DOI 10.31891/2307-5732-2021-301-5-27-31
УДК 621.397

ОГНЄВИЙ О.В.
Хмельницький національний університет
ORCID ID: 0000-0001-6462-3483
e-mail: aognev@i.ua
ХМЕЛЬНИЦЬКИЙ Ю.В.
Хмельницький національний університет
ORCID - 0000-0002-4005-5669
e-mail: getman-58@ukr.net

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Стаття присвячена дослідженню теоретико-методологічних засад та практичних рекомендацій застосування технології захисту інформаційних ресурсів для ефективного функціонування систем відеозв'язку. З розвитком міжнародних відносин в суспільстві, впровадженням інформаційних та телекомунікаційних технологій, в Україні активно розвивається та впроваджується технологія відеоконференцзв'язку, створюються та реалізуються віртуальні заходи, вебінари, відеоконференції та онлайн-трансляції. Для систем відеоконференцій актуальні загрози інформаційної безпеки, які притаманні будь-якій інформаційно-телекомунікаційній системі. Однією з основних проблем організації надійної системи відеоконференцзв'язку є забезпечення оптимальної швидкості передачі даних при максимальній швидкості обробки аудіо- та відеопотоку. Розглянуто основні види інформації та визначено напрямки підтримання інформаційної безпеки інформаційно-телекомунікаційних систем відповідно до законодавства України. Для забезпечення надійності системи відеоконференцій використовується захист відкритої інформації від несанкціонованих дій, що призводить до її випадкової або умисної модифікації чи знищення, авторизація користувачів. Забезпечення захисту інформаційних ресурсів здійснюється шляхом застосування засобів і методів технічного захисту, впровадження організаційних та технічних заходів комплексної системи захисту інформації. Дослідження цих методів надають можливість розподілити навантаження на всі елементи системи пропорційно їх ресурсам і характеристикам.

Ключові слова: відеозв'язок, інформаційна безпека, захист, інформаційні ресурси, ідентифікація, система, технології, конфіденційність, цілісність.

OHNIEVYI OLEKSANDR V.
Khmelnytsky National University
KHMELNYTSKY YURIY V.
Khmelnytsky National University

METHODS OF PROTECTION OF INFORMATION RESOURCES IN TELECOMMUNICATION SYSTEMS

The article is devoted to the study of theoretical and methodological principles and practical recommendations for the use of information resource protection technology for the effective functioning of video communication systems. With the development of international relations in society, the introduction of information and telecommunication technologies, Ukraine is actively developing and implementing video conferencing technology, creating and implementing virtual events, webinars, video conferencing and online broadcasts. The use of such systems allows you to get a variety of information, use textual and visual graphics, and so on. For video conferencing systems are relevant threats to information security, which are inherent in any information and telecommunications system. One of the main problems of organizing a reliable video conferencing system is to ensure the optimal data rate at the maximum speed of audio and video processing. The main types of information are considered and the directions of maintaining information security of information and telecommunication systems in accordance with the legislation of Ukraine are determined. The main types of information security are related to the protection of confidentiality, integrity and accessibility and to the confirmation of authorship. To ensure the reliability of the video conferencing system, the protection of open information from unauthorized actions is used, which leads to its accidental or intentional modification or destruction, authorization of users. The tasks of user authorization are management of access rights, collection of statistics and acts as an additional means of ensuring the reliability of the system. Ensuring the protection of information resources is carried out through the use of means and methods of technical protection, implementation of organizational and technical measures of a comprehensive information protection system. Studies of these methods make it possible to distribute the load on all elements of the system in proportion to their resources and characteristics.

Keywords: video communication, information security, protection, information resources, identification, system, technologies, confidentiality, integrity.

