МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Факультет кібербезпеки, комп'ютерної та програмної інженерії (ЗФН)
Кафедра комп'ютерних інформаційних технологій

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____Аліна САВЧЕНКО
«___»_____2021 р.

ДИПЛОМНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИЦІ ОСВІТНЬОГО СТУПЕНЯ

"МАГІСТРА"

ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ "ІНФОРМАЦІЙНІ УПРАВЛЯЮЧІ СИСТЕМИ ТА ТЕХНОЛОГІЇ"

Тема: «Моніторинг польотної інформації на базі VPN»

Виконавиця: Мурашко Світлана Миколаївна

Керівник: к.т.н., доцент Холявкіна Тетяна Володимирівна

Нормоконтролер: _____ Ігор РАЙЧЕВ

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії (ЗФН)

Кафедра Комп'ютерних інформаційних технологій

Галузь знань, спеціальність, освітньо-професійна програма: 12"Інформаційні технології", 122 "Комп'ютерні науки", "Інформаційні управляючі системи та технології" .

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Аліна САВЧЕНКО
«____»_____2021р.

ЗАВДАННЯ

на виконання дипломної роботи студентки

Мурашко Світлани Миколаївни
(прізвище, ім'я, по батькові)

1. **Тема роботи:** "Моніторинг польотної інформації на базі VPN" затверджена наказом ректора від 12.10.2021 № 2229/ст.
2. **Термін виконання роботи:** з 11.10.2021 р. по 31.12.2021 р.
3. **Зміст пояснювальної записки:** Аналіз структури інформаційних об'єктів комп'ютеризованої системи моніторингу польотної інформації на основі VPN. Розробка формальної моделі віртуальної мережі системи моніторингу польотної інформації на основі VPN. Порівняльний аналіз залежності характеристик функціонування та стабільності роботи мережі відносно використовуваного коефіцієнта фрагментації пакетів даних, шо передаються по віртуальній приватній мережі.
4. **Перелік обов'язкового графічного (ілюстративного) матеріалу:**

1) модель багаторівневої ієрархічної структури мережі ЄЦОАПІ;
2) процеси фрагментації, обслуговування і об'єднання фрагментів пакету;
3) результати дослідження;
4) залежність імовірності спотворення пакету від коефіцієнта фрагментації;
5) розкид часу доставки фрагментів різноманітної довжини.

5. **Календарний план-графік**

№ п/п	Етапи виконання дипломного проекту	Термін виконання	Підпис керівника
1	Визначити тему дипломного проекту.	11.10.2021– 14.10.2021	
2	Проаналізувати існуючу нормативну бази. Накопичити матеріали з теми.	15.10.2021– 19.10.2021	
3	Дослідити підходи щодо створення комп'ютеризованої системи моніторингу польотної інформації на основі VPN.	20.10.2021– 24.10.2021	
4	Розробити формальну модель віртуальної мережі системи моніторингу польотної інформації на основі VPN.	25.10.2021– 30.10.2021	
5	Скласти порівняльний аналіз залежності характеристик функціонування та стабільності роботи мережі відносно використовуваного коефіцієнта фрагментації пакетів даних.	31.10.2021– 10.11.2021	
6	Підготувати графічні матеріали.	12.11.2021– 20.11.2021	
7	Завершити оформлення пояснювальної записки.	21.11.2021– 10.12.2021	
8	Підготувати доповідь до захисту дипломної роботи.	11.12.2021– 17.12.2021	
9	Підготуватися до захисту дипломної роботи.	18.12.2021– 20.12.2021	

7. **Дата видачі завдання:** 11 жовтня 2021 р.

Керівник дипломної роботи (проекту) _____ Холявкіна Т.В.
(підпис керівника) (ПІБ)

Завдання прийняла до виконання _____ Мурашко С.М.
(підпис випускниці) (ПІБ)

РЕФЕРАТ

Пояснювальна записка до магістерської дипломної роботи «Моніторинг польотної інформації на базі VPN» викладена на 92 сторінках. Містить 22 рисунки, 2 таблиці, 51 наукове джерело.

Ключові слова: ВІДДАЛЕНИЙ ДОСТУП, ПЕРЕДАЧА ДАНИХ, ТУНЕЛЮВАННЯ, ФРАГМЕНТАЦІЯ, ATM, BER, IP, QoS, VPN.

Об'єктом дослідження є процес моніторингу польотної інформації у спеціалізованій розподіленій інформаційній обчислювальній системі.

Предмет дослідження: математичні моделі і методи обслуговування потоків даних в мережах з гетерогенною структурою системи контролю безпеки польотів.

Мета роботи: розробка методики проектування автоматизованої комп'ютеризованої системи моніторингу польотної інформації на основі VPN.

Методи дослідження. У дипломній роботі застосовувалися методи теорії масового обслуговування, теорії ймовірності та математичної статистики, математичне моделювання.

Отримані результати: розроблено методику проектування автоматизованої системи моніторингу польотної інформації на основі VPN, досліджено вплив характеристики фрагментації пакетів на характеристики функціонування та стабільність роботи мережі комп’ютеризованої системи моніторингу польотної інформації на основі VPN.

Результати магістерської роботи можуть бути використані при проектуванні автоматизованої комп’ютерної системи моніторингу польотної інформації.

Прогнозні припущення про розвиток об’єкту та предмету дослідження: дослідження доцільно продовжити у напрямі обліку порівняльної важливості вибраних приватних показників ефективності і імовірнісних характеристик збереження цілісності інформації в процесі передачі фрагментованих даних.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АП	авіаційна подія
АТС	авіаційно-транспортна система
АТК	авіаційно-технічний комплекс
АС	автоматизована система
АФТН	автоматизований комп'ютерний комплекс телефонної мережі
БП	безпека польоту
БПР	бортові пристрої реєстрації
БД	база даних
ЄЦОАПІ	Єдиний центр по обробці авіапригод та інцидентів
ПС	повітряне судно
ЦА	цивільна авіація
ДП БП	державна програма безпеки польотів
ЗП	Запамятуючий пристрій
ІКАО	Міжнародна організація цивільної авіації
КД	керування доступом
НКС	наземна комп'ютеризована система
НКС ОПІ	наземна комп'ютеризована система обробки польотної інформації
НД	несанкціонований доступ
ОрПР	організація повітряного руху
ОПР	обслуговування повітряного руху
ПІ	польотна інформація
ПК	персональний комп'ютер
КУБП	керівництво з управління безпекою польотів
РБД і З	розподілена база даних і знань
РБД	розподілена база даних
ЗОК	засоби об'єктивного контролю

ЗУБД	засоби управління базами даних
ЗА	засоби автоматизації
МПД	мережа передачі даних
СТД	система транспорту даних
МСРП	магнітний самописець реєстрації параметрів
СЗ	система захисту
УПР	управління повітряним рухом
ЕОМ	електронно-обчислювальна машина
ЕЦП	електронний цифровий підпис
ADREP	*Accident Data REPorting System* (система представлення даних про авіаційні події/інциденти)
ANSI-SPARC	*American National Standards Institute - Standards Plannibg and Requrements Committee* (Американський національний інститут стандартів – стандарти і планування вимог комітету)
ATM	*Asynchronous Transfer Mode* (мережева високопродуктивна технологія комутації та мультиплексування, заснована на передачі даних у вигляді ячейок (cell) фіксованого розміру (53 байта)
ATN	*Aeronauthical Telecommunication Network* (авіаційна телекомунікаційна мережа)
BER	*Bit Error Rate* (коефіцієнт помилок по бітах)
FR	*Frame Relay* (протокол канального рівня мережевої моделі OSI)
SAE	*System Architecture Evolution* (розвиток системи архітектури)
LTE	*Long Term Evolution* (тривалий розвиток)
VTF	*Virtual Technical Functions* (віртуальна технічна функція)
VPN	*Virtual Private Network* (віртуальна приватна мережа)

SARPS	*Standard And Recommended Practice* (стандарті та рекомендовани процедури)
OSI	*Open System Interconnection* (еталонна модель взаємодії відкритих систем)
QoS	Quality of Service (якість сервісу)

ВСТУП

Сучасні системи контролю, моніторингу, аналізу і управління безпекою польотів побудовані за "острівним" принципом. Кожна авіакомпанія, хоча і у рамках єдиних вимог ІКАО і національних авіаційних адміністрацій, але створює власні системи зі значною розбіжністю технічних характеристик, протоколів та інтерфейсів.

Існуюче обладнання є різнорідним і найчастіше недостатньо автоматизованим, що призводить до затримок, низької достовірності результатів аналізу інформації і, як наслідок, до зниження ефективності управлінських рішень.

В рамках глобальної інформаційно-обчислювальної системи безпеки польотів необхідно постійно забезпечувати гарантований рівень достовірності і безпеки на всіх етапах передачі і обробки даних. Необхідно впроваджувати багатошарові (ешелоновані) системи забезпечення збереження інформації.

Механізми обміну інформацією передбачають можливість організації віртуальної приватної мережі.

На будь-яких етапах повітряного руху, у тому числі і при виникненні нештатних польотних ситуацій, мають бути гарантовані своєчасність доставки і цілісність інформації.

Таким чином, розробка захищеної розподіленої системи моніторингу польотної інформації з високим ступенем автоматизації і комп'ютеризації являється актуальною науковою задачею.

За вимогами ІСАО, ЄЦОАПІ займається реалізацією програм по вирішенню питань пов’язаних з безпекою польотів та ефективним обміном інформацією з відповідними організаціями. Дана дипломна робота присвячена реалізації програми забезпечення ефективного обміну даними.

Інформація, що підлягає обробці та обробляється в АС ЄЦОАПІ та зокрема в комп’ютеризованій системі моніторингу польотної інформації на основі VPN, має високу цінність, яку можна представити у матеріальному вираженні і потребує захисту від різноманітних за своєю природою несприятливих впливів, які можуть призвести до зниження її ціннісної ваги.

Загрози інформації, що обробляється в АС, можуть залежати від багатьох чинників. З них особливої уваги заслуговують такі, як: характеристики операційних систем (ОС), що їх обслуговують, персонал, що займається обробкою цієї інформації, характер оброблюваної інформації. Як бачимо, природа загроз може бути як об'єктивною, так і суб'єктивною. Серед суб'єктивних загроз особливої уваги заслуговує суттєва частка загроз, які є пов'язаними з несанціонованим доступом (НД), вона становить біля 15% [1].

При взаємозв'язку видів діяльності ІКАО з видами діяльності місцевих українських авіакомпаній, ставляться наздвичайно суворі вимоги до збереження конфіденційності оброблюваної польотної інофрмації, адже ці дані не повинні бути доступні широкому колу осіб, що не мають відношення до роботи з ними. А дотримання високого ступеню конфіденційності отриманої польотної інофрмації та постійно зростаючої швидкості обробки польотної інофрмації забезпечує більш якісне розслідування авіапригод у разі їх місця.

Боротьба з вирішенням проблеми захисту від НД в наш час досягла достатньо великих масштабів. Вона може проводитися як програмно-технічними засобами, так і організаційними засобами. В наш час, епоху іновацій, більшого розмаху набула саме боротьба програмно-технічними засобами [2].

Наслідками НД є порушення базових принципів інформаційної безпеки:

1) конфіденційність;

2) цілісність;

3) доступність.

Порушення конфіденційності, що спрямоване на розголошення конфіденційної або секретної інформації, вважається здійсненим, як тільки отримано несанкціонований доступ до деякої закритої інформації.

Порушення цілісності інформації, які можуть відбуватися у мережі або під час передачі інформації по каналах зв'язку з метою порушення якості інформації або повному її знищенню, є особливо актуальним питанням для систем передачі інформації. Навмисні ж порушення цілісності інформації не можна плутати з її санкціоно-

ваною зміною, які, наприклад, відбуваються повноваженими для корекції деякої бази даних.

Стосовно доступності інформації, то може бути порушення працездатності ІС або відмова в обслуговуванні користувача даною системою. Така ситуація виникає, коли блокується доступ до деяких ресурсів. У такий спосіб відбувається вплив на інформацію, яку захищають [3].

Чинним Кримінальним кодексом передбачено розділ XVI, який присвячено злочинам у сфері використання електронно-обчислювальних машин (ЕОМ), систем та комп'ютерних мереж і мереж електрозв'язку [4].

Керування доступом (КД) є одним із провідних процесів захисту від НД. З традиційної точки зору засоби управління доступом дозволяють специфікувати і контролювати дії, які суб'єкти (користувачі та процеси) можуть виконувати над об'єктами (інформацією та іншими комп'ютерними ресурсами). Керування доступом виконується за допомогою програмно-технічних засобів, які є частиною АС. Додатково необхідно зауважити, що в основі будь-якого з видів керування доступом, лежить своя специфічна методика та технологія.

Оптимальним рішенням для захисту конфіденційних даних стає шифрування та аутентифікація при доступі до інформації. Такі методи захисту інформації присутні у технології VPN.

Були розроблені технології, що дозволяють передавати дані практично через будь-яку відкриту мережу загального користування таким чином, що для учасників інформаційного обміну це виглядає так, як ніби використовується приватна захищена локальна мережа. Сімейство таких технологій отримало назву віртуальна приватна мережа – VPN (Virtual Private Network).

Віртуальна приватна мережа базується на трьох базових принципах: тунелюванні, шифруванні і аутентифікації.

Туннелювання забезпечує передачу даних між двома точками - закінченнями тунелю - таким чином, що для джерела і приймача даних виявляється прихованою вся мережева інфраструктура, що лежить між ними.

Щоб перешкодити внесенню несанкціонованих змін в пакет з даними на шляху його проходження по тунелю, використовується метод електронного цифрового підпису (ЕЦП). Захист переданих через тунель даних від несанкціонованого перегляду досягається шляхом використання сильних алгоритмів шифрування.

Зв’язка «тунелювання + аутентифікація + шифрування» дозволяє передавати дані між двома точками через мережу загального користування, моделюючи роботу приватної (локальної) мережі. Іншими словами, розглянуті засоби дозволяють побудувати віртуальну приватну мережу. Додатковою корисною властивістю VPN-з'єднання є можливість (і навіть необхідність) використання системи адресації, прийнятої в локальній мережі [5].

Таким чином, використання VPN забезпечує надійний захист конфіденційних даних, які були отримані під час моніторингу польотної інформації, що передаються по віртуальній приватній мережі.

На основі аналізу інформаційних об’єктів, які складають АС, була розроблена методика реалізації моделі віртуальної мережі системи моніторингу. Результатом аналізу є формальна модель віртуальної мережі системи моніторингу польотної інформації на основі VPN. Модель, що є отриманою, надає можливість опису всіх основних елементів та параметрів дослідження обслуговування потоків даних в мережах з гетероденною структурою системи контролю безпеки польотів, наприклад такого, як вибір оптимального показника фрагментації пакетів у мережі.

Для забезпечення збільшення швидкості передачі інформації по тунелям VPN (VPN являється повільнокомутованим з’єднанням) використовуються поняття фрагментації та дефрагментації пакетів. Як результат отримаємо значне збільшення швидкості передаваних конфіденційних даних та більший ступінь конфіденційності передаваних даних (окрім того, що дані будуть зашифровані, вони ще й будуть передаватись по декількох каналах, що зведе практично до нуля перехоплення зловмисниками, об’єднання та дешифрування конфіденційних даних).

У даній дипломній роботі отримано наступний новий науковий результат: розроблено метод вибору оптимального числа фрагментів пакету при розподіленій пе-

редачі, при якій не тільки підвищується швидкість передачі, а й безпека обміну даними, їх цілісність та конфіденційність.

Практичне значення отриманих результатів дипломної роботи визначається тим, що теоретичні результати та висновки доведені до конкретних алгоритмів, структурних та функціональних схем, та полягає в наступному:

1. Розроблені методи та алгоритми зведені до конкретних структур, які можуть бути реалізовані при встановленні та модифікації мережного обладнання.

2. Розроблені методи фрагментації пакетів для підвищення надійності передачі даних придатні до застосування у широкому колі мереж загального та спеціального призначення при відповідних модернізаціях та масштабуваннях розподілених баз даних.

3. Обґрунтовано можливості реалізації методів захисту інформації апаратними чи програмними засобами при організації багаторубіжної системи захисту.

Розроблена формальна модель дозволяє спроектувати та створити комп’ютеризовану системи моніторингу польотної інформації на основі VPN. За бажанням, модель може бути модернізована чи видозмінена по аналогії до проекту в залежності від умов конкретного технічного завдання.

РОЗДІЛ 1
АНАЛІТИЧНИЙ ОГЛЯД І ПОСТАНОВКА ЗАДАЧІ

1.1. Загальна концепція авіаційної безпеки

Розвиток авіації неможливий без вдосконалення систем в області контролю і розробки методів, які знижують загрозу небезпеці польотів. Знайдено багато шляхів уникнення жертв в результаті польоту, оскільки ще на зорі авіації почали займатися питаннями запобігання авіаційним подіям. Завдяки забезпеченню безпеки польотів, частота і серйозність авіаційних подій значно знизилися. Загальна кількість подій на регулярних комерційних рейсах зменшилася на 21 відсоток в порівнянні з 2018 роком, незважаючи на те, що число перевезень збільшилося незначно (приблизно на один відсоток) за той же період часу. У підсумку кількість пригод в 2019 році знизилася до 3,2 пригод на мільйон рейсів. По Україні цей показник дорівнює 10 – 12 авіапригод на 1 млн. льотних годин. На даний момент інформація з авіаподій вкрай обмежена, оскільки офіційні звіти за останніми авіаподіями ще не були повністю представлені [6].

Оскільки глобальна авіаційна діяльність розширюється з кожним роком, традиційні методи зниження ризику до прийнятного рівня можуть виявитися недостатніми.

Тому сьогодні розробляються нові концепції розуміння управління і безпеки польотів (БП).

Це, перш за все, дві стратегії забезпечення безпеки польотів.

Традиційна стратегія, або ретроактивна стратегія, яка передбачає:

1) дотримання мінімальних вимог БП;

2) оцінка допустимого рівня БП, що проводиться в умовах обмежень;

3) запізнювання профілактичних заходів.

В цьому випадку кількість авіаційних подій перестала зростати, але авіакатастроф – ні. Це привело до того, що замість підвищення бажаних стандартів такий підхід відповідав мінімальним стандартам. При ймовірності авіаційних подій з фатальним результатом 10^{-6} (тобто одна авіакатастрофа з фатальним результатом на мільйон польотів) задача досягнення подальшого підвищення безпеки польотів ставала все важчою.

За допомогою сучасних стратегій забезпечується збір інформації про БП з різних джерел. Передбачається, що ризик авіаційної події (АП) може бути зведений до мінімуму шляхом виявлення "вразливих" місць перш, ніж вони дадуть збій. При цьому виявляються системні небезпечні умови, для чого використовуються:

1) системи представлення даних, необхідних для виявлення прихованих небезпечних умов (тобто даних про небезпечні чинники та інциденти);

2) результати обстеження стану авіаційно-транспортної системи (АТС), що виконуються з метою отримання інформації (зауважень) про чинники і умови, які сприяють розвитку авіаційних подій;

3) аналіз польотної інформації з бортових реєстраторів (аналіз реєстрованих і виявлених порушень і відхилень у польоті);

4) результати оперативної інспекції і перевірок аспектів виробництва польотів, виявлені "тонкі " місця (до їх безпосереднього прояву у польоті).

В цьому випадку до міцної законодавчої структури, нормативним вимогам і порядку виконання польотів ще вводиться чинників, які цілком описані в Керівництві по управлінню безпекою польотів (КУБП) [7].

На рис.1.1. детальніше представлено дві стратегії безпеки польотів.

Щоб зрозуміти, що таке забезпечення безпеки польотів, перш за все, потрібно знати, що розуміється під безпекою польотів.

В даний час безпека все більше розглядається як контроль ризику. Тому безпека - це *стан, при якому ризик завдання шкоди людині або майну скорочується до прийнятного рівня шляхом постійного процесу розпізнавання небезпечної ситуації і контролю ризику* [7].

SARSPS ІКАО: Дві стратегії забезпечення БП

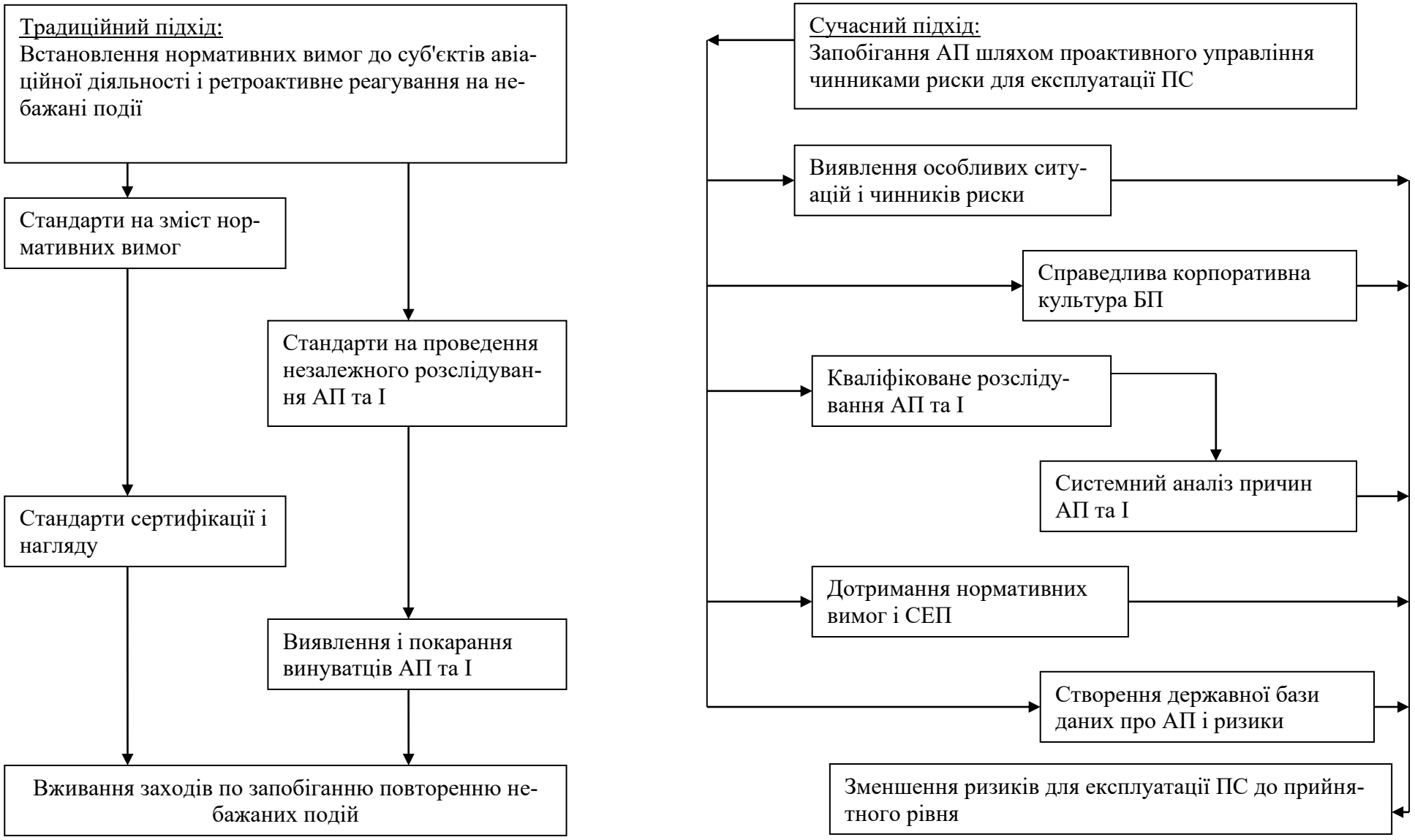

Рис.1.1. Дві стратегії БП

Безпека завжди була і є важливою умовою у роботі авіації [8]. Це відображається в цілях і завданнях ІКАО, як затверджується в статті 44 Конвенції по Міжнародній Цивільній Авіації, відомій як Конвенція Чикаго. Вона поклала на ІКАО відповідальність за забезпечення безпеки польотів і за більше розповсюдження Міжнародної Цивільної авіації по всьому світу.

На рис.1.2. показані загальні вимоги ІКАО до держав і постачальників обслуговування по управлінню БП.

