

ПОВЫШЕНИЕ ВЕРОЯТНОСТИ ДОСТАВКИ СООБЩЕНИЙ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр Дреев, Алексей Смирнов

Кировоградский национальный технический университет, Украина



ДРЕЕВ Александр Николаевич

Год и место рождения: 1976 год, г. Кировоград, Украина.

Образование: Кировоградский государственный педагогический университет им. В.В. Винниченко, 1999 год.

Должность: ассистент кафедры программного обеспечения с 2002 года.

Научные интересы: сжатие информации, телекоммуникационные системы, численные методы.

Публикации: более 20 научных публикаций, среди которых монографии, научные статьи, материалы и тезы докладов на конференциях.

E-mail: drey_sanya@ukr.net



СМИРНОВ Алексей Анатольевич, д.т.н.

Год и место рождения: 1977 год, г. Кировоград, Украина.

Образование: Харьковский военный университет, 1999 год.

Должность: заведующий кафедрой программного обеспечения с 2014 года.

Научные интересы: информационная безопасность, телекоммуникационные сети и системы.

Публикации: более 100 научных публикаций, среди которых монографии, научные статьи, материалы и тезы докладов на конференциях, патенты.

E-mail: assa_s@mail.ru

Аннотация. Безопасность информации определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и на другие ресурсы телекоммуникационной системы. Для обеспечения информационной безопасности телекоммуникационных систем важной задачей является обеспечение не только повышенных требований к оперативности, но и к надёжности доставки данных. В данной статье предложен метод повышения вероятности и скорости доставки сообщений посредством промежуточного использования сервера повторного сжатия мультимедийной информации. В результате уменьшения трафика менее приоритетной информации, в телекоммуникационном канале уменьшаются вероятности потери пакетов а также время их доставки, что в свою очередь улучшает целостность и доступность переданной информации.

Ключевые слова: телекоммуникационные сети и системы, доступность, целостность, сжатие, защита информации, доставка.

Вступление

Как известно, под информационной безопасностью понимается состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере. Исходя из приведенного выше определения, информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации, где [6, 8-12 с.]:

– конфиденциальность – обеспечение доступа к информации только авторизованным пользователям;

– целостность – обеспечение достоверности и

полноты информации и методов ее обработки;

– доступность – обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

Безопасность информации – состояние защищенности данных, при котором обеспечиваются их конфиденциальность, доступность и целостность. Безопасность информации определяется отсутствием недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы телекоммуникационной системы (ТКС).

Таким образом, для обеспечения информа-

ционной безопасности в ТКС важной задачей является обеспечение не только повышенных требований к оперативности, но и к надёжности доставки данных. При этом, скорость доставки и вероятность передачи без ошибок данных, определяется также размером самих данных [3]. Фактически дополнительно сжав данные, получаем возможность не только оперативнее доставить их получателю, но и понижаем вероятность появления ошибок.

Наиболее перспективным направлением считается сжатие графической и мультимедийной информации, для которой допустимо сжатие с потерями [1]. Это связано с тем, что графическая и мультимедийная информация занимает наиболее существенную долю трафика современных ТКС. Таким образом, в данной работе необходимо решить задачу повышения вероятности доставки сообщений в телекоммуникационных системах и сетях для обеспечения информационной безопасности, за счет реализации предложенной системы повторного сжатия графической информации прогрессивным кодеком с оптимальными показателями сохранения контуров на промежуточном сервере. При этом необходимо учитывать в процессе эксплуатации системы то, что сервера имеют ограниченную

пропускную способность и при высоких нагрузках растёт вероятность отказа в обслуживании.

Основная часть

Для реализации поставленной задачи, сервер дополнительного сжатия изображений можно представить как систему массового обслуживания с очередью. При этом отказ в обслуживании зависит от количества заявок в системе и, следовательно, от исходящего трафика. Вероятность отказа в обслуживании $P_{отк}$ для системы обслуживания с очередью длиной N возможно рассчитать по формуле:

$$P_{отк} = \frac{1-p}{1-p^{N+2}} p^{N+1},$$

где p – относительная интенсивность потока заявок. Для сервера дополнительного сжатия мультимедийной информации низкого приоритета относительную интенсивность p можно выразить отношением количества поступивших заявок за единицу времени m к пропускной способности сервера z : $p=m/z$.

