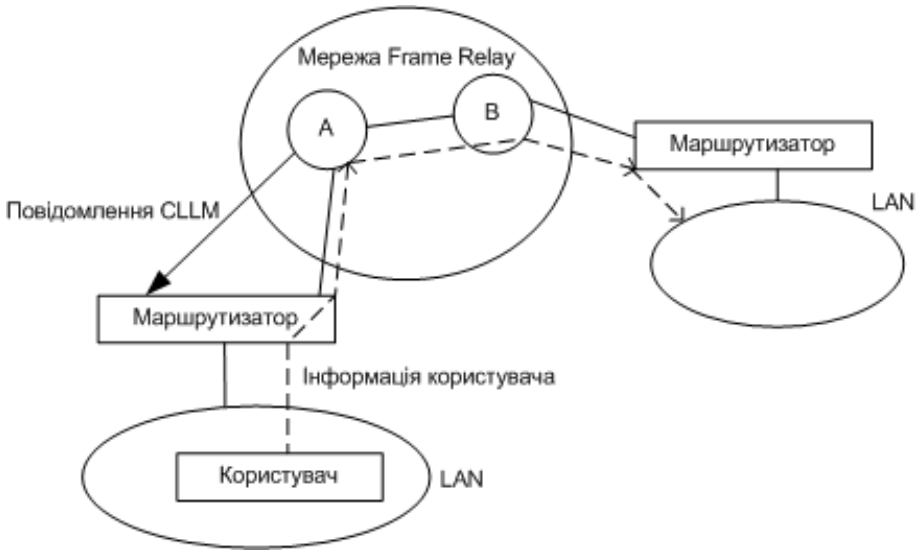

Рисунок 2.11 - Використання CLLM при передачі сигналів повідомлення про перевантаження

2.2.3.3. Неявне повідомлення про перевантаження.

Деякі протоколи верхніх рівнів, які реалізовані в кінцевих пристроях, мають механізм неявного виявлення перевантаження. Ці протоколи використовуються для ефективної передачі інформації по мережах з невизначеною місткістю. Такі протоколи обмежують потік даних за допомогою "вікна", яке дозволяє тільки обмеженому числу кадрів бути посланими до отримання підтвердження. Протокол може виявити перевантаження по збільшенню затримки передачі повідомлення до одержувача і назад або з аналізу втрати кадрів у мережі. Цей механізм відомий як "неявне повідомлення про перевантаження" [56, 57].

Якщо ознаки вказують на виникнення перевантаження, протокол може зменшити розмір вікна, що призведе до зменшення вхідного навантаження на мережу. Відповідно, при зменшенні перевантаження розмір вікна може поступово збільшуватися. Регулювання розміру вікна може бути одним з механізмів відповіді і на явне повідомлення про перенавантаження. У стандартах ANSI зазначено, що неявне і явне повідомлення про перенавантаження є додатковим засобом для підвищення ефективності мережі.

2.2.3.4. Реакція пристрою користувача на перевантаження.

У відповідності зі стандартами Frame Relay пристрій користувача має регулювати свій трафік. Для цього запропоновані деякі підходи, що включають

принципи регулювання розміру вікна. Виконання пристроєм користувача рекомендованих дій призводить до зменшення обсягу переданої інформації, тим самим до скорочення перевантаження. Однак, пристрій користувача може і не виконувати дані рекомендації. Воно може просто ігнорувати сигнал перевантаження і продовжувати передавати дані з тією ж інтенсивністю. Це призвело б до появи складного перевантаження або блокування (вузла, частини мережі, мережі повністю). Якщо є проблема з обробкою кадру, то він сам знищується. Тому, якщо виникає перевантаження, то частина кадрів знищується. Це збільшить час відповіді і зменшить повну продуктивність мережі, але мережа буде продовжувати функціонувати. Крім того, якщо мережа досить інтелектуальна, може відбуватися знищення кадрів конкретного користувача, гарантуючи іншим збереження їх кадрів [48, 56].

2.2.3.5. Стан PVC.

Наступний механізм управління визначає, яким чином дві сторони інтерфейсу Frame Relay (наприклад, мережа і маршрутизатор) організують обмін інформацією про стан інтерфейсу і різних PVC цього інтерфейсу. Керуюча інформація включає:

а) повідомлення про активність інтерфейсу;

б) DLCI, визначені для даного інтерфейсу;

в) стан кожного PVC (наприклад, перевантажений чи ні).

Вперше визначення стану PVC було реалізовано в LMI. Передача сигналів відбувається по DLCI з номером 1023. (Так як в LMI передача сигналів відбувається по каналу з тим же DLCI, що і для CLLM, ці два види сигналізації взаємно виключаються.) LMI передбачає сигнальне повідомлення "запит стану", яке ініціюється пристроєм користувача (наприклад, маршрутизатором), і повідомлення "keep alive ". Дане повідомлення інформує мережу про те, що з'єднання з пристроєм користувача активно, або як прохання повідомити стан PVC. Мережа відповідає повідомленням "стан" у формі "keep alive" або у формі повного повідомлення про стан PVC [56].

LMI асиметричний. Це означає, що тільки пристрій користувача може посилати повідомлення "запит стану", і тільки мережа може відповісти з повідомленням "стан". Цей підхід найбільш простий для реалізації, але вносить деякі обмеження в можливості LMI. Одна з особливостей даного методу полягає в тому що, односторонній механізм не підходить для інтерфейсу "мережа - мережа". Тому, перш ніж завершити схвалення стандарту, визначальну передачу керуючих сигналів Frame Relay, ANSI розширило цей стандарт, щоб забезпечити двосторонній механізм для передачі сигналів стану PVC. Механізм є симетричним (тобто обидві сторони інтерфейсу можуть генерувати ті ж самі команди і відповіді) [56, 57].

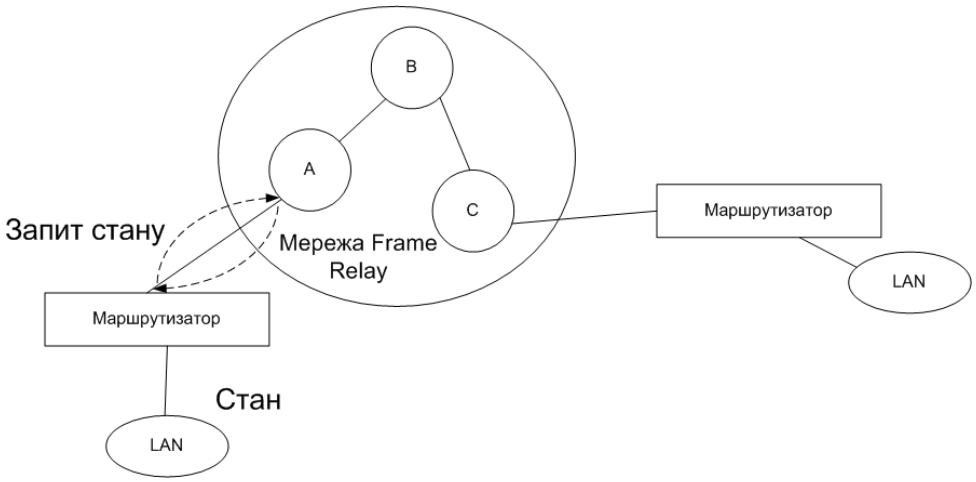

Рисунок 2.12 - Передача сигналів стану PVC в LMI

2.2.3.6. Забезпечення рівних прав доступу.

Трафік в мережах Frame Relay генерується широким діапазоном джерел від повільних (наприклад, операційний термінал, який посилає невеликі потоки даних) до швидкодіючих пристроїв (графічні автоматизовані робочі місця, здатні послати мультімегабітні потоки даних). Проблема полягає в забезпеченні джерел невеликих потоків даних гарантованою смугою пропускання, яка в загальному випадку може бути перекрита джерелами мультімегабітних потоків. Однак, пристрої користувачів можуть ігнорувати сигнали перевантаження [48].

У цьому випадку виробники вирішують проблему гарантії смуги пропускання відповідно до стандарту ANSI.

Один з бітів в заголовку кадру Frame Relay використовується як "Дозвіл скидання" (DE) (рис. 2.13).

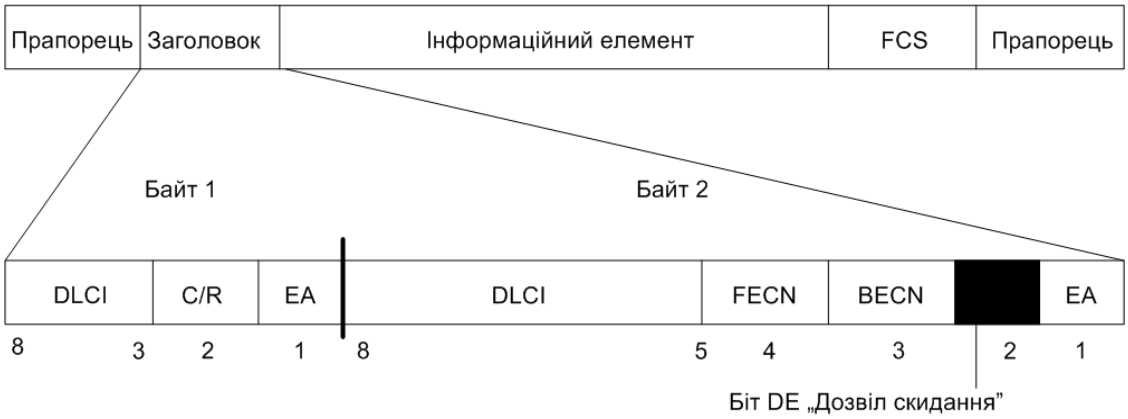

Рисунок 2.13 - Біт DE

Біт DE вказує, що у разі перевантаження мережа буде першими нищити кадри з встановленим бітом DE. Цей біт може бути встановлений пристроєм користувача для деяких кадрів з низьким пріоритетом. Звичайно не всі пристрої користувачів будуть дотримуватися цього принципу. Тому біт DE може встановлюватися безпосередньо вузлом мережі для вказівки подальшим вузлам, що при необхідності даний кадр може бути знищений в першу чергу [55, 56].

Таким чином, біт DE є інструментом, який дає можливість мережі керувати продуктивністю. В результаті цей інструмент може використовуватися для забезпечення користувачу передбачуваної і навіть гарантованої продуктивності.

2.2.4. Внутрішня організація мережі Frame Relay.

Нормальне функціонування мережі визначається її внутрішніми процесами. Функції, які повинні бути виконані в рамках мережі, включають:

а) визначення шляхів PVC;

б) прийняття рішення при наближенні перевантаження і заходи для її запобігання;

в) ефективна реакція на перевантаження;

г) прийняття рішення про видалення кадру, коли це видалення необхідно;

д) забезпечення гарантованого рівня обслуговування користувачів;

е) надання режиму пріоритетного обслуговування;

є) зв'язок між вузлами мережі;

ж) забезпечення управління мережею;

з) забезпечення необхідного рівня продуктивності [56].

Визначення шляхів PVC.

Використання постійних віртуальних каналів означає, що всі з'єднані кінцеві пристрої віртуальних каналів визначені оператором мережі. Однак активний шлях трафіку від вузла до вузла може бути вибраний з кількох можливих. При самому примітивному підході оператор мережі повинен визначити шлях (і кілька додаткових шляхів) від вузла до вузла. Ці шляхи мають бути відображені в маршрутних таблицях вузлів або, що менш надійно, в центральній системі управління мережею. Генерація такої таблиці забирає досить багато часу для забезпечення оптимальної маршрутизації у великій мережі. Більш ефективним є визначення маршрутних таблиць автоматично системою управління мережи [48, 56].

Кращий підхід полягає в тому, щоб маршрут визначався автоматично в вузлах комутації. У разі відмови каналу або при послідовному перевантаженні мережа повинна автоматично та динамічно знайти кращий доступний додатковий маршрут. У найбільш складних підходах передбачається, що в кожному вузлі закладений маршрут кожного PVC, і при виборі маршруту вузол здатний врахувати різні типи каналів для гарантії автоматичної оптимізації використання ресурсів мережі для різних категорій користувачів. Архітектура мережі та система керування мережею повинна надати оператору мережі здатність "налаштувати" автоматичну маршрутизацію для відповідності потребам мережі [56].

Визначення перевантаження та способи виходу з перевантаження.

Є різні способи визначення перевантаження. Найбільш простий підхід полягає в тому, щоб розпізнати перевантаження по видаленню кадрів. Більш досконалі алгоритми контролюють внутрішні параметри, наприклад, довжину

черги, щоб виявити перевантаження перш, ніж це призведе до видалення кадрів. При виявленні перевантаження мережа повинна розумно прийняти рішення про те, які джерела повинні зменшити вхідне навантаження. Вибірковий підхід набагато краще (і справедливіше) ніж загальний підхід, коли сповільнюються всі джерела трафіку [26].

Видалення кадру.

У разі перевантаження вузли повинні прийняти рішення про видалення кадрів. Найпростіший підхід полягає в тому, що кадр вибирається навмання. У цьому випадку збільшується число кінцевих пристроїв, які повинні вести відновлення кадрів через їх втрати. Можливо поліпшити роботу мережі, відмовляючись від кадрів в конкретному PVC, так як багаторазове відновлення одного кадру простіше.

Гарантована продуктивність.

Як обговорювалося раніше, використання біта DE – потужний механізм для оптимізації рішення про видалення кадру, і використовується як у прикордонних, так і у внутрішніх транзитних вузлах мережі. Цей механізм може використовуватися як інструмент для забезпечення гарантованого рівня обслуговування користувачам. Кожен користувач вибирає "Гарантовану швидкість передачі даних" (CIR), яка визначає потребу користувача для передачі трафіку протягом певного періоду часу. Мережа вимірює трафік користувача через певні інтервали. Якщо користувач посилає дані зі швидкістю не більшою, ніж CIR, мережа не буде змінювати біт DE, і кадр гарантовано буде переданий по мережі. Якщо швидкість перевищить CIR протягом даного періоду часу, то вхідний вузол встановить біт DE на надлишкових кадрах і буде продовжувати передавати ці кадри, якщо мережа не перевантажена. Нарешті, якщо швидкість надходження кадрів виявиться вище максимальної, то всі надлишкові кадри будуть видалятися і не будуть впливати на інших користувачів [49, 56].

Рисунок 2.14 - Використання CIR забезпечує гарантований рівень продуктивності

Рис. 2.15. ілюструє, як CIR може використовуватися в мережі Frame Relay для двох користувачів, що мають постійну швидкість доступу T1. Висока швидкість бажана для того, щоб час затримки в мережі було низьким. Але так як трафік "вибуховий", швидкість нормального трафіку для більшості користувачів буде трохи нижче, ніж повна швидкість в каналі навіть протягом пікових годин. Трафік користувача "H" може скласти в середньому 512 Кбіт/с протягом пікових періодів. Користувач "L" має менші вимоги до трафіку, чия пікова потреба становить в середньому 64 Кбіт/с [56, 57].

