МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет радіоелектроніки

Центр післядипломної освіти
Кафедра Програмної інженерії

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Дослідження алгоритмів підвищення надійності та оптимізації трафіку відео конференц зв'язку

Виконав:
студент 2 курсу групи ІПЗздм-21-2
Шрамко В.С.
(прізвище, ініціали)

Спеціальність	121 – Інженерія програмного забезпечення
Тип програми	Освітньо-наукова
Керівник	проф. Шубін І. Ю.

(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ З.В. Дудар

2023 р.

Харківський національний університет радіоелектроніки

Центр післядипломної освіти

Кафедра програмної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 121– Інженерія програмного забезпечення
(код і повна назва)

Освітньо-наукова програма Інженерія програмного забезпечення
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____20____р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові Шрамку Віталію Сергійовичу
(прізвище, ім'я, по-батькові)

1. Тема роботи Дослідження алгоритмів підвищення надійності та оптимізації трафіку відео конференц зв'язку

затверджена наказом по університету від «03» квітня 2023 р. № 83 Стз

2. Термін подання студентом роботи до екзаменаційної комісії «12» травня 2023 р.

3. Вихідні дані до роботи *електронні ресурси за обраною тематикою, алгоритми прогнозування кривих ціноутворення цифрових активі, принципи розробки програмного забезпечення*

4. Перелік питань, що потрібно опрацювати в роботі *реферат, вступ, аналіз предметної галузі, дослідження існуючих алгоритмів прогнозування, підготовка даних та встановлення метрик, проведення експериментального дослідження, проєктування архітектури ансамблю моделей, тренування моделей, розробка програмної системи, висновки, перелік джерел посилань.*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1.	Аналіз предметної галузі	03 квітня 2023 р.	*виконано*
2.	Огляд існуючих методів	10 квітня 2023	*виконано*
3.	Розробка алгоритмів, проектування та розробка ПЗ	15 квітня 2023	*виконано*
4.	Підготовка пояснювальної записки	20 квітня 2023 р.	*виконано*
5.	Спецчастина	28 квітня 2023 р.	*виконано*
6.	Підготовка презентації та доповіді	03 травня 2023 р.	*виконано*
7.	Попередній захист	05 травня 2023 р.	*виконано*
8.	Нормоконтроль, рецензування	07 травня 2023	*виконано*
9.	Занесення роботи в електронний архів	08 травня 2023	*виконано*
10	Допуск до захисту в зав. кафедри	11 травня 2023 р.	*виконано*

Дата видачі завдання _ «03»_ _квітня___2023 р.

Студент _____ Віталій ШРАМКО

Керівник роботи _____ Ігор ШУБІН

РЕФЕРАТ/ ABSTRACT

Пояснювальна записка до атестаційної роботи: 94 с., 43 рис., 8 табл., 6дод., 32 дж.

ВІДЕОКОНФЕРЕНЦІЇ, ГЕОМЕТРИЧНИЙ АНАЛІЗ, НАДІЙНІСТЬ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, РОЗПІЗНАВАННЯ ОБ'ЄКТІВ, СТЕГАНОГРАФІЯ.

Об'єктом дослідження є відео інформація, процес створення відео конференцій та теорія масового обслуговування

Метою роботи є дослідження алгоритмів підвищення надійності систем відео-конференц зв'язку.

Методи розробки – математичне моделювання, теорія масового обслуговування й теорія ймовірностей

У результаті роботи досліджені алгоритми та створена програмна реалізація системи гарантованої доставки відеоповідомлень.

VIDEO CONFERENCIES, STEGANOGRAPHY, GEOMETRIC ANALYSIS, OBJECTS RECOGNITION, RELIABILITY OF SOFTWARE

The subject of the study is video information, the process of creating video conferences and the theory of mass service

The purpose of the work is to study the algorithms for improving the reliabilityof video conferencing systems.

Methods of development - mathematical modeling, theory of mass service and probability theory

As a result of the work algorithms were investigated and program implementation of the system of guaranteed delivery of video messages was created.

Умови публікації пояснювальної записки

Я, _____ Шрамко Віталій Сергійович, _____
(прізвище, ім’я, по батькові)

студент групи ___ІПЗздм-21-2_ здобувач вищої освіти на другому (магістерському) рівні кафедра програмної інженерії,
(повна назва кафедри)

заявляю: моя кваліфікаційна робота на тему ___ Дослідження алгоритмів підвищення надійності та оптимізації трафіку відео конференц зв'язку___,
(назва роботи)

що буде представлена до ЕК для публічного захисту, виконана самостійно, в ній не містяться елементи плагіату і вона може бути опублікована в електронному архіві відкритого доступу ElArKhNURE. Всі запозичення з друкованих та електронних джерел мають відповідні посилання.

Я ознайомлений з діючим положенням «Про протидію академічному плагіату в ХНУРЕ», згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування дисциплінарних заходів.

ЗМІСТ

ВСТУП

Використання систем відео-конференц зв'язку дуже поширене для спільної роботи над проектами. Наприклад, в ракетно-космічній галузі вони використовуються для забезпечення зв'язку між різними майданчиками. Однак відео трафік має свої особливості, такі як велика потреба у пропускній здатності каналу, необхідність мінімізації часу доставки відеокадрів та регулярні затримки між пакетами повідомлень. У сферах, де важливі точні операції, важливо забезпечити надійність систем відео-конференц зв'язку. Під час проведення відеоконференцій інформаційні потоки транспортуються по відкритих телекомунікаційних мережах з використанням стандартних протоколів, що підкреслює актуальність досліджень проблем забезпечення інформаційної безпеки відеоконференцій. Щоб зменшити ризики порушення цілісності та доступності, необхідно застосовувати комп'ютерний метод підвищення надійності систем відео-конференц зв'язку.

Наразі однією з перспективних стратегій для забезпечення надійності систем відео-конференц зв'язку є використання технологій розподілу навантаження мережі. Це дозволяє забезпечити задані характеристики відео-конференц зв'язку за допомогою керування інформаційними потоками та оптимального розподілу мережевого навантаження. Однак, дослідження не містили імовірнісну модель доступу до інформаційних ресурсів систем відео-конференц зв'язку, що може адекватно описати інформаційні системи з гарантованою доставкою повідомлень для авторизованих користувачів. Критерій надійності систем відео-конференц зв'язку раніше не враховував ймовірність доступу до різних ресурсів систем відео-конференц зв'язку. [1].

Дослідження в області відео-конференц зв’язку проводилися в основному закордонними вченими – дослідження системи оцінки якості аудіо-відео в системі відеоконференцій, розробка та впровадження системи веб-відеоконференцій на базі Reds, відео по IP: IPTV, Інтернет-відео, H 264, P2P, Webtv і Streaming, масштабована платформа відео зв’язку на основі D-bus, обробка відео та зображення в мультимедійних системах, розробка підсистеми

MC Gateway на базі H.323 для відеоконференції.

Метод досліджень в цій роботі полягає в системному підході до розробки методу, моделей і алгоритму, які допомагають підвищити надійність відео-конференц зв’язку. Для досягнення цієї мети було використано теорію масового обслуговування та теорію ймовірностей. Також були використані методи структурного програмування, які дозволили розробити надійне програмне забезпечення, і методи доказового програмування, для систематичного аналізу правильності алгоритмів і розробки програм без помилок. У цій роботі було використано сучасну технологію об'єктно-орієнтованого програмування, яка має модульну структуру програмного засобу і дозволяє в майбутньому здійснювати його модифікацію для подальшого збільшення функціональності.

Розроблений метод підвищення надійності системи відео-конференц зв’язку для авторизованих користувачів включає оптимізацію потоків інформації та виділення привілейованого трафіку. Також були розроблені імовірнісні моделі доступу до інформаційних ресурсів системи відео-конференц зв’язку, які дозволяють оцінити рівень надійності системи та визначити ймовірність одержання доступу до інформаційних ресурсів. Для підвищення надійності відео-конференц зв’язку був розроблений алгоритм керування доступом до інформаційних ресурсів, який заснований на додаванні міток привілеїв у службове поле пакета та зміні маршруту передачі пакетів. Цей алгоритм дозволяє підвищити надійність відео-конференц зв’язку для авторизованих користувачів шляхом підвищення ймовірності одержання доступу до інформаційних ресурсів до заданого значення. Крім того, був розроблений комп'ютерний метод, який включає в себе імовірнісні моделі доступу та алгоритм керування доступом до інформаційних ресурсів системи відео-конференц зв’язку. [2].

Завдання підвищення надійності систем відео-конференц зв'язку вимагає розробки моделей та алгоритмів, що дозволяють забезпечувати якість передачі даних між вузлами системи з мінімальною відмовністю. Для досягнення цієї мети розроблено імовірнісну модель доступу верхнього рівня, яка може бути використана для створення моделей нижнього рівня. Програмний засіб для

проведення захищених відеоконференцій має бути реалізований на основі алгоритму керування навантаженням мережі, запропонованого в роботі. Цей алгоритм дозволяє розподіляти навантаження між вузлами системи та каналами зв'язку з метою забезпечення максимальної продуктивності та надійності системи. Система відео-конференц зв'язку розглядається як сукупність закінчених вузлів системи, які складаються з серверів та клієнтів, та каналів зв'язку, що з'єднують ці вузли. Сервери відповідають за керування сеансом відео-конференц зв'язку, а клієнти є джерелом даних для системи. Канали зв'язку включають в себе всі лінії зв'язку та засоби передачі даних, що приймають участь у сеансі відео-конференц зв'язку. Для успішного розроблення та впровадження програмного засобу для проведення захищених відеоконференцій, необхідно визначити основні терміни та технології відео-конференц зв'язку, що дозволить створити адекватну модель системи та розробити необхідний функціонал. З погляду теорії масового обслуговування, системи відео-конференц зв’язку являють собою багатоканальні системи масового обслуговування із чергою. Потік пакетів клієнтів є найпростішим або Пуасоновським, тому що є стаціонарним, одинарним і в ньому відсутні післядії. Через розгляд у роботі Марківських процесів використовується Марківська модель.

Об'єктом є система комп'ютерного відео-конференц зв’язку з гарантованою доставкою повідомлень, побудована на основі протоколу TCP (Transmission Control Protocol), призначена для авторизованих користувачів.

Переваги алгоритмів та результатів, що розробляються, підтверджується застосуванням методів теорії масового обслуговування й теорії імовірності й збігом теоретичних значень і результатів, отриманих у ході тестування програмного забезпечення.

Метою роботи є підвищення надійності систем відео-конференц зв’язку.

Щоб досягти цієї мети, в роботі вирішено декілька завдань. По-перше, проведено аналітичний огляд існуючих методів підвищення надійності систем відео-конференц зв'язку та моделей доступу до них. По-друге, розроблено комп'ютерний метод обробки інформації, який забезпечує авторизованим

користувачам гарантовану доставку повідомлень та підвищення надійності системи відео-конференц зв'язку. По-третє, розроблено алгоритм керування доступом до інформаційних ресурсів системи відео-конференц зв'язку, що дозволяє авторизованим користувачам підвищити надійність відео-конференц зв'язку та гарантує доставку повідомлень. Крім того, в роботі визначені основні терміни та технології відео-конференц зв'язку. Система відео-конференц зв'язку розглядається як сукупність закінчених вузлів, що складаються з серверів, клієнтів та каналів зв'язку, які забезпечують керування сеансом відео-конференц зв'язку та передачу даних.

1 АНАЛІЗ СТАНУ РОЗВ'ЯЗАННЯ ПРОБЛЕМИ ТА ОБҐРУНТУВАННЯ ЦІЛЕЙ ДОСЛІДЖЕННЯ

1.1 Аналіз проблем й досліджень в області відео-конференц зв’язку

На сьогоднішній день технологія відео-конференц зв’язку активно розвивається, це пов'язано в основному із впливом процесів глобалізації, розвитком міжнародних відносин у суспільстві й, як наслідок, з необхідністю в оперативному зв'язку по усьому світу. Використання голосового зв'язку не дозволяє одержати такий же обсяг інформації, який стає доступним з використанням відео-конференц зв’язку: дуже важливі емоції особи, міміка співрозмовника. Також сучасні технології дозволяють задіяти при спілкуванні візуальні графічні матеріали: малюнки, таблиці, схеми й діаграми [3].

Збільшення пропускної здатності каналів передачі інформації зробило відео-конференц зв’язок зручним засобом спілкування: сеанси проводяться для обміну досвідом між фахівцями, організації корпоративних нарад, також відео-конференц зв’язок широко використовується в освітніх цілях. В основному технології відео-конференц зв’язку знаходять застосування в наступних областях:

- виробничі завдання (бізнес переговори, спільні проекти);
- утвір (дистанційне навчання, конференції, майстер-класи й семінари);
- особисті потреби людей (спілкування з родичкою й друзями).

відео-конференц зв’язок (ВКЗ) – це телекомунікаційна технологія інтерактивної участі двох і більше абонентів, під час якої між ними відбувається обмін аудіо й відеоінформацією в режимі реального часу. Історія розвитку відео-конференц зв’язку починається з того моменту, коли компанія «AT&T» представила в 1964 році Videophone – першу аудіовізуальну систему електронної взаємодії, яка призначена для взаємодії двох осіб у режимі реального часу. Початок поширення ВКЗ відноситься до 80-х років – від телевізійних систем, що забезпечують інтерактивні контакти між вилученими партнерами. За наступні п'ятдесят із зайвим років, системи ВКС перетерпіли значні зміни, незмінним залишилося те, що співрозмовники бачать один одного у себе на екрані [4].

Систему відео-конференц зв’язку прийнято вважати сукупністю трьох функціональних елементів: закінчених вузлів системи – серверів і клієнтів відеоконференцій, а також каналів зв'язку, що з'єднують ці вузли. Під сервером відеоконференції розуміється комплекс програмно-технічних засобів і систем, що забезпечує керування відеоконференцією, виконання функції ідентифікації й аутентифікації клієнтів, приймання, обробки й перенаправлення даних відеоконференцій. Сервер є вузлом на стороні адміністратора відеоконференції. Клієнти також являють собою комплекс програмного й апаратного забезпеченняі є джерелом даних системи. Зв'язок клієнтів відбувається тільки через сервери за допомогою каналів зв'язку. Під каналом зв'язку прийнято розуміти всю безліч ліній зв'язку й засобів передачі даних, що приймають участь у процесі відеоконференції. Без втрати спільності міркувань, структуру каналу зв'язку за «останньою милею» можна вважати тривіальною. У цьому контексті провайдер послуг зв'язку вважається складовою частиною каналу зв'язку [5].

З поняттям «відео-конференц зв’язок» безпосередньо зв'язані поняття «трафік» і «інформація». Трафік – навантаження, створювана потоком викликів, повідомлень і сигналів, що надходять на засоби зв'язку [6]. Інформація – відомості (повідомлення, дані) незалежно від форми їх вистави. Як було сказано вище, проведення відеоконференцій стало невід'ємною частиною нашого життя, однак, з появою технології відео-конференц зв’язку виникли й певні проблеми з надійністю передачі даних. Багато відеоконференцій призначені для вузького кола осіб, що припускає необхідність організації захищеного доступу до відео даним несанкціонованого доступу, що виключає можливість неавторизованих користувачів для підтримки надійності відео-конференц зв’язку [7].

Виділяють два основні типи систем відео-конференц зв’язку з погляду топології системи: система з виділеним центром і розподілена система. Використання одного вузла як центрального елемента негативно позначається на характеристиках роботи системи у випадку проведення сеансу багатокористувацької відео-конференц зв’язку. У свою чергу, розподілені системи, що використовують у якості каналу передачі мережу Інтернет,

відрізняються низькою якістю зв'язку . За іншою класифікацією системи відео-конференц зв’язку можна розділити на програмні й апаратні. Програмні рішення суттєво обмежують число одночасних учасників сеансу відео-конференц зв’язку. Застосування спеціальних апаратних модулів значно збільшує вартість подібних систем. Варто відзначити, що як для програмних, так і для апаратних систем існує проблема стандартизації, і, як наслідок, необхідність використовувати спеціальні технології й протоколи залежно від виробника системи відео-конференц зв’язку [8].

У відповідності до рейтингу Tadviser оцінка проводилася за наступними параметрами:

- можливість масштабування;
- стійкість до відмов;
- підтримувані комунікаційні протоколи;
- сумісність із устаткуванням;
- якість відео [6].

Квадрат Gartner представлено на рисунку 1.1.

