Міністерство освіти і науки України
Тернопільський національний педагогічний університет ім.. В. Гнатюка
фізико-математичний факультет

Кафедра інформатики та
методики її викладання

ІНДЗ
Моніторинг мережного трафіку за допомогою утиліти системний монітор ОС Windows

Виконала:
студентки групи І-24
Горак Ірина
Науковий керівник:
Олексюк В. П.

Тернопіль 2013

Зміст

ВСТУП

На сьогоднішній день будь-який комп’ютер, чи то домашній, чи робочий, підключений до мережі локальної або глобальної. Постійно відбувається обмін інформацією, щось приходить нам, а щось ми відправляємо. Як наслідок, виникає проблема контролю цього трафіку(моніторингу).

Трафік — узагальнений термін, яким позначають потоки інформації в телекомунікаційних мережах. Все що проходить через мережеві канали називається трафіком.

Моніторинг — комплекс технічних та програмних засобів, які забезпечують систематичний контроль (стеження) за станом та тенденціями розвитку природних, техногенних та суспільних процесів.

Види моніторингу

Залежно від методології

Динамічний — аналізуються дані про динаміку розвитку або зміни об'єкта, явища або певної характеристики. Це найпростіший спосіб моніторингу, який використовується для аналізу відносно простих
систем: цін, доходів і витрат населення, зайнятості громадян тощо. Основною ціллю такого дослідження є встановлення тенденцій, а не виявлення їх причин чи передумов.

Конкурентний — паралельно за єдиною методологією досліджуються одна, кілька чи низка ідентичних або подібних систем. Дає можливість оцінити і порівняти показники систем, виявити різницю між ними, встановити переваги та недоліки.

Порівняльний — порівняються окремі показники або результати більш комплексних досліджень, проведених за ідентичними критеріями, кількох систем одного рівня або вищих і нижчих систем. Такий підхід дає можливість рандомізувати показники, виявити причини, що збільшують або зменшують різницю між ними.

Комплексний — поєднує в собі методи дослідження, що використовуються у різних видах моніторингів.

Залежно від цілей

Інформаційний — полягає у структуризації, накопиченні і розповсюдженні інформації.

Базовий (фоновий) — виявляє нові проблеми, небезпеки, тенденції до того, як вони стануть осмисленими на рівні управління. За об'єктом моніторингу організовується постійне спостереження з періодичним вимірюванням показників.

Проблемний — з'ясування закономірностей, процесів, небезпек, проблем, які вже відомі і розуміння, усунення, коригування яких є важливим з погляду управління.

Підрахунок трафіку може знадобитсь для отримання статистики використання інтернет-каналу, оптимизації навантаження на вузли локальної мережі, тощо.

На сьогоднішній день створено багато програмного забезпечення, що дозволяє виконати ці дії. В пакеті ОС Windows є стандартна утиліта, яка має функцію моніторингу трафіку, це Системний монітор.

ОПИС УТИЛІТИ СИТЕМНИЙ МОНІТОР WINDOWS

Системний монітор Windows - це оснащення панелі управління, що надає засоби аналізу продуктивності системи, зокрема і об’єму мережного трафіку За допомогою однієї консолі можна в реальному часі здійснювати контроль за кількістю вхідного та вихідного трафіку, вибирати дані, які будуть зберігатися у файлах журналів, задавати порогові значення для оповіщень і автоматичних дій, генерувати звіти і переглядати історію, використовуючи різні способи зберігання.

Утиліта Системний монітор виводить результати моніторингу у вигляді графіків залежності числового значення лічильника від часу.