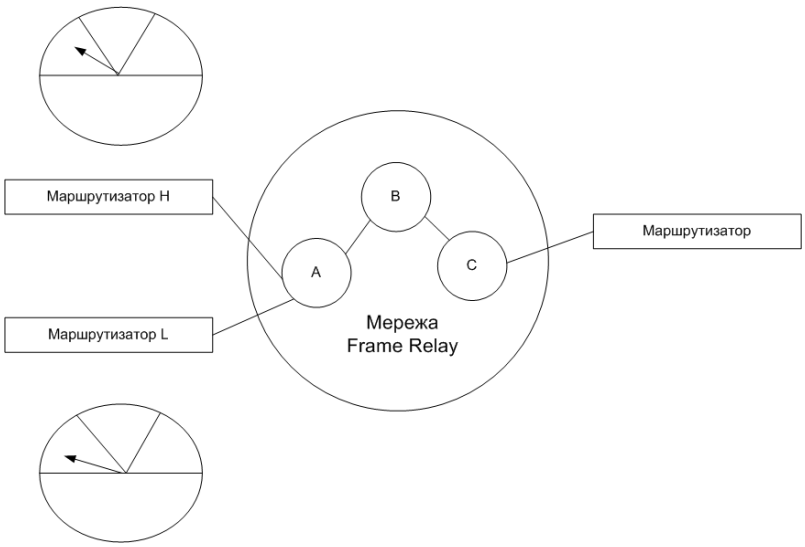

Рисунок 2.15 - Використання біта DE і CIR

При використанні біта DE і з урахуванням "вимірювання" трафіку мережа може гарантувати передбачуваний рівень обслуговування. Ця здатність може бути дуже цінною. Такий механізм використовується в мережах загального користування або корпоративних із відомчої системою оплати. Там, де оплата не використовуються, цей метод може бути застосований для проектування та управління мережею, щоб кожен користувач отримав відповідний рівень обслуговування.

Механізм пріоритетів.

Подальша робота по організації мережі Frame Relay полягає у використанні рівнів пріоритетів для трафіку Frame Relay. Дані з більш високим пріоритетом отримали б найменшу затримку в порівнянні з кадрами більш низького пріоритету і гарантію доставки. Ця особливість важлива в мережах, які підтримують чутливі до затримки додатки, і в той же час використовуються для передачі об'ємних файлів, які більш інтенсивно займають смугу пропускання, але менш чутливі до часу відповіді. Для чутливих до затримки даних призначався б більш високий пріоритет, гарантуючи швидку доставку.

Рівні пріоритетів мають додаткові переваги в мережах із змішаними протоколами. Трафік SDLC і HDLC може бути перетворений в трафік Frame Relay за допомогою Frame Relay access/device (FRAD). Деякі з цих протоколів чутливі до затримки, тому, що вони розроблені для роботи на аналогових каналах з великою ймовірністю виникнення помилки. Використання пріоритетів дозволяє таким протоколам отримувати вигоду від використання Frame Relay при підтримці характеристик затримки, необхідних для хорошої роботи [48, 57].

Міжвузлові зв'язки.

Гарний зв'язок між вузлами необхідна для надійного та ефективного функціонування мережі. Вузли повинні обмінюватися інформацією про стан перевантажень, готовності смуги пропускання, маршрутів з найменшою вартістю для PVC, станів каналів і апаратних засобів, і т. д.

Якщо вузли не можуть зв'язуватися безпосередньо, то вони повинні зв'язуватися через окремий пристрій (наприклад, центральну систему управління

мережею). У цьому випадку ефективність і надійність мережі стає строго обмеженою [57].

Продуктивність Frame Relay.

Проектувальники WAN стикаються з вибором реалізації обладнання Frame Relay. Один з підходів передбачає використання тільки програмного забезпечення. Цей підхід часто використовується при додаванні режиму Frame Relay до пакетного комутатора X. 25. У цьому випадку передача кадру виконується тим же самим процесором, який здійснює процедури протоколу X.25. Так як Frame Relay передбачає меншу обробку кадру, ніж X. 25, продуктивність Frame Relay може бути значно вище, ніж X. 25 для тих же самих апаратних засобів.

Інший підхід дозволяє ще збільшувати продуктивність. Він полягає в наступному. Спрощений характер обробки в Frame Relay дає можливість виробникам здійснити деякі кроки обробки кадру на більш високошвидкісних апаратних засобах замість виконання всієї обробки кадру на процесорах загального призначення, необхідних для більш складного X. 25. Тому, додаткова продуктивність Frame Relay може бути досягнута зміною апаратних засобів і програмного забезпечення вузлів [26, 57].

2.2.5. Взаємодія та функціонування.

Маса додаткових можливостей в стандартах і цілий діапазон рішень, пропонованих виробниками, може привести до труднощів при виборі обладнання для створення сумісних мереж.

Мінімальні вимоги: основна обробка даних.

Для досягнення сумісності обладнання Frame Relay має реалізовувати основний стандартизований метод транспортування даних, описаний в першому розділі. Передача кадру проводиться на підставі DLCI в багатобайтових заголовках кадру Frame Relay. Решта просто визначає додаткові можливості по управлінню [57].

Вимоги для реальних міжнародних мереж.

Механізми управління необов'язкові, тобто передача даних може здійснюватися і без них. Однак в реальних мережах, користувачі можуть зажадати гарантію сплаченого ними рівня обслуговування. У цьому випадку застосування механізмів управління просто необхідно [13, 21].

Для маршрутизатора або іншого пристрою користувача досить підтримувати тільки певне число різних додаткових механізмів. Однак для опорної мережі (backbone) WAN важливо, щоб була можливість підтримувати більшість запропонованих механізмів. В цьому випадку мережа зможе успішно працювати з широким діапазоном маршрутизаторів, мостів та мереж загального користування. Крім того, кожен порт в мережі повинен бути конфігуруємим, щоб підтримати різні комбінації цих механізмів.

2.3. Висновки до розділу 2

На сьогоднішній день для забезпечення роботи з глобальними та локальними обчислювальними мережами використовують такі протоколи канального рівня як ATM, X.25 та Frame Relay. На даний момент технологія ATM не використовується, так як вона об'єднує принципи комутації пакетів і каналів для передачі інформації різного типу. Мережа X.25 не забезпечує показник оперативності. Frame Relay забезпечує високу швидкість передачі даних (100 Мбіт/с), менші затримки, але і меншу надійність доставки інформації. Гарантує більшу швидкодію, ніж інші мережі.

3 ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ТЕОРЕТИЧНИХ РЕЗУЛЬТАТІВ НА ОСНОВІ МЕТОДІВ СТАТИСТИЧНОГО, ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ, ЗА ДОПОМОГОЮ ПРОГРАМНИХ ПАКЕТІВ

3.1. Оцінка показника функціональної ефективності комп'ютерної мережі на основі протоколу Frame Relay, в каналах без пам'яті

Сучасні мережеві технології стрімко розвиваються та обчислювальні можливості дозволяють збільшити обсяги даних, що надходять. Серед протоколів комп'ютерних мереж (КМ) широке поширення отримала технологія Frame Relay, яка дозволяє реалізувати переваги пакетної комутації на швидкісних лініях зв'язку. Frame Relay дозволяє об'єднати статистичне мультиплексування й розподіл портів комутаторів мереж пакетної комутації X.25 зі швидкодією й низькою затримкою мереж з комутацією каналів [13, 21].

Оцінка ефективності обміну даними в комп'ютерній мережі характеризується приватними показниками комп'ютерних систем і систем зв'язку[13]. У роботі [55] запропонована методика оцінки загального показника ефективності обміну даними. В статті [49] досліджується ефективність обміну даними в комп'ютерній мережі при різних способах управління обміном на основі протоколу X.25 щодо забезпечення користувачам потенційної можливості доступу до поділюваних ресурсів усіх комп'ютерів, об'єднаних у мережу.

У даній роботі будемо досліджувати узагальнений показник на основі протоколу Frame Relay і його порівняння з результатами дослідження ефективності обміну даними на основі протоколу X.25.

Існує чотири способи управління обміном даними для підвищення значення показника функціональної ефективності комп'ютерної мережі:

а) без зворотного зв'язку з виправленням t-кратних помилок;

б) без зворотного зв'язку з виявленням r-кратних помилок;

в) з вирішальним зворотним зв'язком і безперервною передачею кадрів (ВЗЗбп) "Повернення-на-N";

г) з вирішальним зворотним зв'язком і позитивною квитанцією (ВЗЗпк).

Стратегія u_1. Значення показника ефективності комп'ютерних мереж, що використовують циклічні коди в режимі виявлення помилок визначається за формулою [49, 55]:

$$W(u_1) = \frac{n^{(u_1)} - t^{(u_1)}}{n^{(u_1)}} \cdot \frac{B^{(u_1)} - \Psi^{(u_1)}}{B^{(u_1)}} \cdot P_{прп}^{(u_1)}, \quad (3.1)$$

Стратегія u_2. Значення показника ефективності комп'ютерних мереж без зворотного зв'язку при виправленні t-кратної помилки циклічним кодом визначається за формулою [49, 55]:

$$W(u_2) = \frac{n^{(u_2)} - t^{(u_2)}}{n^{(u_2)}} \cdot \frac{B^{(u_2)} - \Psi^{(u_2)}}{B^{(u_2)}} \cdot P_{прп}^{(u_2)}, \quad (3.2)$$

Стратегія u_3 Значення показника ефективності комп'ютерних мереж з вирішальним зворотним зв'язком і безперервною передачею кадрів "Повернення-на-N" визначається за формулою [49, 55]:

$$W(u_3) = \frac{n^{(u_3)} - t^{(u_3)}}{n^{(u_3)}} \cdot \frac{B^{(u_3)} - \Psi^{(u_3)}}{B^{(u_3)}} \cdot P_{прп}^{(u_3)}, \quad (3.3)$$

Стратегія u4. Значення показника ефективності комп'ютерних мереж з вирішальним зворотним зв'язком і позитивною квитанцією визначається за формулою [49, 55]:

$$W(u_4) = \frac{n^{(u_4)} - t^{(u_4)}}{n^{(u_4)}} \cdot \frac{B^{(u_4)} - \Psi^{(u_4)}}{B^{(u_4)}} \cdot P_{прп}^{(u_4)}, \quad (3.4)$$

де: n – довжина інформаційного кадру n (при розрахунках значення вибиралося виходячи зі стандартних довжин кадрів стека протоколів Frame Relay);

s – довжина квитанції s (для систем зі зворотним зв'язком, відповідає стандартним довжинам службових кадрів Frame Relay);

C – пропускна здатність каналу передачі даних;

L – довжина лінії зв'язку;

$V_р$ – швидкість поширення сигналу в середовищі;

$t_ш$ – час шифрування I-кадру;

$t_{рш}$ – час розшифрування I-кадру;

r – число виявлених помилок;

P_0 – імовірність помилки біта, є характеристикою достовірності передачі інформації, змінюється в межах від 10^{-6} до 10^{-8}.

У результаті дослідження комп'ютерних мереж, вихідними даними також виступали наступні параметри:

а) необхідна ймовірність доставки пакета $P_{тр}$ (при розрахунках використовувалося $P_{тр} = 0,95$);

б) розмір вікна Z (використовується для систем з ВЗЗСбп "Повернення-на-N", в протоколі Frame Relay може змінюватися в діапазоні від 1 до 7);

в) кратність виявляються помилок r (використовується для систем з виявленням помилок);

г) кратність виправляються помилок t (використовується для систем з виправленням помилок);

д) задана імовірність доставки пакета $P_З$ (використовується для систем з ВЗЗпк) [49].

У результаті дослідження була виявлена залежність між отриманими значеннями показника ефективності комп'ютерної мережі W і змінами ймовірності бітових помилок P0.

Для побудови даного графіка були використані наступні дані: L = 1000 км; s = 32; Vp = 3·108 м/с; C = 56000 бит/с; r = 16; n1 = 4056; n2 = 51; Z = 6; PЗ = 0,95;

t = 8; тш_1 = 0,01 с; трш_1 = 0,01 с; тш_2 = 100 с; трш_2 = 100 с; В1 = 1024, В2 = 1030; Ψ = 1015; Р0 = 0,0000001.

Результати дослідження наведені на рис. 3.1 та рис. 3.2.

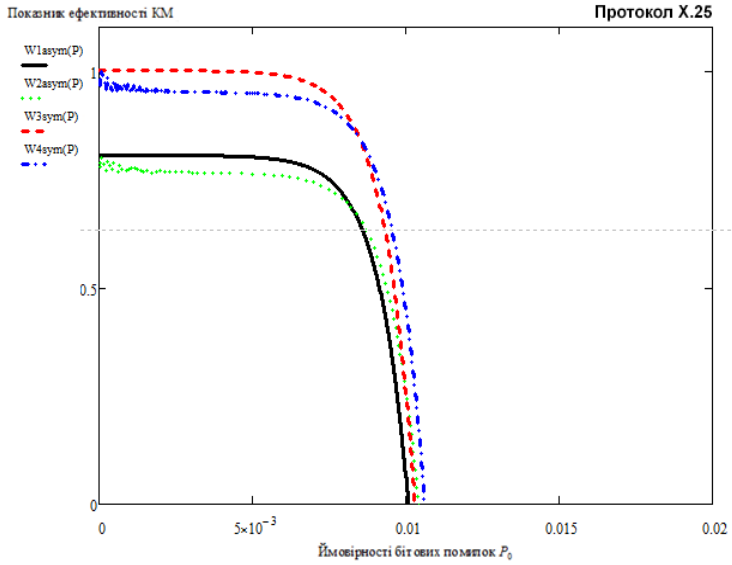

Рисунок 3.1 - Залежність між показником ефективності комп'ютерної мережі W і зміною ймовірності бітових помилок P_0 на основі протоколу X.25

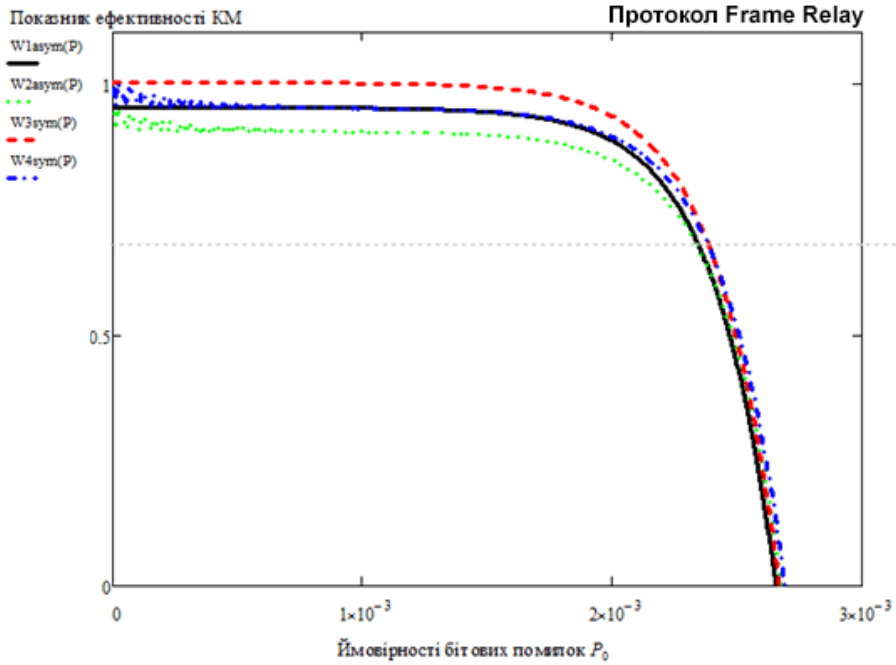

Рисунок 3.2 - Залежність між показником ефективності комп'ютерної мережі W і зміною ймовірності бітових помилок P_0 на основі протоколу Frame Relay

W1asym(P) – Повернення-на-N (асиметричне шифрування);

W2asym(P) – Састре (з вирішальною зворотним зв'язком і позитивною квитанцією) (асиметричне шифрування);

W3asym(P) – Повернення-на-N (симетричне шифрування);

W4asym(P) – Састре (з вирішальним зворотним зв'язком і позитивною квитанцією) (симетричне шифрування).

