УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»

Коледж економіки, права та інформаційних технологій

Циклова комісія з програмної інженерії

Циклова комісія з комп'ютерних наук

АДМІНІСТРУВАННЯ ПРОГРАМНИХ СИСТЕМ І КОМПЛЕКСІВ

Методичні рекомендації для виконання практичних занять

Для студентів спеціальностей 121 «Інженерія програмного забезпечення»
122 «Комп'ютерні науки»

Київ – 2017 р.

УДК 004.416

Розглянуто на засіданні циклової комісії з програмної інженерії протокол № 7 від «20» березня 2017 р. Рекомендовано до видання методичною радою Коледжу економіки, права та інформаційних технологій Університет економіки та права «КРОК» протокол № 5 від «24» березня 2017 р

Укладач: Ю.Є. Добришин, кандидат технічних наук, доцент кафедри комп'ютерних наук Навчально-наукового інституту інформаційних та комунікаційних технологій «Університет економіки та права «КРОК»

АДМІНІСТРУВАННЯ ПРОГРАМНИХ СИСТЕМ І КОМПЛЕКСІВ [Текст]: методичні рекомендації для виконання практичних занять / [уклад.: Ю. Є. Добришин,]; Університет економіки та права «КРОК» – Київ - 2017. – 49 с.

Методичні рекомендації для виконання практичних занять містять теоретичні та практичні питання з найбільш важливих тем навчальної дисципліни «Адміністрування програмних систем і комплексів» та визначають порядок та технологію виконання технологічних операцій з адміністрування сучасних програмних систем та комплексів.

Видання призначене для студентів спеціальностей 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» денної форми навчання.

РОЗГЛЯНУТО І СХВАЛЕНО
Педагогічною радою Коледжу економіки, права та інформаційних технологій
Протокол № 5 від «24» березня 2017 р.

УДК 004.416

ЗМІСТ

ВСТУП..... 4

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ..... 5

КРИТЕРІЇ ОЦІНКИ ВИКОНАННЯ ПРАКТИЧНОЇ РОБОТИ..... 7

Практичне заняття №1 Перевірка стану служб операційного середовища Windows..... 8

Практичне заняття №2 Моніторинг операційної системи за допомогою програмного забезпечення Performance Monitor..... 18

Практичне заняття №3 Перевірка програмного забезпечення ПЕОМ на наявність комп'ютерних вірусів. 23

Практичне заняття №4 Перегляд журналів подій та системного журналу безпеки операційної системи Windows 30

Практичне заняття №5 Перевірка функціонування та величини завантаження локальної мережі, швидкості та активності мережевого серверу..... 40

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАНЯТТЬ..... 49

РЕКОМЕНДОВАНА ЛІТЕРАТУРА 49

ВСТУП

Метою навчальної дисципліни «Адміністрування програмних систем та комплексів» є формування у слухачів сучасного рівня інформаційної та програмістської культури, отримання знань та практичних навиків з виконання операцій з адміністрування програмних систем та комплексів, оволодіння методиками та правилами планування заходів щодо здійснення основних операції з адміністрування операційних систем та баз даних, програмних додатків та мережевих компонентів, розташованих на базі сучасного серверного обладнання та персональних комп'ютерів.

Програма дисципліни передбачає проведення практичних занять з застосуванням комп'ютерів, локальних мереж та мережі Internet у комп'ютерних класах.

Завданнями, які ставляться на практичних заняттях є формування практичних навичок у відповідності з поставленою метою. За результатами вивчення навчальної дисципліни **студенти повинні вміти:**

1. Виконувати операції з встановлення, налаштування та адміністрування системного та загальносистемного програмного забезпечення сучасних операційної системи (ОС) Windows.
2. Встановлювати, налагоджувати програмне забезпечення на основі клієнт серверної архітектури.
3. Виконувати практичні роботи з ліквідації збоїв в роботі програмного забезпечення.
4. Проводити моніторинг продуктивності роботи та підтримувати працездатність програмних систем і комплексів в процесі їх супроводження та системотехнічного обслуговування.
5. Виконувати роботи з адміністрування та супроводження мережного програмного забезпечення автоматизованих систем та комплексів, здійснювати операції з налагодження роботи DNS та DHCP сервера, програмних компонентів локальної мережі.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теми навчальної дисципліни «Адміністрування програмних систем та комплексів»
Тема 1. Завдання та мета системного адміністрування.
Тема 2. Системне адміністрування програмного забезпечення операційної системи Windows
Тема 3. Адміністрування програмних засобів мережі ОС Windows
Тема 4. Моніторинг та відновлення роботи серверного програмного забезпечення ОС Windows.
Тема 5. Особливості адміністрування операційної системи з відкритим кодом.
Тема 6. Адміністрування мережі під керівництвом Linux сервера.
Тема.7. Адміністрування СКБД MS SQL Server
Тема.8. Резервне копіювання та відновлення бази даних MS SQL Server
Тема.9. Структурні компоненти СКБД Oracle
Тема.10. Файли даних СКБД Oracle
Тема.11. Резервне копіювання файлів СКБД Oracle

Теми практичних занять

№ з/п	**Назва теми**
1	Перевірка стану служб операційного середовища Windows. Моніторинг завантаженості операційної системи Windows
2	Моніторинг операційної системи за допомогою програмного забезпечення «Performance Monitor»
3	Перевірка програмного забезпечення ПЕОМ на наявність комп’ютерних вірусів
3	Перегляд журналів подій та системного журналу безпеки операційної системи Windows
5	Перевірка функціонування та величини завантаження локальної мережі, швидкості та активності мережевого серверу

Теми лабораторних занять

№ з/п	**Назва теми**
1	Перевірка зберігання облікових записів користувачів
2	Аналіз вільного місця на жорстких дисках. Виконання та де фрагментації дискової пам’яті, очищення тимчасових каталогів операційної системи
3	Аналіз і перегляд працездатності DNS серверу
4	Перевірка функціонування та завантаження локальної мережі шляхом тестування
5	Перевірка працездатності драйверів та їх переустановлення

Самостійна робота

№ з/п	Назва теми
1	**Тема 1.** Характеристика серверних операційних систем Windows. Поняття домену. Встановлення та налаштування Active Directory ОС Windows
2	**Тема 2.** Встановлення та налаштування DNS та DHCP сервера ОС Windows
3	**Тема 3**. Адміністрування сервера терміналів. Налаштування та адміністрування служби маршрутизації та віддаленого доступу.
4	**Тема 4.** Тестування роботи жорстких дисків системи, визначення збійних блоків та їх відновлення засобами ОС.
5	**Тема 5**. Встановлення та налаштування серверної операційної системи Linux.
6	**Тема 6**. Організація політик безпеки облікових записів користувачів
7	**Тема 7.** Фізична та логічна структура СКБД MS SQL Server
8	**Тема 8.** Програмні засоби, що використовуються для виконання резервного копіювання файлів даних СКБД MS SQL Server
9	**Тема 9.** Склад екземпляра та служби СКБД Oracle
10	**Тема 10.** Програмні засоби адміністрування СКБД. SQL Developer та SQL Plus, Enterprise Manager
11	**Тема 11.** Моніторинг використання пам’яті екземпляра та вільного міста в табличних просторах бази
12	**Тема 12.** Програма RMAN. Поняття холодного та гарячого резервного копіювання.
13	**Тема 13.** Відновлення роботи СКБД Oracle

КРИТЕРІЇ ОЦІНКИ ВИКОНАННЯ ПРАКТИЧНОЇ РОБОТИ

Основа мета перевірки виконання практичних занять – виявлення здатності студента застосовувати одержані теоретичні знання на практиці.

Оцінка за виконання практичного заняття ставиться як середньоарифметична суми оцінок безпосередньо за виконану роботу та захист.

Оцінка “відмінно” ставиться, якщо результати виконання роботи збігаються з результатами контрольного прикладу, завдання до практичної роботи виконані в повному обсязі, студент демонструє знання про матеріали роботи на рівні 90–100 %.

Оцінка “добре” – якщо результати виконання роботи частково збігаються з результатами контрольного прикладу, завдання до практичної роботи виконані в повному обсязі, але студент демонструє знання матеріалів практичної роботи на рівні 75–90 %.

Оцінка “задовільно” – якщо результати виконання роботи частково збігаються з результатами контрольного прикладу, завдання до практичної роботи виконані не в повному обсязі, студент демонструє знання наведеного матеріалу роботи на рівні 50–75 %.

Оцінка “незадовільно” – якщо студент не виконав завдання, що зазначені у практичної роботі, не відповідає на теоретичні питання, які відносяться до теми роботи.

Практичне заняття №1

(Перевірка стану служб операційного середовища Windows).

Метою заняття є вивчення та відпрацювання слухачами послідовності виконання технологічних операцій з перевірки переліку та стану працездатності служб операційної системи Windows (далі – ОС) та порядку проведення моніторингу завантаженості операційної системи. Операції, що виконуються, здійснюються під обліковим записом адміністратор системи.

Практичні питання, що відпрацьовуються на занятті

1. Перевірка переліку та стану працездатності служб ОС Windows.
2. Моніторинг завантаженості операційної системи Windows.
3. Визначення розміру файлу підкачки ОС Windows.

Порядок виконання технологічних операцій :

1. Перевірка переліку та стану працездатності служб ОС на прикладі вузла ВМР.

1.1. На робочому столі операційної системи сервера бази даних або АРМ вузла за допомогою лівою кнопки миші активізувати ярлик **«Мой комп'ютер»,** далі натиснути на праву кнопку миші. У контекстному меню за допомогою лівої кнопки миші вибрати команду **«Управление»** (рис. 1).

