

**МЕТОДИКА ПОВЫШЕНИЯ НАДЕЖНОСТИ ВИДЕОКОНФЕРЕНЦСВЯЗИ**

К. Е. Лебедева\*, Р. В. Лебедев, А. В. Мурыгин

Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева  
Российская Федерация, 660037, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31

\*E-mail: shudrova87@mail.ru

*Основной проблемой организации надежной системы видеоконференцсвязи является обеспечение минимальной скорости передачи данных при поддержании максимальной скорости обработки аудио- и видеопотока. Существующие программные решения имеют ограничения по числу одновременных участников сеанса видеоконференцсвязи, аппаратные системы обладают значительной стоимостью. Основными методами повышения надежности систем видеоконференцсвязи на сегодняшний день являются способы распределения нагрузки. Авторами предложена новая методика повышения надежности видеоконференцсвязи для авторизованных пользователей с гарантированной доставкой сообщений и модели вероятностного доступа к системам видеоконференцсвязи, пригодные для оценки надежности таких систем. Модель верхнего уровня позволяет описать различные системы видеоконференцсвязи, учитывая их характерные особенности. Модель нижнего уровня описывает системы видеоконференцсвязи для авторизованных пользователей с гарантированной доставкой сообщений. Вероятностные модели доступа, предложенные в работе, основаны на следующих понятиях: субъекты, объекты, действия. Для определения вероятности полного доступа к системе видеоконференцсвязи, состоящей из нескольких серверов и клиентов, необходимо определить вероятность доступности серверов и вероятность доступности клиентов. Математический аппарат оценки системы видеоконференцсвязи строится на основе многоканальных систем массового обслуживания (СМО) с ограниченной очередью для случая стандартного режима работы системы и совокупности однородных одноканальных СМО с ограниченной очередью. Приведена оценка эффективности специального режима по отношению к стандартному посредством сравнения вероятностей отказа системы в стандартном и специальном режимах. Используется программное обеспечение, разработанное авторами. На выходе программное обеспечение выдает график в трех координатах  $P(k_{total}, k_{spec}), k_{total}, k_{spec}$ . При заданном уровне  $P(k_{total}, k_{spec})$  по графику определяются  $k_{total}$  и  $k_{spec}$ . В качестве примера приведен график, отражающий целесообразность использования специального режима в системе видеоконференцсвязи, заданной числовыми параметрами. Представлен график зависимости максимально возможного количества специальных клиентов при заранее заданном общем количестве клиентов и заданном уровне  $P(k_{total}, k_{spec})$ .*

*Ключевые слова:* видеоконференцсвязь, надежность, система массового обслуживания, вероятность получения доступа.

Siberian Journal of Science and Technology. 2017, Vol. 18, No. 2, P. 274–282

**METHODOLOGY OF IMPROVING VIDEO CONFERENCE RELIABILITY**

К. Е. Лебедева\*, Р. В. Лебедев, А. В. Мурыгин

<sup>2</sup>Reshetnev Siberian State University of Science and Technologies  
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russian Federation

\*E-mail: shudrova87@mail.ru

*One of the main problems of organizing a reliable videoconference system is to provide minimum data transfer speed while maintaining maximum speed of audio and video stream processing. Existing software solutions have limitations on number of simultaneous participants in a videoconferencing session, hardware systems are expensive. Today the main methods for improving reliability of videoconferencing systems are methods of load sharing. The authors propose a new technique for increasing the reliability of videoconferencing for authorized users with guaranteed messages delivery and model of probabilistic access to videoconference. The model contains two levels. The top-level model allows describing various videoconference systems taking into account their specific features. The low-level model describes videoconference systems for authorized users with guaranteed message delivery. The model is based on the following concepts: subjects, objects, actions. To determine the probability of full access to a videoconference system consisting of several servers and clients it is necessary to determine the probability of their availability. The mathematical apparatus for evaluating the videoconference system for the standard mode is based on the multi-channel queue system with limited queue, and a set of homogeneous single-channel queue systems with limited queue for special mode.*

Evaluating of effectiveness of special and standard mode is performed by comparing the probability of access failure. For those calculations software developed by the authors is used. At the output software issues a graph in three coordinates  $P(k_{total}, k_{spec}), k_{total}, k_{spec}$ . From the graph for a given level  $P(k_{total}, k_{spec})$  can be defined  $k_{total}$  and  $k_{spec}$ . As the example, the article contains the graph reflecting advisability of using a special mode in a videoconference system specified by numerical parameters. The graph shows the maximum number of special clients for predetermined total number of clients and given level of threshold probability  $P(k_{total}, k_{spec})$ .

*Keywords:* videoconferencing, reliability, queuing system, probability of access.

**Введение.** Увеличение пропускной способности каналов передачи информации сделало видеоконференции удобным средством общения. Видеоконференции проводятся для обмена опытом специалистами в различных областях, проведения корпоративных совещаний, также видеосвязь широко используется в образовательных целях. Системы видеоконференцсвязи активно используются в ракетно-космической отрасли для организации связи между удаленными площадками во время работы над совместными проектами. Одним из приоритетных направлений развития систем видеоконференцсвязи на сегодняшний день является обеспечение их надежности [1]. В сферах применения систем видеоконференцсвязи, связанных с точными операциями (медицина, обучение работе на станке), очень важно поддерживать заданные характеристики качества. Любые искажения могут привести к неправильной трактовке информации и, как следствие, ошибочным действиям участников видеоконференции [2].

