верификации протоколов когерентности кэш-памяти масштабируемых систем / В. С. Буренков // Вопросы радиоэлектроники. – 2015. – Выпуск 1. – Сер. ЭВТ. – С. 105–116.

2. Буренков В. С. Генератор тестов для верификации протокола когерентности кэш-памяти / В. С. Буренков // Вопросы радиоэлектроники. – 2014. – Выпуск 3. – Сер. ЭВТ. – С. 56–63.

3. Chou C. A Simple Method for Parameterized Verification of Cache Coherence Protocols / Ching-Tsun Chou, Phanindra K. Mannava, Seungjoon Park //Formal Methods in Computer-Aided Design. – Springer Berlin Heidelberg, 2004. – P. 382–398.

Особливості захисту інформаційних ресурсів під час проведення відеоконференцзв'язку

Огнєвий О.В., Огнева А.М., Капустян М.В.
Хмельницький національний університет

На сьогоднішній день технологія відеоконференцзв'язку активно розвивається та впроваджується в Україні, що пов'язано з розвитком міжнародних відносин в суспільстві та з необхідністю оперативного зв'язку між користувачами в країні та по всьому світі. Використання систем відеоконференцзв'язку стало доступним з розвитком сучасних технології та на відміну від голосового зв'язку або електронної пошти, дозволяє отримати різноманітний обсяг інформації, задіяти при спілкуванні текстові та візуальні графічні матеріали: малюнки, таблиці, схеми і діаграми, враховувати вираз обличчя та міміку співрозмовника. Організація відеоконференцзв'язку використовується для проведення переговорів та групових обговорень, в тих випадках, коли у користувачів немає можливості, або це недоцільно, бути присутнім особисто, що дає можливість значної економії засобів і часу.

Розвиток та впровадження інформаційних та телекомунікаційних технологій, збільшення пропускної здатності каналів передачі інформації зробило проведення конференцій, з використанням засобів аудіо та відео зв'язку, зручним засобом спілкування. Сеанси відеозв’язку проводяться для обміну досвідом між різними фахівцями, організації корпоративних нарад, широко використовується для дистанційних занять в освітніх цілях. На сьогодні технології відеозв'язку в основному знаходять застосування в наступних областях: виробнича діяльність (бізнес переговори, спільні проекти), освітні процеси (дистанційне навчання, наукові конференції, семінари), при проведенні судових засідань, для особистих потреб людей (спілкування з родичами і друзями) тощо.

Великою популярністю користуються різні системи для проведення відеоконференцій (ВК) за допомогою глобальних телекомунікаційних мереж.

Найчастіше такі конференції призначені для обмеженого кола користувачів, тому питання захисту інформації в таких системах виходять на передній план. Існує велика кількість таких систем, їх використання пов'язано з підвищеними ризиками, які призводять до виникнення проблем з можливим несанкціонованим доступом, прослуховуванням чи аналізом сигнальної інформації використовуваних протоколів.

В зв’язку із запровадженням карантину в Україні, органи державної влади та місцевого самоврядування, підприємства та організації, особливо ті, що належать до об’єктів критичної інфраструктури, забезпечили роботу своїх працівників в режимі реального часу через мережу Інтернет. Віддалена робота співробітників установи з системами, в яких обробляються державні інформаційні ресурси, інформація з обмеженим доступом, вимога щодо захисту якої визначена законодавчо, повинна відповідати політиці безпеки інформації та вимогам законодавства у сфері захисту інформації.

Відеоконференцзв'язок (ВКЗ) - це телекомунікаційна технологія інтерактивної участі двох і більше віддалених абонентів, при якому між ними відбувається обмін аудіо та відео у режимі реального часу.

Необхідність підтримання інформаційної безпеки автоматизованих систем визначена на державному рівні та спрямована на забезпечення інформаційної безпеки відносин, пов’язаних із збиранням, накопиченням, обробкою та передачею інформації.

Забезпечення захисту інформаційних ресурсів ВКЗ здійснюється шляхом застосування засобів і методів технічного захисту інформації, впровадження організаційних та інженерно-технічних заходів комплексної системи захисту інформації, спрямованих на недопущення блокування інформації, несанкціонованого доступу до неї, її модифікації або спотворення.