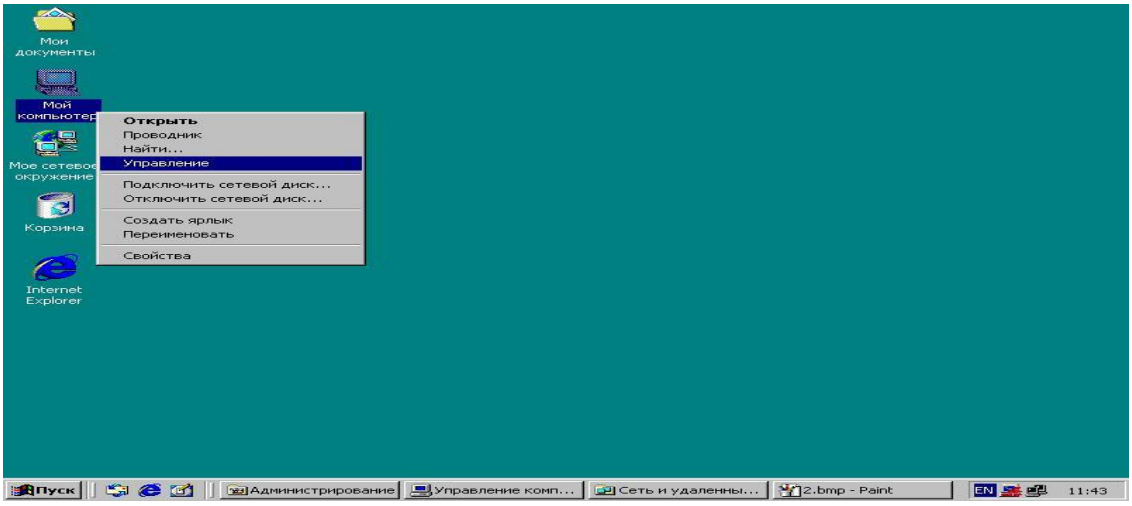


Рис 1. Виклик вікна «Управління комп'ютером»

1.2. У вікні «**Управление компьютером**» за допомогою лівої кнопки миші активізувати розділ **«Службы и приложения»**, далі **«Службы»** (рис.2).

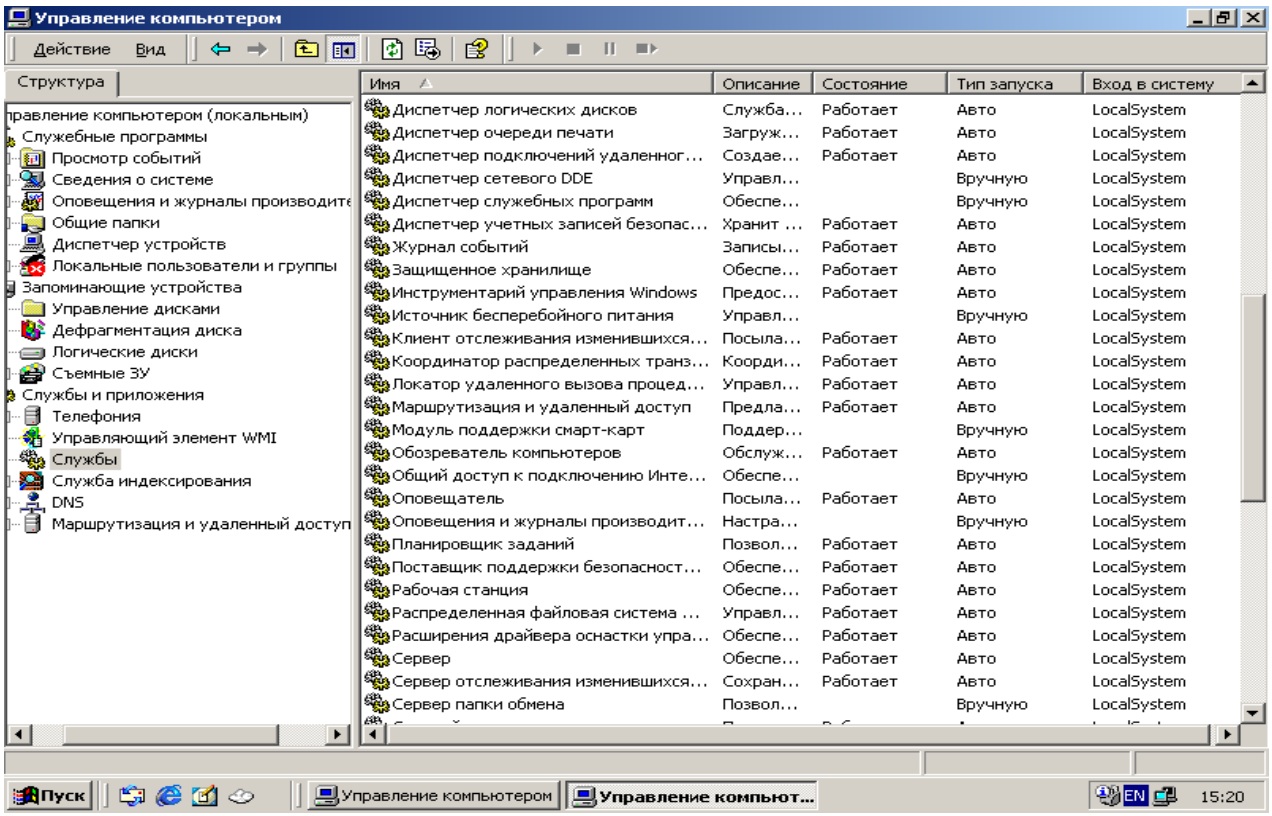


Рис. 2. Виклик вікна «Службы»

1.3. Перевірити перелік, стан завантаження та тип запуску служб операційної системи Windows. Під час перевірки стану служб, особливо звернути увагу на запуск служб, які забезпечують працездатність спеціалізованого програмного забезпечення та бази даних.

1.4. У разі необхідності можливо перевірити наявність та стан запуску служб за допомогою командного рядку операційної системи. Для цього на сервері бази даних вузла натиснути на кнопку **«Пуск»** панелі задач ОС, далі вибрати команду **«Выполнить»** та ввести у командному рядку команду «**cmd**» (рис. 4) далі **«ОК»**.

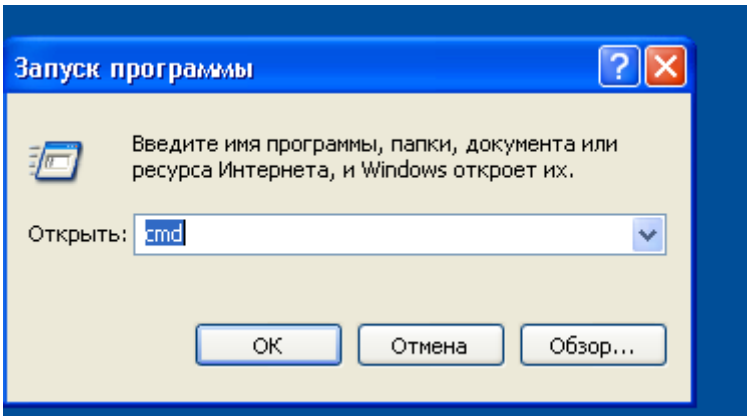


Рис. 4. Запуск команди «**cmd**»

1.5. У вікні, що з’явиться (рис. 5), ввести в командному рядку команду **«net start»**.

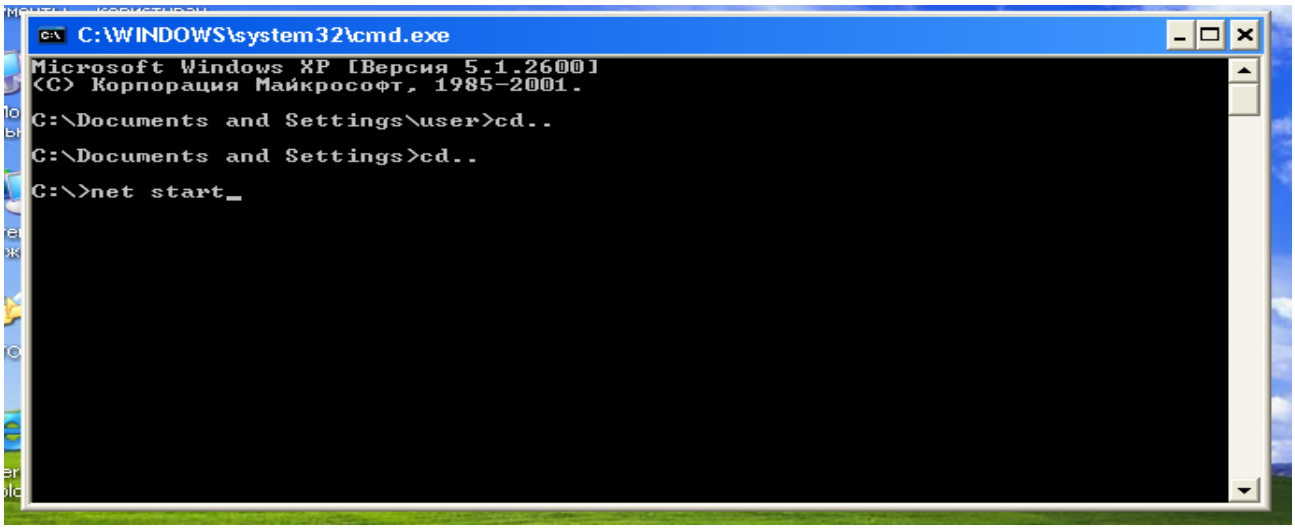


Рис. 5. Запуск команди **«net start»**

1.6. Виконати перегляд служб, які завантажені та знаходяться у працездатному стані (рис. 6).

