

УДК 004.032.6:654(043.2)

ІНФРАСТРУКТУРА МУЛЬТИМЕДІЙНИХ СИСТЕМ ЗАХИЩЕНОГО КОНФЕРЕНЦ ЗВ'ЯЗКУ

Матвійчук-Юдін О.О., здобувач вищої освіти 4 курсу

Національний Авіаційний університет м.Київ

Науковий керівник – Одарченко Р.С., д.т.н., проф., зав.кафедри ТРС

***Анотація.** В роботі надано визначення поняття інфраструктури мультимедійних систем захищеного конференц зв'язку. Описано базові складники інфраструктури системи для забезпечення безпеки та конфіденційності комунікацій, що представляє собою складну систему, спроектовану для забезпечення безпеки, ефективності мультимедійних заходів та обміну інформацією в умовах конфіденційності.*

***Ключові слова:** мультимедійні системи, захищеність каналів зв'язку, інформаційні потоки даних.*

В епоху швидкого розвитку цифрових технологій та зростаючої потреби в обміні інформацією, забезпечення безпеки та конфіденційності стає основним завданням. Це стосується особливо сфер, де регулярно обговорюється чутлива інформація, - це урядові установи, корпорації, оборонні структури та інші.

Інфраструктура мультимедійних систем захищеного конференц зв'язку (МСЗК) є ключовим компонентом для забезпечення безпеки та конфіденційності комунікацій, що представляє собою складну систему, спроектовану для забезпечення безпеки, ефективності мультимедійних конференцій та обміну інформацією в умовах конфіденційності [1]. Така інфраструктура має ряд компонентів і функцій, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації під час комунікації. Основними аспектами інфраструктури МСЗК є: захищена мережа, аутентифікація та авторизація, шифрування даних, керування ключами, захист від атак, інтеграція з іншими системами (відеоконференції, системи управління доступом і системи моніторингу безпеки), аудит та журналювання,

інструкції та навчання користувачів, резервне копіювання та відновлення, регулювання та відповідність (зберігання та обробки інформації, захист персональних даних)

Загальною метою інфраструктури МСЗК є забезпечення безпеки і конфіденційності комунікацій і інформації під час мультимедійних конференцій, особливо в чутливих сферах, таких як урядові установи, оборонні сектори та фінансові організації.

Розглянемо основні складові архітектури мультимедійних систем: засоби аутентифікації (паролі, біометричні дані (відбитки пальців, розпізнавання обличчя), смарт-карти тощо.); захист аудіо та відео потоків (шифрування даних, аудіо- та відеопотоків, захист від запису та перехоплення) [2]; конфіденційність голосового обміну (спеціалізовані алгоритми обробки сигналу для захисту голосових даних в реальному часі); захист від програмного та апаратного зламу від можливого внутрішнього, зовнішнього програмного та апаратного зламу); масштабованість і надійність (забезпечення випадку виникнення помилок при великій кількості одночасних користувачів); інтегровані інструменти аналізу та моніторингу (виявлення підозрілу діяльність та порушення безпеки); запасні копії і відновлення даних (створення резервних копій даних та можливості їх швидкого відновлення); інтеграція з різними пристроями і платформами (комп'ютери, мобільні пристрої, системи відеоконференцій тощо); захист від соціального інженерінгу; інформаційна гігієна (заборона використання ненадійних мереж і пристроїв для доступу до системи): Загалом, інфраструктура МСЗК вимагає інтеграції технологій, процедур та навчання користувачів для забезпечення найвищого рівня безпеки, конфіденційності та доступності у мультимедійних конференціях та спілкуванні.

Інфраструктура МСЗК включає забезпечення вище перелічених заходів такі протоколи та стандарти:

- SIP (Session Initiation Protocol): протокол використовується для ініціації, підтримки та закінчення мультимедійних сесій.

- SRTP (Secure Real-time Transport Protocol): SRTP використовується для шифрування мультимедійних даних в реальному часі під час передачі.

- H.323 та H.264: Стандарти H.323 та H.264 визначають параметри та кодеки для відеоконференцій та аудіоконференцій.