Проведений аналіз залежностей на рис. 3.1 та рис. 3.2 підтверджує низький показник ефективності спостерігається у протоколу з вирішальним зворотним зв'язком и позитивною квитанцією. Протоколи, які використовують циклічні коди в режимі виявлення помилок і протоколи з вирішальним зворотним зв'язком і позитивною квитанцією є практично однаковими за показниками ефективності комп'ютерної мережі. На відміну від X. 25, Frame Relay повністю усуває всю обробку на мережному рівні. Крім того, Frame Relay використовує тільки частину функцій канального рівня, так звані “основні аспекти”, які включають перевірку помилок кадру, але не вимагають повторної передачі кадра при виявленні помилки. Таким чином, такі традиційні функції протоколу передачі даних як перевірка послідовності кадрів, регулювання розміру “вікна”, механізм підтверджень не використовуються в мережі Frame Relay.

Результатом виключення цих функцій є істотне збільшення продуктивності (тобто числа кадрів, які можуть бути оброблені в секунду за дану вартість апаратних засобів). По тій же самій причині, затримка при використанні методу Frame Relay більш низька, чим в мережах X. 25, тому узагальнений показник ефективності комп'ютерної мережі W при використанні методу Frame Relay дозволяє підвищити його достовірність і продуктивність при обміні даних за рахунок використання цифрових каналів зв’язку з малою ймовірністю виникнення помилки та більшою швидкістю передачі.

3.2. Оцінка показника функціональної ефективності комп'ютерної мережі на основі Frame Relay, в каналах з пам'яттю

Для обліку статистичних властивостей послідовностей помилок в реальних каналах зв'язку розглянемо модель каналу з пам'яттю.

При розрахунках замість ймовірності помилки біта P_0 задаємо наступні параметри:

а) $P_п$ – ймовірність виникнення пакета помилок;

б) $P_ε$ – ймовірність помилки усередині пакета;

в) mln математичне очікування довжини пакета помилок;

г) σln – середньоквадратичне відхилення довжини пакета помилок.

Стратегія (u_1). Значення показника ефективності комп'ютерних мереж, які використовують циклічні коди в режимі виявлення помилок визначається за формулою [49, 55]:

$$W(u_1)=\frac{n^{(u_1)}-t^{(u_1)}}{n^{(u_1)}}\cdot\frac{B^{(u_1)}-\Psi^{(u_1)}}{B^{(u_1)}}\cdot P_{прп}{}^{(u_1)}, \qquad (3.5)$$

Стратегія (u_2). Значення показника ефективності комп'ютерних мереж без зворотного зв'язку при виправленні t-кратної помилки циклічним кодом визначається за формулою [49, 55]:

$$W(u_2)=\frac{n^{(u_2)}-t^{(u_2)}}{n^{(u_2)}}\cdot\frac{B^{(u_2)}-\Psi^{(u_2)}}{B^{(u_2)}}\cdot P_{прп}{}^{(u_2)}, \qquad (3.6)$$

Стратегія (u_3). Значення показника ефективності комп'ютерних мереж з вирішальним зворотним зв'язком і безперервною передачею кадрів "Повернення-на-N" визначається за формулою [49, 55]:

$$W(u_3)=\frac{n^{(u3)}-t^{(u3)}}{n^{(u3)}}\cdot\frac{B^{(u3)}-\Psi^{(u3)}}{B^{(u3)}}\cdot P_{прп}{}^{(u3)}, \quad (3.7)$$

Стратегія (u_4). Значення показника ефективності комп'ютерних мереж з вирішальним зворотним зв'язком і позитивною квитанцією кадрів визначається за формулою [49, 55]:

$$W(u_4)=\frac{n^{(u4)}-t^{(u4)}}{n^{(u4)}}\cdot\frac{B^{(u4)}-\Psi^{(u4)}}{B^{(u4)}}\cdot P_{прп}{}^{(u4)}, \quad (3.8)$$

Для побудови даного графіка були використані наступні дані: $m_{ln} = 10$; $\sigma_{ln} = 2$; $C = 56000$ бит/с; $L = 1000$ км; $V_p = 3\cdot10^8$ м/с; $r = 16$; $t = 8$; $n_1 = 4056$; $n_2 = 4056$; $s = 32$; $Z = 6$; $P_3 = 0{,}95$; $t_{ш\_1} = 0{,}01$ с; $t_{рш\_1} = 0{,}01$ с; $t_{ш\_2} = 100$ с; $t_{рш\_2} = 100$ с; $B_1 = 10^{24}$, $B_2 = 10^{30}$, $\Psi = 10^{15}$; Рп = 0,0000001.

Результати дослідження оцінки показника функціональної ефективності мережі при різних методах управління обміном даними на основі протоколу Frame Relay, в каналах з пам'яттю наведені на рис. 3.3 та рис. 3.4.

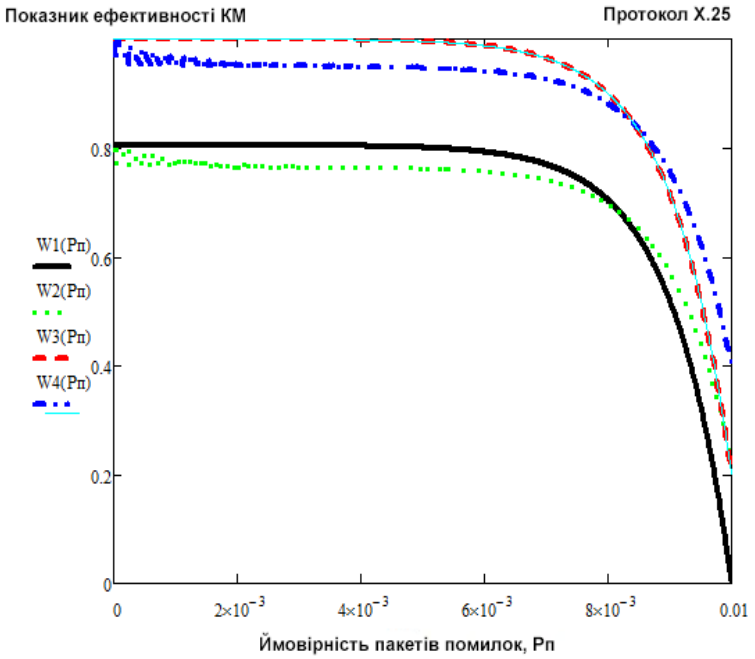

Рисунок 3.3 - Залежність між показником ефективності обміну даними W від імовірності пакетів помилок $P_п$ (протокол X.25)

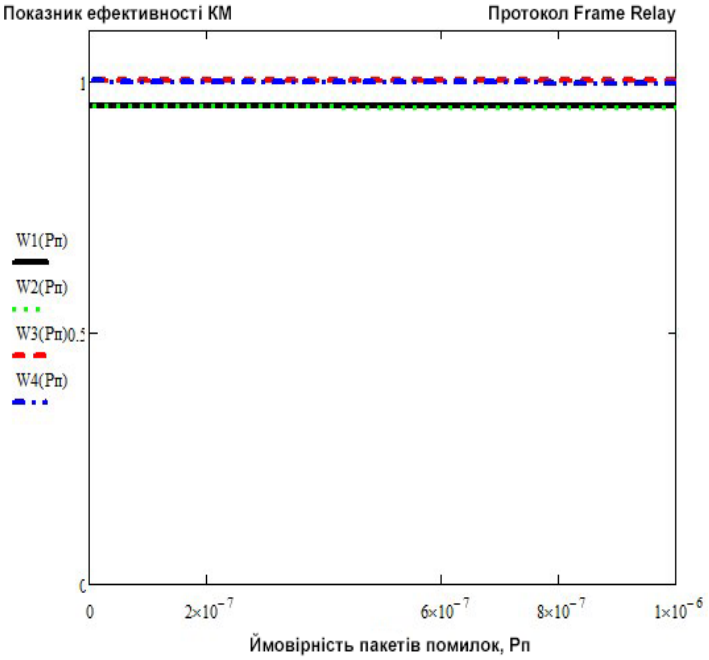

Рисунок 3.4 - Залежність між показником ефективності обміну даними W від імовірності пакетів помилок $P_п$ (протокол Frame Relay)

W1asym(Pп) – Повернення-на-N (асиметричне шифрування);

W2asym(Pп) – Састре (з вирішальним зворотним зв'язком і позитивною квитанцією) (асиметричне шифрування);

W3asym(Pп) – Повернення-на-N (симетричне шифрування);

W4asym(Pп) – Састре (з вирішальним зворотним зв'язком і позитивною квитанцією) (симетричне шифрування).

Проведений аналіз залежностей на рис. 3.3 та рис. 3.4 підтверджує, що найбільш ефективними протоколами управління обміну даними є з вирішальним зворотним зв'язком і безперервною передачею кадрів "Повернення-на-N".

Протоколи, які використовують циклічні коди в режимі виявлення помилок і протоколи без зворотного зв'язку при виправленні t-кратної помилки циклічним кодом мають більш низький показник ефективності. Відновлення кадрів протоколами вищих рівнів може бути неефективним. Єдиний загублений кадр буде вимагати, щоб усі інші кадри були передані повторно. Таке відновлення вимагає додаткових ресурсів у комп'ютерах кінцевих пунктів, а також додаткову смугу пропущення мережі, щоб повторно передати велику кількість кадрів. У підсумку така процедура може привести до більших затримок. Помилка в кадрі

виявляється за допомогою перевірочної послідовності кадру (FCS). У відмінність протоколу X. 25 вузол Frame Relay при виявленні помилки не просить відправника виправити цю помилку повторною передачею кадра. Вузол просто відмовляється від кадра й переходить до обробки наступного. Процедура виявлення помилок і перезапиту покладає на можливості персональних комп'ютерів або робочих станцій, які є відправниками даних. Використання механізму виправлення помилок на високих рівнях не виправдане, якщо використовувати канали, які зашумлені з високою ймовірністю появи помилки. У цей час у світі стає усе більше оптоволоконних ліній передачі з надзвичайно низькими показниками ймовірності появи помилки, тому відновлення даних на таких лініях відбувається досить рідко й не є істотною проблемою. Таким чином, Frame Relay максимально ефективний тільки на цифрових каналах зв'язку (з малою ймовірністю виникнення помилки). Порівняння ефективності обміну даними в комп'ютерній мережі при різних засобах управління обміном на основі протоколів X.25 та Frame Relay представлено в табл. 3.1.

Таблиця 3.1 -Ефективність обміну даними в комп'ютерній мережі при різних засобах управління обміном на основі протоколів X.25 та Frame Relay

Протокол	Коєфіцієнт готовності			
	Без пам`яті		З пам`яттю	
	X.25	Frame Relay	X.25	Frame Relay
Використовують циклічні коди в режимі виявлення помилок	0.80466	0.95067	0,00381	0.95067
Без зворотного зв'язку при виправленні t-кратної помилки циклічним кодом	0.79703	0.95028	0,21937	0.95028
З вирішальним зворотним зв'язком і безперервною передачею кадрів "Повернення-на-N"	0.99995	0.99998	0,19908	0.99998
З вирішальним зворотним зв'язком і позитивною квитанцією кадрів	0.99995	0.9997	0,40490	0.99956

Аналіз результатів табл. 3.1 свідчить, що при розгляді моделі каналу з пам'яттю різко падає показник ефективності обміну даними в КМ при використанні стратегій W2 і W1, протоколи з автоперезапитом (стратегії W3 і W4) задовольняють вимогам узагальненого показника ефективності тільки при використанні симетричних криптоалгоритмів. При використанні протоколів обміну на основі асиметричних криптоалгоритмів вимоги з оперативності знижують узагальнений показник ефективності обміну даними в КМ на 20%. Ефективність обміну даними в КМ при різних засобах управління на основі технології Frame Relay з вирішальним зворотним зв'язком і безперервною передачею кадрів "Повернення-на-N" (з вирішальним зворотним зв'язком і позитивною квитанцією кадрів) забезпечує основні вимоги щодо надійності потенційної можливості доступу до розподілюваних ресурсів усіх комп'ютерів, об'єднаних у мережу, але тільки при використані цифрових каналів зв’язку з малою ймовірністю виникнення помилки при передачі даних. Для збільшення продуктивності КМ на основі технології Frame Relay використовують наступні підходи:

а) Використання тільки програмного забезпечення. Цей підхід часто використовується при додаванні режиму Frame Relay до пакетного комутатора X. 25. У цьому випадку передача кадра виконується тим же самим процесором, який здійснює процедури протоколу X.25. Тому що Frame Relay передбачає меншу обробку кадра, ніж X. 25, продуктивність Frame Relay може бути значно вище, чим X. 25 для тих же самих апаратних засобів.

б) Використання спрощеного характеру обробки в Frame Relay який дає можливість виробникам здійснити деякі кроки обробки кадра на більш високошвидкісних апаратних засобах замість виконання всієї обробки кадра на процесорах загального призначення, необхідних для більш складного X. 25. Тому, додаткова продуктивність Frame Relay може бути досягнута зміною апаратних засобів і програмного забезпечення вузлів.

Таким чином, проведений порівняльний аналіз забезпечення потенційної можливості доступу до розподілюваних ресурсів усіх комп'ютерів, об'єднаних у

мережу на основі міжмережних канальних протоколів X.25 та Frame Relay з різними протоколами зворотного зв'язку на основі використання методики оцінки загального показника ефективності обміну даними показав, що при розгляді моделі каналу з пам'яттю різко падає показник ефективності обміну даними в КМ при використанні стратегій W2 и W1. Протоколи з автоперезапитом (стратегії W3 і W4) задовольняють вимогам узагальненого показника ефективності тільки при використанні методу Frame Relay з цифровими каналами зв'язку в протоколах з вирішальним зворотним зв'язком і безперервною передачею кадрів "Поверенення-на-N" або з вирішальним зворотним зв'язком і позитивною квитанцією з несиметричними криптосистемами, які дозволяють забезпечити потрібні параметри надійності і безпеки комп'ютерної системи. Разом з тим, їх застосування знижує вимоги з оперативності – час формування пакету даних на 20%.