**Основные проблемы.** Сложность обеспечения надежности видеоконференцсвязи связана с необходимостью одновременного поддержания высокой скорости обработки информации и передачи данных с минимальными задержками, а также высокого разрешения изображения и качества звука, при этом современным системам желательно обладать дополнительным инструментарием интерактивного взаимодействия.

Существующие решения также плохо совместимы между собой, так как производители не заинтересованы в интеграции различных систем, напротив, система видеоконференцсвязи чаще всего представляет собой единое целое из программных и аппаратных компонентов, масштабировать такую систему возможно, лишь применяя компоненты того же производителя. Такой подход приводит к дороговизне существующих решений.

Одним из перспективных решений проблемы обеспечения надежности видеоконференцсвязи является использование технологий распределения нагрузки сети. Оптимальное распределение сетевой нагрузки позволяет обеспечивать заданные характеристики видеоконференцсвязи за счет управления информационными потоками.

В настоящее время на рынке средств защиты информации в основном представлены средства зарубежного производства, что несет в себе определенную угрозу при использовании таких систем в государственных учреждениях [3]. Все большей популярностью пользуются различные приложения для проведения видеоконференций через глобальные телекоммуникационные сети [4].

Исследования в области видеоконференцсвязи проводились в основном зарубежными учеными: C. Zhou, W. Feng, Z. Zhou, X. Tian, J. Tian (Research on audio-video quality evaluation system of video conferencing system), J. Li, J. Wang, W. Wu, L. Chen (Design and implementation of web video conferencing system based on Red5), W. Simpson (Video over IP: IPTV, Internet video, H.264, P2P, WebTV and Streaming: a complete guide to understanding the technology), H. Yan, Z. Sun, L. Zhang, H. Yuan (A scalable video communications framework based on D-bus), S. Braun, J. Taylor (Video-conference and remote interpreting in legal proceedings), B. Furht, S. W. Smoliar, H. Zhang (Video and image processing in multimedia systems), Z. Kang, L. Yian-Feng (Design of H.323-based MC Gateway subsystem for video conference) и др.

В работах отечественных авторов В. С. Синепола, И. А. Цикина, Д. О. Кривошеи, В. В. Тупицына, А. Власкина, А. И. Савельева и М. А. Прищепы, Е. А. Будникова и Н. А. Филипповой, Т. Ж. Айдынабай и Г. Ж. Шуйтенова, П. П. Кравченко, Н. Ш. Хусаинова и А. Н. Шкурко, В. А. Ягупова, М. В. Стремоухова, О. О. Басова рассматриваются цифровые методы передачи аудио- и видеoinформации в компьютерных сетях, дан анализ состояния работ по компьютерной видеоконференцсвязи в России, рассмотрены основные проблемы отрасли [1; 5–12].

В работах А. И. Савельева, В. В. Прохорова, И. П. Манаковой, А. А. Кузнецова, С. Г. Семенова, С. Н. Симоненко и Е. В. Мелешко рассмотрены способы повышения надежности видеоконференцсвязи. К таким способам относят:

- управление потоками данных, которое достигается упрощением клиентской части приложения и реорганизацией серверной;
- переподключение для смены источников плееров зрителей;
- управление сетевыми ресурсами с помощью статистики;
- динамическое распределение ресурсов сети [8].

Основными методами повышения надежности систем видеоконференцсвязи на сегодняшний день являются:

1. Использование оптимизированных современных протоколов маршрутизации для оптимального и рационального использования канального ресурса системы.
2. Использование алгоритмов децентрализованных самоорганизующихся сетей, которые позволяют распределить нагрузку на все элементы пропорционально их ресурсам и характеристикам, тем самым увеличивая масштабируемость и уменьшая стоимость такого решения при отсутствии необходимости поддержки

протоколов прикладного уровня на сетевом оборудовании [13].

3. Применение механизмов динамического перераспределения скорости передачи информации при совместном обслуживании трафика сервисов реального времени и трафика данных, допускающего задержку [14].

4. Автоматический способ определения текущего говорящего для назначения его потокам мультимедийных данных наибольшего приоритета при передаче остальным участникам [15].

Основным способом применения управления нагрузкой для организации надежной видеоконференцсвязи на сегодняшний день является обеспечение минимальной скорости передачи данных и максимальной скорости обработки аудио- и видеопотока. Для решения этих проблем разработаны кодеки, позволяющие сжимать сигнал и кодировать его для канала связи, а также восстанавливать и декодировать на приемной стороне. Для организации надежного сеанса видеоконференцсвязи требуется кодек, позволяющий сжать видеоданные, сохранив заданные характеристики качества, и канал, по которому эти данные можно будет передать с приемлемой скоростью.

Существует два основных типа решений с точки зрения топологии системы: система с выделенным центром и распределенная система [16]. Использование одного узла в качестве центрального элемента негативно сказывается на характеристиках работы системы в случае проведения сеанса многопользовательской видеоконференцсвязи. Распределенные системы, использующие в качестве канала передачи сеть Интернет, отличаются низким качеством связи. Использование выделенных каналов связи значительно повышает стоимость системы.

Существует проблема стандартизации, необходимость использования специальных технологий и протоколов в зависимости от производителя системы видеоконференцсвязи. Программные решения существенно ограничивают число одновременных участников сеанса видеоконференцсвязи. С другой стороны, применение специальных аппаратных модулей значительно увеличивает стоимость подобных систем.