Інтерфейс користувача утиліти:

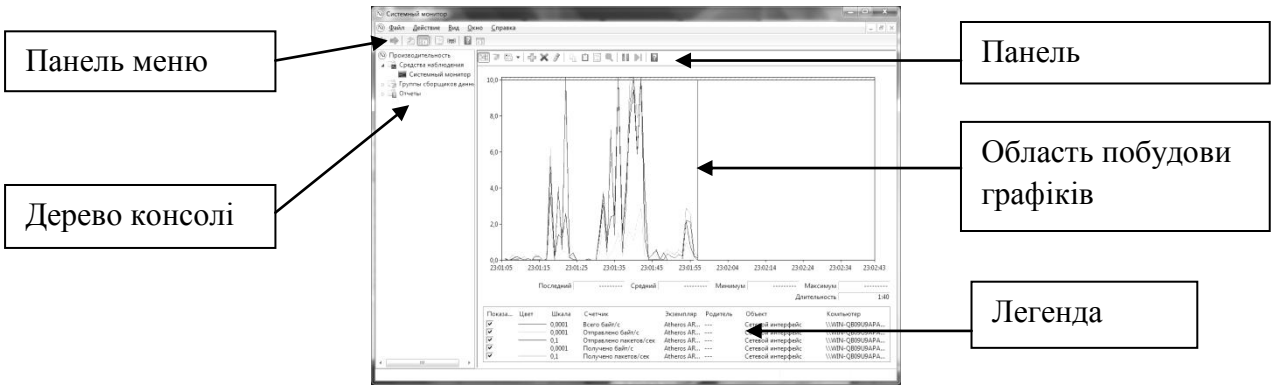

Рисунок 1

Запуск системного монітора:

- У меню Пуск в полі пошуку введемо perfmon і натиснути клавішу ENTER;
- В панелі управління вибрати категорію Адміністрування а потім Системний монітор.

Налаштування системного монітора

Системний монітор має велику функціональність і, відповідно, має безліч налаштувань для найкращого відображення даних. Відкрити діалогове вікно налаштувань системного монітора можна одним з трьох наступних способів :

- У дереві консолі натиснути правою кнопкою миші на вузлі «Системний монітор» і з контекстного меню виберати команду « Властивості» ;
- Перебуваючи у вузлі «Системний монітор» відкрити меню «Дія», а потім виберати команду «Властивості» ;
- Натиснути правою кнопкою миші на панелі відомостей з графіком продуктивності і з контекстного меню виберати команду « Властивості».

За допомогою монітора продуктивності можна також переглядати дані продуктивності на віддаленому комп'ютері в режимі реального часу.

Щоб підключити монітор продуктивності до віддаленого комп'ютера потрібно:

- Запустити монітор продуктивності.
- У дереві переходів клацнути правою кнопкою миші пункт Продуктивність, а потім вибрати команду Підключитися до іншого комп'ютера.
- Ввести ім'я комп'ютера, дані якого необхідно переглянути, в діалоговому вікні Вибір комп'ютера або натиснути кнопку Огляд та вибрати його у списку.
- Натиснути кнопку ОК .

КЕРУВАННЯ ЛІЧИЛЬНИКАМИ

Додавання лічильників продуктивності

Для виконання моніторингу мережного трафіку, нам необхідно в Системний монітор додати конкретний лічильник. Наприклад, операційна система Windows підтримує кілька лічильників, які дозволяють відслідковувати процеси, які виконуються в системі. Дані цих лічильників можна переглядати в оснащенні Системний монітор. Для моніторингу мережного трафіку будем використовувати лічильники із групи «Мережний інтерфейс»: Всього байт/с, Відправлено байт/с, Відправлено пакетів/с, Отримано байт/с, Отримано пакетів/с. Для додавання лічильників продуктивності, виконайте такі дії :

- Відкрийте утиліту «Системний монітор» ;
- Вибрати команду « Додати лічильники » одним із таких способів:
  - Натиснути на кнопку "Додати" на панелі інструментів ;
  - Натиснути правою кнопкою миші на панелі відомостей з графіком продуктивності і з контекстного меню вибрати команду «Додати лічильники».

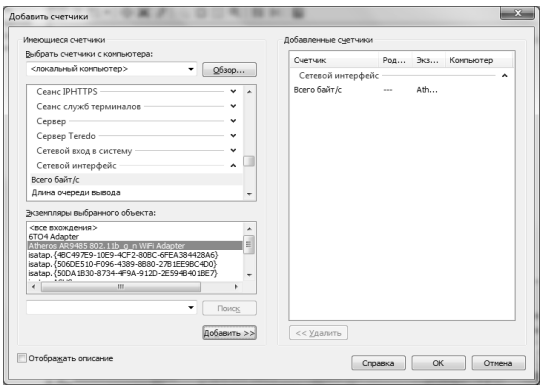

Рисунок 2

●У діалоговому вікні «Додати лічильники» нам належить вибрати наступне:

— У групі « Вибрати лічильники з комп'ютера» вкажемо комп'ютер, за яким вестиметься спостереження. Типово вибрано локальний комп'ютер, на якому відкрита сама утиліта. За бажанням можна вказати ім'я іншого комп'ютера.