Графики зависимости вероятности отказа в обслуживании от интенсивности заявок для очередей длиной $N=25$ и $N=50$ приведены на рис. 1.

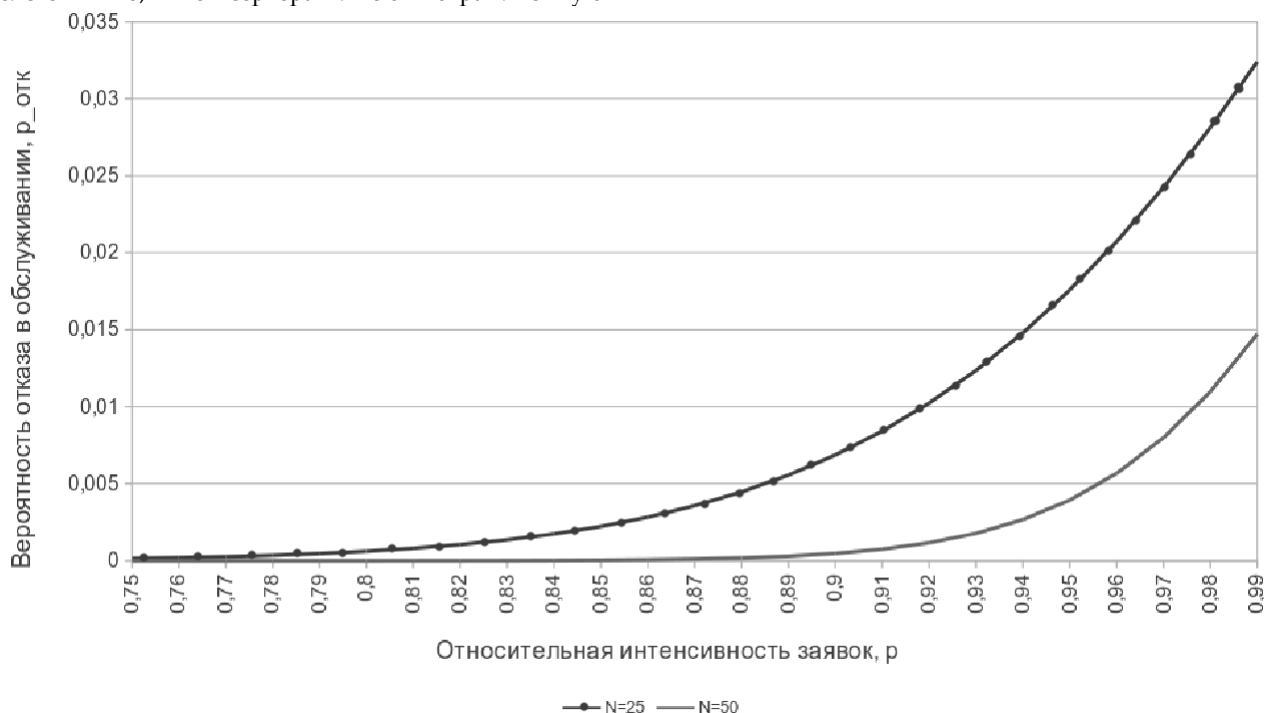


Рис. 1. Зависимость вероятности отказа в обслуживании от относительной интенсивности потока заявок на обслуживание

Из проведенного анализа графика видно, что для системы повторного сжатия изображений с ограничением вероятности отказа в обслуживании 0,005, относительная интенсивность потока к пропускной способности сервера не должна превышать 0,91 для очереди длиной $N=50$ и 0,88 для очереди длиной $N=25$. Однако, при более длинной очереди, что дает увеличение разрешенного трафика, увеличивается и время пребывания заявки в системе. Однако увеличение времени доставки сообщения не всегда допустимо. Таким образом, выходом из ситуации ограниченного трафика через

сервер дополнительного сжатия графической информации, является частичное обслуживание по стандартной схеме. Одно из возможных решений представлено на схеме рис. 2.

По схеме (рис. 2) имеется ограничение значения вероятности отказа в обслуживании, из которого определяется (по эмпирическим или теоретическим соотношениям) значение максимального трафика. Далее по собранной ранее статистике входящего трафика производится прогнозирование трафика на время достаточное для оповещения (активного или пассивного)

пользователей о доле запросов k , которые будут происходить через сервер дополнительного сжатия информации. Остальная часть запросов $(1-k)$ будет обработана без дополнительного сжатия по стандартной схеме.