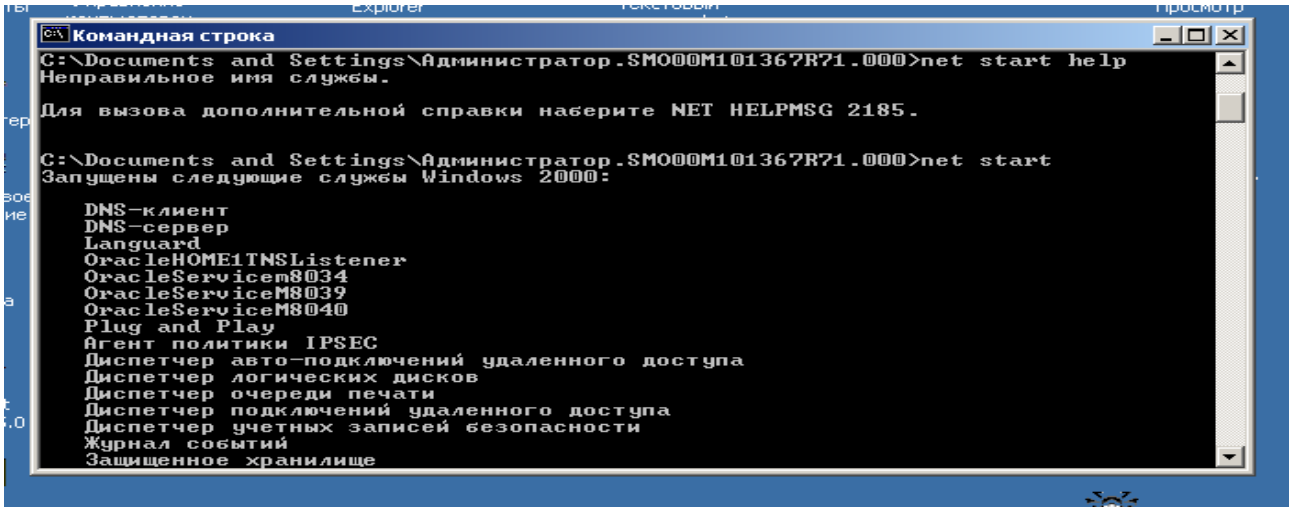


Рис 6. Вікно перегляду служб, що завантажені

1.7. У разі виявлення порушень щодо функціонування служб операційної системи, здійснити додаткові заходи з приведення служб операційної системи до працездатного стану або їх перезавантаження, для цього у вікні **«Управление компьютером»** на правої половині вікна необхідно активізувати лівою кнопкою миші службу та натиснути на кнопку «**Запуск службы**» або «**Перезапуск службы**» (рис 7).

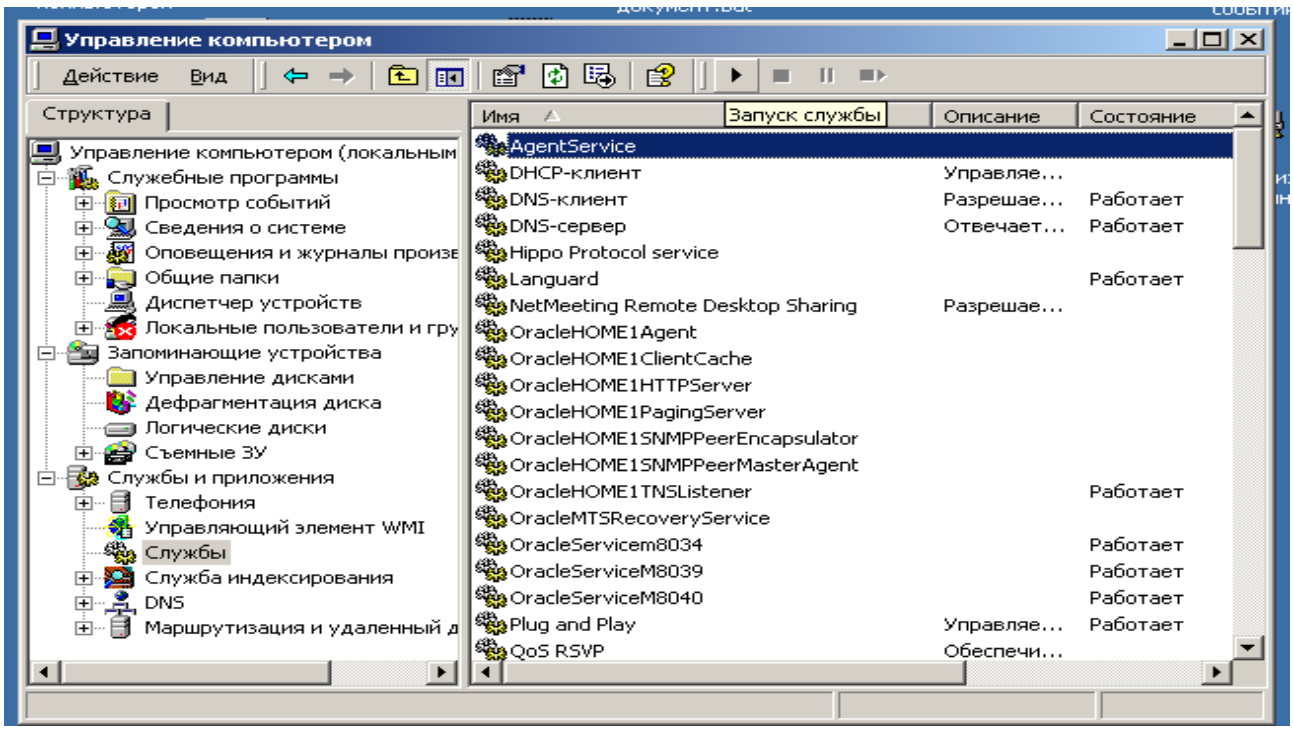


Рис 7. Порядок запуску служби

1.8. За результатами робіт зробити остаточний висновок щодо наявності та стану працездатності програмних служб ОС ПЕОМ.

2. Моніторинг завантаженості операційної системи Windows

2.1. Контроль за станом пам’яті ПЕОМ.

2.1.1. Послідовно на ПЕОМ навчального класу перевірити параметри пам’яті ОС, а саме:

- розмір фізичної оперативної пам’яті, що виділяється;
- загальний розмір пам’яті, яку на даний час займають всі процеси, що використовуються ОС.

Для цього запустити програмне забезпечення «**Диспетчер задач Windows»** та протягом 20-30 хвилин здійснити аналіз параметрів пам’яті, які використовує операційна система (рис.1).

2.1.2. На приклад, під час роботи ПЕОМ видно, що розмір фізичної оперативної пам’яті, виділений ОС складає **785904 Кб,** загальний розмір пам’яті, яку на даний час займають всі процеси ОС – **450392 Кб** (рис.1).

2.1.3. Перевірити розмір файлу підкачки оперативної пам’яті ОС, для цього лівою кнопкою миші активізувати значок **«Мой компьютер**», далі натиснути на праву кнопку миші та вибрати **«Свойства».** У вікні, що з’явиться вибрати закладку **«Дополнительно», «Параметры»,** далі закладку **«Дополнительно».**

В розділі віртуальної пам’яті визначити розмір файлу підкачки, що встановлюється для роботи ОС (рис.2.). На прикладі роботи ПЕОМ видно, що розмір файлу підкачки складає **1152** Мб, що приблизно в **1,5 рази більше** розміру встановленої фізичної пам’яті.

2.1.4. Визначити розмір пам’яті, що використовують програми (процеси), які запущені на ПЕОМ користувача (рис.3).

Для цього у вікні «**Диспетчера задач»** необхідно активізувати закладку **«Процессы»** (рис.3) та прослідкувати за станом зміни розміру пам’яті, що використовують програми які запущені.

Якщо протягом тривалого часу, програма коректна не звільняє пам’ять, що виділяється для неї, а її робочий простір постійно збільшується, це означає, що програма працює некоректно. У таких випадках погіршується продуктивність роботи ОС та збільшується її завантаженість.