**Методика повышения надежности.** Авторами предложена новая методика повышения надежности видеоконференцсвязи для авторизованных пользователей с гарантированной доставкой сообщений и модели вероятностного доступа к системам видеоконференцсвязи, пригодные для оценки надежности таких систем. Модель верхнего уровня позволяет описать различные системы видеоконференцсвязи, учитывая их характерные особенности. Модель нижнего уровня

описывает системы видеоконференцсвязи для авторизованных пользователей с гарантированной доставкой сообщений. Полученные вероятностные значения доступа позволяют определить надежность системы, что ранее являлось трудоемкой задачей (в иных реализациях вероятностной модели доступа) или не рассматривалось (в логических моделях доступа). Результаты получены с учетом широко представленных в научной литературе мандатной модели, дискреционной модели и ролевой модели доступа.

Методика повышения надежности систем видеоконференцсвязи состоит из следующих шагов:

1. Определение исходных параметров системы видеоконференцсвязи.

2. Определение требований к надежности через вероятность получения доступа.

3. Построение моделей доступа верхнего и нижнего уровня: определение значения  $P$  – вероятности получения доступа для каждого субъекта.

4. Анализ полученного результата сравнения текущего уровня вероятности доступа с требуемым уровнем вероятности доступа.

5. При необходимости – увеличение вероятности получения доступа с помощью алгоритма повышения надежности.

**Модель вероятностного доступа к информационным ресурсам для повышения надежности видеоконференцсвязи (модель верхнего уровня).**

В ходе исследований была предложена вероятностная модель доступа к системам видеоконференцсвязи, пригодная для оценки надежности таких систем. Разработанная модель позволяет описать различные системы видеоконференцсвязи и учитывает их характерные особенности.

Значение вероятности доступа может быть рассчитано на основе аппарата марковских случайных процессов с дискретными состояниями и непрерывным временем.

Вероятностная модель доступа, предложенная в работе, основана на следующих понятиях: субъекты (*subjects*), объекты (*objects*), действия (*actions*). Для каждого объекта доступным является определенный перечень действий.

Отношения субъектов и объектов представлены в табл. 1, где  $P_{ijk}$  – вероятность совершения действия,  $i$  – количество действий, которые можно выполнить над объектом,  $j$  – количество объектов,  $k$  – количество субъектов. Чтобы получить доступ, субъект должен иметь возможность совершить любое из  $k$  допустимых действий с  $j$  объектами.

Таблица 1

Возможные действия субъектов к объектам

	Object <sub>1</sub>			Object <sub>2</sub>			...	Object <sub>j</sub>		
	subject <sub>1</sub>	...	subject <sub>i</sub>	subject <sub>1</sub>	...	subject <sub>i</sub>		...	subject <sub>1</sub>	...
Action <sub>1</sub>	$P_{111}$	...	$P_{i11}$	$P_{121}$	...	$P_{i21}$	...	$P_{1j1}$	...	$P_{ij1}$
Action <sub>2</sub>	$P_{112}$	...	$P_{i12}$	$P_{122}$	...	$P_{i22}$	...	$P_{1j2}$	...	$P_{ij2}$
...	...	...	...	...	...	...	...	...	...	...
Action <sub>k</sub>	$P_{11k}$	...	$P_{i1k}$	$P_{12k}$	...	$P_{i2k}$	...	$P_{1jk}$	...	$P_{ijk}$

Вероятность получения каждым субъектом полного доступа к каждому объекту выражена формулой:

$$P = \prod_i P_i. \tag{1}$$

Понятие вероятности получения  $i$ -м субъектом доступа к любому объекту для каждого субъекта определено следующим образом:

$$P_i = \prod_j P_{ij}. \tag{2}$$

Вероятность получения доступа субъекта к объекту равна произведению вероятностей всех действий субъекта к объекту:

$$P_{ij} = \prod_k P_{ijk}. \tag{3}$$

Тогда вероятность получения каждым субъектом полного доступа к каждому объекту выражена формулой

$$P = \prod_i \prod_j \prod_k P_{ijk}. \tag{4}$$

**Модель вероятностного доступа к информационным ресурсам для повышения надежности видеоконференцсвязи для авторизованных пользователей с гарантированной доставкой сообщений (модель нижнего уровня).** Рассмотрим пример. Вероятностная модель доступа, предложенная в работе, основана на следующих понятиях: субъекты, объекты, действия. Ниже приведены используемые обозначения.

Субъекты (*subjects*):  $S$  – сервер,  $C$  – клиент.

Объекты (*objects*): видеoinформация (*video*), аудиoinформация (*audio*), файл (*file*), сообщение (*message*), виртуальная доска (*board*).

Действия (*actions*): чтение (*read*), запись (*write*), отправка (*send*), редактирование (*edit*), выполнение (*execute*), удаление (*delete*), создание (*create*).

Для каждого объекта доступным является определенный перечень действий. Отношения субъектов и объектов представлены в табл. 2, где «+» – действие возможно с некоей вероятностью, «-» – действие по отношению к данному объекту не применяется.

Критерий надежности системы сформулирован следующим образом:

$$P \rightarrow 1, \tag{5}$$

Вероятность получения каждым субъектом полного доступа к каждому объекту выражена формулой

$$P = P_s \cdot P_c, \tag{6}$$

где  $P_s$  – вероятность доступности сервера;  $P_c$  – вероятность доступности клиента;

$$P_s = P_{sv} \cdot P_{sa} \cdot P_{sf} \cdot P_{sm} \cdot P_{sb}, \tag{7}$$

где  $P_{sv}$  – доступность видеoinформации на сервере;  $P_{sa}$  – доступность аудиoinформации на сервере;  $P_{sf}$  – доступность файлов на сервере;  $P_{sm}$  – доступность сообщений на сервере;  $P_{sb}$  – доступность виртуальной доски на сервере;

