ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ
INFOCOMMUNICATION TEGHNOLOGIES

УДК 004.724.4
DOI 10.18413/2411-3808-2018-45-3-584-593

МОДЕЛИРОВАНИЕ ПОТОКОВ ДАННЫХ РЕАЛЬНОГО ВРЕМЕНИ В ЗАЩИЩЕННЫХ КОРПОРАТИВНЫХ МУЛЬТИСЕРВИСНЫХ СЕТЯХ СВЯЗИ НА ОСНОВЕ ДЕТЕРМИНИРОВАННОГО СЕТЕВОГО ИСЧИСЛЕНИЯ

THE REAL-TIME DATA STREAMS MODELLING IN SECURE CORPORATE MULTISERVICE COMMUNICATION NETWORKS BY APPLICATION OF DETERMINISTIC NETWORK CALCULUS THEORY

Д.В. Шелковый [1], О.Ю. Миронов [1], О.О. Басов [2]
D.V. Shelkovyy [1], O.Y. Mironov [1], O.O. Basov [2]

[1] Федеральное государственное казённое военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации», Россия, 302014, г. Орёл, ул. Приборостроительная, 35
[2] Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Россия, 197101, г. Санкт-Петербург, Кронверкский пр., 49

[1] The Federal state government military educational institution of higher education «The Academy of the Federal Guard Service of the Russian Federation», 35 Priborostroitelnaya St, Orel, 302014, Russia
[2] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, 49 Kronverkskiy ave, Saint-Petersburg, 197101, Russia

E-mail: shelkovoydenis@mail.ru, mironnn101992@mail.ru, oobasov@mail.ru

Аннотация
В статье представлены экспериментальные результаты применения существующего математического аппарата теории детерминированного сетевого исчисления к обслуживанию потоков данных реального времени в защищенных корпоративных мультисервисных сетях связи (ЗКМСС). Для получения оценок достижимого уровня качества обслуживания (КО) проведено исследование параметров пиковой, средней скоростей передачи данных, а также длин пакетов, генерируемых терминальными аппаратами ЗКМСС, и межпакетного интервала. Полученные результаты свидетельствуют о невозможности обеспечения заданной задержки обработки пакетов в пограничном маршрутизаторе ЗКМСС при резервировании канального ресурса по существующим математическим моделям узла группирования. В настоящей работе доказано, что при обслуживании потоков IP-телефонии достижимая задержка превышает требуемую во всем исследуемом диапазоне изменения количественного состава одновременно обрабатываемых потоков данных в пограничном маршрутизаторе. При обслуживании потоков видеотелефонии заданный уровень КО обеспечивается за счет резервирования ресурса, значительно превышающего достижимую пиковую скорость передачи данных.

Abstract
The investigation results of using guaranteed quality of service models with real time traffic in the secure corporate multiservice communication networks are presented in this paper. First of all the authors measured the peak and the mean data transmit speed, packet lengths and time between packets after terminal equipment using in secure corporate multiservice communication networks. These data were included in mathematical apparatus of deterministic network calculus theory for the real-time data streams modelling. The application results are witnessed about the inability to provide a specified delay-processing package

in a border router, using guaranteed quality of service models, when grouping voice over IP data streams. More than that, in this paper the authors proved that application these models to description the speed parameters of video telephone data streams group, the real QoS complies with desired service, but only thanks to bandwidth over reserve. This paper consists of the introduction where the authors paid much attention to the relevance of the study, the theoretical analysis of existing mathematical network calculus models that supplies the readers by common definitions and terms of its applying, the experimental study of the adequacy of existing math models, the investigation results and conclusion.

Ключевые слова: защищенная корпоративная мультисервисная сеть связи, качество обслуживания, криптотуннель, теория детерминированного сетевого исчисления, пропускная способность.
Keywords: secure corporate multiservice communication networks, quality of service, criptotunnel, deterministic network calculus theory, bandwidth.

Введение

В процессе информатизации происходит существенное расширение информационного пространства каждого отдельного гражданина, которое потенциально может достигать размеров информационного пространства страны. В своей деятельности индивид (в соответствии со своими социальными правами и статусом, субъективными желаниями и возможностями) имеет необходимость (или склонность) к потреблению информации, выходящей за рамки традиционной совокупности услуг связи и информатизации, предоставляемых существующими инфокоммуникационными системами. Так, в настоящее время все больше наблюдаются процессы слияния или взаимопроникновения традиционных услуг связи, появление новых информационных технологий, позволяющих пользователям расширять функциональность абонентских терминалов инфокоммуникационных систем, интеллектуализировать последние с целью комфортного обслуживания пользователей [Basov, 2017; Указ Президента РФ от 09.05.2017 № 203, 2017].