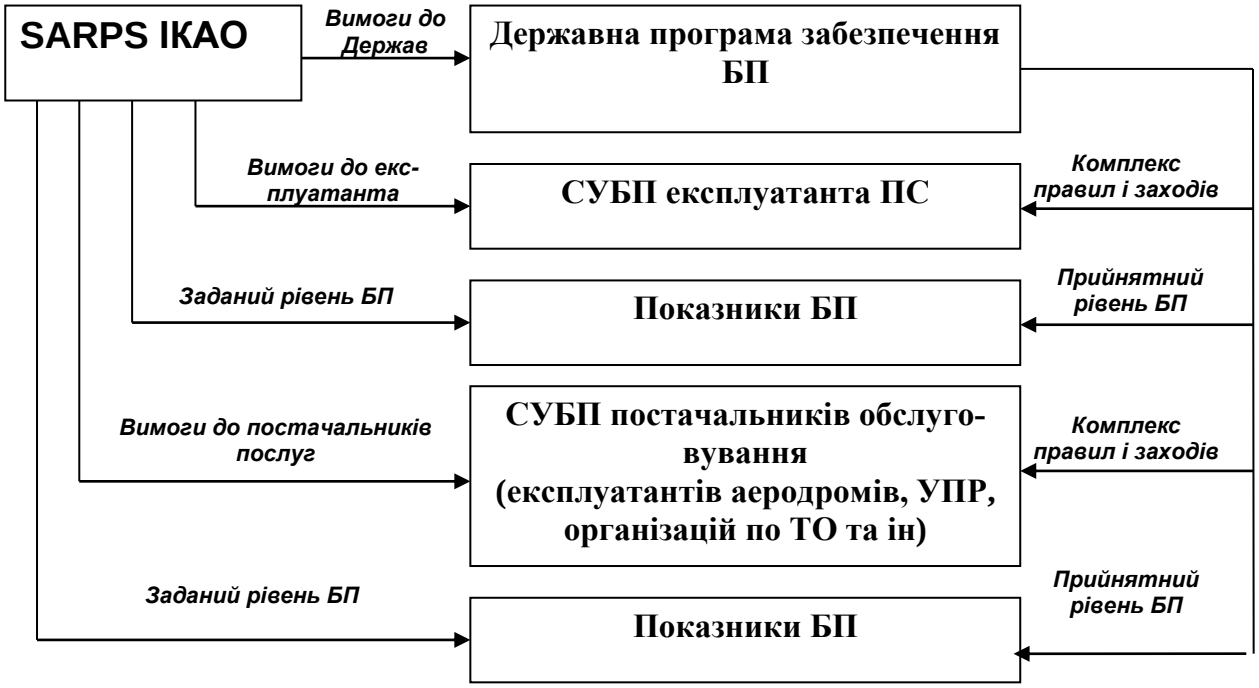

Рис.1.2. Загальні вимоги ІКАО по управлінню БП з 2006 р.

Стандарти і практика ІКАО (Standard And Recommended Practice - SARPS), вимагають, щоб держави розробляли програму безпеки польотів, з метою зменшення допустимого рівня безпеки авіаперевезень.

Програма безпеки польотів (БП) має бути повною, включати безліч видів діяльності по забезпеченню БП. *Це – єдиний комплекс правил і видів діяльності, направлених на підвищення БП* [9].

Перерахуємо основні компоненти програми БП.

1) Авіаційні правила.

2) Система збору польотних даних про події, які створюють або можуть створювати загрозу для експлуатації повітряного судна (ПС).

3) Створення структури, відповідальної за інформаційне забезпечення програми по БП.

4) Створення інфраструктури системи організаційно-адміністративного управління БП на рівнях ЄЦОАПІ і інших суб'єктів АТС, проведення моніторингу і аудиту її ефективності.

Метою системи управління безпекою є попередження авіаційних подій і забезпечення безпеки польотів.

Причини авіаційних подій або серйозних інцидентів повинні встановлюватися в цілях запобігання подібним подіям в майбутньому. Визначити причинні чинники найнадійніше шляхом проведення належним чином організованого розслідування.

Процес розслідування включає збір, реєстрацію і аналіз такою, що має відношення до події, встановлення причин, вироблення рекомендацій по забезпеченню безпеки польотів.

Для того, щоб попередити авіаційні події, насамперед потрібно своєчасно виявити і усунути аварійні чинники.

Чинники, які впливають на безпеку польотів, розділяються на три основні групи: людський, технічний і чинник середовища, пов'язаний з недоліками обслуговування повітряного руху, метеоозабезпечення і аеродромно-технічного забезпечення польотів [10].

1.2. Бортові засоби об'єктивного контролю

Важливу роль в забезпеченні безпеки польотів відіграють польотна інформація і засоби об'єктивного контролю.

Польотна інформація (ПІ) - це параметрична і мовна інформація бортових реєстраторів про політ ПС, доповнена, при необхідності, інформацією, яка занесена екіпажем ПС в паспорт до носія ПІ.

Бортові засоби об'єктивного контролю (бортові ЗОК) - технічні засоби, призначені для реєстрації і збереження польотної інформації, що характеризує умови польоту, дії екіпажу і функціонування бортового обладнання. ЗОК використовуються для: аналізу причин і попередження льотних подій; технічної діагностики бортового обладнання і прогнозування його технічного стану; оцінки дій льотного складу при виконанні польотного завдання. Існує два види ЗОК - бортові пристрої реєстрації (бортові самописці) і бортові магнітофони, останнім часом починають розроблятися інтегральні пристрої, що поєднують в собі функції обох видів. [11,12]

Аналіз польотних даних - процес аналізу зареєстрованих польотних даних в цілях підвищення рівня безпеки польотів.

Бортові реєстратори встановлюються на ПС відповідно до вимог ІКАО, як додаткове джерело відомостей для проведення розслідувань авіаційних подій і інцидентів. У документах ІКАО, крім того, вказується на високу цінність інформації в записах бортових реєстраторів для вивчення дій екіпажу в звичайних польотах і технічного обслуговування ПС.

Бортові пристрої реєстрації (БПР) призначені для автоматичного запису параметрів польоту (висоти, швидкості польоту, частоти обертання авіадвигунів, кутів атаки, прискорень) і параметрів найбільш важливих агрегатів і систем.

По функціональному призначенню БПР піділяються на аварійні, експлуатаційні і випробувальні.

Аварійні БПР для накопичення і збереження польотної інформації, яка може бути використана при розслідуванні інцидентів, аварій і катастроф. Експлуатаційні системи реєстрації записують значно більше число параметрів, чим аварійні БПР. Накопичувач експлуатаційного реєстратора захисту не має і при аваріях не зберігається.

Випробувальні системи реєстрації використовуються при проведенні різного роду льотних випробувань зразків авіаційної техніки.

За принципом запису інформації БПР поділяються на механічні, оптичні (осцилографічні), магнітні. А також із твердотілими ЗП (запамятуючий пристрій). У

механічних і оптичних накопичувачах сигнал записується у аналоговій формі. У магнітних і твердотілих - в цифровій.

У магнітних накопичувачах, як носій використовується магнітна стрічка, інколи дріт, запис інформації проводиться у вигляді часу - імпульсного, частотного або цифрового коду. Прикладами магнітних БПР можуть служити МСРП-64, МСРП-256 (магнітна система реєстрації параметрів польоту).

БПР із твердотілим накопичувачем - нове покоління пристроїв реєстрації, приклади таких пристроїв: ТБН-К-4 - експлуатаційний і ЗБН-1-3 - захищений (аварійний).

Бортові магнітофони призначені для запису мовної інформації - переговорів екіпажу по зовнішньому або внутрішньому зв'язку (у деяких спеціальних випадках можливо використання в якості ЗОК відеомагнітофонів - для запису відеоінформації, що відбувається на борту).

Бортові магнітофони можна класифікувати по різним типам носіїв інформації, що використовуються:

1. Магнітофони із записом на сталевий дріт, наприклад: МС-61Б, П-503б.
2. Магнітофони із записом на магнітну стрічку, наприклад: МАРС-БМ.
3. Магнітофони із записом на твердотілий ЗП, наприклад: П-507м.

Основними недоліками оптичних та механічних реєстраторів є:

1) невелика кількість параметрів, що реєструються;

2) нетривалий запис, який призводить до необхідності перезарядки носія після кожного польоту;

3) аналоговий вид запису, який обумовлює великі похибки реєстрації, що в свою чергу робить неможливим використання ЕОМ для обробки інформації;

4) відсутність термозахисту носія що приводить до великих пошкоджень при пожежі.

Норми ІКАО передбачають збереження не менше ніж 95% інформації при комплексній дії наступних руйнівних чинників [7]:

1) температура 1100° С протягом 15 хв.;

2) ударного навантаження в 9800 н;

3) бензину, гасу, гідравлічних і вогнегасних рідин протягом 2 діб;

4) морської води протягом 2 діб, тощо.

Високі вимоги пред'являються до систем реєстрації по надійності і ресурсу.

1.3. Обробка польотної інформації

Раніше обробка польотної інформації (ПІ) здійснювалася в нестартстопному або в стартстопному режимах.

Нестартстопний режим заснований на покадровій обробці інформації в темпі її введення в ЕОМ. Він дозволяє обробляти інформацію в реальному і прискореному часі і забезпечує економію обчислювальних ресурсів, а також використовується для контролю авіаційно-технічного комплексу (АТК), його елементів і зв'язків і управління ними у польоті.

Стартстопний режим реалізується шляхом введення додаткової операції перезапису ПІ з бортового носія на магнітний диск ЕОМ. При перезаписі, інформація ущільнюється і форматується. Це дозволяє використовувати спеціальне математичне і програмне забезпечення для фільтрації збоїв і відновлення збійних кадрів [10].

До недоліків обробки польотної інформації в таких режимах, перш за все, слідує зниження якості роботи (функціонування) пристроїв введення і процесора.

У пристрої введення при зчитуванні інформації з магнітної стрічки є ймовірність прояву збоїв і пропуску кадрів, а збої в роботі процесора можуть виникати із-за незадовільного технічного обслуговування, наприклад: своєчасно не виявлені несправності його елементів, неякісне заземлення, незадовільне електропостачання, вплив статичної електрики.

Таким чином, до чинників, які знижують достовірність результатів автоматизованого контролю можна віднести наступні:

1) недосконаліть діагностичних моделей;

2) недосконаліть апаратури, математичне і програмне забезпечення системи контролю польотів;

3) відхилення в діях операторів при невиконанні правил експлуатації апаратури і програмного забезпечення контролю польотів, в помилках при підтвердженні повідомлень, що знижують достовірність отриманих результатів.

Для уникнення вище вказаних недоліків при обробці польотної інформації, в даний час обробка ПІ проводиться наземною комп'ютеризованою системою (НКС).

Вимоги до НКС такі:

1) наземні комп'ютеризовані системи і інформаційні технології обробки і аналізу польотних даних повинні забезпечувати автоматизовану обробку записів бортових реєстраторів польотних даних з метою подальшого аналізу і узагальнення результатів обробки для використання при здійсненні програми моніторингу польотних даних, а також використовуються при розслідуванні авіаційних подій;

2) до експлуатації на підприємствах і в організаціях Цивільної Авіації (ЦА) можуть бути допущені в установленому порядку тільки НКС ОПІ з попереднім перезаписом інформації з бортового носія на носій комп'ютера;

3) НКС ОПІ, які застосовує Державіаадміністрація, повинна забезпечувати вирішення всіх завдань, що передбачені державними і міжнародними авіаційними правилами щодо контролю над роботою бортових реєстраторів, у тому числі завдання, які передбачені програмою інспекторських перевірок;

4) конфігурація і програмне забезпечення НКС ОПІ мають бути орієнтовані на обробку записів бортових реєстраторів всіх типів ПС, яким дозволено перетинати повітряний простір України [11].

Результати контролю польоту заносяться в базу даних після обробки польотної інформації.

Створення баз даних ПІ дає можливість комплексного або вибіркового аналізу за будь-який проміжок часу з метою вироблення коректуючого впливу, як за станом техніки, так і по пілотуванню.

У базах даних рекомендується зберігати початкову ПІ (файли прямої копії), що згодом дасть можливість переобробки її по змінених алгоритмах (якщо такі матимуть місце) або при виявленні помилок налаштування, наприклад - при помилок у характеристиках градуювання.

Якщо дозволяють ресурси, можна зберігати проміжні результати обробки і аналізу по кожному польоту для виявлення тенденцій змін або стабільних відхилень від заданих норм, допусків, тощо.

Найбільш мобільним способом зберігання і обробки ПІ є реляційні бази даних. Робота з такими базами здійснюється за допомогою засобів управління базами даних (ЗУБД).

Характерна особливість цієї бази даних полягає в наступному.

База даних повинна мати розподілений характер. Завдяки цьому, по-перше, забезпечується більш швидкий доступ до інформації приватного характеру, необхідної для оперативного функціонування регіональних органів УПР, окремих підприємств обробки польотної інформації, тощо. По-друге, підвищується надійність зберігання даних на термінальних вузлах і проміжних серверах мережі.

По суті, дана база даних є розподіленою базою даних і знань (РБД і З), оскільки, окрім завдань зберігання, вирішуються також завдання обробки даних.

Крім того, здійснюється архівне копіювання і страхувальний перезапис даних з періодом, який вибирається з міркувань надійності зберігання.

РБД і З є структурою критичного використання з міркувань безпеки і захисту інформації. Втрата або інші порушення цілісності інформації можуть спричинити серйозні і непередбачені наслідки, аж до порушення роботи всієї авіаційної транспортної інфраструктури.

Розшифровка даних бортових пристроїв реєстрації дозволяє експлуатантам отримати спільну картину по своєму парку ПС, а державним авіаційним адміністраціям - інформацію про всіх експлуатантів. Ця інформація після обробки перетворюється на статистику, на основі якої можна більш узагальнено робити висновки, відносно до стану безпеки авіації. Можливість отримати відомість для проведення розслідувань авіаційних подій та інцидентів, а також для вивчення дій екіпажу в звичайних польотах і технічного обслуговування ПС.

Автоматизовані бази даних значною мірою полегшують зберігання і аналіз інформації про авіаційні події і інциденти. Вважається, що вирішальне значення для успіху роботи по запобіганню авіаційним подіям має спільне використання такої ін-

формації по безпеці польотів. ІКАО веде автоматизовану базу даних, відому як "Система представлення даних про авіаційні події та інциденти" (ADREP), детальніше зупинимося на цій базі в другому розділі даної роботи.

ІКАО рекомендує [12] створення системи баз даних і засобів аналізу даних про безпеку польотів, що містяться в цих базах, а також визначає порядок використання таких даних в цілях визначення необхідних попереджувальних заходів. Держави повинні заохочувати створення мереж колективного використання інформації про безпеку польотів з метою сприяння вільному обміну інформацією про фактичні і потенційні недоліки в області забезпечення безпеки польотів.

1.4. Концепція глобальної системи організації повітряного руху

Концепція глобальної системи організації повітряного руху (ОрПР) відображає бачення ІКАО єдиної узгодженої і основної на глобальній взаємодії системи ОрПР. Цю концепцію можна адаптувати до експлуатаційних умов в будь-якій державі і регіоні і корегувати з урахуванням їх специфічних потреб.

Система ОрПР заснована на наданні обслуговування. Такий підхід розглядає всі ресурси, включаючи повітряний простір, аеродроми, повітряні судна, і людські ресурси, як складову частину системи ОрПР. Головним завданням системи ОрПР є забезпечення польоту в повітряному просторі на безпечному віддаленні від джерела небезпеки в рамках пропускної спроможності і з оптимальним використанням всіх ресурсів системи.

Таким чином, система ОрПР є системою, яка забезпечує організацію повітряного руху за допомогою інтеграції зусиль людини, інформації, технології, засобів і служб з підтримки бортових, наземних і/або космічних систем зв'язку, навігації і спостереження, що реалізуються спільними зусиллями [13,14].

Держави забезпечують відповідний рівень обслуговування повітряного руху (ОПР) і зв'язку, навігацію і спостереження, контролюють виконання правил УПР, які застосовуються у відповідному повітряному просторі або на аеродромі, і в цілому підтримка прийнятного рівня безпеки польотів при забезпеченні УПР.

Тому на органи ОПР покладаються наступні функції:

1) запобігання зіткненням між повітряними судами в повітрі;

2) запобігання зіткненням між повітряними судами на площі маневрування, а також зіткнень із перешкодами на цій площі;

3) прискорення і підтримка впорядкованого потоку повітряного руху;

4) представлення рекомендацій і інформації в цілях забезпечення безпеки і ефективності польотів;

5) повідомлення відповідних організацій про ПС, що потребують допомоги пошуково-рятувальних служб, і надання необхідної допомоги таким організаціям [15].

Одним з визначальних чинників забезпечення безпеки і економічності повітряного руху є автоматизація управління повітряним рухом.

Управління повітряним рухом (УПР) є системою організаційних і технічних заходів, для забезпечення порядку і безпеки польотів ПС в повітряному просторі, обміну інформацією між авіадиспетчерами і екіпажами ПС з використанням засобів радіозв'язку, аеронавігації і ЕОМ.

На рис. 1.3. представлена структурна схема типової АС УПР. Вона є комплексом технічних засобів, які забезпечують повний обсяг вирішення завдань організації УПР.

Структурна схема будується на базі семи центрів (блоків). Система має блок контролю і діагностики, який забезпечує централізоване управління всіма системами і оперативне резервування її структурних елементів.

Система здійснює документування процесів функціонування системи і переговорів по каналах УПР із забезпеченням можливості відтворення в прискореному і реальному масштабах часу.

Центр – система автоматизований комп'ютерний комплекс телеграфної мережі (АФТН) і планування служить для прийому і передачі аеронавігаційної і метеорологічної інформації, планів польотів, а також оперативної інформації про рух ПС і іншу виробничу інформацію. Програмне забезпечення цього центру включає дві ча-

стини: прийом, передача і обробка повідомлень каналу АФТН і збір, та обробку планової інформації.

Апаратура сполучення призначена для сполучення автоматизованих систем (АС) і засобів автоматизації (ЗА) управління повітряним рухом з джерелами, радіопеленгації і метеорологічної інформації радіолокації, а також для перетворення інформації джерел у форму, необхідну для передачі в системи і засоби УПС.

Контроль польоту ПС здійснюється на основі автоматичних залежних спостережень, тобто навігаційних вимірів, котрі отримуються на борту ПС за допомогою супутникової навігаційної апаратури і переданих на диспетчерський пункт по відповідному радіоканалу.

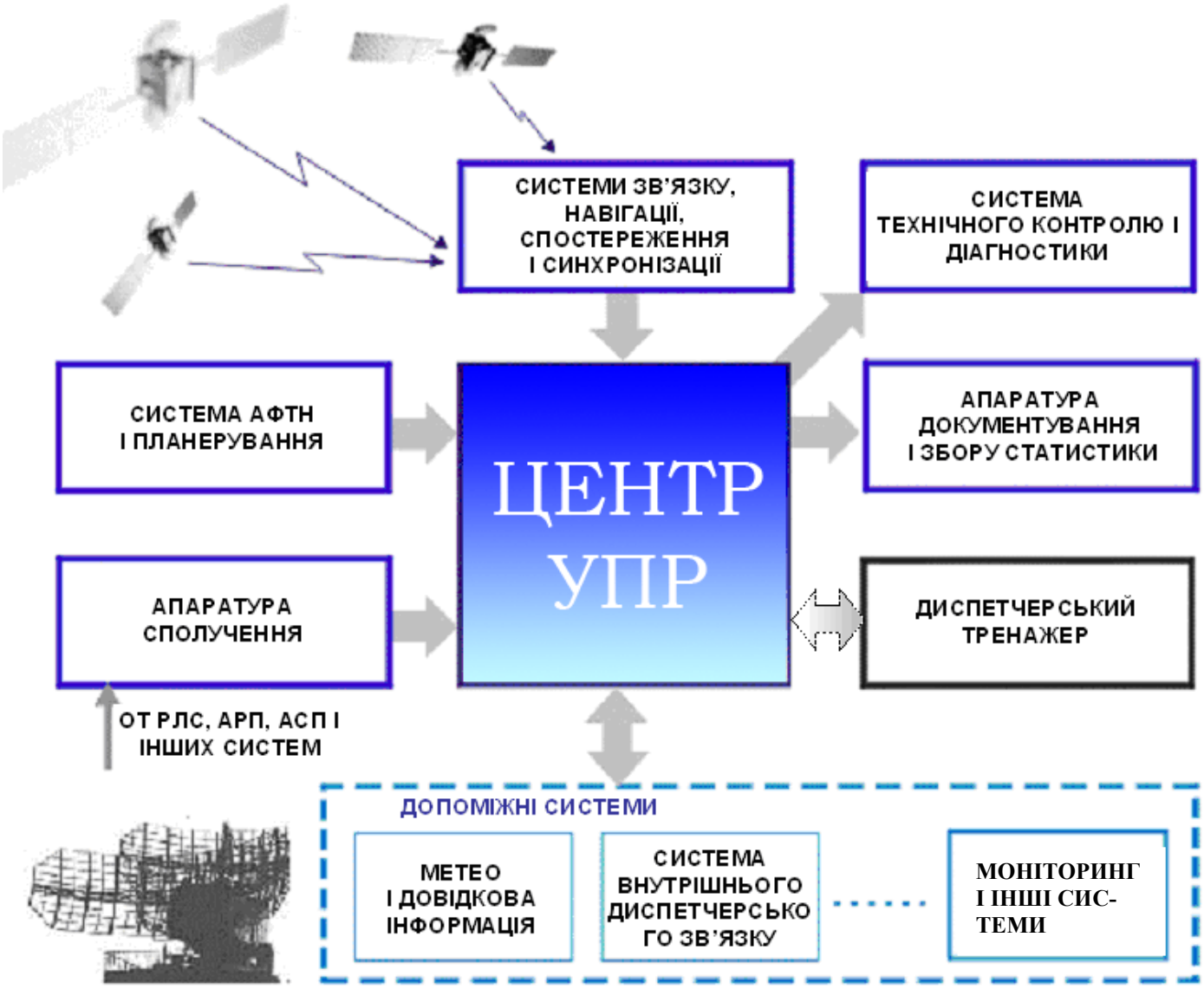

Рис. 1.3. Структурна схема АС УПР

1.5. Загальна характеристика сучасних телекомунікаційних технологій в авіаційних телекомунікаційних мережах (ATN)

Сучасний період науково-технічного прогресу характеризується стрімким розвитком телекомунікаційних систем і мереж. Характерною рисою цього розвитку є впровадження прогресивних телекомунікаційних технологій , які базуються на цифрових методах передачі , приймання та обробки повідомлень. Еволюційний розвиток телекомунікаційних технологій добре відбиває так звана "хвильова теорія" розвитку[16, 17]. Її суть в тому, що будь-яка нова технологія поступово з'являється на ринку, досягає, залежно від попиту, максимального поширення, після чого поступово зникає з ринку. Схематично хід такої еволюції показаний на рис.1.4.