С целью уменьшения трафика через локальную сеть на сервере реализовано службу дополнительного сжатия графической информации с потерями. Дополнительное сжатие обеспечивает

сжатие изображений дополнительно в 2-10 раз, при этом используя прогрессивность кодирования. В результате прогрессивности кода, пользователь имеет возможность уточнить информацию подгрузив только недостающий фрагмент файла изображения. Кеширование запросов к файлам изображения позволяет при повторных запросах не использовать внешние телекоммуникационные соединения.

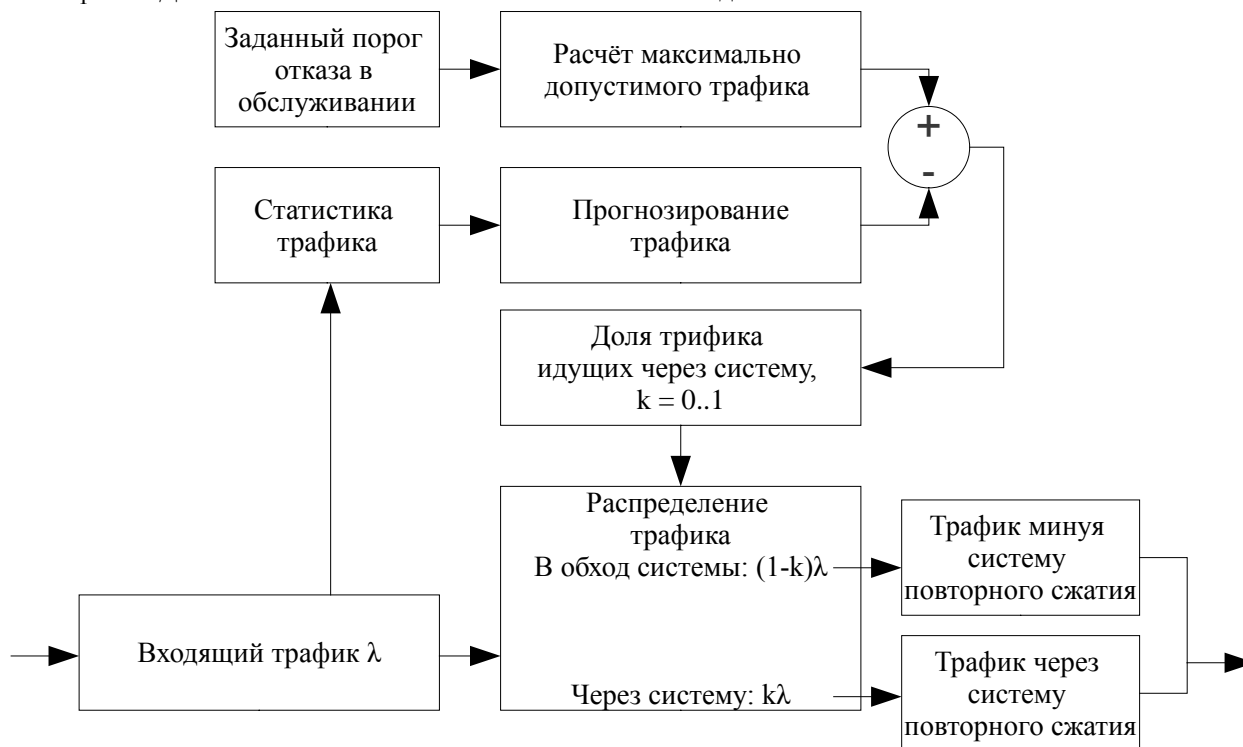


Рис. 2. Схема перераспределения трафика с целью ограничения нагрузки на сервер повторного сжатия изображений

Таблица 1

Фрагмент данных результатов сравнительного исследования совпадения контурного соответствия классическим алгоритмом сжатия SPIHT и модификации с отложенной передачи данных