При наблюдаемом сегодня росте числа компьютерных атак на инфраструктуру и ресурсы информационного пространства существующие технические средства инфокоммуникационных систем оказываются функционально ограниченными и не обеспечивают требуемого уровня защиты обрабатываемой информации на прикладном уровне модели ЭМВОС. В данных условиях важнейшим принципом построения интеллектуальных инфокоммуникационных систем является развертывание защищенных корпоративных мультисервисных сетей связи (ЗКМСС). Реализация этого принципа обуславливает необходимость модернизации ЗКМСС в направлении предоставления актуальных широкополосных интерактивных сервисов [Ефимов, 2006; Указ Президента РФ от 17.03.2008 № 351, 2015; Указ Президента РФ от 05.12.2016 № 646, 2016].

ЗКМСС технологически представляют собой виртуальные частные сети (VPN) с двухуровневой архитектурой телекоммуникационной плоскости: транспортной сетью и сетью доступа [Захватов, 2001; Росляков, 2006; Бакланов, 2008]. На границе данных сетей устанавливаются программные и аппаратные средства криптографической защиты информации (СКЗИ), функционирующие, как правило, в качестве криптошлюза [Приказ ФСТЭК РФ от 18.02.2013 № 21, 2013; Миронов, 2017]. Выбор данного способа использования СКЗИ в ЗКМСС обусловлен не только потребностью в снижении экономических затрат на создание защищенного контура обработки информации, но и необходимостью управления канальным ресурсом, приоритезацией трафика, допуском потоков данных реального времени (ПДРВ), их маршрутизацией и фильтрацией.

На выходе СКЗИ потоки данных агрегируются в криптотуннели, а их идентификация на маршрутизаторах, расположенных в открытой сети, становится возможной только по IP-адресам внешних портов СКЗИ источника и получателя соответственно. Вышеуказанная особенность защищенных сетей связи вносит определенные сложности в надстройку архитектуры интегрированного обслуживания потоков данных IntServ. Так, применение СКЗИ в туннельном режиме приводит к шифрованию полезных данных заголовка транспортного уровня, информация которого используется протоколом сигнализации Resource reservation protocol (RSVP) архитектуры IntServ для резервирования требуемых канальных ресурсов на всех маршрутизаторах сети направления «из конца в конец».

Пакеты данных, принадлежащие различным сеансам связи, нумеруются в порядке их поступления в криптомодуль СКЗИ для зашифрования. Нарушение очередности прибытия пакетов в СКЗИ, за которым расположены терминалы-приемники, расценивается как возможная атака злоумышленника, в результате чего взаимодействующие криптомаршрутизаторы могут повторно воспроизвести стадии вхождения в синхронизм, привести к аутентификации сторон и обмену ключевой информацией, что, несомненно, приведет к снижению уровня качества обслуживания (КО) ПДРВ, оцениваемого с позиции транспортировки пакетов [Recommendation Y. 1541, 2000; Morton, Claise, 2009; Миронов, 2015]. Для избежания этого требуется производить обработку всех пакетов данных группированного потока (трафика криптотуннеля) в маршрутизаторах одинаково, т.е. в одном буфере с одной дисциплиной обслуживания. Однако доказано, что обслуживание группированного потока позволяет минимизировать ресурсопотребление за счет возникновения эффекта статистического мультиплексирования потоков данных с переменной скоростью, заключающегося в маловероятном наступлении события одновременной передачи данных несколькими источниками на пиковой скорости [Кучерявый, 2004; Шелковый, Саитов и др., 2017; Шелковый, Фокин и др., 2017].

В настоящее время рабочими группами Internet Engineering Task Force (IETF) разработаны подходы к описанию параметров группированного трафика на основе теории детерминированного сетевого исчисления [LeBoudec, 2000], в которых учитывается служебная информация, транслируемая в сообщениях протокола RSVP о параметрах генерируемых потоков и требованиях к уровню качества их обслуживания. Разработанные математические модели позволяют гарантировать максимально достижимую задержку обработки пакетов ПДРВ «из конца в конец» при заданной конфигурации механизмов формирования трафика на всех промежуточных сетевых устройствах или позволяют решить альтернативную задачу – при заданной максимально допустимой задержке «из конца в конец» оценивают необходимую пропускную способность для заданной группы потоков.

С учетом существующих технических сложностей функционирования RSVP в сетях связи, использующих протоколы шифрования IPSec [Berger, O'Malley, 1997], в настоящей работе производится практическое исследование применимости разработанных моделей к зашифрованным потокам данных IP-телефонии и видеотелефонии.