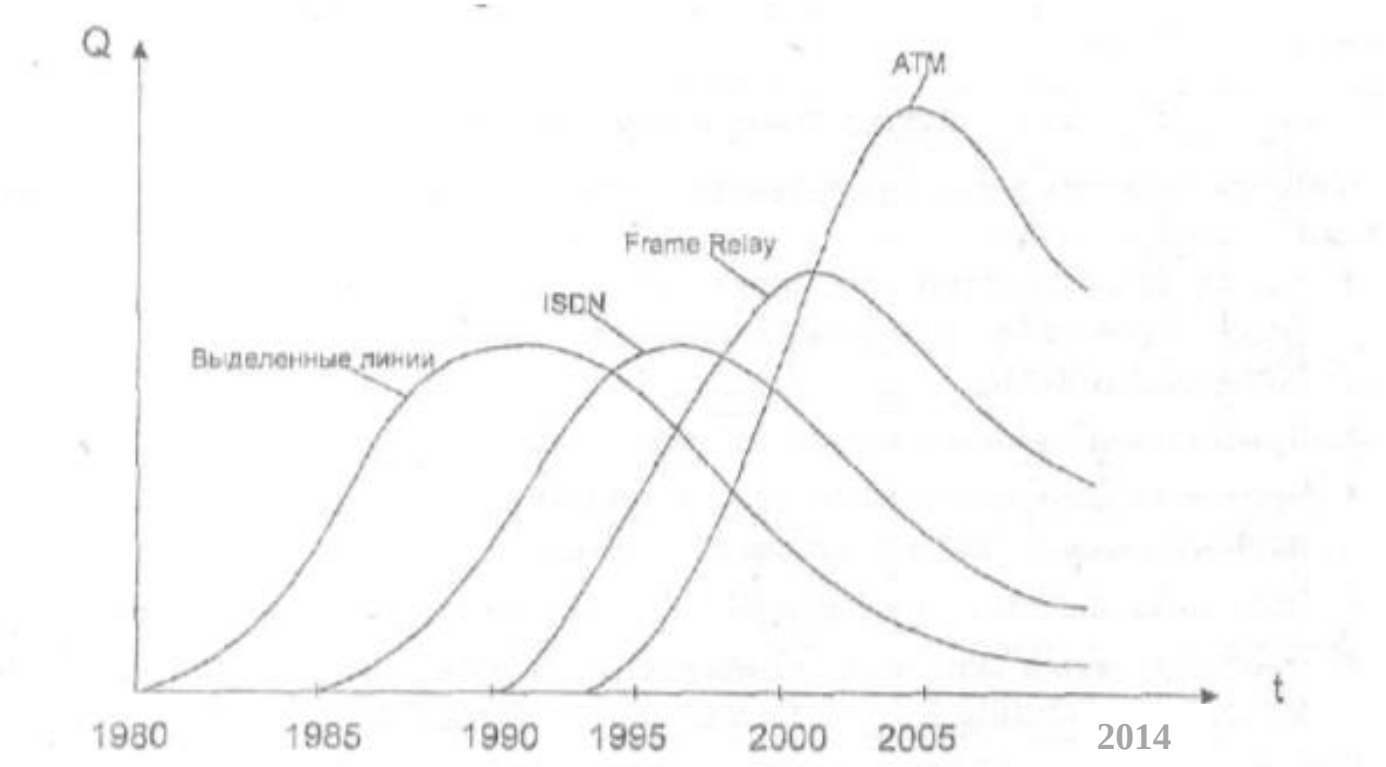

Рис.1.4. Розвиток окремих цифрових телекомунікаційних технологій

ISDN і Frame Relay. Обсяги Q використання виділених цифрових ліній передачі поступово знижуються. Попит на асинхронну технологію ATM поступово підвищується. Для кожної країни або окремого регіону хід кривих на рис. 1.4 може відрізнятися за термінами настання піків та їх амплітудам, однак загальний характер сімейства таких кривих, як правило, зберігається. Причиною зміни технологій за-

звичай є велика економічна конкурентоспроможність нових технологічних рішень в порівнянні з діючими технологіями . При цьому не виключається можливість співіснування різних технологій (наприклад, ISDN і FR). Першим етапом перехода від аналогової до цифрової первинної мережі був етап створення інтегированих цифрових мереж IDN (Integrated Digital Networks) в галузі цифрової телефонії. У мережах передачі даних в цей період на дільницях "вузол-вузол" починається використання виділених цифрових каналів мережі PDN (плезіохронна цифрова ієрархія). Це істотно підвищило якість передачі і стимулювало розвиток пакетної комутації (наприклад, протокол X.25). Подальший розвиток телекомунікаційних технологій вимагало зростання пропускної здатності мереж та об'єднання телефонії і передачі даних на єдиній цифровій основі. Це дало поштовх до переходу від IDN до ISDN. Технологія ISDN забезпечила транспортну середовище для передачі цифрового потоку від користувача до користувача. Якість цифрових каналів виявилася настільки високою, що протокол X.25 став збитковим і з нього стало можливим виділити алгоритми відновлення та квітування даних. В результаті з'явився протокол Frame Relay (FR). Структура протоколу FR має багато спільного зі структурою протоколів ISDN , тому що основні технології базуються на протоколі ITU-T G921/G931. Третім етапом удосконалення сучасних телекомунікаційних технологій є введення широкосмугових послуг, інтеграція їх з ISDN і перехід до B-ISDN (Broadband ISDN - широкосмугова ISDN) з ростом обсягів використання технології ATM. Технологія ATM в даний час дозволяє інтегрувати в єдиний трафік різні за характером потоки різних користувачів і тому є більш складною, ніж попередні технології [18, 19].

1.6. VPN як засіб збереження конфіденційності передаваних даних.

Як відомо, VPN (Віртуальна приватна мережа, англ. Virtual Private Network) — це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Internet). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією [20].

Напевно, самою головною задачею технології VPN є забезпечння захисту потоків даних, що передаються по загальнодоступних мережах. Постає питання відносно захисту таких даних від несанкціонованого використання та крадіжки.

Питання безпеки – важлива частина концепції впровадження нових інформаційних технологій у всі сфери життя людства. Тому широкомас-штабне використання обчислювальної техніки та телекомунікаційних систем призводить до якісно нових можливостей несанкціонованого доступу до ре-сурсів та даних інформаційної системи, тобто до їх високої вразливості. Фо-рмула успіху будь-якої діяльності проголошує : «Хто володіє достовірною та повною інформацією – той володіє ситуацією, хто володіє ситуацією – той в праві управляти нею в своїх інтересах, хто вміє управляти – той здатен пе-ремагати» [21]. Таким чином, управління безпекою обчислювальних систем охоплює широке коло питань, в число яких входить: забезпечення цілісності, конфіденційності та автентичності інформації; розмежування прав користу-вачів по доступу до ресурсів автоматизованої системи; захист автоматизова-ної системи та її елементів від несанкціонованого доступу. Тому, інформація, як сукупність знань про фактичні дані та залежностях між ними, стала стратегічним ресурсом; вона – основа для створення будь-якого рішення.

Назалежно від використовуваного ПО, усі VPN працюють по наступних принципах:

1. Кожен з вузлів ідентифікує один одного перед створенням тунеля, щоб упевнитися, що шифровані дані будуть відправлені на потрібний вузол.
2. Обидва вузли вимагають заздалегідь налаштованої політики, що вказує, які протоколи можуть використовуватися для шифрування і забезпечення цілісності даних.
3. Вузли звіряють політики, щоб домовитися про використовувані алгоритми; якщо це не виходить, то тунель не встановлюється.
4. Як тільки досягнута угода по алгоритмах, створюється ключ, який буде використаний в симетричному алгоритмі для шифрування/розшифровки даних.

Реалізація VPN може також принести додаткові грошові витрати, і, як усі інші, має недоліки та переваги. Основними перевагами використання будь-якого VPN є

перш за все безпечність передачі даних по віртуальній приватній мережі та наявність власної захищеної мережі при фатично відсутності фізичного мережевого з’єднання. Недоліки VPN присутні не в самій технології VPN, а в способі її проектування і реалізації.

Існує багато реалізацій VPN, проте рекомендується використовувати VPN на основі маршрутизаторів. Цей спосіб надає багато варіацій налаштування віртуальної приватної мережі, можливим це стає завдяки гнучким налаштуванням мережі осередком веб-інтерфейсу вище згаданого мережевого пристрою.

VPN є дуже гарним способом захисту конфіденційних даних, проте є деякі нюанси, які можуть навести на думку про недоцільність використання технології віртуальних приватних мереж, нижче приведений опис деяких з них.

По-перше, необхідно сказати, що в будь-якій сучасній мережі переважає використання мережевих пристроїв, таких, як маршрутизаторів. Маршрутизація полягає в можливості передавати пакети даних між мережами будь-яких типів. Застосування маршрутизаторів дозволяє використовувати комірчасті мережеві топології, забезпечуючи альтернативні шляхи доставки пакетів. Недоліком сучасних маршрутизаторів є те, що *процес обробки пакетів даних маршрутизатором складний і тривалий, він вимагає витрат процесорного часу та пам'яті*. Тому при недостатній потужності маршрутизатора та великого за об’ємом трафіку, VPN створює достатні затримки при пересиланні пакетів.

По-друге, випливає із першого пункту, що якщо пакети можуть передаватися по різним шляхам, частина пакетів може не дійти до отримувача або прийти з великим відставанням. З іншого боку, розпаралелення передачі задійснює інші маршрутизатори мережі, при чому значно збільшується швидкість обробки та пересилання даних.

Виходячи з вище приведених факторів, необхідно чи модернізовувати усю мережу передачі даних, застосовувати більш потужне мережеве обладнання або якимись способами зменшувати час обробки маршрутизатором пакетів. У пригоді стає фрагментація пакетів. Завдякій цій технології можливий поділ пакетів на більш дрі-

бніші з доданням до кожної із складових частин додаткового заголовку пакету, за допомогою якого стає можливим подальший збір фрагментів у єдине ціле.

Існує дві альтернативні стратегії для відтворення вихідних пакетів із фрагментів. Перша заключається в тому, щоб фрагментація пакету, що викликана мережею з пакетами малих розмірів, залишалась прозорою для обидвох хостів, що обмінюються пакетами. Цей варіант зображений на рис.1.5,а. З'єднання мережі навіть не уявляють те, що в них під боком пакети «страшним способом» нарізаються, а потім знову склеюються. В мережах АТМ навіть є спеціальна апаратура для забезпечення прозорої фрагментації пакетів (розбиття на комірки) та оберненого склеювання комірок в пакети. В світі АТМ фрагментацію називають сегментацією. Концепція при цьому зберігається такою же, а відмінності є лише в деяких деталях. Прозора фрагментація є простою тому, але, тим не менш, створює певні проблеми. Головна із них – всі фрагменти повинні виходити через один і той же шлюз. Таким чином накладається заборона на використання фрагментами різних шляхів до кінцевого отримувача, і в результаті може бути втраченою частина продуктивності. На кінець, процеси фрагментації та наступної збірки пакетів при проходженні кожної з мереж з малим розміром пакетів призводять до додаткових накладних витрат. Мережам АТМ необхідна саме прозора фрагментація.

Інша стратегія фрагментації заснована на відмові від відтворення пакетів із фрагментів на проміжних маршрутизаторах. Як тільки пакет опиняється розбитим на пакети, з кожним фрагментом поводяться як з окремим пакетом. Всі фрагменти проходять через вихідний шлюз (чи декілька вихідних шлюзів), як показано на рисунку 1.5,б. Задача відтворення ж оригінального пакету покладена на отримуючий хост. Так працює IP.

З непрозорою фрагментацією зв'язані свої проблеми. Наприклад, вона потребує, щоб кожен хост зміг відтворити пакет із фрагментів. Крім цього при фрагментації великого пакету стрімко збільшуються сумарні накладні витрати, так, як кожен фрагмент повинен мати заголовок. Однак перевага непрозорої фрагментації зберігається при можливості використання для передачі фрагментів декількох різних маршрутів, що підвищує продуктивність [22].

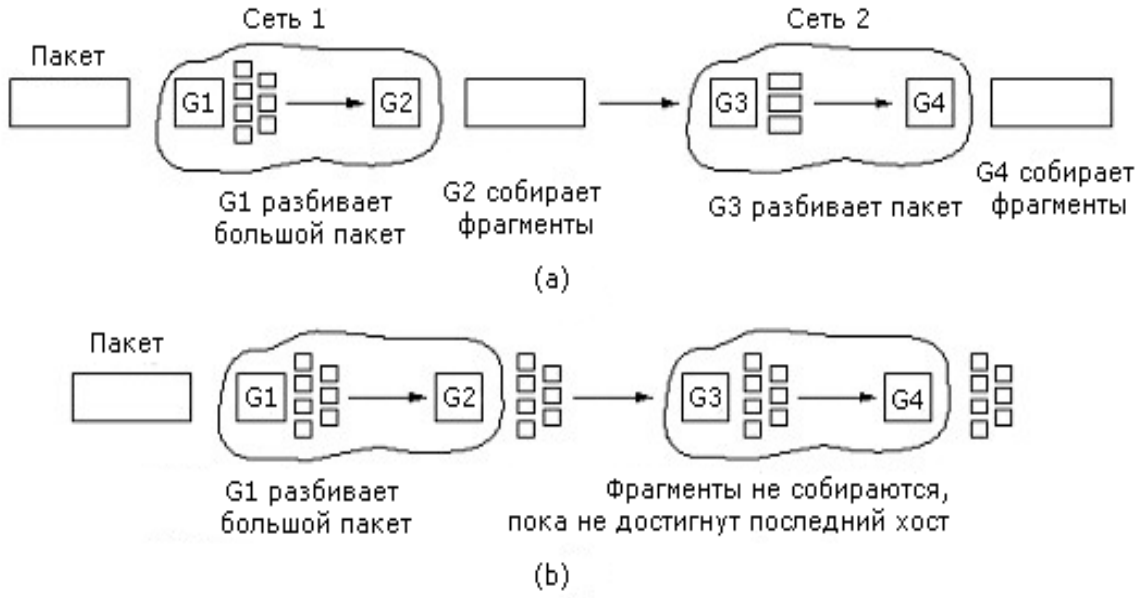

Рис.1.5. Прозора (а) та непрозора (б) фрагментації

Аналізуюче два типи фрагментації, необхідно зробити висновок – у кожної є свої недоліки. Проте, якщо при прокетуванні мережі, по якій будуть передаватися конфіденційні дані, припустити що:

1) глобальна мережа матиме непрозору фрагментацію (по умовчанню, для того щоб розвантажувати магістральні маршрутизатори);

2) локальна мережа авіапідприємтсв матиме прозору фрагментацію (для контролю цілісності передаваних даних),

то тоді недоліки фактично компенсуються один одним. Аргументувати це положення можливо таким чином:

1. Звичайно відстань між авіакомпаніями та Центром УПР велика. Логічно, що на великій відстані потребується велика кількість маршрутизаторів при розгалудженій глобальній мережі провайдерів Інтернет. Тут здійснюється баланс у паритеті велика відстань передачі даних – один маршрутизатор, що збирає фрагменти пакетів в єдине.

2. Між підприємством та Інтернет-провайдером мала відстань. Маршрутизаторів може бути не так уж і багато. В цьому випадку здійснюється баланс у паритеті невелика кількість проміжних маршрутизаторів, що збирають фрагменти пакетів в єдине мала відстань передачі даних до мережі провайдера.

Для визначення оптимального розміру фрагменту пакету, при якому будуть підтримуватись:

1) мінімальний показник помилкових бітів при передачі даних (BER);
2) максимальна швидкість передачі даних по мережі;
3) мінімальний показник затримки пакета (Delay),

тобто будуть підпримуватись найвищі показники QoS, необхідним буде експериментальна перевірка оптимального розміру фрагментів пакетів.

ВИСНОВОК ДО РОЗДІЛУ 1

Проведений аналіз Концепції безпеки польоту в цивільній авіації. На підставі Концепції в кожній державі має бути створена державна програма по безпеці польотів (ДПБП). Основною частиною програми по безпеці польотів є система збору польотних даних про події, які створюють або можуть створити загрозу для експлуатації повітряного судна. Ця система надалі повинна використовуватися при створенні бази даних авіакомпанії.

Існуюча база даних використовується тільки для накопичення статистики, а не як джерело інформації для запобігання небажаним подіям які відбувалися раніше, і зменшення ризику до прийнятного рівня при експлуатації повітряних суден.

При створенні НКС ОПІ повинні виконуватись завдання, які передбачені державними і міжнародними авіаційними правилами. При цьому структура обладнання автоматизованого робочого місця для обробки інформації бортових параметричних і мовних реєстраторів повинна відповідати передбаченим вимогам і допускати можливості періодичної модернізації.

Раніш створені засоби управління повітряним рухом в основному застарілі і практично виробили свій ресурс. Багато з них вимагають заміни. Тому виникла необхідність створення, розробки і впровадження нових систем. Ці системи повинні будуватися на базі стандартних обчислювальних засобів з використанням засобів відображення широкого застосування і стандартних засобів системного і загального програмного забезпечення.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1) створити вище вказану структуру бази даних авіакомпанії для виконання вимог і рекомендацій ІКАО. Взаємозв'язок між елементами такої структури має бути надійним і рентабельним, а елементи - взаємозамінними;

2) у центрах або дільницях обробки польотної інформації структура робочого місця має бути цілком комп'ютеризованою. Програмне забезпечення і комп'ютерні інформаційні технології мають бути орієнтовані на обробку записів бортових

реєстраторів всіх типів ПС, які допущені до перетину повітряного простору України;

3) розробити інформаційно-обчислювальну мережу АС ЄЦОАПІ, яка дозволила б максимально розвантажити операторів ЄЦОАПІ, а також працюючи в реальному режимі часу, при усуненні нештатних ситуацій (особливо конфліктів ПС), змогла б швидко адаптуватися і перерозподілити обчислювальні і мережні ресурси.

Під час розроблення методики та дослідження засобу створення комп'ютеризованої системи моніторингу польотної інформації на основі VPN необхідно належну увагу надати питанню захисту даних, що будуть передаватися по каналам зв'язку АС ЄЦОАПІ. Для цього необхідно, обрати реалізацію та протокол VPN.

Для обслуговування даних, що передаються в телекомунікаційних системах авіапідприємств, рекомендується використовувати протокол ATM по причині його досить широкого застосування для передачі конфіденційних даних та перевазі його при передачі відео- та аудіоінформації.

Для підвищення сумарної швидкості доставки пакетів в мережі VPN знадобиться проводити фрагментацію та дефрагментацію пакетів для підвищення сумарних показників QoS передачі даних.

Рекомендується використати реалізацію віртуальної приватної мережі на основі маршрутизаторів по причині легкій конфігурації та гнучкому налаштуванню віртуальної приватної мережі на основі VPN.

РОЗДІЛ 2
РОЗРОБКА МОДЕЛІ РОЗПОДІЛЕНОЇ КОМП'ЮТЕРНОЇ СИСТЕМИ ОБРОБКИ І ЗБЕРІГАННЯ ДАНИХ

2.1. Структура системи управління базами даних

Управління безпекою польотів пов'язане зі збором, накопиченням (зберіганням), обробкою, аналізом, а також володінням інформацією про попередній, поточний і майбутній стан авіаційно-транспортної системи. З цього витікає необхідність розробки і впровадження баз даних (БД), причому управління БД повинні визначатися рівнем користування, тобто, міжнародним, державним, відомчим і корпоративним рівнями.

Міжнародний рівень. На цьому рівні основою є розробка, що використовується Європейським координаційним центром системи пред'явлення даних про АП, – система ADREP. ADREP є методикою обробки даних і створення повідомлень за допомогою модифікованій Системі представлення даних про авіаційні події/інциденти у всьому світі. Після отримання звітів ADREP від держав, вся інформація перевіряється і вводиться в пам'ять ЕОМ. Ці звіти є банком даних про світові авіаційни події, при цьому розроблені заходи щодо забезпечення конфіденційності інформації про БП [23,24].

У ІКАО початок автоматизованої обробки даних про АП та ПАП був покладено в 1976 р. введенням у дію системи ADREP. У зв'язку з цим було видано Керівництво за поданням даних про авіаційні події (інциденти), основні розділи якого містять інструкції щодо порядку складання звітів про АП і ПАП та подання їх до ІКАО, а також інструкції зі складання та подання запитів про видачу інформації з системи. Керівництво містить також перелік показників та їх значень, використовуваних для опису обставин і причин АП та ПАП, а також кодові позначення цих показників і зразки формалізованих звітів для введення в систему.

Так як розслідування АП займає, як правило, значний період часу то дані в систему представляються двічі: у вигляді попереднього звіту, а потім у вигляді інформаційного звіту. У попередній звіт включається інформація, яка може бути отримана протягом перших трьох-чотирьох тижнів розслідування: короткий опис події, обставин, рекомендації щодо забезпечення безпеки, вжиті заходи. Інформаційний звіт в систему ADREP направляється по завершенні розслідування та затвердження остаточного звіту відповідним органом держави, яка проводить розслідування. Інформація попереднього і повного звітів ділиться на інформацію обов'язкового і рекомендованого подання.

На базі наявного масиву відомостей про АП і ПАП в системі ADREP ІКАО представляє державам наступну інформацію:

Щомісячні зведення попередніх звітів за попередній місяць;

Щорічні збірники статичних даних про АП та ПАП, що містять узагальнені дані за типами НД, видам АП і тенденціям у зміні відносних показників безпеки польотів.

Відповіді на запити з конкретних проблем по можливості в найкоротші терміни після надходження запиту.

Таким чином, ІКАО за допомогою бази даних систем ADREP здатна представляти державам найширшу інформацію з різних аспектів безпеки польотів і для проведення різного роду досліджень з метою запобігання АП та ПАП.

В даний час практично у всіх країнах, що мають розвитку цивільну авіацію і високий рівень безпеки польотів є або інтенсивно розробляються національні АСУ, за допомогою яких відбувається збір та обробка даних про АП та ПАП. Стандарти і рекомендації ІКАО з розслідування авіаційних подій розроблені з метою забезпечення якості розслідування, участі зацікавлених держав у розслідуванні та вжиття заходів з попередження авіаційних подій як окремими країнами, так і в рамках ІКАО в цілому. Вони стосуються в основному питань охорони місця події, повідомлення про подію, організації розслідування та звітності за його результатами.

Для того, щоб була досягнута максимальна ефективність, перш за все, необхідно, щоб основні методи кодування інформації були сумісні з іншими системами представлення даних. Мова йде про державні і відомчі бази даних, оскільки це є важливим для електронної обробки даних (EDP) [25,26].

Окрім цього, в рамках ІКАО на міжнародному рівні впроваджені і ведуться спеціалізовані бази даних, наприклад, бази даних про зіткнення з птахами (Керівництво за системою інформації ІКАО про зіткнення з птахами (IBIS) (Doc 9332)), "база даних про технічні характеристики аеропортів (Довідник з двосторонніх угод про повітряні сполучення (Doc 9511) і ін.

Державний рівень. Додаток 13 рекомендує державам створювати бази даних про авіаційні події та інциденти в цілях сприяння ефективному аналізу інформації про БП. В той час згідно вимог директив Європарламенту 2003|42|ЕС від 13.06.2003р. - прийнятний рівень БП не може бути досягнутий при малій інформативності системи повідомлень, що реалізовується кожною державою - членом окремо. Тому:

1. Держави - члени призначають одну або декілька компетентних адміністрацій для запуску механізму збору, оцінки, обробки і зберігання повідомлень про небезпечні події, що надходять від держав.

2. Компетентна адміністрація зберігає зібрані повідомлення в базі даних.

3. Інформація про серйозні інциденти та авіаційні події повинна також зберігатися в цій базі даних.

У роботі [11] визначена класифікація подій, які загрожують, або, якщо їх не усунути, можуть загрожувати ПС особам, що знаходиться в ньому, або будь-яким іншим особам.

Спираючись на "Положення про систему управління безпекою польотів на авіаційному транспорті", ЄЦОАПІ створює базу даних з метою ефективного аналізу отриманої інформації, у тому числі за результатами розслідування авіаційних подій і добровільних сповіщень про небезпечні чинники та розробками профілактичних заходів.

Що стосується *відомчого рівня*, то Глобальним планом по забезпеченню БП ІКАО передбачається створення баз даних в масштабах галузі (Глобальна ініціатива БП №6 "Ефективна система уявлення і аналізу даних про помилки і інциденти в галузі", п.3) [27].

Корпоративний рівень. Окрім державних систем представлення даних про інциденти авіакомпаніям, постачальникам обслуговування ЄЦОАПІ, а також експлуатантам аеропортів пропонується мати свою внутрішню систему про небезпечні чинники та інциденти [7]. Корпоративні БД будуються на основі обраної або виробленої стратегії управління БП в авіакомпанії.

Згідно визначення, база даних – це сукупність даних, організованих за певними правилами, що передбачають загальні принципи опису, зберігання і маніпулювання даними, незалежна від прикладних програм [28].

Слід зазначити, що при виборі бази що, будь-яка БД за своєю суттю або ж за своїм змістом є тільки часткою інформаційної системи, а інформаційна система включає в себе не лише зберігання даних, але і їх обробку.

Згідно з матеріалами наведених документів розробимо структуру розподільної бази даних (РБД).

Розподільна база даних – це система баз даних, в яких самі дані територіально або іншим чином розсіяні, тобто знаходяться в декількох абонентських системах інформаційної мережі. Як правило, розподільна база даних створюється як інтеграція (сукупність) групи баз даних, що вже функціонує у ряді систем [29,30]. Такі бази даних називаються гетерогенними тому, що в кожній конкретній абонентській системі унікальна організація зберігання даних і всі об'єкти є автономними.

Для роботи з БД потрібні програмні засоби, які могли б забезпечити створення і управління БД. Для цього існують Системи управління базами даних (СУБД): локальні і мережеві. Для реалізації нашого задачі вибираємо мережеві СУБД, оскільки локальні - це СУБД, що працюють на одному комп'ютері. Мережеві (серверні) ж СУБД дозволяють використовувати декільком комп'ютерам одну й чу саму БД, при цьому працюють за допомогою технології клієнт-сервер [31,32].

При побудові такої бази, за основу була прийнята архітектура ANSI-SPARC, яка є результатом багаторічного дослідження, насамперед того, як може підтримуватися незалежність даних в системі баз даних. Система управління базами даних і її застосування мають тривалий термін дії, тоді як засіб накопичення даних або зовнішні інтерфейси модифікуються або розширюються протягом певного часу.