$$P_c = P_{cv} \cdot P_{ca} \cdot P_{cf} \cdot P_{cm} \cdot P_{cb}, \tag{8}$$

где  $P_{cv}$  – доступность видеoinформации у клиента;  $P_{ca}$  – доступность аудиoinформации у клиента;  $P_{cf}$  – доступность файлов у клиента;  $P_{cm}$  – доступность сообщений у клиента;  $P_{cb}$  – доступность виртуальной доски у клиента;

$$P_{sv} = \prod_k P_{svk}, \quad P_{sa} = \prod_k P_{sak}, \quad P_{sf} = \prod_k P_{sfk},$$

$$P_{sm} = \prod_k P_{smk}, \quad P_{sb} = \prod_k P_{sbk},$$

где  $P_{svk}$  – вероятность совершения  $k$ -го действия с видеoinформацией на сервере;  $P_{sak}$  – вероятность совершения  $k$ -го действия с аудиoinформацией на сервере;  $P_{sfk}$  – вероятность совершения  $k$ -го действия с файлами на сервере;  $P_{smk}$  – вероятность совершения  $k$ -го действия с сообщениями на сервере;  $P_{sbk}$  – вероятность совершения  $k$ -го действия с виртуальной доской на сервере;

$$P_{cv} = \prod_k P_{cvk}, \quad P_{ca} = \prod_k P_{cak}, \quad P_{cf} = \prod_k P_{cfk},$$

$$P_{cm} = \prod_k P_{cmk}, \quad P_{cb} = \prod_k P_{cbk},$$

где  $P_{cvk}$  – вероятность совершения  $k$ -го действия с видеoinформацией у клиента;  $P_{cak}$  – вероятность совершения  $k$ -го действия с аудиoinформацией у клиента;  $P_{cfk}$  – вероятность совершения  $k$ -го действия с файлами у клиента;  $P_{cmk}$  – вероятность совершения  $k$ -го действия с сообщениями у клиента;  $P_{cbk}$  – вероятность совершения  $k$ -го действия с виртуальной доской у клиента.

Для определения вероятности полного доступа к системе видеоконференцсвязи, состоящей из нескольких серверов и клиентов, необходимо определить вероятность доступности серверов и вероятность доступности клиентов. Вероятность доступности клиентов в рамках решаемой задачи принята равной 1. Определим вероятность доступности серверов.

Таблица 2

Возможные действия субъектов к объектам

	Video		Audio		File		Message		Board	
	$S$	$C$	$S$	$C$	$S$	$C$	$S$	$C$	$S$	$C$
Read	+	+	+	+	+	+	+	+	+	+
Write	+	+	+	+	+	+	+	+	+	+
Create	-	-	-	-	+	+	+	+	+	+
Edit	-	-	-	-	+	+	+	+	+	+
Execute	-	-	-	-	+	+	+	-	-	-
Delete	-	-	-	-	+	+	+	+	+	+
Send	+	+	+	+	+	+	+	+	-	-

Состояния сервера:

– сервер свободен (или сервер обрабатывает заявки, но принимает новые, поступающие идут на обработку);

– сервер занят обслуживанием заявок и не может больше принимать заявки, все приходящие заявки – в очереди, ограниченной по времени (или неисправен).

$P_0$  – вероятность того, что все серверы свободны;

$P_1$  – вероятность того, что один сервер занят, остальные свободны;

$P_n$  – вероятность того, что все серверы заняты, ноль заявок в очереди;

$P_{n+m}$  – вероятность того, что все серверы заняты,  $m$  заявок в очереди (вероятность отказа) [17].

Математический аппарат оценки системы видеоконференцсвязи строится на основе многоканальных систем массового обслуживания (СМО) с ограниченной очередью для случая стандартного режима работы системы и совокупности однородных одноканальных СМО с ограниченной очередью.

**Модель стандартного режима.** Ниже представлены исходные данные:

$S = \{s_i, i = \overline{1, n}\}$  – множество серверов в системе;

$C = \{c_j, j = \overline{1, k}\}$  – множество клиентов в системе;

$M(S) = n$  – количество серверов в системе;

$M(C) = k$  – количество клиентов в системе.

Для каждого сервера  $s_i \in S$  определено  $\mu_i$  – скорость обработки заявок. Считаем, что все серверы в системе одинаковы со скоростью обработки заявок  $\mu$ :

$$\forall s_i, s_j \in S : \mu_i = \mu_j = \mu. \quad (9)$$

Для каждого клиента  $c_i \in C$  поступающий поток заявок рассматривается как простой пуассоновский процесс интенсивности  $\lambda_i$ . Считаем, что все клиенты в системе имеют одинаковые характеристики и создают поток заявок (пакетов) одинаковой интенсивности:

$$\forall c_i, c_j \in C : \lambda_i = \lambda_j = \lambda_1, \quad (10)$$

$$\lambda = \sum_{i=1}^k \lambda_i = k \lambda_1, \quad (11)$$

где  $\lambda$  – общая интенсивность потока клиентов в системе.