Перспективним напрямом подальших досліджень є оцінка продуктивності Frame Relay в контексті інших особливостей організації мережі, як основною продуктивністю, так і здатністю ефективно й автоматично управляти потоками.

3.3. Дослідження узагальненого показника ефективності передачі даних у комп'ютерних системах і мережах

Оцінимо узагальнений показник ефективності комп'ютерної мережі (Wi) при різних стандартних довжинах кадрів стека. Зафіксуємо показник часової складності криптоалгоритму B = 10^{24} групових операцій; продуктивність обчислювальної системи, доступної криптоаналітику Ψ = 10^{15} групових операцій/с; довжини кадрів виберемо для W1 – 16 байт, для W2 – 128 байта, W3 – 512 байт, W4 – 4096 байт [49]. На рис. 3.5 наведені залежності Wi від імовірності помилки при використанні асиметричних алгоритмів шифрування для забезпечення конфіденційності передачі даних, на рис. 3.6 залежності при використанні симетричних алгоритмів шифрування.

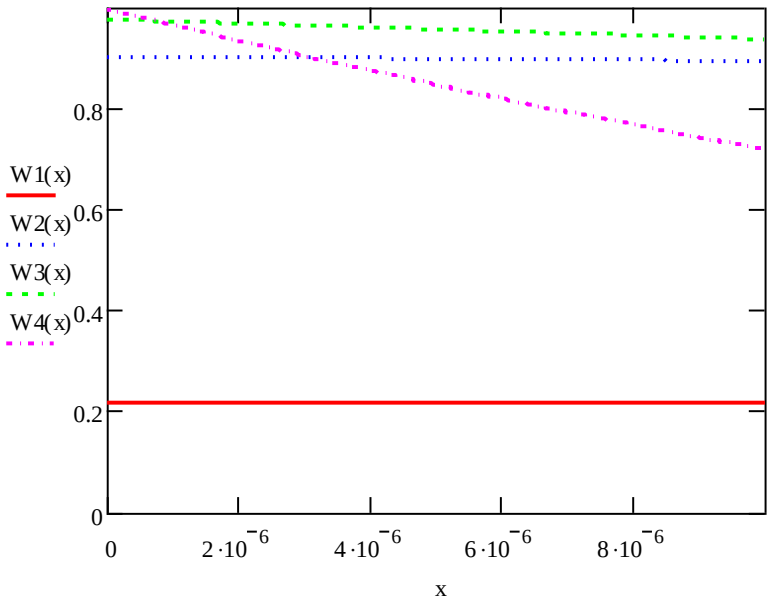

Рисунок 3.5 - Залежність показника ефективності комп'ютерної мережі від імовірності помилки при асиметричних алгоритмах шифрування

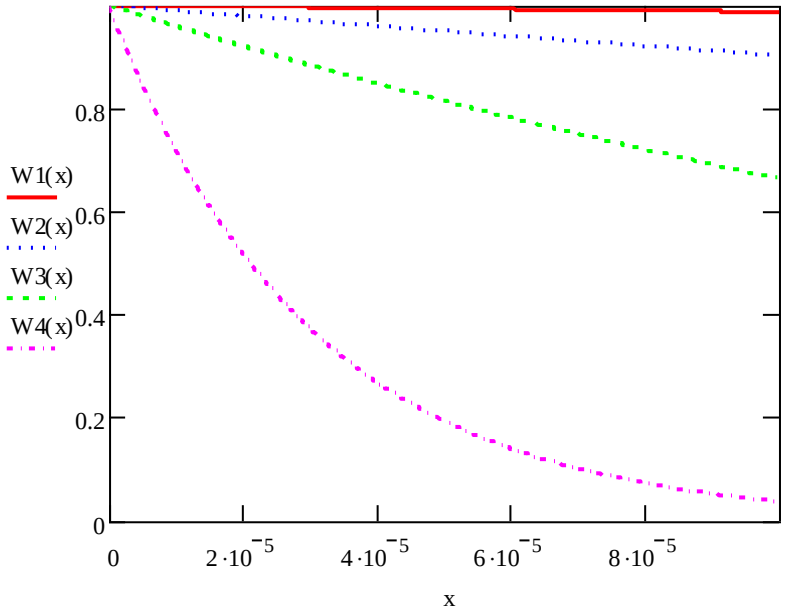

Рисунок 3.6 - Залежність показника ефективності комп'ютерної мережі від імовірності помилки при симетричних алгоритмах шифрування

Наведені на рис. 3.5 – 3.6 залежності свідчать, що при збільшенні стандартних довжин кадрів і ймовірності помилки, узагальнений показник ефективності мережі різко падає, при цьому використання асиметричних схем шифрування значно впливає на показник ефективності мережі, чим при симетричних схемах шифрування.

Далі проведемо дослідження часу доставки кадру при різних ймовірностях помилки в каналі передачі. Зафіксуємо показник часової складності криптоалгоритму B = 10^{24} групових операцій; продуктивність обчислювальної системи, доступної криптоаналітику Ψ1 = 10^{15} групових операцій/с. Імовірність помилки в оптоволоконних кабелях $P_{o1} = 10^{-9}$; імовірність помилки в крученому парі UTP (категорії 3), коаксіальному кабелі $P_{o2} = 10^{-4}$; у повітряних телеграфних лініях зв'язку $P_{o3} = 10^{-3}$; у повітряних телефонних лініях зв'язку $P_{o4} = 10^{-2}$ [49].

На рис. 3.7 наведені залежності часу доставки кадру від імовірності помилки в каналі передачі при використанні асиметричних алгоритмів шифрування для забезпечення конфіденційності передачі даних, на рис. 3.8 залежності при використанні симетричних алгоритмів шифрування [48].

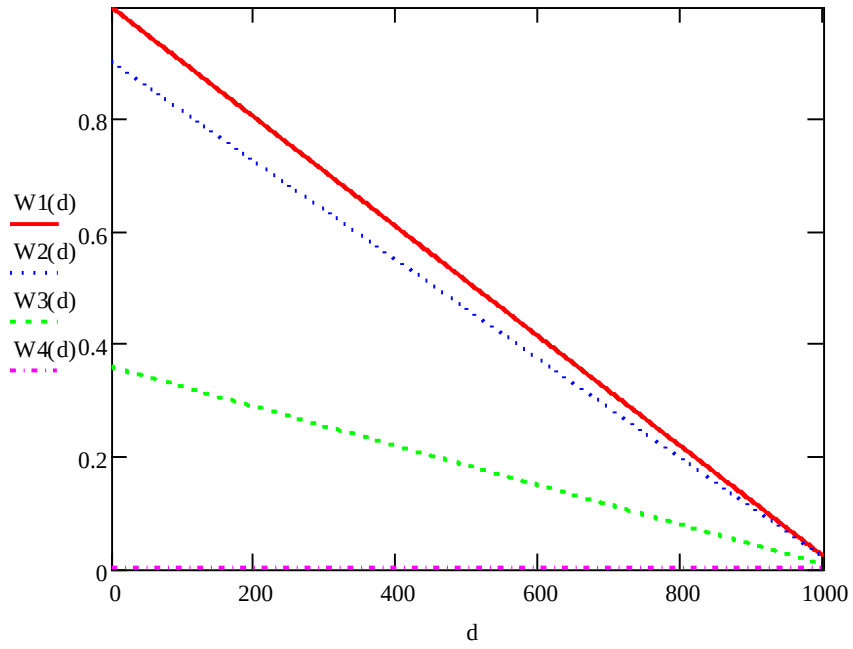

Рисунок 3.7 - Залежність часу доставки кадру від імовірності помилки в каналі передачі при асиметричних алгоритмах шифрування

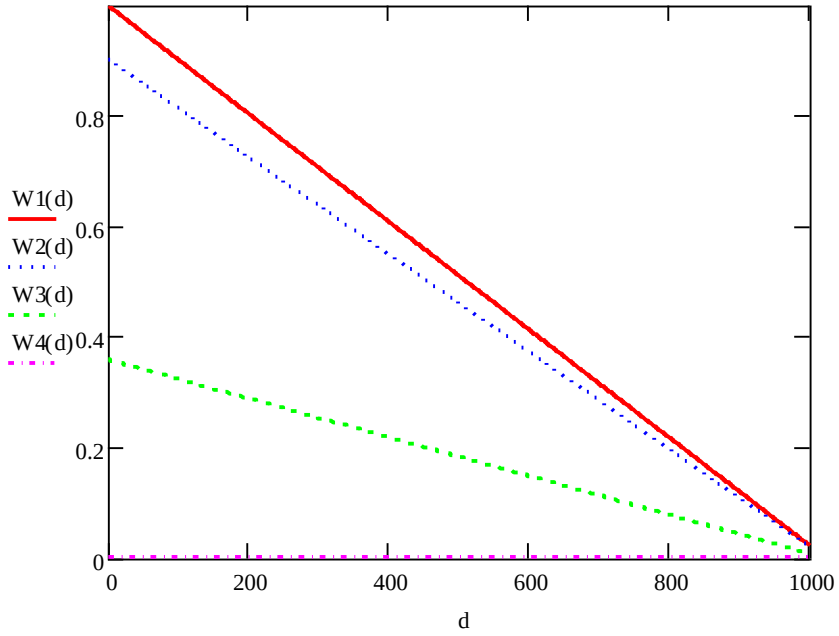

Рисунок 3.8 - Залежність часу доставки кадру від імовірності помилки в каналі передачі при симетричних алгоритмах шифрування

Аналіз наведених на рис. 3.7 – 3.8 залежностей показує, що при використанні каналів передачі з меншою ймовірністю помилки в каналі час доставки кадру значно скорочується [48].

3.4. Висновки до розділу 3

Для проведення дослідження був введений узагальнений показник ефективності комп'ютерної мережі (W_i). При цьому були досліджені залежності коєфіцієнта готовності від довжини кадру, часу доставки кадру при різних ймовірностях помилки в каналі передачі з використанням асиметричних та симетричних алгоритмів шифрування. Для дослідження були використані різні стратегії управління обміном даних.

У результаті дослідження було виявлено, що на коєфіцієнт готовності істотно впливає довжина кадру (оперативність), час шифрування та розшифрування (безпека), ймовірність помилки (надійність). При чому збільшення довжини кадру є причиною збільшення ймовірності помилки, що

призводить до зниження коєфіцієнта готовності. В цифрових каналах ймовірність помилки є низькою і її використання призводить до збільшення коєфіцієнта готовності, що є практичним результатом. Також алгоритми шифрування неістотно впливають на оперативність, тому що збільшується продуктивність обчислювальних технологій та систем на основі закону Мура.

Проведене дослідження показало, що для забезпечення ефективності узагальненого показника необхідно використовувати довжини пакетів стандартів фізичного рівня (стандарт IEEE.802.X) та канали зв'язку UTP5, СТР, оптоволоконні кабелі, які забезпечують ймовірність помилки $10^{-8} – 10^{-12}$. Стратегії з вирішальним зворотним зв’язком і безперервною передачею кадрів “Повернення-на-*N*” та з вирішальним зворотним зв’язком і позитивною квитанцією є найкращими на основі каналів з пам’яттю та без пам’яті та показують необхідні показники.

4 СПЕЦІАЛЬНА ЧАСТИНА

В розділі описано криптографічні методи захисту інформації.

Криптологія (cryptology) є галуззю науки, яка вивчає основні закономірності, протиріччя, принципи, механізми, методи, протоколи, моделі, системи та засоби криптографічного захисту інформації, здійснення криптоаналізу та певною мірою й приховування фактів оброблення інформації та її змісту. Послуги конфіденційності, цілісності та аутентифікації інформації повною мірою можуть бути надані засобом використання симетричних і асиметричних криптографічних перетворень, а також застосуванням криптографічних механізмів і протоколів

4.1 Симетричні криптографічні перетворення

Симетричні криптосистеми – це спосіб шифрування, у якому один й той самий криптографічний ключ, що обирається перед обміном інформації та зберігається в секреті, застосовується як для шифрування, так і для дешифрування, при цьому інформація може шифруватися потоком або блоками.[22] Першим блоковим шифром, що широко використовується на практиці, став DES (Data Encryption Standart). Згодом з'явилося достатня кількість блокових алгоритмів - IDEA, Blowfish, радянський ДЕРЖСТАНДАРТ 28147-89 та інші. При блоковому шифруванні інформація розбивається на блоки й шифрується по 64 або 128 біт, або блоками змінної довжини. При цьому по особливій системі за допомогою циклів переміщення й підстановки (раундів) до кожного з блоків застосовується ключ. Лавинний ефект, що виникає в результаті повторення раундів, призводить до втрати бітів між блоками відкритих і зашифрованих даних.

Як відомо, за класифікацією блокові шифри бувають двох основних видів: шифр перестановки (transposition, permutation, P-Блоки) і шифр заміни (підстановки, substitution, S-Блоки). Шифри перестановки в новій послідовності

переставляють елементи відкритих даних (шифри горизонтальної, вертикальної, подвійної перестановки, ґрати, лабіринти, лозунгові й ін.).

Шифри заміни заміняють за певним правилом елементи відкритих даних на інші елементи. Бувають шифри простої, складної, парної заміни, буквено-складове шифрування й шифри колонної заміни. Шифри заміни діляться на дві групи: моноалфавітні й поліалфавітні. У моноалфавітних шифрах буква вихідного тексту заміняється на іншу, заздалегідь відому букву (код Цезаря). У поліалфавітних шифрах деякий символ вихідного повідомлення в кожному випадку його появи послідовно заміняють одним із символів деякого набору (шифр Відженера, циліндр Джефферсона, диск Уетстоуна, Enigma). У даний час у криптографічних системах використовуються обидва способи шифрування (заміни й перестановки). Вони більше стійкі, ніж системи, що використовують тільки заміни або тільки перестановки.

Більшість сучасних стійких симетричних алгоритмів використовують ключ довжини 64-256 біт (8-32 байта).

Слід зазначити, що крім блокових шифрів активно використовуються і потокові шифри. Вони, як і блокові шифри, використовують симетричний ключ, але виконують шифрування вхідного потоку побайтно або іноді побітно. Ідея потокового шифру полягає в тому, що на основі симетричного ключа виробляється ключова послідовність або гама. Принцип шифрування гамуванням - це генерація гами шифру за допомогою датчика псевдовипадкових чисел і накладення отриманої гами на відриті дані оберненим образом (наприклад, використовуючи додавання за модулем 2).[3] Процес дешифрування даних – це повторна генерація гами шифру при відомому ключу й накладення такої гами на зашифровані дані. Потокові шифри бувають із одноразовим або нескінченним ключем (infinite-key cipher), з кінцевим ключем (система Вернама - Vernam) також на основі генератора псевдовипадкових чисел (ПСЧ).