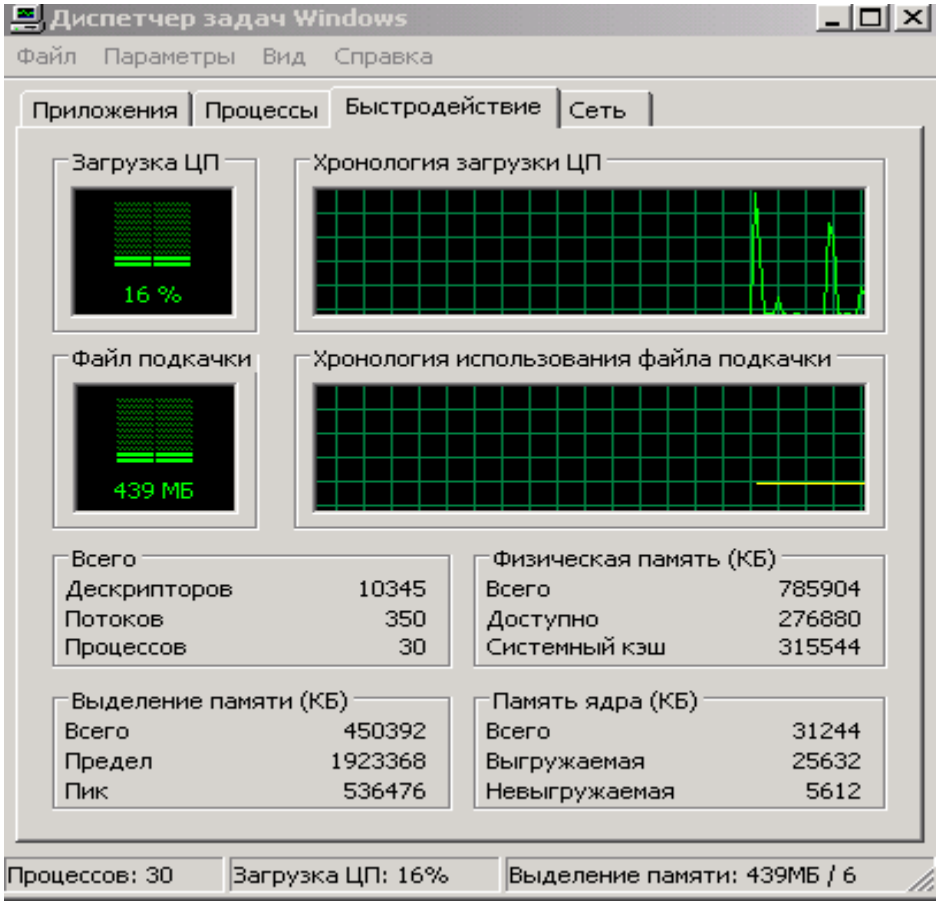


Рис.1. Від вікна Диспетчера задач Windows

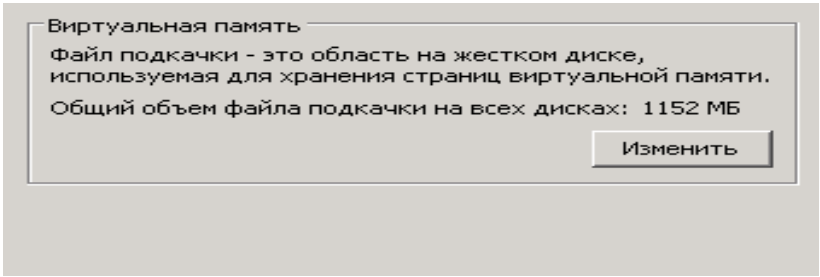


Рис.2. Визначення розміру файлу підкачки ОС Windows

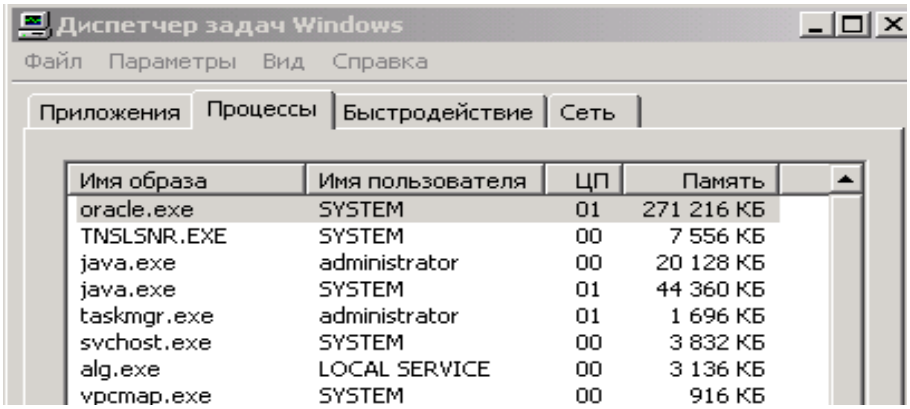


Рис.3. Від вікна щодо запущених процесів ОС Windows

2.1.5. Виконати заходи щодо усунення некоректної роботи програми шляхом її перезапуску. Якщо у подальшому витяг пам'яті для процесу (програми) продовжується, повідомити про це викладачу.

3. Визначення розміру файлу підкачки ОС Windows

3.1. Перевірити розмір файлу підкачки ОС ПЕОМ.

За рекомендаціями фірми Microsoft розмір файлу підкачки підраховується за наступною формулою: **FP*1,5**, де **FP –** розмір фізичної пам'яті **(Мб)**. Для АРМ користувача вузла ДІС, наведеного у прикладі, розмір файлу підкачки складає **785*1,5 = 1177Мб**, що приблизно співпадає з існуючим його розміром **(1152 Мб).**

3.2. Зазначений метод використовується у випадках малої фізичної пам'яті на ПЕОМ, якщо фізичної пам'яті більше, то розмір файлу підкачки потрібно встановлювати меншим.

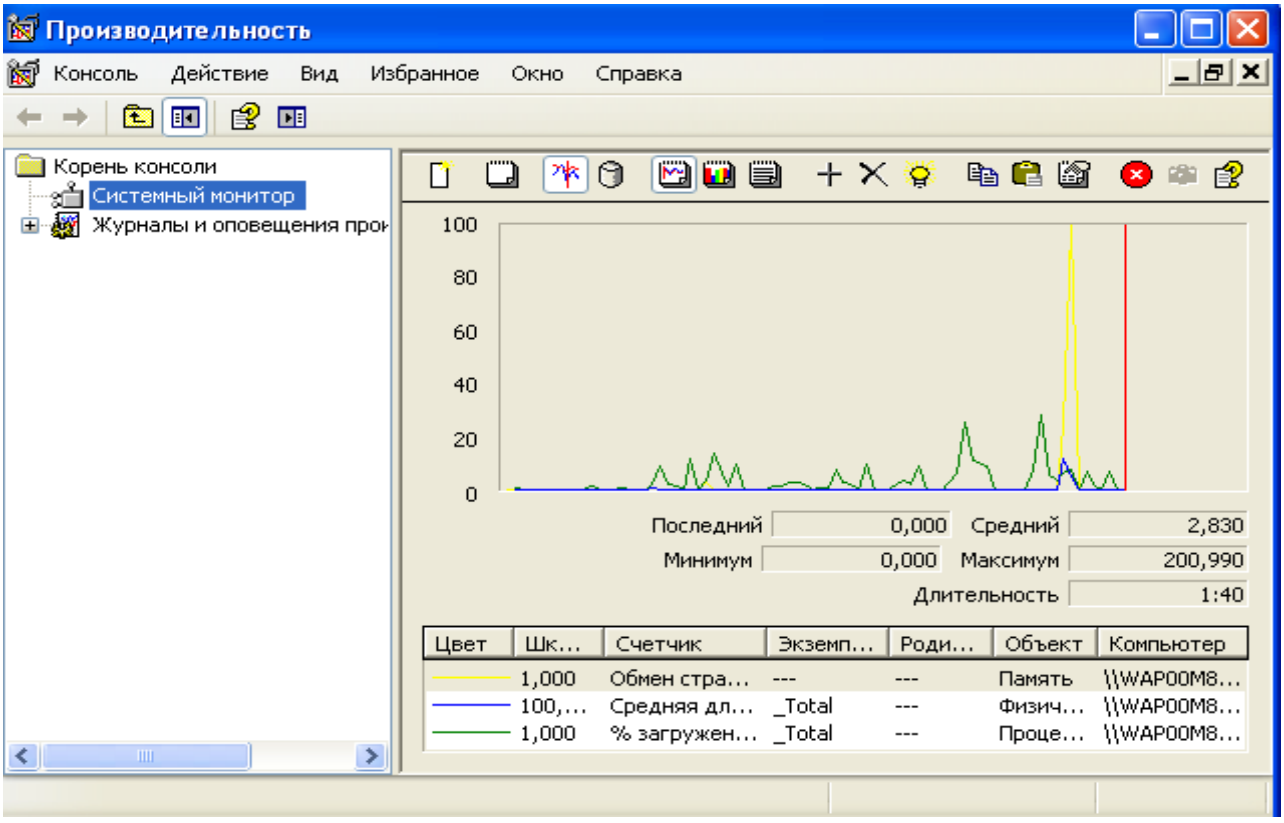
3.3. Для виконання операцій зміну розміру файлу підкачки необхідно на панелі задач операційної системи ПЕОМ натиснути на кнопку **«Пуск»**, далі **«Настройка», «Панель управления», «Администрирование»,** вибрати **«Производительность».** У вікні **«Производительность»**, активізувати розділ **«Системный монитор»**(рис.4).

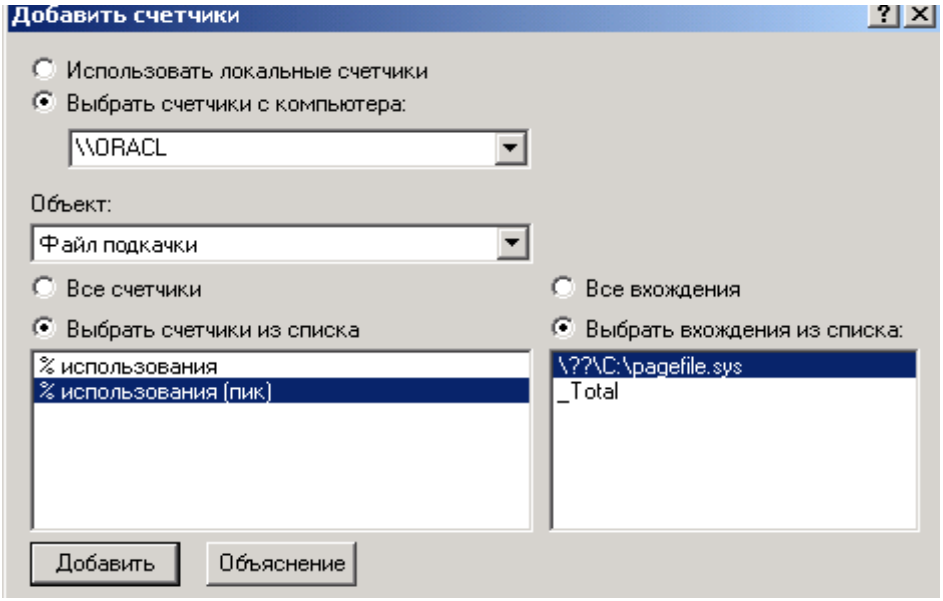
3.4. На панелі інструментів вікна **«Системный мониторинг»** натиснути на кнопку **«Добавить»**, яка має позначку «+», далі у полі з назвою **«Объект»** вибрати **«Файл подкачки»** та активізувати лічильник **«% использования», далі натиснути на кнопку «Добавить»,** після чого на кнопку **«Закрыть»** (рис.5).