Расчет вероятностей состояния системы:

$$\lambda P_0 = \mu P_1 \rightarrow P_1 = \frac{\lambda}{\mu} P_0, \quad (12)$$

$$\lambda P_1 = 2\mu P_2 \rightarrow \frac{\lambda^2}{\mu} P_0 = 2\mu P_2 \rightarrow P_2 = \frac{1}{2} \frac{\lambda^2}{\mu^2} P_0. \quad (13)$$

Формулы (12) и (13) определяют значение вероятности  $P_i$  для  $i=1, i=2$ . Данные формулы можно использовать в качестве базы для применения метода математической индукции. Сделаем предположение для случая  $i=k$ , запишем формулу для  $P_k$  в следующем виде:

$$P_k = \frac{1}{k!} \frac{\lambda^k}{\mu^k} P_0. \quad (14)$$

Тогда

$$\begin{aligned} \lambda P_k &= (k+1)\mu P_{k+1} \rightarrow P_{k+1} = \\ &= \frac{1}{k+1} \frac{\lambda}{\mu} P_k = \frac{1}{(k+1)!} \frac{\lambda^{k+1}}{\mu^{k+1}} P_0. \end{aligned} \quad (15)$$

Из (15) следует, что формула (14) для  $P_k$  справедлива. Данная формула имеет место для всех  $s_k$ , где  $k \leq n$ .

Для случая  $k > n$  имеем следующий расчет вероятностей:

$$\lambda P_n = n\mu P_{n+1} \rightarrow P_{n+1} = \frac{\lambda}{\mu} \cdot \frac{1}{n} \cdot P_n, \quad (16)$$

$$\lambda P_{n+1} = n\mu P_{n+2} \rightarrow P_{n+2} = \frac{\lambda^2}{\mu^2} \cdot \frac{1}{n^2} \cdot P_n. \quad (17)$$

Указанные выражения (16), (17) определяют значение вероятности  $P_i$  для  $i=n+1, i=n+2$ , они также могут быть рассмотрены в качестве базы математической индукции. Сделаем индуктивное предположение для  $i=t$ :

$$P_{n+t} = \frac{\lambda^t}{\mu^t} \cdot \frac{1}{n^t} \cdot P_n, \quad (18)$$

$$\lambda P_{n+t} = n\mu P_{n+t+1} \rightarrow P_{n+t+1} = \frac{\lambda}{\mu} \cdot \frac{1}{n} \cdot P_{n+t} = \quad (19)$$

$$= \frac{\lambda}{\mu} \cdot \frac{1}{n} \cdot \frac{\lambda^t}{\mu^t} \cdot \frac{1}{n^t} \cdot P_n = \frac{\lambda^{t+1}}{\mu^{t+1}} \cdot \frac{1}{n^{t+1}} \cdot P_n.$$

Из (19) следует, что формула (18) для  $P_t$  справедлива. Данная формула имеет место для всех  $s_t$ , где  $t \leq m$ , где  $m$  – длина очереди СМО.

Исходя из полученных расчетов вероятностей состояний системы, справедливы следующие выражения:

$$P_0 + P_1 + \dots + P_n + P_{n+1} + \dots + P_{n+m} = 1, \quad (20)$$

$$P_0 + \sum_{i=1}^n \left(\frac{\lambda}{\mu}\right)^i \cdot \frac{1}{i!} \cdot P_0 + \sum_{j=1}^m \left(\frac{\lambda}{\mu}\right)^{n+j} \cdot \frac{1}{n^j n!} \cdot P_0 = 1. \quad (21)$$

Отсюда выразим вероятность «нулевого» состояния системы  $P_0$ . Для упрощения записи формулы

примем  $\rho = \frac{\lambda}{\mu}$ :

$$P_0 = \left[ 1 + \sum_{i=1}^n \frac{\rho^i}{i!} + \sum_{j=1}^m \frac{\rho^{j+n}}{n^j n!} \right]^{-1}. \quad (22)$$

Тогда вероятность отказа  $P_{n+m}$  можно представить следующим образом:

$$P_{n+m} = \frac{\rho^{n+m}}{n^m n!} \left[ 1 + \sum_{i=1}^n \frac{\rho^i}{i!} + \sum_{j=1}^m \frac{\rho^{n+j}}{n^j n!} \right]^{-1}. \quad (23)$$

Тогда

$$P = 1 - P_{n+m} = 1 - \left( \frac{\rho^{n+m}}{n^m n!} \left[ 1 + \sum_{i=1}^n \frac{\rho^i}{i!} + \sum_{j=1}^m \frac{\rho^{n+j}}{n^j n!} \right]^{-1} \right).$$

**Модель специального режима.** В специальном режиме системы все клиенты разделяются на группы. Каждая группа клиентов привязывается к определенному серверу. То есть

$$C = \bigcup_{i=1}^n C_i, \bigcap_{i=1}^n C_i = \emptyset, \quad (24)$$

где  $C_i$  – группы клиентов, привязанные к серверу  $i$ .

Без потери общности рассуждений можно полагать, что клиенты распределяются на равные группы:

$$\forall C_i, C_j : M(C_i) = M(C_j) = k/n = \bar{k}.$$

Система в специальном режиме может рассматриваться как совокупность независимых однородных одноканальных СМО с ограниченной очередью и отказами. В этом случае суммарный поток заявок (пакетов) от группы клиентов  $C_i$  для  $i$ -го сервера равен

$$\lambda = \sum_{i=1}^{\bar{k}} \lambda_i = \bar{k} \lambda_1. \quad (25)$$

Интенсивность обработки заявок  $\mu = \text{const}$  для всех состояний системы.

