DOI 10.31891/2307-5732-2019-275-4-92-96
УДК 004.891

О.В. ОГНЄВИЙ, Л.Л. СИЧ
Хмельницький національний університет

МЕТОД ПІДВИЩЕННЯ НАДІЙНОСТІ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ СИСТЕМ ВІДЕОКОНФЕРЕНЦЗВ'ЯЗКУ

В роботі запропоновано актуальний метод обробки інформації, який, шляхом виділення привілейованого трафіку і оптимізації потоків інформації, дозволяє підвищити надійність системи відеоконференцзв'язку для авторизованих користувачів з гарантованою доставкою повідомлень і підвищити ймовірність отримання доступу до ресурсів систем відеоконференцзв'язку. Розроблено новий алгоритм управління доступом до інформаційних ресурсів, заснований на додаванні міток привілеїв в службове поле пакету і зміни маршруту передачі пакетів, що дозволяє підвищити надійність відеоконференцзв'язку для авторизованих користувачів з гарантованою доставкою повідомлень шляхом підвищення ймовірності отримання доступу до інформаційних ресурсів до заданого значення. На сьогоднішній день технологія відеоконференцзв'язку активно розвивається, це пов'язано в основному з впливом процесів глобалізації, розвитком міжнародних відносин у суспільстві. Використання виключно голосового зв'язку не дозволяє отримати такий же обсяг інформації, який стає доступним з використанням. Також сучасні технології дозволяють задіяти при спілкуванні візуальні графічні матеріали: малюнки, таблиці, схеми і діаграми. У сучасних дослідженнях практично не розглядається задача одночасного розділення користувачів на класи з одночасним розподілом навантаження для привілейованих користувачів. В інших методах підвищення надійності традиційно найважливішим критерієм виступають використовувані технології, в тому числі вид мережевого обладнання, а пропоновані рішення часто засновані на використанні специфічних протоколів. Застосування рішення на практиці дозволить організувати надійне з'єднання учасників відеоконференцзв'язку.

Ключові слова: інформаційний трафік, оптимізація потоків, передача пакетів, інформаційна безпека.

O.V. OHNIEVYI, L.L. SYCH
Khmelnytsky National University

METHOD OF INCREASING RELIABILITY ACCESS TO INFORMATION RECOURSES VIDEOCONFERENCING SYSTEMS

The article proposes an actual method of information processing. By allocating privileged traffic and streamlining information flows, it can increase the reliability of the video conferencing system for authorized users with guaranteed delivery of messages. Also, the method can increase the likelihood of access to resources of video conferencing systems. A new algorithm for access control to information resources has been developed. It is based on the addition of privilege labels in the service field of the packet and the change of the data transmission path, which increases the reliability of video conferencing for authorized users with guaranteed delivery of messages by increasing the likelihood of access to information resources. Today, videoconferencing technology is actively developing. This is mainly due to the following: the influence of the processes of globalization, the development of international relations in society. Therefore, there is a need for operative communication around the world. The use of voice communication alone does not allow for the same amount of information that becomes available through videoconferencing. Also, modern technology allows you to engage in communication visual graphic materials such as: drawings, tables, schematics and diagrams. Increasing the bandwidth of the transmission channels made video conferencing a convenient means of communication. Video conferencing sessions are held to exchange experience among professionals, organize corporate meetings, and videoconferencing is widely used for educational purposes. The transmission of information flows during videoconferences is most often carried out on open telecommunication networks using standard protocols. The method of improving the reliability of video conferencing systems is needed to minimize the likelihood of a threat of integrity and availability. In modern research, the task of simultaneously dividing users into classes with simultaneous distribution of load for privileged users is practically not considered. In other methods of increasing the reliability of traditionally the most important criterion are the technologies used. Including the kind of network equipment, and the proposed solutions are often based on the use of specific protocols. Application of the decision in practice will allow to organize a reliable connection of participants of video conferencing.

Key words: information traffic, flow optimization, packet transmission, information security.

Вступ

На сьогоднішній день технологія відеоконференцзв'язку активно розвивається, це пов'язано в основному з впливом процесів глобалізації, розвитком міжнародних відносин у суспільстві і, як наслідок, з необхідністю оперативного зв'язку по всьому світу. Використання виключно голосового зв'язку не дозволяє отримати такий же обсяг інформації, який стає доступним з використанням відеоконференцзв'язку дуже важливі вираз обличчя, міміка співрозмовника. Також сучасні технології дозволяють задіяти при спілкуванні візуальні графічні матеріали: малюнки, таблиці, схеми і діаграми.