Потокові шифри, як правило, більше продуктивні, чим блокові й використовуються для шифрування мови, мережного трафіку та інших даних із заздалегідь відомою довжиною. Але потокові шифри не повною мірою підходять

для програмних реалізацій, оскільки шифрують і дешифрують лише по одному біту даних. Блокові ж шифри легко реалізовувати програмно, оскільки вони дозволяють уникнути значних маніпуляцій з бітами й оперують зручними для комп'ютера блоками даних. З іншого боку, потокові шифри протіші за блокові для апаратної реалізації.

Але, якими б складними та надійними не були симетричні криптографічні системи, їхнє слабке місце при практичній реалізації - проблема розподілу ключів. Для того, щоб був можливий обмін конфіденційною інформацією між двома суб'єктами інформаційних відносин, ключ повинен бути згенерований одним з них, а потім певним чином, знову ж у конфіденційному порядку, переданий іншому.

4.2 Асиметричні криптографічні перетворення

Для вирішення цієї проблеми на основі результатів, отриманих класичною й сучасною алгеброю, у сімдесятих роках минулого століття було запропоновано абсолютно нову криптографію – криптографію з відкритим ключем. Її ще називають «відкритою криптографією», «несиметричною криптографією» або «асиметричною криптографією». Саме в асиметричних алгоритмах шифрування для закриття інформації використовують один ключ (відкритий), а для розшифровування - інший (секретний).[3] Ці ключі різні й не можуть бути отримані один з іншого. Першим алгоритмом асиметричного шифрування був алгоритм, створений Вітфілдом Діффі й Мартіном Хеллманом. Діффі й Хелман запропонували для створення криптографічних систем з відкритим ключем функцію дискретного піднесення до спепеня. Автори статті не ставили за мету в даному огляді наводити математичні викладки й формули, однак слід відзначити, що криптографічна стійкість алгоритму Діффі — Хеллмана заснована на передбачуваній складності проблеми дискретного логарифмування. Тобто, необерненість перетворення в цьому випадку забезпечується тим, що досить легко обчислити показникову функцію в кінцевому полі, що

складається з елементів. Обчислення ж логарифмів у таких полях - досить трудомістка операція.[2]

Схожим на алгоритм Діффі — Хеллмана є алгоритм Ель-Гамаля, криптостійкість якого заснована на обчислювальній складності завдання логарифмування цілих чисел у кінцевих полях. Однак, схема Ель Гамаля має певні недоліки, серед яких- відсутність семантичної стійкості та подільність шифру. Як засіб усунення цих недоліків можна використати об'єднання схеми Ель – Гамаля з цифровим підписом Шнорра, що дозволить не тільки шифрувати повідомлення, а й аутентифікувати його.

Найвідомішим несиметричним алгоритмом на сьогоднішній день є алгоритм, запропонований Ривестом, Шаміром і Адельманом, - алгоритм RSA. Безпека алгоритму RSA заснована на труднощі вирішення задачі розкладання чисел на прості множники: як відомо, час виконання найкращих з існуючих алгоритмів розкладання, наприклад, при виходить за межі сучасних технологічних можливостей. Як варіант RSA можливо використовувати криптосистему з функцією Кармайля замість функції Ейлера. RSA може застосовуватися не тільки для шифрування, але й для цифрового підпису. Також він використовується у відкритій системі шифрування PGP і інших системах шифрування (приміром, DarkCryptTC і формат xdc) у сполученні із симетричними алгоритмами. Але важливою проблемою практичної реалізації RSA є генерація великих простих чисел.

Отже, розглянувши основні види криптографічних систем та проаналізувавши їх особливості, можна зробити висновок, що, з огляду на наведені вище критерії, доцільно використовувати асиметричні методи шифрування даних. Хоча несиметрична криптографія є досить повільною у порівнянні зі швидкими і перевіреними часом і практикою симетричних алгоритмів, все ж таки використання несиметричної криптографії радикально спрощує процедуру розподілу ключів між учасниками інформаційних відносин. До того ж, за допомогою відкритого й секретного ключів стає можливим використання електронно-цифрового підпису. Але, в той же час, хоча описані

асиметричні алгоритми дозволяють обійти проблему схованої передачі ключа, необхідність аутентифікації залишається. Без додаткових засобів, один з користувачів не може бути впевнений, що він обмінявся ключами саме з тим користувачем, який йому потрібний. Небезпека імітації в цьому випадку залишається.

4.3 Висновки до розділу 4

В розділі коротко описано суть симетричних та асиметричних криптографічних перетворень та описано різницю між ними.

РОЗДІЛ 5. ОБГРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

Об’єктом дослідження є відділ E-commerce підприємства ТОВ «NitraLabs». Компанія спеціалізується на розробці програмного забезпечення й інтеграції систем керування інформацією.

Мережі frame relay — порівняно нові мережі, що набагато краще підходять для передачі пульсуючого трафіка локальних мереж у порівнянні з мережами X.25, правда, ця перевага виявляється тільки тоді, коли канали зв'язку наближаються по якості до каналів локальних мереж, а для глобальних каналів така якість зазвичай досяжна тільки при використанні волоконо-оптичних кабелів.

Перевага мереж frame relay полягає в їх низькій протокольній надмірності і дейтаграмному режимі роботи, що забезпечує високу пропускну здатність і невеликі затримки кадрів. Надійну передачу кадрів технологія frame relay не забезпечує. Мережі frame relay спеціально розроблялися як суспільні мережі для з'єднання приватних локальних мереж. Вони забезпечують швидкість передачі даних до 2 Мбіт/с.

Дослідимо економічну доцільність розгортання мережі типу frame relay для підприємства ТОВ «NitraLabs». Мережа frame relay складається з перемикачів (switches), з’єднаних цифровим середовищем передачі даних. Кінцеве обладнання, наприклад, маршрутизатори, зв’язуються через FR мережу в одному чи кількох напрямах. У стандартній термінології, перемикачі FR належать до класу пристроїв DCE (Data Communications Equipment), а кінцеве обладнання користувача — до класу DTE (Data Terminal Equipment).

5.1. Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{вi} = q_i \cdot p_i \,, \tag{5.1}$$

де: q_i – кількість витраченого матеріалу і–го виду; p_i – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{вi} \,. \tag{5.2}$$

Розрахунки занесемо у таблицю 5.1.

Таблиця 5.1 - Специфікація обладнання для розгортання мережі frame relay.

№ п/п	Назва обладнання	Ціна	Кількість	Вартість
1.	Коммутатор Cisco SB SF250-48HP 48-port 10/100 PoE Switch (SF250-48HP-K9-EU)	₴ 17 155	3	₴ 51 465
2.	Кабель оптичний FinMark UT004-SM-15	₴ 4,06	1000	₴ 4060
3.	Маршрутизатор Cisco RV345 Dual WAN Gigabit VPN Router (RV345-K9-G5)	₴ 9435	2	₴ 18870
Всього				**₴ 74395**

5.2. Розрахунок норм часу на розгортання мережі frame relay

Ефективне використання часу має велике значення тому, що коефіцієнт корисної дії залежить від оптимального використання часу.

Основні етапи розгортання мережі frame relay:

- розробка топології мережі;
- встановлення обладнання;
- налаштування обладнання.

Для оцінки тривалості виконання окремих робіт використовують нормативи часу.

Витрати часу по окремих операціях технологічного процесу відображені в таблиці 5.2.

Таблиця 5.2 – Операції технологічного процесу та час їх виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Розробка топології мережі	системний адміністратор	26
2.	Встановлення обладнання	інженер	48
3.	Налаштування обладнання	системний адміністратор	52
Разом			126

Загальні затрати часу на реалізацію даної роботи становить 126 години, найбільш трудомістким є налаштування обладнання – 52 годин.

5.3 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України “Про оплату праці” заробітна плата – це “винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу”.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується за виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов’язані з виплатами за фактично

відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

При розрахунку заробітної плати кількість робочих днів у місяці слід в середньому приймати – 24,5 дні/міс., або ж 196 год./міс. (тривалість робочого дня – 8 год.).

Місячний оклад кожного працівника слід враховувати згідно існуючих на даний час тарифних окладів. Згідно закону України «Про Державний бюджет України на 2019 рік», зокрема статтею восьмою мінімальна заробітна плата у погодинному розмірі становить 25,13 грн. Рекомендовані тарифні ставки: системний адміністратор – 150,00-250,00 грн./год., інженер – 100,00-200,00 грн./год.

Основна заробітна плата розраховується за формулою:

$$З_{осн.} = Т_с \cdot К_г \, , \qquad (5.3)$$

де $Т_с$ – тарифна ставка, грн.; $К_г$ – кількість відпрацьованих годин.

Основна заробітна плата буде розраховуватись за формулами 5.4, 5.5.

$$З_{осн.\ сисадм.} = 200{,}00 \cdot 78 = 15600{,}00 \text{ грн.} \qquad (5.4)$$

$$З_{осн.\ інж.} = 150{,}00 \cdot 48 = 7200{,}00 \text{ грн.} \qquad (5.5)$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати.

$$З_{дод.} = З_{осн.} \cdot К_{допл.}, \qquad (5.6)$$

де $К_{допл}$ – коефіцієнт додаткових виплат працівникам, 0,1–0,15 (візьмемо його рівним 0,15).

$$З_{дод} = 22800{,}00 \cdot 0{,}15 = 3420{,}00 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п.} = З_{осн.} + З_{дод.} \quad (5.7)$$

$$В_{о.п.} = 22800{,}00 + 3420{,}00 = 26220{,}00 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи:

- єдиний соціальний внесок ЄСВ (прибутковий податок) – 22%;
- військовий збір – 1,5%.

У сумі зазначені відрахування становлять 23,5 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.} = Ф_{оп} \cdot 0{,}235 \quad (5.8)$$

де $Ф_{оп}$ – фонд оплати праці, грн.

$$В_{с.з.} = 26220{,}00 \cdot 0{,}235 = 6161{,}70 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці наведено у таблиці 5.2.

Таблиця 5.2 – Розрахунки витрат на оплату праці

з/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Відрахування $Ф_{ОП}$, грн.	Всього витрати на плату праці, грн. (6=3+4+5)
		Тарифна	Кількість відпрац	Фактично нарах.			
А	Б	1	2	3	4	5	6
1.	Системний адміністратор	200	78	15600	2340	3666	21606
2.	Інженер	150	48	7200	1080	1692	9972
Всього							**31578**

З таблиці розрахунки витрат на оплату праці видно що всього витрати на плату праці становить 31578 грн.

Надамо основні техніко-економічні та фінансові показники інвестиційного проекту, розрахованого на суму інвестицій 105973 грн.

1) для придбання обладнання необхідна сума 74395 грн;

2) на заробітну плату фахівців з розгортання мережі 31578 грн;

3) тарифи оренди волоконно-оптичних каналів передбачають плату за підключення 23000 грн та щомісячну абонплату 12500 грн.

Період окупності (PP) є одним з найбільш розповсюджених і зрозумілих показників ефективності інвестицій.

Період окупності – це термін, по закінченні якого суми, що надходять, стають прибутком. Упродовж цього періоду відбувається відшкодування капітальних витрат по проекту за рахунок чистого грошового потоку.

Для визначення терміну окупності отриманий чистий грошовий потік сумують до тих пір, поки він не стане рівний величині початкових інвестицій проекту, тобто:

$$\sum_{t=0}^{n} \frac{B_t - C_t}{(1+i)^t} = \sum_{t=0}^{n} \frac{K_t}{(1+i)^t}, \qquad (5.9)$$

Термін окупності інвестиційного проекту для ТОВ «NitraLabs» становить 7 місяців.

Основною позитивною рисою методу оцінки ефективності проектів за періодом окупності є простота. Цей показник корисний також для оцінки ризикованості проекту (чим вищий термін окупності, тим вищий ризик). Особливістю розглянутого показника є те, що він не враховує динаміку подій після того, як проект окупить себе, не вимірює прибутковості інвестиційного проекту, а виявляє його ліквідність.

5.4 Висновки до розділу 5

В розділі обчислено основні економічні показники ефективності розробки та обчислено термін окупності проекту.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Охорона праці

Забезпеченню безпечних умов праці на підприємстві в Україні приділяється підвищена увага. Право кожного громадянина на працю та умови праці, які відповідають умовам безпеки та гігієни, закріплено основним державним документом — Конституцією України, а також підтверджено законодавчими документами, нормами та правилами.

Охорона праці включає систему законодавчих актів та соціально-економічні, технічні, санітарно-гігієнічні, організаційні засоби, які направлені на забезпечення безпеки та створення умов збереження здоров'я та працездатності людини в процесі праці. Навчання та інструктаж працівників з питань охорони праці є складовою частиною системи управління охороною праці підприємства і проводиться з усіма працівниками в процесі їх трудової діяльності.

Забезпечення безпечних і не шкідливих умов праці цілком лягає на власника підприємства. Власник підприємства зобов’язаний дотримуватись санітарних норми і міжгалузевих стандартів.

Під час розробки політики безпеки інформаційної системи, розробка якої вимагає використання ПОЕМ виділяють декілька видів небезпеки :

- порушення роботи кістково-м’язового апарату внаслідок тривалих статичних навантажень при роботі з ПК.

- незадовільні ергономічні характеристики робочого місця внаслідок нераціонального планування робочого місця, що може призвести до механічних травм, уражень електричним струмом та порушень кістково- м’язового апарату;

- нервово-психічні перевантаження внаслідок інцидентів порушень політики безпеки підприємства, контакту колегами по роботі, керівництвом при вирішенні робочих питань, які можуть носити конфліктний характер і призвести до емоційного дискомфорту, внутрішнього роздратування, емоційної нестабільності та захворювань нервової системи;

- негативний вплив недостатнього освітлення робочої зони на зір та продуктивність роботи працюючого, внаслідок несправності освітлювальних приладів або неправильного проектування освітлювальної системи;

- негативний вплив підвищеного рівня шуму на психоемоційний стан працюючого, який пов’язаний з використанням застарілої периферійної техніки, кондиціонерів, копіювальної техніки, освітлювальних приладів;

- неправильні дії персоналу у надзвичайних ситуаціях.

- безпека загоряння у зв'язку із несправністю електричного обладнання, недотримання, або порушення правил протипожежної безпеки обслуговуючим персоналом, що може призвести до пожежі.

- небезпека ураження електричним струмом, внаслідок недотримання правил електробезпеки або виходу з ладу електроприладів;

Діяльність операторів ПОЕМ характеризується тривалою багатогодинною (8 год. і більше) працею в одноманітному напруженому сидячому положенні, малою руховою активністю при значних локальних динамічних навантаженнях, що припадають лише на кисті рук. Такий характер роботи може призвести до появи низки хворобливих симптомів, що об'єднані загальною назвою — синдром довготривалих статичних навантажень (СДСН). Узагальнюючи статистичні дані можна зробити висновок про те, що СДСН може проявлятись втомою, скутістю, болем, судомою, онімінням та ін., локалізуватись у різних частинах тіла (шия, спина, руки, ноги та ін.) і виникати індивідуально з різною частотою (ніколи, рідко, епізодично, щоденно).