2.2. Забезпечення збереження інформації

Відповідно з вимогами ІКАО, які викладені в доповненні до конвенції (Доповнення Е від 03.03.2006 р.) Чикаго, захист інформації про БП від неналежного використання є важливим елементом забезпечення постійного доступу до неї. Використання цієї інформації в інших цілях, окрім забезпечення безпеки польотів, може ускладнити отримання такої інформації в майбутньому з негативними наслідками для вирішення задач БП.

Заборона неналежного використання означає, що не допускається використання інформації про БП для цілей, які відрізняються від тих, для яких вона збиралася, таких, як використання інформації для дисциплінарного, цивільного, адміністративного і кримінального розгляду по відношенню до експлуатаційного персоналу і/або опрелюдненню гласності цієї інформації.

Згідно до рекомендацій ІКАО основним принципом захисту інформації є визначення того, що:

1) єдиною метою захисту інформації про безпеку польотів від неналежного використання є забезпечення доступу до неї, що гарантує можливість вживання відповідних і своєчасних привентивних заходів по підвищенню рівня безпеки польотів;

2) захист інформації про безпеку польотів не ставить за мету втручання в процес належного здійснення правосуддя;

3) захист конфіденційної інформації про безпеку польотів з врахуванням конкретних умов є складовою частиною зобов'язань держави щодо забезпечення безпеки польотів;

4) інформацію про безпеку польотів не слід використовувати в інших цілях, окрім тих, для яких вона збиралася;

5) з метою дисциплінарного, цивільного, адміністративного і кримінального розгляду інформація про безпеку польотів повинна використовуватися лише при наявності відповідних гарантій, передбачених чинним законодавством України.

Посадові особи, відповідальні за зберігання інформації про безпеку польотів, зобов'язані забезпечувати всі види можливого захисту від оприлюднення інформації.

Концептуальна схема БД БП зображена на рисл. 2.1. За своєю організацією вона є багаторівневою (ієрархічною):

1) БД Єдиного центру по обробці авіапригод та інцидентів (ЄЦОАПІ);
2) БД регіональних підрозділів;
3) БД авіакомпаній.

Запити в БД БП прямують як зверху вниз, так і знизу до верху. Запити зверху “вниз” - це, як правило, запити з метою отримання інформації про події, що мали місце поаторно. Ці запити поступають у всі авіакомпанії з періодичністю, яка визначається ЄЦОАПІ. Відповіді на запити обробляються в центральному сервері БД БП.

Запити "знизу до верху" - це, з одного боку, запити авіакомпаній щодо поточного стану проблеми безпеки польотів в регіоні, країні та світі. З іншого боку – це запити на розміщення і обробку інформації про екстремальні події: льотніх події і передумови до них, серйозніх інцидентів в повітрі і на землі, і, звичайно, про аварії і катастрофи. Запити на передачу даних про екстремальні події, за визначенням, передаються і обробляються з вищим пріоритетом.

За своїм типом БД БП є розподільною реляційною базою даних і знань зі всіма наступними вимогами:

1) оптимальний розподіл інформації між центральним сервером, регіональними підрозділами і авіакомпаніями;

2) оптимізація планів виконання запитів;

3) забезпечення необхідної якості сервісу (насамперед - достовірності передачі даних);

4) забезпечення захисту мережі від несанкціонованого доступу (НСД).

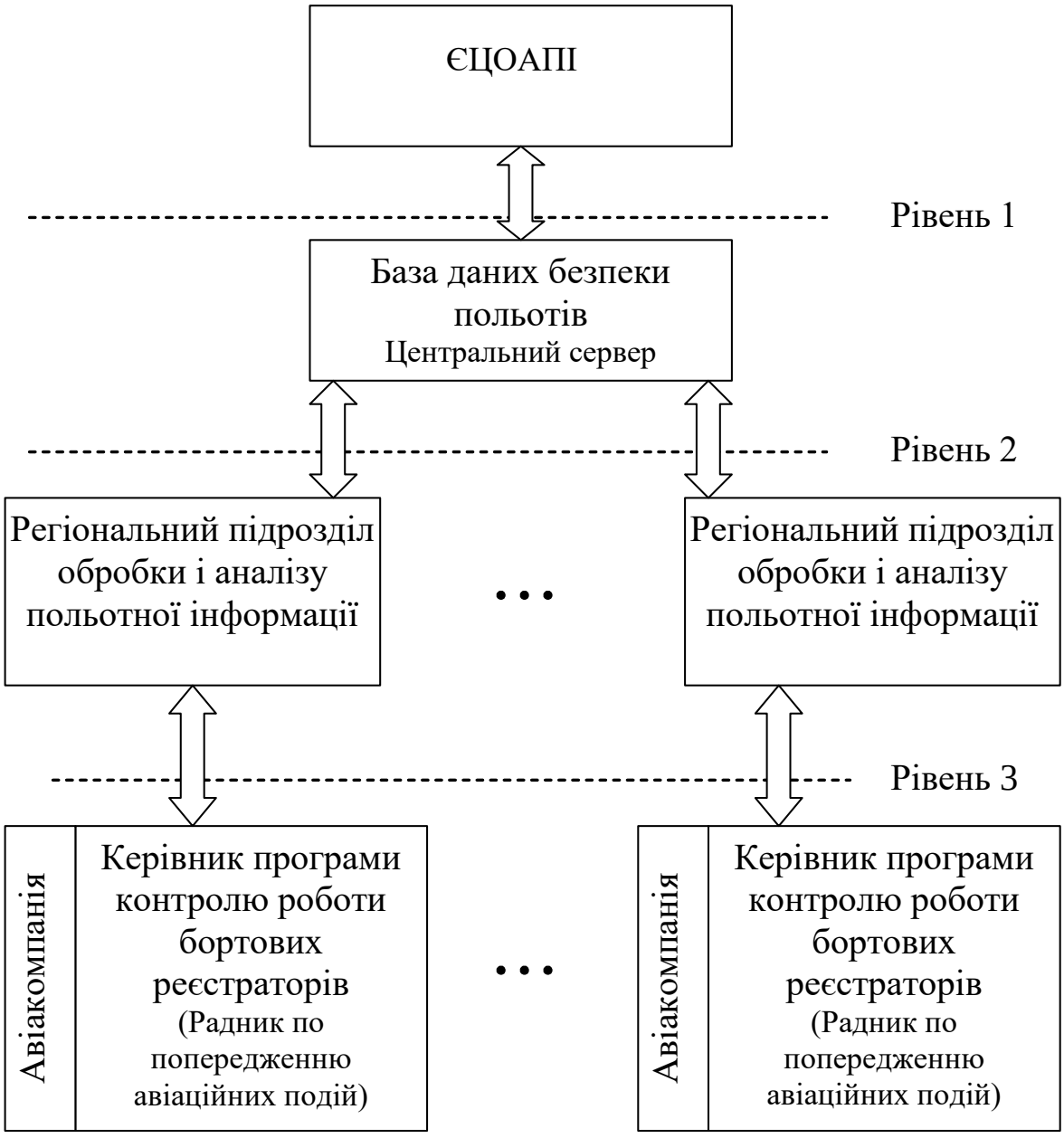

Рис. 2.1. Концептуальна схема БД БП

Очевидно, дві останні задачі є взаємозв'язаними. БД БП є структурою критичного використання за вимогами роботи в реальному масштабі часу і з міркувань

безпеки і захисту інформації. Втрата, модифікація або інші порушення цілісності інформації можуть спричинити серйозні і непередбачувані наслідки, аж до порушення роботи всієї авіаційної транспортної інфраструктури.

Враховуючи вище сказане, для ефективного функціонування БД БП, окрім використання високонадійного обладнання, необхідно забезпечити захист мереж передачі даних (МПД) від загроз різного походження, як техногенних і природних, так і через людський чинник. Відновлення пошкодженого устаткування пов'язане з великими матеріальними і часовими витратами. Потрібно з високою точністю визначити місце і характер пошкодження, внести відповідні зміни до трафіку, топології і алгоритмів роботи вузлів мережі на період її відновлення, відремонтувати пошкоджені ділянки і вузли мережі. В деяких випадках витрати на відновлення обладнання можуть бути значно нижчими, ніж збитки зв’язку з простоєм ділянки мережі.

Тому задача комплексного захисту інформації про безпеку польотів є надзвичайно актуальної.

Навантаження на мережу є випадковим і змінюється в широких межах в залежності від часу інтенсивності обміну інформацією в штатних і екстремальних ситуаціях та інших умов. Інформація про стан мережі як правило, не є повною і достовірною. Склад і характеристики устаткування мережі також відомі не повністю. Тому для аналізу мережі вцілому і її окремих фрагментів необхідно використовувати стохастичний підхід. При цьому в багатьох задачах фільтрації і управління в системах з випадковими параметрами і структурою можна обмежитися гауссовим наближенням, що практично грунтується на ефекті нормалізації законів розподілу в складних (великих) системах [33]. Це також полегшує аналіз.

Таким чином, мережу можна розглядати як гетерогенну, нестаціонарну, стохастичну структуру з гаусівськими розподілами параметрів.

За наявності систем захисту процес взаємодії об'єкта мережі і суб'єкта, який робить спробу проникнення (злому, несанкціонованого доступу - НСД), розглядатимемо як конфлікт між двома супротивниками:

1) перший - велика людино-машинна система захисту, яка обслуговує безліч об'єктів мережі, що захищаються;

2) другий - суб'єкт-зловмисник (надалі скорочено називатимемо його просто суб'єктом або супротивником досить високої кваліфікації, озброєний відповідними технічними засобами.

Відповідно до класичної теорії конфлікту [34] взаємодію між даними сторонами можна класифікувати як антагонізм з можливим переходом в суворе суперництво, а якщо в процесі взаємодії ефективність другої сторони зменшується швидше, ніж ефективність першої, можливий перехід в несуворе суперництво.

Дамо коротку характеристику найбільш вірогідних екстремальних станів мережі.

1. Спроба НСД з метою розкрадання або здійснення акту вандалізму. Ефект виявляється відразу; основні задачі - виявлення і розпізнавання для виключення інших станів (відмова обладнання, природні чинники - блискавка, підтоплення, зсув грунтових шарів, ураган і так далі). Необхідна негайна реакція, та певний час на нейтралізацію. На час локалізації спроби НСД необхідна перемаршрутизація транспортної підсистеми БД БП.

2. Спроба НСД з метою зняття інформації. Зовнішні ефекти можуть бути відсутніми. Основна задача - ідентифікація - виявлення противника за характером наслідків - потрібний час, інколи тривалий.

3. Раптова відмова обладнання. Виявляється відразу - виникає задача локалізації пристрою, що відмовив (вузла, блоку). Потрібний певний час на відновлення.

4. Поступова відмова устаткування: плавне збільшення числа помилок, збоїв аж до критичного значення - повної відмови. Необхідний постійний аналіз стану мережі. При стабільному зростанні числа помилок - локалізація критичного пристрою, перемаршрутизація трафіку.

5. Перевантаження мережі - збільшення затримки передачі інформації вище допустимої - перемаршрутизація трафіку.

6. Інші екстремальні ситуації, що виникають, наприклад, через людський чинник (низька кваліфікація або втрата лояльності персоналу), стихійні лиха, акти тероризму, не направлені спеціально проти інформаційно-телекомунікаційних мереж, і так далі.

Розглянемо задачу багаторівневого захисту МПД від спроб несанкціонованого доступу того або іншого типу.

Передбачимо, що об'єкт D_d, що захищається, знаходиться всередині N захищених споруд (екранів). При цьому виконуються наступні умови:

1. Кожен захисний екран є замкнутим. Його не можна обійти, а можна тільки подолати (розкрити).

2. Екрани вкладені один в одний за принципом матрьошки. Об'єкт, що захищається, знаходиться всередині останнього (внутрішнього) екрану. Таким чином, для проникнення всередину об'єкту необхідно послідовно розкрити всі N екранів, від першого (зовнішнього) до *N-го (*внутрішнього).

Якщо розглядати процес подолання *і-го* екрану як обслуговування якоїсь заявки, то, відповідно до класичного завдання теорії масового обслуговування, [35,36,37] тривалість обслуговування є випадковою величиною t_{pi} з показовим розподілом щільності ймовірності:

$$W_1(t_{pi}) = \gamma_i \exp(-\gamma_i t_{pi}) \text{ при } t_{pi} > 0 \text{ ;}$$

$$W_1(t_{pi}) = 0 \text{ при } t_{pi} < 0 \qquad (2.1)$$

де $\gamma_i > 0$ – постійна величина

або з розподілом щільності ймовірності Ерланга:

$$W_1(t_{pi}) = \gamma_i \frac{(\gamma_i t_{pi})^{k-1}}{(k-1)!} \exp(-\gamma_i t_{pi}) \qquad \text{при } t_{pi} > 0 \text{ ;}$$

$$W_1(t_{pi}) = 0 \qquad \text{при } t_{pi} < 0 \qquad (2.2)$$

де $\gamma_i > 0$ – постійна величина;

k – ціле позитивне число.

Позначимо середній час подолання *і-го* екрану через T_{pi} .

Для розподілу (2.1) , $$T_{pi1} = \frac{1}{\gamma_i} \tag{2.3}$$

а для розподілу (2.2) $$T_{pi2} = \frac{k}{\gamma_i} \tag{2.4}$$

Постійною γ_i є функція стійкості *і-го* рубежу захисту і кваліфікації суб'єкта.

Вирази (2.3 – 2.4) можна використовувати для оцінки параметра γ_i за експериментальними даними.

Задамо наступні умови:

$$T_{p1j} < T_{p2j} ... < T_{p,N-1,j} < T_{pNj}, \quad j = 1,2, \tag{2.5}$$

$$\sum_{i=1}^{N} T_{pij} > T_r \quad \text{з ймовірністю} \quad P_r \geq P_{r\min} \tag{2.6}$$

де T_r - час реакції на спробу НСД;

$P_{r\min}$ - гранично допустима (мінімальна) ймовірність виконання умови (2.6).

Умовою (2.5) визначається вимога наростаючої складності подолання рубежів захисту від першого до останнього.

При виконанні умови (2.6) гарантується своєчасність реакції на спробу проникнення і нейтралізації з ймовірністю не нижче гранично допустимої.

У даному випадку має місце процес послідовного подолання вкладених рубежів захисту, тобто послідовність переходів від стану i до стану $i+1, i=1,2,\ldots,N-1$ з ймовірністю переходу

$$P_{ij}(t_0,t) = P\{\vartheta(t) = \vartheta_j / \vartheta(t_0) = \vartheta_i\}, \; t > t_0, \; j = \begin{cases} i \\ i+1 \end{cases}. \tag{2.7}$$

Досягнувши N – го стани процес завершується. Відповідно, можна вважати, що на N – му рівні розташований поглинаючий екран. Необхідно оцінити середній час досягнення цього поглинаючого екрану.

Зворотний перехід від стану i до стану $i-1$ (у межах – до нульового стану) можливий, наприклад, при відмові суб'єкта від спроби НСД з якої-небудь причини. Оскільки така подія на етапі фізичного подолання системи інженерного захисту

спостерігається рідко, ймовірність такого переходу вважатимемо величиної другого порядку малості:

$$P_{i,i-1}(t_0,t)=0(t). \qquad (2.8)$$

У першому наближенні можна вважати, що ймовірність переходу

$$P_{ik}(t_0,t)=0(t),\ t>t_0,\ k>i+1 \qquad (2.9)$$

(подолання відразу двох і більше за рубежів захисту) також є величинами другого порядку малості.

Нарешті, для малих тимчасових інтервалів $\Delta t<<T_{pi1}$, $\Delta t<<T_{pi2}$, де T_{pi1}, T_{pi2} визначаються виразами (2.3) і (2.4) відповідно, ймовірність залишитися в попередньому стані описується виразом:

$$P_{ii}(t,t+\Delta t)=P\{\vartheta(t+\Delta t)=\vartheta_i / \vartheta(t)=\vartheta_i\}=1+a_{ii}(t)\Delta t+0(\Delta t), \qquad (2.10)$$

а ймовінірсть переходу із i стану в j стан – виразом

$$P_{ij}(t,t+\Delta t)=P\{\vartheta(t+\Delta t)=\vartheta_j / \vartheta(t)=\vartheta_i\}=a_{ij}(t)\Delta t+0(\Delta t). \qquad (2.11)$$

Величини $a_{ij}(t)$ - деякі невід'ємні безперервні функції, що мають сенс питомої ймовірності переходу із i стану в j стан.

З врахуванням умов (2.7-2.11) можна представити процес подолання рубежів захисту у вигляді послідовності процесів переходу від $i-$го рубежу до рубежу $(i+1)$. На кожному рубежі можуть мати місце два стани: перейти до наступного по порядку рубежу з вірогідністю $P_{i,i+1}(t_{0i},t)$ або залишитися в колишньому стані з ймовірністю $P_{ii}(t_{0i},t)$. Тут t_{0i} - момент переходу на поточний й рубіж.

Управління БД БП, як і будь-якою автоматизованою (великою) системою, неможливе без зворотного зв'язку. По каналам зворотного зв'язку поступають дані про внутрішній стан БД БП і ситуації, що складається на кожному периферійному об'єкті. Як наголошувалося вище, ці дані реєструються, аналізуються і обробляються в корпоративній інформаційній системі - базі даних і знань. Джерела даних організаційно і територіально розподілені, а самі дані різнорідні. В той же час правила доступу до даних мають бути одноманітними, а процедури доступу повинні виконуватися в реальному або квазіреальному масштабі часу. (Під квазіреальним мас-

штабом часу ми розуміємо роботу за наявності затримок, що не фіксуються оператором і що не приводять до паралізації БД БП.)

Для ефективного моніторингу стану мережі доцільно використовувати розподілену БД і З з реляційною системою управління (СУБД).

На рис. 2.2. зображена узагальнена структурна схема системи збору та обробки інформації про екстремальні стани регіональної мережі. Важливою особливістю її є наявність підсистеми обробки - розпізнавання типів екстремальних ситуацій. Обробка здійснюється в регіональній БД и З. Периферійні БД грають роль проміжних накопичувачів.

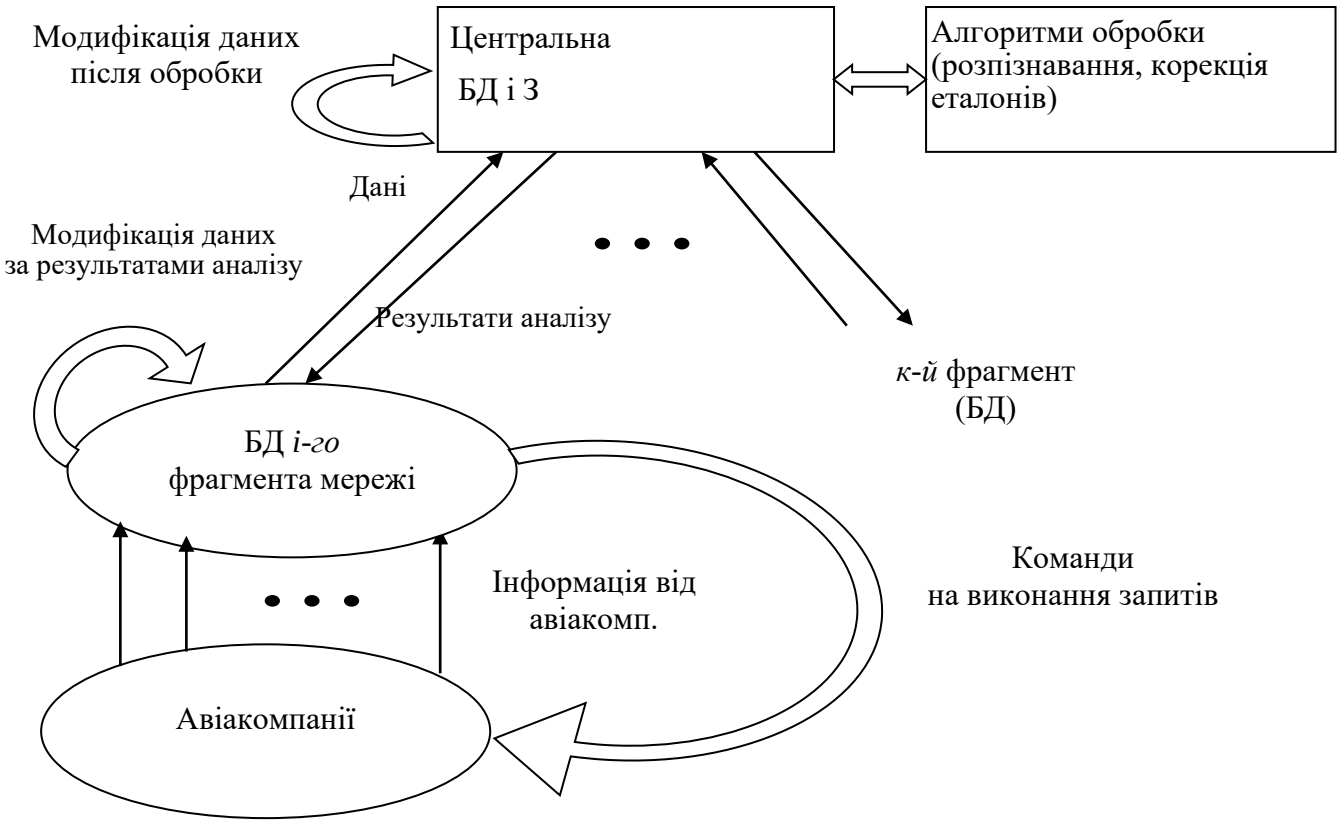

Рис.2.2. Структурна схема системи збору та обробки інформації

Для спрощення модернізації і нарощування БД БП, підключення нових об'єктів у роботі [34] пропонується використовувати СУБД типу MS SQL Server з мовою запитів SQL.

У роботах [38,39] наголошуються переваги використання SQL як стандартної мови запитів, насамперед, його статусу як загальноприйнятого стандарту. Крім того, в даний час розроблені методи перетворення запитів на мові SQL алгебраїчній фор-

мі. Це дозволяє використовувати реляційну алгебру як уніфікований інтерфейс реляційної СУБД.

Як видно на рисунку, система має структуру типу «віртуальної зірки» [39]: як центральна таблиця БД і 3, так і периферійні таблиці БД кожного з фрагментів є змінними. Вони, по-перше, оперативно створюються і заповнюються даними, що поступають від елементів БД БП. Подруге, за результатами обробки, відповідно до закладених алгоритмів, здійснюється модернізація цих таблиць.

Команди на виконання захисних дій можуть генеруватися автоматично. Проте ЛПР - оператор центру збору інформації - завжди може ухвалити своє рішення і дати пріоритетну команду на БД БП [38].

2.3. Структура бази даних ЄЦОАПІ

В процесі доступу до БД запит формується відповідною мовою (у нашому випадку SQL). Потім він піддається лексичному і синтаксичному аналізу. В результаті виробляється його внутрішнє уявлення, і запит перетворюється в алгебраїчну форму. Подальші етапи оптимізації плану і виконання запиту виконуються вже з використанням форми алгебри. Як наголошувалося раніше, при цьому спрощуються задачія оптимізації і взагалі функціонування розподіленої БД завдяки уніфікації і відносній простоті мови реляційної алгебри. Полегшується також вирішення задач побудови оптимізаторів з гнучкою структурою.

Завдяки частковій децентралізації і модульній архітектурі БД системи збору та аналізу інформації задача модифікації БД БП також спрощується: при змінах параметрів і структури даних БД і-го фрагмента не потрібно буде вносити зміни в БД j-го фрагмента.

Кожен підрозділ обробки і аналізу польотної інформації повинен в обов'язковому порядку передавати інформацію в базу даних ЄЦОАПІ. Це стосується і регіональних підрозділів.

Ці дані потрібні для збору інформації та обробки статистичних даних по тому або іншому виду відмов, з подальшою видачею певних рекомендацій для усунення або запобігання цих подій за даним типом ВС.

Об'єктивну оцінку можна отримати лише шляхом статистичної переробки результатів оперативного контролю безлічі польотів.

Зазвичай [22] під глобальними мережами мають на увазі мережі, які служать для представлення сервісу великій кількості кінцевих абонентів. Вони розкидані на великій території, в нашому випадку по Україні.

При проектуванні мережі, головною задачею є виконання основної функції мережі - забезпечення спільного використання ресурсів в реальному часі. Для виконання цієї задачі, мережа повинна відповідати вимогам продуктивності, надійності, сумісності, керованості, захищеності, розширюваності і масштабованості [35,40].

Продуктивність мережі визначає об'єм даних що передаються і час, потрібний на їх передачу. У мережах спільного призначення, для оцінки продуктивності мережі використовують наступні основні характеристики: час реакції, пропускну спроможність, затримку передачі і різні варіанти затримки передачі.

