УДК004.78

МЕТОД УМЕНЬШЕНИЯ НАГРУЗКИ СЛУЖЕБНОГО ТРАФИКА В КОМПЬЮТЕРНОЙ СЕТИ

САЕНКО В.И., КОЛЕНЦЕВА Т.А.

Рассматривается задача уменьшения служебного трафика в компьютерной сети. Обсуждаются вопросы поиска эффективных решений обеспечения допустимой нагрузки для рабочих станций. Предлагаются оценки нагрузки служебным трафиком компьютерной сети с учетом достаточной обеспеченности информативности процесса мониторинга. Правильность полученного решения подтверждается на примере.

1. Введение

В современных компьютерных сетях одной из немаловажных проблем является снижение служебного трафика. Его объемы зачастую составляют слишком большой процент по отношению ко всему передаваемому трафику. Это затрудняет работу и пользователей, и администраторов сетей, и владельцев сервисов в сети.

2. Описание проблемы и анализ известных результатов исследований

Вопросы сокращения служебного трафика являются весьма актуальными.

Пропускная способность любого канала компьютерной сети ограничивается максимальной эффективной пропускной способностью используемого логического канала. Часть этой пропускной способности используется для передачи пользовательских данных, а часть – не для пользовательских. Сюда входит служебный трафик и множество специальных пакетов. Иногда из-за большого объема служебного трафика и шума эффективная пропускная способность сети уменьшается. Во избежание подобной ситуации были разработаны разные подходы по уменьшению служебного трафика [1].

Исследования в области компьютерных сетей показали, что из-за стохастического характера состояния системы очень сложно использовать детерминированные подходы [2]. Ограничение пользовательского трафика или применение сеансового времени имеют три основных недостатка [3]. Во-первых, это приводит к большим финансовым затратам, во-вторых – к недовольству со стороны пользователей [4], в-третьих – к снижению гибкости системы [5].

Большинство существующих предложений по уменьшению нагрузки информационной системы существуют на основе таких методов, как фильтрация пакетов [6].

Тем не менее, предлагаемых идей не достаточно для решения проблемы эффективного уменьшения нагрузки на каналы передачи данных, когда потребности в ресурсах явно превышают пропускную способность системы.

Интересным представляется поиск решения задач реализации процедур мониторинга, учитывающего ограничение на служебный трафик и обеспечение информативности собираемых данных [7]. Первый заключается в возможном изменении объема планируемого для передачи служебного трафика, второй – в изменении степени информативности для всех передаваемых данных в рамках решения задач мониторинга состояния компонентов компьютерной сети.

Цель работы: поиск путей уменьшения нагрузки служебным трафиком в компьютерной сети.

Структура статьи. Постановка задачи описывает сеть, как объект исследования. Далее предоставляется методология формирования служебного трафика. В следующем пункте дается краткое описание методов уменьшения нагрузки служебным трафиком общих каналов передачи данных в компьютерной сети. Методы представляются как обобщение и систематизация предыдущих пунктов. Далее описывается анализ предоставленных методов, после которого дается пример, подтверждающий правильность полученных результатов. В завершение формализованы основные научные и практические результаты.

Постановка задачи:

Пусть рассматривается распределенная информационная система, пример которой изображен на рис. 1, где Net – компьютерная сеть, WS – рабочие станции системы, Manager – менеджер компьютерной сети (администратор), Server – сервер компьютерной сети, U – пользовательский трафик, S – служебный трафик.

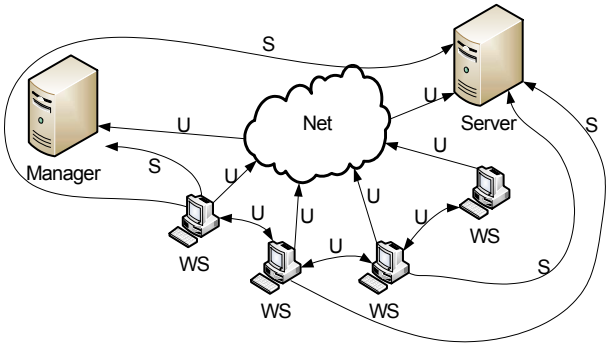

Рис. 1. Пример распределенной информационной системы

Нагрузка на каналы передачи данных в компьютерной сети состоит из пользовательского трафика, служебного и шумов. Задача сводится к построению механизма уменьшения нагрузки служебным трафиком, что приведет к возможности увеличения пользовательского трафика.

Используется архитектура агент-менеджер с центральным сбором и накоплением.