Одними з найбільш відомих програмних засобів відео-конференц зв’язку на сьогоднішній день є: Skype, Trueconfserver, Videomost, Videograce, Ciscowebex, oovoo, Apacheopenmeetings, Microsoftlyncserver, Googlehangouts, Gotomeeting.

Велика різноманітність систем комп'ютерного відео-конференц зв’язку, що представлена на ринку, дозволяє вибрати систему, що володіє необхідним функціоналом, однак рішення, що існують, не здатні повною мірою забезпечити надійність передачі інформації. У наш час на ринку систем захищеного ВКЗ в основному представлені засоби закордонного виробництва, що несе в собі певну погрозу при використанні таких систем у державних установах [7]. Усе більшою популярністю користуються різні додатки для проведення відеоконференцій через глобальні телекомунікаційні мережі, питання забезпечення надійності в таких системах виходять на перший план [9].

Рисунок 1.1 – Основні виробники систем ВКЗ [7]

Крім переваг використання технології відео-конференц зв’язку існують також проблеми й обмеження. Відеотрафік має певні особливості: вимагає значної пропускної здатності каналу, мінімізації часу доставки відеокадрів до одержувача, регулярного характеру затримок між пакетами .

Проблеми надійності систем відеоконференцій є як ніколи актуальними на сьогоднішній день, тому що мережне навчання у виді своєї доступності в будь-якій точці світу стає усе більш популярним, при цьому організаторами конференцій висуваються високі вимоги до якості надаваних послуг. При великій кількості бажаючих приєднатися до відкритої конференції й невеликої пропускної здатності каналу, найважливішим стає забезпечення доступності для всіх учасників. Для забезпечення надійності відеоконференцій існує необхідність обмежити доступ сторонніх осіб (неавторизованих користувачів), а також організувати ідентифікацію користувацьких обладнань і аутентифікацію учасників конференції (авторизацію).

Основною проблемою організації надійної системи відео-конференц зв’язку на сьогоднішній день є забезпечення мінімальної швидкості передачі даних при

максимальній швидкості обробки аудіо й відеопотоку. Для рішення цієї проблеми розроблені кодеки, що дозволяють стискати сигнал і кодувати його для каналу зв'язку, а також відновлювати й декодувати на прийомній стороні. Кодек дозволяє стиснути відеодані, зберігши задані характеристики якості, і канал, за допомогою яких ці дані можна буде передати із прийнятною швидкістю [10].

Більша частина сучасних систем відео-конференц зв’язку функціонує на основі протоколу IP (Internet Protocol), транспорт інформаційних потоків при проведенні відеоконференцій найчастіше здійснюється по відкритих телекомунікаційних мережах з використанням стандартних протоколів, тому дослідження проблем забезпечення надійності відеоконференцій здобувають особливу актуальність. Згідно із загальноприйнятою класифікацією, загрози інформаційної безпеки можна розділити на три види: загрози конфіденційності, цілісності й доступності, іноді додають загрози підтвердження авторства. Тією чи іншою мірою для відеоконференцій актуальні всі види загроз, однак, у рамках розгляду питань надійності актуальними вважаються загрози цілісності й доступності.

1.2 Аналіз алгоритмів покращення надійності систем ВКЗ

В продовж аналізу джерел наведено визначення ключових термінів, які будуть використовуватися в роботі.

Надійність (dependability) – властивість об'єкта зберігати в часі здатність виконувати необхідні функції в заданих режимах і умовах застосування, технічного обслуговування, зберігання й транспортування.

Безвідмовність (Reliability) – властивість об'єкта безупинно зберігати працездатний стан протягом деякого часу або наробітку в заданих режимах і умовах застосування.

Показник надійності (dependability measure) – кількісна характеристика одного або декількох властивостей, що становлять надійність об'єкта.

Імовірність безвідмовної роботи (Reliability function) – імовірність того, що в межах заданого наробітку відмова об'єкта не виникне [11].

Функціональна надійність визначається як можливість надання з'єднання абонентам протягом заданого інтервалу часу з моменту вступу виклику. Показником функціональної надійності є ймовірність встановлення (невстановлення) з'єднання мережі при вступі відповідного вимоги. Встановлення з'єднання зберігає її живучість [12].

На надійність системи відео-конференц зв’язку впливають організаційне, економічне, тимчасове, структурне, технологічне, експлуатаційне, соціальне, ергатичне, алгоритмічне, синтаксичне й семантичне забезпечення [28]. У роботі в основному розглядається фактор алгоритмічного забезпечення. Найпоширенішими методами розрахунку надійності є: метод Монте-Карло, метод Шику Волвертона, модель Муса, модель перехідних імовірностей і Марківска модель [12]. Через розгляд у роботі Марківських процесів надалі буде використовуватися Марківска модель. У дослідженнях інших авторів, з надійністю нерозривно зв'язаний показник живучості. Умовна функція живучості визначається через співвідношення ефективності виконання функцій поточної структури до повністю працездатної .

Надійність системи визначається надійністю її функціональних компонентів. Сучасними дослідниками у визначенні надійності інформаційної системи широко використовуються методи теорії імовірності [13]. Для оцінки надійності системи відео-конференц зв’язку використовують поняття:

- «коефіцієнт готовності» – відношення часу наробітку на відмову об'єкта зв'язку (сервера або клієнта) до суми часу наробітку на відмову об'єкта зв'язку й часу відновлення об'єкта зв'язку;
- «коефіцієнт оперативної готовності» – добуток коефіцієнта готовності й імовірності збереження працездатності каналу зв'язку при зовнішньому впливі.

Надійність обчислювальної мережі, до якої співставляються системи відео-конференц зв’язку, визначається надійністю як програмних, так і апаратних засобів, які розглядаються незалежно друг від друга. Для апаратної складової коефіцієнт оперативної готовності, визначений як добуток імовірності

безвідмовної роботи обчислювальної мережі за необхідний час для експонентного закону зміни надійності й коефіцієнт готовності обчислювальної мережі. Для програмної складової відповідно добуток імовірності безвідмовної роботи програми за необхідний час для експонентного закону зміни надійності й коефіцієнт готовності програми [6]. Одним із критеріїв оптимізації в досліджуваних джерелах визначений максимум функціональної надійності, що має дві складові:

- імовірність збереження працездатності системи при відмовах;
- імовірність виконання запиту в системі за час, що не перевищує гранично припустимого значення [11].

За результатами аналізу досліджень, визначене, що для розподілених обчислювальних систем, до яких можна віднести системи відео-конференц зв’язку, функціональна надійність і стійкість до відмов може забезпечуватися перерозподілом запитів між вузлами кластерів. Незважаючи на те, що перерозподіл вносить додаткову затримку, ступінь адаптації системи до зміни потоку запитів збільшується, що приводить до зменшення відмов.

1.3 Системи відео-конференц зв’язку з гарантованою доставкою для авторизованих користувачів

Проведений аналіз показує, що на сьогоднішній день найпоширенішими технологіями відео-конференц зв’язку є:

- системи відео-конференц зв’язку високої якості, засновані на застосуванні спеціальних протоколів;
- серверні системи, в основу принципу дії яких покладений стиск відеопотоку.

Більшість систем комп'ютерного відео-конференц зв’язку складається з наступних частин:

- програмно-апаратного забезпечення серверу;
- програмно-апаратного забезпечення клієнта;

– лінії зв'язку;

– мережного устаткування.

Відео-конференц зв’язок може бути реалізований на основі технологій ISDN (Integrated Services Digital Network), H.323, SIP (Session Initiation Protocol) [14]. ISDN – технологія із позаканальною сигналізацією. Недоліками ISDN є:

– висока вартість з'єднання за рахунок проведення окремих лінійзв'язку;

– обмежена пропускна здатність;

– низька якість зв'язку [12].

На теперешній день, для організації відео-конференц зв’язку найчастіше використовується технологія H.323 і нова технологія SIP.

Технологія H.323 забезпечує гнучкість і сумісність різних систем відео-конференц зв’язку й передбачає:

– контроль смуги пропуску;

– роботу в різнорідних мережах;

– мультиплатформенність;

– групові конференції;

– багатоадресні розсилання;

– стандарти для кодеків [15].

Технології H.323 і SIP можуть бути реалізовані на стеці протоколів TCP/IP. Відео-конференц зв’язок у свою чергу в основному організований на транспортних протоколах TCP і UDP (User Datagram Protocol) – протоколи транспортного рівня стека TCP/IP. У Таблиці 1 наведене порівняння основних характеристик протоколів TCP і UDP.

З табл. 1.1 випливає, що TCP протокол є більш надійним, чому UDP, тому що використовується механізм гарантованої доставки й орієнтований на створення з'єднання – дуплекса. У роботі розглядаються системи відео-конференц зв’язку з гарантованою доставкою, що функціонують на основі протоколу TCP.

Крім гарантованої доставки, як засобу забезпечення надійності відео-конференц зв’язку, використовується авторизація користувачів.

Авторизація – надання певній особі або групі осіб прав на виконання

певних дій, а також процес перевірки (підтвердження) даних прав при спробі виконання цих дій [16].

Таблиця 1.1 – Протоколи TCP та UDP

№	Характеристика	TCP Протокол	UDP Протокол
1	Гарантована доставка	Використовуються механізми експонентного відкоту й повторних передач сегментів по тайм-ауту	Відсутня функція гарантованої доставки, для гарантованої передачі даних використовуються протоколи верхнього рівня .
2	Швидкість передачі	Повільний протокол	Швидкий протокол
3	Взаємодія з міжмережевими екранами	Не блокується міжмережевим екраном при звичайних умовах.	Деякі міжмережеві екрани блокують.
4	З'єднання	Орієнтований на з'єднання, може використовуватися в мережах з платним контентом. Забезпечує наскрізний байтовий потік. Основа протоколу – сокети.	З'єднання не створюється. Дозволяє відправляти інкапсульовані IP-датаграми без встановлення з'єднань.
	Широкомовне розсилання	Повний дуплекс. Широке віщання й багатоадресність не підтримуються.	Використовується широкомовне розсилання –Udp. Мультикаст – передача сигналу прямо від користувача до користувача.

При збільшенні кількості користувачів навантаження зростає. Авторизація дозволяє обмежити мережне навантаження, що підвищує надійність системи відео-конференц зв’язку й дозволяє забезпечити контролювання смуги пропуску . Для кожного суб'єкта в системі визначається набір прав, які він може використовувати при звертанні до її ресурсів.

До найпоширеніших способів авторизації відносять:

– дискреційний;

– мандатний;

– рольовий;

– контроль доступу на основі контексту;

– контроль доступу на основі решіток .

Завданнями авторизації є:

– керування правами доступу;

– обмеження прав доступу;

– збір статистики.

Поняття «авторизація» тісно пов'язане з поняттями «аутентифікація» і «ідентифікація». Аутентифікація перевірка приналежності суб'єктові доступу пред'явленого ним ідентифікатора; підтвердження справжності. В процесі аутентифікації перевіряється дійсність пред'явленого користувачем ідентифікатора [17]. Аутентифікація дозволяє вірогідно переконатися в тому, що суб'єкт, що пред'явив свій ідентифікатор, насправді є саме тим суб'єктом, ідентифікатор якого він використовує. Для цього суб'єкт повинен підтвердити факт володіння деякою інформацією, яка може бути доступна тільки йому одному (пароль, ключ і т.д.).

Ідентифікація – це процедура розпізнавання суб'єкта по його ідентифікатору . У процесі реєстрації суб'єкт пред'являє свій ідентифікатор для перевірки його присутності в базі даних. Суб'єкти з відомими системі ідентифікаторами – легальні, з невідомими – нелегальні.

У роботі розглядаються системи відео-конференц зв’язку для авторизованих користувачів, авторизація виступає в ролі додаткового засобу забезпечення надійності.

1.4 Моделі доступу до інформаційних ресурсів систем відео-конференц зв’язку

Для вибору відповідного методу підвищення надійності необхідно побудувати модель доступу. Найчастіше на практиці використовуються дискреційна, мандатна й рольові моделі доступу, при неможливості чіткого

визначення параметрів системи використовуються імовірнісні моделі доступу. Система дискреційного керування доступом зручна, коли всі ресурси належать користувачам системи й розрахована на невелику кількість користувачів. Мандатна модель застосовна в організаціях із чіткою централізованою системою керування, у якій безпека даних є основним пріоритетом [18] [19]. При необхідності сполучення гнучкості конфігурування із централізованим керуванням можливе використання комбінації мандатного й дискреційного контролю над доступом. Системи з рольовим керуванням доступом доцільно використовувати в більших організаціях, зі складною ієрархією й більшою кількістю поділюваних операцій. Моделі дискреційного, мандатного й рольового керування доступом з погляду безпеки інформаційних потоків і ізольованого програмного середовища розглянуті в [20] [21].

Переважна більшість існуючих моделей доступу строго регламентовані, через що дуже громіздкі й вимагають більших вкладень. Наразі запропонований підхід до побудови рольових моделей для інформаційних систем з ієрархією сутностей, описана імітаційна модель проходження відео трафіка в каналах зв'язку на базі апарата Марківського ланцюга для системи бездротового доступу, також розроблено математичну модель мережної системи керування з передачею даних по каналу [10].

Імовірнісну модель доступу можна одержати за допомогою спеціального графоаналітичного методу з логічної моделі доступу. У якості основного параметра використовується коефіцієнт готовності, проводиться оцінка величини збитку від впливу на інформацію різних погроз, у якості критерію надійності інформаційної системи розглядається ймовірність несанкціонованого доступу. Проаналізовано представлену математичну модель керування доступом через стаціонарні ймовірності, розраховані ймовірності втрат запитів. За результатами аналізу досліджень визначене, що на сьогоднішній день відсутня імовірнісна модель доступу до систем відео-конференц зв’язку згарантованою доставкою для авторизованих користувачів [22]. Моделі доступу інших авторів в основному орієнтовані на підтримку конфіденційності, а не цілісності й доступності. Існуючі

імовірнісні моделі традиційно використовують у якості критерію надійності коефіцієнт готовності, що визначає працездатність системи, а не цілісність і доступність її ресурсів. У якості критерію надійності систем відео-конференц зв'язку раніше авторами не розглядалася ймовірність одержання доступу до ресурсів систем відео-конференц зв'язку. Існуючі імовірнісні моделі доступу звичайно не враховують характерні риси систем відео-конференц зв'язку або прив'язані до конкретних технологій, наприклад, бездротовий відео-конференц зв'язок, що звужує їхню область застосування.

Для відео-конференц зв'язку характерне використання багатоканальних систем масового обслуговування із чергою. Система відео-конференц зв'язку найчастіше являє собою систему масового обслуговування змішаного типу (багатоканальна із чергою й обмеженим часом очікування). Заявки – пакети клієнтів, канали – сервери. Стани сервера:

- сервер вільний (або сервер обробляє заявки, але ухвалює нові, що надходять ідуть на обробку);
- сервер зайнятий обслуговуванням заявок і не може більше прийняти заявки, усі нові заявки в черзі, обмеженої за часом (або несправний).

Стани серверів: S_0 – усі сервери вільні;S_1 – один сервер зайнятий, інші вільні;S_2 – два сервери зайняті, інші вільні; S_n – усі сервери зайняті, нуль заявок у черзі; S – усі сервери зайняті, одна заявка в черзі; S_{n*m} – усі сервера зайняті, m заявок у черзі.

В системах відео-конференц зв'язку потік заявок (пакетів клієнтів) є найпростішим або пуасоновським, тому що є стаціонарним, одинарним і в ньому відсутні післядії. Характеристики механізму обслуговування системи відео-конференц зв'язку: n – число серверів, μ – середнє число пакетів, що обслуговуються одним сервером в одиницю часу, дисципліна черги (обсяг черги m, порядок відбору із черги в механізм обслуговування). Для моделюваннясистем масового обслуговування слід задати наступні вихідні дані [23]:

- основні параметри;
- граф станів.

До основних параметрів звичайно відносять:

– характеристики вхідного потоку заявок (підключення клієнтів);
– характеристики механізму обслуговування (алгоритм підключення).