Теоретический анализ существующих математических моделей детерминированного сетевого исчисления

В теории детерминированного сетевого исчисления поток данных на выходе формирователя трафика «корзина маркеров» и «дырявое ведро» ограничивается некой детерминированной кусочно-линейной функцией, называемой функцией входящего потока $A_i(t)$ [Boudec, 1998]. В служебном сообщении RSVP Sender_TSpec передается информация о потоке данных, генерируемом источником и требуемом уровнем обслуживания посредством настройки механизма «дырявое ведро» с ориентацией на нижеперечисленные параметры: r_i – средняя скорость генерации «жетонов», байт/с; b_i – размер буфера («ведра»), байт; p_i – пиковая скорость генерации «жетонов», байт/с; L_i – максимальный размер передаваемого кадра, байт.

Поведение потока данных с точки зрения наихудшего возможного случая расположения пакетов на выходе механизма «корзина с маркерами» приобретает детерминированный характер (выражение 1):

$$A_i(t) = \begin{cases} L_i + p_i t & t < \dfrac{b_i - L_i}{p_i - r_i} \\ b_i + r_i t & t \geq \dfrac{b_i - L_i}{p_i - r_i} \end{cases}, \; p_i > r_i . \qquad (1)$$

Поток на выходе узла коммутации при резервировании доли пропускной способности канала связи R_i (байт/с) описывается функцией обслуживания $W_i(t)$ (выражение 2), определяющей минимальный объем переданных в канал связи данных:

$$W_i(t) = R_i\left(t - t_{\text{зап}}\right), \tag{2}$$

где $t_{\text{зап}i} = \frac{L_i}{R_i} + \frac{L_{mtu}}{R}$ – время запаздывания в обслуживании пакетов i-го потока из буфера, из-за обслуживания кадра максимальной длины (Maximum Transfer Unit) L_{mtu} платой линейного интерфейса, с; R – пропускная способность выходного порта узла коммутации (на канальном уровне).

Совместное рассмотрение двух функций для потоков данных с переменной скоростью передачи ($p_i > r_i$) позволяет получить верхние граничные значения возможной задержки пакета $t_{\max}$ в узле коммутации при выделенном ресурсе R_i:

$$t_{\max} = \begin{cases} \dfrac{(b_i - L_i)(p_i - R_i)}{R_i(p_i - r_i)} + \dfrac{2L_i}{R_i} + \dfrac{L_{mtu}}{R}, & p_i \ge R_i \ge r_i \\ \dfrac{2L_i}{R_i} + \dfrac{L_{mtu}}{c}, & R_i \ge p_i \ge r_i \end{cases} \tag{3}$$

Эффект в ресурсопотреблении при групповом обслуживании потоков данных будет наблюдаться только при резервировании для каждого потока канального ресурса, ориентированного на эффективную скорость передачи данных, т.е. при выполнении условия:

$$p_i \ge R_i \ge r_i . \tag{4}$$

Введем параметр максимальной длительности передачи «пачки» пакетов (Maximum Burst Duration) как $t_{MBDi} = \frac{b_i - L_i}{p_i - r_i}$ и параметр гарантированной задержки обработки пакета i-го, находящегося в буфере узла коммутации $t_{\max i}$, оцениваемые в секундах.

С учетом вышеизложенного объемные характеристики потоков данных на выходе формирователя трафика «корзина с маркерами» и узла коммутации представлены на рисунке 1.

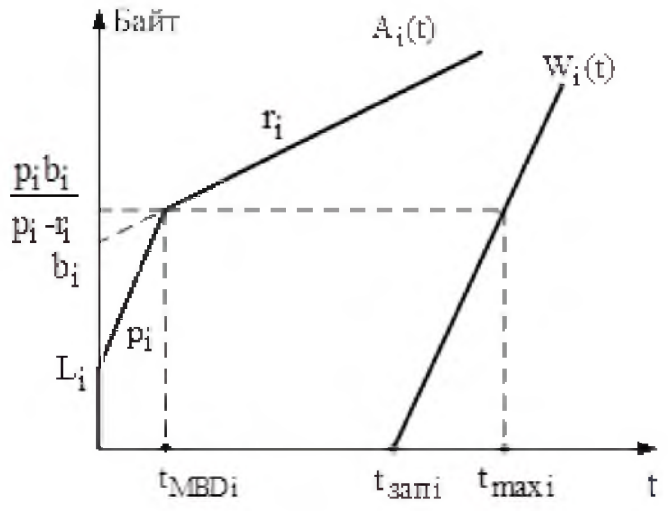

Рис. 1. Графическое представление объемных характеристик потоков данных на выходе формирователя трафика и узла коммутации

Fig. 1. Graphical representation of output data streams volumetric characteristics

При эксплуатации сети связи зачастую возникает обратная задача: на основании выражения (3) при заданной допустимой задержке передачи пакета через узел коммутации требуется оценить необходимый канальный ресурс:

$$R_i = \frac{p_i \dfrac{(b_i - L_i)}{(p_i - r_i)} + 2L_i}{t_{\max i} + \dfrac{(b_i - L_i)}{(p_i - r_i)} - \dfrac{L_{mtu}}{R}}, \quad p_i \geq R_i \geq r_i . \tag{5}$$

Оценка требуемого буферного пространства маршрутизатора в данной работе не рассматривается в связи с тем, что стоимость элементов памяти значительно меньше, чем стоимость линий связи, предоставляющих заданную пропускную способность.