Збільшення пропускної здатності каналів передачі інформації зробило відеоконференцзв'язок зручним засобом спілкування: сеанси проводяться для обміну досвідом між фахівцями, організації корпоративних нарад, також відеоконференцзв'язок широко використовується в освітніх цілях.

В основному технології відеоконференцзв'язку знаходять застосування в наступних областях:

виробничі завдання (бізнес переговори, спільні проекти);

освіта (дистанційне навчання, конференції, майстер-класи та семінари);

особисті потреби людей (спілкування з родичами і друзями).

Відеоконференцзв'язок (ВКЗ) – це телекомунікаційна технологія інтерактивної участі двох і більше віддалених абонентів, при якому між ними відбувається обмін аудіо та відеоінформацією в режимі

реального часу. Історія розвитку відеоконференцзв'язку починається з того моменту, коли компанія «AT&T» представила в 1964 році Videophone – першу аудіовізуальну систему електронної взаємодії, яка призначалася для взаємодії двох осіб в режимі реального часу. Початок поширення ВКЗ відноситься до 80-х років – від телевізійних систем, що забезпечують інтерактивні контакти між віддаленими партнерами. За наступні п'ятдесят з гаком років системи ВКЗ зазнали значних змін, незмінним залишилося те, що співрозмовники бачать один одного у себе на екрані.

Систему відеоконференцзв'язку прийнято вважати сукупністю трьох функціональних елементів: кінцевих 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, забезпечує управління відеоконференцією, виконання функції ідентифікації та аутентифікації клієнтів, приймання, обробки і перенаправлення даних відеоконференцій. Сервер є вузлом на стороні адміністратора відеоконференції. Клієнти також являють собою комплекс програмного і апаратного забезпечення і є джерелом даних системи. Зв'язок клієнтів відбувається тільки через сервера за допомогою канал зв'язку. Під каналом зв'язку прийнято розуміти всі безліч ліній зв'язку і засобів передачі даних, що беруть участь в 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.

Як було сказано вище, проведення відеоконференцій стало невід'ємною частиною нашого життя, проте, з появою технології відеоконференцзв'язку виникли і певні проблеми з надійністю передачі даних. Багато відеоконференцій призначені для вузького кола осіб, що передбачає необхідність організації захищеного доступу до відео даних, що виключає можливість несанкціонованого доступу неавторизованих користувачів для підтримки надійності відеоконференцзв'язку.

Системи відеоконференцзв'язку активно використовуються для роботи над спільними проектами, в тому числі в ракетно-космічній галузі для організації зв'язку між віддаленими майданчиками. Відео-трафік має певні особливості: вимагає значної пропускної здатності 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.

Транспорт інформаційних потоків при проведенні відеоконференцій найчастіше здійснюється по відкритим телекомунікаційним мережам з використанням стандартних протоколів, тому дослідження проблем забезпечення інформаційної безпеки відеоконференцій набувають особливої актуальності. Для мінімізації ймовірності виникнення загроз цілісності та доступності потрібен комп'ютерний метод підвищення надійності систем відеоконференцзв'язку.

Одним з перспективних рішень проблеми забезпечення надійності систем відеоконференцзв'язку на сьогоднішній день є використання технологій розподілу навантаження мережі. Оптимальний розподіл навантаження дозволяє забезпечувати задані характеристики відеоконференцзв'язку за рахунок управління інформаційними потоками.

В якості критерію надійності систем відеоконференцзв'язку раніше не розглядалася ймовірність отримання доступу до різних ресурсів систем відеоконференцзв'язку.

Постановка задачі

В результаті проведеного дослідження відмічено, що для розподілених обчислювальних систем, до яких можна віднести системи відеоконференцзв'язку, функціональна надійність і відмовостійкість може забезпечуватися перерозподілом запитів між вузлами кластера. Незважаючи на те, що перерозподіл вносить додаткову затримку, ступінь адаптації системи до зміни потоку запитів збільшується, що призводить до зменшення відмов.