Постановка проблеми

Інформаційно-телекомунікаційні системи відіграють важливу роль в сферах державного управління, економіці, освіті, науці, обороні, забезпечені безпеки життєдіяльності тощо. Розвиток та впровадження інформаційних та телекомунікаційних технологій, збільшення пропускної здатності каналів передачі інформації, з використанням засобів аудіо та відео зв'язку, зробило зручним засобом спілкування. Особливо це стало актуальним в наш час під проведення відеоконференцій (ВК). Використання систем відеоконференцзв'язку (ВКЗ) дозволяє отримати різноманітний обсяг інформації, задіяти при спілкуванні текстові та візуальні графічні матеріали: малюнки, таблиці, схеми і діаграми, враховувати вираз обличчя та міміку співрозмовника.

З розвитком міжнародних відносин в суспільстві, необхідністю оперативного зв'язку між користувачами в країні та по всьому світі, технологія відеоконференцзв'язку активно розвивається та

впроваджується і в Україні. Організація ВКЗ 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.

Великою популярністю користуються системи для проведення ВК за допомогою глобальних телекомунікаційних мереж. Їх використання пов'язано з підвищеними ризиками, які призводять до виникнення проблем з можливим несанкціонованим доступом, прослуховуванням чи аналізом сигнальної інформації використовуваних протоколів. Найчастіше такі конференції призначені для обмеженого кола користувачів, тому питання захисту інформації в таких системах виходять на передній план.

Із запровадженням карантину в Україні, за допомогою ВКЗ 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.

Аналіз останніх досліджень

Необхідність підтримання інформаційної безпеки інформаційно-телекомунікаційних систем визначена на державному рівні та спрямована на забезпечення інформаційної безпеки відносин, що пов'язані із збиранням, накопиченням, обробкою та передачею інформації. Забезпечення захисту інформаційних ресурсів при використанні 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.

Дослідженню та розробці теоретичних положень, що стосуються інформаційної безпеки і захисту інформації в інформаційно-телекомунікаційних системах та можуть бути використані у процесі відеоконференцій присвячено багато наукових праць. Питання пов'язані з науковими дослідженнями проблем інформаційної безпеки досліджуються в роботах таких вчених як Астахов А.М., Бараннік В.В., Власов А.В., Живко З.Б., Євдоченко Л.О.,Карпенко О.В.,Климчук В.П., Кузьменко Б.В., Конахович Г.Ф., Лебедєва К.Е., Литвиненко О.,Семенов С. Г., Хорошко В.О. Франчук В.М., Юдін О. К. та інших.

Незважаючи на значний рівень наукового дослідження проблем інформаційної безпеки, їх класифікації та нормативно-законодавчого забезпечення, питання захисту інформаційних ресурсів відеоконференцій мають актуальне значення, що й обумовлює тему статті. Теоретичні розробки досліджуваного питання необхідні для формування дієвої системи моніторингу та управління у сфері інформаційної безпеки відеозв'язку, а також вдосконалення методів захисту інформаційних ресурсів під час проведення ВК.

Формулювання цілей статті

Метою статті є дослідження методів захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах та використання їх під час проведення відеоконференцзв'язку.

Виклад основного матеріалу

Відеоконференція (videoconference, або videoteleconference) – це телекомунікаційна технологія інтерактивної участі двох і більше віддалених абонентів, при якому забезпечується одночасна двостороння передача, обробка, перетворення та представлення інтерактивної інформації у режимі реального часу за допомогою апаратно-програмних засобів обчислювальної техніки.

Систему ВКЗ прийнято вважати сукупністю наступних елементів: кінцевих вузлів системи – серверів, клієнтів відеоконференцій та каналів зв'язку, що з'єднують ці вузли. Сервером ВК є комплекс програмно-технічних засобів і систем, що забезпечує управління конференцією, виконання функції ідентифікації і аутентифікації клієнтів, прийому, обробки та перенаправлення даних ВК. 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 відеоконференції [3, с.87].

Сучасна ВКЗ має масу унікальних можливостей, найзначніші з них: телеприсутність. багатоточкове з'єднання, трансляція різних аудіо та відео матеріалів, інтеграція в автоматизовану систему управління, формування якісного зображення.