В настоящее время в рамках теории детерминированного сетевого исчисления применяются следующие математические модели: модель изолированного обслуживания потоков данных и модель группового обслуживания потоков данных на основе суммарной функции поступления (СФП).

Модель изолированного обслуживания представляет собой простейший способ оценивания суммарного канального ресурса для группированного потока как суммы требуемых значений канального ресурса для каждого потока, входящего в состав данной группы:

$$R^{\text{ИЗОЛ}}(n) = \sum_{i=1}^{n} \frac{p_i \dfrac{(b_i - L_i)}{(p_i - r_i)} + L_i + \max(L_i)}{t_{\max} + \dfrac{(b_i - L_i)}{(p_i - r_i)} - \dfrac{L_{mtu}}{R}}. \tag{6}$$

Модель группового обслуживания потоков данных на основе суммарной функции поступления (СФП) является усовершенствованной моделью, позволяющей снизить ресурсопотребление за счет однократного учета появления ошибок планирования для всех потоков группы:

$$R^{\text{СФП}}(n) = \frac{\sum_{i=1}^{n} p_i \dfrac{\sum_{i=1}^{n} b_i - \max(L_i)}{\sum_{i=1}^{n} p_i - \sum_{i=1}^{n} r_i} + \max(L_i) + L_{mtu}}{\min(t_{\max i}) + \dfrac{\sum_{i=1}^{n} b_i - \max(L_i)}{\sum_{i=1}^{n} p_i - \sum_{i=1}^{n} r_i} - \dfrac{L_{mtu}}{R}}. \tag{7}$$

Модель на основе СФП дает завышенную оценку поступающей нагрузки при суммировании однотипных параметров для неоднородных потоков, что может свести к нулю эффект ресурсопотребления.

Экспериментальное исследование адекватности существующих математических моделей детерминированного сетевого исчисления

С целью идентификации параметров устанавливаемых сеансов связи и требуемого уровня КО, транслируемых в сеть с оконечного терминального оборудования с помощью сигнального протокола RSVP, была собрана схема сегмента сети, представленная на рисунке 2.

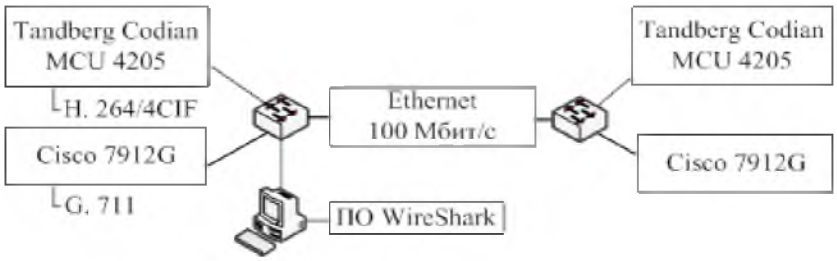

Рис. 2. Схема сегмента сети для анализа параметров трафика, генерируемого оконечным терминальным оборудованием
Fig. 2. Network diagram for analysis of traffic parameters generated by termimal equipment

Полученные численные значения параметров представлены в таблице.

Таблица
Table

Численные значения транслируемых параметров
Numerical values of translated parameters

Значения транслируемых параметров трафика в запросах на резервирование ресурса при предоставлении услуг							
VoIP (G.711) Терминал Cisco 7912G				Video over IP (H.264/4CIF) Терминал Tandberg Codian MCU 4205			
p_i, кбит/с	b_i, кбайт	r_i, кбит/с	L_i, байт	p_i, Мбит/с	b_i, кбайт	r_i, Мбит/с	L_i, байт
112	8000	96	214	2,1	8000	0,87	1346

Данные значения параметров трафика использовались при расчете требуемого канального ресурса при группировании 100 потоков IP-телефонии и 40 потоков видеотелефонии. Рассчитанные значения требуемого канального ресурса в зависимости от количества установленных сеансов связи при описании группированного потока как суммы изолированных, а также на основе СФП при максимально допустимой задержке обработки пакета группового потока, в пограничном маршрутизаторе равной 5 мс, для трафика IP-телефонии представлены на рисунке 3, для видеотелефонии – на рисунке 4.