В якості основних показників систем масового обслуговування стосовно до систем відео-конференц зв’язку можна виділити наступне :

– відносна пропускна здатність – середня частка поступаючих пакетів, що обслуговуються серверами;
– абсолютна пропускна здатність – середнє число пакетів, що обслуговуються серверами в одиницю часу;
– імовірність відмови – імовірність того, що пакет не дійде до клієнта;
– середнє число зайнятих серверів;
– середнє число пакетів за час сеансу відео-конференц зв’язку;
– середній час перебування пакета на сервері;
– середнє число пакетів у черзі – довжина черги;
– середній час перебування пакета в черзі;
– середній час перебування пакета на сервері;
– середній час передачі пакета від одного клієнта іншому;
– ступінь завантаження каналу – імовірність, що сервер зайнятий;
– середнє число пакетів, що обслуговуються в одиницю часу;
– середнє число відхилених з'єднань;
– середній час очікування обслуговування;
– імовірність того, що число пакетів у черзі перевищить певнезначення;
– довжина черги.

Побудова графа станів:

– скласти перелік усіх можливих станів систем масового обслуговування (СМО);
– графічно представити стану СМО;
– відобразити переходи стрілками;
– призначити стрілкам ваги залежно від λ і μ.

Для системи масового обслуговування з n серверами й припустимою довжиною черги m можливі наступні стани: □ □ {*si*, *i* □ 1, *n*} – множина серверів у системі та □ □ {*c j*, *j* □ 1, *k*} – множина клієнтів у системі.

Для кожного сервера *s* □□ визначене □ – швидкість обробки заявок. Для *ii* кожного клієнта *ci* □□ вступник потік заявок розглядається як простий Пуасонівський процес інтенсивності □□.

1.5 Постановка задач дослідження

Таким чином, основною проблемою технології відео-конференц зв'язку є забезпечення мінімальної швидкості передачі даних при підтримці максимальної швидкості обробки аудіо- й відеопотоку. Для систем відео-конференц зв'язку також актуальна проблема стандартизації: виробники використовують різні технології й протоколи, що погано сумісні між собою. Незважаючи на велику різноманітність систем комп'ютерного відео-конференц зв'язку, на ринку здебільше представлені засоби іноземного виробництва, що робить актуальними дослідження в області створення надійних вітчизняних систем відео-конференц зв'язку. Показана необхідність розробки методу обробки інформації, який дозволить підвищити надійність системи відео-конференц зв'язку для авторизованих користувачів з гарантованою доставкою повідомлень. У результаті проведення аналізу досліджень визначено, що на сьогоднішній день відсутні ймовірнісні моделі доступу, які враховують характерні риси різних систем відео-конференц зв'язку. Існуючі імовірнісні моделі традиційно використовують у якості критерію надійності коефіцієнт готовності, що визначає працездатність системи, й не зачіпає питання цілісності й доступності інформаційних ресурсів. У якості критерію надійності систем відео-конференц зв'язку раніше не розглядалася ймовірність одержання доступу до інформаційних ресурсів систем ВКЗ.

В атестаційній роботі показана необхідність розробки моделі імовірнісного доступу до інформаційних ресурсів ВКЗ, що дозволяє оцінити рівень надійності системи й визначити ймовірність одержання доступу до інформаційних ресурсів.

В існуючих рішеннях практично не розглядається завдання одночасного поділу користувачів на класи з одночасним розподілом навантаження для привілейованих користувачів. Існує необхідність у розробці алгоритму керування навантаженням мережі, який буде складовою частиною методу підвищення надійності систем відео-конференц зв’язку.

Необхідно розробити новий метод підвищення надійності ВКЗ для авторизованих користувачів з гарантованою доставкою повідомлень і побудувати ймовірнісні моделі доступу до інформаційних ресурсів систем відео-конференц зв’язку, що придатні для оцінки надійності таких систем. Модель верхнього рівня дозволить описати різні системи відео-конференц зв’язку, враховуючи їхні характерні риси. На першому етапі роботи методу підвищення надійності ВКЗ визначаються вихідні параметри системи й необхідний рівень імовірності одержання доступу до інформаційних ресурсів. На другому етапі, з метою визначення фактичного значення ймовірності одержання доступу, будуються моделі доступу верхнього й нижнього рівня. На третьому етапі отримані результати аналізуються, відбувається порівняння поточного значення ймовірності одержання доступу з необхідним значенням імовірності одержання доступу. При необхідності збільшення поточного значення імовірності одержання доступу до інформаційних ресурсів відео-конференц зв’язку застосовується алгоритм керування навантаженням мережі, розроблений автором.

Імовірнісна модель доступу верхнього рівня, запропонована в роботі, заснована на поняттях: суб'єкта, об'єкта, дії. Зв’язки суб'єктів і об'єктів представлені в табличному виді. Значення ймовірності одержання доступу розраховується на основі апарата Марківських випадкових процесів з дискретними станами й безперервним часом. Отримане значення ймовірності одержання доступу рівняється з необхідним рівнем імовірності одержання доступу, при необхідності підвищення ймовірності одержання доступу за допомогою алгоритму керування навантаженням мережі.

2 ОПИС ПРОВЕДЕНИХ ТЕОРЕТИЧНИХ ДОСЛІДЖЕНЬ

2.1 Аналіз алгоритмів підвищення надійності відео-конференц зв’язку

За результатами проведення аналітичної роботи було виділено наступні способи організації захищеного доступу до систем ВКЗ:

- захист клієнтських комп'ютерів програмними й апаратними засобами;
- захист сервера програмним і апаратними засобами;
- використання мережного устаткування в захищеному виконанні;
- захист каналу зв'язку (канал зв'язку – це сукупність ліній зв'язку й мережевого устаткування).

Для організації надійного каналу зв'язку застосовують наступні методи: виділені лінії зв'язку на фізичному рівні й логічні канали зв'язку. Фізичний захист каналу – екранування кабелю й розташування ліній зв'язку у важкодоступному місці. Логічний захист каналу – шифрування й стеганографія.Кожний з наведених методів має свої недоліки й переваги. Перевагою виділених ліній є ізоляція потоків даних на фізичному рівні, що обумовлює необхідність захисту каналу тільки від підключення в розрив і побічних електромагнітних випромінювань і наведень. Недоліком виділених ліній є порівняна висока вартість й неможливість застосування для організації дистанційного доступу.

Перевагою логічних каналів зв'язку є підтримка користувачів у будь-якій точці миру. Недоліком є поширення інформації, що захищається, у поділюваному середовищі передачі [16]. Враховуючи особливості систем відео-конференц зв’язку, у роботі був обраний для розгляду логічний спосіб організації каналу.

Для організації логічного каналу використовуються Virtual Private Network і Network Address Translation. Virtual Private Network (VPN) – віртуальна приватна мережа – технологія вилученого захищеного доступу, у якої виділяють як основний недолік: ефект танення трафіка й затримки потокового віщання. Загублені пакети відправляються повторно. Якщо пакет з якоїсь причини знову не буде отриманий, протокол TCP застосовує механізм збільшення тайм-ауту повторної передачі. При застосуванні протоколу TCP поверх TCP, внутрішньому TCP протоколу не доставляється вчасно повідомлення про одержання пакета TCP,

виникає збільшення сумарних затримок, зменшення швидкості передачі – ефект танення трафіка. Призастосуванні протоколу UDP поверх TCP, якщо пакет не був доставлений, відбувається повторна посилка даного пакета. Пакети, що перебувають у черзі чекають доставки даного пакета, через що виникають затримки потокового віщання.

Network Address Translation (NAT) – перетворення мережних адрес. Технологія призначена для спрощення й збереження IP Адрес. Дана функція є частиною можливостей маршрутизатора. Застосування Nat-таблиць дозволяє вирішити відразу кілька завдань:

- економія Ip-адрес за допомогою транслювання внутрішніх адресів у меншу кількість зовнішніх;
- обмеження запитів до внутрішніх хостів зовні, тому що ховається внутрішнє розташування вузлів.

Незважаючи на переваги, в NAT таблиць є й недоліки, які можуть приводити до появи вразливих місць. Нижче наведені основні види недоліків: NAT не є універсальним для всіх протоколів, наприклад, Ip підтримує NAT не у всіх режимах функціонування. Несумісність по протоколу вирішується застосуванням міжмережевих екранів, які заміняють Ip адреси не тільки в заголовках, але й на вищих рівнях.

Існує складність ідентифікації користувачів і, як наслідок, необхідність зберігати журнали трансляцій. Якщо одночасно працює велика кількість користувачів, робота мережі вповільнюється, тому що всі вхідні пакети повинні спочатку приходити на один вузол, де шляхом накладення маски перетворитися на адресу, а тільки потім відправлятися адресатові.

Адреси доставки повідомлень прописуються в тілі датаграми, також не застосовується при одночасній роботі великої кількості користувачів у мережі [15].

Одним зі способів організації захищеного (надійного) каналу є аутентифікація шляхом з'ясування координат користувача. Користувачвідправляє координати супутників, що перебувають у зоні прямої видимості. На сервері

аутентифікації зберігаються орбіти всіх супутників, що дозволяє з високою точністю визначити легітимність користувача, знаючи його дійсне географічне положення. Підробка координат украй ускладнена коливаннями, яким піддані орбіти. Недоліком даного методу є необхідність безперервного відправлення координат і наявність спеціалізованого апаратного модуля [23].

До засобів підвищення надійності відео-конференц зв'язку відносять:

- керування потоками даних, яке досягається спрощенням клієнтської частини додатка й реорганізацією серверної;
- перепідключення для зміни джерел плеєрів глядачів;
- керування мережними ресурсами за допомогою статистики;
- динамічний розподіл ресурсів мережі.

Основні методи підвищення надійності систем відео-конференц зв'язку на сьогоднішній день.

Використання оптимізованих сучасних протоколів маршрутизації для оптимального й раціонального використання канального ресурсу системи.

Використання алгоритму децентралізованих, що само організуються мереж, які дозволяють розподілити навантаження на всі елемент і пропорційно їх ресурсів і характеристикам, тим самим збільшуючи масштабованість і зменшуючи вартість такого рішення за відсутності необхідності підтримки протоколів прикладного рівня на мережевому.

Застосування механізмів динамічного перерозподілу швидкості передачі інформації при спільному обслуговуванні трафіку сервісів реального часу й трафіку даних, що допускає затримку [8].

Автоматичний спосіб визначення поточного мовця для призначення його потокам мультимедійних даних найбільшого пріоритету при передачі іншим учасникам.

Засоби розподілу (балансування) навантаження можуть бути програмнимий апаратними. Також системи балансування навантаження розділяють за рівнем, на якому вони працюють: рівень додатків, мережний або транспортний рівень. Системи ґрунтуються на інтелектуальних алгоритмах і можуть працювати як з

виділеним центром (клієнт-серверне рішення), так і бути розподіленими.

2.2 Аналіз класифікації основних способів навантаження мережі

Класифікація основних способів розподілу навантаження мережі представлено на рисунку 2.1.

Рисунок 2.1 – Класифікація способів розподілу навантаження

Поділ потоків інформації за змістом – навантаження на канали передачі даних може бути знижене за рахунок поділу маршрутів передачі пакетів з різним типом даних (відео, аудіо, текст і т. д.).

Розподіл за пропускною здатністю – при виборі маршруту передачі пакетів і вузла обробки в розподіленій системі враховуються кількісні характеристики каналу. Пропорційний розподіл навантаження – кожному компоненту системи ставиться у відповідність певна частка від усіх надходячих запитів. Рівномірний розподіл навантаження – метод застосовується, якщо компоненти розподіленої системи мають порівнянні технічні характеристики. Розподіл з урахуванням

максимальної кількості з'єднань – установлюється кількість з'єднань, при перевищенні якого запити не надходять доти, поки їх кількість не зменшиться. Розподіл по користувачах – за кожним користувачем закріплений маршрут передачі пакетів.

Інші алгоритми можна одержати, використовуючи комбінації декількох алгоритмів. Наприклад, використовувати процентний розподіл, але до досягнення максимального числа з'єднань. Для ухвалення оптимального рішення при виборі алгоритму керування навантаженням мережі необхідно враховувати трохи факторів:

- кількість користувачів;
- кількість пакетів в одиницю часу;
- вимоги до надійності;
- вимоги до швидкодії.

Існує два види балансування навантаження – апаратний й програмний, кожний із цих видів має як переваги, так і недоліки. Програмна реалізація більш інтелектуальна: системні утиліти швидше можуть аналізувати ситуацію, мають більш низьку вартість володіння. Апаратна реалізація на основі комутатора більш стабільна, тому що розподіл навантаження відбувається на нижніх рівнях моделі OSI (Open Systems Interconnection), відсутня прив'язка до конкретної операційної системи. Плюсом програмного балансування навантаження можна назвати можливість простого відновлення версії засобу.

Програмний розподіл навантаження може бути реалізований на основі централізованого або розподіленого алгоритму. Рішення з виділеним центром реалізується на основі топології «зірка», у центрі якого перебуває сервер балансування навантаження із установленої на нього програмою, яка ухвалює рішення щодо маршруту відправлення запитів. Централізоване рішення дозволяє ефективно управляти більшою кількістю серверів.

Перевагою розподіленого алгоритму є підвищена надійність. Недоліком розподіленого алгоритму є вповільнення роботи в мережі внаслідок постійного обміну повідомлення між серверами з метою визначення вільних серверів.

Розподілений алгоритм використовується переважно для невеликої кількості серверів, тому що обмін повідомленнями між ними не займає багато часу, а виділення центрального вузла, призначеного тільки для розподілу навантаження, економічно недоцільно.

Розглянуто як приклад продукт компанії Microsoft – технологію Windows Network load-balancing. У додатку використовується широкомовна доставка пакетів, у результаті чого швидкість передачі інформації зростає, також не виключена можливість лавинної маршрутизації. Ця проблема вирішується використанням комутатора вихідних даних по протоколу третього рівня, що породжує додаткові витрати [5] У зв'язку з одночасною доставкою вхідних даних на кожний сервер підвищується навантаження на концентратор або комутатор.

Для розподілу навантаження мережі широко застосовується технологія від компанії Microsoft Quality of Service (Qos). Qos цим терміном називають імовірність відповідності мережі зв'язку заданій угоді про трафік.

Технологія Qos являє собою набір технологій, що забезпечують пріоритетне використання каналу зв'язку деякими видами трафіка або програмами в порівнянні з методом «рівних можливостей». Існує 3 моделі реалізації Qos (Quality of service): найкраща можлива, інтегральна й диференційована. Інтегральна модель дозволяє контролювати пропускну здатність і затримки. Диференціальна модель являє собою набір засобів класифікації й механізмів організації черг, що забезпечують роботу із пріоритетами. Таким чином, інтегрований і диференціальний вид послуг взаємно доповнюють один одного, являють собою два різні способи керування навантаженням мережі.

Для реалізації технології Qos, використовується поняття так званої «розумної черги», повідомлення якої містять відомості про тип сервісу Type of Service (Tos) [95]. Поділ реалізується по типу протоколу. Необхідна умова: пакети повинні вже нести мітку типу сервісу для створення «розумної» черги. Підтримка механізмів Qos вбудована в Microsoft Windows. Мережева служба Qos в ОС Windows дозволяє виділити зарезервовану пропускну здатність (за замовчуванням вона рівна 20%). Недоліком технології є її прив'язка до типу

операційної системи.

2.3 Методи стеганографії для захисту відеоінформації

Методи стеганографії спрямовані на приховання факту передачі інформації. Загальною рисою цих методів є те, що приховуване повідомлення вбудовується в деякий невинний об'єкт, що не залучає уваги, [27]. Останнім часом стеганографія набирає все більшу популярність. Завдяки збільшенню пропускної здатності каналів стало можливим застосовувати методи стегокодування стосовно потокового відео.

Використання стеганографічних методів дозволяє додатково підвищити надійність системи відео-конференц зв’язку. До відомих стеганографічних методів відносять:

- використання полєй комп'ютерних форматів даних;
- спеціальне форматування файлів;
- використання зсуву слів, пропозицій;
- вибір певних позицій букв;
- видалення ідентифікуючого файлу заголовка;
- використання надмірності відео зображення, звуку й фотографій.

Одним з перспективних методів стеганографії є непряма стеганографія.

Принцип дії полягає в тому, що у відправника й одержувача є однакові масиви даних, які є закритими ключами. Байти інформації, що підлягають захисту, заміняються по певному алгоритму байтами конфіденційного масиву. Отриманий у результаті заміни масив передається адресатові. Адресат на своїй стороні застосовує дзеркальний алгоритм і одержує вихідне повідомлення [16].

