УДК 621.391

М. В. Васильківський, О. В. Ремінський, О. В. Попов
(Україна, Вінниця, Вінницький національний технічний університет)

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОГО ЗАХИСТУ СИСТЕМ ВІДЕОЗВ'ЯЗКУ

Анотація. Представлений огляд існуючих способів підвищення надійності системи відеоконференцзв'язку для авторизованих користувачів з гарантованою доставкою повідомлень шляхом підвищення вірогідності отримання доступу до ресурсів систем широкосмугового спецзв'язку.

Ключові слова: відеоконференцзв'язок, відеотрафік, канал зв'язку, стеганографія.

Abstract. The review of the existing methods of increasing the reliability of the video conferencing system for authorized users with guaranteed message delivery by increasing the probability of gaining access to the resources of broadband special communication systems is presented.

Keywords: video conferencing, video traffic, communication channel, steganography.

Вступ

Системи відеоконференцзв'язку активно використовуються для роботи над спільними проектами, у тому числі в ракетно-космічній галузі для організації зв'язку між віддаленими станціями. Відео-трафік має певні особливості: вимагає значної пропускної спроможності каналу, мінімізації часу доставки відеокадрів до одержувача, регулярного характеру затримок між повідомленнями (пакетами). У сферах застосування систем відеоконференцзв'язку, пов'язаних з точними операціями, важливо підтримувати заданий рівень надійності [1].

Одним з перспективних рішень проблеми забезпечення надійності систем відеоконференцзв'язку на сьогодні є використання технологій розподілу навантаження інфокомунікаційної мережі.

Метою роботи є підвищення надійності систем відеоконференцзв'язку.

Алгоритми підвищення надійності відеоконференцзв'язку

Для організації надійного каналу зв'язку застосовують наступні методи: виділені лінії зв'язку на фізичному рівні і логічні канали зв'язку. Фізичний захист каналу - екранування кабелю і розташування ліній зв'язку у важко доступному місці. Логічний захист каналу - шифрування і стеганографія. Кожен з приведених методів має свої недоліки та переваги. Перевагою виділених ліній є ізоляція потоків даних на фізичному рівні, що обумовлює необхідність захисту каналу тільки від підключення в розрив та побічних

електромагнітних випромінювань та наведень. Недоліком виділених ліній є порівняно висока собівартість та неможливість застосування для організації віддаленого доступу.

Одним із способів організації захищеного (надійного) каналу є автентифікація шляхом з'ясування координат користувача. Користувач відправляє координати супутників, що знаходяться в зоні прямої видимості. На сервері автентифікації зберігаються орбіти усіх супутників, що дозволяє з високою точністю визначити легітимність користувача, знаючи його істинне географічне положення. Підробка координат досить ускладнена коливаннями орбіт. Недоліком цього методу є необхідність безперервної відправки координат і наявність спеціалізованого апаратного модуля [2].

Основними методами підвищення надійності систем відеоконференцзв'язку на сьогодні є: застосування маршрутизації для оптимального і раціонального використання канального ресурсу системи; використання алгоритмів децентралізованих самоорганізованих мереж, які дозволяють розподілити навантаження на усі елементи пропорційно їх ресурсам і характеристикам, тим самим збільшуючи масштабованість та зменшуючи вартість такого рішення за відсутності необхідності підтримки протоколів прикладного рівня на мережевому обладнанні; застосування механізмів динамічного перерозподілу швидкості передачі інформації при спільному обслуговуванні трафіку сервісів реального часу і трафіку даних, що допускає затримку [3].

Висновок

Оптимальний розподіл мережевого навантаження дозволяє забезпечувати задані характеристики відеоконференцзв'язку за рахунок керування інформаційними потоками.

Література

1. Власкин, А. Видеоконференцсвязь: прошлое, настоящее, будущее [Текст] // Интернет журнал по широкополосным сетям и мультимедийным технологиям. – Владивосток: ТОВВМУ, 2015. –[б. н.]. – С. 92.

2. Лебедева, К. Е. Методика повышения надежности видеоконференцсвязи / К. Е. Лебедева, Р. В. Лебедев, А. В. Мурыгин // Сибирский журнал науки и технологий: СибГАУ, – 2017. – № 2, т. 18. – С. 274-282.

3. Лебедева, К. Е. Угрозы безопасности систем видео-конференц-связи [Текст] / К. Е. Лебедева, Р. В. Лебедев // Управление риском. – М.: Анкил, 2015. – № 2. – С. 25-28.