На сьогоднішній день відсутня ймовірнісна модель доступу до систем відеоконференцзв'язку з гарантованою доставкою для авторизованих користувачів. Моделі доступу інших авторів в основному орієнтовані на підтримку конфіденційності, а не цілісності та доступності. Існуючі ймовірнісні моделі традиційно використовують в якості критерію надійності коефіцієнт готовності, що визначає працездатність системи, а не цілісність і доступність її ресурсів. В якості критерію надійності систем відеоконференцзв'язку раніше авторами не розглядалася ймовірність отримання доступу до ресурсів систем відеоконференцзв'язку. Існуючі ймовірнісні моделі доступу зазвичай не враховують характерні особливості систем відеоконференцзв'язку або прив'язані до конкретних технологій, наприклад, бездротовий відеоконференцзв'язок, що звужує їх область застосування.

Основна частина

В ході досліджень була запропонована ймовірнісна модель доступу до системам відеоконференцзв'язку, придатна для оцінки надійності таких систем.

Розроблена модель дозволяє описати різні системи відеоконференцзв'язку і враховує їх характерні особливості.

Значення ймовірності отримання доступу може бути розраховане на основі апарату марківських випадкових процесів з дискретними станами і безперервним часом.

Ймовірнісна модель доступу верхнього рівня, запропонована в роботі, заснована на поняттях: суб'єкти, об'єкти, дії. Для кожного об'єкта доступним є певний перелік дій, де $\tilde{P}_{ijk}$ – ймовірність вчинення

дії, A – кількість дій, які можна виконати над об'єктом, B – кількість об'єктів, R – кількість суб'єктів, щоб отримати доступ, всі R суб'єкти повинні мати можливість здійснити будь-яку з A допущених дій з B об'єктами.

Ймовірність отримання кожним суб'єктом повного доступу до кожного об'єкта виражена формулою (1):

$$\tilde{P} = \Pi_{i=1}^{R} \tilde{P}_i \quad (1)$$

Ймовірність отримання i-м суб'єктом доступу до будь-якого об'єкта для кожного суб'єкта (2):

$$\tilde{P}_i = \Pi_{j=1}^{B} \tilde{P}_{ij} \quad (2)$$

Ймовірність отримання доступу суб'єкта до об'єкта дорівнює добутку ймовірностей усіх дій суб'єкта до об'єкта (3):

$$\tilde{P}_{ij} = \Pi_{k=1}^{A} \tilde{P}_{ijk} \quad (3)$$

Тоді ймовірність отримання кожним суб'єктом повного доступу до кожного об'єкта виражена формулою (4):

$$\tilde{P} = \Pi_{i=1}^{R} \Pi_{j=1}^{B} \Pi_{k=1}^{A} \tilde{P}_{ijk} \quad (4)$$

Значення ймовірності отримання повного доступу визначається на підставі статистичних даних ймовірностей вчинення k дій i суб'єктів до j об'єктів.

Критерій надійності системи сформульований наступним чином (5):

$$\tilde{P} \to 1 \quad (5)$$

Ймовірність отримання кожним суб'єктом повного доступу до кожного об'єкта виражена формулою (6):

$$\tilde{P} = \tilde{P}_1 * \tilde{P}_2 \quad (6)$$

де $\tilde{P}_1$ – ймовірність доступності сервера, $\tilde{P}_2$ – ймовірність доступності клієнта.

Ймовірність доступності сервера складається з ймовірностей доступності інформаційних ресурсів (7):

$$\tilde{P}_1 = \tilde{P}_{11} * \tilde{P}_{12} * \tilde{P}_{13} * \tilde{P}_{14} * \tilde{P}_{15} \quad (7)$$

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.

Ймовірність доступності клієнта (8):

$$\tilde{P}_2 = \tilde{P}_{21} * \tilde{P}_{22} * \tilde{P}_{23} * \tilde{P}_{24} * \tilde{P}_{25} \quad (8)$$

де $\tilde{P}_{21}$ – доступність відеоінформації у клієнта, $\tilde{P}_{22}$ – доступність аудіо інформації у клієнта, $\tilde{P}_{23}$ – доступність файлів у клієнта, $\tilde{P}_{24}$ – доступність повідомлень у клієнта, $\tilde{P}_{25}$ – доступність віртуальної дошки у клієнта.