Методи непрямої стеганографії використовуються для організації захищеного відео-конференц зв’язку. Система захисту постійно стежить за мережною активністю додатка, коли додаток ініціалізує мережеве підключення до вилученого ПК, система блокує передачу інформації від додатка в мережу, перенаправляє потік даних на себе й виконує підключення від свого імені до запитуваної вилученої системи. Даний метод має недоліки у вигляді великого

розміру ключа, рівного розміру переданої інформації, який необхідно потай передати [3]. Для підвищення надійності систем відео-конференц зв’язку може застосовуватися мережна стеганографія – це вид стеганографії, у якому у якості носіїв конфіденційної інформації використовуються мережні протоколи еталонної моделі OSI. Мережна стеганографія являє собою сімейство методів модифікації даних у заголовках мережних протоколів і в полях даних пакетів, а також зміни способів передачі пактів. Зустрічаються також гібридні методи. Передача даних у мережній стеганографії здійснюється через «схований канал», який можна організувати усередині будь-якого відкритого каналу за умови надмірності переданих пакетів. Дослідження в області мережної стеганографії проводяться польськими вченими [25], американськими вченими E. Cauich, R. Gomez [26]. Методи мережної стеганографії можна розділити на три групи.

Зміна даних у полях заголовків мережних протоколів і в полях корисного навантаження пакетів: зміна інформації в полях заголовків; модифікація даних; комбіновані методи.

Зміна способу передачі пакетів: зміна порядку послідовності пакетів, зміна затримки між пакетами, уведення навмисної втрати пакетів шляхом пропуску порядкових номерів у відправника.

Гібридні методи – зміна вмісту пакетів, строків доставки пакетів і порядкуїх передачі.

В роботі застосовується гібридний метод, заснований на зміні даних в полях заголовків, а також модифікації даних і застосуванні алгоритму розподілу навантаження.

Технологія вбудовування стегоконтейнерів у відеопотік слабо пророблена, тому що приховання інформації пов'язане з певними труднощами. В області створення стеганографічних систем для передачі схованої інформації в мультимедіа даних найчастіше застосовуються два методи – заміна найменш значущих бітів і вейвлет-перетворення.

Перший метод має істотний недолік у тому, що він широко відомий і порушник може не тільки легко відновити сховану інформацію, але й вилучити її

без втрати якості (привласнити останнім бітам значення «0»). Можливе використання заміни значущих бітів по певній таблиці. Недоліком у цьому випадку буде поява викривлень сигналу. Також виникає проблема безпечної передачі таблиці підстановок, яка є закритим ключем.

Таким чином, незважаючи на велику різноманітність системкомп'ютерного відео-конференц зв’язку, на ринку в основному представлені засоби закордонного виробництва, що несе в собі певну погрозу при використанні таких систем у державних установах і робить актуальними дослідження в області створення надійних систем відео-конференц зв’язку.

2.4 Імовірнісні методи доступу до систем ВКЗ

На першому етапі роботи методу підвищення надійності ВКЗ визначаються вихідні параметри системи й необхідний рівень імовірності одержання доступу до інформаційних ресурсів системи ВКЗ. На другому етапі**, з** метою визначення фактичного значення ймовірності одержання доступу, будуються моделі доступу верхнього й нижнього рівня. На третьому етапі отримані результати аналізуються та відбувається порівняння поточного значення ймовірності одержання доступу з необхідним значенням імовірності одержання доступу. При необхідності збільшення поточного значення імовірності одержання доступу до інформаційних ресурсів відео-конференц зв’язку застосовується алгоритм керування навантаженням мережі, розроблений автором.

В ході досліджень була запропонована імовірнісна модель доступу до систем відео-конференц зв’язку, придатна для оцінки надійності таких систем. Розроблена модель дозволяє описати різні системи відео-конференц зв’язку й ураховує їхні характерні риси.

Значення ймовірності одержання доступу може бути розраховане на основі апарата Марківських випадкових процесів з дискретними станами й безперервним часом. Імовірнісна модель доступу верхнього рівня, запропонована в роботі, заснована на поняттях: суб'єкти, об'єкти, дії. Для кожного об'єкта доступним є певний перелік дій. Відносини суб'єктів і об'єктів,що представлено в таблиці 2.1,

де P_{ijk} – імовірність здійснення дії, A_k– кількість дій, які можна виконати над об'єктом, B – кількість об'єктів, R – кількість суб'єктів, щоб одержати доступ, усі R суб'єкти повинні мати можливість зробити кожне з A припустимих дій з B об'єктами.

Імовірність одержання кожним суб'єктом повного доступу до кожного об'єкта виражена формулою (2.1):

Таблиця 2.1 – Відносини суб’єктів доступу і об’єктів доступу

	Об’єкт 1		Об’єкт Б	
Дія 1	Суб’єкт 1	Суб’єкт R	Суб’єкт 1	Суб’єкт R
	P	P	P	P
	111	P	1B1	1R1
	112	R12	1B2	RB2

Імовірність одержання кожним суб'єктом повного доступу до кожного об'єкта виражена формулою (2.1):

$$\widetilde{P} = \prod_{i=1}^{R} \widetilde{P}_i \ . \tag{2.1}$$

Імовірність одержання *i*-суб'єктом доступу до довільного об’єкта (формула 2.2):

$$\widetilde{P}_i = \prod_{j=1}^{B} \widetilde{P}_{ij} \ . \tag{2.2}$$

Імовірність одержання доступу суб'єкта до об'єкта дорівнює добутку ймовірностей усіх дій суб'єкта до об'єкта (формула 2.3):

$$\widetilde{P}_{ij} = \prod_{k=1}^{A} \widetilde{P}_{ijk} \ . \tag{2.3}$$

Тоді ймовірність одержання кожним суб'єктом повного доступу кожному об'єкту виражена формулою 2.4:

$$\widetilde{P} = \prod_{i=1}^{R} \prod_{j=1}^{B} \prod_{k=1}^{A} \widetilde{P}_{ijk} \,. \tag{2.4}$$

Значення ймовірності одержання повного доступу на підставі статистичних даних ймовірностей суб'єктів до j об'єктів визначається здійсненням *k* дій *i* суб'єктів до *j* об’єктів.

2.5 Проектування ймовірнісних моделей нижнього рівня

Суб'єктами імовірнісної моделі нижнього рівня є сервер (*s*) і клієнт (*c*) . Об'єкти: відео, аудіо, текстовий файл, повідомлення, віртуальна дошка. Дії: читання, запис, створення, редагування, виконання, видалення, відправлення. Для кожного об'єкта доступним є певний перелік дій. Відносини суб'єктів і об'єктів представлено в таблиці 2.2, де «-» – дія стосовно даного об'єкта не застосовується.

Таблиця 2.2 – Можливі дії суб'єктів до об'єктів

	відео		аудіо		файл		повідомлення		дошка	
	S	C	S	C	S	C	S	C	S	C
читання	$\widetilde{P_{111}}$	$\widetilde{P_{211}}$	$\widetilde{P_{121}}$	$\widetilde{P_{221}}$	$\widetilde{P_{131}}$	$\widetilde{P_{231}}$	$\widetilde{P_{141}}$	$\widetilde{P_{241}}$	$\widetilde{P_{151}}$	$\widetilde{P_{251}}$
запис	$\widetilde{P_{112}}$	$\widetilde{P_{212}}$	$\widetilde{P_{122}}$	$\widetilde{P_{222}}$	$\widetilde{P_{132}}$	$\widetilde{P_{232}}$	$\widetilde{P_{142}}$	$\widetilde{P_{242}}$	$\widetilde{P_{152}}$	$\widetilde{P_{252}}$
створення	-	-	-	-	$\widetilde{P_{133}}$	$\widetilde{P_{233}}$	$\widetilde{P_{143}}$	$\widetilde{P_{243}}$	$\widetilde{P_{153}}$	$\widetilde{P_{253}}$
редагування	-	-	-	-	$\widetilde{P_{134}}$	$\widetilde{P_{234}}$	$\widetilde{P_{144}}$	$\widetilde{P_{244}}$	$\widetilde{P_{154}}$	$\widetilde{P_{254}}$
виконання	-	-	-	-	$\widetilde{P_{135}}$	$\widetilde{P_{235}}$	$\widetilde{P_{145}}$	-	-	-
видалення	-	-	-	-	$\widetilde{P_{136}}$	$\widetilde{P_{236}}$	$\widetilde{P_{146}}$	$\widetilde{P_{246}}$	$\widetilde{P_{156}}$	$\widetilde{P_{256}}$
відправлення	$\widetilde{P_{117}}$	$\widetilde{P_{217}}$	$\widetilde{P_{127}}$	$\widetilde{P_{227}}$	$\widetilde{P_{137}}$	$\widetilde{P_{237}}$	$\widetilde{P_{147}}$	$\widetilde{P_{247}}$	-	-

Критерій надійності системи сформульований у такий спосіб (формула 2.5):

$$\widetilde{P} \to 1. \tag{2.5}$$

Імовірність одержання кожним суб'єктом повного доступу до кожного об'єкта виражена формулою (формула 2.6):

$$\widetilde{P} = \widetilde{P}_1 \cdot \widetilde{P}_2, \tag{2.6}$$

де $\tilde{P}_1$ – імовірність доступності сервера,

$\tilde{P}_2$ – ймовірність доступності сервера

Складається з ймовірностей (формула 2.7):

$$\widetilde{P}_1 = \tilde{P}_{11} * \tilde{P}_{12} * \tilde{P}_{13} * \tilde{P}_{14} * \tilde{P}_{15}, 9 \tag{2.7}$$

де $\tilde{P}_{11}$ – доступність відеоінформації на сервері,

$\tilde{P}_{12}$ – доступність аудіо інформації на сервері,

$\tilde{P}_{13}$ – доступність файлів на сервері,

$\tilde{P}_{14}$ – доступність повідомлень на сервері,

$\tilde{P}_{15}$ – доступність віртуальної дошки на сервері.

Імовірність доступності клієнта (формула 2.8):

$$\widetilde{P}_2 = \tilde{P}_{21} * \tilde{P}_{22} * \tilde{P}_{23} * \tilde{P}_{24} * \tilde{P}_{25} \tag{2.8}$$

де $\tilde{P}_{21}$ – доступність відеоінформації у клієнта,

$\tilde{P}_{22}$ – доступність аудіо інформації клієнта,

$\tilde{P}_{23}$ – доступність файлів у клієнта,

$\tilde{P}_{24}$ – доступність повідомлень у клієнта,

$\tilde{P}_{25}$ – доступність віртуальної дошки в клієнта.

Імовірності здійснення k-ї дії для сервера (формула 2.9):

$$\tilde{P}_{11} = \Pi_{k=1}^{5} \tilde{P}_{11k} \ , \ \tilde{P}_{12} = \Pi_{k=1}^{5} \tilde{P}_{12k} , \ \tilde{P}_{12} = \Pi_{k=1}^{5} \tilde{P}_{12k} , \ \tilde{P}_{12} = \Pi_{k=1}^{5} \tilde{P}_{12k} , \ \tilde{P}_{12} = \Pi_{k=1}^{5} \tilde{P}_{12k} , \quad (2.9)$$

де $\tilde{P}_{1_1k}$ – імовірність здійснення k-ї дії з відеоінформацією на сервері,

$\tilde{P}_{1_2k}$ – імовірність здійснення k-ї дії з аудіо інформацією на сервері,

$\tilde{P}_{1_3k}$ – імовірність здійснення k-ї дії з файлами на сервері,

$\tilde{P}_{1_4}k$ – імовірність здійснення k-ї дії з повідомленнями на сервері,

$\tilde{P}_{1_5k}$ – імовірність здійснення k-ї дії з віртуальною дошкою на сервері.

Імовірність здійснення k-ї дії для клієнта (формула 2.10):

$$\tilde{P}_{21} = \Pi_{k=1}^{5} \tilde{P}_{21k} , \ \tilde{P}_{22} = \Pi_{k=1}^{5} \tilde{P}_{22k} , \ \tilde{P}_{23} = \Pi_{k=1}^{5} \tilde{P}_{23k} , \ \tilde{P}_{24} = \Pi_{k=1}^{5} \tilde{P}_{24k} , \ \tilde{P}_{25} = \Pi_{k=1}^{5} \tilde{P}_{25k} , \quad (2.10)$$

де $\tilde{P}_{2_1k}$ – імовірність здійснення k-ї дії з відеоінформацією на сервері,

$\tilde{P}_{2_2k}$ – імовірність здійснення k-ї дії з аудіо інформацією на сервері,

$\tilde{P}_{2_3k}$ – імовірність здійснення k-ї дії з файлами на сервері,

$\tilde{P}_{2_4k}$ – імовірність здійснення k-ї дії з повідомленнями на сервері,

$\tilde{P}_{2_5k}$ – імовірність здійснення k-ї дії з віртуальною дошкою на сервері.

Суб'єктами імовірнісної моделі нижнього рівня є сервер (s) і клієнт (c) . Об'єкти: відео, аудіо, текстовий файл, повідомлення, віртуальна дошка. Дії: читання, запис, створення, редагування, виконання, видалення, відправлення.

3 ПРОЕКТУВАННЯ АЛГОРИТМІВ ГАРАНТОВАНОЇ ДОСТАВКИ ПОВІДОМЛЕНЬ

3.1 Оцінювання ймовірності одержання доступу

Введено припущення: при одержанні доступу до серверу клієнт одночасно одержує доступ до всіх інформаційних ресурсів. Тоді для визначення ймовірності повного доступу до системи ВКЗ, що складається з декількох серверів і клієнтів, необхідно визначити ймовірність доступності серверів і ймовірність доступності клієнтів. Імовірність доступності клієнтів у рамках розв'язуваного завдання прийнята рівної 1, а ймовірність одержання доступу до інформаційних ресурсів системи відео-конференц зв’язку визначається ймовірністю доступності серверів.

Стани сервера: сервер вільний (або сервер обробляє заявки, але ухвалює нові, що надходять на обробку); сервер зайнятий обслуговуванням заявок і не може більше ухвалювати заявки, усі прихожі заявки в черзі, обмеженої за часом (або несправний). Позначення:

- P_0 – імовірність того, що всі сервери вільні;
- P_1 – імовірність того, що один сервер зайнятий, інші вільні;
- Pn – імовірність того, що всі сервери зайняті, нуль заявок у черзі;
- $Pn+m$ – імовірність того, що всі сервери зайняті, m заявок у черзі (імовірність відмови).

Значення ймовірності одержання доступу розраховується на основі апарата Марківських випадкових процесів з дискретними станами й безперервним часом. Отримане значення ймовірності одержання доступу рівняється з необхідним рівнем імовірності одержання доступу, при необхідності підвищення рівня ймовірності одержання доступу за допомогою алгоритму керування навантаженням мережі.

Представлений метод підвищення надійності ВКЗ для авторизованих користувачів з гарантованою доставкою повідомлень. Автором побудовані імовірнісної моделі доступу верхнього й нижнього рівня до інформаційних ресурсів систем ВКЗ. Імовірнісні значення доступу дозволяють визначити надійність системи, що раніше було трудомістким завданням (в інших реалізаціях

імовірнісної моделі доступу) або не розглядалося (у логічних моделях доступу). Отримане значення ймовірності одержання кожним суб'єктом повного доступу до кожного об'єкта рівняється з необхідним значенням імовірності одержання кожним суб'єктом повного доступу до кожного об'єкта, при необхідності надалі застосовується алгоритм керування навантаженням мережі, який розглянутий у третьому розділі.

3.2 Алгоритм керування навантаженням мережі

Розроблено алгоритм керування доступом до інформаційних ресурсів системи ВКЗ з метою підвищення надійності для авторизованих користувачів з гарантованою доставкою повідомлень. У роботі запропонований алгоритм, призначений для використання в системах з гарантованою доставкою повідомлень, що функціонують із використанням мережного протоколу TCP стека TCP/IP. Запропонований алгоритм керування доступом до інформаційних ресурсів систем відео-конференц зв’язку – алгоритм керування навантаженням мережі «Мітка привілеїв», призначений для використання в системах з гарантованою доставкою повідомлень, заснованих на мережному протоколі TCP стека TCP/IP [18]. Застосування алгоритму керування навантаженням мережі дозволяє системі відео-конференц зв’язку функціонувати у двох режимах: стандартному й спеціальному. У стандартному режимі TCP-пакети передаються від джерела адресатові через будь-який доступний сервер. У спеціальному режимі сервер вибирається за певним алгоритмом, а пакети клієнтів модифікуються: пакет містить мітку початку спеціального режиму, мітку привілеїв і мітку останнього спеціального пакета. Мітки додаються вслужбове зарезервоване поле.