Систему ВКЗ прийнято вважати сукупністю наступних елементів: кінцевих вузлів системи - серверів і клієнтів відеоконференцій, та каналів зв'язку, що з’єднують ці вузли. Сервером відеоконференції є комплекс програмно-технічних засобів і систем, що забезпечує управління відеоконференцією, виконання функції ідентифікації і аутентифікації клієнтів, прийому, обробки та перенаправлення даних відеоконференцій. Клієнти представляють собою комплекс програмного і апаратного забезпечення і є джерелом даних системи. Зв'язок клієнтів відбувається через сервера за допомогою каналів зв'язку. Під каналом зв'язку прийнято розуміти множину лінії зв’язку та засобів передачі даних, що беруть участь в процесі відео конференції [3].

До головних особливостей технології ВКЗ можна віднести наступні: мінімізація витрат на поїздки, інтерактивне спілкування між учасниками, групове спілкування або навчання співробітників, проведення оперативних зустрічей з візуальним контролем, легкість в управлінні та підключенні, практично в будь-якому місці, де є доступ до Інтернету, надійність і безпека інформації.

Сучасна ВКЗ має масу унікальних можливостей, найзначніші з них:

– Телеприсутність. Засоби ВКЗ дозволяють обробляти і транслювати високу якість зображення, яке формуються на спеціально розташованих дисплеях з високою роздільною здатністю, створюючи ефект присутності кількох учасників з протилежного боку лінії зв'язку.

– Багатоточкове з'єднання. Дає можливість одночасно вести конференцію з великою кількістю програмних і апаратних пристроїв, створюючи сучасний центр з обміну оперативною інформацією та спільної роботи.

– Трансляція різних аудіо та відео матеріалів. Дана можливість надає підключення до ВКЗ будь-якого аудіо або відео обладнання для показу документів, презентацій, аудіо-відео записів і багато іншого.

– Інтеграція в автоматизовану систему управління. ВКЗ без проблем впроваджується в будь-яку сучасну технологію автоматизації, об’єднуючи всі системи в централізоване управління.

– Формування якісного зображення. Апаратні системи ВКС дозволяють відображати на екрані монітора відмінне і стабільне зображення в Full HD якості.

Система ВКЗ - це технічний комплекс програмно-апаратних засобів для організації аудіо-відео зв'язку між двома та більш користувачами, через мережу Інтернет. В даний момент, на ринку ВКЗ присутні два основних типи виконання: програмне і апаратне. Під програмним рішенням мається на увазі оснащення обчислювальної техніки (комп'ютера або ноутбука) спеціальним ПЗ, за допомогою якого буде організовуватися індивідуальний або груповий відеозв'язок в HD якості. Апаратне, має на увазі професійне обладнання (відеотермінал, аудіовізуальні технології) для побудови повноцінного аудіо-відео зв'язку між абонентами.

Проблеми надійності систем відеоконференцій є як ніколи актуальними на сьогоднішній день, так як дистанційне навчання з причини своєї доступності в будь-якій точці світу стає все більш популярним, при цьому організаторами конференцій висуваються високі вимоги до якості послуг, що надаються. При великій кількості бажаючих приєднатися до відкритої конференції і невеликої пропускної спроможності каналу найважливішим стає забезпечення доступності для всіх учасників.

Для забезпечення надійності відеоконференцій існує необхідність обмежити доступ сторонніх осіб (неавторизованих користувачів), а також організувати ідентифікацію користувача пристроїв і аутентифікацію учасників конференції (авторизацію).

Основною проблемою організації надійної системи відеоконференцзв'язку на сьогоднішній день є забезпечення оптимальної швидкості передачі даних при максимальній швидкості обробки аудіо та відео потоку. Для вирішення цієї проблеми розроблено кодеки, що дозволяють стискати сигнал і кодувати його для каналу зв'язку, а також відновлювати і декодувати на приймальній стороні.

Питання, пов'язані із захистом інформації в мережах ВКЗ є дуже важливими. Відповідно до законодавства України, як засоби захисту інформації можуть використовуватися тільки сертифіковані засоби [1].

Для систем ВКЗ актуальні різні загрози інформаційної безпеці, які притаманні будь-якій інформаційній системі (рис. 1).

Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами повинні блокуватися.

Рисунок 1 – Види інформації, що встановлені законом та підлягають захисту в інформаційних, телекомунікаційних та інформаційно - телекомунікаційних системах

ВКЗ схильні до загроз з боку зловмисників, форс-мажорних обставин, випадкових дій користувачів і адміністраторів [2]. Відповідно до загальноприйнятої класифікації, загрози інформаційної безпеки можна

поділити на такі види: загрози конфіденційності, цілісності і доступності та загрозу підтвердження авторства. В тій чи іншій мірі для ВК актуальні всі ці види загроз, однак, в рамках розгляду питань надійності ВКЗ найбільш актуальними є загрози цілісності та доступності.