Робоче положення "сидячи" забезпечується статичною працею значної кількості м'язів, що дуже втомлює. При такому положенні тіла м'язи ніг, плечей, шиї та рук довгий час перебувають у скороченому стані. Оскільки м'язи не розслабляються, в них погіршується кровообіг.

Тривала робота за ПЕОМ при неправильному, з фізіологічної точки зору, положенні тіла може викликати такі вади постави, як сутулість, викривлення хребта (сколіоз) та ін. У спеціалісті з кібербезпеки при розробці КСЗІ розробка якої вимагає тривалої роботи за ПЕОМ часто виникають наступні симптоми:

- больові відчуття різної сили у суглобах та м'язах кистей рук;
- оніміння та повільна рухливість пальців;
- судоми м'язів кисті;
- поява ниючого болю в ділянці зап'ястка.

Праця за клавіатурою є інтенсивною динамічною роботою кістково-м’язового апарату кистей, одночасно зі статичним напруженням м'язів передпліччя і плеча. Виконання однотипних фізично неважких рухів кистей, що здаються зовсім необтяжливими можуть призвести до поступових функціональних змін, які непомітно розвиваються протягом кількох років.

Для того щоб зменшити вплив на організм довготривалої роботи з клавіатурою і мишею слід дотримуватися певних правила. Коли ви набираєте текст, рука повинна бути зігнута в лікті під прямим кутом (90°С), а при роботі з мишкою стежте, щоб кисть була прямою і лежала на столі якнайдалі від краю. Час роботи з комп'ютером варто обмежити до дійсно необхідного.

Робоче місце оператора ЕОМ при розробці КСЗІ має відповідати «Вимогам щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» Наказу Міністерства соціальної політики України 14.02.2018 № 207.

Робоче місце оператора ЕОМ обладнується робочим столом, кріслом і підставкою для ніг. Висота робочого стола регулюється в межах 0,68—0,80 м, а при відсутності такої можливості має складати 0,72 м. Мінімальна ширина стола 0,6 м, поверхня стола не блискуча. Робоче крісло оператора забезпечується підіймально-поворотним пристроєм з регулюванням висоти сидіння та спинки. На одного працюючого з урахуванням роботи з ПЕОМ має відводитись не менше 6,0 $м^2$ та не менше 20 $м^3$ об’єму приміщення.

А також щоб зменшити навантаження на організм при роботі за ПЕОМ рекомендовано використовувати перерви в роботі 15 хв. через кожні дві години.

Для зниження нервово-емоційного напруження, втомлення зорового аналізатора, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіподинамії, запобігання втомі доцільно деякі перерви використовувати для виконання комплексу вправ, які наведені у Державних санітарних правилах і

нормах роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСПІН 3.3.2.007–98.

Крім того, для профілактики втоми працівників застосовуються специфічні методи, до яких можна віднести засоби відновлення функціонального стану зорового та опорно-рухового апарату, підсилення мозкового кровообігу, оптимізацію розумової діяльності.

В робочому приміщені показники мікроклімату відповідають встановленим санітарним санітарно-гігієнічним вимогам ДСН3.3.6-042-99 «Санітарні норми мікроклімату виробничих приміщень», ГОСТ 12.1.005-88 (1991) «ССБТ.

- у теплий період року: температура +23-+25С; відносна вологість: 40- 60%; швидкість переміщення повітря: 0,3 м/с.

- у холодний період року: температура +20-+24С; відносна вологість: 40-60%; швидкість переміщення повітря: 0,1 м/с;

Для живлення обладнання, що використовується в приміщені є споживачем електроенергії, що живиться від змінного струму 220 В від мережі з заземленою нейтраллю. Із цієї причини при роботі з електроприладами існує потенційна небезпека ураження людини електричним струмом.

Тому для захисту людини від ураження електричним струмом мають бути виконанні вимоги з ГОСТ 12.2.007.0-75* (2001) «ССБТ. Изделия электротехнические. Общие требования безопасности».

6.2 Безпека в надзвичайних ситуаціях

6.2.1. Фактори виробничого середовища і їх вплив на життєдіяльність людини

Деякі фактори праці, умови і види зайнятості (тривалість робочого дня, тижня, ступінь важкості праці, поєднання декількох видів зайнятості) носять постійний характер при впливі на людину і пов'язані з його фізичним і психічним здоров'ям. Вони можуть впливати на здоров'я поряд з іншими соціальними чинниками.

Трудовий процес здійснюється в певних умовах виробничого середовища, що характеризуються сукупністю елементів та факторів матеріально-виробничого середовища, що впливають на працездатність та стан здоров'я людини в процесі роботи. Виробнича середовище й фактори трудового процесу становлять в сукупності умови праці.

На здоров'я людини, її життєдіяльність великий вплив мають небезпечні і шкідливі фактори.

Небезпека - це наслідок такої дії деяких факторів на людину, яке при їх невідповідності фізіологічним характеристикам останнього зумовлює феномен самої небезпеки. Небезпечний фактор - це дія на людину, що в певних умовах призводить до травми, а в окремих випадках - до раптового погіршення здоров'я або до смерті.

Шкідливий фактор - це дія на людину, яке в певних умовах призводить до захворювань або зниження працездатності.

Небезпечні та шкідливі фактори, що впливають на людину, діляться на три групи: активні, пасивно-активні і пасивні.

До активних належать фактори, що можуть вплинути на людину, впливаючи своєю енергією:

- механічні, що характеризуються кінетичною і потенціальною енергією і механічним впливом на людину; до них відносяться кінетична енергія рухомих елементів, потенційна енергія; шум; вібрація; прискорення; гравітаційне тяжіння; невагомість; статичне напруження; дим, туман, пил в повітрі; аномальний барометричний тиск та ін .;
- термічні, що характеризуються тепловою енергією та аномальною температурою; до них належать температура нагрітих і охолоджених предметів і поверхонь, температура відкритого вогню і пожежі, температура хімічних реакцій і інших джерел; до цієї групи належать також аномальні мікрокліматичні параметри - вологість, температура і рухомість повітря, що призводять до порушення терморегуляції організму;

- електричні: електричний струм, статичний електричний заряд, електричне поле, аномальна іонізація повітря;

- електромагнітні: радіохвилі, видиме світло, ультрафіолетові та інфрачервоні промені, іонізуючі випромінювання, магнітні поля;

- хімічні: їдкі, отруйні речовини, а також порушення природного газового складу повітря, наявність шкідливих домішок у повітрі;

- біологічні: небезпечні властивості мікро- і макроорганизмов, продукти життєдіяльності людей і інших біологічних об'єктів;

- психофізіологічні: стрес, втома та ін.

До пасивно-активної групи належать фактори, що активізуються за рахунок енергії, носіями якої є людина або обладнання: гострі нерухомі предмети, малий коефіцієнт тертя, нерівність поверхні, по якій переміщується людина і машина, а також нахил і підйом.

До пасивних належать ті фактори, які впливають опосередковано, небезпечні властивості яких пов'язані з корозією матеріалів, накипом, недостатньою міцністю конструкцій, та ін. Формою прояву цих факторів є руйнування, вибухи та інші види аварій.

Істотне значення для продуктивності праці і охорони здоров'я мають спрямованість виробничої діяльності, конкретні виробничі операції, знаряддя праці, форми організації праці та ін. Кожен з цих показників вимагає певних фізичних і психофізіологічних якостей.

Наприклад, для роботи на малих обчислювальних машинах і комп'ютерах необхідна тонка координація пальців рук, витривалість зорових аналізаторів. При колективній роботі необхідні розвинені комунікативні здібності і т.д.

Продуктивність праці, стан здоров'я та рівень працездатності людини значною мірою залежать від впливу факторів зовнішнього виробничого середовища.

Ці фактори окремо і особливо в комплексі можуть надавати несприятливий вплив на організм людини в процесі виробничої діяльності. До них, зокрема, відносяться метеорологічні умови (мікроклімат), шум, вібрація, заколисування,

радіаційне випромінювання, освітленість робочого місця, психологічна напруженість, режим праці та ін.

Метеорологічні фактори характеризуються поєднанням температури, відносної вологості і швидкості руху повітря. Систематичні відхилення від нормального (комфортного) метеорологічного режиму у виробничих приміщеннях призводять до хронічних простудних захворювань, захворювань суглобів, теплових ударів, судом, стресових станів. Порушується тепловий баланс, знижується здатність до розумової та фізичної роботі, коли змінюється температура зовнішнього середовища.

Фізичне тренування і загартування підвищують стійкість організму людини до різко мінливих погодних умов, до зміни мікроклімату, значно скорочують період акліматизації і сприяють більш швидкому відновленню розумової та фізичної працездатності після втоми. Різка зміна барометричного тиску, наприклад, може супроводжуватися порушенням функції вестибулярного апарату і середнього вуха, втратою координації рухів. Негативний вплив на органи слуху і нервову систему надає також високий рівень шуму. Під впливом вібрації може розвиватися так звана вібраційна хвороба, коли знижується гострота зору, тактильна, теплова та больова чутливість, уражаються кровоносні судини, відбуваються небажані зміни в суглобах і т.д.

Фізична підготовленість набуває великого значення при необхідності адаптуватися до вібрації і закачування, які можуть істотно знижувати продуктивність праці і навіть приводити до повної втрати працездатності.

Освітлення робочого місця - один з найважливіших факторів трудової діяльності. Головні проблеми, пов'язані з органами зору, на виробництві стосуються адекватності і зручності освітлення. Достатня (оптимальна) освітленість робочого місця позитивно впливає на органи зору, знижує втому. Незадовільне освітлення викликає передчасне стомлення, очні хвороби, головні болі і може бути причиною травматизму

6.2.2 Вплив електромагнітного випромінювання

Електромагнітні випромінювання розрізняють за частотою коливань або довжиною хвилі. Найдовші хвилі – це коливання промислової або іншої звукової частоти, а також ультразвукові. Вони мають довжину хвилі понад 10 км (або частоту менш як 30 кГц), довгі і середні радіохвилі (від 10 км до 100 м або до 3 МГц) застосовують не тільки в радіотехніці, а й для плавлення металу, гартування деталей, сушіння деревини та ін. У промисловій електротермії для нагрівання діелектриків використовують також короткі радіохвилі (завдовжки 100—10 м або до 30 МГц), що, як і ультракороткі (10–1 м або до 300 МГц), належать до коливань ультрависокої частоти (УВЧ).

До електромагнітних випромінювань належать також випромінювання оптичного діапазону, рентгенівські промені та радіоактивне випромінювання.

При промисловій частоті спеціальні заходи захисту від дії електричних полів доводиться застосовувати тільки під час обслуговування електроустановок напругою 330—500 кВ і вище. Тоді використовують спеціальні костюми і взуття, які дають можливість навідним зарядам стікати в землю без неприємних для людини відчуттів, а також екрануючі металеві козирки над робочими місцями (приводами роз'єднувачів та ін.). Використовувати ці козирки і костюми (так звані індивідуальні екрануючі комплекти) обов'язково тільки в розподільних пристроях напругою 750 кВ, під час робіт на опорах ЛЕП – 330–750 кВ або ж при напругах понад 5 кВ/м, коли перебування у такому електричному полі повинно тривати більше за гігієнічно допустимий час (понад 3 год при 5–10 кВ/м, 1,5 год при 10–15 кВ/м, 10 хв при 15–20 кВ/м і 5 хв при 20–25 кВ/м).

Тривале перебування на землі під ЛЕП теж шкідливе. Під крайньою фазою в середині прольоту на ЛЕП напругою 330 кВ напруга становить 6 кВ/м, а на ЛЕП-500 – 14 кВ/м. Тому під час польових робіт під ЛЕП напругою 330 кВ і вище треба враховувати цю обставину і краще використовувати трактори та інші машини з металевою кабіною або з встановленими зверху і з боків екранами, які виготовлені з металевої сітки.

Автомашини і трактори на пневматичних шинах заряджаються в електричному полі ЛЕП зарядами хоч і малого значення, але напругою, що становить кілька кіловольт. Дотик до них людини, яка стоїть на землі, не смертельний, але спричиняє болісний удар розрядним струмом, що може призвести до мимовільних рухів, а отже, і до механічних травм від дотику до рухомих частин та ін. Тому бажано не залишати машину під ЛЕП, якщо треба зупинитися, то до виходу з кабіни заземлити машину спеціальним заземлювачем (у вигляді гирі з штирем), прикріпленим до машини гнучким проводом. Заземлення може бути постійним у вигляді диска або сошника. Електроогорожі під ЛЕП 330–750 кВ краще взагалі не робити, бо в протяжних металевих частинах наводяться такі електрорушійні сили (ерс), що, наприклад, електроогорожа завдовжки 300 м навіть під ЛЕП напругою 220 кВ може при замиканні на опір 1000 Ом (людина) створити струм 10 мА, а на опір 500 Ом (корова) – 30 мА. Провід для виноградників, оскільки він не ізолюється спеціально від землі, порівняно безпечний, особливо при розташуванні перпендикулярно до траси ЛЕП і заземленні на кінцях.

Для захисту робітників від випромінювання високої частоти (ВЧ) і УВЧ застосовують екранування листовим металом високої електропровідності завтовшки не менш як 0,5 мм. Отвори в екрані для штурвалів і кнопок екранують металевою сіткою з вічками не більш як 4 х 4 мм. Екрани заземлюють. Максимально допустима напруженість електромагнітного поля випромінювання ВЧ і УВЧ на робочих місцях, згідно з ГОСТ 12.1.006-76, для частот 60 кГц дорівнює 50 В/м – 3 МГц, 20 В/м для частот 3–30 МГц, 10 В/м для частот 30–50 МГц і 5 В/м для частот 50–300 МГц. Тільки для індукційних плавильних печей і нагрівальних індикаторів тимчасово допускають 10 В/м через технічні труднощі повного екранування їх.

Напруженість магнітного поля не має перевищувати 5 А/м для частот 60 кГц – 1,5 МГц і 0,3 А/м для 30–50 МГц.

Тривалий вплив електромагнітних полів ВЧ і УВЧ з напругою, більшою за допустиму, призводить до функціональних змін у печінці, селезінці та особливо в

центральній нервовій системі, які виявляються в головному болі, підвищеній втомлюваності, порушенні сну, дратівливості, в уповільненні пульсу, зниженні кров'яного тиску. При дії випромінювань УВЧ також підвищується температура тіла. Коливання, які мають довжину хвилі від 1 м до 1 мм (частотою до 300 тис МГц), називаються надвисокочастотними (НВЧ), їх використовують у радіолокації і для деяких приладів. Розроблявся, наприклад, прилад для вимірювання жирності молока, який використовував НВЧ випромінювання.