«Опції» заголовка TCP пакета (розташовані з160 по 192 біт).Мітка привілеїв призначена для виконання авторизації з метою підвищення надійності систем відео-конференц зв’язку. Для додавання у відеопотік міток з авторизаційною інформацією використовуються методи стеганографії [19]. Мітки привілеїв призначаються виходячи з необхідного значення ймовірності одержання доступу до інформаційних ресурсів систем ВКЗ. Структура пакета представлена на

рисунку 3.1.

<table>
<tr><td colspan="8">16 біт номер порту джерела</td><td colspan="2">16 біт номер порту призначення</td></tr>
<tr><td colspan="10">32 біта номер послідовності</td></tr>
<tr><td colspan="10">32 біта номер підтвердження</td></tr>
<tr><td>4 біта довжина заголовка</td><td>6 біт зарезервовано</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="2">16 біт розмір вікна</td></tr>
<tr><td colspan="8">16 біт контрольна сума TCP</td><td colspan="2">16 біт покажчик терміновості</td></tr>
<tr><td>4 бітамітка

початку спеціального режиму</td><td>4 біта мітка

останнього спеціального пакету</td><td colspan="4">8 біт міткапривілеїв</td><td colspan="4"></td></tr>
<tr><td colspan="2">8 бітів авторизаційна інформація</td><td colspan="8">Дані</td></tr>
</table>

Рисунок 3.1 – Структура пакету

Перехід зі стандартного режиму роботи мережі в спеціальний режим здійснюється в такий спосіб: після приймання пакета сервер перевіряє наявність мітки початку спеціального режиму, якщо результати перевірки позитивні – мережа переходить до спеціального режиму, інакше пакет доставляється адресатові й ухвалюється новий пакет. Спеціальний режим складається із трьох етапів: підготовка, безпосередньо спеціальний режим і завершення роботи [18].

В стандартному режимі роботи мережі пакети передаються безпосередньо від джерела до адресата через будь-який сервер, у спеціальному режимі сервера й клієнти з'єднуються між собою особливим образом. На першому етапі роботи

алгоритму клієнт відправляє пакет з міткою початку спеціального режиму першому серверу відповідно до таблиці привілеїв серверів. У випадку позитивної відповіді сервера встановлюється з'єднання, у випадку негативної відповіді – пакет з міткою початку спеціального режиму відправляється наступному серверу. Перший сервер, що відповів позитивно, записує мітку привілеїв клієнта.

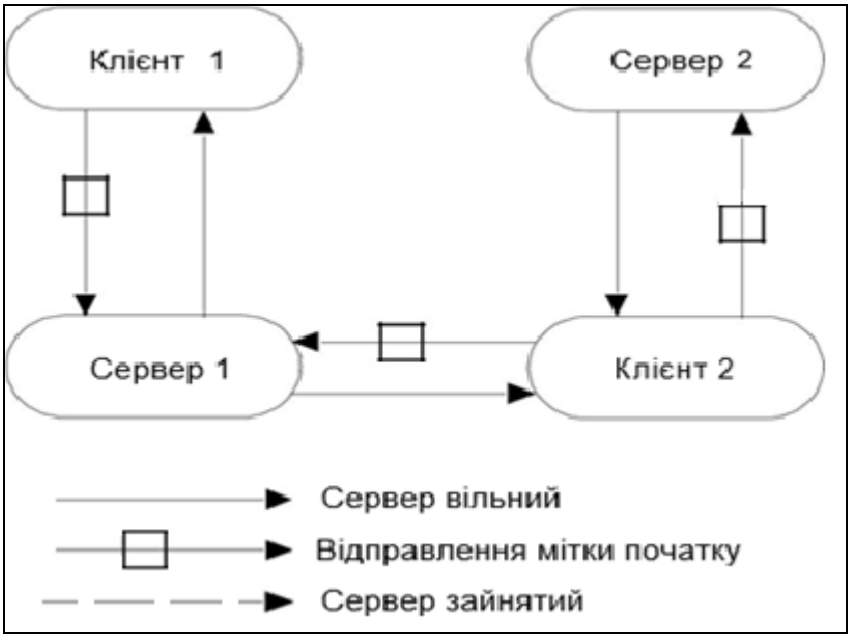

Рисунок 3.2 – Алгоритм підготовки

Сервера накопичують мітки привілеїв клієнтів, щоб визначити, наскільки вони зайняті, і відхилити мітки привілеїв нових клієнтів при досягненні критичного значення. Кожний сервер підтримує заздалегідь певну кількість таких з'єднань, на час спеціального режиму клієнт закріплений за одним сервером.

3.3 Опис алгоритму для спеціального режиму

Другий етап роботи алгоритму є безпосередньо спеціальним режимом. Відправлення всіх пакетів клієнта відбувається через закріплений сервер. Кожний клієнт відправляє дані серверу, за яким він закріплений, сервер у свою чергу перенаправляє дані адресатові. Клієнт може ухвалювати інформацію від будь-якого сервера. Трафік без міток привілеїв у спеціальному режимі не обробляється (див. рис. 3.3). У спеціальному режимі відбувається обов'язкова перевірка дійсності мітки привілеїв, тільки при позитивному результаті пакет доставляється

адресатові.

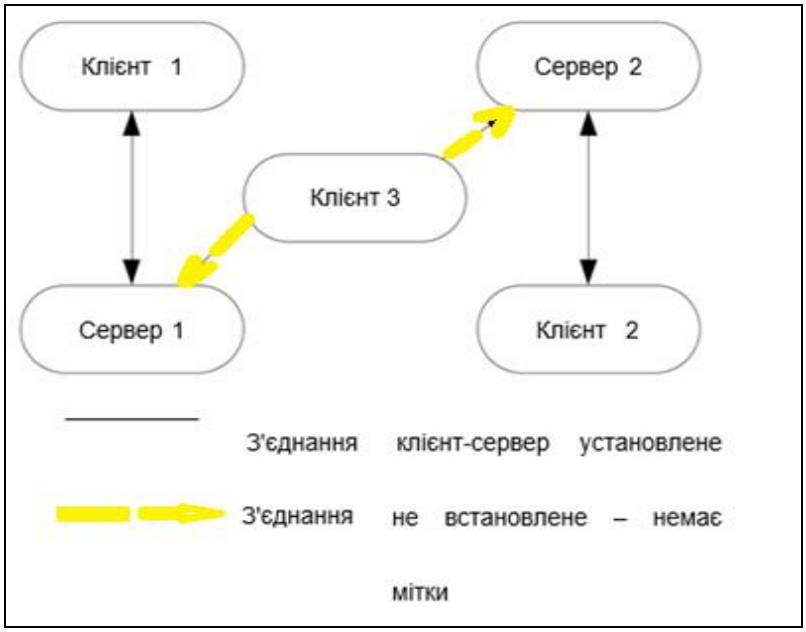

Рисунок 3.3 – Спеціальний режим

Якщо мітки привілеїв нема, то визначається, чи ввійшла вже мережа в спеціальний режим. Для цього на сервері вводиться змінна – маркер початку спеціального режиму. Якщо значення маркера початку спеціального режиму рівно 0, і алгоритм не повинен завершити свою роботу, то проводиться звичайна обробка повідомлень. При одержанні першого спеціального пакета маркеру початку спеціального режиму привласнюється значення 1. Інакше, якщо сесія в спеціальному режимі вже почалася, то звичайне повідомлення зупиняється. Через певні періоди часу проводиться повторна перевірка наявності мітки початку спеціального режиму. У спеціальному режимі відбувається обов'язкова перевірка авторизаційної інформації, при позитивному результаті пакет доставляється адресатові [22].

На третьому етапі відбувається завершення спеціалізованого режиму. Клієнт відправляє серверу мітку останнього пакета, після чого сервер може встановити з'єднання із ще одним клієнтом. Потім відбувається перевірка мітки останнього пакета, вона означає, що необхідно привласнити маркеру початку спеціального режиму значення – 1, доставити останній пакет і перейти до звичайної роботи мережі (див. рис. 3.4).

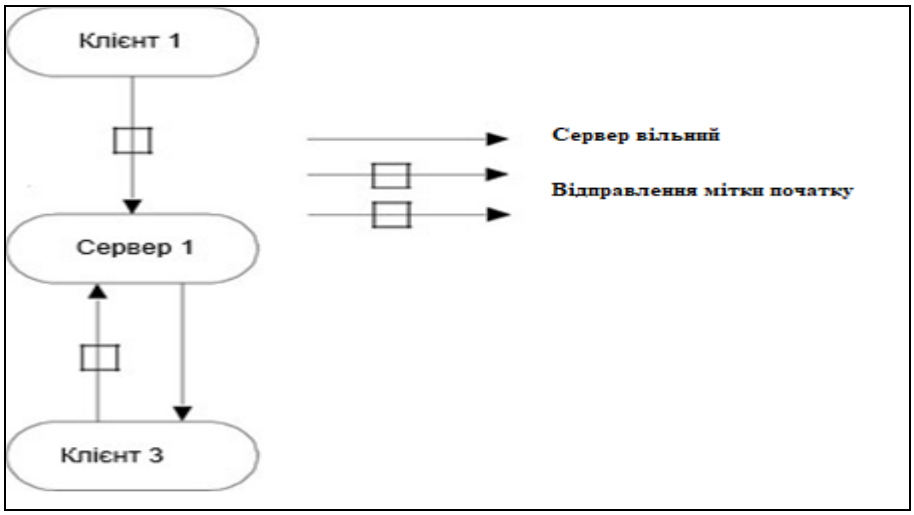

Рисунок 3.4 – Завершення роботи

Для рішення можливої проблеми, пов'язаної із блокуванням сервера при втраті пакета з міткою останнього спеціального пакета необхідно припиняти з’єднання із клієнтом по досягненню певного часу з моменту передачіостаннього пакета.

3.4 Опис алгоритму для єдиного серверу

Окремий випадок роботи алгоритму – єдиний сервер представлено на рисунку 3.5.

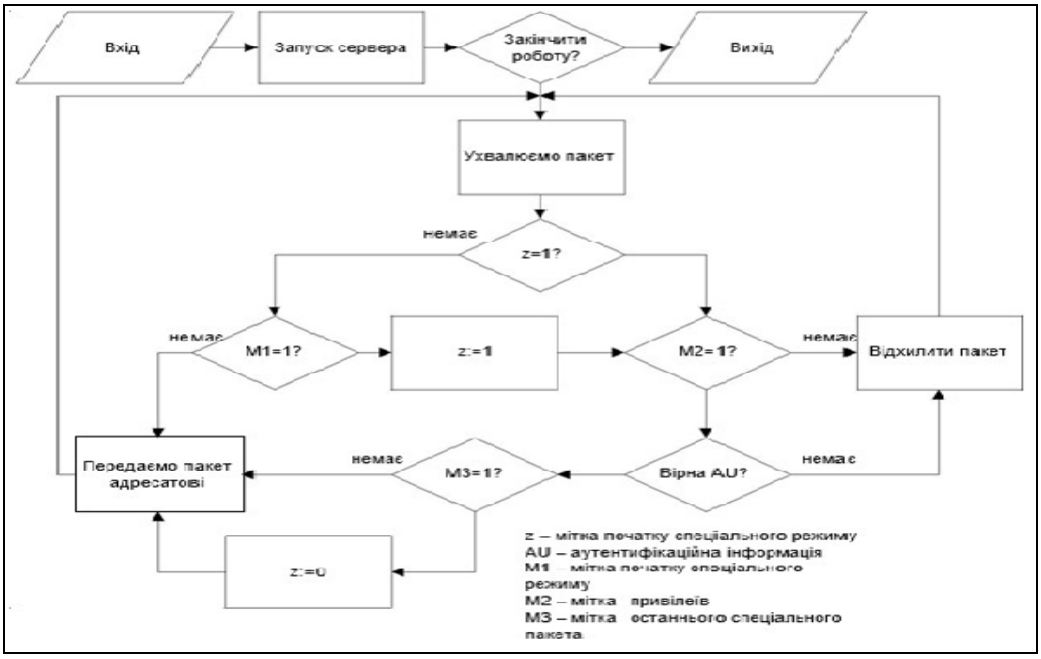

Рисунок 3.5 – Алгоритм роботи сервера

Алгоритм роботи клієнта представлено на рисунку 3.6.

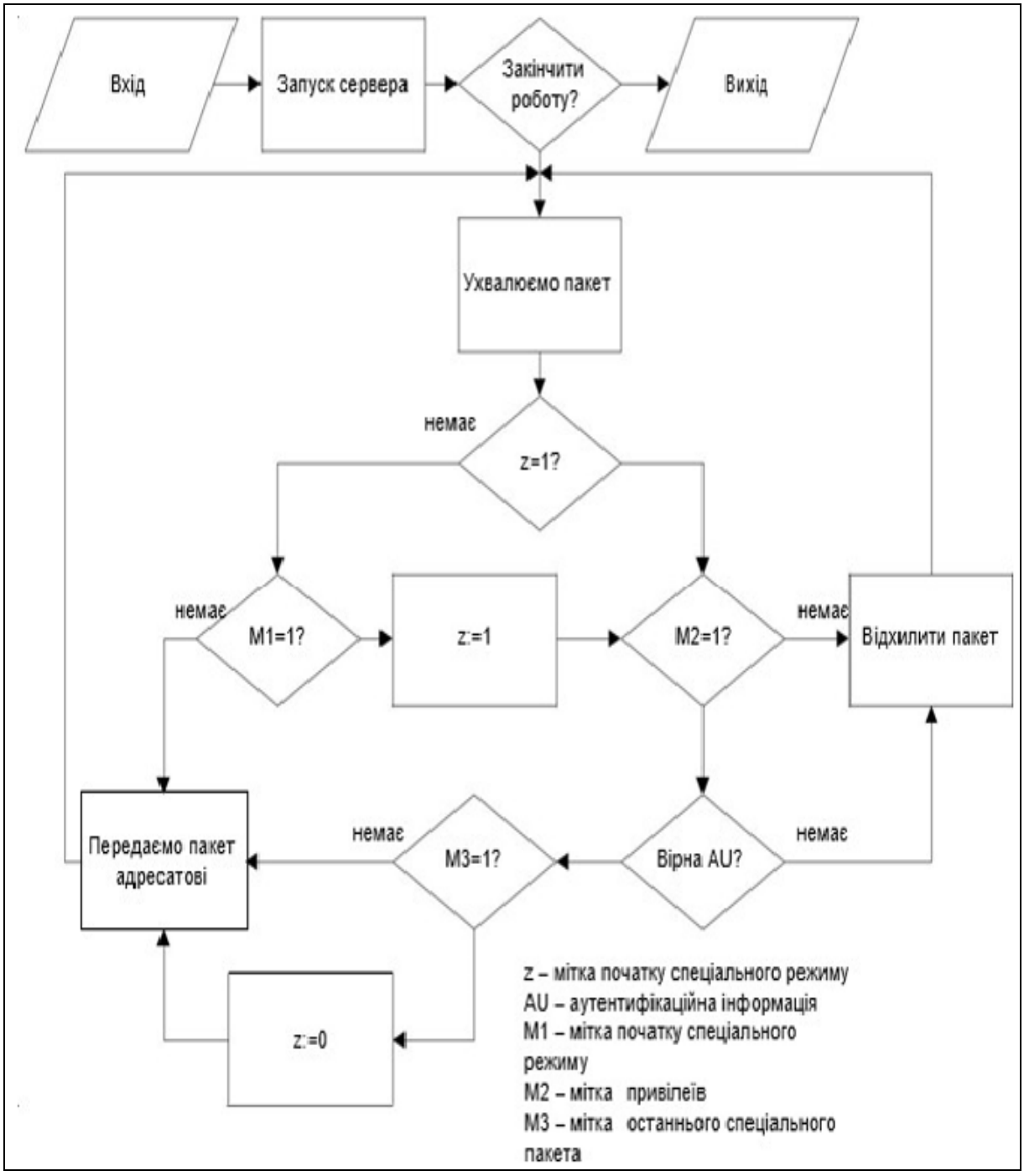

Рисунок 3.6 – Алгоритм роботи клієнта

На рисунку 3.7 представлений алгоритм приймання/передачі пакетів. Усі пакети проходять через сервер, де відбувається перевірка інформації про авторизацію.