Ймовірності здійснення k-ї дії для сервера (9):

$$\tilde{P}_{11} = \Pi_{k=1}^{5} \tilde{P}_{11k}, \tilde{P}_{12} = \Pi_{k=1}^{5} \tilde{P}_{12k}, \tilde{P}_{13} = \Pi_{k=1}^{5} \tilde{P}_{13k}, \tilde{P}_{14} = \Pi_{k=1}^{5} \tilde{P}_{14k}, \tilde{P}_{15} = \Pi_{k=1}^{5} \tilde{P}_{15k}, \quad (9)$$

де $\tilde{P}_{11k}$ – ймовірність здійснення k-ї дії з відеоінформацією на сервері, $\tilde{P}_{12k}$ – ймовірність здійснення k-ї дії з аудіо інформацією на сервері, $\tilde{P}_{13k}$ ймовірність здійснення k-ї дії з файлами на сервері, $\tilde{P}_{14k}$ – ймовірність здійснення k-ї дії з повідомленнями на сервері, $\tilde{P}_{15k}$ – ймовірність здійснення k-ї дії з віртуальної дошкою на сервері.

Ймовірності здійснення k –ї дії для клієнта (10):

$$\tilde{P}_{21} = \Pi_{k=1}^{5} \tilde{P}_{21k}, \tilde{P}_{22} = \Pi_{k=1}^{5} \tilde{P}_{22k}, \tilde{P}_{23} = \Pi_{k=1}^{5} \tilde{P}_{23k}, \tilde{P}_{24} = \Pi_{k=1}^{5} \tilde{P}_{24k}, \tilde{P}_{25} = \Pi_{k=1}^{5} \tilde{P}_{25k}, \quad (10)$$

де $\tilde{P}_{21k}$ – ймовірність здійснення k-ї дії з відеоінформацією у клієнта, $\tilde{P}_{22k}$ – ймовірність здійснення k-ї дії з аудіо інформацією у клієнта, $\tilde{P}_{23k}$ ймовірність здійснення k-ї дії з файлами у клієнта, $\tilde{P}_{24k}$ – ймовірність здійснення k-ї дії з повідомленнями у клієнта, $\tilde{P}_{25k}$ – ймовірність здійснення k-ї дії з віртуальної дошкою у клієнта.

У роботі запропоновано алгоритм управління доступом до інформаційних ресурсів систем відеоконференцзв'язку – алгоритм управління навантаженням мережі, призначений для використання в системах з гарантованою доставкою повідомлень, заснованих на мережному протоколі TCP стека TCP/IP.

Застосування алгоритму управління навантаженням мережі дозволяє системі відеоконференцзв'язку

функціонувати в двох режимах: стандартному і спеціальному.

Спеціальний режим складається з трьох етапів: підготовка, безпосередньо спеціальний режим і завершення роботи.

На першому етапі роботи алгоритму клієнт відправляє пакет з міткою початку спеціального режиму першому серверу відповідно до таблиці привілеїв серверів. У разі позитивної відповіді сервера встановлюється з'єднання, у разі негативної відповіді – пакет з міткою початку спеціального режиму відправляється наступному серверу.

Другий етап роботи алгоритму є безпосередньо спеціальним режимом. Відправка всіх пакетів клієнта відбувається через закріплений сервер. Кожен клієнт відправляє дані серверу, за яким він закріплений, сервер в свою чергу перенаправляє дані адресату. Клієнт може приймати інформацію від будь-якого сервера. Трафік без міток привілеїв в спеціальному режимі не обробляється. У спеціальному режимі відбувається обов'язкова перевірка автентичності мітки привілеїв, тільки при позитивному результаті пакет доставляється адресату.

На третьому етапі відбувається завершення спеціалізованого режиму.

Клієнт відправляє серверу мітку останнього пакету, після чого сервер може встановити з'єднання з ще одним клієнтом. Потім відбувається перевірка мітки останнього пакету, вона означає, що необхідно присвоїти маркеру початку спеціального режиму значення – 1, доставити останній пакет і перейти до звичайної роботі мережі.

Для вирішення можливої проблеми, пов'язаної з блокуванням сервера при втраті пакету з міткою останнього спеціального пакета, необхідно припиняти з'єднання з клієнтом в момент досягнення певного часу з моменту передачі останнього пакету.