Гігієнічні норми НВЧ випромінювань визначаються в одиницях густини потоку потужності (вектора Пойнтінга) і залежить від тривалості впливу на людину: 0,1 Вт/м^2 при опроміненні протягом усього робочого дня; 10 Вт/м^2 при опроміненні протягом 20 хв. на день. Але при цьому треба працювати в захисних окулярах, які зроблені з мідної сітки та екранують очі. Без цих окулярів уражується кришталик ока (утворюється катаракта).

Екрануванням захищаються і від інфрачервоних (теплових) променів (з довжиною хвилі 100–0,76 мкм).

Видиме світло має довжину хвилі від 0,76–0,38 мкм, а ультрафіолетове проміння – від 0,38 до 0,005 мкм, тобто до 5 нм. Ці промені виникають, наприклад, при електрозварюванні і можуть уражати очі (електроофтальмія) або спричинити запалення шкіри відкритих частин тіла. Для захисту очей і шкіри обличчя застосовують щитки зі світлофільтрами, а для захисту шкіри рук – рукавиці.

Рентгенівські промені (від 5 до 0,004 нм) використовують в установках промислової рентгеноскопії. Вони випромінюються і під час випробування кабелів та електроустаткування випрямленим струмом високої напруги. Застосований тут високовольтний кенотрон є джерелом м'якого рентгенівського випромінювання (тобто довжина хвилі понад 0,01 нм) і має бути екранований. Для екрана досить мати залізний лист завтовшки 0,5–1 мм. У промисловій рентгеноскопії застосовують також фартухи, рукавиці, шапочки з просвинцьованої гуми. Дозу рентгенівського або будь-якого іншого іонізуючого випромінювання, поглинутого тканинами опроміненого тіла, вимірюють

кількістю поглинутої тілом енергії в джоулях на 1 кг речовини. Вживають також поняття: величина дози рентгенівського випромінювання (А/кг).

Наприклад, при 36-годинному робочому тижні в осіб, зайнятих випробуванням електроустановок з використанням кенотронів, величина дози рентгенівського випромінювання у будь-якій точці на відстані 5–10 см від захисного кожуха кенотрона або всього випробувального пристрою не має перевищувати 20,6 * 1012 А/кг. Останнім часом почали застосовувати замість кенотронів високовольтні напівпровідникові випрямлячі, які усувають появу рентгенівського випромінювання.

Порушення санітарно-гігієнічних норм призводить до зміни складу крові і функціональних порушень центральної нервової системи, які виявляються в дратівливості, сонливості або безсонні, пітливості, головних болях, ослабленні пам'яті, загальній слабості. Порушується робота серцево-судинної системи. При великих дозах може виникнути променева хвороба, тобто порушення нормального кровотворення, розлад нервової системи, травлення, що супроводжуються загальною слабістю, болями і зниженням опірності проти інфекції. М'яке рентгенівське випромінювання призводить насамперед до місцевого впливу на опромінені ділянки тіла; може мутніти кришталик ока (катаракта), випадати волосся.

Гамма-промені випромінюються радіоактивною речовиною. Вони мають довжину хвилі від 4 до 0,1 нм. Як і два інших види ядерних випромінювань (альфа- і бета-випромінювання, які є вже не потоком електромагнітних хвиль, а потоком заряджених частинок), гамма-випромінювання дедалі ширше застосовують у науці і техніці, зокрема в гамма-дефектоскопії та в автоматиці. Гамма-випромінювання використовують також і для передпосівного опромінювання насіння, знищення комах-шкідників, опромінювання харчових продуктів, щоб подовжити строки зберігання та для знешкодження сільськогосподарської сировини.

Альфа-випромінювання мають дуже малу проникну здатність і при зовнішньому опромінюванні затримуються зовнішнім шаром шкіри без помітної

шкідливої дії. Проте потрапляння альфа-частинок всередину організму з повітрям або їжею дуже небезпечне.

Бета-промені мають невелику проникну здатність, але шкідливо діють на шкіру й очі. Проникна здатність гамма-променів набагато більша. Це випромінювання може спричинити променеву хворобу. Однак додержуючись санітарних правил роботи з радіоактивними речовинами та джерелами іонізуючих випромінювань, можна тривалий час працювати без шкоди для здоров'я.

Нижче наведено максимально допустимі поглинуті тілом дози рентгенівського, гамма- і бета-випромінювань. Для альфа-випромінювань вони в 10 разів вищі. Норми різні для персоналу, що обслуговує установки і апарати, які створюють випромінювання, і для окремих осіб, що не зв'язані з обслуговуванням цих установок, але зазнають дії випромінювання.

Для першої групи тканин (червоний кістковий мозок, статеві залози або взагалі усе тіло) допускається для персоналу не більш як 30 мДж/кг на 13 тижнів (квартал) і не більш як 50 мДж/кг на рік, а для інших осіб – 5 мДж/кг на рік; для другої групи тканин і органів (це будь-який орган тіла, крім зазначених в інших групах) – 80 мДж/кг на квартал і 150 мДж/кг на рік для персоналу або 15 мДж/кг для інших осіб; для третьої групи тканин (щитовидна залоза, кісткова тканина і шкіра, крім частин тіла, які належать до зазначених у наступній групі) – 150 мДж/кг на квартал і 300 мДж/кг на рік для персоналу або 30 мДж/кг для інших осіб віком старше 16 років (для тих, хто ще не досяг 16 років – 15 мДж/кг на рік); для четвертої групи органів (повністю кисті, передпліччя, кісточки і ступні) – 400 мДж/кг на квартал і 750 мДж/кг на рік для персоналу або 75 мДж/кг для інших осіб.

Сумарна доза опромінення за ряд років органів першої групи у персоналу, що обслуговує установки і апарати, які створюють іонізуюче випромінювання, не має перевищувати Б = 50 (М – 18), де N – вік (років).

Захист від радіоактивних випромінювань полягає в застосуванні захисних кожухів або екранів, спецодягу, індивідуальних захисних засобів. Важливу роль відіграє також дозиметричний і лікарський контроль.

.

6. 3 Висновок до шостого розділу

В розділі про охорону праці, багато уваги було зосереджено на правилах роботи з комп’ютером, а також важливість емоційного стану працівника і сприятливих умов у приміщенні де буде здійснюватися робота.

7 ЕКОЛОГІЯ

7.1 Статистичні показники екологічних явищ

Статистичний показник - узагальнююча характеристика для кількісного виміру екологічних явищ. Кожен з статистичних показників має три характеристики:

- визначеність, кількість і якість;
- модель розрахунку, екологічний зміст і числове значення змісту;
- адекватність відображення, точність вимірювання і достовірність інформації

За допомогою статистичних показників вирішується одна з головних задач статистики: визначається кількісна сторона явища чи процесу у поєднанні з якісною стороною.

Показник — кількісно-якісна характеристика соціально-екологічних явищ і процесів. Якісна сторона показника відображає сутність явища або процесу в конкретних умовах місця й часу, а кількісна - розмір, абсолютну або відносну його величину.

Якісний зміст показника залежить від суті досліджуваного явища (процесу) і відображається у назві показника (викиди, скиди, відходи) та поєднується з його числовим вираженням за допомогою моделі показника.

Різноманіття явищ громадського життя, їхніх властивостей, руху, відносин обумовило й різноманіття статистичних показників. Показники поділяються на види залежно від їх аналітичної функції, способу обчислення та ознаки часу, виконання своїх функцій. Існує багато видів показників, що потребує їх упорядкування і класифікації.

Класифікація - це розчленовування показників за суттєвими ознаками на групи. Ознаками класифікації виступають: спосіб вирахування, час, до якого відносяться показники, характер взаємозв'язку показників.

Класифікація показників за способом, часом і характером:

Первинні - визначаються шляхом зведення та групування даних і подаються у формі абсолютних величин (наприклад, кількість джерел забруднення, об'єм викидів чи скидів).

Похідні - обчислюються на базі первинних і мають форму середніх або відносних величин (наприклад, викиди в розрахунку на одну особу або одиницю площі).

Інтервальні - характеризують явище за певний період часу (місяць, квартал, рік): наприклад, середньомісячні викиди забруднюючих речовин в атмосферне повітря.

Моментні - дають кількісну характеристику явищ на певний момент часу: на початок або кінець року): наприклад, залишок обігових коштів на початок місяця.

Інтервальні та моментні показники можуть бути як первинними, так і похідними.

Адитивні (підсумовуючі) показники - це всі абсолютні показники, що здатні підсумовуватися; неадитивні (моментні, відносні, середні) показники не можна підсумовувати.

Індивідуальні показники характеризують окрему одиницю статистичної сукупності - окреме явище, об'єкт і т.п.; групові (частки) -групу одиниць того самого виду; загальні (зведені) - всю їхню сукупність.

Серед статистичних показників окрему групу становлять взаємообернені показники — пара характеристик одного і того явища, але прямий показник змінюється в напрямі зміни явища, а обернений — у протилежному напрямі. Наприклад, щільність викидів забруднюючих речовин (прямий) та стан атмосферного повітря (обернений).

Показники, що характеризують галузь народного господарства з кількісної сторони (за кількісною ознакою), називають галузевими, народне господарство у цілому - народногосподарськими, а окремі територіальні підрозділи - територіальними або регіональними.

Всі статистичні показники поділяються перш за все на результативні і факторні. Результативні показники - величини, які є наслідками дії певних факторів. Факторні показники - величини, які виступають причиною зміну результативних показників

Узагальнюючі показники — величини, які отримують у результаті обробки статистичних матеріалів.

Екстенсивні показники - це об'ємні показники, що характеризують об'єм ознаки або сукупності. Інтенсивні показники - це якісні показники визначені в розрахунку на одиницю сукупності або на одиницю другого показника.

Основні показники - це кількісні характеристики певних суттєвих властивостей об'єктів чи процесів. Другорядні показники - це характеристики окремих несуттєвих властивостей об'єктів.

Укрупненні показники - це узагальнюючі характеристики об'єкта.

Деталізовані показники - це характеристики окремих часткових властивостей об'єктів.

Комплексні показники - це інтегровані показники за рядом ознак.

Прості показники - це характеристики певних ознак об'єкта.

Сукупність статистичних показників називається системою показників.

Щоб статистичні показники правильно характеризували явище, що розглядається, необхідно виконувати такі вимоги:

- спиратися при їх побудові на положення економічної теорії, статистичну методологію, досвід статистичних робіт;
- добиватися повноти статистичної інформації як за охопленням одиниць об'єкта, так і за комплексним відображенням усіх сторін процесу, що вивчається;
- забезпечувати зіставлення статистичних показників за рахунок подібності вихідних даних за часом та у просторі;
- забезпечувати точність та надійність вихідної інформації для достовірності змісту процесу, що досліджується.

Статистичний показник - найважливіша категорія статистичної науки. Він служить узагальнюючою кількісною характеристикою властивостей сукупності загалом чи її частин зокрема.

7.2 Моніторинг довкілля та система спостережень за впливом на довкілля антропогенних факторів

Для аналізу та прогнозування розвитку екологічної ситуації у глобальному і регіональному масштабах необхідні знання різноманітних геофізичних процесів, антропогенних ефектів, а також факторів, що їх спричинюють. Вивчення й оцінювання негативних наслідків антропогенних дій з метою запобігання або зменшення збитків є однією із найважливіших умов організації економіки, гарантування екологічної безпеки. Проблема людського втручання у природні процеси особливо актуалізувалася з розвитком науково-технічного прогресу в середині XX ст. Саме тоді антропогенний вплив почав зумовлювати глобальні, іноді незворотні наслідки.

Антропогенні фактори − форми господарської діяльності людини, що впливають на організми чи екосистеми, природне середовище загалом. Дію антропогенних факторів на біосферу оцінюють, зважаючи на зміни властивостей основних її елементів, геофізичні, геохімічні, біологічні, екологічні наслідки їх впливу (порушення в екосистемах), а також на зміни стану здоров'я людей. Кожна з груп антропогенних факторів зумовлює своїм впливом такі перетворення у біосфері:

− викид у біосферу хімічно та фізично активних речовин спричинює зміни стану і властивостей атмосфери; великомасштабні перетворення циркуляції в атмосфері й океані; порушення стійкості земних та водних екосистем; зниження працездатності людей;

− викид у біосферу інертного матеріалу (аерозольних частинок) зумовлює зміни складу і властивостей вод суші; погоди і клімату; екосистеми світового океану; погіршення настрою у людей;

− пряме нагрівання атмосфер спричиняє зміни складу і властивостей вод світового океану; перерозподіл та зміни відновлюваних абіотичних 15 (водних, кліматичних) ресурсів; негативні генетичні ефекти; хвороби, стресові ситуації;

− фізичні дії, які змінюють поверхню суші та рослинний покрив (ерозія, пожежі) виявляються у трансформації стану біоценозу і біогеофізичного середовища; озонового шару (зміна проходження ультрафіолетового випромінювання, радіохвиль); зникненні та генетичних змінах існуючих видів, появі нових;

− біологічна дія (розвиток агроценозів) виражається у зміні літосфери, прозорості атмосфери, проходженні сонячного випромінювання; зменшенні біопродуктивності екологічних систем і кількості популяцій; деградації лісів; скороченні тривалості життя;

− знищення ресурсів (невідновних і відновних) призводить до зміни кріосфери (оболонки землі, у складі якої наявний лід); ерозії земної поверхні, коливань альбедо (відношення кількості променистої енергії сонця, відбитого від поверхні будь-якого тіла, до кількості спрямованої на цю поверхню енергії); деградації ґрунтів; зниження темпів приросту населення;

− антропогенні впорядковані потоки речовин зумовлюють зміну геофізичних властивостей великих систем; властивостей суші й ґрунту; здатності біосфери до відновлення ресурсів, виснаження невідновних ресурсів; зменшення чисельності населення; порушення природних кругообігів.

Спостереження у межах системи моніторингу за дією основних антропогенних факторів і процесів, які вони зумовлюють, групують за такими напрямами:

1. Спостереження за локальними джерелами забруднення й забруднюючими факторами. Вони здійснюються на територіях окремих об’єктів (підприємств, населених пунктів, ділянок ландшафтів тощо) у формі контролювання кількісного та якісного складу забруднюючих речовин, що містяться у викидах і скидах, місцях їх зберігання.

2. Спостереження за станом навколишнього природного середовища. Зосереджені такі спостереження на відстежуванні геофізичних (природні явища катастрофічного характеру: вулкани, землетруси, ерозії, цунамі), фізико-географічних (розподіл суші та води, рельєф, природні ресурси, народонаселення, урбанізація), геохімічних (кругообіг речовин, хімічні, шумові забруднення атмосфери), хімічних (хімічний склад атмосферних домішок природного й антропогенного походження, опади, поверхневі та підземні води, ґрунт, рослини, основні шляхи поширення забруднювачів) процесів і змін з фіксуванням відповідних даних.

3. Спостереження за станом біотичної складової біосфери. У їх процесі відстежують реакції біоти на різні фактори, тобто реакції окремих організмів, популяцій, або угруповань (груп рослинних і тваринних організмів , що постійно чи тимчасово співіснують на певних територіях),

4. Спостереження за реакцією великих систем (клімату, Світового океану, біосфери).