Проблеми надійності систем ВК є як ніколи актуальними з причини своєї доступності в будь-якій точці світу. Відеозв'язок стає все більш популярним і 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 авторизованих учасників, обмеження доступу сторонніх осіб (неавторизованих користувачів), ідентифікації користувача пристроїв та аутентифікації учасників конференції (авторизація).

Однією з основних проблем організації надійної системи ВКЗ є забезпечення оптимальної швидкості передачі даних при максимальній швидкості обробки аудіо та відео потоку. Для вирішення цієї проблеми розроблено кодеки, що дозволяють, зберігаючи задані характеристики якості, стискати сигнал і кодувати його, а також відновлювати і декодувати на приймальній стороні. Для організації ВКЗ між різним

програмним забезпеченням та обладнанням сторонніх виробників використовуються стандартні протоколи передачі даних.

Системи ВКЗ базуються на універсальних комунікаціях – IP мережах, стандартних протоколах пакетної передачі мовної та відеоінформації, стандартних алгоритмах її кодування. Сучасні системи ВКЗ базуються на основі протоколу IP (Internet Protocol). Транспорт інформаційних потоків при проведенні ВК часто здійснюється по відкритим телекомунікаційним мережам з використанням стандартних протоколів, тому дослідження проблем забезпечення надійності ВКЗ набувають особливої актуальності. В основному використовується протокол SIP, який дозволяє забезпечувати простоту впровадження комплексу ВКЗ, дає можливість застосувати обладнання різних виробників та забезпечує безпеку з'єднань сеансів ВК на основі механізмів TLS та SRTP [8].

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 [7]. Для систем ВКЗ актуальні різні загрози інформаційної безпеці, які притаманні будь-якій інформаційно-телекомунікаційній системі (рис. 1).

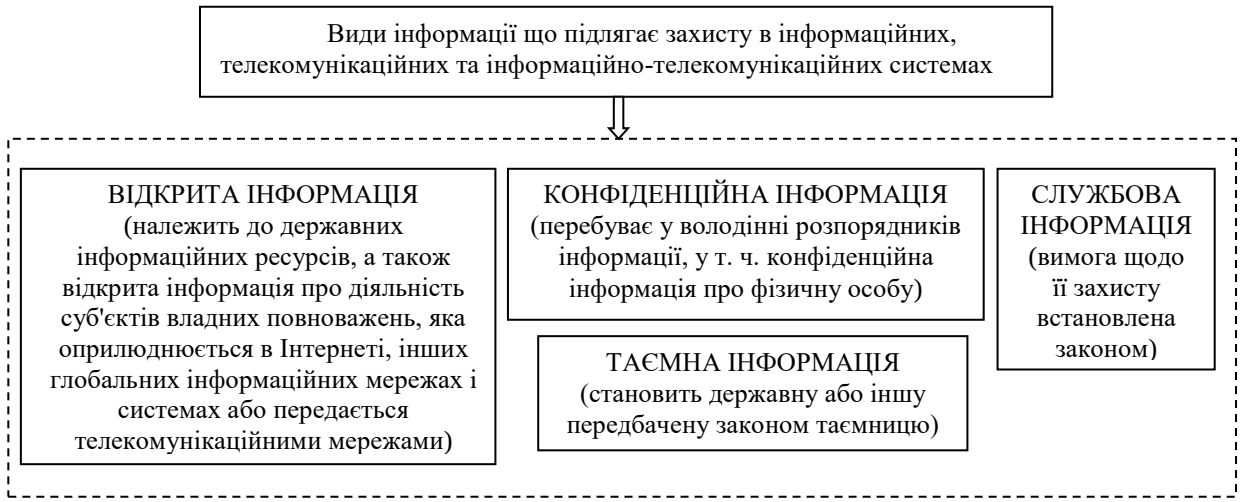

Рис. 1. Види інформації, встановлені законом, що підлягають захисту в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах

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 [7]. 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 або користувачами з непідтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися [3].

Під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення. Доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні також блокуватися.