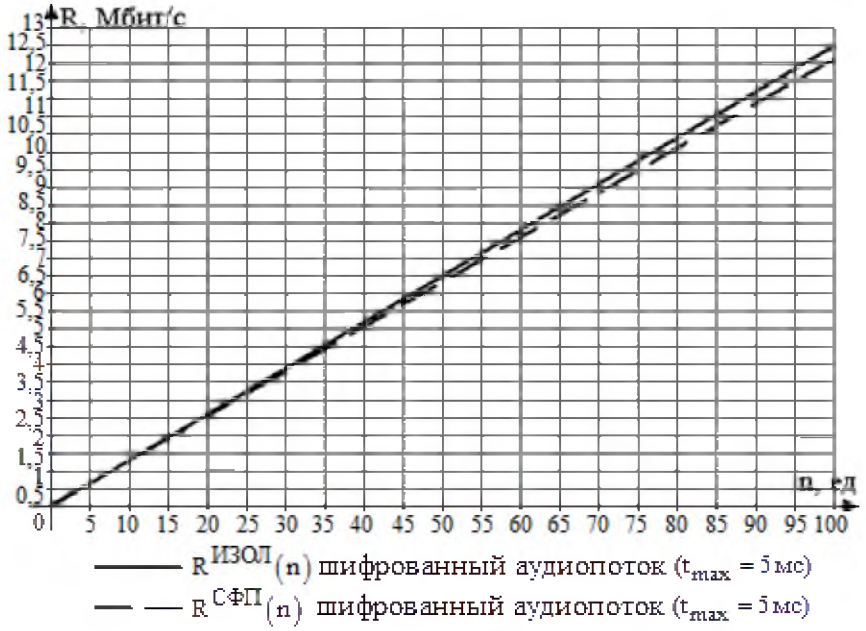

Рис. 3. Оценка требуемого канального ресурса для обслуживания трафика IP-телефонии с заданной задержкой
Fig. 3. The required bandwidth estimation for providing a specified delay-processing package for VoIP streams

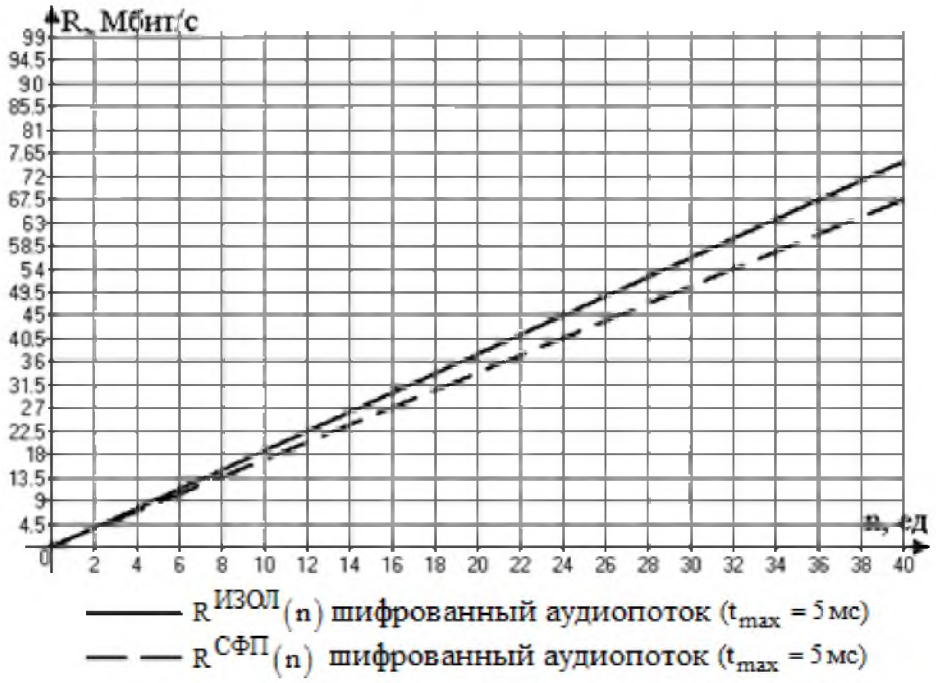

Рис. 4. Оценка требуемого канального ресурса для обслуживания трафика видеотелефонии с заданной задержкой

Fig. 4. The required bandwidth estimation for providing a specified delay-processing package for Video over IP streams

Результаты экспериментального исследования

Максимально достижимая задержка обработки пакета в маршрутизаторе исследовалась с помощью полунатурного эксперимента. Источником требуемого количества сеансов связи с заданными характеристиками пиковой и средней скоростей выступал генератор трафика IXIA XM12. Задержка пакетов при распространении в транспортной MPLS сети воспроизводилась эмулятором IP-каналов IXIA ANUE. Длительность оценивания максимально достижимой задержки составляла 5 мин., что в 3 раза превышает среднюю длительность сеанса связи, согласно статистическим данным, используемым при проектировании сетей телефонной связи [РД 45.120, 2000].