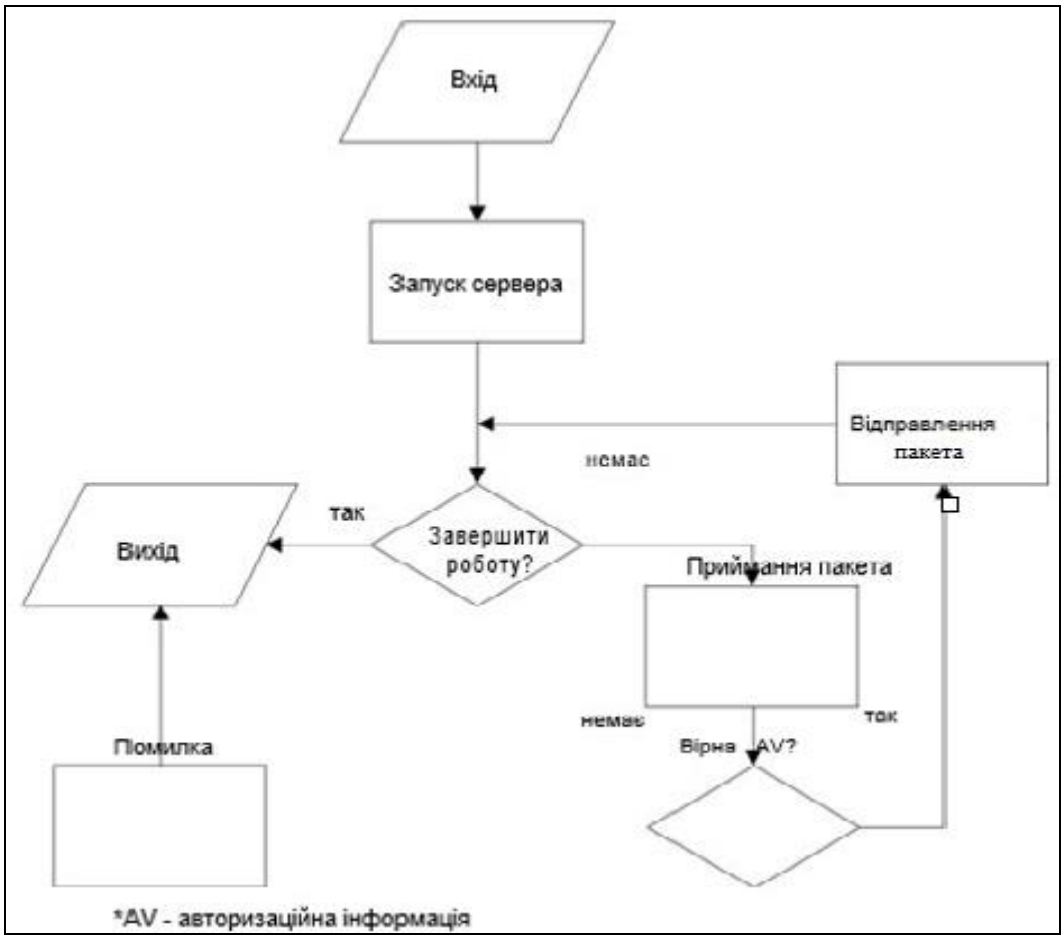

Рисунок 3.7 – Відправлення пакетів

3.5 Опис алгоритму стеганографічного перетворення

В алгоритмі керування навантаженням мережі «Мітка привілеїв» авторизаційні мітки додаються за допомогою методів стеганографії. Авторизаційна інформація передається в такий спосіб: у пакет включається зсув до наступного пакета з авторизаційною інформацією: кожний пакет зі стегоконтейнером на початку поля даних буде містити інформацію про номер наступного пакета зі стегоконтейнером. Задається зсув, а не номер пакета, тому що в загальному випадку на кодування зсуву буде потрібно менша кількість біт.

У налаштуваннях програми, що реалізує алгоритм керування навантаженням мережі «Мітка привілеїв» визначається кількість біт на початку пакета, виділенепід адресу наступного пакета.

Кожний виділений під зсув біт дозволяє суттєво збільшити відстань між пакетами й тим самим згладити статистичні характеристики відеопотоку.

Альтернативним способом передачі інформації про авторизаційні пакети є запис таблиці, що містить номера пакетів з авторизаційною інформацією на апаратні ключі. У цьому випадку перетворення відбуваються в клієнта, що забезпечує додаткову надійність, тому що інформація у відкритому виді не переміщається по мережі.

Математичний апарат оцінки системи відео-конференц зв'язку будується на основі багатоканальних систем масового обслуговування з обмеженою чергою для випадку стандартного режиму роботи системи й сукупності однорідних одно канальних СМО з обмеженою чергою [32].

Для побудови моделі стандартного режиму були прийняті наступні вихідні дані:

- $S = \{\sigma_\iota, i = 1, n\}$ – множина серверів у системі;
- $C = \{\chi_j, j = 1, k\}$ – множина клієнтів у системі;
- $M(S) = n$ – кількість серверів у системі;
- $M(C) = k$ кількість клієнтів у системі.

Для кожного сервера $s_i \in S$ визначене μ_ι – швидкість обробки заявок, усі сервери в системі однакові зі швидкістю обробки заявок μ (формула 3.1):

$$\forall s_i, s_j \in S : \mu_i = \mu_j = \mu . \tag{3.1}$$

Для кожного клієнта $Ci \in \chi$ простий Пуасоновський процес однакові характеристики й інтенсивності (формула 3.2) і вступний потік заявок розглядається як інтенсивності λ_ι, усі клієнти в системі створюють потік заявок (пакетів) однакової (формула 3.3):

$$\forall \chi\iota, c_j \in C : \lambda\iota = \lambda_j = \lambda_1, \tag{3.2}$$

$$\lambda = \sum_{i=1}^{k} \lambda\iota = k\lambda_1, \tag{3.3}$$

де λ – загальна інтенсивність потоку від клієнтів.

Розрахунок імовірностей стану системи представлений нижче. Формули 3.4 і 3.5 визначають значення ймовірності Pi для $i = 1$, $i = 2$. Дані формули можна використовувати в якості бази для застосування методу математичної індукції. Для випадку $k > n$:

$$\lambda \quad Pn = \text{n } \mu\pi\nu+1 \rightarrow Pn + 1 = \frac{\lambda\mu}{n} Pn \tag{3.4}$$

$$\lambda \quad Pn +1 = \text{n } \mu\pi\nu+2 \rightarrow Pn + 2 = \frac{\lambda_2}{\mu_2 n_2} PnPk \tag{3.5}$$

Можна починати, що клієнти розподіляються на рівні групи (формула 3.6).

$$\forall \chi\iota, C_j : M(\chi\iota) = M(X_j) = k/n = k \tag{3.6}$$

Система в спеціальному режимі розглядається як сукупність незалежних однорідних одноканальних СМО з обмеженою чергою й відмовами. У цьому випадку сумарний потік заявок (пакетів) від групи клієнтів для *i*-сервера рівний.

Оцінка ефективності застосування комп'ютерного методу підвищення надійності проводиться шляхом порівняння стандартного (аналогічний режиму роботи мережі, у якому не застосовується алгоритм «Мітка привілеїв») і спеціального режимів алгоритму керування навантаженням мережі «Мітка привілеїв».

Обрані наступні характеристики:

- принцип роботи;
- час передачі пакета;
- відмови;
- час зв'язку із сервером;
- система масового обслуговування, що імітує режим.

4 ОПИС РОЗРОБЛЕНОЇ ПРОГРАМНОЇ СИСТЕМИ

4.1 Опис вимог до програмного засобу

Програмний засіб, що реалізує розроблений алгоритм «Мітка привілеїв», повинен відповідати наступним загальним вимогам:

- програма повинна підтримувати операційні системи сімейства Windows і Linux, важливо, щоб система була кросплатформенною, тому що мережа може бути гетерогенною;
- програма повинна передбачати можливість роботи декількох клієнтів з декількома серверами;
- відновлення при збоях повинне здійснюватися автоматично при перезапуску програми;
- програма повинна забезпечувати підвищення надійності відео-конференц зв’язку із завданим критерієм – імовірність одержання доступу до інформаційних ресурсів.

Вимоги до функціоналу:

- програма повинна забезпечувати можливість участі клієнтів у відеоконференції за допомогою авторизації по паролю;
- програма повинна дозволяти адміністраторові призначати привілеї користувачам для керування привілейованим доступом до інформаційних ресурсів системи відео-конференц зв’язку, а також додавання й видалення користувачів і IP-адрес (на підставі сканування локальної мережі, а також вручну), можливість збору статистики звертань до мережних ресурсів (графік активності користувачів).

Вимоги до зручності експлуатації:

- інтерфейс програми повинен бути інтуїтивно зрозумілим і містити мінімум вікон з об'єднанням функцій вибору в одне вікно з метою забезпечення прозорості для користувача;
- програма повинна підтримувати роботу адміністратора у фоновому режимі.

- у програмі повинна забезпечуватися сумісність різного мережного встаткування.
- програма повинна підтримувати можливість вилученої установки клієнтських додатків .
- додаткова вимога: таблиці відповідності номерів, що містять стегоконтейнери з авторизаційною інформацією, повинні зберігатися на апаратних ключах.

4.2 Інструменти розробки

В рамках роботи над створенням програмного засобу, що реалізує алгоритм керування навантаженням мережі, була вивченаспецифікація RFC 793, що описує структуру пакета TCP, і були підібрані інструменти розробки: бібліотеки Pcap (Packet Capture) і libnet, а також отриманий досвід низькорівневого мережного програмування. Бібліотеки PCAP і libnet є кросплатформеними, з їхньою допомогою можна створити власну програму, що реалізує функції обробки TCP заголовків. У ході роботи над програмою була вивчена кросплатформена бібліотека QT, за допомогою якої була реалізована можливість сумісність програми з різними операційними системами [22].

Для кодування відео була обрана технологія MJPEG (Motion Joint Photographic Experts Group), при використанні якої після стиску кадра авторизаційна інформація вбудовується шляхом заміни окремих байт. У розроблювальній програмі необхідно кодувати відео в реальному часі, а вбудовування схованої інформації збільшує час кодування, тому швидкість роботи алгоритму є важливим параметром при виборі технології кодування.

Варто відзначити, що MJPEG має меншу ступінь стиску, чому MPEG2 або MPEG4 [4], [12], однак, перевагою відеокодеку є швидкість кодування. Ще одна перевага MJPEG перед MPEG2 і MPEG4 – вільна ліцензія, вона дозволяє розробляти власні алгоритми на основі MJPEG без необхідності ліцензування.За перерахованими вище причинами як основу для розробки власного алгоритму стегокодування був обраний MJPEG .

Допущення, прийняті при проектуванні програми:

- пропускна здатність (транзакції в секунду) обмежується швидкістю мережі, середній і максимальний час відповіді для транзакцій: залежить від потужності встаткування;
- час відновлення екрана залежить від установленої частоти відновлення монітора (за замовчуванням 1/60 секунди);
- час реакції на дію користувача 50 мс (обмежується роботою системного таймера);
- відновлення при збоях відбувається автоматично при перезапуску програми.

Програма припускає наявність двох видів користувачів:

- «Клієнт» – за допомогою клієнтської частини додатка авторизується в системі й одержує доступ до відеоконференції, у ході якої передає й одержує інформацію;
- «Адміністратор» – управляє налаштуваннями мережі за допомогою серверної частини додатка. Додає й видаляє користувачів, дозволені Ip-адреси.

Для реалізації алгоритму «Мітка привілеїв» необхідно реалізувати зміни на рівні TCP пакетів, що зажадає написання власного механізму обробки пакетів на мережному рівні. У специфікації протоколу TCP зазначене службове поле «Опції», мітки привілеїв: мітка першого повідомлення, мітка останнього повідомлення й мітка привілеїв можуть бути записані в дану область.

4.3 Опис логічної структури програмного засобу

В роботі розроблений програмний засіб, призначений для організації надійної системи відео-конференц зв’язку. Для кодування відео використовується технологія MJPEG, після стиску кадра авторизаційна інформація вбудовується шляхом заміни окремих байт. Удосконалений продукт надалі буде включати апаратну частину, представлену у вигляді апаратних ключів. Особливістю програми є вбудовування міток у службове поле «Опції» TCP пакету й додавання

авторизаційної інформації в поле даних стенографічними методами. Зміни відбуваються на рівні TCP пакетів, що призвело до написання власного механізму обробки пакетів на мережному рівні: мітка початку спеціального режиму, мітка привілеїв і мітка останнього спеціального пакета вносяться в службове поле «Опції», яке розташовано з 160 по 192 біт. Програма являє собою клієнт-серверний додаток. Програма може функціонувати під операційними системами сімейства Windows і Linux. Можлива робота під іншими ОС, підтримуваними бібліотекою Qt, але необхіднакомпіляція вихідного коду.

Програма написана з використанням класів об'єктів. Найбільш важливий клас – Koder відповідає за вбудовування повідомлень у поступаючі контейнери.

Keys – клас доступу до статичних об'єктів ключів кодування/декодування. Клієнтська частина програми складається з наступних модулів: «Авторизаційна інформація», «Відео дані», «Список контактів». Модуль «Авторизаційна інформація» містить у собі кнопку «Авторизація», поле введення пароля. Модуль «Відео дані» містить у собі вікно «Відео». Модуль «Список контактів» містить у собі вікно «Контакти».

Клієнтська частина запускається як служба, надаючи мінімальний набір можливостей: пройти процедуру авторизації й брати участь у відеоконференції. Користувач не бачить процесу вбудовування міток і авторизаційної інформації у відеопотік, усі перетворення програма робить на рівні пакетів самостійно. Для здійснення доступу до відеоконференції користувачеві необхідно мати:

- веб-камеру й доступ у мережу для організації сеансу відео-конференц зв’язку;
- установлену програму «Мітка привілеїв»;
- пароль або апаратний ключ із авторизаційною інформацією;
- веб-камеру й доступ у мережу для організації сеансу відео-конференц зв’язку.

Серверна частина призначена для адміністратора. Адміністратор вручну додає IP-адреси привілейованих користувачів і призначає мітки привілеїв (напроти привілейованої адреси ставиться оцінка).

Конфігурація сервера завдається в текстовому файлі, а сам сервер запускається як консольний додаток. Адміністратор вручну виконує наступні дії: уведення Ір-адрес користувачів відеоконференції; налаштування привілеїв; перше налаштування апаратних ключів.

Перед початком спеціального режиму, адміністратор запускає службу на сервері – на початковому етапі роботи програми створюється дуплексний канал (сокет), що з'єднує два процеси – відправлення й передачі даних. Режими «джерело-сервер» і «сервер-адресат». Відправлення повідомлень відбувається в такий спосіб: у пакет додається інформація про ко ристувача й мітка привілеї(при необхідності – мітка початку спеціального режиму й мітка останнього спеціального пакета), а також авторизаційна інформація. Пакет відсилається, згідно з таблицею стеганографічних перетворень виділяються пакети з авторизаційною інформацією.

Програма дозволяє створити сокет: сервер очікує підключення клієнта, клієнти підключаються до сервера. У програмі самостійно формуються TCP пакети, реалізована можливість додавання в поле «Опції» TCP заголовка спеціалізованих міток. Надалі планується доробити користувацький інтерфейс.

Удосконалений продукт має включати апаратну частину, представлену у вигляді апаратних ключів.

4.3 Використання єдиного серверу

Робота мережі з єдиним сервером представлено на рисунку 4.1.

Встановлені клієнтська й серверна частини додатка Пакети від другого комп'ютера не доходять до адресата (комп'ютера №3), тому що вони не мають у службовім полі мітки. Пакети від першого комп'ютера доставляються. З пакетів, що містять стегоконтейнер и, відновлюється авторізаційна інформація, відповідальна за забезпечення надійності системи відео-конференц зв’язку. Усі інформаційні потоки йдуть через сервер, на якім установлена серверна частина додатка.