ВКЗ схильні до загроз з боку зловмисників, форс-мажорних обставин, випадкових дій користувачів і адміністраторів [2, с.104]. 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 розрізі питань надійності ВКЗ найбільш актуальними є загрози цілісності та доступності. Також, крім гарантованої доставки, в якості засобу забезпечення надійності ВКЗ використовується авторизація користувачів (надання певній особі або групі осіб прав на виконання певних дій, а також процес перевірки (підтвердження) даних прав при спробі виконання цих дій) [8, с.53]. 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) [1, с.56].

Завданнями авторизації є: управління правами доступу; обмеження прав доступу; збір статистики. Воно тісно пов'язане з поняттями «аутентифікація» і «ідентифікація». У процесі аутентифікації перевіряється справжність пред'явленого користувачем ідентифікатора [4, с.117]. Вона дозволяє достовірно

переконатися в тому, що суб'єкт, який пред'явив свій ідентифікатор, насправді є саме тим суб'єктом, ідентифікатор якого він використовує. Для цього суб'єкт повинен підтвердити факт володіння певною інформацією, яка може бути доступна тільки йому одному (пароль, ключ і тощо). Ідентифікація – це процедура розпізнавання суб'єкта за його ідентифікатором. 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. Отже авторизація виступає в ролі додаткового засобу забезпечення надійності.

В роботі [5] запропоновано методику підвищення надійності систем ВКЗ за рахунок порівняння вихідних фактичних параметрів надійності системи ВКЗ з необхідними параметрами системи, що враховують вимоги до надійності. З врахуванням збільшення інформаційного потоку критерій надійності $P \to 1.$

Імовірність отримання кожним суб'єктом повного доступу до кожного об'єкта:

$$P = P_c \cdot P_k ,$$

де P_c – імовірність доступності сервера, P_k – імовірність доступності клієнта.

Імовірність доступності сервера складається з ймовірностей доступності до інформаційних ресурсів:

$$P_c = P_{c1} \cdot P_{c2} \cdot P_{c3} \cdots P_{cn} ,$$

де P_{c1} – доступ до відеоінформації на сервері; P_{c2} – доступність аудіоінформації на сервері; P_{c3} – доступність файлів на сервері; P_{cn} – доступність до повідомлень на сервері та інших даних.

Аналогічно можна представити ймовірність доступності клієнта, враховуючи відповідні значення доступності відео- та аудіоінформації у клієнта, файлів, повідомлень тощо: $P_k = P_{k1} \cdot P_{k2} \cdot P_{k3} \cdots P_{kn}$.

Імовірність отримання кожним суб'єктом повного доступу до кожного об'єкта розраховується як добуток ймовірностей доступу до n об'єктів.

Таким чином, для визначення ймовірності доступу до системи ВКЗ необхідно визначити ймовірності доступності серверів P_c та доступності клієнтів P_k. Тестове значення ймовірності отримання повного доступу визначається виходячи з статистичних даних ймовірностей виконання n дій клієнтів до k об'єктів. Отримані ймовірнісні значення доступу дозволяють визначити надійність системи ВКЗ, що є досить трудомістким завданням. Розраховані значення ймовірності отримання суб'єктом повного доступу порівнюються з необхідним рівнем ймовірності отримання повного доступу до об'єкту та в подальшому, при необхідності, застосовується алгоритм управління навантаженням мережі.

Одним з перспективних рішень проблеми забезпечення надійності систем ВКЗ на сьогодні є використання технологій розподілу навантаження інфокомунікаційної мережі [7].

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 [4].

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Проведений аналіз показує, що на сьогоднішній день найбільш поширеними технологіями ВКЗ є: системи ВК високої якості, засновані на застосуванні спеціальних протоколів; серверні системи, в основу принципу дії яких покладено стиснення відеопотоку. Більшість систем комп'ютерного ВКЗ складається з наступних частин: програмно-апаратне забезпечення сервера; програмно-апаратне забезпечення клієнта; лінії зв'язку; мережеве обладнання. Авторами було виділено такі способи організації захищеного доступу до ВКЗ, як захист клієнтських комп'ютерів та серверів програмними та апаратними засобами; захист обладнання, захист каналу зв'язку, захист інформації.