Структурная схема стенда для исследования с сетевым и криптографическим оборудованием, применяемым в ЗКМСС, представлена на рисунке 5.

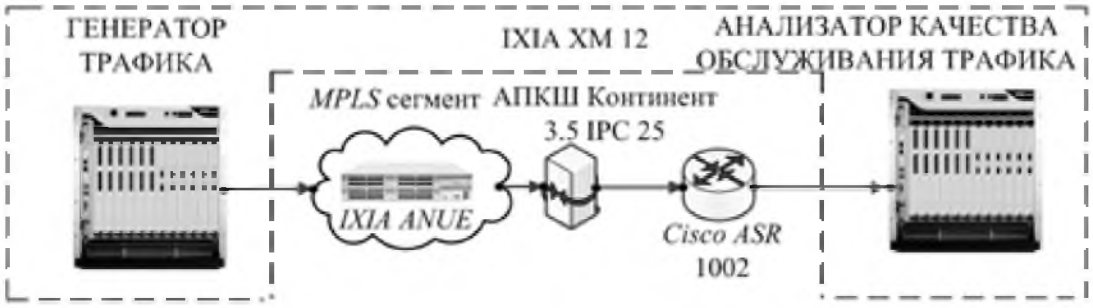

Рис. 5. Структурная схема стенда защищенной корпоративной мультисервисной сети связи

Fig. 5. The structural stand scheme of secure corporate multiservice communication network

Оцененные максимальные значения достижимой задержки для трафика IP-телефонии и видеотелефонии, а также кривая, соединяющая их средние значения в течение опыта, представлены на рисунках 6 и 7 соответственно.

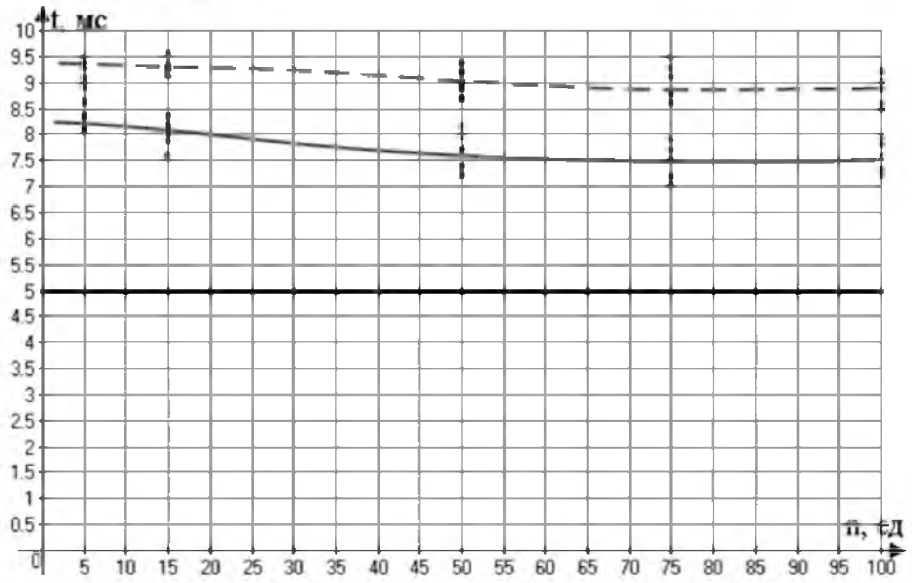

Рис. 6. Экспериментальное оценивание максимально достижимой задержки в пограничном маршрутизаторе (IP-телефония)
Fig. 6. The experimental estimation of the maximum achievable delay in a border router (VoIP)