Классический SPIHT		Отложенная передача значимых битов		Разница параметров	
Среднеквадратическое отклонение	PSNR	Среднеквадратическое отклонение	PSNR	Среднеквадратическое отклонение	PSNR
0,00206051	76,0504	0,0016145	74,9911	0,0004460	1,0593
0,00368715	73,7158	0,00276376	72,4639	0,0009234	1,2519
0,00134325	81,2518	0,000487414	76,8492	0,0008558	4,4026
0,0103765	67,0264	0,0128956	67,9703	-0,002519	-0,9439
0,00212063	77,4197	0,00117791	74,8662	0,0009427	2,5535
...
0,00245235	75,6699	0,00176235	74,235	0,0006900	1,4349
			Среднее значение:	0,0003112	0,4900

Для сервера дополнительного сжатия информации авторами усовершенствован метод SPIHT прогрессивного сжатия изображений [5], путём отложенной передачи уточнений значимых коэффициентов. Это позволило при увеличении абсолютной погрешности значимых коэффициентов повысить количество таких коэффициентов. Это приводит к большей детализации изображения. Данное утверждение было подтверждено экспериментально при обработке более 1000

изображений разного характера. При восстановлении сжатого в 50 раз изображения проверялось совпадение контуров с эталоном полученным из первоначального изображения. Результаты показаны в следующей таблице 1.

Проведенные исследования показали, что при эксплуатации сервера за время t , относительная интенсивность заявок не превышает допустимый порог $t_{доп}$ времени. Тогда в течении времени $t_{кр}=t-t_{доп}$, вероятность отказа в обслуживании будет выше

допустимого порога. В случае использования прогнозирования интенсивности поступления заявок [2, 4], имеется возможность с вероятностью P_H снизить интенсивность заявок, пустив их в обход системы или иным способом. В таком случае среднее время превышения порога интенсивности потока

заявок будет следующее:

$$t_{кр}^* = (1 - P_H)(t - t_{доп}),$$

где $(1 - P_H)$ – вероятность ошибочности прогнозирования. Результат применения системы прогнозирования показан на рис. 3.

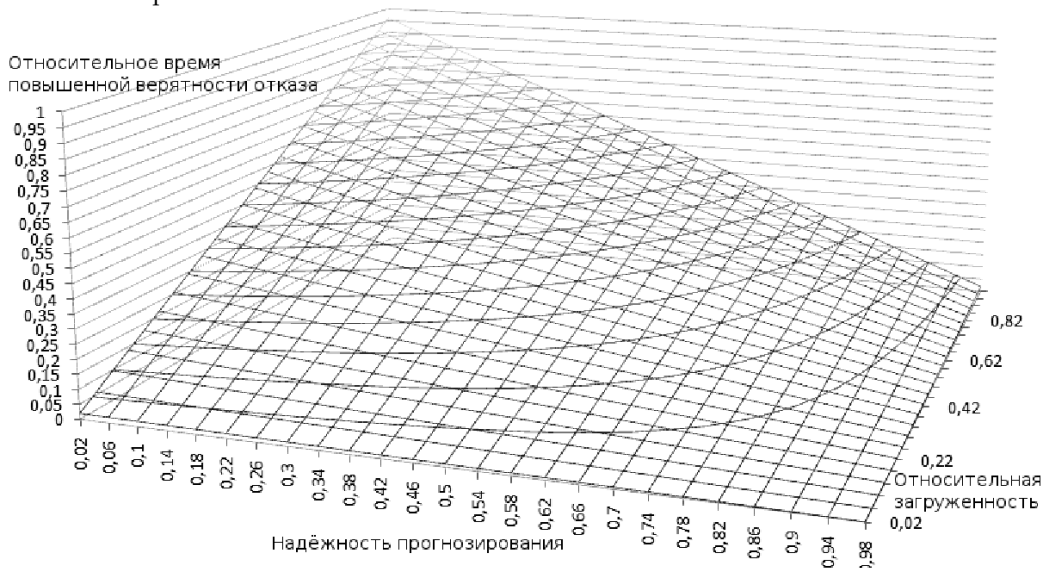


Рис. 3. Доля времени работы сервера в режиме повышенной нагрузки в зависимости от трафика и вероятности его верного прогнозирования

Максимум времени работы сервера в границах допустимой нагрузки может быть достигнут при максимальной точности прогнозирования. Однако, при прогнозировании доверительный интервал прогнозируемых значений пропорционально вероятности попадания в этот интервал, что при высоких вероятностях даёт меньшую точность прогнозируемых значений. В

связи с этим, точность прогнозирования или доверительный интервал значений выбирают по индивидуальным параметрам надёжности системы.