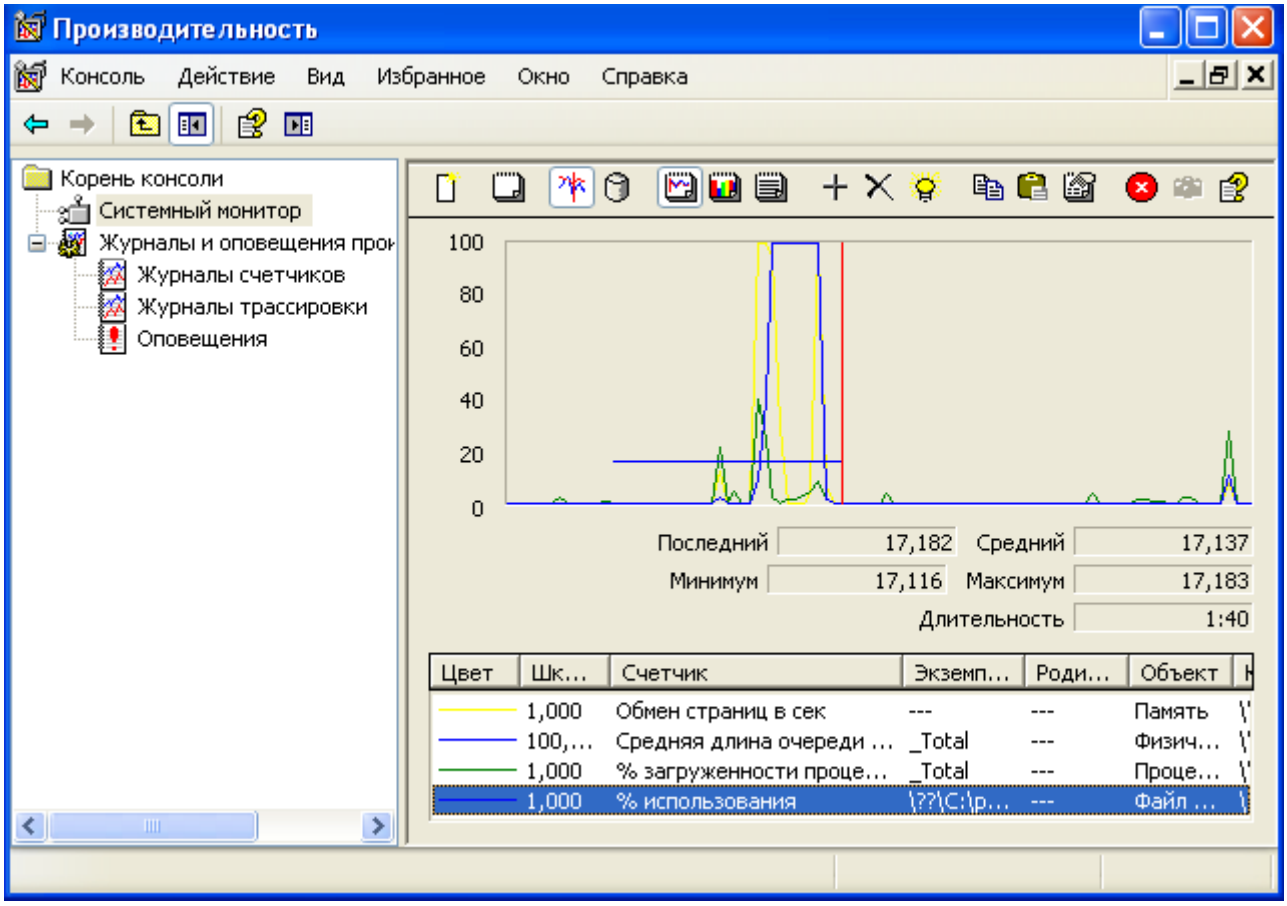
3.5. Протягом певного часу прослідкувати за використанням файлу подкачки (рис.6), після чого у вікні **«Системный мониторинг»** натиснути на кнопку **«Просмотр отчета»** та здійснити підрахунок відсотка використання файлу підкачки та визначити його середній розмір у **%** (рис.7).

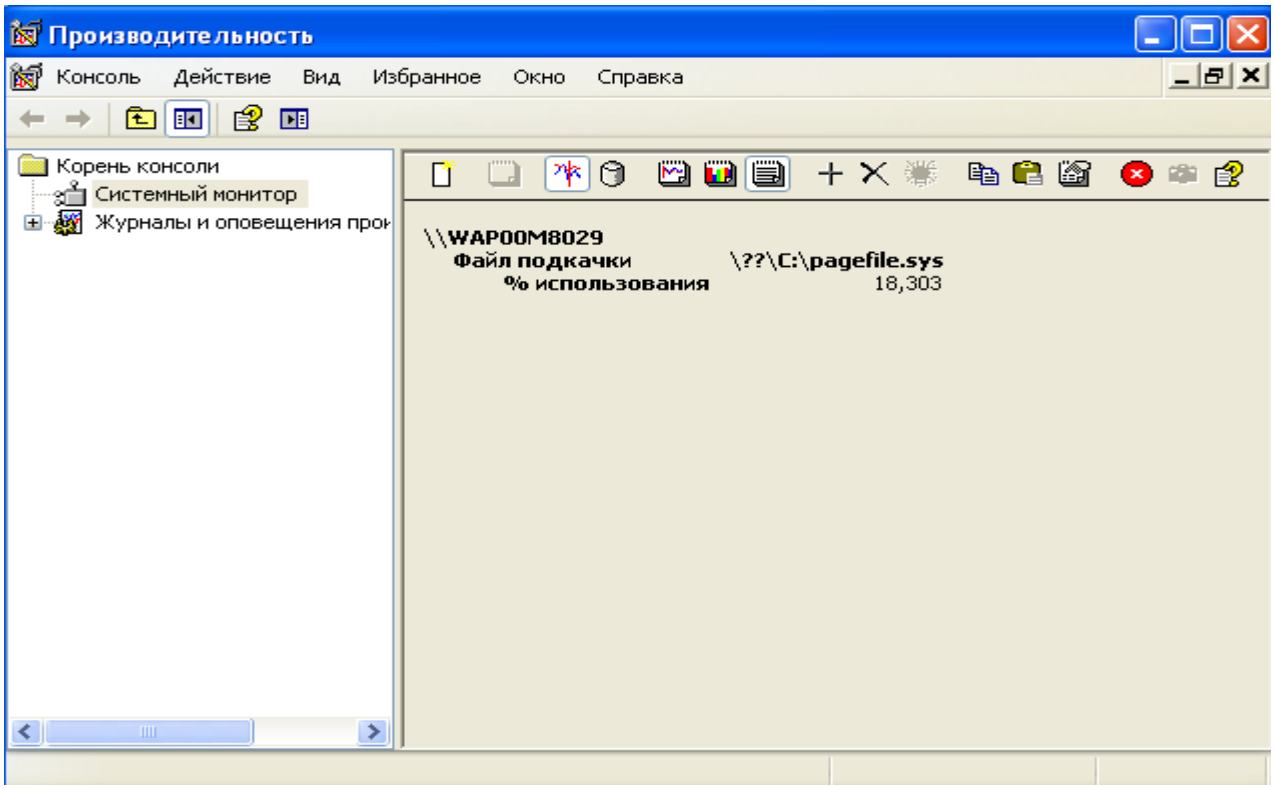
3.6. Наприклад, при пікових навантаженнях ПЕОМ відсоток використання файлу підкачки складає **40, 28, 36 и 30** середнє значення завантаженості складає **34.5%.** Якщо раніше файл підкачки для ПЕОМ був встановлений **1152 Мб** то приймаємо зазначений показник за **100%**, далі підрахуємо його остаточний розмір: **1152:100*34.5%=2*34.5%**=приблизно **398MB.** Якщо додати до визначеного розміру **20Мб** (враховуючі максимальний пик навантаження) то остаточний розмір файлу буде **418Мб**.

Примітка: Включення лічильників на ПЕОМ може сприяти погіршенню на деякій час продуктивності програмних компонентів ОС.




Добавить счетчики
Использовать локальные счетчики
Выбрать счетчики с компьютера:
\\ORACL
Объект:
Файл подкачки
Все счетчики
Выбрать счетчики из списка
% использования
% использования (пик)
Все вхождения
Выбрать вхождения из списка:
\??\C:\pagefile.sys
_Total
Добавить
Объяснение


Производительность
Консоль
Действие
Вид
Избранное
Окно
Справка
Корень консоли
Системный монитор
Журналы и оповещения прои
Журналы счетчиков
Журналы трассировки
Оповещения
100
80
60
40
20
0
Последний 17,182
Средний 17,137
Минимум 17,116
Максимум 17,183
Длительность 1:40
Цвет
Шк...
Счетчик
Экземп...
Роди...
Объект
1,000 Обмен страниц в сек --- --- Память
100,... Средняя длина очереди ... _Total --- Физич...
1,000 % загруженности проце... _Total --- Проце...
1,000 % использования \??\C:\p... --- Файл ...



3.7. Після закінчення робіт здійснити заходи з **віддалення лічильника «% использования».** Для цього у вікні **«Системный мониторинг»** на правій половині вікна активізувати лівою кнопкою миші лічильник **«% использования»,** далі натиснути на кнопку **«Удалить»,** яка має позначення **«Х».**

3.8. За результатами робіт підготувати звіт щодо завантаженості операційної системи Windows та визначення розміру файлу підкачки.

ЗРАЗОК ЗВІТУ

№ з.п.	розмір фізичної оперативної пам'яті	загальний розмір пам'яті	розмір файлу підкачки	відсоток використання файлу підкачки під час пікових навантажень

Практичне заняття №2

(Моніторинг операційної системи за допомогою програмного забезпечення Performance Monitor)

Мета заняття: перевірка параметрів (характеристик) складових ОС, розміру та витоку пам'яті, працездатності процесора, оцінку впливу параметрів налаштування на роботу ОС. У роботі виконується контроль інших параметрів, що впливають на завантаженість роботи ОС, зокрема, характеристик роботи твердих магнітних дисків.

Контроль за параметрами пам'яті та процесора здійснюється як на етапі начальної загрузки ПЕОМ, так і під час її тривалої роботи.