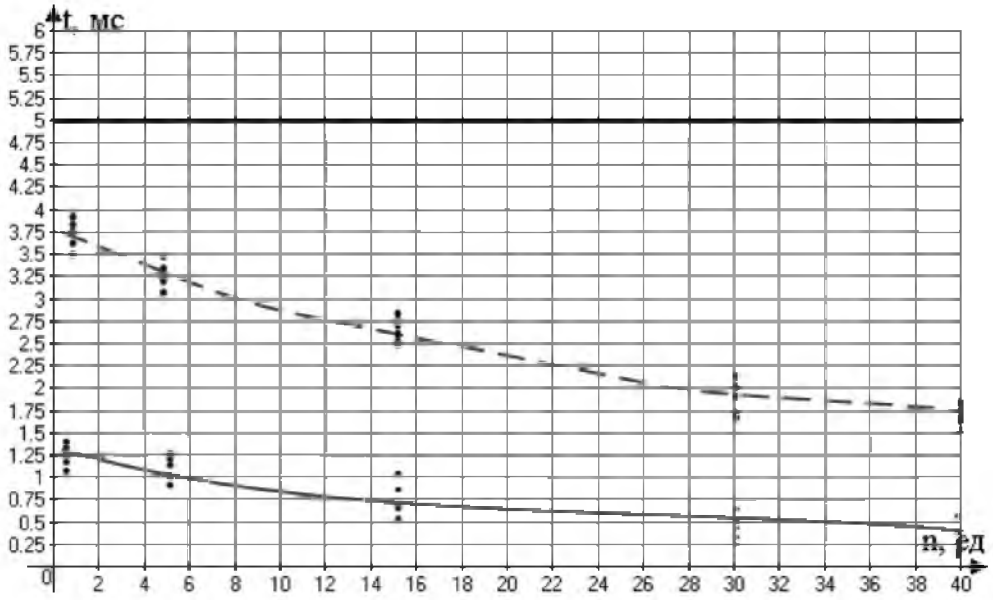

Рис. 7. Экспериментальное оценивание максимально достижимой задержки в пограничном маршрутизаторе (видеотелефония)
Fig. 7. The experimental estimation of the maximum achievable delay in a border router (Video over IP)

На основании анализа полученных зависимостей можно сделать вывод о том, что применение существующего математического аппарата оценивания требуемого канального ресурса для обслуживания группированного потока IP-телефонии не позволяет обеспечить заданной задержки обработки пакетов данных в пограничном маршрутизаторе. При обслуживании потоков видеотелефонии заданный уровень качества обслуживания обеспечивается.

Заключение

По мнению авторов, вышеизложенное свидетельствует о несоответствии скорости поступления пакетов скорости их обслуживания: в первом случае выделенный канальный ресурс меньше пиковой скорости передачи, во втором, наоборот, превышает ее. Незначи-

тельный разброс экспериментальных оценок достижимой задержки при различных опытных итерациях сводит к минимуму возможность проявления случайных выбросов.

Неадекватное оценивание требуемого канального ресурса для обслуживания группированного потока видится во влиянии СКЗИ на долгосрочные параметры генерируемого трафика (пиковую и среднюю скорости передачи данных). Исследование и учет данного влияния позволит добиться более точного описания параметров группированного потока, что, в свою очередь, позволит гарантировать качество обслуживания.

Работа выполнена при финансовой поддержке фонда РФФИ (проект № 18-07-00380).

Список литературы
References

1. Бакланов И.Г. 2008. NGN: принципы построения и организации. М., Эко-Трендз, 400.

Baklanov I.G. 2008. NGN: principy postroeniya i organizacii. M., EHko-Trendz, 400. (in Russian)

2. Ефимов А.А. 2006. Информационная безопасность ОАО «Газпром»: проблемы гиганта. Information Security/Информационная безопасность, 5: 4–6.

Efimov A.A. 2006. Informacionnaya bezopasnost' OAO «Gazprom»: problemy giganta. Information Security/Informacionnaya bezopasnost', 5: 4–6. (in Russian)

3. Захватов М.А. 2001. Построение виртуальных частных сетей на базе технологии MPLS. Cisco Systems Технология и протоколы MPLS, 47.

Zahvatov M.A. 2001. Postroenie virtual'nyh chastnyh setej na baze tekhnologii MPLS. Cisco Systems Tekhnologiya i protokoly MPLS, 47. (in Russian)

4. Кучерявый Е.А. 2004. Управление трафиком и качество обслуживания в сети Internet. СПб., Наука и техника, 336.

Kucheryavyj E.A. 2004. Upravlenie trafikom i kachestvo obsluzhivaniya v seti Internet. SPb., Nauka i tekhnika, 336. (in Russian)

5. Министерство РФ по связи и информатизации. 2000. РД 45.120-2000. Нормы технологического проектирования: городские и сельские телефонные сети. М., 128.

Ministerstvo RF po svyazi i informatizacii. 2000. RD 45.120-2000. Normy tekhnologicheskogo proektirovaniya: gorodskie i sel'skie telefonnye seti. M., 128. (in Russian)

6. Миронов О.Ю. 2015. Обеспечение гарантированного обслуживания потоков данных в мультисервисных сетях связи промышленного назначения. В кн.: Сборник материалов XVIII Международной молодежной научно-практической конференции «ИНФОКОМ-2015» в СКФ МТУСИ. Ч. 1. Ростов-на-Дону, Изд-во МТУСИ: 202–205 .