Проведем расчет вероятностей состояний системы в специальном режиме:

$$\lambda P_0 = \mu P_1 \rightarrow P_1 = \frac{\lambda}{\mu} P_0, \quad (26)$$

$$\lambda P_1 = \mu P_2 \rightarrow \frac{\lambda^2}{\mu} P_0 = \mu P_2 \rightarrow P_2 = \frac{\lambda^2}{\mu^2} P_0. \quad (27)$$

По аналогии с расчетами, проведенными для обычного режима, применяя метод математической индукции, получим общую формулу расчета вероятности состояния системы для  $P_k$ :

$$P_k = \left(\frac{\lambda}{\mu}\right)^k P_0. \quad (28)$$

Отсюда, исходя из  $P_0 + P_1 + \dots + P_m = 1$ ,

$$P_0 = \left[ \sum_{i=0}^m \left(\frac{\lambda}{\mu}\right)^i \right]^{-1},$$

$$P_m = \left(\frac{\lambda}{\mu}\right)^m \left[ \sum_{i=0}^m \left(\frac{\lambda}{\mu}\right)^i \right]^{-1} = \rho^m \left[ \sum_{i=0}^m \rho^i \right]^{-1}. \quad (29)$$

**Эффективность методики повышения надежности.** Полагая, что основу системы видеоконференцсвязи составляют серверы видеоконференцсвязи, во время проведения сеанса видеоконференцсвязи справедливо считать количество серверов неизменным,  $n = \text{const}$ . Тогда вероятность отказа будет зависеть только от количества клиентов в системе. Необходимо отметить, что для каждого режима работы системы количество клиентов считается независимым:

$k_{total}$  – общее количество клиентов для стандартного режима;

$k_{spec}$  – общее количество клиентов для специального режима.

Оценка эффективности специального режима по отношению к стандартному выполняется посредством сравнения вероятностей отказа системы в стандартном и специальном режимах для определенных значений  $k_{total}$  и  $k_{spec}$ :

$$P(k_{total}, k_{spec}) = P_{n+m} - P_m. \quad (30)$$

Специальный режим считается эффективным, когда  $P(k_{total}, k_{spec}) > 0$ .

На практике необходимо определить  $k_{total}$  и  $k_{spec}$  при желаемом уровне  $P(k_{total}, k_{spec})$ . Используется программное обеспечение, разработанное авторами. На вход подаются следующие параметры:

- поток от одного клиента;
- скорость обработки запросов сервером;
- длина очереди;
- коэффициент наполнения очереди;
- максимум серверов и клиентов.

На выходе программное обеспечение выдает график в трех координатах  $(P(k_{total}, k_{spec}), k_{total}, k_{spec})$ .

При заданном уровне  $P(k_{total}, k_{spec})$  по графику определяются  $k_{total}$  и  $k_{spec}$ .

На рис. 1 в качестве примера приведен график, отражающий целесообразность использования специального режима в системе видеоконференцсвязи, заданной следующими параметрами:

- $\rho = \lambda_1/\mu = 1/16$  – отношение интенсивности поступления пакетов от одного клиента к интенсивности обработки пакетов сервером;

отношение задано из соображений соотношения количества ядер процессоров для персонального компьютера и вычислительного сервера;

- $n = 5$  – количество серверов в системе;
- $m = \rho^{-1} = 16$  – средняя длина очереди сервера;
- $K = 200$  – общее количество клиентов в системе.

На рис. 2 представлен график зависимости максимально возможного количества специальных клиентов при заранее заданном общем количестве клиентов и заданном уровне  $P(k_{total}, k_{spec})$  (в примере

$(k_{total}, k_{spec}) > 0, 2$ ). Если количество специальных клиентов в системе видеоконференцсвязи меньше максимально возможного, применение алгоритма «Метка привилегий» считается целесообразным при заданном  $P(k_{total}, k_{spec})$ .

Рис. 1 и 2 подтверждают эффективность применяемой методики и определяют границы применимости для заданных числовых значений.

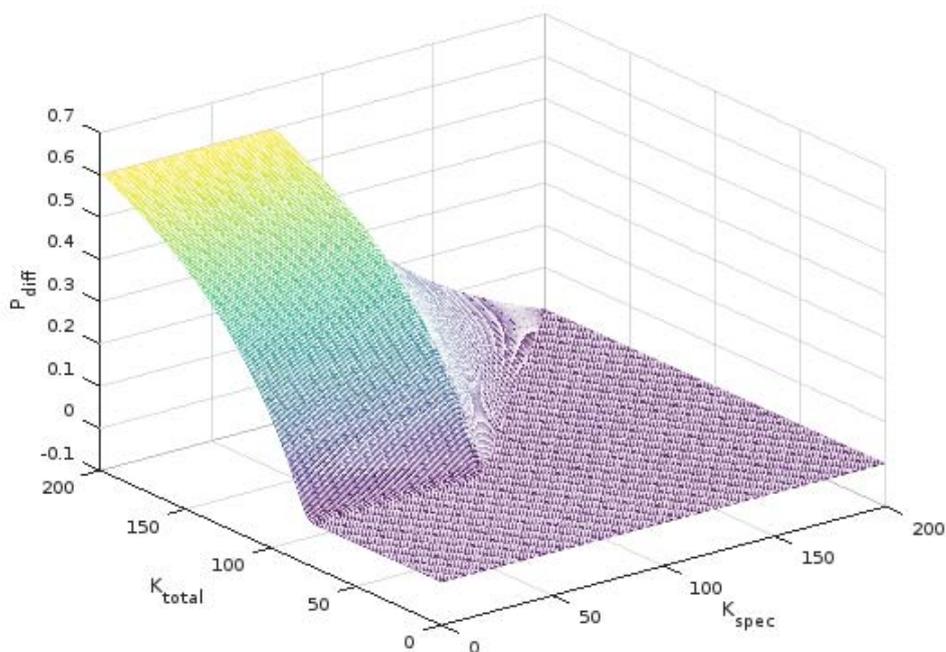


Рис. 1. График эффективности системы видеоконференцсвязи  $(P(k_{total}, k_{spec}), k_{total}, k_{spec})$