Практичні питання, що відпрацьовуються на занятті

1. Контроль за станом завантаженості процесора на ПЕОМ.
2. Контроль за станом завантаженості ОС Windows за допомогою програмної утиліти msconfig.exe.
3. Моніторинг завантаженості операційної системи за допомогою програмного забезпечення Performance Monitor

Порядок виконання технологічних операцій :

1. Контроль за станом завантаженості процесора на ПЕОМ

1.1. Перевірити ступень завантаженості процесора прикладними програмами або процесами, що використовує операційна система. Особливо необхідно проконтролювати те процеси, що знаходяться в циклі очікування. Такі процеси в окремих випадках створюють сто відсоткову завантаженість процесора, але не заважають роботу ПЕОМ та серверу.

1.2. Виконати перевірку загальної завантаженості процесора за допомогою вікна **«Диспечер задач».** Для цього проаналізувати стовпчик на закладці **«Процессы»** справа від назви процесів, що працюють **«ЦП»**. Цей стовпчик показує скільки відсотків від загальної завантаженості процесора займає кожний процес окремо. (рис.3.).

1.3. Якщо під час перевірки з’ясовано, що процес займає значну частину ресурсу **(наприклад більше 30%)**, то він є причиною повільної роботи АРМ або серверу. Причина зависання АРМ або серверу може буде з’ясована за результатами огляду стовпчику **«Память»,** а саме, за кількістю пам’яті, що використовує кожний процес.

1.4. Для усунення зависання ОС необхідно активізувати програму (процес), що заважає роботі, далі натиснути на праву кнопку миші, у контекстному меню вибрати команду **«Завершить процесс»**, далі натиснути на кнопку **«Да»** (рис.1).

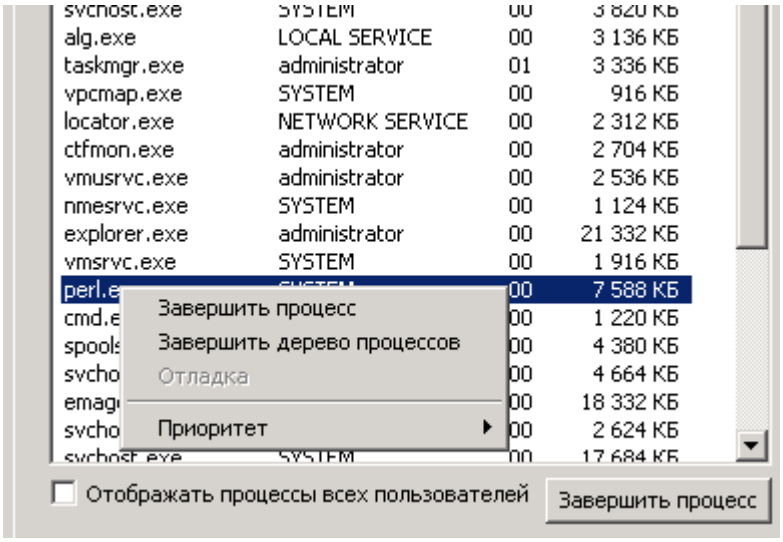


Рис.1. Відключення процесів, що заважають роботі ОС

2. Контроль за станом завантаженості ОС Windows за допомогою команди msconfig.exe

2.1 Натиснути на кнопку **«Пуск»** панелі задач ОС на ПЕОМ користувача або сервера вузла, далі необхідно вибрати кнопку **«Выполнить»**, у вікні, що з’явиться набрати команду **msconfig.exe** (рис.2). У вікні, що з’явиться активізувати закладку **«Атозагрузка»** (рис.3).

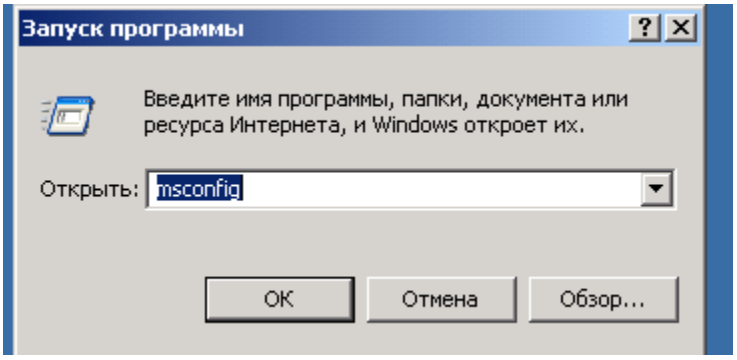


Рис.9. Запуск команди **msconfig.exe**

3.8.4.2 Перевірити перелік програм, що завантажуються разом з ОС. Якщо під час перевірки виявлено програми, які не повинні бути автоматично запущені на етапі начальної загрузки ОС, то виконати їх зупинку шляхом видалення мітки, що встановлена проти відповідної програми (рис.3).

3. Моніторинг завантаженості операційної системи за допомогою програмного забезпечення Performance Monitor

3.1. Здійснити запуск програмного забезпечення **Performance Monitor**. Враховуючи пропозиції, що наведені у таблиці визначити необхідні лічильники, що будуть використовуватися протягом виконання операцій з моніторингу завантаження ОС.

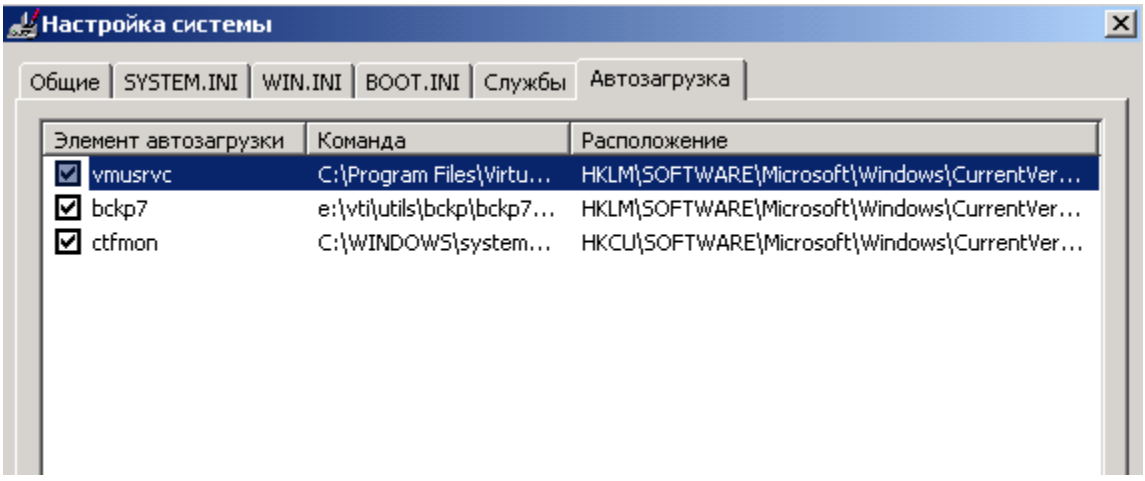


Рис.3. Відключення автозавантаження програм ОС

3.2. На протязі 40 хвилин навчального часу здійснити підрахунок необхідних характеристик завантаженості пам’яті та процесору ПЕОМ на якому

здійснювалася перевірка. Назва лічильників та об’єкти, що вони контролюють, надаються у таблиці.

Таблиця - Назва та призначення основних лічильників Performance Monitor

Об’єкт: Лічильник	**Призначення**
Process: **Working Set** (Процес: Робоче середовище)	Кількість фізичної оперативної пам’яті, що використовується процесором
Process: **Pagefile Byte**s (Процес: Байт файлу підкачки)	Кількість пам’яті, що процес використовує у файлі підкачки.
Memory: Committed Bytes (Память: Байт віртуальної пам’яті)	Загальний розмір віртуальної пам’яті, яку на даний час займають всі процеси користувачів.
Memory: Commit Limit (Память: Предел віртуальної пам’яті	Величина, яка визначає кількість віртуальної пам’яті система може надати без збільшення розміру файла підкачки.
Process: % Processor Time (Процес: % завантаженості процесора)	Ступень використання процесора заданим процесом.

3.3. Після закінчення робіт здійснити заходи з **віддалення лічильників.** Для цього у вікні **«Системный мониторинг»** на правій половині вікна активізувати лівою кнопкою миші необхідний лічильник**,** далі натиснути на кнопку **«Удалить»,** яка має позначення **«Х»**

3.4. Підготувати висновки щодо ступені завантаженості операційної системи та покращення роботи її компонентів.

3.5. За результатами робіт підготувати звіт щодо завантаженості параметрів операційної системи та надати його для захисту викладачу.

ЗРАЗОК ЗВІТУ

Об’єкт перевірки	**Призначення**	**Одиниця вимірювання**	**Середнє значення параметру**
Process: **Working Set**	Кількість фізичної оперативної пам’яті, що використовується процесором		
Process: **Pagefile Byte**s	Кількість пам’яті, що процес використовує у файлі підкачки.		
Memory: Committed Bytes	Загальний розмір віртуальної пам’яті, яку на даний час займають всі процеси користувачів.		
Memory: Commit Limit	Величина, яка визначає кількість віртуальної пам’яті система може надати без збільшення розміру файла підкачки.		
Process: % Processor Time	Ступень використання процесора заданим процесом.		

Практичне заняття №3

(Перевірка програмного забезпечення ПЕОМ на наявність комп'ютерних вірусів).

Метою роботи є виконання слухачами технологічних операцій щодо здійснення антивірусного контролю програмного забезпечення на ПЕОМ та серверному обладнанні.

Для виконання практичних робіт використовується спеціалізоване програмне забезпечення, яке встановлюється на ПЕОМ на передодні практичного заняття.

Питання, що відпрацьовуються на занятті

1. Перевірку інформації, яка надається для завантаження на ПЕОМ сервер, щодо наявності комп'ютерних вірусів.

2. Здійснення оновлення антивірусних баз.

Порядок виконання технологічних операцій:

1. Перевірка носіїв інформації на наявність комп'ютерних вірусів (антивірусний контроль).