Надійність – це показник працездатності мережі, тобто, мережа виконує свої функції. Для технічних пристроїв зазвичай використовують показники надійності, такі як інтенсивність відмови, вірогідність відмови і середній час напрацювання на відмову, а також готовність або коефіцієнт готовності (відсоток часу, протягом якого система може використовуватись).

Безпека мережі означає здатність системи забезпечувати захист даних від несанкціонованого доступу.

Розширюваність - можливість порівняно легкого додавання окремих нових елементів мережі.

Масштабованість - це можливість нарощування розмірів мережі, у тому числі шляхом приєднання додаткових сегментів, при цьому продуктивність мережі не порушується.

Прозорість мережі - можливість мережі використовувати ресурси одним і тим же способом, не залежно від фактичного розміщення. Вона досягається на 2-х різних рівнях на рівні користувача і рівні програміста.

Підтримка різних видів трафіку - це можливість поєднувати функції різних мереж, наприклад, комп'ютерної, зв'язкової, телефонної та ін..

Сумісність мережі - це можливість мережі включати найрізноманітніше апаратне і програмне забезпечення.

Під *керованістю* мережі розуміють можливість централізованого контролю, виявлення і вирішення проблеми стану основних елементів мережі, а також планування розвитку мережі і виконання аналізу продуктивності.

Типовими абонентами глобальної комп'ютерної мережі є локальні мережі підприємств.

Повідомлення про події до авіаційної адміністрації в порядку виконання своїх посадових обов'язків направляють:

1) експлуатанти або командири ВС;
2) посадові особи служби ОВД;
3) менеджери аеропортів;
4) посадові особи організації по ТЕ;
5) інспектори по БП.

При знятті з літака бортових реєстраторів, вони передаються для обробки в центр обробки інформації, де відбувається зчитування, обробка і зберігання даних, обмін інформацією з авіакомпанією. Передача результатів обробки інформації відбувається по різних каналах. У авіакомпаніях створюється архів цих даних, паралельно відбувається обробка даних у двох напрямах: аналіз відмов і несправностей вузлів і агрегатів, а також аналіз техніки пілотування.

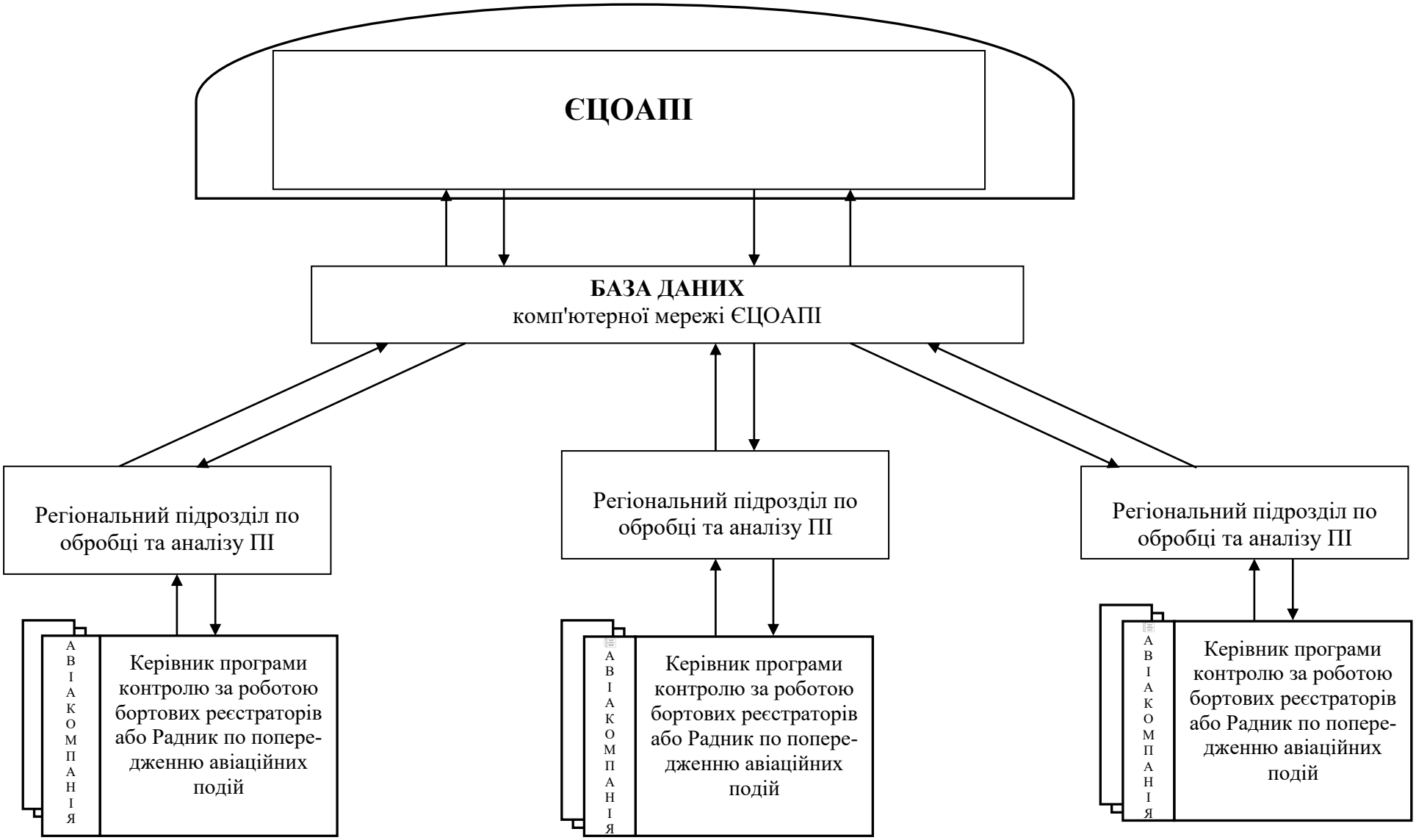

Рис.2.3. Структура бази даних ЄЦОАПІ

ВИСНОВОК ДО РОЗДІЛУ 2

При організації розподіленої бази даних безпеки польотів виникає дві зв'язаніх між собою задачі: забезпечення передачі даних з необхідною якістю і достовірністю і захист від несанкціонованого доступу. Ці задачі необхідно вирішувати в комплексі.

Для управління безпекою польотів і обробки позаштатних ситуацій необхідно застосовувати систему управління зі змінними параметрами і метод багаторівневої оптимізації запитів в розподіленій базі даних.

У розділі запропонована модифікована модель рубежів захисту на основі вкладених екранів. Тільки після подолання всіх рубежів зловмисник може проникнути всередину БД БП. При цьому поставлена умова гарантованої локалізації спроби НСД за час подолання всіх рубежів захисту.

Для побудови захищеної і при цьому досить швидкодіючої системи обміну інформацією на основі розподіленої БД і З, необхідно оптимізувати як структуру власне БД, так і структуру запитів, що циркулюють зверху вниз і знизу догори.

РОЗДІЛ 3
МЕРЕЖА БАЗ ДАНИХ ЄЦОАПІ НА ОСНОВІ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

3.1. Особливості відомчої магістральної цифрової мережі ЦА

Відповідно до рекомендацій керівних документів ІСАО, відомча мережа АНЕЗ (авіаційного наземного електрозв'язку) ЦА будується, як правило, на базі орендованих магістральних ліній передачі мереж загального користування (МЗК), зокрема мереж передачі даних (МПД). Ця особливість зумовлює техніко-економічну доцільність і необхідність:

1) облік і використання в АНЕЗ ЦА технологій мереж загального користування, зокрема, ISDN (PDH і SDH), ATM, IP/TCP;

2) шлюзування потоків повідомлень між АНЕЗ ЦА і МЗК;

3) використання для транспорту даних сучасних технологій пакетної комутації.

Особливість використання систем транспорту даних (СТД) в ЦА полягає у тому, що в результаті зрозумілих обставин (насамперед, необхідності дотримуватися суворих заходів безпеки) роль стандартизації, регламентації та уніфікації, в т.ч. обладнання ТД і правил його використання, має визначальне значення. З цієї причини, завдяки добре налагодженому міжнародному співробітництву по лінії ІКАО і ІТ, для задоволення потреб зв'язку у сфері авіаційного транспорту можливо і доцільно будувати однорідні мережі передачі даних. Це дає можливість орієнтуватися на використання АТМ обладнання. Особливо велике практичне значення для побудови авіаційних корпоративних СТД має той факт , що в найбільш поширених українських мережах ТД національного рівня (мережі "Укртелеком" і "Інфоком") в якості основного технологічного обладнання (в першу чергу, в мережах абонентського доступу) викори

стовується обладнання АТМ. Отже, існує можливість оренди такого обладнання для утворення корпоративних і (або) віртуально корпоративних мереж ТД в галузі ЦА [18, 52].

Топологічна структура транспортної мережі НВДП для АНЕЗ показана на рис.3.1. Вона являє собою полігональну мережу з головним комутаційним центром у м. Київ.

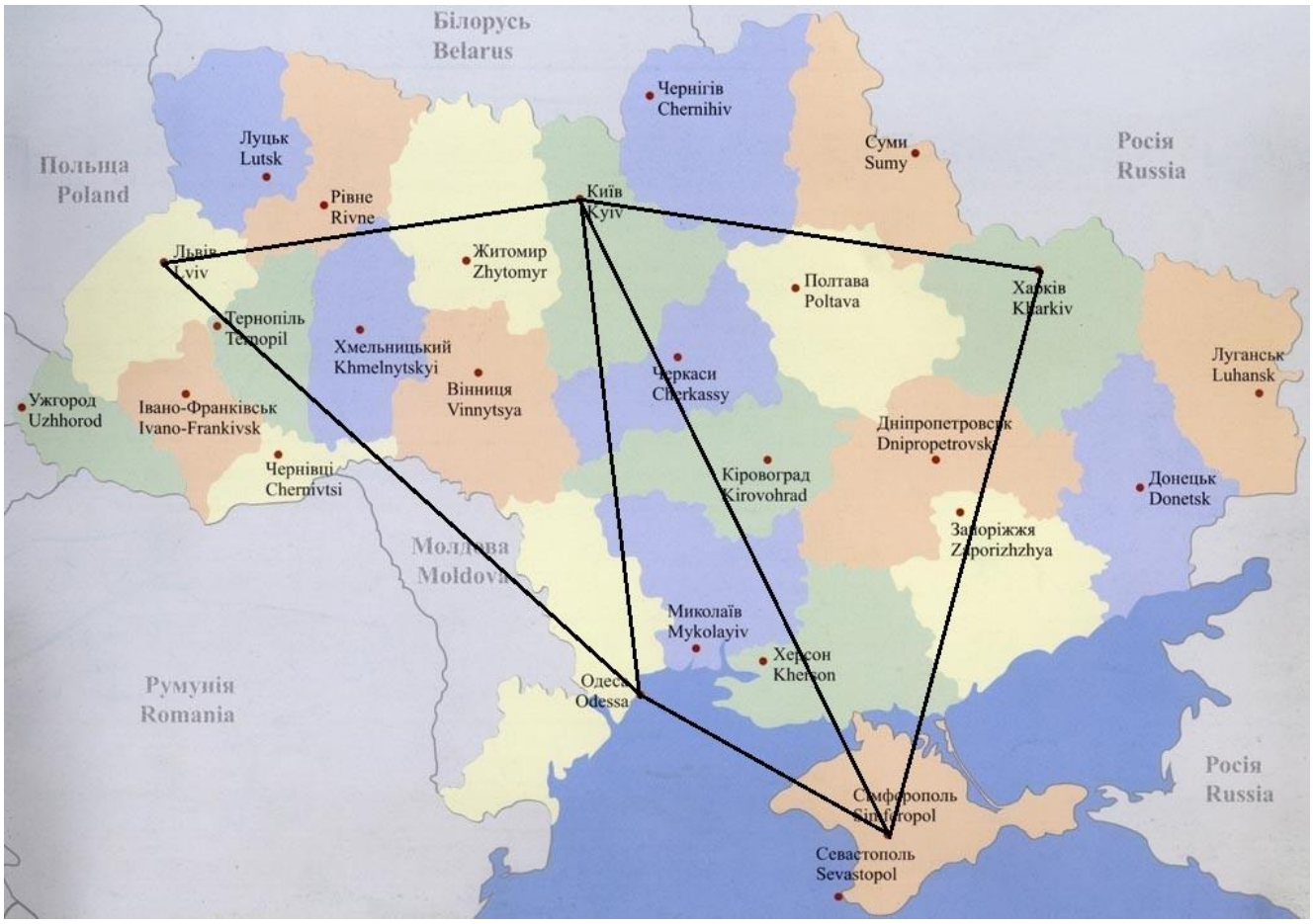

Рис.3.1. Топологічна структура транспортної мережі НВДП для АНЕЗ

Варіант узагальненої архітектури транспортної мережі передачі даних (МПД) між підприємствами ЦА, відображений на рис.3.2.

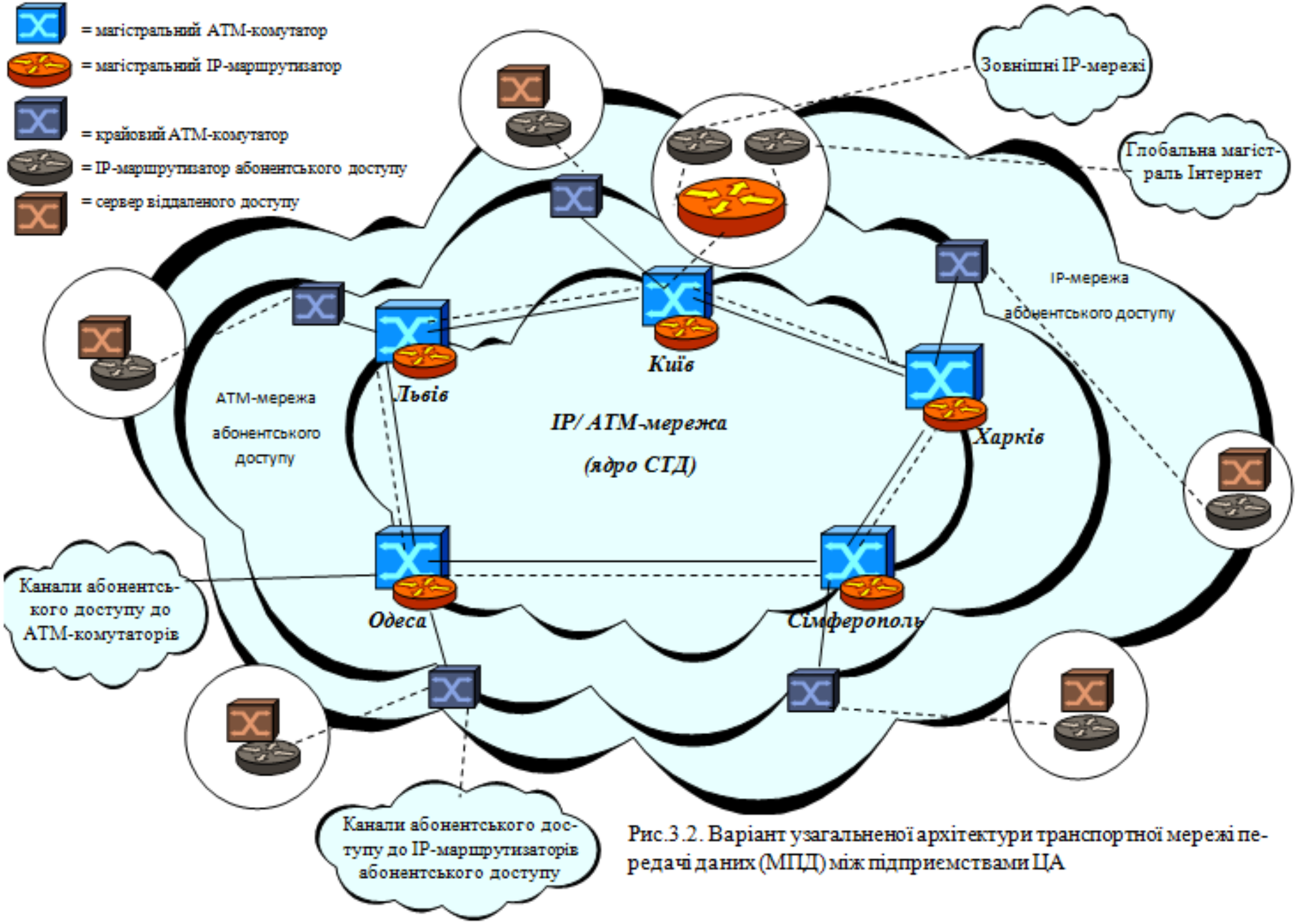

Рис.3.2. Варіант узагальненої архітектури транспортної мережі передачі даних (МПД) між підприємствами ЦА

Вона являє собою двошарову структуру. Внутрішній шар структурно представляє магістральну транспортну мережу, доступ до якої побудований на базі технологій ATM/ IP, а зовнішній шар утворює мережу абоненського доступу IP/ATM. Мережі абонентського обладнання ATM використовуються в двох основних напрямках застосування:

1) для забезпечення транспорту IP-пакетів від абонентних вузлів авіа підприємства до вузлів IP- мереж (як спеціалізованих, так і загального користування);

2) для організації підключень до магістральної транспортної мережі (тобто, до ядра СТД) з використанням HDLC - подібних протоколів.

Ядро транспортної мережі (внутрішній шар в архітектурі СТД) являє собою магістральну мережу ATM / IP. Її вузли з'єднуються між собою високошвидкісними магістральними каналами ТД за схемою "з резервуванням напрямків". Міжвузлові з'єднання в магістральній мережі здійснюються за технологією ATM. Пропускна здатність кожного магістрального каналу передачі даних у цій мережі - 155 Мбіт / с. Через неї циркулюють мультиплексовані потоки даних від магістральних ATM-комутаторів і IP- маршрутизаторів , а також комутаторів / маршрутизаторів мереж доступу. Зовнішній (по відношенню до ядра) шар у структурі СТД розділяється на два прошарки . Перший прошарок - це ATM- мережа абонентського доступу. Вузли цієї мережі приєднуються до ATM- комутаторів магістральної мережі через високошвидкісні канали ТД. У цих вузлах розташовані крайові IP- комутатори, до портів яких під'єднується авіапідприємство через канали абонентського доступу. Для передачі даних у мережі абонентського доступу використовується технологія постійних віртуальних каналів (PVC). Друга прошарок зовнішнього шару в структурі СТД - це IP- мережа доступу, призначена , головним чином, для надання послуг Internet і intranet . Вузли цієї мережі приєднуються до IP- маршрутизаторів магістральної мережі ATM/IP з використанням цифрових потоків типу E3 (зі швидкістю 34.368 Мбіт/с) , які утворюються за допомогою обладнання первинної мережі. Ця мережа може бути власністю держави , і надана в розпорядження Міністерству транспорту або бути власністю національних телекомунікаційних компаній (на Україні - АТ "Укртелеком" і "Інфоком").

Користувачі IP- мережі підключаються до вузлів доступу IP (до IP- маршрутизаторів абонентського доступу) за допомогою синхронних і (або) асинхронних некомутованих ліній, TDM- каналів, а також комутованих каналів телефонних мереж загального користування (ТМЗК). Через IP-мережу авіапідприємство може мати доступ до глобальної мережі Internet. Транспортна СТД повинна мати у своєму складі вузли взаємодії з іншими мережами. За допомогою обладнання пакетної маршрутизації вона повинна сполучатися з СТД інших національних операторів , а також підключатися до закордонних вузлам - зокрема , з метою організації інформаційного взаємообміну з підприємствами інших держав. Для вирішення завдань управління транспортної СТД та контролю за її працездатності необхідно створити відповідну мережу управління . Бажано реалізувати управління типу "out-of-band" [13,14]. Такий тип управління передбачає створення потоків сигналів управління та іншої технологічної інформації через фізично відокремлені канали зв'язку. Це сприятиме підвищенню живучості та надійності функціонування мереж, що дуже важливо в діяльності підприємств ЦА. Транспортна СТД повинна надавати більш широкий спектр мережевих послуг практично на всіх семи рівнях EMBOC [16]. На фізичному і канальному рівнях цієї моделі повинні надаватися послуги абонентського доступу до вузлів СТД. На канальному рівні - послуги транспорту фреймів (фрейм - це формат блоку даних у протоколах канального рівня) через ATM- канали , а також організація підключень до СТД з використанням протоколу IPSec та інших HDLC - подібних протоколів; на мережевому - послуга транспортування IP- пакетів; на сеансовому рівні і вище - базовий набір Internet - послуг, створення віртуальних приватних мереж, відеоконференцзв'язок і т.п. Слід підкреслити , що на базі СТД з використанням каналів ATM створена і діє національна транспортна мережа "Укртелекому", послуги якої на умовах оренди доступні підприємствам. Транспортна мережа "Укртелекому" забезпечує корпоративним клієнтам можливість об'єднувати свої локальні обчислювальні мережі (ЛОМ), які можуть бути розосереджені по всій території України і навіть за кордоном, в глобальні корпоративні мережі, здійснювати віддалений доступ до вузлів таких корпоративних мереж і т.п. Номенклатура надаваних послуг і глибина охоплення цими послугами території України постійно розширюються. Це дає

можливість "Укртелекому" надавати послуги за доступними цінами майже в будь-якому населеному пункті України, що, враховуючи специфіку розташування українських авіапідприємств, може бути в деяких випадках безальтернативній можливістю отримання доступу до корпоративних даних. Транспортну СТД, яка обслуговуватиме підприємство, доцільно побудувати на базі обладнання IP- маршрутизації і ATM комутації, а також серверів різного функціонального призначення. Функціональна й організаційна структура СТД повинна бути ієрархічних і багаторівневою, а топологія – близька до «зірки» . Для об'єднання вузлів СТД між собою доцільно використовувати цифрові канали первинної мережі з пропускною здатністю від 34.368 до 155 Мбіт/с. Само собою зрозуміло, для забезпечення доступу користувачів до магістральної СТД існують відповідні мережі абонентського доступу. При цьому слід розрізняти мережі абонентського доступу, що забезпечують доступ до вузлів транспортної мережі канального рівня (тобто, до ATM- комутаторів) з метою отримання послуг транспортних каналів, та мережі абонентського доступу до IP- вузлів (зокрема, з метою отримання Internet- послуг, а також для хостингу або побудови віртуальних приватних мереж). В обох вищеназваних типах мереж абонентського доступу в якості абонентських каналів використовуються будь-які доступні для користувачів канали зв'язку: аналогові або цифрові, комутовані або виділені канали тональної частоти, фізичні лінії (двопровідні або чотирипровідні), оптичні канали, канали радіодоступу і т.д. Вибір каналів доступу здійснюється з урахуванням наявних можливостей щодо підключення та місця розташування абонентського обладнання і вузлів СТД [45]. Один з можливих варіантів фізичної топології СТД представлений на рис.3.3.