Технология реализации. На каждом узле системы расположено программное обеспечение для мониторинга, называемое агентами мониторинга. Агент мо-

ниторинга может быть настроен с помощью узла управления для периодической передачи информации в случае, если удовлетворены определенные условия. Такая настройка позволяет узлу управления адаптироваться, основываясь на структуре статистических запросов.

Считаем, что рассматриваемая система мониторинга поддерживает концепцию push и pull.

Это означает, что центральный менеджер рассылает условия мониторинга каждой станции (push), а далее осуществляется сбор данных со всех станций (pull).

3. Методология формирования служебного трафика в компьютерной сети

Предоставляется решение для задач по обеспечению уменьшения нагрузки служебным трафиком общих каналов передачи данных. Решение основано на 3-х методах уменьшения нагрузки.

В первом методе (нисходящее оценивание) предлагается оценить допустимый порог для разрешенного объема передаваемого служебного трафика для каждой рабочей станции и допустимый объем измеряемых переменных. Второй метод (восходящее оценивание) предназначается для оценки общего объема передаваемого служебного трафика при полной информационной обеспеченности задачи мониторинга для каждой рабочей станции.

Третий метод позволит объединить первые два и стать их обобщением (рис. 2).

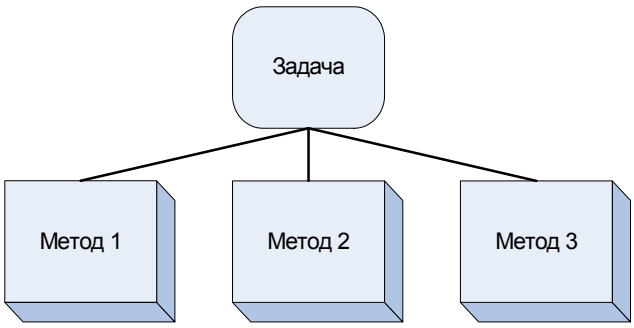

Рис. 2. Решение задачи уменьшения нагрузки

Первый метод, предназначенный для оценивания допустимого порога передаваемого служебного трафика, предлагается представить в виде трех этапов:

1. Формирование групп контролируемых рабочих станций.

2. Оценивание допустимого порога для разрешенного объема передаваемого служебного трафика для каждой рабочей станции.

3. Оценивание допустимого объема измеряемых переменных.

Этап 1. Формирование групп контролируемых рабочих станций.

Все имеющиеся компьютерные станции {WS} в сети можно разделить на группы по некоторым признакам.

Число групп N_G определяется на основе допуска о максимальном числе компьютеров в группе N_J:

$$N_G \le N / N_J, \quad (1)$$

где N – число всех компьютеров.

Группы можно формировать по следующим таксономическим признакам (E_G):

1) IP адресация;

2) функциональная однородность;

3) организационная однородность;

4) активность пользователей;

5) компьютеры из возможной области закрытого доступа;

6) подобное системное наполнение.

Группирование по IP адресам означает, что выбирается область с похожими IP адресами. Это могут быть либо различные подсети, либо группировка по возрастанию адресов, т.е. в группу будут входить компьютеры из тех же самых подсетей (приоритет по сетям).

Функциональная однородность обычно применятся для различных корпораций, чтобы разделить пользователей, которые должны иметь доступ к различным базам данных. Тогда в группу входят станции, на которых решаются функционально однородные задачи (приоритет по функциям).

Группирование по организационной однородности может быть необходимым для применения, к примеру, в университете: различные группы факультетов (приоритет организационный).

Разделение по активности пользователей можно использовать для того, чтобы было затрачено больше ресурсов на обеспечение бесперебойной работы у тех пользователей, которые в этом нуждаются больше других (приоритет по активности).

Разделение по группам компьютеров, которым и только которым будет открыт доступ в те или иные участки сети, тоже является немаловажным (приоритет по правам).

Группирование по подобному системному наполнению можно применять, чтобы облегчить устранение возможных неполадок для целой группы. Например, Windows XP, Windows 7, Windows 2003, Linux (приоритет по ПО).

Группирование дает дополнительную возможность управлять приоритетами доступа к ресурсам для соответствующих групп пользователей. Как следствие, это позволяет формировать общую политику менеджмента компьютерной сети.

Этап 2. Оценивание допустимого порога для разрешенного объема передаваемого служебного трафика для каждой рабочей станции.