Окрім гарантованої доставки, в якості засобу забезпечення надійності ВКЗ 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 [2]. При збільшенні кількості користувачів навантаження зростає і саме авторизація дозволяє обмежити мережеве навантаження, що підвищує надійність системи ВКЗ і дозволяє забезпечити контролювання смуги пропускання. Для кожного суб'єкта в системі визначається набір прав, які він може використовувати при зверненні до ресурсів ВКЗ. До найбільш поширених способів авторизації відносять: дискреційний (DAC), мандатний (MAC), управління доступом на основі ролей, контроль доступу на основі контексту (CBAC), контроль доступу на основі решітки (LBAC)[3] .

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

Основними методами підвищення надійності систем ВКЗ 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].

Оптимальний розподіл мережевого навантаження дозволяє забезпечувати задані характеристики ВКЗ за рахунок керування інформаційними потоками.

Проведений аналіз показує, що на сьогоднішній день найбільш поширеними технологіями відеоконференцзв'язку є: системи відеоконференцзв'язку високої якості, засновані на застосуванні спеціальних протоколів; серверні системи, в основу принципу дії яких покладено стиснення відеопотоку. Більшість систем комп'ютерного відеоконференцзв'язку складається з наступних частин: - програмно-апаратне забезпечення сервера; - програмно-апаратне забезпечення клієнта; - лінії зв'язку; - мережеве обладнання.

Перелік посилань

1. Бараннік В. В. Модель загроз безпеки відеоінформаційного ресурсу систем відеоконференцзв'язку / В. В. Бараннік, А. В. Власов, Р. В. Тарнополов // Наукоємні технології. - 2014. - № 1. - С. 55-60. - Режим доступу: http://nbuv.gov.ua/UJRN/Nt_2014_1_13.

2. Живко З. Б. Інформаційні загрози: суть і проблеми / З.Б. Живко, М.О. Живко // Системи обробки інформації. – 2009. – № 7(81). – С. 116-118.

3. Лебедева К. Алгоритмы и программные решения организации защищенного доступа к компьютерным видеоконференциям / К. Лебедева, А. Томилина // XVIII Решетневские чтения : Международная научная конференция, посвященной 90-летию со дня рождения генерального конструктора ракетно-космических систем академика М.Ф. Решетнева, 11-14 ноября 2014 : материалы конференции. – в 3 ч. – Красноярск : СибГАУ, 2014. – Ч. 2. – С. 320-322.

Діагностично-тренувальні прилади для відновлення рефлексів ушкоджених кістей та пальців рук

Полянічкін В. Г., Гнезділов М. Д.
Науковий керівник – д.т.н., проф..Журавська І. М.
Чорноморський національний університет ім. Петра Могили

Після пошкодження шийно-грудного відділу хребта та нервів кисті рук рухові та/або сенсорні функції порушуються, особливо дрібна моторика окремих пальців або групи пальців. Посттравматична та постінсультна спастичність кінцівки – одне з найчастіших рухових порушень. Спастичність від ураження верхніх кінцівок відзначається більш ніж у 12 мільйонів осіб у всьому світі [1]. Програми реабілітації поєднують фізичну терапію з набуттям та відновленням рефлексів. Використанням апаратних тренажерів в амбулаторних та/або у домашніх умовах дозволяє досягти максимального результату [2].

Підвищити ефективність зазначеного процесу можливо за допомогою серії малогабаритних діагностично-тренувальних (ДТ) приладів «Reflex-Txx». Прилади розроблені на основі платформи Arduino з використанням на рухомій робочій зоні датчиків Холла або датчиків дотику та світлодіодів, частота спалахів яких регулюється в залежності від результатів тренувань. Авторизація пацієнта виконується за допомогою RFID-карти.

Якщо тренуванню підлягають декілька пальців, то використовується ДТ-прилад з датчиками Холла на рухомій робочий зоні – «Reflex-TH3» («Training Hall 3 Sensors»). В такому разі до кольорового майданчика біля спалахнувшого світлодіода треба доторкнутися магнітним інструментом («холдером»), що утримується щепотью з пальців, які підлягають тренуванню (на рис. 1, а – два пальці). Для тренування одного пальця (рис. 1, б)