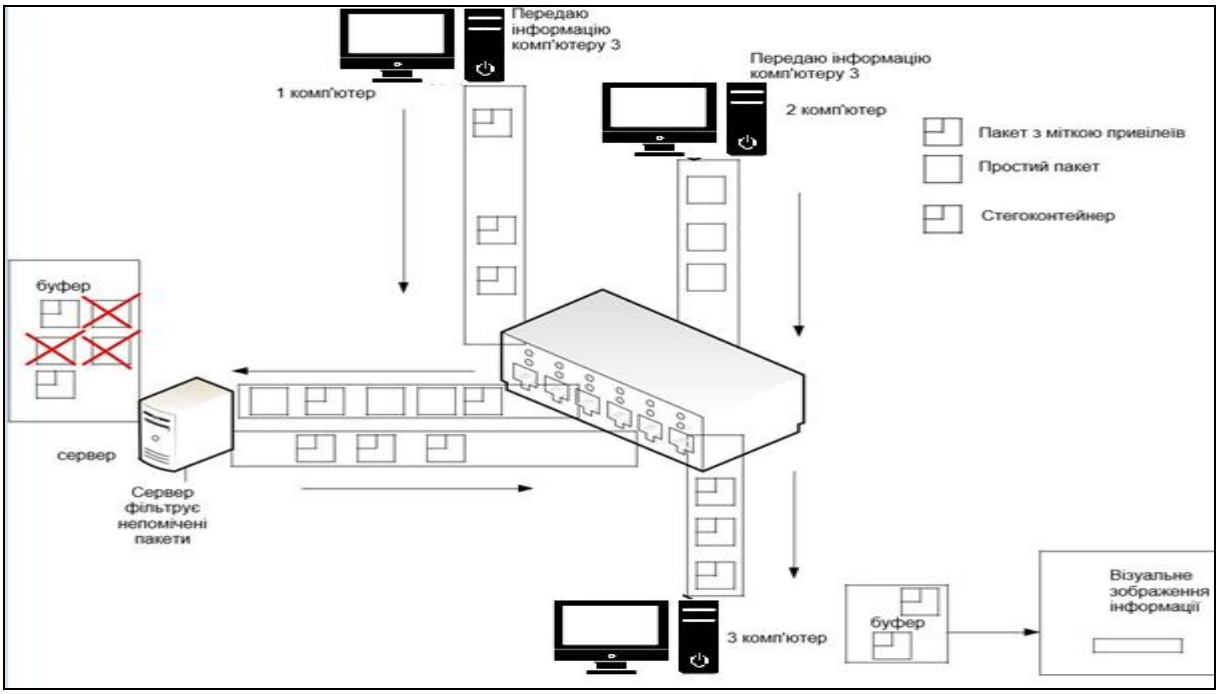

Рисунок 4.1 – Робота мережі з єдиним сервером у спеціальному режимі

Програма може бути використана для проведення нарад, закритих освітніх конференцій, оперативному зв'язку із працівниками філій великих компаній і в багатьох інших сферах діяльності, що вимагають надійної відео-конференц зв’язку.

5 ОПИС МОЖЛИВОСТІ ВИКОРИСТАННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

5.1 Порівняння алгоритму з існуючими рішеннями

Необхідно провести оцінка ефективності запропонованого автором методу підвищення надійності ВКЗ. Наведені моделі стандартного й спеціального режимів алгоритму керування доступом – алгоритму керування навантаженням мережі «Мітка привілеїв», призначені для проведення експериментальної оцінки ефективності застосування комп'ютерного методу підвищення надійності ВКЗ для авторизованих користувачів з гарантованою доставкою повідомлень. Експериментальна оцінка проводиться за допомогою розробленого автором програмного забезпечення, результатом роботи якого є таблиці й графіки, призначені для визначення ефективності застосування алгоритму «Мітка привілеїв» у системі ВКЗ із заданими параметрами.

Пропонований комп'ютерний метод підвищення надійності відео-конференц зв’язку порівнюється з існуючими технологіями керування навантаженням мережі, результати аналізу представлено в таблиці 5.1. У роботі були обрані Windows Network Balancing, Qos, VPN і NAT. Варто відзначити, що на сьогоднішній день відсутні повні аналоги запропонованого комп'ютерного методу підвищення надійності відео-конференц зв’язку, обрані для порівняння технології мають частину функціонала запропонованого комп'ютерного методу. Розглянуто порівняння алгоритму керування навантаженням мережі «Мітка привілеїв» з технологією Qos. На відміну від алгоритму керування навантаженням мережі «Мітка привілеїв» ця технологія не дозволяє призначати привілеї кожному користувачеві, а також вимагає підтримки з боку мережного встаткування. У технології Qos реалізований поділ по виду трафіка: в окремий клас виділяється трафік, призначений для керування мережею, голосові дані, відео трафік, трафік, критичний по втратах, а також звичайний трафік.

В алгоритмі керування навантаженням мережі «Мітка привілеїв» розглядається поділ не по виду трафіка, а по користувачах, привілеї встановлюються виходячи з необхідного рівня ймовірності одержання доступу до інформаційних ресурсів системи відео-конференц зв’язку.

Таблиця 5.1 – Порівняння технологій

№	Технологія	Характеристики	Розроблений алгоритм
1	Windows Network Balancing	1. Використовуються пріоритети вузлів, які призначаються адміністратором. 2. Пріоритети призначаються серверам у кластері.	Привілеї призначаються клієнтам системи відео-конференц зв'язку.
2	Qos	1. Пріоретизація трафіка. 2. Застосовуються спеціалізовані протоколи. 3. Залежність технології Qos від мережного встаткування. 4. Пріоритети в Qos по типу трафіка. 5. Різна організація черг.	1. Пріоретизація клієнтів. 2. Зміни вносяться в поля TCP пакета. 3. Не залежить від устаткування, усі перетворення виконуються програмою. 4. Черга організована привілеїв клієнтів.
3	VPN	1. Відбувається захищене з'єднання з довіреними вузлами. 2. Застосовується шифрування. 3. Застосовуються спеціалізовані протоколи.	1.Доступ до інформаційних ресурсів системи відео-конференц зв'язку одержують клієнти із привілеями. 2. Для передачі авторизаційної інформації в тілі TCP пакета застосовуються методи стеганографії. 3.Модифікації відбуваються на рівні протоколу TCP.
4	NAT	Перенапрямок усього трафіка на одну адресу.	Увесь трафік перенаправляється з сервера за особливим алгоритмом. IP-адреси зберігаються.

Для реалізації технологій балансування навантаження застосовуються спеціалізовані протоколи: RSVP (Resource Reservation Protocol) – для інтегральної моделі й MPLS (Multiprotocol Label Switching) – для диференційованої. Протокол RSVP призначений для резервування мережних ресурсів. Протокол MPLS є протоколом другого з половиною рівня (канального й мережного), являє собою механізм передачі даних, який проводить емуляцію різних властивостей

мереж з комутацією каналів. Обидва ці протоколи є практичною реалізацією технології Qos. Відмінність алгоритму «Мітка привілеїв» полягає у відсутності необхідності використання додаткових протоколів. Усі зміни реалізовані безпосередньо із самим пакетом даних. Обробка проводиться не маршрутизаторами, а сервером із установленим програмним засобом проведення захищених відеоконференцій «Мітка привілеїв».

Також слід зазначити відмінність між Qos технологією й алгоритмом керування навантаженням мережі «Мітка привілеїв» в організації черг. У реалізації Qos використовується WFQ (Weighted Fair Queuing) WRED (Weighted Random Early Detection). Перший алгоритм регулює частку кожної черги в загальному потоці. Другий алгоритм дозволяє регулювати довжину черги, виходячи з її пріоритету. В алгоритмі «Мітка привілеїв» черга організована у такий спосіб: з появою пакетів з мітками привілеїв, інші пакети відхиляються.

5.2 Порівняння програмного засобу

Особливістю програмного засобу проведення захищених відеоконференцій «Мітка привілеїв» є організація виділеного логічного каналу за допомогою міток привілеїв з використанням стеганографічних методів. Розглянуто існуючі програмні продукти.

MSU Stego video – дозволяє вбудовувати будь-який файл в відеопослідовність, використовуються спеціалізовані кодеки для перетворення кадра, виправлення виникаючих помилок проводиться методами завадостійкого кодування. Переваги: слабко спотворює відео при вбудовуванні файлу, можливий витяг інформації навіть після стиску з відносно низьким бітрейтом, інформація захищається паролем. Недоліки: відсутня можливість вбудовування стегоконтейнеров у реальному часі, працює тільки з файлами, а не з потоком; відсутня можливість організації виділеного логічного каналу передачі інформації, відсутні додаткові механізми аутентифікації.

Steghide дозволяє приховувати дані усередині графічних, звукових і відео файлів, а так стискати й шифрувати різними криптоалгоритмами перед

прихованням. Приховувані дані так само захищаються контрольною сумою, що дозволяє перевірити їхня цілісність За замовчуванням використовується крипто алгоритм Advanced encryption standard (далі AES). Переваги – можливість шифрування до вбудовування стегоконтейнеров. Недоліки: відсутня можливість вбудовування стегоконтейнеров у реальному часі, працює тільки з файлами, а не з потоком, відсутня можливість організації виділеного логічного каналу передачі інформації, відсутні механізми аутентифікації.

Stegtunnel забезпечує схований канал на основі сеансу зв'язки TCP. Включає додаткову інформацію в службові поля пакетів. Переваги – дозволяє вбудовувати інформацію в реальному часі. Недоліки: працює тільки під Linux; не має графічного інтерфейсу.

Надійність відео-конференц зв’язку при використанні програмного засобу проведення захищених відеоконференцій «Мітка привілеїв» забезпечується наступними засобами:

- у конференції можуть брати участь тільки користувачі, дані від яких приходять зі спеціальними мітками в службових полях пакетів TCP;
- Ір-адреси легітимних користувачів задаються адміністратором у серверній частині додатка, що розроблений;
- авторизаційна інформація вбудовується стенографічними методами;
- для доступу до відео-конференц зв’язку необхідно ввести пароль, надалі апаратний ключ.

5.3 Експериментальна оцінка ефективності методу підвищення надійності ВКЗ

Під час проведення сеансу відео-конференц зв’язку кількість серверів уважається незмінною $n=Const$, тоді імовірність відмови залежить тільки від кількості клієнтів у системи: k_{total} – загальна кількість клієнтів для стандартного режиму, k_{spec} – загальна кількість клієнтів для спеціального режиму (табл. 5.2).

Таблиця 5.2 – Порівняння стандартного й спеціального режимів

№	Характеристика	Стандартний режим	Спеціальний режим
1	Принцип роботи	Обмін пакетами між клієнтами здійснюється через будь-який сервер.	Клієнт передає інформацію серверу, за яким закріплений, одержуєінформацію від будь-якого сервера.
2	Час передачі пакета	Час передачі пакета залежить від того, як швидко знайдеться вільний сервер.	Час передачі пакета для привілейованого клієнта мінімальне, стабільне й прогнозоване.
3	Відмови	Пакети клієнтів відхиляються, якщо всі сервери зайняті.	Пакети привілейованих клієнтів ухвалюються, інші відхиляються.
4	Час зв'язку з сервером	Визначається загальним кількістю клієнтів.	Визначається кількістю клієнтів, закріплених за серверами.
5	Система масового обслуговування, що імітує режим	Система масового обслуговування з обмеженою за часом чергою.	Система масового обслуговування з обмеженою за часом чергою для клієнтів з привілеями й відмовами для клієнтів без привілеїв.

Оцінка ефективності застосування алгоритму керування навантаженням мережі «Мітка привілеїв» виконується за допомогою порівняння ймовірностей відмови системи відео-конференц зв’язку із заданими параметрами в стандартному й спеціальному режимах (формула 5.1):

$$P\left(k_{total}, k_{spec}\right) = P_{n+m} - P_m \qquad (5.1)$$

Спеціальний режим вважається ефективним, коли для коефіцієнта ефективності вірна нерівність $P(ktotal, k_{spec}) > 0$. На практиці часто вирішується зворотне завдання: визначити *ktotal* і *kspec* при бажаному рівні $P(ktotal, k_{spec})$, для цієї мети використовується програмне забезпечення, розроблене авторами. На вхід

програмного забезпечення для оцінки ефективності алгоритму керування навантаженням мережі «Мітка привілеїв» подаються наступні параметри: середня інтенсивність вступу пакетів; швидкість обробки запитів сервером; довжина черги; коефіцієнт наповнення черги; максимум серверів і клієнтів. На виході програмне забезпечення видає графік у трьох координатах. При заданому рівні за графіком визначаються ktotal і kspec. На рисунку 5.1 наведений графік, що відображає доцільність використання спеціального режиму в системі відео-конференц зв'язку, з наступними параметрами.

Відношення інтенсивності вступу пакетів від одного клієнта до інтенсивності обробки пакетів сервером (формула 5.2).

$$\rho = \lambda_1 / \mu = 1/16 \tag{5.2}$$

Відношення завдане з міркувань співвідношення кількості ядер процесорів для персонального комп'ютера й обчислювального сервера, при цьому: $n = 5$ – кількість серверів у системі, $m = \rho^{-1} = 16$ – середня довжина чергисервера, $K = 200$ – загальна кількість клієнтів у системі/

Із графіка на рисунку 5.1 можна побачити, яка кількість клієнтів у стандартному або спеціальному режимі забезпечує необхідний рівень надійності системи відео-конференц зв'язку.

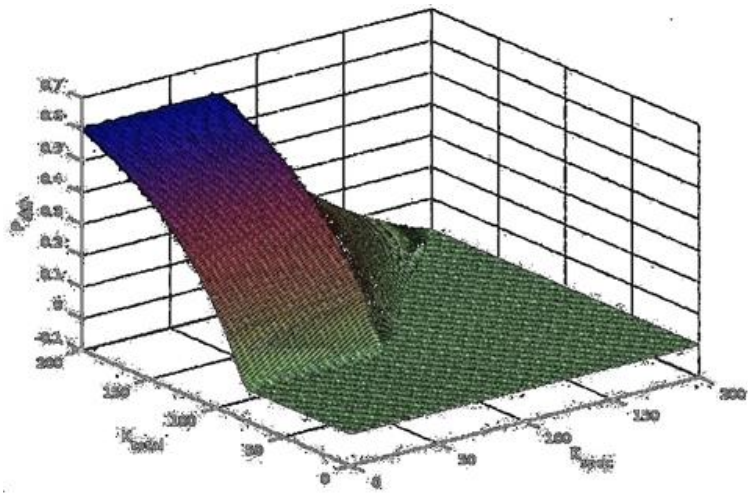

Рисунок 5.1 – Графік $P(k_{total}, k_{spec})$ при n = 5

У якості коефіцієнта ефективності алгоритму керування навантаженням мережі «Мітка привілеїв» використовується різниця ймовірностей відмови системи відео-конференц зв'язку з заданими параметрами в стандартному й спеціальномурежимах P (k_{total}, k_{spec}).

На рисунку 5.2 представлений графік залежності максимально можливої кількості спеціальних клієнтів при заздалегідь заданій загальній кількості Клієнтів і заданому рівні P (ктотαλ, *kspec*) за умови P(*ktotal*, *kspec*) > 0,2 .

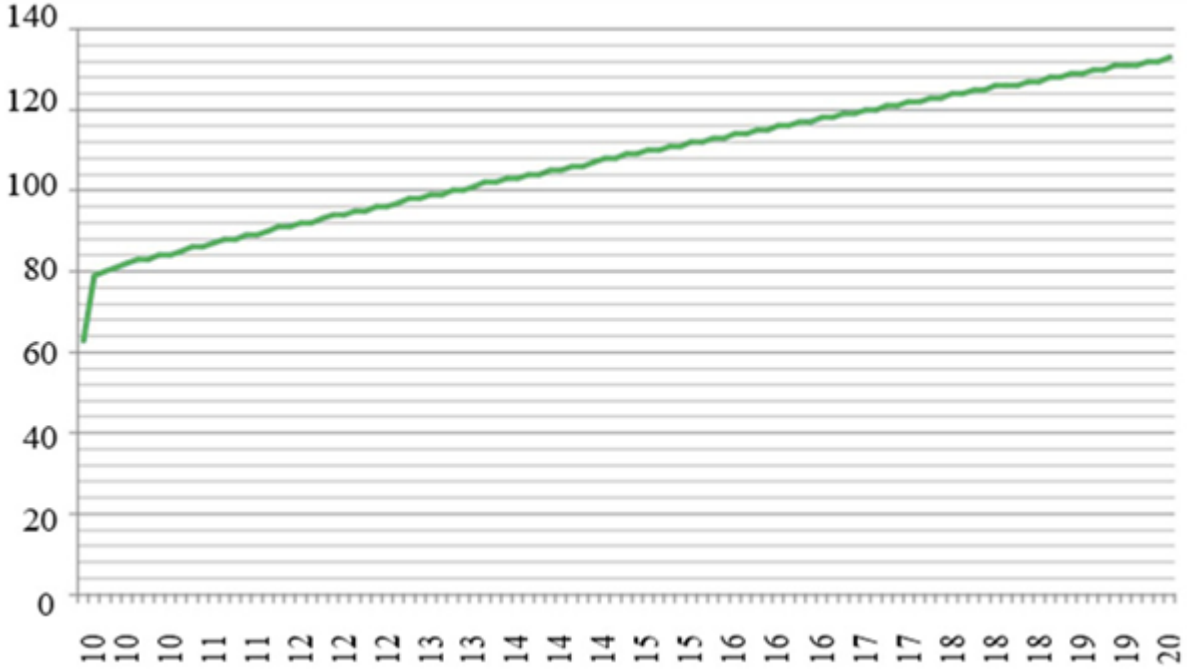

Рисунок 5.2 – Графік k_{spec} при P (k_{total}, k_{spec}) >0.2

Якщо кількість спеціальних клієнтів у системі відео-конференц зв'язку менше максимально можливого, застосування алгоритму «Мітка привілеїв» уважаєтьсядоцільним при заданому P (k_{total}, k_{spec}) [50].