З технологічним ростом можливостей та нововведень важливо долучити до розгляду інфраструктури МСЗК деякі перспективні ключові переваги:

- Штучний інтелект та аналітика: Впровадження інтелектуальних систем аналізу даних і штучного інтелекту може допомогти вчасно виявляти загрози та ідентифікувати аномалії в мережі МСЗК. Машинне навчання може допомогти випереджати кібератаки та реагувати на них швидше.

- Блокчейн-технології: Використання блокчейн-технологій може покращити відстеження та захист від несанкціонованого доступу до обміну даними в МСЗК [3].

- Розвиток кіберфізичних систем: Розширення інфраструктури МСЗК на користь кіберфізичних систем може відкрити нові можливості в сферах, таких як автономні автомобілі, медична діагностика та інші області [4].

- Забезпечення масштабованості та доступності: Зростання обсягу інформації та кількості користувачів потребує стабільної та масштабованої інфраструктури МСЗК, яка б забезпечувала високу якість обслуговування та доступність.

Попри всі переваги МСЗК, їхній розвиток та застосування також постають перед викликами, інфраструктура МСЗК постійно стикається з викликами. Швидкий розвиток технологій означає, що кіберзагрози також стають більш складними та вдосконаленими. Тому інфраструктура МСЗК повинна постійно адаптуватися до нових загроз і вдосконалювати свої заходи безпеки.

Зараз також спостерігається зростання інтересу до квантової криптографії, яка може революціонізувати сферу безпеки. Квантові обчислення можуть вразливими зробити існуючі методи шифрування, і МСЗК повинні готувати плани для впровадження квантової стійкої криптографії.

У майбутньому МСЗК можуть стати все більш важливими для захисту інтернету речей (IoT), мобільних додатків та інших аспектів цифрового життя. Забезпечуючи безпеку та конфіденційність в таких областях, вони відіграють центральну роль у світі, який залишається динамічно зв'язаним та небезпечним

Висновок. Таким чином можна констатувати, що інфраструктура мультимедійних систем захищеного конференц зв'язку відіграє важливу роль у забезпеченні безпеки та конфіденційності комунікацій у світі, де інформація - це ключовий ресурс. Вона дозволяє користувачам вести обговорення, обмінюватися інформацією та вирішувати важливі завдання, знаючи, що їх дані захищені від несанкціонованого доступу та загроз безпеки. Інфраструктура МСЗК - це ключовий елемент у сфері інформаційної безпеки, який допомагає залишати сучасний світ з'єднаним та захищеним.

СПИСОК ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. ER Hassan, M. Tahoun і GS ElTaweel, 2020. A robust DRM computational framework for protecting multimedia content using AES and ECC, *Alexandria Engineering Journal* , vol. 59, № 3. p. 1275–1286
2. Y. Luo, 2019. Development of multimedia broadcast multicast service in LTE together with cognitive radio on TV bands, *International Journal of Electronics Engineering Research* , vol. 11, № 2. P.171–182
3. B Ngabonziza, D Martin, A Bailey 2016 Trustzone explained: Architectural features and use cases. 2016 IEEE 2nd International Conference on Collaboration and Internet Computing p.445-451.
4. De Mi, Joe Eyles, Tero Jokela, Swen Petersen, Roman Odarchenko Demonstrating Immersive Media Delivery on 5G Broadcast and Multicast Testing Networks. *IEEE Transactions on broadcasting*. vol. 66. №2. p.555-570

INFRASTRUCTURE OF MULTIMEDIA SECURE CONFERENCE COMMUNICATION SYSTEMS

Matviichuk-Yudin O.O., student of the 4th year higher education
National Aviation University, Kyiv

Abstract. *The work provides a definition of the concept of the infrastructure of multimedia systems of secure conference communication. The basic components of the infrastructure of the system for ensuring the security and confidentiality of communications are described, which is a complex system designed to ensure the security, effectiveness of multimedia activities and information exchange in conditions of confidentiality*

Keywords: *multimedia systems, security of communication channels, information data flows.*