— У групах наявних лічильників виберемо групу «Мережний інтерфейс» і з неї такі об’єкти перевірки: Всього байт/с, Відправлено байт/с, Відправлено пакетів/с, Отримано байт/с, Отримано пакетів/с

— Група « Примірники вибраного об'єкту » призначена для вибору лічильника продуктивності, який буде відображатися на самій діаграмі в утиліті "Системний монітор». Для того щоб вибрати зазначений лічильник – виділимо його та натиснемо на кнопку "Додати", яка розташована в нижній лівій частині даного діалогового вікна . При необхідності можна додати одразу кілька лічильників, вибравши їх із списку, утримуючи клавішу CTRL . Крім цього можна додати відразу всю групу, просто вибравши її та натиснувши на кнопку «Додати ». Варто звернути увагу на те, що елемент _Total призначений для відображення суми значень всіх примірників певного лічильника .

— Типово в утиліті «Системний монітор» відображається лічильник «Відомості про процесор (_Total) % завантаженості процесора».

— Також, в цьому діалоговому вікні для спрощення знаходження необхідних об'єктів, можна скористатися функціоналом пошуку примірників лічильників. Для цього достатньо вибрати групу лічильників, виділити конкретний об'єкт продуктивності і в списку під полем «Примірники вибраного об'єкту» ввести ім'я необхідного процесу, а потім натиснути на кнопку «Знайти».

— Якщо ви сумніваєтеся в призначенні обраного лічильника, то можете переглянути його докладний опис. Для цього потрібно встановити

прапорець «Відображати опис», розташований у лівому нижньому куті даного діалогового вікна. Після того як прапорець буде встановлений, опис буде змінюватися при виборі кожного лічильника продуктивності.

— Після вибору всіх необхідних лічильників, натиснути на кнопку «ОК» для збереження зазначених нами лічильників продуктивності.

Після того як необхідні лічильники продуктивності були додані, діаграма буде виглядати приблизно так :

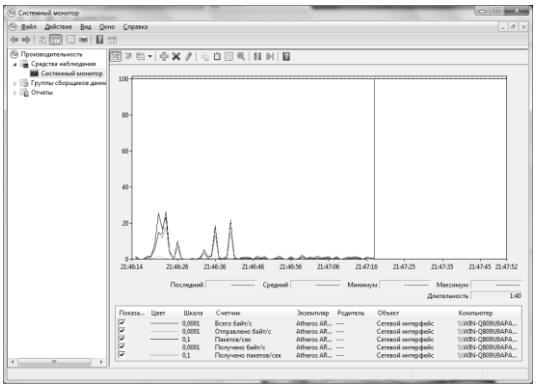

Рисунок 3

<u>Видалення лічильників продуктивності</u>

При проведенні аналізу продуктивності системи може знадобитися видалити кілька лічильників з отриманого звіту. Видалити лічильники можна так само просто, як і додати . Для цього виконайте одну з таких дій :

- в області відомостей оснащення «Системний монітор» виділіть лічильник, який потрібно видалити і натиснути на клавішу «Видалити» на панелі інструментів ✕;
- відкрийте діалогове вікно властивостей оснащення, перейдіть на вкладку «Дані », вибрати лічильник , який для подальшого аналізу нам більше не потрібно (також можна вибрати відразу кілька лічильників, утримуючи клавішу CTRL) і натиснути на кнопку «Видалити».

Якщо у нас одночасно відображаються кілька лічильників, а на даний момент необхідно стежити тільки за певними, можна приховати всі непотрібні на даний момент лічильники. Для цього, утримуючи клавішу CTRL, виділіть на легенді кілька лічильників, натиснути правою кнопкою миші і вибрати команду «Сховати виділені лічильники». Також можна з кожного непотрібного лічильника знімати прапорці у стовпці «Показувати». Коли нам потрібно буде заново відобразити всі приховані лічильники, виділіть їх, натиснути на легенді правою кнопкою миші і з контекстного меню вибрати команду «Показати виділені лічильники».