Окремий випадок роботи алгоритму – єдиний сервер, представлений на рис. 1.

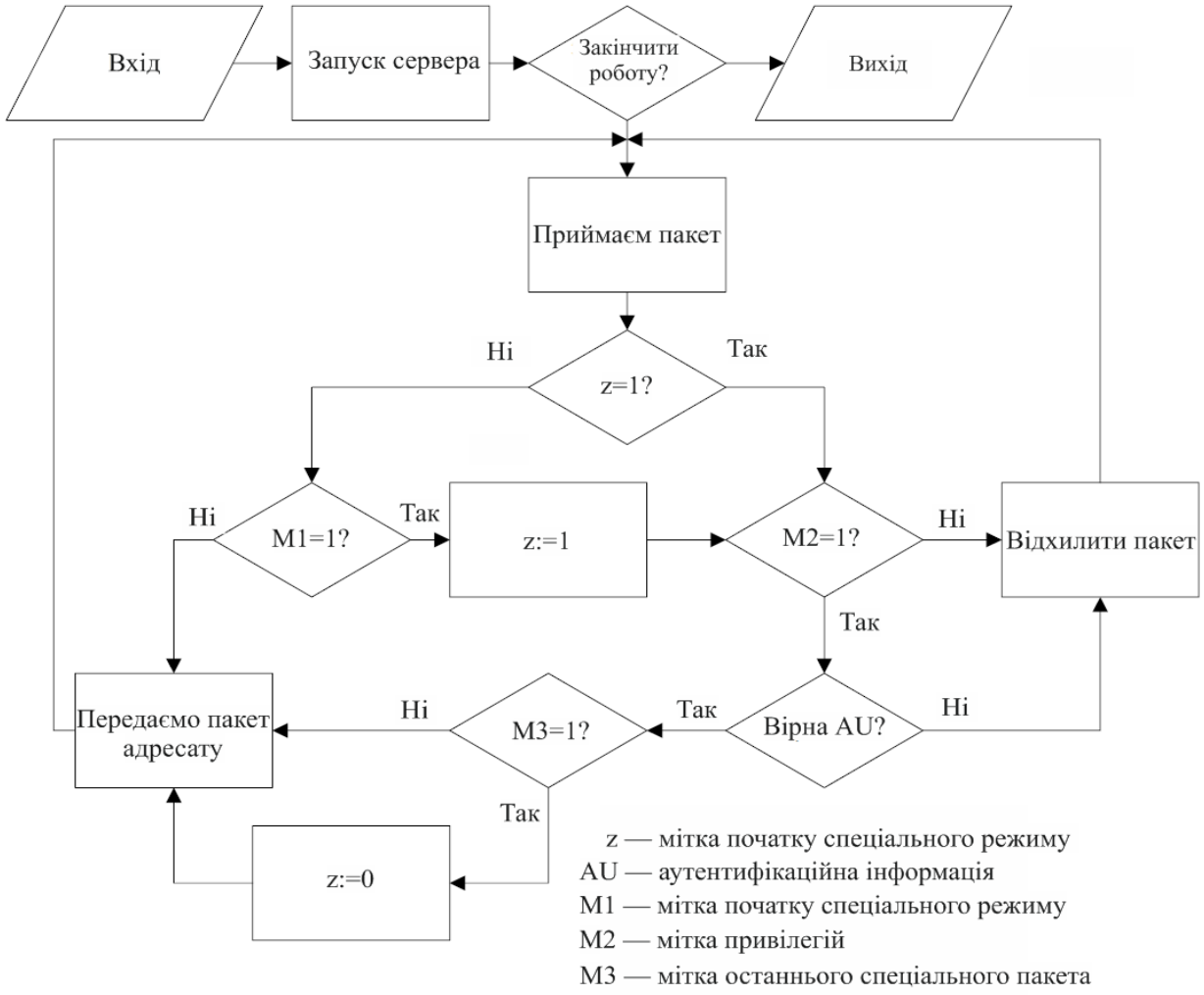

Рис. 1. Алгоритм роботи сервера

Висновки

Представлений новий метод підвищення надійності відеоконференцзв'язку для авторизованих користувачів з гарантованою доставкою повідомлень.