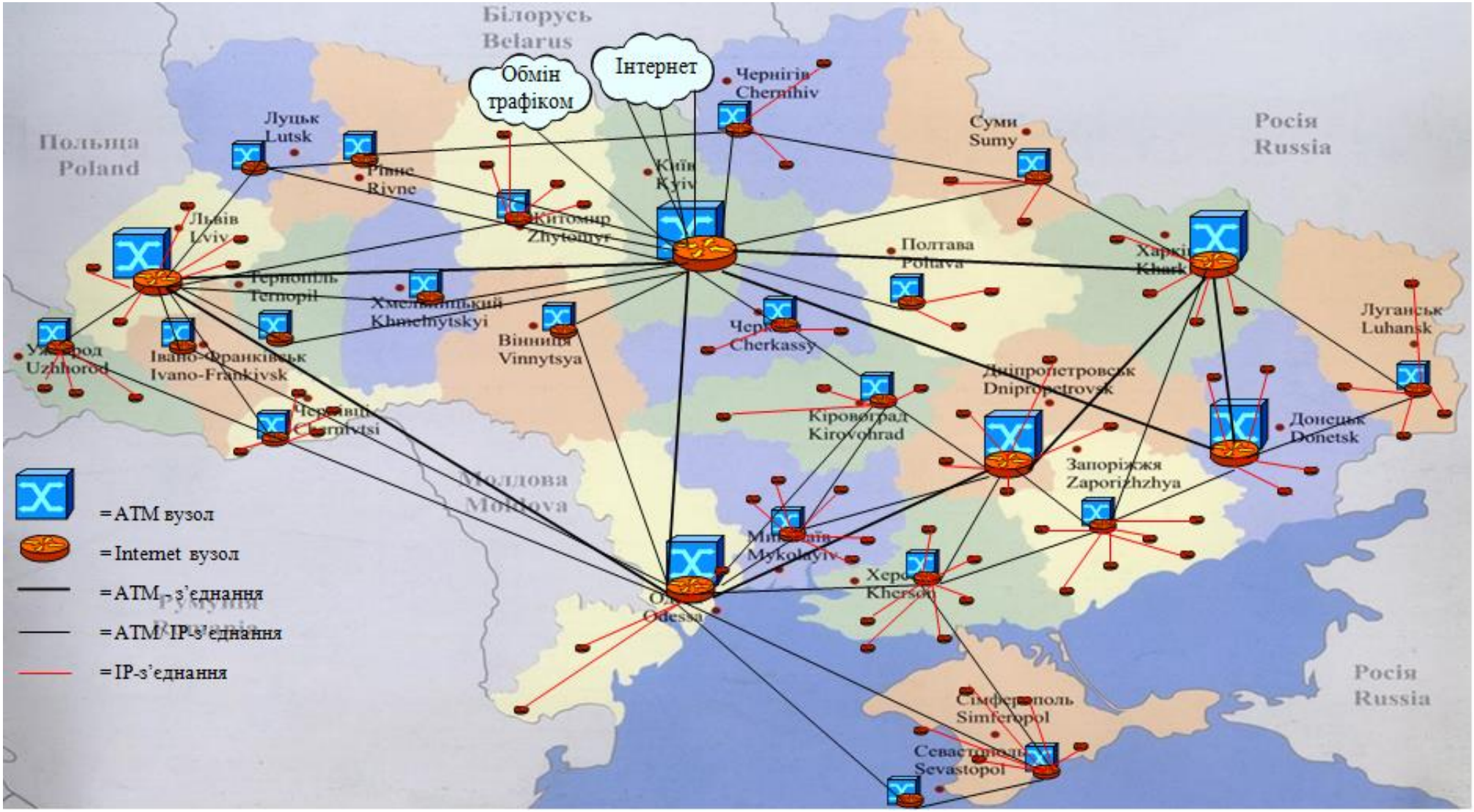

Рис.3.3. Один із можливих варіантів фізичної топології СТД

Згідно з цим варіантом , з урахуванням існуючої МПД, регіонально - транзитні вузли (РТВ) у Харкові, Дніпропетровську, Донецьку, Одесі та Львові з'єднані з центральним вузлом (ЦВ) у м. Києві за допомогою цифрових каналів первинної мережі з пропускною здатністю 155 Мбіт / с. Для передачі даних між регіонально - транзитними вузлами і центральним вузлом в сучасних умовах найбільш придатною є технологія АТМ [4]. Регіональні вузли (РВ) в обласних центрах України доцільно з'єднати з регіонально - транзитними вузлами за допомогою цифрових каналів первинної мережі з пропускною здатністю n x 34.368 Мбіт / с. Кожен регіональний вузол бажано підключити ще, як мінімум , до одного вузла свого чи вищого ієрархічного рівня. Для передачі даних між регіональними та регіонально - транзитними вузлами слід використовувати технології АТМ і IP [45].

До складу центрального вузла у м. Києві доцільно включити:

1) магістральні маршрутизатори, маршрутизатори абонентського доступу, міжмережеві шлюзи (національні та міжнародні);

2) магістральні АТМ- комутатори та комутатори / мультиплексори абонентського АТМ доступу.

До складу регіонально - транзитних вузлів СТД у містах Харків, Дніпропетровськ, Донецьк, Одеса та Львів бажано включити:

1) магістральні маршрутизатори, маршрутизатор абонентського доступу, а також міжмережеві шлюзи;

2) магістральний АТМ- комутатор і комутатори / мультиплексори абонентського АТМ -доступу. Магістральні АТМ- комутатори з'єднуються між собою через цифрові канали первинної мережі зі швидкістю 155 Мбіт / с. До складу регіональних вузлів СТД , які розміщуються в обласних центрах України, входять:

1) маршрутизатори абонентського доступу ;

2) комутатори / мультиплексори абонентського АТМ-доступу. Кожен з регіональних маршрутизаторів повинен з'єднуватися з регіонально-транзитними магістралями маршрутизаторами через цифрові канали первинної мережі зі швидкістю 34.368 Мбіт / с. У межах СТД, що обслуговує підприємство, доцільно створити і розвивати два види мереж абонентського доступу: IP- доступ і АТМ- доступ.

3.2. Вимоги щодо якості надання послуг в ATN. Критерії QoS

Поняття якості, відповідно до ITU -T, E.430 і E.800, формулюється як "сукупність показників, що характеризують задоволеність користувача наданими телекомунікаційними послугами". Складовими частинами оцінки якості послуги є три основні стадії надання послуги: доступ до передачі даних , передача даних, завершення сеансу передачі (порушення з'єднання). Кожна з цих стадій характеризується трьома основними показниками: швидкість, достовірність, гарантованість . Представлене визначення показників якості в рекомендації E.430 є базовим для інших рекомендацій ITU -T щодо якості послуг для різних типів мереж .

У рекомендації X.140 для СТД загального користування (PDN - Public Data Network) параметри не залежать ні від структури мережі, ні від послуги . Так, основними параметрами якості обслуговування мереж PDN (зокрема, мережі ATM) є наступні:

1) затримка доступу; імовірність організації неправильного доступу; ймовірність відмови у встановленні доступу;

2) затримка передачі інформації користувача; швидкість передачі інформації користувача; ймовірність помилок передачі інформації;

3) вірогідність передачі зайвої інформації ; ймовірність помилкової доставки інформації користувача; ймовірність втрати інформації користувача;

4) затримка в руйнуванні з'єднання; ймовірність відмови в роз'єднанні доступу;

5) доступність послуги, ймовірність відмови у передачі інформації користувача; час недоступності послуги.

Перераховані вище параметри організовані відповідно до концепції QoS , представленої в рекомендації ITU- T E.430 . Остання група параметрів є похідною від основних, і тому вони в об'єднану табл. 3.1 не увійшли.

Таблиця 3.1.

Показники якості

Фаза надання	**Показники якості**		
	Швидкість	**Точність**	**Гарантовність**
Організація доступу	Затримка встановлення доступу	Імовірність організації невірного доступу	Імовірність відмови при встановленні доступу
Передача даних	Затримки передачі даних користувача Швидкість передачі даних користувача Пропускна здатність	Імовірність помилки в інформації користувача Вероятность передачи лишней информації Імовірність передачі зайвої інформації Імовірність помилкової передачі інформації	Імовірність втрати інформації користувача
Роз’єднання доступу	Затримка звільнення мережевого з’єднання	Імовірність невдалого завершення мережевого з’єднання	Імовірність неуспішного звільненя мережевого з’єднання

Основними параметрами QoS, які важливі в ATN для кінцевих користувачів, є затримка передачі повідомлення T_3, пропускна здатність системи зв'язку R_o і коефіцієнт помилок K_o. Ці параметри в ATN використовують для прогнозування рівня QoS в підмережах, через які проходить маршрут між кінцевими користувачами. Від рівня QoS безпосередньо залежать також орендні витрати D_a на надання послуг користувача протягом певного часу T_a (надання каналу зв'язку на термін T_a) .

Затримка T_3 визначається як час, що минув між моментом передання одиниці інформації на рівень MAC і моментом успішного її отримання відповідним обладнанням приймача. Наприклад, в СТД ACARS математичне сподівання плюс середнє квадратичне відхилення затримки проходження становить близько п'яти секунд. В системі AMSS норми на Т3 залежать від пріоритету повідомлення Q , швидкості передачі і напрями - до ПС або від ПС (табл.3.2.).

Таблиця 3.2.

Затримка повідомлення в AMSS

Швидкість передачі, Кбіт/с	Максимальна затримка встановлення з'єднання,с	Транзитна затримка, с			Затримка передачі даних, с		
		до ПС		від ПС	до ПС		від ПС
		Q=15	Q=3	Q=15	Q=15	Q=3	Q=15
0,6	70	12	40	40	15	110	80
1,2	45	8	25	30	9	60	65
2,4	25	5	12	15	6	30	35
4,8	25	4	7	13	5	20	30
10,5	25	4	5	13	4	10	30

Пропускна здатність R_0 (біт / с) визначається типом лінії передачі (каналу передачі), використовуваної в системі зв'язку. Зазвичай в реальних умовах при бінарної кодуванні швидкість передачі інформації $R_t < R_0$. Ступінь цієї нерівності оцінюють продуктивністю системи . Продуктивність визначається як відсоток пропускної здатності каналу зв'язку , яка споживається для успішної передачі інформації на фізичному рівні :

$$P = R_t < R_0.$$

Величина p зазвичай нормується з урахуванням допустимого значення $T_з$. Так, в системі ACARS (США) $p < 0,45$. Для системи VDL / CSMA $p < 0,6$, в одноканальних лініях передачі AFTN відносна завантаженість $p < 0,4$.

Коефіцієнт помилок K_o при передачі дискретних повідомлень нормується залежно від типу каналу зв'язку, типу інформаційної технології та методу підвищення завадостійкості системи зв'язку. Для кінцевих користувачів мережі ATN в каналах з технологією ISDN та циклічної кодуванням рівень бітових помилок BER (Bit Error Rate) оцінюється значенням 11 жовтня. При технології ATM як K_o використовують відносна кількість загублених ячейок $\gamma_r \leq 10^{-7}$.

Розглянутий перелік основних параметрів QoS може бути розширений залежно від призначення системи зв'язку та характеру розв'язуваних завдань. Наприклад, параметри QoS можуть бути використані для оцінки ефективності засобів захисту інформації.

3.3. Основні принципи побудови віртуальних приватних мереж

Віртуальна приватна мережа (Virtual Private Network - VPN) є логічною мережею, яка створюється поверх іншої мережі. У нашому випадку, наприклад, Інтернет. Сама технологія віртуальної приватної мережі застосовується в тих випадках, коли потрібний захист корпоративної мережі від вірусів, від несанкціонованого доступу, а також від інших погроз. При використанні Інтернет, як транспортного середовища, організація VPN через Інтернет є "туннулювання" транзитних пакетних мереж. Для передачі даних через VPN, ці дані зникають "з поверхні" в точці відправки і знов з'являються тільки в точці призначення, тобто створюється логічний тунель в мережі Інтернет, який з'єднує дві крайні точки. Цей процес називається "тунелювання". При попаданні в Інтернет - тунель, дані при цьому ще й шифруються, інформація стає невидимою для інших користувачів. Все це забезпечує додатковий захист переданої інформації. Протоколи шифрування бувають різні, вибір протоколу залежить від вибору VPN-рішення. Правильно побудована віртуальна приватна мережа може принести тій або іншій організації велику користь.

На рис.3.4. пропонується віртуальна мережа ЄЦОАПІ. На базі цієї мережі, через VPN - тунелі відбувається обмін даними. Це обмін між основними корпоративними (мережа авіакомпанії), регіональними і магістральною (магістральна мережа ЄЦОАПІ) мережами з БД БП ЄЦОАПІ.

До переваг віртуальної приватної мережі хотілося б віднести такі показники, як, гарантія захищеного трафіку, направленого через Інтернет, а також достатню гнучкість при розширенні мережі (прогноз на майбутнє).

При цьому зберігається висока надійність і безпека. Обмін інформацією між віддаленими сайтами здійснюється негайно, а користувачі при доступі до системи не відчувають себе ізольованими від неї. До основних недоліків можна віднести лише одне – висока вартість, але при використанні менш швидкісних каналів зв'язку, віддалені користувачі насамперед відмітять недолік в швидкості, а потім і перераховані вище переваги стануть менш очевидними.

Основне завдання забезпечення якості обслуговування в мережі – мінімальні втрати інформації при її передачі. Найбільш реальний шлях рішення цієї задачі - фрагментація пакетів і розподілена передача. Розглянемо особливості фрагментації пакетів:

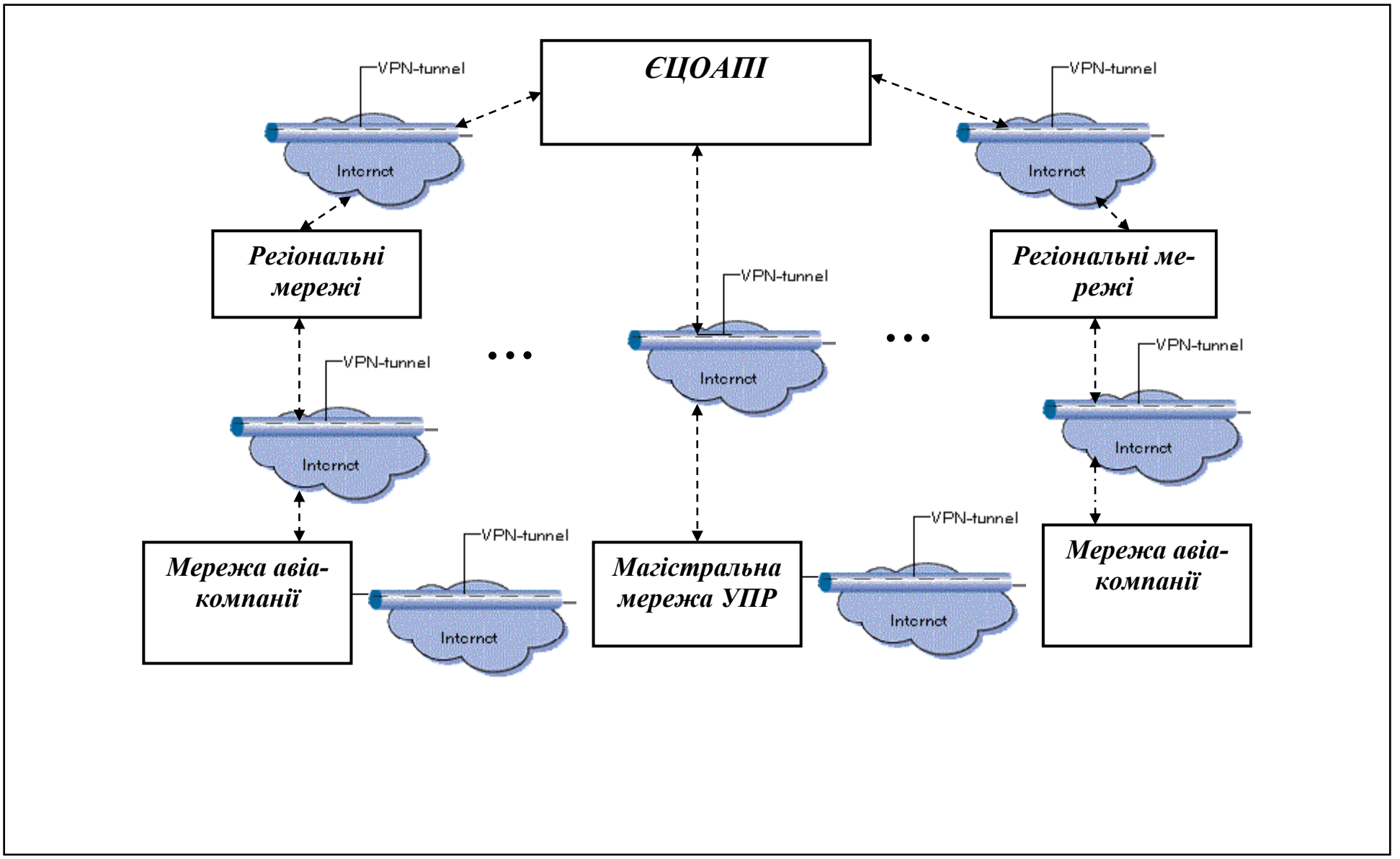

Рис.3.4. Віртуальна мережа ЄЦОАПІ

3.4. Адаптація процесів організації запитів до бази даних

Розподілена БД безпеки польотів, по суті, є інформаційно-обчислювальною системою, що складається з N пристроїв обробки і зберігання, М клієнтських застосувань і ієрархічної системи управління базою даних. У спільному випадку M≠N. У кожному пристрої обробки і зберігання (сервер) виділена область пам'яті об'ємом (i=1, n) тільки для зберігання інформації БД БП.

Крім того, в мережі можуть бути К серверів, що грають роль пристроїв проміжного зберігання даних системи управління безпекою польотів. Дані з цих серверів використовуються для вирішення завдань прогнозування, локалізації і обробки позаштатних ситуацій, що виникають.

Припустимо, що вся інформація БД БП є множина блоків

$$\{aj\},\ j=1,\ldots,m \qquad (3.1)$$

де aj об'єм кожного блоку інформації, причому не обов'язково, щоб ці об'єми були однакові для кожного блоку.

Кожен сервер може звернутися до будь-якого іншого сервера за будь-яким числом блоків з множиною {aj} і отримати необхідні дані. Час, який витрачається на отримання цих даних, залежить від об'єму необхідної інформації, стану каналу передачі (наприклад, тунеля віртуальної приватної мережі), наявності і довжини черги, числа транзитних вузлів комунікації.

Крім того, кожен сервер в межах свого об'єму пам'яті може мати деяку кількість інформації, для звернення до якої додаткового часу не потрібно.

Заявки на обслуговування, що поступають з СУБД, містять перелік службової інформації, деяку необхідно використовувати при обслуговуванні кожного завдання-заявки. Кожна j-я заявка характеризується множиною I, інформаційних блоків БД, що використовуються для обслуговування цієї заявки в ІОМ.

Дисципліну обслуговування в штатній ситуації природно пов'язати з середнім часом рішення задачі на виділеному для цього сервері, в пам'яті якого є частина необхідної інформації. Решта необхідної інформації, що залишилася, сервер отримує від інших джерел.

У позаштатній ситуації дисципліна обслуговування цілком визначається пріоритетом нової задачі, що виникає. Очевидно, що більшість (або навіть всі) задачі штатних ситуацій відкладаються в черзі, поки не буде вирішено задачу, що виникає.

Таким чином, мета адаптації (оптимізації, налаштування) системи полягає в тому, щоб розподілити ресурси ІОМ відповідно до наступних правил:

1) дисципліною обслуговування, тобто правилом напрямку чергової заявки на один з серверів, керуючись при цьому даними про параметри необхідних блоків інформації, стан пам'яті всіх серверів мережі і їх завантаження;

2) правилом розподілу даних по серверах мережі.

Задамо кодову матрицю $U = \|u_{ij}\|$, елементами якої є двійкові змінні, визначальна наявність $(u_{ij} = 1)$або відсутність $(u_{ij} = 0)$ в пам'яті *i-го* сервера *j-го* блоку даних. Очевидно, що має місце наступне обмеження, пов'язане з кінцевими розмірами області пам'яті, що виділяється на кожному сервері для зберігання даних БД БП:

$$\sum_{j=1}^{m} a_j u_{ij} \le C_i,\ i=1\ .,m \tag{3.2}$$

Припустимо, що потік заявок на запити даних утворюється з *K* різних потоків, кожен з яких характеризується своїм дискретним розподілом ймовірності використання блоків інформації $\{a_j\}$:

$$P_l = (P_{1l},...,P_{ml}), l = 1,...,k \tag{3.3}$$

де P_{jl} - ймовірність того, що при рішенні задачі l – го потоку буде потрібно j – й блок інформації. Без втрати загальності задачі можна ввести спрощуючи правила нормування:

$$\sum_{j=1}^{m} P_{jl} = 1, \tag{3.4}$$

хоча це і не обов'язково, тому що при запиті по тому або іншому завданню може бути потрібно декілька блоків даних.

Визначимо ймовірність попадання завдання l – го потоку на *i-й* сервер при наступній простій і цілком логічній дисципліні обслуговування: задача прямує для ви-

рішення на той сервер, де частина спільного об'єму необхідних даних більш всього. Вираз має наступний вигляд:

$$P_{li}(U) = \frac{\sum_{j=1}^{m} U_{ij} P_{lj}}{\sum_{i=1}^{n} \sum_{j=1}^{m} U_{ij} P_{ij}} \tag{3.5}$$

Аналогічно визначаємо ймовірність того, що для вирішення задачі *l-го* потоку, направленого на *i-й* сервер, знайдеться вся необхідна інформація, і звертатися до всієї бази даних не доведеться:

$$\overline{P_{li}} = P_{li}(U).$$

Приймемо середні інтенсивності потоків запитів для задач, що вирішуються $\lambda_1,...,\lambda_k$ і середні інтенсивності обслуговування (доставки заявок і рішення задачі) $\mu_1,...,\mu_n$.

Тоді проста задача оптимального розміщення блоків даних (3.1) на серверах, при якому мінімізується загальна інтенсивність запитів до БД:

$$Q(U) = \sum_{i=1}^{n} \sum_{l=1}^{k} \lambda_i \left[1 - \overline{P_{li}}(U)\right] P_{li}(U) \to min \tag{3.6}$$

де

$$S: \begin{cases} \sum_{l=1}^{k} \lambda_l P_{lj}(V) \prec \mu_i \\ \sum_{i-1}^{m} a_i u_{ij} \le C_i, \qquad i = 1,...,n. \end{cases} \tag{3.7}$$

$$V^T = \| \; V_{11,} ... V_{n1,...} V_{nm} \; \| \tag{3.8}$$

Таким чином, функціонал $Q(U)$ характеризує середню інтенсивність запитів всіх серверів мережі.

Обмеження (3.7) пов'язані з пропускною спроможністю системи: при порушенні хоча би одного з них черга необмежено зростає. Необхідно також враховувати обмеження області пам'яті на кожному сервері.

Отримана задача є задачею стохастичного програмування з булевими змінними великої розмірності $n \times m$. Для умов усереднення λ_i і μ_i на інтервалі спостереження можна, використовувати результати теореми Куна-Таккера [36-38], усереднити стохастичний квазіградієнт вигляду (3.6) і, таким чином, звести задачу до задачі квадратичного програмування. Таким чином, задача зводиться до мінімізації квадратичної цільової функції з нелінійними обмеженнями вигляду (3.7).

Умови Куна-Таккера сформовані для спільної задачі нелінійного програмування з обмеженнями, як у вигляді рівностей, так і у вигляді нерівностей. Розглядимо ці умови для нашої задачі з обмеженнями тільки у вигляді нерівностей: мінімізувати функцію $Q(U)$ при обмеженнях вигляду (3.7).

Запишемо умови Куна-Таккера

$$\tilde{\nabla} Q(U) - \sum_i \xi_i \tilde{\nabla} g_i(U) = 0, \qquad (3.9)$$

де

$\tilde{\nabla} Q(U) = E\left[\dfrac{Q(U) - Q(U_{n-1})}{\Delta_S}\right]$ - стохастичний квазіградієнт; E – символ математичного очікування; Δ_S - величина кроку квазіградієнта між послідовними значеннями U на *(n-1)* – м і *n* – м кроках; $\xi_i \geq 0$ - множник, сенс якого визначимо нижче;

$\tilde{\nabla} g_i(U)$ - стохастичний квазіградієнт функції $g_i(U) = \mu_i - \sum_{l=1}^{k} \lambda_l P_{li}(U)$:

$$\tilde{\nabla} g_i(U) = E\,\frac{g_i(U_n) - g_i(U_{n-1})}{\Delta_S}$$

При такому виборі функції обмеження (4.7) набирають вигляду:

$$g_i(U) = \mu_i - \sum_{l=1}^{k} \lambda_l P_{li}(U) \geq 0 \qquad (3.10)$$

Правомірність такого перетворення витікає з того, що всі змінні $\lambda_i, \lambda_l, P_{li}$ - невід'ємні величини.

Умови оптимальності записуються як

$$\tilde{\nabla} Q(U) - \sum_j \xi_j g_j(U) = 0, \qquad (3.11)$$

$$g_j(U) = 0, \quad j = 1,..., J. \tag{3.12}$$

Множник ξ_j в даному випадку є невизначеним множником Лагранжа, відповідним *j-му* обмеженню. Він представляє собою значення неявної функції вартості, що відображає зміну мінімального значення цільової функції. Підбір значення ξ_j здійснюється так, щоб координата точки безумовного мінімуму задовольняла умові . $g_j(U) = 0$.

Це легко зробити, якщо, розглядаючи ξ_j як незалежну змінну, знайти безумовний мінімум функції $Q(U)$ без врахування впливу другого доданку у вираженні (3.11), а потім вибрати значення, при якому виконується рівність в цьому виразі цілком. Іншими словами, ми зводимо початкове завдання мінімізації (3.6) в завдання мінімізації більшої розмірності (3.11).

3.5. Фрагментація пакетів у віртуальних приватних мережах

Фрагментація означає ділення великого цілого на дрібніші частини. Тому, фрагментація пакетів - це дозвіл на розбиття пакету на фрагменти шлюзом, кожен з яких має вид окремого між мережного пакету [43,44,45].