Для того чтобы установить порог C_m^* на центральный менеджер в компьютерной сети, вычисляем:

$$C_m[t] \le C_m^*, \quad (2)$$

где $C_m[t]$ – передаваемый служебный трафик; t – момент времени.

В любой момент времени значение передаваемого служебного трафика не должно превышать некое пороговое значение.

Зная количество групп, зная пороговое значение передаваемого трафика, вычисляем нагрузку на каждую группу:

$$C_m = \sum_{j \in J} C_j, \quad (3)$$

где C_j – объем служебного трафика, передаваемого с одной группы; J – множество групп.

Учитывая количество компьютеров в группе, вычисляем допустимый порог нагрузки на центральный менеджер.

Считаем, что наибольшая нагрузка на каждый компьютер C_{ij} не должна быть больше, чем C_{ij}^*:

$$C_{ij}[t] \le C_{ij}^*; (C_j(t) \le C_j^*), \quad (4)$$

где C_{ij} – объем служебного трафика, передаваемого с каждой рабочей станции; t – момент времени; C_{ij}^* – критическое значение передаваемого служебного трафика от рабочей станции к менеджеру; C_j^* – критическое значение передаваемого служебного трафика от одной группы к менеджеру.

Этап 3. Оценивание допустимого объема измеряемых переменных.

Примем некоторые допущения. Пусть для каждой измеряемой переменной заданы информационные затраты $I(V_j)$ и кратность ее измерения $\nu(V_j)$; за интервал T_d, где V_j – измеряемая переменная.

Тогда справедливо

$$C_{ij}^{**} = (n_V \times I(V_j) \times \nu(V_j)) / T_d, \quad (5)$$

где n_V – число измеряемых переменных; T_d – интервал цикла мониторинга.

Следовательно, зная C_{ij}^*, можно определить допустимое число измеряемых переменных:

$$n_V = C_{ij}^* / ((I(V_j) \times \nu(V_j)) / T_d). \quad (6)$$

Если полагать, что заданному уровню информативности соответствует определенное число измеряемых переменных n_V', то сравнивая полученные решения n_V, можно сделать вывод о степени информационной обеспеченности в данной процедуре задачи мониторинга.

Второй метод задачи уменьшения нагрузки предназначен для оценки общего объема передаваемого служебного трафика. Он состоит из трех этапов:

1. Определение объема передаваемого трафика для одной рабочей станции.

2. Определение объема передаваемого трафика для центрального сервера менеджмента (для всей сети).

3. Анализ и коррекция полученных результатов для объема предаваемого служебного трафика.

Этап 1. Определение нагрузки, исходя из количества измеряемых переменных.

Для задачи мониторинга выбирается количество необходимых для оценивания измеряемых переменных n_V на каждой рабочей станции.

Зная информационные затраты каждой переменной $I(V_j)$, кратность их измерения $\nu(V_j)$ и интервалы цикла мониторинга T_d, где V_j – измеряемая переменная, вычисляем нагрузку на каждую рабочую станцию:

$$C_{ij} = (n_V \times I(V_j) \times \nu(V_j)) / T_d. \quad (7)$$

Этап 2. Определение объема передаваемого трафика для центрального сервера менеджмента (для всей сети).

Учитывая количество компьютеров в группе N_J и критическое значение передаваемого служебного трафика от рабочей станции менеджеру C_{ij}^*, вычисляем нагрузку на группу:

$$C_j = C_{ij} N_J. \quad (8)$$

Зная количество групп N_G и нагрузку на группу C_j, проводим подсчет нагрузки на всю сеть:

$$C_m = C_j N_G. \quad (9)$$

Вычисляем процент служебного трафика сети, исходя из данных об общем передаваемом трафике C:

$$\eta_\% = C / C_m. \quad (10)$$

Этап 3. Анализ и коррекция полученных результатов для объема предаваемого служебного трафика.

Сравниваем полученные значения коэффициентов использования основного канала $\eta_\%$ с допустимыми $\eta_\%^*$. Если соотношение $\eta_\% \le \eta_\%^*$ не выполняется, то возвращаемся к этапу 1. Уменьшаем число наблюдаемых переменных n_V и снова пересчитываем нагрузку на сеть. Понимая, что уменьшение числа наблюдаемых переменных приводит к уменьшению информативности, рассматриваем вариант разделения сети на области (сайты). Для каждой области можно рассматривать оценивание нагрузки отдельно.

Третий метод задачи уменьшения нагрузки содержит в себе комбинацию первых двух методов (рис. 3). Он состоит из трех этапов:

1. Оценивание допустимого порога для разрешенного объема передаваемого служебного трафика для каждой рабочей станции.