Побудовано ймовірнісні моделі доступу верхнього і нижнього рівня до інформаційних ресурсів систем відеоконференцзв'язку. Ймовірнісні значення доступу дозволяють визначити надійність системи, що

раніше було трудомістким завданням (в інших реалізаціях ймовірнісної моделі доступу) або не розглядалося (в логічних моделях доступу). Отримане значення ймовірності отримання кожним суб'єктом повного доступу до кожного об'єкту порівнюється з необхідним значенням ймовірності отримання кожним суб'єктом повного доступу до кожного об'єкту, за необхідності в подальшому застосовується алгоритм управління навантаженням мережі.

Розроблено алгоритм керування навантаженням мережі, представлено опис алгоритму, докладно розглянуто спеціальний режим, що складається з трьох етапів: підготовка, безпосередньо спеціальний режим і завершення роботи. Більш детально розглянуто окремий випадок роботи алгоритму-мережа з єдиним сервером.

Досліджено ефективність запропонованого методу, дослідження показали, що найбільшу ефективність комп'ютерний метод підвищення надійності відеоконференцзв'язку показує при кількості серверів $n < 10$ та $P(k_{total}, k_{spec}) < 0.1$.

Література

1. Барышников А. А. Моделирование вероятности взлома системы информационной безопасности (системно-интегральный подход) / А. А. Барышников, И. А. Исаев // Горный информационно-аналитический бюллетень : научно-технический журнал. – М. : Горная книга, 2010. – № 5. – С. 152–156.

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

3. Битюков В. К. Обобщенная математическая модель сетевой системы управления с конкурирующим методом доступа / В. К. Битюков, А. Е. Емельянов // Вестник ТГТУ. – Тамбов : ТГТУ, 2012. – № 2. Том 18. – С. 319–326.

4. Богатырев В. А. Функциональная надежность вычислительных систем с перераспределением запросов / В. А. Богатырев, С. В. Богатырев, А. В. Богатырев // Известия ВУЗов : Приборостроение. – СПб : СПбГУ ИМТО, 2012. – Т. 55, № 10. – С. 53–57.

5. Власенко А. В. Системный анализ моделей информационной безопасности, разработка математической модели управления доступом, влияющей на оценку эффективности комплексных систем защиты / А. В. Власенко // Политематический сетевой журнал КубГАУ. – Краснодар : КубГАУ, 2014. – № 101(07). – С. 1–13.

References

1. Baryshnikov A. A. Modelirovanie veroyatnosti vzloma sistemy informacionnoj bezopasnosti (sistemno-integralnyj podhod) / A. A. Baryshnikov, I. A. Isaev // Gornyj informacionno-analiticheskij byulleten : nauchno-tehnicheskij zhurnal. – M. : Gornaya kniga, 2010. – № 5. – S. 152–156.

2. Lebedeva K. E. Metodika povysheniya nadezhnosti videokonferencsvyazi [Tekst] / K. E. Lebedeva, R. V. Lebedev, A. V. Murygin // Sibirskij zhurnal nauki i tehnologij. – Krasnoyarsk : SibGAU, 2017. – № 2, t. 18. – S. 274–282.

3. Bityukov V. K. Obobshennaya matematicheskaya model setevoj sistemy upravleniya s konkuriruyushim metodom dostupa / V. K. Bityukov, A. E. Emelyanov // Vestnik TGTU. – Tambov : TGTU, 2012. – № 2. Tom 18. – S. 319–326.

4. Bogatyrev V. A. Funkcionalnaya nadezhnost vychislitelnyh sistem s pererаspredeleniem zaprosov / V. A. Bogatyrev, S. V. Bogatyrev, A. V. Bogatyrev // Izvestiya VUZov : Priborostroenie. – SPb : SPbGU IMTO, 2012. – T. 55, № 10. – S. 53–57.

5. Vlasenko A. V. Sistemnyj analiz modelej informacionnoj bezopasnosti, razrabotka matematicheskoj modeli upravleniya dostupom, vliyayushej na ocenku effektivnosti kompleksnyh sistem zashity / A. V. Vlasenko // Politematicheskij setevoj zhurnal KubGAU. – Krasnodar : KubGAU, 2014. – № 101(07). – S. 1–13.

Рецензія/Peer review : 27.6.2019 р. Надрукована/Printed :18.7.2019 р.
Рецензент: д.т.н., проф. Мясіщев О.А.