Можна виділити конкретний лічильник, щоб він відображався з напівжирним зображенням . Для цього вибрати певний лічильник на легенді, а

потім натиснути на кнопку «Виділити»,  яка розташована на панелі інструментів. Для того щоб зняти виділення з лічильника, натиснути ще раз на кнопку «Виділити».

Збереження звіту про продуктивність

Функціональніс системного монітора дозволяє нам зберігати отримані звіти у формат HTML і в графічний формат для подальшого використання та вивчення.

Для того щоб зберегти звіт в HTML форматі, клацніть правою кнопкою миші на панелі відомостей і з контекстного меню вибрати команду "Зберегти параметри як ». Типово звіт зберігається з розширенням *. html і його можна буде відкрити в будь-якому браузері . Також із списку « Тип файлу » можна вибрати розширення . tsv. Цей формат використовується для експорту даних з журналу в електронні таблиці.

Крім цього можна зберегти діаграму у вигляді файлу зображення з розширенням *. gif . Для цього клацніть правою кнопкою миші на панелі відомостей і з контекстного меню вибрати команду "Зберегти образ як ».

ГРУПИ ЗБИРАЧІВ ДАНИХ

Групи збирачів даних збирають системну інформацію, в тому числі параметри і дані продуктивності, і зберігають їх у файлі даних. Також група збирачів даних може створюватися, а потім окремо записуватися, об'єднуватися з іншими групами збирачами даних у файлах журналів, відображатися для перегляду у вікні системного монітора, генерувати повідомлення з досягнення порогових значень або використовуватися додатками сторонніх розробників і багато іншого. Після того як група збирачів даних зберігає свої дані у файлі, цей файл можна використовувати для аналізу докладних відомостей продуктивності в системному моніторі або для перегляду звіту. За бажанням, можна налаштувати автоматичний запуск завдань інструментарію керування Windows після закінчення роботи групи збирачів даних.

Для отримання інформації про продуктивність можна використовувати стандартні групи збирачів даних, а можна створити свої власні, додавши необхідні нам збирачі даних.

У лівому меню відкрийте Продуктивність - > Групи збирачів даних - > Системний.

System Diagnostics (Діагностика системи) створює докладний звіт про стан локальних ресурсів устаткування, час відгуку системи і процеси локального комп'ютера, що містить також системні і конфігураційні дані. Цей звіт містить рекомендації щодо підвищення продуктивності та прискоренню системних операцій. Натиснути правою кнопкою миші пункт System Diagnostics

(Діагностика системи) і в контекстному меню натиснути Пуск . Час виконання діагностики за замовчуванням - 1 хвилина.

System Performance в основному використовується для виявлення можливих проблем, пов'язаних з продуктивністю системи. Він реєструє 14 різних лічильників продуктивності, включаючи деякі лічильники та шаблону System Diagnostics, і також реєструє дані протягом хвилини;

<u>Створення груп збирачів даних</u>

Створення групи збирачів даних безпосередньо за допомогою вузла «Системний монітор»

Найпростішим способом створення групи збирачів даних є створення такої групи безпосередньо з вузла «Системний монітор». Для того щоб створити групу збирачів даних цим способом, виконайте такі дії :

У дереві консолі натиснути правою кнопкою миші на вузлі «Системний монітор» і з контекстного меню вибрати команду « Створити», а потім «Група збирачів даних», як показано нижче ;

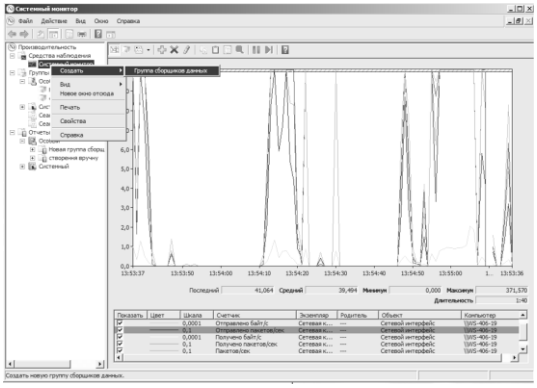

Рисунок 4

На першій сторінці діалогового вікна майстра створення груп збирачів даних, вказати назву своєї групи і натиснути на кнопку «Далі», як показано нижче:

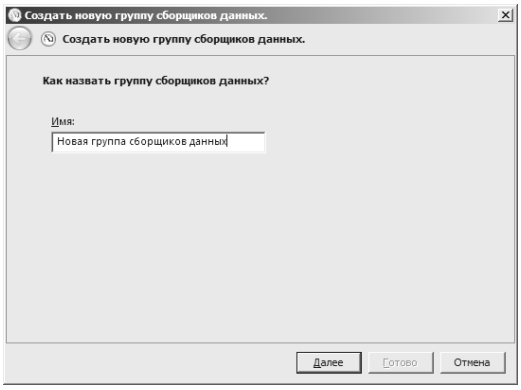

Рисунок 5

На наступному кроці, на сторінці «Де необхідно зберігати дані » можна вказати папку, в якій будуть розташовані дані, що збираються цією групою збирачів даних. Типово дані будуть розташовані в папці% systemdrive %

PerfLogsAdmin Група відомостей про процесор, де ім'ям останньої папки є назва нашої групи ;

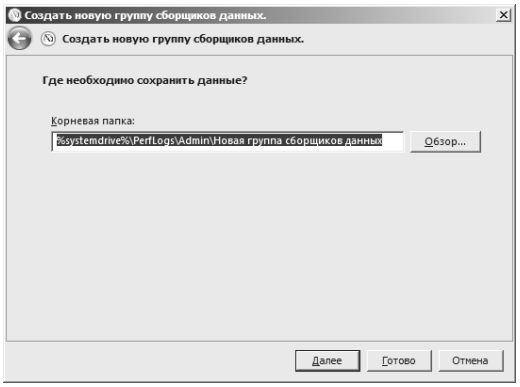

Рисунок 6

На наступному кроці належить вказати користувача, від імені якого буде запускатися група збирачів даних. Для того щоб змінити користувача, натиснути на кнопку "Змінити" і в діалоговому вікні вибору користувача для набору збирачів даних вибрати користувача, який належить до групи «Адміністратори». Після того як користувач буде обраний можна встановити перемикач на опцію «Запустити групу збирачів даних зараз» і після натискання на кнопку «Готово» автоматично запуститься група збирачів даних.

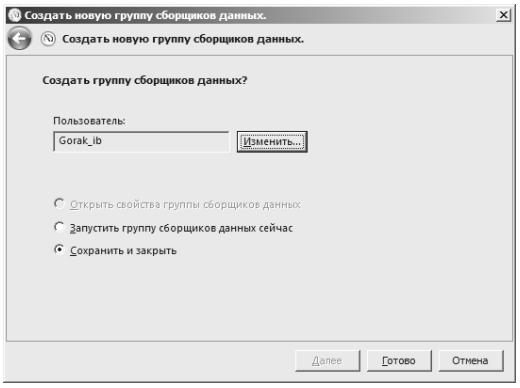

Рисунок 7

Створення групи збирачів даних за допомогою шаблону

Крім способу, зазначеного в попередньому підрозділі, можна створювати групи збирачів даних за допомогою шаблонів. Самі шаблони груп збирачів даних зберігаються у вигляді XML - файлів, які можна імпортувати або експортувати. Для того щоб створити групу збирачів даних , використовуючи встановлені шаблон, виконують такі дії :

У дереві консолі відкрити вузол «Групи збирачів даних» і клацнути правою кнопкою миші на дочірньому вузлі «Особливий». У контекстному меню вибрати команду «Створити», а потім «Група збирачів даних».

На сторінці « Як створювати нову групу збирачів даних» ввести у текстовому полі назву створюваної групи і встановити перемикач на опцію «Створити з шаблону», після чого натиснути на кнопку «Далі».