2. Оценивание общего объема передаваемого служебного трафика при полной информационной обеспеченности задачи мониторинга для каждой рабочей станции.

3. Сравнительный анализ и коррекция объема контролируемой информации.

Этап 1. Проводим оценивание допустимого порога для разрешенного объема передаваемого служебного трафика для каждой рабочей станции согласно методу 1.

Получаем значения: n_V – число измеряемых переменных, T_d – интервал цикла мониторинга информационных затрат $I(V_j)$ и кратности измерения $\nu(V_j)$ для каждой V_j (измеряемая переменная). А также имеем значения для допустимых пропускных способностей для служебного трафика C^*_m. В итоге имеем

$$(nv, I(Vj), v(Vj), C^*_m)^{(a)}.$$

Этап 2. Проводим оценивание общего объема передаваемого служебного трафика при полной информационной обеспеченности задачи мониторинга для каждой рабочей станции. Получаем значения расчетной (требуемой пропускной способности) C_m. При этом имеем требуемые значения для n_V, T_d, $I(V_j)$ и кратности измерения $\nu(V_j)$. В итоге имеем $(nv, I(Vj), v(Vj), C^*_m)^{(b)}$. Использование метода 2 ограничиваем только одой итерацией.

Этап 3. Сравниваем полученные наборы $(nv, I(Vj), v(Vj), C^*_m)^{(a)}$ и $(nv, I(Vj), v(Vj), C^*_m)^{(b)}$. В случае несовпадения проводим коррекцию либо по числу наблюдаемых переменных n_V, либо по числу кратности измерения $\nu(V_j)$, либо по допустимому уровню служебного трафика C^*_m, либо по числу менеджеров мониторинга (как следствие – числу групп в сети). Коррекцию проводим несколько раз (итераций) так, чтобы нисходящее и восходящее оценивание давало одинаковый результат.

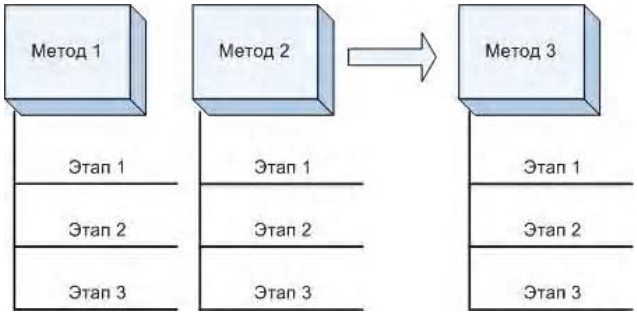

Рис. 3. Объединение методов для решения задачи

4. Метод оценки допустимой нагрузки для рабочей станции

Этап 1. Формирование групп контролируемых рабочих станций.

– Вычисляем количество групп J по (1).

Этап 2. Оценивание расчетных значений нагрузки на сеть каждой рабочей станции в отдельной группе.

– Принимаем допущения о значениях C_{ij}^* и C_j^*.

– Вычисляем C^*_m исходя из (2).

– Проводим подсчет C_j по (3).

– Вычисляем C_{ij} по (4).

Этап 3. Оценивание допустимого объема измеряемых переменных.

- Проводим проверку на превышение пороговых значений.

- Принимаем допущения по T_d, $I(V_j)$ и $\nu(V_j)$.

- Вычисляем число измеряемых переменных n_V по (6).

- Вычисляем допустимый объем C_{ij}^{**} по (5).

5. Метод оценки нагрузки служебным трафиком при полной обеспеченности каждой задачи.

Этап 1. Определение нагрузки, исходя их количества переменных.

- Выбираем N_x'.

- Исходя из C_{ij}^* по (6) вычисляем C_j^*.

- Проводим подсчет C^*_m по (7).

- Вычисляем $C_{\%}$ по (8).

Этап 1. Определение нагрузки, исходя из количества измеряемых переменных.

- Выбираем n_V на каждой рабочей станции.

- Исходя из $I(V_j)$, $\nu(V_j)$, T_d, вычисляем C_{ij} по (7).

Этап 2. Определение объема передаваемого трафика для центрального сервера менеджмента (для всей сети).

– Учитывая N_J и C_{ij}^*, вычисляем C_j на группу по (8).

– Зная N_G и C_j, проводим подсчет C_m на всю сеть, согласно (9).

– Исходя из данных о C, вычисляем $\eta_{\%}$ по (10).

Этап 3. Анализ и коррекция полученных результатов для объема предаваемого служебного трафика.