Mironov O.YU. 2015. Software guaranteed service data flows in multiservice networks of industrial purpose. In: Sbornik materialov XVIII Mezhdunarodnoj molodezhnoj nauchno-prakticheskoj konferencii «INFOKOM-2015» v SKF MTUSI. CH.1. Rostov-na-Donu, Izd-vo MTUSI: 202–205. (in Russian, with English summary)

7. Миронов О.Ю. 2017. Обеспечение защищенной передачи данных в сетях VPN. В кн.: Сборник докладов XXII Международной открытой научной конференции «Современные проблемы информатизации», Воронеж, Изд-во ВГТУ: 133–137.

Mironov O.Yu. 2017. Obespechenie zashchishchennoj peredachi dannyh v setyah VPN. In: Sbornik dokladov XXII mezhdunarodnoj otkrytoj nauchnoj konferencii «Sovremennye problemy informatizacii», Voronezh, Izd-vo VGTU: 133–137. (in Russian)

8. Приказ ФСТЭК РФ от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», М., 2013.

Prikaz FSTEHK RF ot 18.02.2013 № 21 «Ob utverzhdenii sostava i soderzhaniya organizacionnyh i tekhnicheskih mer po obespecheniyu bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah personal'nyh dannyh», M., 2013. (in Russian)

9. Росляков А.В. 2006. Виртуальные частные сети. Основы построения и применения. М., Эко-Трэндз, 304.

Roslyakov A.V. 2006. Virtual'nye chastnye seti. Osnovy postroeniya i primeneniya. M., EHko-Trehndz, 304. (in Russian)

10. Указ Президента РФ от 17.03.2008 № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», М., 2008.

Ukaz Prezidenta RF ot 17.03.2008 № 351 (red. ot 22.05.2015) «O merah po obespecheniyu informacionnoj bezopasnosti Rossijskoj Federacii pri ispol'zovanii informacionno-telekommunikacionnyh setej mezhdunarodnogo informacionnogo obmena», M., 2008. (in Russian)

11. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении доктрины информационной безопасности Российской Федерации», М., 2016.

Ukaz Prezidenta RF ot 05.12.2016 № 646 «Ob utverzhdenii doktriny informacionnoj bezopasnosti Rossijskoj Federacii», M., 2016. (in Russian)

12. Указ Президента РФ от 09.05.2017 № 203 «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», М., 2017.

Ukaz Prezidenta RF ot 09.05.2017 № 203 «O strategii razvitiya informacionnogo obshchestva v Rossijskoj Federacii na 2017 – 2030 gody», M., 2017. (in Russian)

13. Шелковый Д.В., Саитов И.А., Басов О.О., Романюк О.В. 2017. Модель узла коммутации корпоративной мультисервисной сети связи. Научные ведомости Белгородского государственного университета, 9 (258): 148–156.

SHelkovyj D.V., Saitov I.A., Basov O.O., Romanyuk O.V. 2017. Model' uzla kommutacii korporativnoj mul'tiservisnoj seti svyazi. Nauchnye vedomosti Belgorodskogo gosudarstvennogo universiteta, 9 (258): 148–156. (in Russian, with English summary)

14. Шелковый Д.В., Фокин А.Б., Корнилов С.А. 2017. Исследование математической модели узла коммутации защищенной корпоративной мультисервисной сети связи. Экономика и менеджмент систем управления, 2 (2): 291–300.

15. Shelkovyj D.V., Fokin A.B., Kornilov S.A. 2017. The analysis of the protected company multiservice network node mathematical model. Ehkonomika i menedzhment sistem upravleniya, 2 (2): 291–300. (in Russian, with English summary)

16. Basov O.O. 2017. Principles of constructing polymodal infocommunication systems for information space user service. In: 11th IEEE International Conference on Application of Information and Communication Technologies (AICT2017), 70–75.

17. Berger L., O'Malley T. 1997 Requests for comments 2207. RSVP Extensions for IPSEC Data Flows. Available at: http://tools.ietf.org/html/rfc2207 (accessed 20 мая 2018).

18. Boudec J. 1998. Application of Network Calculus To Guaranteed Service Networks. IEEE Trans. on Information Theory, 44 (3). Available at: https://infoscience.epfl.ch/record/27/files/LeBoudec98.pdf. (accessed 20 мая 2018).

19. LeBoudec J.Y. 2000. A proven delay bound for a network with aggregate scheduling. (Technical Report DSC2000/002, EPFLDSC). Available at: https://mfoscience.epfl.ch/record/52333/files/IC_TECH_REPORT_200002.pdf (accessed 20 мая 2018).

20. Morton A., Claise B. 2009. Requests for comments 5481. Packet delay variation applicability statement. Available at: http://tools.ietf.org/html/rfc5481 (accessed 20 мая 2018).

21. Recommendation Y.1541. 2000. Networks Performance Objectives for IP Based Services . ITU-T. Available at: https://www.itu.int/rec/T-REC-Y.1541-201112-I/en (accessed 20 мая 2018).