В результате внедрения системы прогнозирования трафика через сервер дополнительного сжатия информации получено уменьшение трафика без увеличения вероятности отказа в обслуживании.

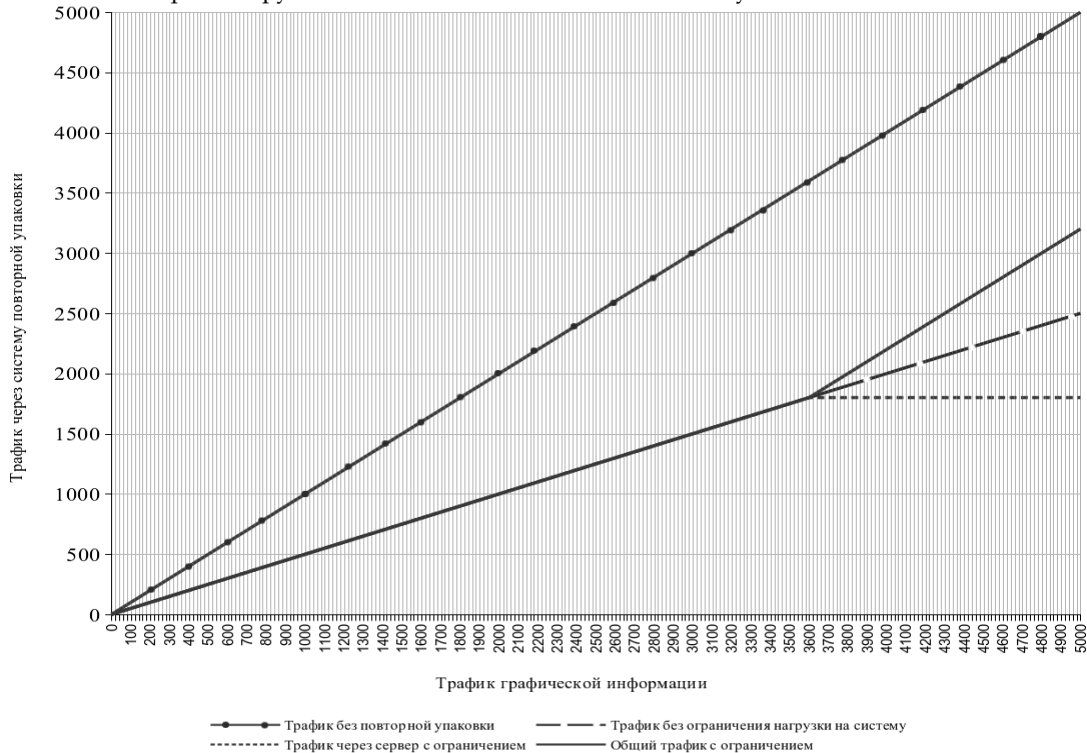


Рис. 4. Сравнение общего трафика графического контента с использованием сервера дополнительного сжатия графической информации и без него

На рис. 4 верхня пряма показує зміну графічного трафіка ТКС без використання сервера додаткового стиснення інформації. Нижня лінія показує трафік при використанні такого сервера. Однак, при досягненні трафіка значення, при якому ймовірність відмови в обслуговуванні сервером додаткового стиснення вище встановленої, лінія розгалужується на три: нижня пунктирна лінія показує трафік через сервер; верхня лінія є сумою трафіка через сервер додаткового стиснення і трафіка, який проходить минуо сервер; середня показує трафік через сервер без використання обмеження при допомозі передбачення, коли ймовірність відмови в обслуговуванні вище встановленого значення.

Висновки

В результаті проведеного дослідження встановлено, що витрати часу на доставку даних і ймовірність їх безпомилкового отримання залежать від розмірів цього повідомлення. Додаткове стиснення графічної інформації дозволяє зменшити час доставки повідомлень. Використання передбачення трафіка дозволило обмежити навантаження на сервер, тим самим знизити ймовірність відмови в обслуговуванні і зменшити загальний графічний трафік в 1.6..2 рази. Таким чином, вирішена задача підвищення ймовірності доставки повідомлень в телекомунікаційних системах і мережах для забезпечення інформаційної безпеки.