Але проблема в мережах з комутацією пакетів полягає у відновленні пакету з його фрагментів. У роботі [43] розглядаються дві стратегії по відновленню початкових пакетів. Одна з них називається прозорою фрагментацією, інша - непрозора фрагментація. Суть прозорої фрагментації є відновлення пакетів на проміжних маршрутизаторах. Недоліки цієї фрагментації полягають в тому, що, кожен фрагмент повинен містити ознаку кінця пакету, або поле лічильника. Крім того, всі фрагменти, проходячи через один і той же шлюз, позбавляються можливості використання різних шляхів до остаточного призначення. Це, звичайно ж, приводить частково до втрати продуктивності.

Друга стратегія фрагментації полягає у відмові від відновлення пакету на проміжних маршрутизаторах. Коли пакет розбивається на фрагменти, він розглядається, як окремий пакет, потім даний пакет проходить через вихідний шлюз і його віднов-

лення відбувається на хості -отримувачі. Основна перевага цієї стратегії полягає в тому, що тут з'являється можливість використовувати декілька різних маршрутів для передачі фрагментів. Тому використання непрозорої фрагментації є доцільнішим.

У роботі [43] розглядувався процес фрагментації, обслуговування і об'єднання фрагментів заявки на послугу.

У системі четвертого покоління *Long Term Evolution* (*LTE*) використовується концепція якості обслуговування, що заснована на класах. Вона пропонує операторам просте, але ефективне рішення для диференціювання різних пакетних послуг. На додаток до *LTE* визначена плоска архітектура мережі на базі *IP-протоколу* як частка програми розвитку архітектури системи – *System Architecture Evolution* (*SAE*). Призначенням архітектури *LTE/SAE* є ефективна підтримка будь-якої *IP-услуги* з точки зору широкого комерційного використання. Однією із значних вимог, що пред'являються до *LTE/SAE*, є зниження витрат на експлуатацію системи. У досягненні цієї мети важлива роль відводиться саме віртуальним технічним функціям, які реалізуються в рамках проекту *SAE/EPS* (*System Architecture Evolution – Evolved Packet System*) з технологією пакетної комутації. Система *SAE/EPS* повинна підтримувати відповідні рівні якості сервісу, такі як:

1) ідентифікація класу Q_oS;

2) розстановка і фіксація пріоритетів;

3) гарантована бітова швидкість;

4) максимальна бітова швидкість;

5) відношення числа спотворених символів до спільного числа переданих символів (*Bit Error Ratio – BER*).

У зв'язку з новизною задачі впровадження *VTF* виникають значні труднощі в отриманні порівняльних оцінок ефективності їх використання, оскільки неясно, по яких критеріях можна порівнювати традиційні послуги мережі мобільного зв'язку з новими послугами *VTF*. Більш того, в процесі майбутнього впровадження *VTF*, очевидно, можуть змінюватися самі набори послуг, що надаються. Тому бажано отримати якісь асимптотичні кількісні оцінки тих показників, від яких безпосередньо за-

лежать тимчасові характеристики надання послуг і навантаження на мережу в цілому. Внаслідок невизначеності умов впровадження і функціонування систем з наборами *VTF* необхідно розробити метод аналізу вибраних оцінок в досить широкому діапазоні умов можливого вживання.

Сучасні комп'ютерні мережі є набором фрагментів з різним фізичним середовищем передачі даних, експлуатаційними і технічними характеристиками, різними топологіями [46]. По суті, вони є складними мережами з високим ступенем гетерогенності.

Завдяки комп'ютеризації мереженого обладнання, вдосконаленню засобів моніторингу, розширенню функціональності з'являється можливість наблизитися до потенційних характеристик мережі, насамперед, по пропускній спроможності і якості сервісу в цілому. Крім того, з'являється можливість управляти логічною топологією в широких межах при фіксованій фізичній топології мережі [43]. Цю задачу можна автоматизувати і вирішувати в реальному часі. Тому проблема фрагментації пакетів при передачі як по мережі в цілому, так і для окремих, слабо пов'язаних між собою сегментів є актуальною.

Шляхом фрагментації пакетів і відправки по N паралельним маршрутам можна добитися таких результатів:

1) прискорення доставки і підвищення надійності доставки (короткі пакети швидше проходять через транзитні вузли, а в бездротових мережах і мережах радіодатчиків зменшується ймовірність колізій, втрат пакетів при зайнятості буфера і так далі);

2) підвищення оперативності передачі, збереженню, цілісності інформації, зниження ймовірності перехоплення, розшифровки і модифікації інформації по перехоплених коротких фрагментах.

При цьому параметри маршрутів (насамперед, середня затримка) не повинні сильно відрізнятися один від одного, наприклад, коефіцієнт варіації затримки σ_x / m_x

має бути помітно менше одиниці: $\frac{\sigma_x}{m_x} < 0{,}1$. Інакше задача оптимізації числа фрагментів, що передаються паралельно матиме безліч локальних екстремумів, скаляризувати задачу не можливо, а глобальний екстремум може розпастися на безліч близьких по величині дрібних локальних екстремумів. Внаслідок цього достовірність, а цінність результату оптимізації буде низькою.

Одним з таких показників якості сервісу є *BER*. Чим гірше *BER*, тим більше спотворень пакетів і повторних передач. Тому завдання кількісної оцінки *BER* в процесі надання послуги *VTF* представляє не лише теоретичний, але і практичний інтерес.

Керуючись роботою [51], при організації процесу передачі розіб'ємо його на послідовність окремих етапів (фаз) по наступним причинам.

1. Деякі фази послуги можуть бути слабо пов'язаними один з одним, тому вони можуть виконуватися паралельно. Більш того, вони можуть розподілятися по обслуговуючих приладах (ОП), які знаходяться в різних сегментах однієї мережі або навіть в мережах різних операторів. При цьому скорочується середній час реалізації послуги.

2. Ймовірність безпомилкової передачі даних і успішного завершення короткої фази вища, ніж сукупності декількох фаз і, тим більше, чим послуги в цілому.

На рис. 3.5 показана умовна схема процесу розбиття пакету даних для заявки на послугу і напрями окремих фрагментів на різних ОП. Відзначимо, що потік заявок інтенсивністю λ ділиться на N потоків з середніми інтенсивностями λ/N, тому задача обслуговування спрощується. Тут формально не ставляться умови, щоб кожен фрагмент пакету містив цілком окрему фазу послуги (або ціле число фаз), хоча такий спосіб фрагментації представляється найбільш логічним. При цьому число фаз послуги в різних фрагментах пакету не обов'язково має бути однаковим.

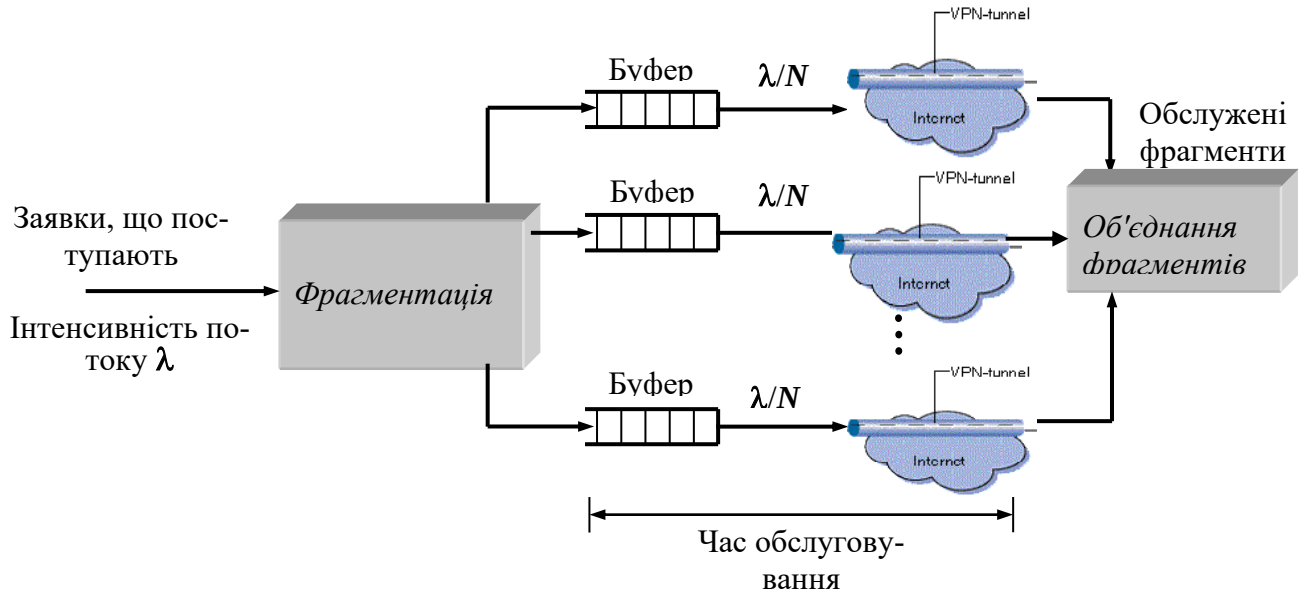

Рис.3.5. Процеси фрагментації, обслуговування і об'єднання фрагментів пакету

Припустимо, що пакет складається з елементарних (неподільних, атомарних) фрагментів з загальним числом N. Безумовна ймовірність виконання n фрагментів:

$$p_n(\alpha) = p(\alpha_n)\, p(\alpha_1, \alpha_2, \ldots, \alpha_{n-1} | \alpha_n), \qquad (3.13)$$

де $p(\alpha_n)$ – апріорна ймовірність виконання n-го фрагмента;

$p(\alpha_1, \alpha_2, \ldots, \alpha_{n-1} | \alpha_n)$ – умовна ймовірність виконання n-го фрагмента при умові успішно виконаній прийому попередніх $(n-1)$ фрагментів.

Конкретизуємо вирази для безумовної ймовірності для фрагментів від першого до N-го.

I етап: $p_1(\alpha) = p(\alpha_1)$;

II етап: $p_2(\alpha) = p(\alpha_2)\, p(\alpha_1 | \alpha_2) = p(\alpha_2)\, p(\alpha_1)$;

III етап: $p_3(\alpha) = p(\alpha_3)\, p(\alpha_1, \alpha_2 | \alpha_3) = p(\alpha_3)\, p(\alpha_2)\, p(\alpha_1)$;

Без втрати спільності можна допустити, що:

$$p(\alpha_1) = p(\alpha_2) = \ldots = p(\alpha_k) = \ldots = p(\alpha_N).$$

Тоді ймовірність, що накопичується $p_s(\alpha)$ при виконанні прийому є показова функція числа атомарних етапів:

$$p_s(\alpha, n) = \left[p(\alpha) \right]^n, \qquad n = \overline{1, N}. \qquad (3.14)$$

При розбитті пакету на короткі фрагменти, що складаються з малого числа *n* атомарних фрагментів, очевидно, ймовірність успішного виконання послуги підвищується.

У свою чергу, для реалізації *J* –фазної передачі необхідно подавати на ОП пакет даних довжиною *K* символів. При цьому виникають проблеми спотворення символів в пакеті і на підставі цього виникає необхідність повторних передач.

Якщо p_k - ймовірність спотворення *k* -го символу в пакеті, то максимальна ймовірність повторної передачі визначається ймовірністю спотворення хоч би одного з *K* символів в пакеті:

$$p_{DL} = 1 - (1 - p_k)^K . \tag{3.15}$$

Припустимо, що середнє число символів в кожному з фрагментів однаково і рівно $L =]K/J[$, де $]x[$ - оператор округлення x до найближчого цілого числа. Розіб'ємо весь пакет довжиною *K* символів на *M* коротких пакетів, в кожному з яких міститься $]J/M[$ атомарних фрагментів і, відповідно, $]K/M[=]LJ/M[$ символів (без врахування службової інформації - заголовка і кінцевика пакету).

Тоді ймовірність спотворення хоча би одного символу і повторної передачі короткого пакету:

$$p_{DN} = 1 - (1 - p_k)^{]K/N[} < p_{DL} . \tag{3.16}$$

Відповідно, ймовірність спотворення *m* пакетів із загального числа *M* пакетів дорівнює $p_{Dm} = (p_{DM})^m$, а ймовірність спотворення всього інформаційного посилання, що складається з *M* коротких пакетів:

$$p_{DN\Sigma} = (p_{DM})^M = \left[1 - (1 - p_k)^{]K/M[}\right]^M \tag{3.17}$$

Очевидно, при збільшенні числа *M* (теоретично - до величини *L*) ймовірність (3.5) прагне до величини $p_{DN\Sigma} = \left[1 - (1 - p_1)\right]^L$.

Теоретично пакет довжиною *L* символів призначеної для користувача інформації можна розбити на *L* пакетів. У кожному пакеті довжиною *K* символів $K = K_{сл} + K_{кор.} + K_0$ буде $K_{сл}$ символів службової інформації (наприклад, у комірці

ATM 5 байт), один символ $K_{кор.}=1=K_1$ призначений для користувача інформації і K_0 порожніх символів (які не використані):

$$K_0= K - K_{сл} –1.$$

Звичайно, ясно, що крайні випадки максимальної довжини пакету $K_{max}=L$ і мінімальної довжини $K_{min}= K_{сл}+K_1+K_0$ неприйнятні по приватним критеріям оптимальності. Якщо вважати, що реальна ймовірність втрати пакету (і повторної передачі із-за втрати), починаючи з деякої тривалості K_A, не залежить від довжини пакету, то розмірність задачі векторної оптимізації зменшується на одиницю. Крім того, при цьому подальше зменшення довжини фрагмента втрачає сенс.

Таким чином, в даній роботі, на відміну від [51], пропонується точніша модель процесу фрагментації і, відповідно, підвищується точність визначення діапазону оптимальних розмірів фрагментів.

При використанні рівнянь (3.13 – 3.17) були виконані розрахунки величин переваги ймовірності успішної передачі фрагментованих пакетів при наступних початкових даних:

1) розмір початкового пакету – від 576 байт – вживане за умовчанням обмеження максимальної довжини *IP-пакетів* – до 1500 байт – широко вживаний стандарт довжини пакетів в мережах доступу на сегментах *Ethernet*;

2) початкові пакети фрагментуються на короткі пакети завдовжки від 53 байт (стандарт *ATM*) до 250 байт;

3) ймовірність спотворень хоч би одного символу в пакеті вибрана рівною 0,001. Це взагалі м'яка вимога. Наприклад, в каналах зв'язку без додаткового захисту вона складає, як правило, 10^{-4}. 10^{-6}, а в оптоволоконних лініях – до 10^{-9} [48].

Приведені результати розрахунків ймовірності повторних передач внаслідок спотворення хоч би одного символу в початковому пакеті завдовжки 576 байт і у фрагментованих пакетах (рис. 3.6, 3.8, 3.10) і перевагу у ймовірності спотворення при фрагментації (рис. 3.7, 3.9, 3.11). Таким чином, p_{DL} - ймовірність спотворення не фрагментованого пакету; p_{DN} - ймовірність спотворення фрагментованого паке-

ту; $p_{DN\Sigma}$ - ймовірність спотворення декількох фрагментованих пакетів. Відзначимо, що при фрагментації на більш дрібні пакети перевага зростає.

1. Фрагментація на пакети по 53 байти.

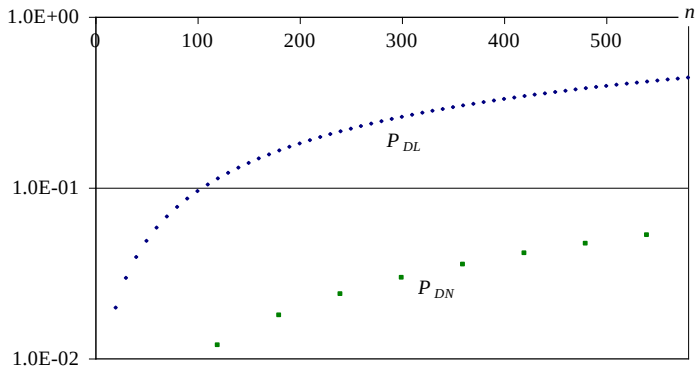

Рис. 3.6. Залежність ймовірності спотворення пакетів від їх довжини n

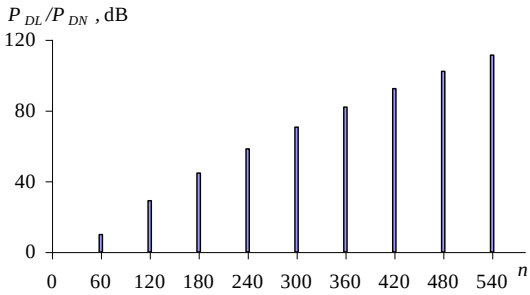

Рис. 3.7. Показник ймовірності спотворення при фрагментації.

2. Фрагментація на пакети по 110 байт.

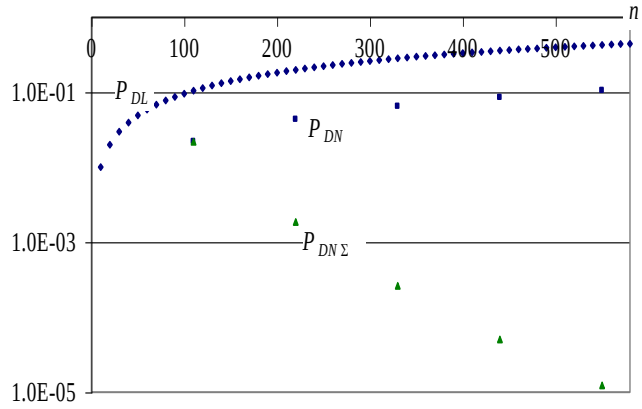

Рис. 3.8. Залежність ймовірності спотворення пакетів від їх довжини n

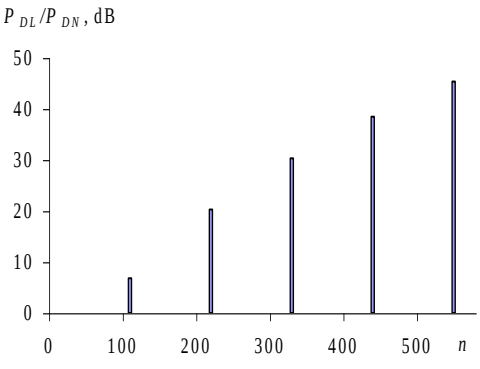

Рис. 3.9. Показник ймовірності спотворення при фрагментації.

3. Фрагментація на пакети по 270 байт.

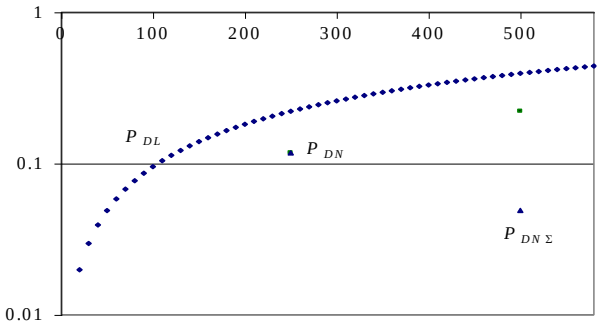

Рис. 3.10. Залежність ймовірності спотворення пакетів від їх довжини n

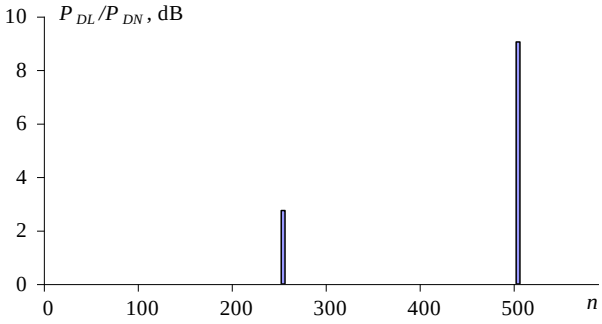

Рис. 3.11. Показник ймовірності спотворення при фрагментації.

На рис. 3.12 приведений графіки залежності ймовірності спотворення символів в пакетах залежно від коефіцієнта фрагментації $k_{fr} = \rceil K/M \lceil$ при різній апріорних ймовірностях спотворень окремого символу.

При виконанні розрахунків по методиці, прийнятій в [47], не враховувалися такі чинники, як затримка обробки в ОП, витрати на фрагментацію і плата за використання декількох ОП (можливо, що належать різним операторам). Крім того, була вибрана недостатньо реалістична модель (довжина фрагмента прагне до нуля, що неможливе в принципі). Відсутній облік втрат часу $t_{очік.}$ на очікування фрагментів і $t_{об}$ – об'єднання фрагментів в пристрої дефрагментації.

Для уточнення моделі приймемо максимальне значення

$T_{очік.} = t_{очік.\ ср} + 3\sigma_{дост}$, де $\sigma_{дост}$ – середньоквадратичне відхилення (СКВ) часу доставки.

На рис. 3.13 зображена типова залежність $\sigma_{дост}$ від довжини фрагмента $l_{фр}$.

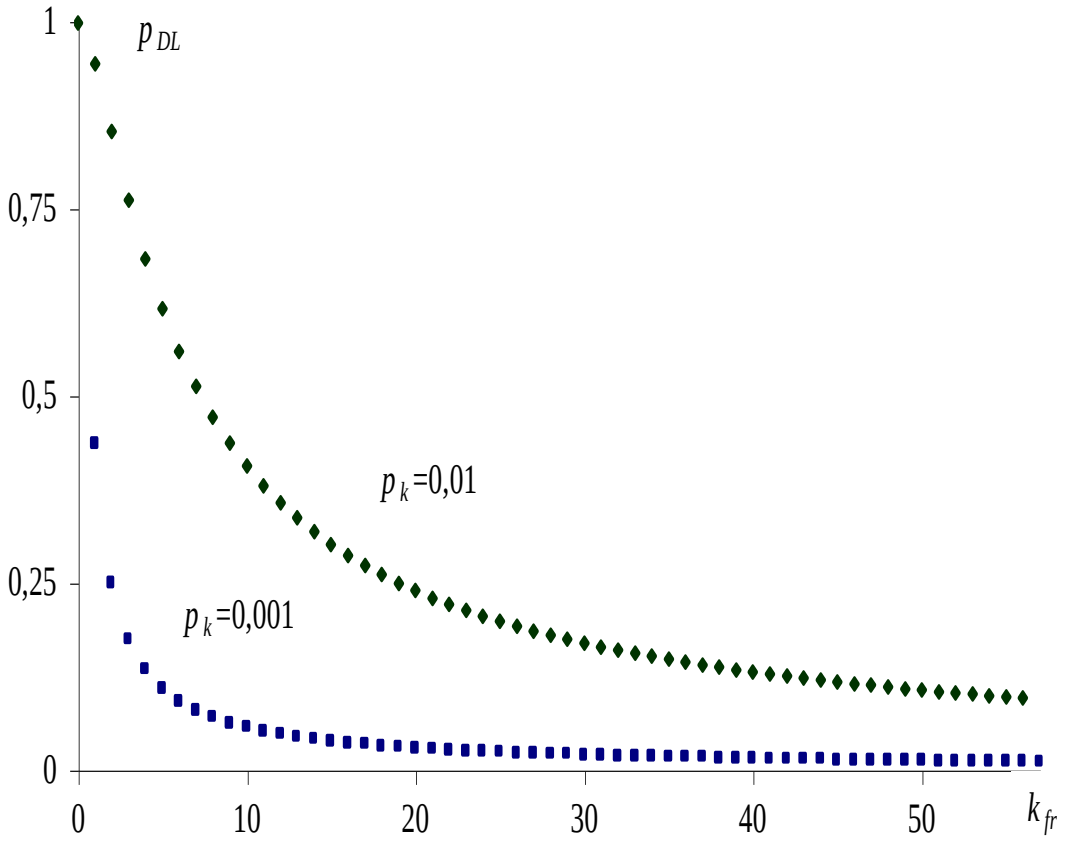

Рис. 3.12. Залежність ймовірності спотворення пакету від коефіцієнта фрагментації

На першій ділянці (короткі фрагменти) розкид обумовлений різною політикою обробки пакетів різної довжини в транзитних вузлах. Для фрагментів середньої довжини (друга ділянка) розкид обумовлений в основному параметрами вузлів мережі комутації і маршрутизації. Зменшення розкиду на третій ділянці цілком логічно обумовлене зменшення числа фрагментів до передачі без фрагментації (падіння до нуля).