1.1. Всі змінні носії інформації, що використовуються на ПЕОМ, потребують перевірки на наявність комп'ютерних вірусів. Перевірка носіїв інформації здійснюється на прикладі програмного забезпечення Kaspersky Antivirus.

1.2. Для перевірки необхідно, на робочому столі ПЕОМ (права половина панелі задач) переглянути наявність та стан функціонування антивірусного програмного забезпечення **Kaspersky Antivirus**, а саме, появи значка червоного коліру програми **Kaspersky Antivirus**.

Рис 1. Перевірка наявності та активності роботи **Kaspersky Antivirus**

1.3. Для роботи з програмою **Kaspersky Antivirus** необхідно активізувати значок зазначеної програми, натиснути на праву кнопку миші та у контекстному

меню вибрати команду **Антивирус Касперского** (рис.2), далі натиснути ліву кнопку миші та переглянути головне вікно програми **Антивирус Касперского** (рис.3).

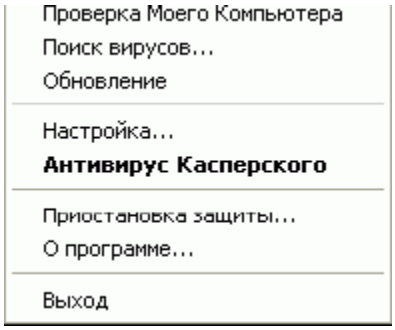


Рис 2. Вид вікна контекстного меню **«Kaspersky Antivirus»**

1.4. Здійснити перевірку змінних носіїв інформації на наявність комп'ютерних вірусів. Для цього у вікні програми **Kaspersky Antivirus** необхідно натиснути на кнопку **«Поиск вирусов»** (рис.3)**.** У вікні, що з'явиться, переглянути області комп'ютера що потребують перевірки. Для перевірки вибрати відповідний об'єкт на натиснути на кнопку **«Запустить проверку»** (рис.4). У разі необхідності необхідно виконати перевірку наявності вірусів на ПЕОМ (жорсткі диски, поштові скриньки).

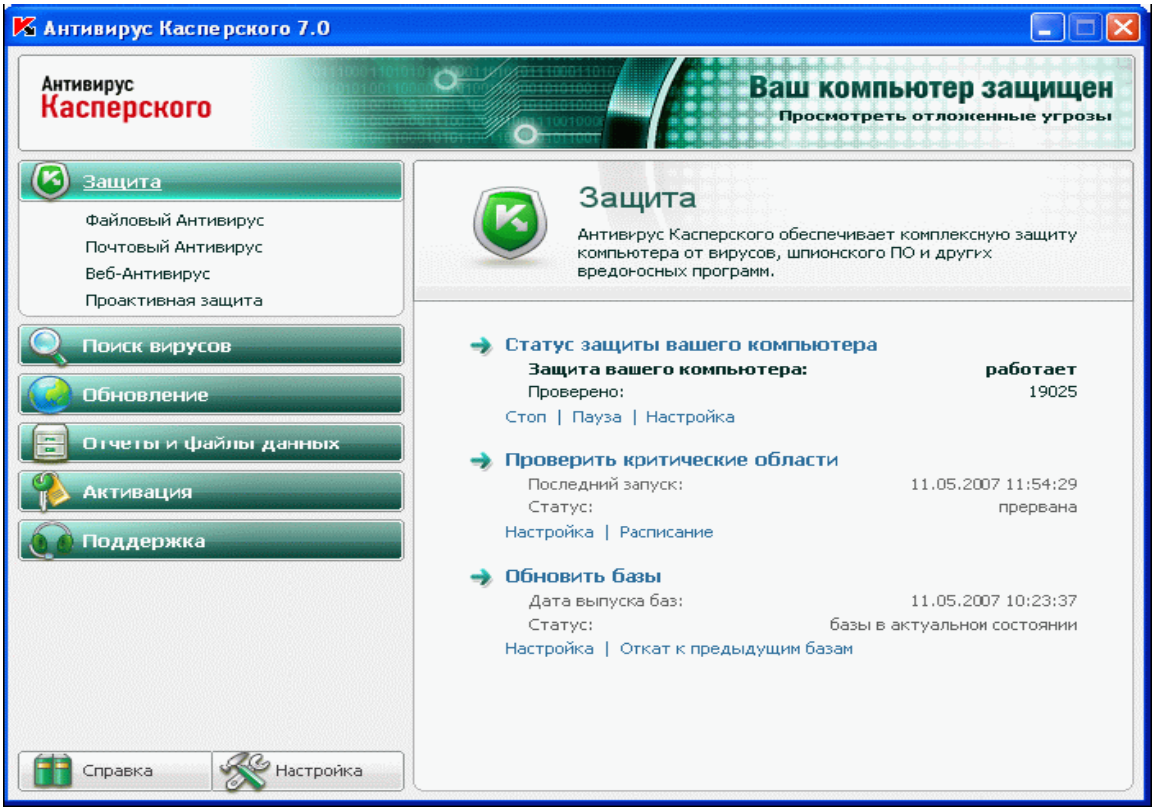


Рис.3. Від головного вікна програми «**Kaspersky Antivirus»**

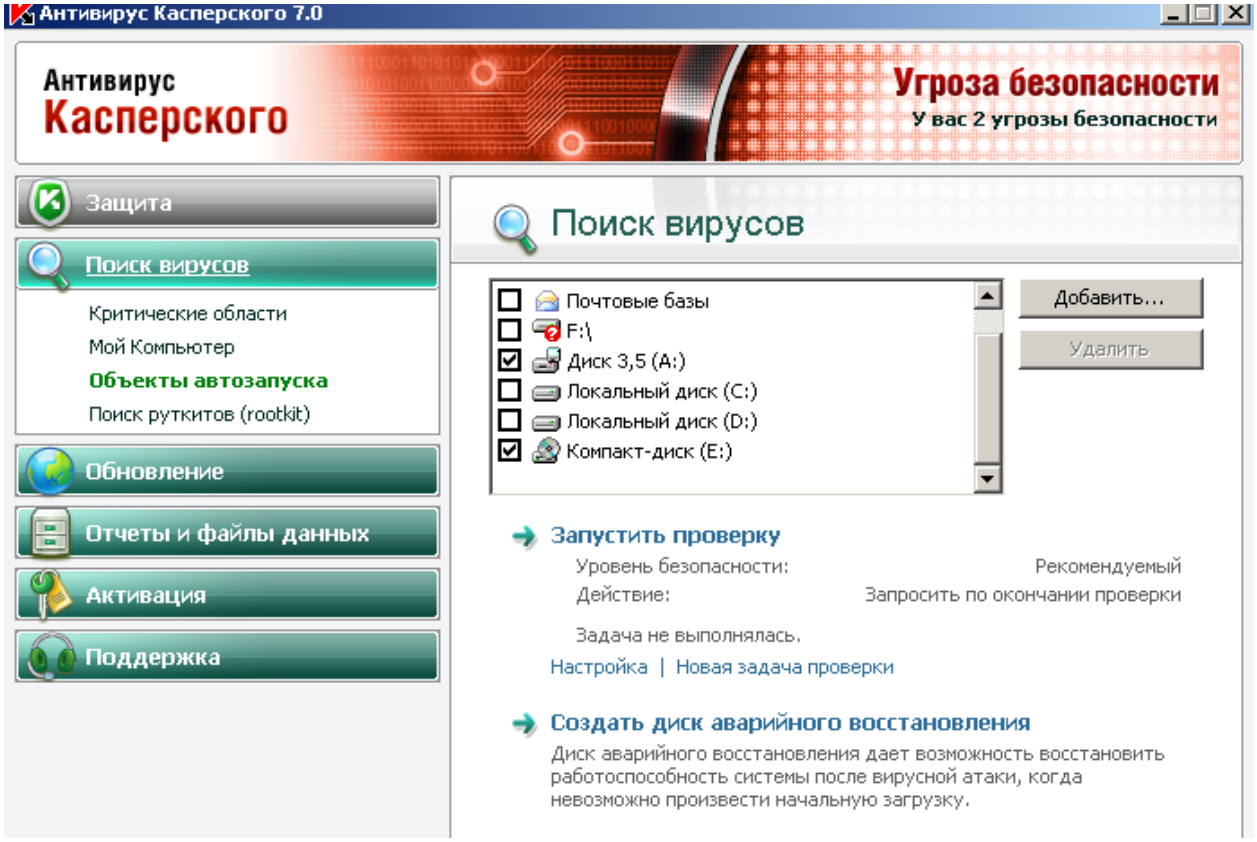


Рис.4. Запуск перевірки об’єктів на наявність комп’ютерних вірусів.

1.5. Активізувати значок програми **«Подробно»** та виконати перегляд стану перевірки зовнішніх носіїв інформації на наявність комп’ютерних вірусів.

1.6. Протягом перевірки уважно слідкуйте за станом роботи програми **Kaspersky Antivirus,** зокрема за кількістю перевірених файлів, статусу об’єктів, що перевіряються. За допомогою закладок вікна **«Поиска вирусов»** (закладка **«События», «Статистика»**) перегляньте результати перевірки (рис.5).