Моніторингу потребують фізичні, хімічні та біологічні показники. Для встановлення динаміки змін стану біосфери замірювання повторюють через певні проміжки часу, а важливі показники відстежують безперервно. Система спостережень може полягати в організації замірювань у конкретних точках (на станціях) або на обширній території й отриманні інтегральних показників. Часто ефективним є комбіноване використання обох підходів. В організації спостережень активно використовують авіаційні та супутникові засоби. Отримані за їх допомогою результати аналізують з огляду на зміни середовища, а також на відповідні реакції біоти, що виникають унаслідок антропогенного впливу. Для цього важливо знати початковий (фоновий) стан середовища, тобто стан, який підтримувався до суттєвого втручання людини. Отже, основною метою моніторингу довкілля є спостереження за змінами в екосистемах, зумовленими антропогенними факторами.

7.3 Висновки до розділу 7

В розділі наведена інформація про статистичні показники екологічних явищ та моніторинг довкілля та систему спостережень за впливом на довкілля антропогенних факторів.

ВИСНОВКИ

У даній роботі були проаналізовані відомі методи забезпечення безпеки та достовірності інформації в комп`ютерних системах та мережах на основі каналів з пам`яттю та без пам`ятті. В процесі проведення дослідження були враховані всі можливі дії та виконанні основні задачі: аналіз умов функціонування та обґрунтування вимог, що пред'являються до сучасних комп'ютерних систем та мереж; аналіз протоколів канального рівня глобальної обчислювальної мережі та оцінка ефективності обміну даними в комп'ютерній мережі при різних засобах управління обміном даних.

Під час дослідження був проведений аналіз локальних та глобальних обчислювальних мереж, канального рівня мережевої моделі OSI для ЛОМ та ГОМ, був наведений закон Мура. Були розглянуті протоколи канального рівня глобальної обчислювальної мережі – X.25, Frame Relay та протокол ATM, наведені відповідні структурні схеми.

У результаті даного дослідження був визначений найліпший протокол забезпечення безпеки та достовірності переданої та оброблюваної інформації в комп'ютерних системах та мережах – Frame Relay. Була розрахована оцінка показника ефективності в комп'ютерних системах та мережах на основі даного протоколу. У результаті даний протокол забезпечує найбільш точну оцінку показника ефективності комп`ютерної мережі. Оцінка розраховувалася при різних стратегіях управління обміном даних: без зворотного зв'язку з виправленням t-кратних помилок, без зворотного зв'язку з виявленням r-кратних помилок, з вирішальним зворотним зв'язком і безперервною передачею кадрів (ВЗЗбп) "Повернення-на-N" та з вирішальним зворотним зв'язком і позитивною квитанцією (ВЗЗпк).

Згідно з проведеним дослідженням було виявлено, що узагальнений показник ефективності комп'ютерної мережі на основі протоколу Frame Relay дозволяє всебічно оцінити протоколи обміну даними. Технологія Frame Relay в

порівнянні з протоколом X.25 більш точно оцінює ефективність протоколів обміну даними в комп'ютерних мережах.

БІБЛІОГРАФІЯ

1. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К. : Держстандарт України, 2002. – 40 с.

2. Захист інформації. Автоматизовані системи у захищеному виконанні. Загальні вимоги: ДСТУ 51624-2000. – К. : Держстандарт України, 2000. – 24 с.

3. Системи оброблення інформації. Управління процесами оброблення даних. Терміни та визначення: ДСТУ 2940-94. – К. : Держстандарт України, 1995. – 28 с.

4. ССБП. Пожежна техніка. Терміни та визначення: ДСТУ 2273-93. – К. : Держстандарт України, 1993. – 30 с.

5. Закон Украины «Об охране труда» // Охрана труда. – №1 (103). – 2003. – 3 – 11 с.

6. Пожарная безопасность зданий и сооружений: СНиП 21-01-97. – М. : Изд-во стандартов, 1997. – 77 с.

7. ССБТ. Общие санитарно-гигиенические требования к воздуху рабочей зоны: ГОСТ 12.1.005-88. – М. : Изд-во стандартов, 1992. – 42 с.

8. ССБТ. Шум. Общие требования безопасности: ГОСТ 12.1.003-83. – М. : Изд-во стандартов, 1991. – 32 с.

9. Гольдштейн В. С. «Протоколы передачи данных». Ч. 2. «Москва-Издат». – 2001. – 245 с.

10. Грушо А. А. Анализ и синтез криптоалгоритмов: курс лекций / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М., 2000. – 110 с.

11. Гусева А. И. Технология межсетевых взаимодействий. – Москва : Диалог-Мифи. – 1997. – 272 с.

12. Дорошенко А. Н. Информационная безопасность. Методы и средства защиты информации в компьютерных системах : учебное пособие. / А. Н. Дорошенко, Л. Л. Ткачев. – М. : МГУПИ, 2006. – 143 с.

13. Евсеев С. П., Сумцов Д. В., Король О. Г, Томашевский Б.П. Анализ эффективности передачи данных в компьютерных системах с использованием интегрированных механизмов обеспечения надежности и безопасности // Восточно-европейский журнал передовых технологий. – 2010. – 5/2(35). – 34 – 38 с.

14. Жидецкий В. Ц. Основы охраны труда. – Львов: Афиша, 2000. – 352 с.

15. Жидецький В. Ц. Охорона праці користувачів комп'ютерів. – Львів : Афіша, 2000. – 174 с.

16. Захист інформації в комп’ютерних системах від несанкціонованого доступу / За ред. С. Г. Лаптєва. – К., 2009. – 321 с.

17. Захист інформації та економічна безпека підприємства : монографія / О. О. Кузнєцов, С. П. Євсеєв, С. В. Кавун. – Харків : Вид. ХНЕУ, 2008. – 360 с.

18. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры : учебное пособие / А. Ю. Зубов. – М. : Гелиос АРВ, 2005. – 192 с.

19. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях // М. : КУДИЦ-ОБРАЗ, 2001. – 368 с.

20. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М. : Кудиц – Образ, 2001. – 368 с.

21. Ирвин Дж., Харль Д. Передача данных в сетях и инженерный подход. – СПб. : Питер, 2002. – 405 с.

22. Конеев И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев // Спб. : БХВ-Петербург, 2003. – 752 с.

23. Корнюшин П. Н. Информационная безопасность: учебное пособие / П. Н. Корнюшин, А. С. Костерин. – Владивосток : ТИДОТ ДВГУ. – 2003. – 154 с.

24. Кузнєцов О. О. Захист інформації та економічна безпека підприємства / О. О. Кузнєцов, С. П. Євсеєв, С. В. Кавун. – Харків : Вид. ХНЕУ, 2009. – 360 с.

25. Ленков С. В. Методы и средства защиты информации / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко ; под ред. В. А. Хорошко. – В 2-х т. – К. : Арий, 2008. – Т.2. Информационная безопасность. – 344 с.

26. Лупаїна К. М. Міжнародна науково-практична конференція молодих вчених, аспірантів та студентів «Аналіз відомих протоколів обміну даних в комп`ютерних системах та мережах», 21-22 квітня 2013р.: тези доповідей. Том І / К.М. Лупаїна. – Харків: ХНЕУ, 2013. – 71 с.

27. Лупаїна К. М. Аналіз ефективності передачі даних в комп`ютерних ситемах з використанням інтегрованих механізмів забезпечення надійності та безпеки. Збірник наукових праць студентів спеціальностей «Інформаційні управляючі системи і технології», «Комп'ютерний еколого-економічний моніторинг» та МБА «Бізнес-інформатика» / К. М. Лупаїна. – Харків : ХНЕУ, 2013. – 84 с.

28. Малюк А. А. Введение в защиту информации в автоматизированных системах / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. – М. : Горячая Линия – Телеком, 2001. – 148 с.

29. Мамаев Е. Технологии защиты информации в Интернете. – СПб. : ИД Питер, 2001. – 848 с.

30. Мао В. Современная криптография. Теория и практика. – М. : «Вильямс», 2005. – 768 с.

31. Милославская Н. Р. Интрасети: доступ в Интернет, защита / Н. Р. Милославская, А. И. Толстой. – М. : Юнити-Дана, 2000. – 527 с.

32. Молдавян Н.А. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдавян, А.А. Молдавян, М.А. Еремееев – СПб. : БХВ, 2004. – 448 с.

33. Олифер В. Г. Компьютерные сети. – СПб. : ИД Питер, 2002. – 864 с.

34. Олифер В. Г. Компьютерные сети. Принцип, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб : издательство "Питер". 2000. – 672 с.

35. Осипян В. О. Криптография в задачах и упражнениях / В. О. Осипян, К. В. Осипян; зав. Ред. Т. А. Денисова. – М. : Гелиос АРВ, 2004. – 144 с.

36. Основы информационной безопасности : учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М. : Горячая линия – Телеком, 2006. – 544 с.

37. Петров А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. – М. : ДМК, 2000. – 448 с.

38. Поповский В. В. Защита информации в элекоммуникационных системах: учебник / В. В. Поповский, А. В. Персиков. – Харьков : ООО “Компания СМИТ”, 2006. – Т.1. – 292 с.

39. Потий А. В. Стандартизация и сертификация в сфере защиты информации. Стандарты механизмов безопасности : учебное пособие / А. В. Потий. – Харьков : ХНУРЕ, 2002. – 80 с.

40. Практикум з охорони праці / Під редакцією В.Ц. Жидецького. – Львів: Афіша, 2000. – 348 с.

41. Практикум з охорони праці. Університетська книга / І. П. Пістун, Ю. В. Кіт, А. П. Березовський. – Суми: 2000. – 208 с.

42. Ростовцев А. Г. Методы криптоанализа классических шифров [Электронный ресурс] / А. Г. Ростовцев, Г. В. Михайлова. – Режим доступа: http://crupto.hotbox.ru/.

43. Сети и системы телекоммуникаций: Учебное пособие / В. А. Погонин, С. Б. Путин, А. А. Третьяков, В. А. Шиганиов. – М. : «Издательство Машиностроение-1», 2005. – 172 с.

44. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр. / Пер. с англ. – М. : Издательский дом “Вильямс”, 2003. – 1104 с.

45. Стеклов В. К. Проектування телекомунікаційних мереж: Підруч. для студ. вищ. навч. закл. за напрямком «Телекомунікації» / В. К. Стеклов, Л. Н. Беркман / за ред. В. К. Стеклова. – К. : Техніка, 2002. – 792 с.

46. Стеклов В. К. Проектування телекомунікаційних мереж: Підруч. для студ. вищ. навч. закл. за напрямком «Телекомунікації» / В. К. Стеклов, Л. Н. Беркман. – К. : Техніка, 2001. – 392 с.

47. Столлингс В. Компьютерные системы передачи данных. – М. : Вильямс, 2002. – 928 с.

48. Сумцов Д. В., Томашевський Б. П. Загальний показник ефективності передачі даних у комп'ютерній мережі // Системи обробки інформації. – 2009.

49. Сумцов Д. В., Євсєєв С. П., Томашевський Б. П., Король О. Г. Ефективність обміну даними в комп'ютерній мережі при різних способах управління обміном / / Збірник наукових праць. – Донецьк : ДонІЖД, 2009.

50. Технології і стандарти комп`ютерних мереж / Смірнов О. А., Евсеев С. П., Жукарев В. Ю., Король О. Г., Сорокін В. Є., Мелешко Є. В. – Д. : ДонІЗТ, 2012. – 453 с.

51. Харин Ю.С. Математические и компьютерные основы криптологии / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич – Мн. : Новое знание, 2003. – 382 с.

52. Хорошко В. А. Методы и средства зашиты информации / В. А. Хорошко, А. А. Чекатков. – К. : Юниор, 2003. – 504 с.

53. Чмора А. Л. Современная прикладная криптография / А. Л. Чмора. – М. : Гелиос АРВ, 2001. – 256 с.

54. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и Техника, 2004. – 384 с.

55. Євсеєв С. П., Огурцов В. В., Лупаїна К. М. Ефективність обміну даними в комп'ютерних мережах з різними методами управління обміну на основі протоколу frame relay // Системи обробки інформації, проблеми і перспективи розвитку іт індустрії, Том 2.

56. Особенности функционирования Frame Relay [Електронний ресурс] // Режим доступу: http://kunegin.narod.ru/.

57. Сети Frame Reley [Електронний ресурс] // Режим доступу: http://www.lessons-tva.info/.

58. Украинский ресурс по безопасности [Электронный ресурс] – Режим доступа: http://kiev-security.org.ua/.

59. Грибан В. Г., Негодченко О. В. Охорона праці : навчальний посібник . -2-е видання. Київ: Центр учбової літератури, 2018.- 280 с, ISBN 978-966-364-832-3

60. Запорожець О. І., Протоєрейський О. С., Франчук Г. М., Боровик І. М. Основи охорони праці підручник Київ: Центр учбової літератури, 2017. - с.264, ISBN 978-617-673-423-9

61. М. С. Одарченко, А. М. Одарченко, В. І. Степанов, Я. М. Черненко. Основи охорони праці: підручник/ – Х. : Стиль-Издат, 2017. – 334 с. ISBN 966-7885-84-4

62. Охрана окружающей среды: учеб. для техн. спец. вузов./ С.В. Белов, Ф.А. Барбинов, А.Ф. Козьяков и др. ; под ред. С.В.Белова М.: Высшая школа, 1991.- 319с. ISBN 5-06-000665-1.

63. Васійчук В.О., Гончарук В.Є., Качан С.І., Мохняк С.М.Основи цивільного захисту: Навч. посібник / В.О. Васійчук, В.Є Гончарук, С.І.Качан, С.М. Мохняк.-Львів:Видавництво Національного університету "Львівська політехніка", 2010.-417с

64. Білявський Г. О. Основи екології: підручник для студ. вищих навч. закладів / Г. О. Білявський, Р. С. Фурдуй, І. Ю. Костіков. К. : Либідь, 2004. - 408 с. ISBN 966-06-0289-8.

65. Запольський А.К. Основи екології: підр. для студ. техн. технол. спец. вищ. навч. закл. / А. К. Запольський, А.І. Салюк; за ред. К.М. Ситника. К.: Вища школа, 2001.- 358с. ISBN 966-642-059-7.

66. Тарасова В.В. Екологічна статистика // Київ: «Центр учбово\ї літератури», 2008 ро.-391с.

67. Бедрій Я. І.; Джигирей В. С.; Кидисюк, А. І. та ін. Основи екології та охорона навколишнього природного середовища: навч. посіб. для студ. вищих навч. закладів // за ред. В. С. Джигирей ; Український держ. лісотехнічний ун-т, Львівський електротехнікум зв'язку. - Л. : [б.в.], 1999. - 239 с. Альтернативна назва : Екологія та охорона природи. - ISBN 5-7763-2641-9.

ДОДАТКИ