– Проводим сравнение $\eta_{\%}$ с допустимыми $\eta^*_{\%}$.

– Если $\eta_{\%} \le \eta^*_{\%}$ не выполняется, то возвращаемся к этапу 1, уменьшая при этом n_v.

6. Метод уменьшения и контроля нагрузки служебным трафиком общих каналов передачи данных в компьютерной сети

Заключается в объединении двух описанных выше методов.

Этап 1. Оценивание допустимого порога для разрешенного объема передаваемого служебного трафика для каждой рабочей станции, согласно методу 1.

– Получаем значения n_V, T_d, $I(V_j)$ и $\nu(V_j)$ для каждой V_j.

– Знаем значения т C^*_m для служебного трафика.

– В итоге имеем $(nv, I(Vj), v(Vj), C^*_m)^{(a)}$.

Этап 2. Оценивание общего объема передаваемого служебного трафика при полной информационной обеспеченности задачи мониторинга для каждой рабочей станции.

– Получаем значения C_m.

– Знаем требуемые значения n_V, T_d, $I(V_j)$ и $\nu(V_j)$.

– В итоге имеем $(nv, I(Vj), v(Vj), C^*_m)^{(b)}$.

Использование метода 2 ограничиваем только одной итерацией.

Этап 3. Сравнительный анализ и коррекция объема контролируемой информации.

– Сравниваем $(nv, I(Vj), v(Vj), C^*_m)^{(a)}$ и $(nv, I(Vj), v(Vj), C^*_m)^{(b)}$.

– В случае несовпадения проводим коррекцию либо по n_V, либо по $\nu(V_j)$, либо по C^*_m, либо по N_G. Коррекцию проводим несколько раз, пока не будут соблюдены условия

$$(nv, I(Vj), v(Vj), C^*_m)^{(a)} = (nv, I(Vj), v(Vj), C^*_m)^{(b)}.$$

7. Анализ метода уменьшения нагрузки служебным трафиком общих каналов передачи данных

Предложенные методы могут быть использованы для разных начальных условий проведения процедур мониторинга в сети. Они дают возможность разной оценки получаемых результатов. Метод 1 позволяет обеспечить требования жесткого ограничения служебного трафика даже за счет потери некоторой информативности (например, за счет уменьшения числа наблюдаемых переменных или кратности их измерения). Метод 2 позволяет оценить требования к расширению сети для обеспечения полной информативности решения задач мониторинга. Метод 3 позволяет получить некоторое компромиссное решение.

8. Пример

Метод 1.

Этап 1. В качестве примера рассмотрим университетская компьютерная сеть. Допустим, в сети находится 300 рабочих станций. К каждой группе должно относиться не больше, чем 50 компьютеров. Значит, у нас должно быть не меньше 6-ти групп. В этом случае все имеющиеся рабочие станции могут быть разделены по одному из таксономических признаков. Пусть будет выбран показатель «IP адресация».

Этап 2. Общий передаваемый трафик в сети составляет около 100 Мб/с.

Пусть критическим значением передаваемого трафика от каждой рабочей станции будет считаться $C^*_{ij} = 1\,КБ/с$, от каждой группы – соответственно $C^*_j = 50\,КБ/с$.

Пусть принимается допущение о том, что порог служебного трафика составляет не более 1%, тогда пороговое значение передаваемого служебного трафика C^*_m не должно превышать 100 КБ\с.

Вычисляем нагрузку на каждую группу:

$$C_j = 100\,КБ/с \div 6 = 17КБ/с$$

Каждая рабочая станция должна передавать не больше, чем $C_{ij} = 17\,КБ/с \div 50 = 0.34КБ/с$ служебного трафика.

В данном конкретном случае передаваемые данные не вышли за предел допустимого значения.

Этап 3. Оценивание допустимого объема измеряемых переменных.

Пусть контроль производится каждую секунду, $T_d = 1с$. Информационные затраты на 1 переменную составляют $I(V_j) = 10Б$. Контроль проводится 1 раз в секунду $\nu(V_j) = 1$. Тогда допустимый объем контроля задается на уровне n_V переменных по формуле (6):

$$n_V = 340(Б)/((10(Б)\times 1))/1(с)) = 34(переменные).$$

Оценим, много это или мало по (5):

$$C^{**}_{ij} = 34(переменных) * 10(Б) * 1/1с = 340Б/с,$$

что не превышает установленный порог в 1Кб/с.