Затримка обробки в ОП складається із затримки комутації, яка може складати від доль до тисяч мілісекунд, часу буферизації і очікування пакету в черзі і часі переміщення пакету у вихідний порт [48]. Основний внесок в затримку обробки вносить час буферизації. При зменшенні довжини пакету затримка буферизації убуває, і величина сумарної затримки асимптотично наближається до величини часу переміщення пакету.

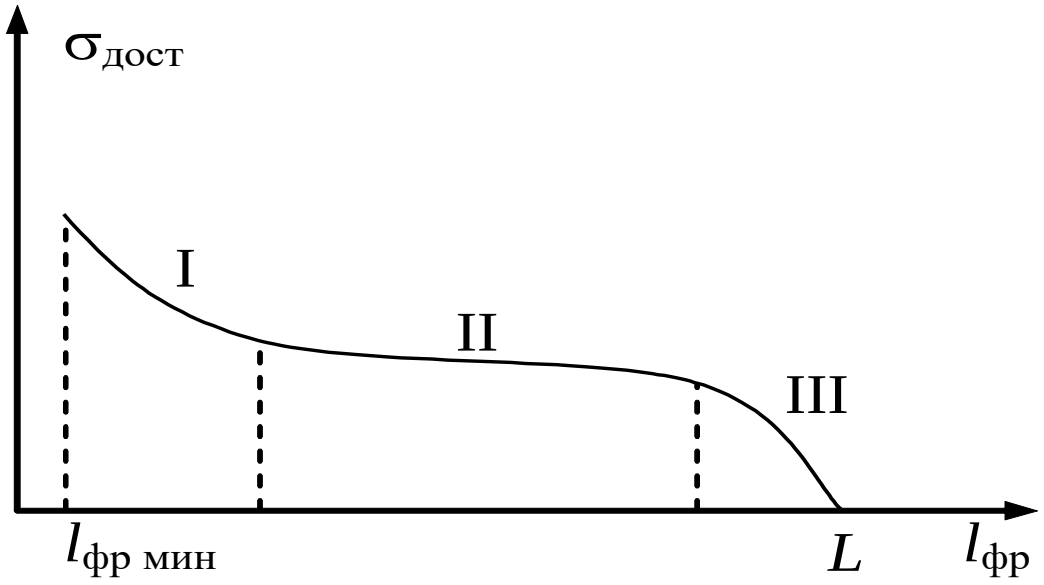

Рис. 3.13. Розкид часу доставки фрагментів різної довжини.

Для опису залежності затримки від довжини пакету можна взяти раціональну функцію виду $\tau_d = \frac{a}{b +]K/M[}$ або експоненту $\tau_d = \exp\left(-c\right]K/M[\right) + d$, де постійні a,b,c,d вибираються з урахуванням технічних і експлуатаційних характеристик обладнання [49].

Витрати на фрагментацію виникають через збільшення загальної тривалості фрагментованих пакетів, оскільки до кожного такого пакету необхідно приєднати заголовок і кінцевик. До них, як раніше відмічалося, додаються витрати на використання обладнання інших операторів.

Для конкретизації функції вартості фрагментації використовуємо загальні підходи системотехніки [50, 51]: витрати пропорційні квадрату збільшення ресурсу – потужності механізму, машини, генератора, витрати пального, числа вживаних приладів, пристроїв, машин тощо. Тому, як функцію вартості візьмемо квадратичну функцію вигляду $C_\Sigma\left(\right]K/M[\right) = c_0\left(\right]K/M[\right)^2 + C_p$, де c_0 – константа, вибирана, з урахуванням вартісних показників обладнання, C_p – умовно-постійні початкові витрати.

З урахуванням приведених міркувань результуючий критерій ефективності фрагментації можна представити у вигляді лінійної згортки приватних показників Q_i:

$$k_{eff} = \sum \beta_i Q_i , \qquad (3.18)$$

де β_i – вагові коефіцієнти, вибирані дослідним шляхом.

Для розрахунку були вибрані досліджений раніше показник – ймовірність спотворень і повторних передач, а також функції затримки і вартості. На рис. 3.14 представлені графіки приватних показників і результуюча функція ефективності фрагментації (для наочності вибрана функція, зворотна коефіцієнту ефективності). Як бачимо, мінімум досягається при коефіцієнтах фрагментації від 10 до 15, що відповідає діапазону розбиття початкового пакету довжиною 576 байт на короткі пакети завдовжки від 40 до 60 байт.

Таким чином, при розбитті пакету даних на окремі фрагменти, і розподілі цих фрагментів по різних обслуговуючих приладах (маршрутам), досягається суттєвий виграш в ефективності обслуговування – від 10 до 100 дБ залежно від величини коефіцієнта фрагментації.

Крім того, пом'якшуються вимоги до якості ліній передачі даних – навіть при достатньо високій ймовірності спотворень окремих символів в пакеті результуюча ймовірність спотворень і повторних передач залишається в допустимих межах.

З урахуванням витрат на розподілене обслуговування – фрагментацію і збір пакетів – визначений діапазон ефективної фрагментації – розбиття пакету на 10 - 12 коротких фрагментів. При цьому виграш в ефективності обслуговування досягатиме 35 - 40дБ.

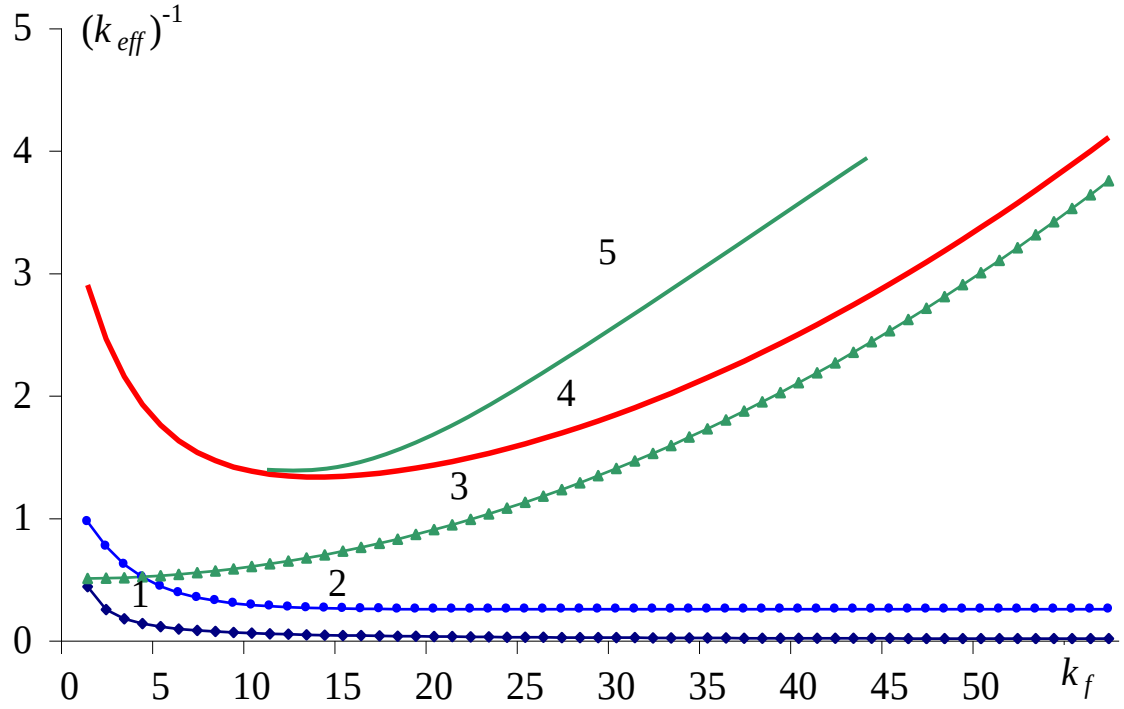

Рис. 3.14. Залежність параметра сумарної ефективності $\left(k_{eff}\right)^{-1}$ від коефіцієнта фрагментації

1 – ймовірність спотворень символів;

2 – затримка;

3 – вартість;

4 – сума показників без врахування розкиду затримки;

5 – сума показників по уточненій методиці.

Дослідження проблеми розподіленої передачі доцільно продовжити у напрямі обліку порівняльної важливості вибраних приватних показників ефективності й імовірнісних характеристик збереження цілісності інформації в процесі передачі фрагментованих даних.

ВИСНОВОК ДО РОЗДІЛУ 3

Задача оптимального розподілу запитів при вирішенні задач БП зведена до задачі квадратичного програмування з обмеженнями типу нерівностей.

Для визначення умов необхідності і достатності рішення модифіковані умови Куна-Таккера з урахуванням дискретності і випадкового характеру квазіградієнта.

Були розраховані кількісні характеристики виграшу для широкого діапазону умов застосування методів передачі з фрагментацією пакетів даних.

Мінімум затримки досягається при коефіцієнтах фрагментації від 10 до 15, що відповідає діапазону розбиття початкового пакету довжиною 576 байт на короткі пакети завдовжки від 40 до 60 байт.

Таким чином, при розбитті пакету даних на окремі фрагменти, і розподілі цих фрагментів по різних обслуговуючих приладах (маршрутам), досягається суттєвий виграш в ефективності обслуговування – від 10 до 100 дБ залежно від величини коефіцієнта фрагментації.

З урахуванням витрат на розподілене обслуговування – фрагментацію і збір пакетів – визначений діапазон ефективної фрагментації – розбиття пакету на 10 - 12 коротких фрагментів. При цьому виграш в ефективності обслуговування досягатиме 35 - 40дБ.

ВИСНОВКИ

У дипломній роботі була розв’язана проблематика забезпечення швидкого надійного обміну конфіденційною інформацією між ЄЦОАПІ та відповідними організаціями, такими, як аеропорти чи авіакомпанії.

Необхідним пунктом є модернізація існуючої база даних, використовуваної тільки для накопичення статистики, ще й як джерело інформації для запобігання небажаним подіям які мали місце раніше.

Додатковою вимогою щодо подальшої модернізації вже існуючої БД є модернізація чи введення в експлуатацію нового автоматизованого робочого місця для обробки інформації, що знімається з параметричних та мовних реєстраторів.

Для забезпечення максимального ефективного та надійного обміну авіаданими необхідно використовувати практично вже готову до застосування сукупність заходів для захисту передаваних по публічній мережі даних, технологію VPN.

Для виведення на новий рівень показників QoS передачі даних рекомендується застосовувати в новостворюваній системі моніторингу ПІ фрагментацію та дефрагментацію пакетів даних, що цією мережею передаються. В результаті досліджень, що були проведені в третьому розділі даної кваліфікаційної роботи, можна сказати, що найбільший виграш ми отримаємо при передачі по мережі фрагментів пакетів, розмір яких становитиме від 40 до 60 байт (а в нашому випадку 53 байти, що дорівнює розміру ATM-комірки разом з її заголовком), а це в свою чергу досягається поділом вихідного пакету з даними на 10…12 фрагментів. Відповідно до цього, час доставки фрагментів пакетів значно зменшиться, коефіцієнт сумарної ефективності по уточненій методиці буде найвищим.

Щодо реалізації VPN, то можливою є рекомендація використовувати VPN на базі конфігурування маршрутизаторів. Така рекомендація не є обов’язковою, але при такому способі реалізація налаштування чи модернізація вже існуючою віртуальної приватної мережі є дуже простою та зручною.

На основі аналізу інформаційних об’єктів, які складають АС, розроблено методика реалізації моделі віртуальної мережі системи моніторингу. Результатом ана-

лізу є формальна модель віртуальної мережі системи моніторингу польотної інформації на основі VPN, яка може дозволити шляхом її впровадження в новостворену систему моніторингу польотної інформації, стати фундаментом для фізичної та програмної реалізації останньої. Отримана модель надає можливість опису всіх основних елементів та параметрів дослідження обслуговування потоків даних в мережах з гетероденною структурою системи контролю безпеки польотів, наприклад такого, як вибір оптимального показника фрагментації пакетів у мережі.

У даній дипломній роботі отримано наступний новий науковий результат: розроблено метод вибору оптимального числа фрагментів пакету при розподіленій передачі, при якій не тільки підвищується швидкість передачі, а й безпека обміну даними, їх цілісність та конфіденційність.

Практичне значення отриманих результатів дипломної роботи визначається тим, що теоретичні результати та висновки доведені до конкретних алгоритмів, структурних та функціональних схем, та полягає в наступному:

1. Розроблені методи та алгоритми зведені до конкретних структур, які можуть бути реалізовані при встановленні та модифікації мережного обладнання.

2. Розроблені методи фрагментації пакетів для підвищення надійності передачі даних придатні до застосування у широкому колі мереж загального та спеціального призначення при відповідних модернізаціях та масштабуваннях розподілених баз даних.

3. Обґрунтовано можливості реалізації методів захисту інформації апаратними чи програмними засобами при організації багаторубіжної системи захисту.

Розроблена формальна модель дозволяє спроектувати та створити комп’ютеризовану системи моніторингу польотної інформації на основі VPN. За бажанням, модель може бути модернізована чи видозмінена по аналогії до проекту в залежності від умов конкретного технічного завдання.

При роботі в реальному режимі часу для усунення нештатних ситуацій (особливо конфліктів ПС) удосконалено інформаційно-обчислювальна мережа АС ЄЦО-

АПІ, яка дозволяє швидко адаптуватися і перерозподіляти обчислювальні і мережні ресурси.

Для забезпечення передачі даних з необхідною якістю і достовірністю, а також захисту від несанкціонованого доступу, запропонована модифікована модель рубежів захисту на основі вкладених екранів.

На підставі того, що при побудові обчислювальних мереж основною метою при їх створенні і реалізації є обробка і передача різнорідного трафіку, для підвищення ефективності роботи ІВС була проаналізована залежність статистичних характеристик трафіку від різних параметрів мережі.

Досліджені залежність необхідного об'єму буферної пам'яті за умови передачі самоподобного трафіку, а також процес формування сумарних потоків в парціальних каналах спільної мережі передачі даних.

Для функціонування ІВС в умовах критичного застосування для покращення якості і надійності роботи мережі проведені розрахунки коефіцієнта використання мережі, а також розрахунки зміни залежності пропускної спроможності від навантаження мережі.

У даній роботі вирішені наступні науково-технічні завдання:

1) розроблений алгоритм реалізації запитів в розподіленій БД БП з логічною оптимізацією, вибором і оптимізацією плану запиту;

2) вибрана і обґрунтована концептуальна структура розподіленої БД БП, в основі якої лежить схема ієрархічної зірки;

3) розраховані кількісні характеристики виграшу для широкого діапазону умов застосування методів передачі з фрагментацією пакетів даних;

Новим в процесі виконання завдання та проведенні обчислень, що виконувались по методиці відмінній від нашої, стало не взятия за увагу таких чинників, як:

1) затримка обробки в ОП;

2) витрати на фрагментацію;

3) плата за використання декількох ОП (можливо, що належать різним операторам).

Це значною мірою призвело би до змарнування високої точності обчислень, що була бажаною.

Додатковими перевагами стало прийняття не рівним нулю довжину фрагмента передаваних даних (таке є неможливим в принципі). Був відсутній облік втрат часу $t_{очік.}$ на очікування фрагментів і $t_{об}$ – об'єднання фрагментів в пристрої де фрагментації, що призводило до зменшення точності обчислення показників ефективності роботи мережі системи моніторингу ПІ на основі VPN. Тому для створення більш точної моделі приймемо максимальне значення $T_{очік.} = t_{очік.\ ср} + 3\sigma_{дост}$, де $\sigma_{дост}$ – у теорії ймовірності і статистиці найпоширеніший показник розсіювання значень випадкової величини відносно її математичного сподівання, а в нашому випадку - показник середньоквадратичного відхилення часу доставки фрагмента пакету до місця його призначення.

Роботу в даному науковому напрямі доцільно продовжити, при цьому необхідно вирішити наступні завдання:

1) аналіз принципів практичної побудови державної мережі БП із застосуванням модульної архітектури;

2) прогноз розвитку мережі, оцінка інтервалів між етапами модернізації, забезпечення умов розширюваності і масштабованості мережі;

3) розробка принципів об'єднання мережі ЄЦОАПІ з мережами інших держав – членів МАК, ІКАО, в тому числі забезпечення глобальної безпеки польотів, підвищення точності прогнозу і локалізації позаштатних ситуацій в повітрі, на аеродромах і так далі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Computer security institute. CSI Computer Crime and Security Survey 2010/2011[Електронний ресурс]. – Режим доступу: http://gocsi.com/survey.
2. Несанкціонований доступ. [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/Несанкціонований_доступ.
3. Необхідність удосконалення системи охорони інформаційних технологій. Нові технології № 1 (31) – 2011. Науковий вісник КУЕІТУ.
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». [Електронний ресурс]. Режим доступу: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.
5. Матеріали статті «Мир ПК», № 09, 2008 [Електронний ресурс]. – Режим доступу: http://www.osp.ru/pcworld/2008/09/5650787/.
6. Видання ІКАО «Состояние безопасности полетов в мире», 2013.
7. Руководство по управлению безопасностью полетов (РУБП) / (Doc 9859-AN/460). – [1-е изд.]. – ИКАО, 2006. – 379 с.
8. Повітряний кодекс України: за станом на 4 квітня 1993 р. (зі змінами у відповідності з Законом № 590/97-ВР від 21.10.97 р.) / Верховна Рада України. – Офіц. Вид. – К.: Парлам. Вид-во, 1997. – 275 с. – (Бібліотека офіційних видань).
9. Положення про систему управління безпекою польотів на авіаційному транспорті: затверджене наказом Державіаслужби від 25.11.05 р., №895 та зареєстроване в Міністерстві юстиції України 14.12.05 р., №1505/11783. – 80 с.
10. Яцков Н.А. Основы построения автоматизированных систем контроля полетов воздушных судов / Яцков Н.А. – К.: КИИГА, 1989. – 343 с.
11. Правила інформаційного забезпечення системи управління безпекою польотів повітряних суден цивільної авіації України: за станом на 19 березня 2009 р., Наказ № 295 / Державна Авіаційна Адміністрація. – Київ, 2009. – 160 с. – (Нормативне видання).
12. Приложение 13 к Конвенции о международной гражданской авиации. Расследование авиационных происшествий. – ИКАО, 2001. – 76 с.

13. Global Aviation Safety Roadmap. – ICAO, 2006. – 23 p.

14. Глобальная эксплуатационная концепция ОрВД / Doc 9854-AN/458. –[1-е изд.]. – ИКАО, 2005. – 100 с.

15. Руководство по координации между органами обслуживания воздушного движения, службами аэронавигационной информации и авиационными метереологическими службами / Doc 9377AN/915. – [3-е изд.]. – Международная организация гражданской авиации, 2007. – 154 с.

16. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф., Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. - 2-е изд., перераб. и доп. — М.: Радио и связь, 2001. - 376 с.

17. Оглтри Т. Firewalls. Практическое применение межсетевых экранов. Пер. с англ. — М.: ДМК Пресс, 2001. - 400 с.

18. Паук С.М. Сети авиационной электросвязи.-М.,:Транспорт,1986-272с.

19. Андрусяк А.І., Дем'янчук В.С., Юр'єв Ю.Н. Мережа авіаційного електрозв'язку. — К.: НАУ, 2001. - 448 с. 5

20. VPN. [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/VPN.

21. Хамидуллин Р.Р., Бригаднов И.А., Морозов А.В. Методы и средс-тва защиты компьютерной информации: Учеб. Пособие. – СПб.: СЗТУ, 2005. – 175 с.

22. Таненбаум Э. – Компьютерные сети. 5-е изд.- СПб.: Питер, 2012. – 992 с.

23. Reinhand Menzel. ICAO safety database strengthened by introduction of new software / Reinhand Menzel // ICAO Journal. – 2003. – №3. –Vol.59.

24. Ноздрин В.И. Некоторые проблемы гражданской авиации / В.И. Ноздрин // Проблемы безопасности полетов. – М.: ВИНИТИ, 2005. – Вып.№1. – С. 8-24.

25. Руководство по предотвращению авиационных происшествий / Doc 9422-AN/923. – [1-е изд.]. – ИКАО, 1984. – 150 с.

26. Руководство по представлению данных об авиационных происшествиях / инцидентах (ADREP) / Doc 9156. – [2-е изд.]. – ИКАО, 1987. – 94 с.

27. Глобальный план обеспечения безопасности полетов. – ИКАО, 2007. – 25 с.

28. Организация данных в системах обработки данных. Термины и определения: ГОСТ 20886-85. – [Действительный от 01.07.1986г.]. – Киев, 2005. – 8 с.

29. Джеффри Д. Ульман. Основы реляционных баз данных / Джеффри Д. Ульман, Дженнифер Уидон. – М.: Издательство «Лори», 2006. – 374 с.

30. Ребекка М. Райордан. Основы реляционных баз данных / Ребекка М. Райордан. – М.: Издатель: Русская редакция, 2001. – 384 с.

31. К. Дж. Дейт. Введение в системы баз данных / К. Дж. Дейт. – [8-е изд.]. – М.: Издательский дом «Вильямс», 2005. – 1315 с.

32. Казаков И.Е. Статистическая динамика систем с переменной структурой / Казаков И.Е. – М.: «Наука», 1977. – 416 с.

33. Дружинин В.В. Введение в теорию конфликта / Дружинин В.В., Конторов Д.С., Конторов М.Д. – М.: Радио и связь, 1989. – 288 с.

34. Гнеденко Б.В., Коваленко И.Н. Введение в теорию массового обслуживания / Б.В. Гнеденко, И.Н. Коваленко. – [2-е изд.]. – М.: Наука, 1987. – 336 с.

35. Вентцель Е.С. Исследование операций. Задачи, принципы, методология: [учеб. пособие для вузов] / Е.С. Вентцель. – [3-е изд., стереотип]. – М.: Дрофа, 2004. – 208 с.

36. Сигорский В.П. Математический аппарат инженера / Сигорский В.П. – К.: Издательство «Техніка», 1975. – 768 с.

37. Кузнецов С. Методы оптимизации выполнения запросов в реляционных СУБД / С. Кузнецов // Центр Информационных Технологий: http://www.citforum.ru/database/articles/art_26.shtml.

38. Коровкин С.Д. Решение проблемы комплексного оперативного анализа информации хранилищ данных / [Коровкин С.Д., Левенец И.А., Ратманова И.Д. и др.] // Центр Информационных Технологий: http://www.citforum.ru/database/articles/art_11.shtml.

39. Таненбаум Э. Компьютерные сети / Э. Таненбаум. – [4-е изд.]. – СПб.: Питер, 2010. – 992 с.

40. Аоки М. введение в методы оптимизации. –М.: Наука, 1977. – 344с.

41. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х книгах. - М.: Энергоатомиздат, 1997.

42. Петраков А. В., Лагутин В. С. Защита абонентского телетрафика. — М.: Радио и связь, 2002. - 504 с.

43. Реклейник Г., Рейвинзрок А., Рэгсдел К. Оптимизация в технике: В 2-х кн., Кн.2 пер. с англ. – М.: Мир, 1986. – 320с.

44. Столингс В. Современные компьютерные сети / Столингс В. – [2-е изд.]. – СПб.: Питер, 2003. – 783 с.

45. Вишневский В.М. Основы передачи информации в вычислительных системах связи: [учебное пособие] / В.М. Вишневский, В.П. Дмитриев, В.С. Жданов. – М.: МГИЭМ, 1998. – 162 с.

46. Громаков Ю.А. Концепции развития мобильной и беспроводной связи общего пользования / Ю.А. Громаков // Электросвязь. – 2008. – № 12. – С. 51-57.

47. Yew A. Quality of Service Management for the Virtual Home Environment / A. Yew, C. Bohoris, A. Liotta, G. Pavlou // Centre for Communication Systems Research, School of Electronics, Computing & Mathematics University of Surrey, UK, 2001.

48. Бестугин, А.Р. Контроль и диагностирование телекоммуникационных сетей / А.Р. Бестугин, А.Ф. Богданова, Г.В. Стогов. – СПБ. : Политехника, 2003. – 174 с.

49. Дружинин В.В. Конфликтная радиолокация / В.В. Дружинин, Д.С. Конторов. – М.: Радио и связь, 1982. – 124 с.

50. Моисеев Н.Н. Математические задачи системного анализа / Моисеев Н.Н. – М.: Наука, 1981. – 488 с.

51. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов] / В.Г. Олифер, Н.А. Олифер. – [4-е изд.]. – СПб.: Питер, 2010. – 944 с.

52. Albert Voronin, Maksym Kuklinskyi, Tetyana Holyavkina, Iryna Gyza, Liudmila Kharlai / Multi-Criteria Synthesis of the Software-Defined Network Structure // CEUR Workshop Proceedings (Computer Science-Information Systems-Information Technology), Volume 2588, 2 April 2020, ISSN 1613-0073. P. 404-417.