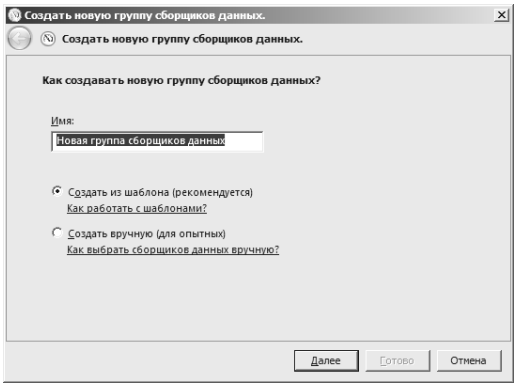

Рисунок 8

На наступному кроці, сторінці «Які шаблони слід використовувати», вибрати один з встановлених шаблонів або натиснути на кнопку "Огляд" і вказати шлях до xml -файлу шаблону, після чого натиснути на кнопку «Далі». В операційних системах Windows 7 і Windows Server 2008 R2 доступні наступні стандартні шаблони :

System Diagnostics та System Performance створенні на основі стандартних груп збирачів даних.

Основний. Він реєструє всі лічильники продуктивності об'єкта «Відомості про процесор», зберігає копію розділу системного реєстру HKLMSoftwareMicrosoftWindows NTCurrentVersion і формує звіт про хід виконання. Пізніше можна відредагувати його властивості, додаючи або видаляючи додаткові лічильники продуктивності.

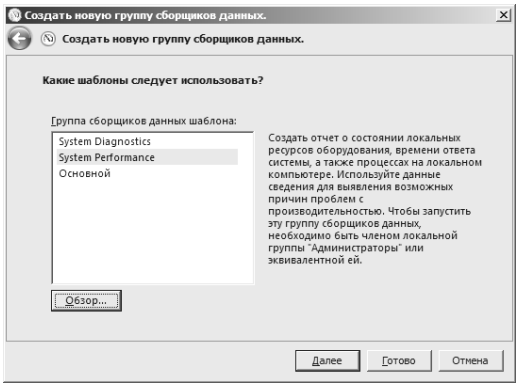

Рисунок 9

Наступні кроки процедури створення групи збирачів даних аналогічні представленим у попередньому підрозділі. Тобто, на сторінці «Де необхідно зберегти дані » вказати розміщення даних, а на сторінці «Створити групу збирачів даних» відкрити діалогове вікно налаштування групи збирачів даних, запустити групу або просто зберегти створену групу збирачів даних не виконуючи додаткових дій .

Створення групи збирачів даних вручну

При створенні груп збирачів даних можна не тільки створювати такі групи з вузла «Системний монітор » на основі активних на даний момент лічильників продуктивності або користуватися встановленими шаблонами. Можна створити нову групу з довільного набору лічильників даних, в які можуть входити різні лічильники. Для того щоб створити групу збирачів даних вручну, виконаємо такі дії:

Відкрити майстер створення груп збирачів даних тим же способом, який був описаний у попередньому підрозділі;

На сторінці «Як створювати нову групу збирачів даних» ввести у текстовому полі назву створюваної групи і встановіть перемикач на опцію «Створити вручну», після чого натиснути на кнопку «Далі»;

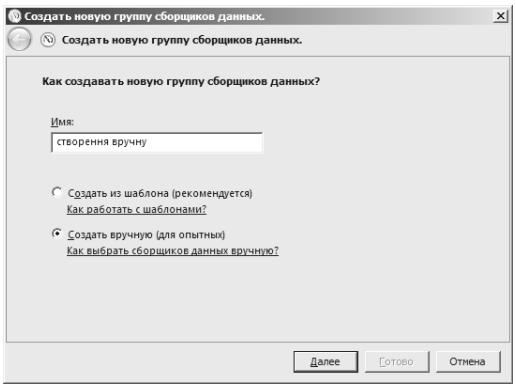

Рисунок 10

На сторінці «Який тип даних необхідно використовувати» встановити перемикач на опції «Створити журнал даних» і встановити прапорці на тих типах збирачів даних, для яких потрібно виконувати збір. Можна вибрати будь-який з наступних трьох типів, куди потім можна додати будь-яку кількість лічильників:

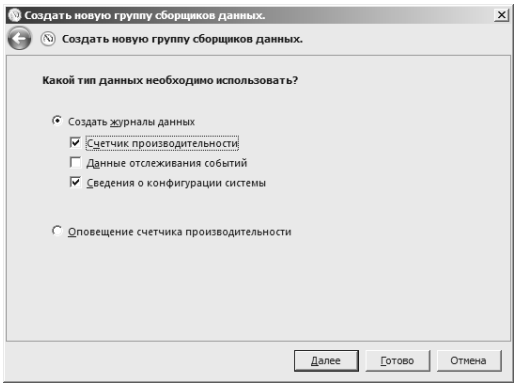

Рисунок 11

Лічильник продуктивності. Даний тип реєструє дані будь-якого лічильника продуктивності, доступного при використанні оснащення «Системний монітор». У складальник даних можна додати будь-яку кількість лічильників і призначити інтервал вибірки, який за замовчуванням дорівнює 15 секундам. В

нашому випадку виберемо лічильники із групи «Мережний інтерфейс»: Всього байт/с, Відправлено байт/с, Відправлено пакетів/с, Отримано байт/с, Отримано пакетів/с.

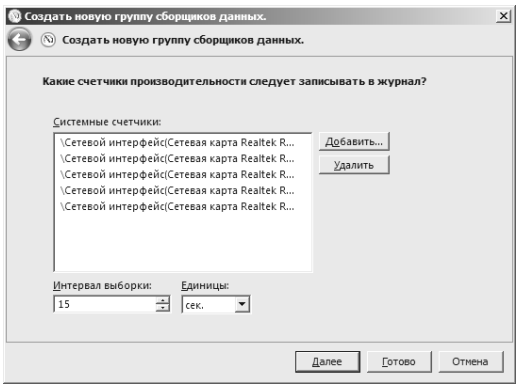

Рисунок 12

Діалогове вікно «Які лічильники продуктивності слід записувати в журнал» відображається в тому випадку, якщо на попередній сторінці був встановлений прапорець на опції «Лічильник продуктивності». У цьому випадку, після натискання на кнопку «Додати» відкриється діалогове вікно додавання лічильників, де потрібно буде вибрати лічильники.

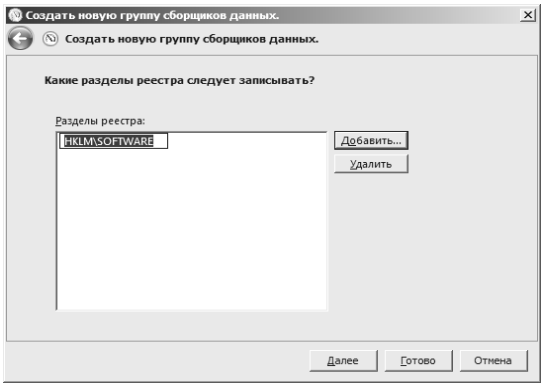

Рисунок 13

Наступні кроки процедури створення групи збирачів даних аналогічні представленим у попередньому підрозділі.

Звіт роботи групи збирачів даних

Запустимо стандартну групу збирачів даних System Diagnostics. Для цього у дереві консолі відкрити вузол «Групи збирачів даних» а потім дочірній вузол «Системний». Клікнути правою клавішею миші на групі і вибрати пункт «пуск».

Після закінчення звіт про його роботу можна подивитися у вузлі «Звіти» дерева консолі.