Таким образом, в первом методе были проведены подсчеты объема передаваемого служебного трафика и проверка на превышение установленного порога.

Поскольку объемы передачи служебного трафика не превысили пороговых значений, мы приступаем ко второму методу.

Метод 2.

Этап 1. Допустим, для расширения контроля функциональности состояния компьютерной сети требуется оценивать по 100 переменных на каждой рабочей станции. Согласно методологии п. 3, контроль 100 переменных создает нагрузку одной рабочей станции в объеме 1КБ/с. Следовательно, исходя из (8) нагрузка на группу будет в объеме 50 КБ/с, а на сеть (9) – 300КБ/с, т.е. (10) 3%.

Этап 2. Далее администратор принимает решение о том, стоит ли соглашаться с данной нагрузкой или нет. В данном случае нагрузка удовлетворяет заданные условия.

Второй метод содержит в себе определение объема передаваемого трафика для всей сети и анализ с коррекцией полученных результатов для объема передаваемого служебного трафика.

Соблюдение заданных условий помогает уложиться в допустимый предельный диапазон, обеспечивая требуемую информативность наблюдаемых процессов.

9. Выводы

В данной работе представлено решение для задач по обеспечению уменьшения нагрузки служебным трафиком общих каналов передачи данных. Задача основана на трех методах уменьшения нагрузки.

Научная новизна состоит в том что получил дальнейшее развитие метод уменьшения нагрузки служебным трафиком общих каналов передачи данных в компьютерной сети.

Практическая значимость состоит в снижении расходов на эксплуатацию сети и повышении ее производительности за счет увеличения пользовательского трафика.

Сравнение с лучшими аналогами. Данная работа предлагает задачу уменьшения нагрузки компьютерной сети. Описанный метод основан на [2-4], но в отличие от ранее предлагаемых методов не требует сокращения пользовательского трафика, что приводит к недовольству со стороны пользователей. Целью метода являлось увеличение пользовательского трафика за счет сокращения служебного трафика и шумов, в отличие от [1, 5]. Предложенный метод является более информативным и требует меньше финансовых затрат по сравнению с [6] и [7].

Направления дальнейших исследований. Дальнейшая работа будет направлена на разработку метода формирования схем запросов для систем мониторинга компьютерной сети.

Литература: **1.**http://technet.microsoft.com/en-us/library/cc181833.aspx. 2. *Kc Clay, Crovella, M., Friedman, T., Shannon, C., Spring, N.* Community-oriented network measurement infrastructure (CONMI) workshop report. SIGCOMM Comput. Commun. Rev. 36(2) (2006) 41–48. **3.** *Cranor, C., Johnson, T., Spataschek, O., Shkapenyuk, V.* Gigascope: A stream database for network applications. In: Proceedings of ACM Sigmod, New York, NY, USA, ACM Press (June 2003). P. 647–651. **4.** *Stankovic J., Lu C., Son S., Tao G.* The case for feedback control real-time scheduling. In: Proceedings of the 11th Euromicro Conference on Real-Time Systems. (June 1999). P. 11–20. **5.** *Keys K., Moore D., Estan C.* A robust system for accurate real-time summaries of internet tra?c. In: Proceedings of ACM Sigmetrics, New York, NY, USA, ACM Press (2005). P. 85–96. **6.** *Estan C., Keys K., Moore D., Varghese G.* Building a better NetFlow. In: Proceedings of ACM Sigcomm, New York, NY, USA, ACM Press (August 2004). P. 245–256. **7.** *Barlet-Ros P., Amores-Lropez D., Iannaccone G., Sanju's-Cuxart J. and Solre-Pareta J.* On-line Predictive Load Shedding for Network Monitoring. In Proc. Of IFIP-TC6 Networking, Atlanta, USA, May 2007. P. 124-136.

Поступила в редколлегию 06.04.2011

Рецензент: д-р техн. наук, проф. Самойленко Н.И.

Саенко Владимир Иванович, канд. техн. наук, доцент, профессор кафедры ИУС ХНУРЭ. Научные интересы: менеджмент компьютерных сетей. Увлечения и хобби: садоводство, видеосъемка. Адрес: Украина, 61166, Харьков, пр. Ленина 14, тел. 7021-415.

Коленцева Татьяна Александровна, аспирантка кафедры ИУС ХНУРЭ. Научные интересы: менеджмент компьютерных сетей. Увлечения и хобби: web-дизайн. Адрес: Украина, 61166, Харьков, пр. Ленина 14, тел. 7021-415.

УДК 658.512.011.681.326.510.713