В таблиці 5.2 наведено розрахунки для 6 серверів, 100 клієнтів (10 з них мають мітки привілеїв). Імовірність відмови в одержанні доступу для спеціального режиму в цьому випадку набагато нижче, чим імовірність відмови в одержанні доступу в стандартному режимі. З таблиці 5.2 випливає, що ймовірність відмови при застосуванні алгоритму керування доступом зменшилася в 6 разів, імовірність порожньої черги збільшилася в 11, 542 рази.

З таблиці 5.3 видно, що при кількості привілейованих клієнтів 25 з 100

імовірність відмов в обох випадках приблизно однакова.

Таблиця 5.2 – Розрахунки для 10 клієнтів із привілеями (6 серверів)

Вихідні дані	Пояснення	Одиниці виміру	Значення
λ	Інтенсивність пакетів від одного клієнта	пакетів у секунду	100
μ	Інтенсивність обробки одним сервером	пакетів у секунду	4000
n	Кількість серверів	одиниця	6
m	Довжина черги сервера	одиниця	1
k	Кількість клієнтів	одиниця	100
Стандартний режим			
Λ	Сумарна інтенсивність від клієнтів	пакетів у секунду	10000
$^{P}0$	Імовірність порожньої черги	-	0,083

При подальшому збільшенні кількості клієнтів імовірність відмови в одержанні доступу до інформаційних ресурсів у спеціальному режимі стає вище, чим імовірність відмови в одержанні доступу у звичайному режимі. У таблиці 5.4 представлено розрахунки для 50 клієнтів. З розрахунків видно, що при такому співвідношенні клієнтів із привілеями й клієнтів без привілеїв застосування алгоритму керування навантаженням мережі «Мітка привілеїв» недоцільно, тому що ймовірність відмови в одержанні доступу в спеціальному режимі вище, чим у стандартному.

Таблиця 5.3 – Розрахунки для 25 клієнтів із привілеями (6 серверів)

Вихідні дані	Пояснення	Одиниці виміру	Значення
λ	Інтенсивність пакетів від одного клієнта	пакетів у секунду	100
μ	Інтенсивність обробки одним сервером	пакетів у секунду	4000
n	Кількість серверів	одиниця	6
m	Довжина черги сервера	одиниця	1
k	Кількість клієнтів	одиниця	100
Звичайний режим			
Λ	Сумарна інтенсивність від клієнтів	пакетів у секунду	10000
$P_{отк}$	Імовірність відмови	-	0,012
Спеціальний			

режим			
K	Кількість особливих клієнтів	одиниця	25
1	Інтенсивність пакетів на сервері	пакетів у секунду	416,667
$P_{отк}$	Імовірність відмови	-	0,010

Таблиця 5.4 – Розрахунки для 50 клієнтів із привілеями (6 серверів)

Вихідні дані	Пояснення	Одиниці виміру	Значення
λ	Інтенсивність пакетів від одного клієнта	пакетів у секунду	100
μ	Інтенсивність обробки одним сервером	пакетів у секунду	4000
n	Кількість серверів	одиниця	6
m	Довжина черги сервера	одиниця	1
k	Кількість клієнтів	одиниця	100
Стандартний режим			
Λ	Сумарна інтенсивність від клієнтів	пакетів у секунду	10000
P $P_{отк}$	Імовірність порожньої черги Імовірність відмови	- -	0,083 0,012
Спеціальний режим			
K	Кількість особливих клієнтів	одиниця	50
k_1	Кількість клієнтів на сервер	одиниця	8,333
Λ_1	Інтенсивність пакетів на сервер	пакетів у секунду	833,333
P_0	Імовірність порожньої черги	-	0,799
$P_{отк}$	Імовірність відмови	-	0,035

На рисунку 5.3 представлені графіки залежності відносини для різної кількостісерверів (від 1 до 10) при завданому значенні (формули 5.3, 5.4)

$$P(k_{total}, k_{spec}) > 0{,}1, \tag{5.3}$$

$$k_{spec} / k_{total} \to 0{,}9. \tag{5.4}$$

За результатами експериментів, було визначене співвідношення (формула 5.5):

$$kspec\ /\ ktotal \to 1 - P(ktotal, kspec\ ) \quad (5.3)$$

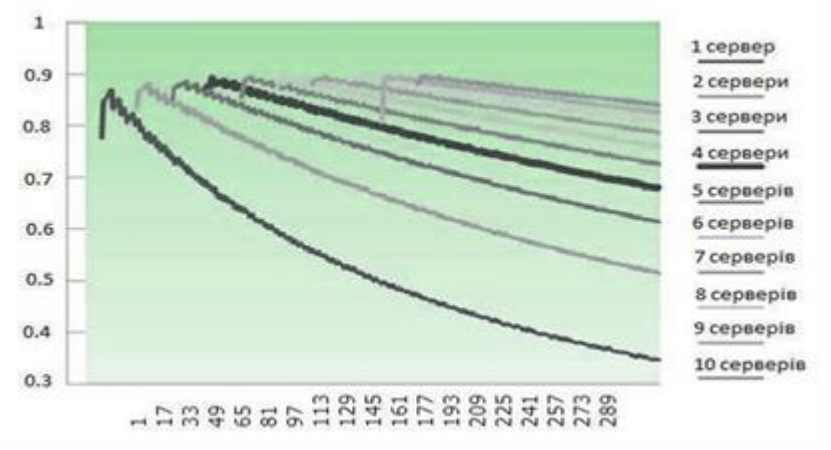

Рисунок 5.3 – Графік залежності $^{kspec}/_{ktotal}$ при $P(k_{total}, k_{spec}) > 0{,}1$

Відношення $^{kspec}/_{ktotal}$ показує максимально можливу частку клієнтів з привілеями для підвищення ймовірності доступу на необхідну величину. З ростом кількості серверів значення $^{kspec}/_{ktotal}$ зростає.

ВИСНОВКИ

В роботі розроблений алгоритм керування навантаженням мережі «Мітка привілеїв», реалізований у вигляді програмного засобу «Мітка привілеїв» . Представлений опис алгоритму, докладно розглянутий спеціальний режим, що складається із трьох етапів: підготовка, безпосередньо спеціальний режим і завершення роботи. Більш докладно розглянутий окремий випадок роботи алгоритму – мережа з єдиним сервером. Розроблений комп'ютерний метод обробки інформації, який, шляхом виділення привілейованого трафіка й оптимізації потоків інформації, дозволяє підвищити надійність системи ВКЗ для авторизованих користувачів з гарантованою доставкою повідомлень і підвищити ймовірність одержання доступу до ресурсів систем відео-конференц зв’язку.

Розроблений алгоритм керування доступом до інформаційних ресурсів, заснований на додаванні міток привілеїв у службове поле пакета зміни маршруту передачі пакетів, що дозволяє підвищити надійності відео-конференц зв’язку для авторизованих користувачів з гарантованою доставкою повідомлень.

Створений програмний засіб проведення захищених відеоконференцій

«Мітка привілеїв», що складається із клієнтської й серверної частин, представлений інтерфейс програми. Окремо розглянута робота програмного засобу в мережі з єдиним сервером для реалізації алгоритму керування доступом інформаційних ресурсів та досліджена його ефективність, підтверджене підвищення ймовірності одержання доступу до інформаційних ресурсів авторизованими користувачами на завдане значення.

Побудовані моделі стандартного й спеціального режимів алгоритму керування доступом – алгоритму керування навантаженням мережі «Мітка привілеїв», призначені для проведення експериментальної оцінки ефективності застосування комп'ютерного методу підвищення надійності ВКЗ для авторизованих користувачів з гарантованою доставкою повідомлень. Експериментальна оцінка проводиться за допомогою розробленого автором програмного забезпечення, результатом роботи якого є таблиці й графіки, призначені для визначення ефективності застосування алгоритму «Мітка

привілеїв» у системі ВКЗ із завданими параметрами.

Представлене порівняння алгоритму керування навантаженням мережі «Мітка привілеїв», а також програмного засобу проведення захищених відеоконференцій «Мітка привілеїв» з існуючими рішеннями.

Визначено, що на сьогоднішній день відсутні повні аналоги як алгоритму керування навантаженням мережі «Мітка привілеїв», так і програмного засобу, що реалізує даний алгоритм.

За результатами досліджень опубліковано тези доповіді

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЯ

1. Wang, D. Red5 Flash Server Analysis and Video Call Service Implementation [Text] / Dongjin Wang, Ke Xu; Beijing University of Posts and Telecommunications // IEEE 2nd Symposium. – Beijing, China : Web Society (SWS), 2010. – Issue 08

2. IEEE Standard for Local and metropolitan area networks. Virtual Bridged Local Area Networks [Electronic resource] : ANSI/IEEE 802.1Q-2005 / IEEE Standards Association; ANSI. – cor. 1 : Corrections to the Multiple Registration Protocol. – New York, USA, 2008. – Access mode: http://standards.ieee.org/findstds/standard/802.1Q-2005.html (15.12.2018).

3. Cauich E. Data Hiding in Identification and Offset IP fields [Electronic resource] / E. Cauich, R. Gómez, R. Watanabe // International Symposium and School on Advanced Distributed Systems : symposium papers. – Guadalajara, Mexico, 2005. – 118-125. – Access mode: http://www.sciweavers.org/read/data-hiding- inidentification-and-offset-ip-fields-124683 (25.12.2018).

4. Changguang, W. Study of Video Applications Based on IP Technology / Wang Changguang, Hou Weihong // Computer & Digital Engineering. – 2005. – 08. – Access mode: http://en.cnki.com.cn/Article_en/CJFD TOTAL-JSSG200508017.htm (25.12.2018).

5. Chen, J. Schemes and Comparisous of Documents Sharing in Video Conference System / Chen Jing-yan, [etc.] // Journal of Jilin University : Information Science Edition. – Changchun : Jilin University Press, 2006. – Issue 03.

6. Donoho D.L., Maleki A., Shahram M., Stodden V., Ur-Rahman I. Fifteen years of reproducible research in computational harmonic analysis // Comput. Sci. Eng. 11 (2016), 8-18.

7. Kutyniok G., Lim W.-Q. Image Separation using Wavelets and Shearlets, preprint, 2016.

8. Guo K., Labate D., W.-Q Lim, Edge analysis and identification using the Continuous Shearlet Transform // Appl. Comput. Harmon. Anal. 27 (2014), 24- 46.

9. Alan Griffiths, H. Claire Luckhurst, and Peter Willett. Using Interdocument

Similarity Information in Document Retrieval Systems. Department of Information Studies, University of Sheffield, Western Bank, Sheffield S10 2TN, United Kingdom. Information Retrieval 1997 p.365-373.

10. Artale A., Franconi E., Guarino N., Pazzi L. Part-Whole Relations in Object-Centered Systems: An Overview // Data and Knowledge Engineering. 1996. V.20. P. 347-383.

11. Whissell John S., Clarke Charles L.A. Improving document clustering using Okapi BM25 feature weighting. Information retrieval. 2011. T. 14, № 5, pp. 513-523.

12. Fouad M. Data mining and fusion techniques for Wsns as a source of the big data / M.M. Fouad, N.E. Oweis, T. Gaber, M. Ahmed, V. Snasel // Procedia Computer Science. – Elsevier, 2015. – Vol.65. – P. 778-786.

13. Methods of multidimensional classification in problems of linguistic localization / Shubin I., Kozyriev A. // Proceedings of the III International Conference "Innovative Technologies in Science and Education". November 14, 2019 in Amsterdam, The Netherlands, 2019. pp 398-402

14. Beloborodov A., Kuznetsov A., Braslavski P. Characterizing Health-Related Community Question Answering // Proc. of the 35th European Conf. on IR research (ECIR'13): LNCS.. Vol. 7814. 2020. , P. 680-683.

15. Beloborodov A., Braslavski P., Driker M. Towards Automatic Evaluation of Health-Related CQA Data // Proc. of the 5th International Conf. of the CLEF Initiative (CLEF'14): LNCS. - Sheeld, UK. Vol. 8685. 2020. , P. 7-18.

16. Sieg A., Mobasher B., Burke R. Inferring User's Information Context from User Pro les and Concept Hierarchies // Classification, Clustering, and Data Mining Applications. | 2019., | P. 563-573.

17. Chirita P., Firan C., Nejdl W. Personalized Query Expansion for theWeb // Proceedings of SIGIR'07 Conference. | 2017. | P. 7-14.

18. Speretta M., Gauch S. Personalized Search Based on User Search Histories // Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence. - 2019 . P. 622-628.

19. Chetverikov G., Puzik O., Vechirska I. Multiple-valued structures of

intellectual systems //Proceedings of the with Internations Computer Sciences and Information Technologies (CSIT). 2016, 7589907. -pp. 204-207

20. M.F. Bondarenko, Z.V. Dudar, N.T. Protsay, V.V. Cherkashyn, V.A. Chykyna, Y.P. Shabanov-Kushnarenko, “Algebra of predicates and predicate operations” Radio electronics and informatics, no. 1, 2004, pp. 5-22.

21. The protégé project// Stanford, California, - 2000-2014. http://protege.stanford.edu/index.html.

22. O. Lassila. The XML Family of Specifications: A Practical Guide// Addison-Wesley, - 2018. http://shop.barnesandnoble.com/booksearch/ isbninquiry.asp?isbn=0201703599

23. Semantic Web Development // World Wide Web Consortium, - January 2000. http://www.w3.org/2000/01/sw/

24. Semantic Web // World Wide Web Consortium, - September 2016. http://www.w3.org/2016/sw/.

25. Naming and Addressing: Uris, Urls // World Wide Web Consortium, - October 2013. http://www.w3.org/Addressing/

26. G.G. Chetverikov, I.D. Vechirska, S.S.Tanyanskiy, “The methods of algebra finite predicates in the intellectual system of complex calculations of telecommunication companies,” International Conference Proceedings Crimean Microwave and Telecommunication Technology (CriMiCo), 6959425, 2014, pp.

27. Shubin, I., Snisar, S., Zhyrnov, V., Slavhorodskyi, V.// Practical Application of Formal Representation of Information for Intelligent Radar Systems 2018 International Scientific-Practical Conference on Problems of Infocommunications Science and Technology, PIC S and T 2018 - Proceedings, 2019, pp. 433-436, 8632103

28. DTD for XML Schema // World Wide Web Consortium, - August 2002. http://www.w3.org/TR/xmlschema-1/#nonnormative-schemadtd

29. XSL Transformations (XSLT), W3C Recommendation // World Wide Web Consortium, - November 1999. http://www.w3.org/TR/1999/ Rec-xslt-19991116.

30. Resource Description Framework (RDF) Model and Syntax Specification, W3C Recommendation // World Wide Web Consortium, – February 1999.

http://www.w3.org/TR/2019/Rec-rdf-syntax-19990222/.

31. Web Ontology // World Wide Web Consortium, – March 2014. http://www.w3.org/Help/siteindex.html#webont.

32. Дудар З.В., Склярук Д.О. Дослідження алгоритмів підвищення надійності відео зв’язку / Информационные системы и технологии (ИСТ-2018): материалы 7-й Международ. Науч.-техн. конф., Харьков-Коблево, 10-15 сентября 2018, – тезисы докладов. – Х.: ХНУРЕ, 2018