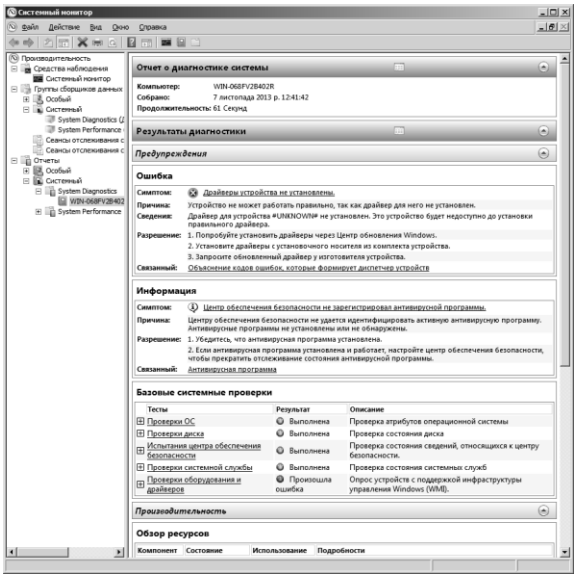

Рисунок 14

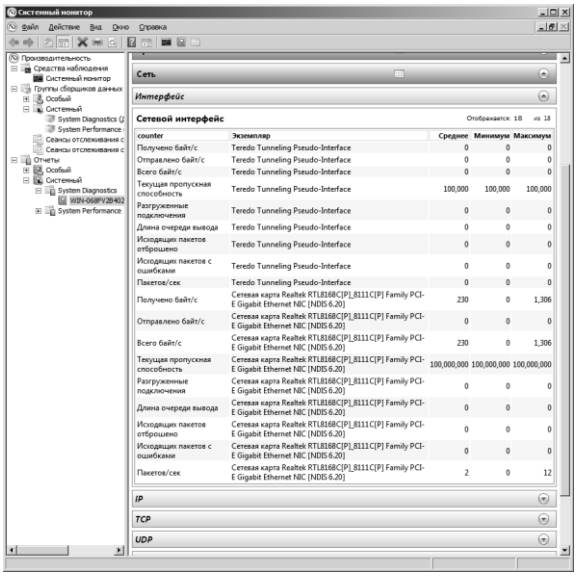

Рисунок 15

Запустивши групу збирачів даних створену вручну, отримаємо такий результат:

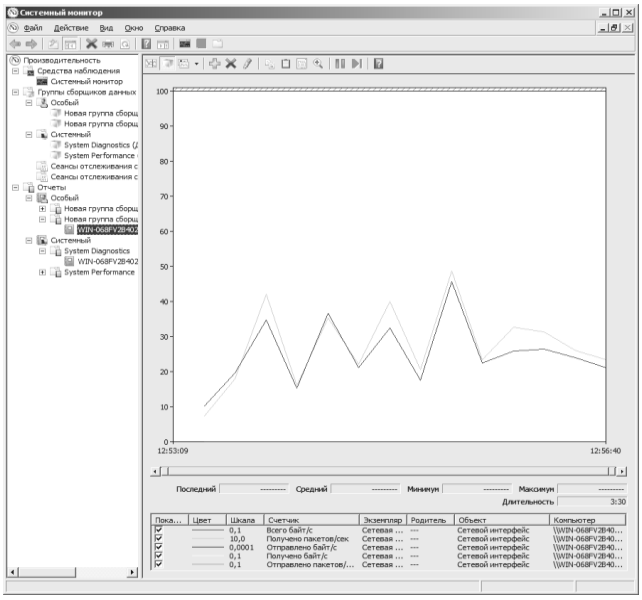

Рисунок 16

ВИСНОВОК

Системний монітор Windows - це оснащення панелі керування, що надає засоби аналізу продуктивності системи, зокрема мережного трафіку. За допомогою однієї консолі можна в реальному часі здійснювати контроль за кількістю вхідного та вихідного трафіку, вибирати дані, які будуть зберігатися у файлах журналів, задавати порогові значення для оповіщень і автоматичних дій, генерувати звіти і переглядати історію, використовуючи різні способи зберігання.

Використані ресурси

1. Довідка по Системному моніторі
2. Як працювати з лічильниками в утиліті Системний монітор : [Електронний ресурс]. – Режим доступу до документа: http://support.microsoft.com/kb/305610/ru
3. Системний монітор Windows: [Електронний ресурс]. – Режим доступу до документа: http://technet.microsoft.com/ru-ru/library/cc749249.aspx
4. Утиліта Системний монітор [Електронний ресурс]. – Режим доступу до документа: http://windata.ru/windows-xp/optimizaciya-xp/utilita-sistemnyj-monitor/
5. Системний монітор: [Електронний ресурс]. – Режим доступу до документа http://pk-help.com/server/perfmon/
6. Системний монітор Windows 7: [Електронний ресурс]. – Режим доступу до документа http://www.wseven.info/system-monitor/