Література

[1] Дреєв О.М. Методи підвищення якості обслуговування у телекомунікаційних системах та мережах / О.М. Дреєв, Г.М. Дреєва, О.А. Смірнов // Зб. тез доп. Акад. внутрішніх військ МВС України «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» 20-21 березня 2013р. - Х. : АВВ. - 2013. С. 18-19.

[2] Дреєв О.М. Метод довгострокового прогнозування навантаження серверу телекомунікаційної мережі / О.М. Дреєв, Г.М. Дреєва // Комбінаторні конфігурації та їх застосування. Кіровоград. 13-14 квітня 2012 р. - Кіровоград: «Експозитив-систем». - 2012. - С. 50

[3] Дреєв О.М. Дослідження впливу ступеня стиснення зображень на оперативність їх доставки у телекомунікаційній системі / О.А. Смірнов, О.М. Дреєв, О.П. Доренський // Зб. наук. пр. «Системи обробки інформації». - Вип.8 (115). - Х.: ХУПС - 2013. - С. 234-239.

[4] Дреєв А.Н. Екстраполяція квазіперіодических процесів з адитивними поємами / А.Н. Дреєв, А.А. Смірнов // П'ята міжнар. наук.-практ. конф. «Інф. технології та моделювання в економіці» 15-16 травня 2014 р. - Черкаси - С. 59

[5] Д.Сэлмон. Сжатие данных, изображений и звука - М. : Техносфера, 2004. - 368с.

[6] Нестеров С.А. Информационная безопасность и защита информации / С.А. Нестеров // Уч. пос. - СПб.: Изд-во Политехн. ун-та, 2009. - 126 с.

[7] Таненбаум Э. Компьютерные сети. пер. с англ. А. Леонтьев. - СПб.: Питер, 2002. - 848 с.

[8] Вегешна Ш. Качество обслуживания в сетях IP / Ш. Вегешна. М.: Вільямс, 2003. - 368 с.

[9] Кузнецов О.О. Протоколи захисту інформації у комп. системах та мережах: навч. посібник. / О.О.Кузнецов, С.Г.Семенов - Х. : ХНУРЕ, 2009, 186 с.

[10] Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. - 2-е изд. - СПб.: Питер, 2007. - 958 с.

[11] Смірнов А.А. Анализ и сравнительное исследование перспективных направлений развития цифровых телекоммуникационных систем и сетей / А.А. Смірнов, В.В. Босько, Е.В. Мелешко // Системи обробки інформації. - Х.: ХУПС, 2008. - Вип. 7(74). - С.120-123.

УДК 004.056.52 (045)

Дреєв О.М., Смірнов О.А. Підвищення ймовірності доставки повідомлень в телекомунікаційних системах та мережах для забезпечення інформаційної безпеки

Анотація. Безпека інформації визначається відсутністю неприпустимого ризику, пов'язаного з витоків інформації технічними каналами, несанкціонованими і ненавмисними впливами на дані і на інші ресурси телекомунікаційної системи. Для забезпечення інформаційної безпеки телекомунікаційних систем важливим завданням є забезпечення не тільки підвищених вимог до оперативності, а й до надійності доставки даних. У цій статті представлено метод збільшення ймовірності та швидкості доставки повідомлень за допомогою посереднього використання серверу повторного стиснення мультимедійної інформації. В результаті зменшення трафіку менш пріоритетної інформації в телекомунікаційному каналі зменшуються ймовірність втрати пакетів а також час їх доставки, що в свою чергу покращує цілісність та доступність інформації.

Ключевые слова: захист інформації, доступність, цілісність, стиснення, телекомунікаційна система, доставка.

Dreyev O., Smirnov O. Probability increasing of message delivery in telecommunication systems and networks for information security

Abstract. Security of information is determined by the absence of unacceptable risk of leakage of information through technical channels, unauthorized and unintended effects on the data and other resources on the telecommunications system. To ensure the information security of telecommunication systems important task is to ensure not only the increasing demands of efficiency, but also to the reliability of data delivery. This paper presents a method of increasing the likelihood and speed of message delivery using indirect application server re-compression of multimedia information. As a result, reduce traffic less priority information in the telecommunications channel reduces packet loss probability and the time of delivery, which in turn improves the integrity and availability of information.

Key words: information security, availability, integrity, compression, telecommunication system, delivery.

Отримано 26 лютого 2015 року, затверджено редколегією 13 березня 2015 року