Fig. 1. Diagram of effectiveness of videoconference system  $(P(k_{total}, k_{spec}), k_{total}, k_{spec})$

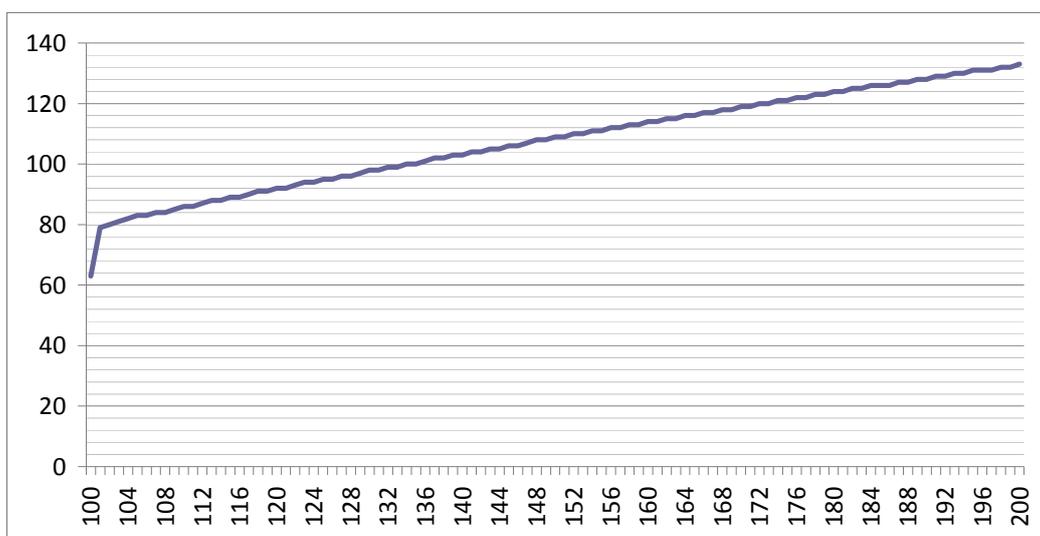


Рис. 2. График эффективности системы видеоконференцсвязи  $(k_{total}, k_{spec})$

Fig. 2. Diagram of effectiveness of videoconference system  $(k_{total}, k_{spec})$

**Заключение.** Разработана новая методика обработки информации, которая путем выделения привилегированного трафика и оптимизации потоков информации позволяет повысить надежность системы видеоконференцсвязи для авторизованных пользователей с гарантированной доставкой сообщений и повысить вероятность получения доступа к ресурсам систем видеоконференцсвязи. Новая модель вероятностного доступа к информационным ресурсам видеоконференцсвязи (модель верхнего уровня и модель

нижнего уровня) позволяет оценить уровень надежности системы видеоконференцсвязи посредством определения вероятности получения доступа к информационным ресурсам. Исследование эффективности предложенной методики повышения надежности подтвердило повышение уровня надежности посредством увеличения вероятности получения доступа к ресурсам системы видеоконференцсвязи путем сравнения вероятностей отказа системы в стандартном и специальном режимах.

**Библиографические ссылки**

1. Синепол В., Цикин И. Системы компьютерной видеоконференцсвязи. М. : ООО «Мобильные телекоммуникации», 1999. 166 с. Сер. «Связь и бизнес».
2. Лебедева К., Томилина А. Алгоритмы и программные решения организации защищенного доступа к компьютерным видеоконференциям // Решетневские чтения : материалы XVIII Междунар. науч. конф., посвященной 90-летию со дня рождения генерального конструктора ракетно-космических систем академика М. Ф. Решетнева (11–14 нояб. 2014, г. Красноярск). В 3 ч. Ч. 2 / СибГАУ. Красноярск, 2014. С. 320–322.
3. Боровик П. Обеспечение информационной безопасности при использовании технологии видеоконференцсвязи в органах внутренних дел // Материалы XVI науч.-практ. конф. Гродно, 2011.
4. Белашенкова Н., Елизаров В., Семерханов И. Исследование проблем обеспечения информационной безопасности при проведении видеоконференций. СПб. : Изд-во Ун-та ИТМО, 2011.
5. Кривошея Д. Подход к оценке функциональной живучести иерархической системы видеоконференцсвязи на беспроводной ячеистой сети : дис. ... к-та техн. наук. Орел, 2014.
6. Тупицын В. Разработка и анализ алгоритма построения топологии сети многоточечной видеоконференцсвязи : дис. ... к-та техн. наук. Ярославль, 2013.
7. Власкин А. Видеоконференцсвязь: прошлое, настоящее, будущее // Интернет-журнал по широкополосным сетям и мультимедийным технологиям. Владивосток : ТОВВМУ, 2015. С. 92.
8. Савельев А., Прищепа М. Архитектура обмена данными без потерь в пиринговом веб-приложении видеоконференцсвязи // Управление, вычислительная техника и информатика : доклады ТУСУР. 2014. № 2. С. 238–245.
9. Будников Е., Филиппов Н. Технологии беспроводной передачи данных для организации видеоконференций // Успехи современного естествознания. 2011. № 7. С. 83.
10. Айдынабай Т., Шуйтенова Г. Технологии передачи данных в системах видеоконференцсвязи // Наука, техника и образование. 2015. № 4(10). С. 77–83.
11. Кравченко П., Хусаинов Н., Шкурко А. Программная система аудиовидеоконференцсвязи для локальных и корпоративных IP-сетей // Программные продукты и системы (Software & Systems). 2004. № 1. С. 27–30.
12. Ягунов В., Стремоухов М., Басов О. Применение пространственной фильтрации в задачах кодирования подвижных изображений // Известия ЮФУ. 2012. С. 123–125.
13. Прохоров В., Манаква И. Построение интернет-видеосистем в условиях существенно ограниченной пропускной способности каналов связи // Аграрный вестник Урала. 2015. № 3 (133). С. 34–38.
14. Павлов А., Датьев И. Протоколы маршрутизации в беспроводных сетях // Труды кольского научно-го центра РАН. Апатиты : КНЦ РАН, 2014. С. 64–75.