Література

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.

2. Голев Д.В. Методики оцінки інформаційної захищеності телекомунікацій : навч. посіб. / Голев Д.В., Кононович В.Г., ХомичС.В. ; за ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса : ОНАЗ ім.О.С.Попова, 2013. – 218 с.

3. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах / [Л.Л. Гончарова, А.Д. Возненко, О.І. Стасюк, Ю.О. Коваль]. – Київ, 2013. – 435 с.

4. Живко З. Б. Інформаційні загрози: суть і проблеми / З.Б. Живко, М.О. Живко // Системи обробки

інформації. – 2009. – № 7(81). – С. 116–118.

5. Лебедева К. Е. Методика повышения надежности систем видеоконференцсвязи с гарантированной доставкой сообщений для авторизованных пользователей [Электронный ресурс] / К.Е. Лебедева. – Режим доступа : https://docplayer.com/61503923-Intellektualnye-sistemy-v-informacionnom-protivoborstve.html.

6. Лісовська Ю. П. Інформаційна безпека України : навч. посібник / Ю.П. Лісовська. – Київ : Кондор, 2018. – 172 с.

7. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електронний ресурс] : постанова Кабінету Міністрів України від 29 березня 2006 р. N 373. – Режим доступу : https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.

8. Франчук В.М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних : посібник для викладачів, вчителів та студентів інформатичних спеціальностей / В.М. Франчук. – К. : НПУ імені М.П. Драгоманова, 2012. – 120 с.

References

1. Barannik V. V. Model zahroz bezpeky videoinformatsiinoho resursu system videokonferentszviazku / V. V. Barannik, A. V. Vlasov, R. V. Tarnopolov // Naukoiemni tekhnolohii. – 2014. – № 1. – S. 55–60.

2. Holev D.V. Metodyky otsinky informatsiinoi zakhyshchenosti telekomunikatsii : navch. posib. / Holev D.V., Kononovych V.H., KhomychS.V. ; za red. chl.-kor. MAZ V.H. Kononovycha. – Odesa : ONAZ im.O.S.Popova, 2013. – 218 s.

3. Osnovy zakhystu informatsii v telekomunikatsiinykh ta kompiuternykh merezhakh / [L.L. Honcharova, A.D. Voznenko, O.I. Stasiuk, Yu.O. Koval]. – Kyiv, 2013. – 435 s.

4. Zhyvko Z. B. Informatsiini zahrozy: sut i problemy / Z.B. Zhyvko, M.O. Zhyvko // Systemy obrobky informatsii. – 2009. – № 7(81). – S. 116–118.

5. Lebedeva K. E. Metodika povysheniya nadezhnosti sistem videokonferencsvyazi s garantirovannoj dostavkoj soobshenij dlya avtorizovannyh polzovatelej [Elektronnyj resurs] / K.E. Lebedeva. – Rezhim dostupa : https://docplayer.com/61503923-Intellektualnye-sistemy-v-informacionnom-protivoborstve.html.

6. Lisovska Yu. P. Informatsiina bezpeka Ukrainy : navch. posibnyk / Yu.P. Lisovska. – Kyiv : Kondor, 2018. – 172 s.

7. Pravyla zabezpechennia zakhystu informatsii v informatsiinykh, telekomunikatsiinykh ta informatsiino-telekomunikatsiinykh systemakh [Elektronnyi resurs] : postanova Kabinetu Ministriv Ukrainy vid 29 bereznia 2006 r. N 373. – Rezhym dostupu : https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF.

8. Franchuk V.M. Zakhyst informatsiinykh resursiv: kryptohrafichni ta stehanohrafichni metody zakhystu danykh : posibnyk dlia vykladachiv, vchyteliv ta studentiv informatychnykh spetsialnostei / V.M. Franchuk. – K. : NPU imeni M.P. Drahomanova, 2012. – 120 s.

Рецензія/Peer review : 06.09.2021 р. Надрукована/Printed :10.10.2021 р.