15. Коханович Г., Вербицкий И. Метод динамического перераспределения потоков между портами устройства пакетной коммутации, позволяющий увеличить нагрузку сетевого оборудования // Математические машины и системы. Киев : Ин-т проблем математических машин и систем Национальной академии наук Украины, 2005. С. 148–160.
16. Шудрова К. Анализ видов балансировки нагрузки сети // Актуальные проблемы безопасности информационных технологий : материалы II Междунар. науч.-практ. конф. (9–12 сент. 2008, г. Красноярск). / СибГАУ. Красноярск, 2008. С. 86–90.
17. Экономико-математическое моделирование : учеб.-метод. пособие / О. Казаков, С. Миненко, Г. Смирнов. М. : МГИУ, 2006. С. 73–85.

**References**

1. Sinepol V., Cikin I. *Sistemy komp'yuternoy videokonferentsyazi* [Computer video conferencing systems]. Moscow, Mobil'nye telekommunikatsii Publ., 1999, p. 166.
2. Lebedeva K., Tomilina A. [Algorithms and software solutions for secure access to computer video conferencing]. *Reshetnevskie chteniya: materialy XVIII Mezhdunarodnoy nauchnoy konferentsii*. Krasnoyarsk, SibGAU Publ., 2014, Vol. 2, P. 320–322 (In Russ.).
3. Borovik P. *Obespechenie informacionnoj bezopasnosti pri ispolzovanii tehnologii videokonferentsyazi v organah vnutrennih del* [Providing information security when using videoconferencing technology in the internal affairs agencies]. Grodno (Belarus), 2011.
4. Belashenkova N., Elisarov V., Semerhanov I. *Issledovanie problem obespecheniya informatsionnoy bezopasnosti pri provedenii videokonferentsiy* [Investigation of problems of information security in videoconferences]. St. Petersburg, UITMO Publ., 2011.
5. Krivosheya D. *Podhod k ocenke funktsionalnoj zhivuchesti ierarhicheskoy sistemi videokonferentsyazi na besprovodnoj yacheistoy seti*. Dis. kan. tehn. nauk [An approach to assessing the functional survivability of a hierarchical video conferencing system on a wireless mesh network. Dr. techn. sci. diss]. Orel, 2014.
6. Tupicin V. *Razrabotka i analiz algoritma postroenia topologii seti mnogotochechnoy videokonferentsyazi*. Dis. kan. tehn. nauk [Development and analysis of the algorithm for building the topology of the network of multipoint video conferencing. Dr. techn. sci. diss]. Yaroslavl, 2013.
7. Vlaskin A. *Videokonferentsyaz: proshloe, nastoyashee, budushee* [Videoconferencing: past, present, future]. Vladivostok, TOVVMU Publ., 2015, P. 92.
8. Saveljev A., Prishepa M. [Lossless data exchange architecture in peer-to-peer videoconferencing Web applications]. *Doklady TUSURa*. 2014, No. 2, P. 238–245 (In Russ.).
9. Budnikov E., Filippov N. [Wireless data transmission technologies for video conferencing]. *Uspekhii sovremennogo estestvoznaniya*. 2011, No. 7, P. 83 (In Russ.).
10. Ajdinabaj T., Shujtenova G. [Technologies of data transmission in videoconferencing systems]. *Nauka, tekhnika i obrazovanie*. 2015, No. 4(10), P. 77–83 (In Russ.).

11. Kravchenko P., Husainov N., Shkurko A. [Software audio-video conferencing system for local and corporate IP networks]. *Programmnye produkty i sistemy (Software & Systems)*. 2004, No. 1, P. 27–30 (In Russ.).
12. Yagupov V., Stremouhov V., Basov O. [Application of spatial filtering in moving picture encoding problems]. *Izvestiya YuFU*. 2012, P. 123–125 (In Russ.).
13. Prohorov V., Manakova I. [The construction of Internet video systems in conditions of significantly limited bandwidth channels]. *Agrarnyy vestnik Urala*. 2015, No. 3 (133), P. 34–38 (In Russ.).
14. Pavlov A., Datjev I. *Protokoli marshrutizatsii v besprovodnih setyah* [Routing protocols in wireless networks]. Apatiti, Murmanskaya obl.: KNC RAN Publ., 2014, P. 64–75.
15. Kohanovich G., Verbickij I. [The method of dynamic redistribution of flows between the ports of the packet switching device, which allows increasing the load of network equipment]. *Matematicheskie mashiny i sistemy*. 2005, P. 148–160 (In Russ.).
16. Shudrova K. *Analiz vidov balansirovki nagruzki seti* [Analysis of types of network load balancing]. Krasnoyarsk, SibGAU Publ., 2008, P. 86–90.
17. Kazarov O., Minenko S., Smirnov G. *Ekonomiko-matematicheskoe modelirovanie* [Economic-mathematical modeling]. Moscow, MGIU Publ., 2006, P. 73–85.

© Лебедева К. Е., Лебедев Р. В.,  
Мурыгин А. В., 2017