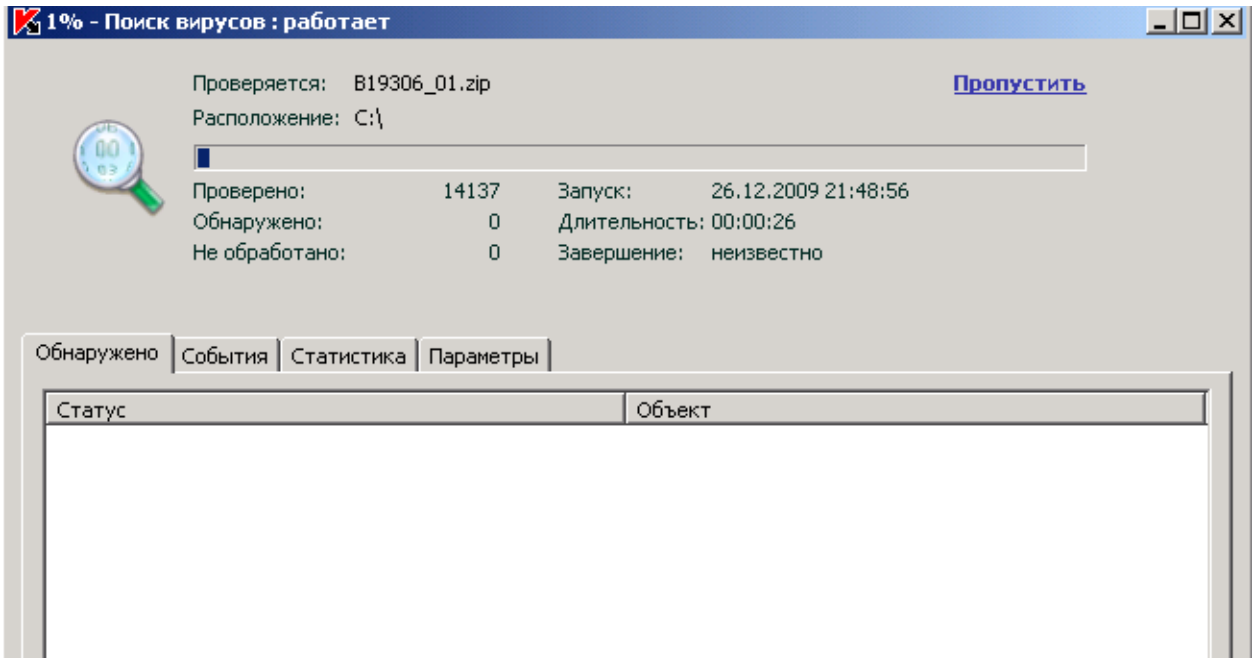


Рис.5. Стан перевірки носія з інформації на ПЕОМ

1.7. У разі появи комп'ютерних вірусів здійснити перевірку статусу їх активності. Для цього лівою кнопкою миші активізувати вірус, виявлений під час перевірки, далі необхідно натиснути на праву кнопку миші та у контекстному меню вибрати команду **«Лечить»,** або **«Удалить»**, при необхідності здійснити переміщення вірусу в **«Доверительную зону»** з метою його подальшого аналізу (рис.6.).

2. Технологія актуалізації антивірусних баз на ПЕОМ.

2.1. Засобами операційної системи створити на одному з логічних дисків ПЕОМ робочий каталог «**kav_upd_xxxxxxxx**», де «**kav_upd**» назва каталогу для розміщення порцій оновлення, **xxxxxxxx** - дата оновлення. Наприклад: **E:\kav_upd_2611200** де **26112009** – дата оновлення.

2.2. Здійснити копіювання порцій оновлення на логічний диск ПЕОМ за адресою **E:\kav_upd_2611200** та перевірити результати копіювання**.**

Примітка: Робочий каталог з порціями оновлення пропонується залишити на логічному диску до чергового оновлення антивірусних баз. Після виконання чергового отримання порцій оновлення зазначений каталог потребує віддалення.

2.3. Для виконання оновлення запустити програму **Kaspersky Antivirus** та у головному вікні програми натиснути на кнопку **«Обновление».** На правій

половині вікна **«Обновление»** перевірити дату випуска баз, кількість записів в базах та їх статус, після чого натиснути на кнопку **«Настройка»** (рис.7).

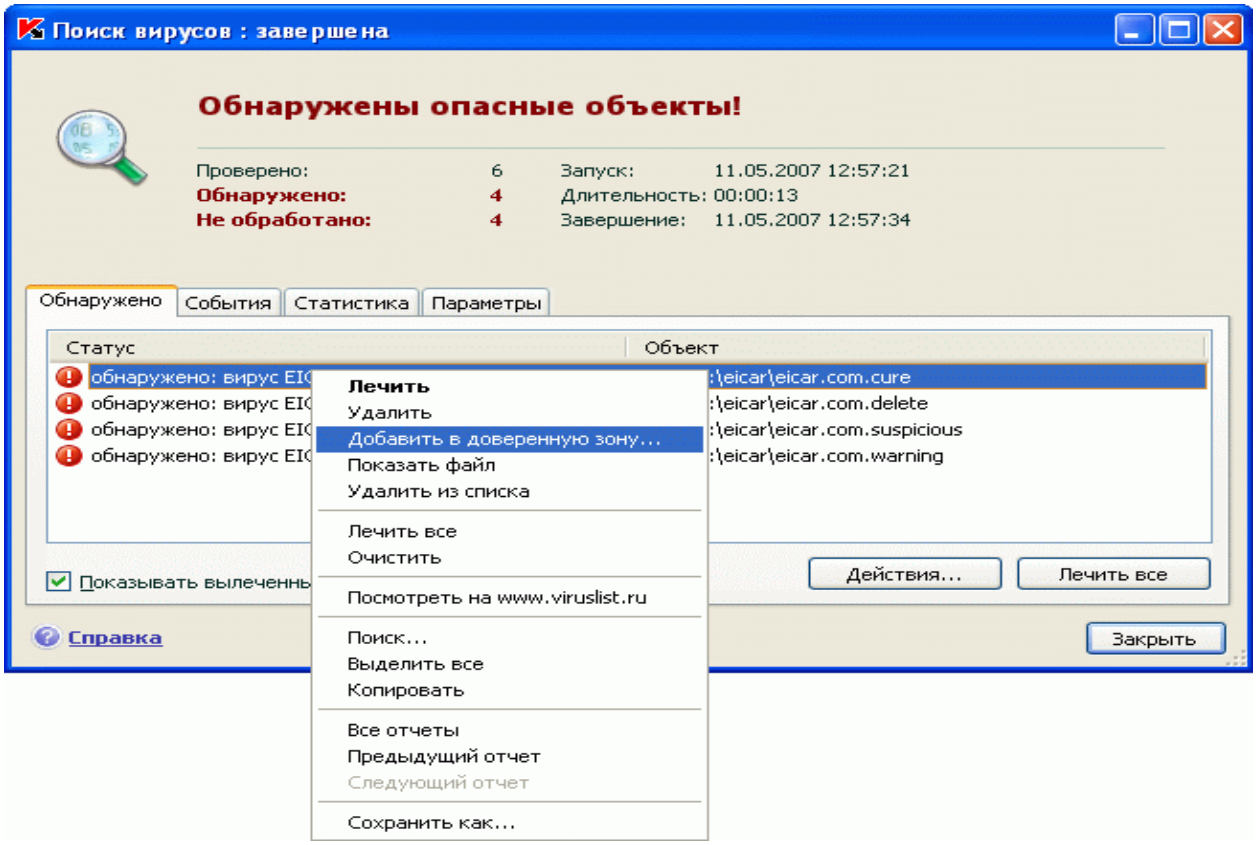


Рис.6. Дії під час виявлення комп’ютерних вірусів на ПЕОМ

Рис.7. Від вікна **«Обновление»** програми **Kaspersky Antivirus**

2.4. У вікні **«Настройка обновлений»** перевірити режим активації **«Обновление»,** та на правій половині вікна натиснути на кнопку **«Настройка»**, у вікні, що з’явиться, зняти мітку у боксі проти **«Серверы обновлений Лаборатории Касперского»** та натиснути на кнопку **«Добавить»**, після чого вибрати каталог де розміщені порції оновлень антивірусних баз, наприклад **E:\kav_upd_26112009** та натиснути на кнопку **«ОК»** (рис.8).

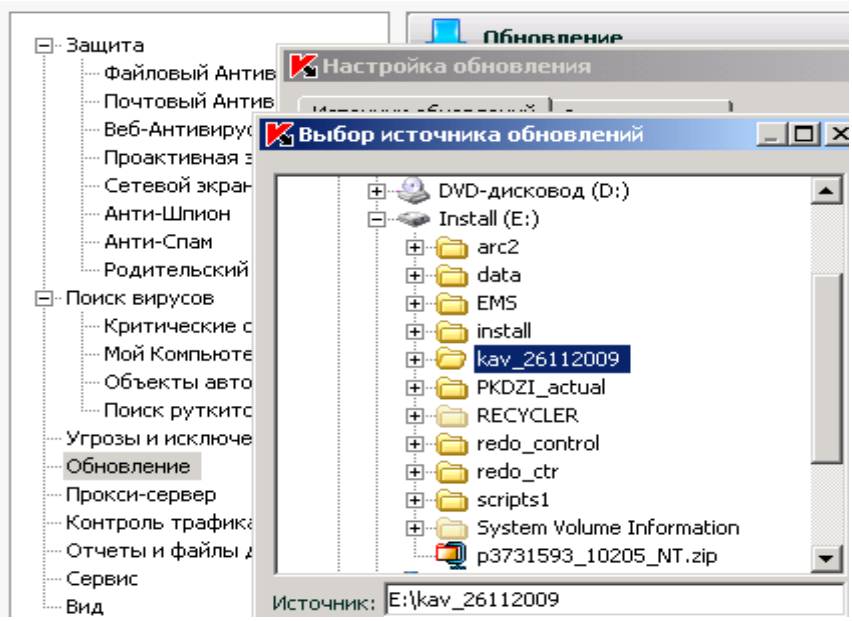


Рис.8. Вибір каталогу з порціями оновлень антивірусних баз

2.5. Запустити процедуру оновлення антивірусних баз, для цього у головному вікні програми **Kaspersky Antivirus** натиснути на кнопку **«Обновить базы».** Після закінчення оновлення перевірити дату антивірусних баз, кількість записів в базах та їх статус.

2.6. За результатами робіт підготувати звіт щодо повноти виконання технологічних операцій з перевірки програмного забезпечення ПЕОМ на наявність комп'ютерних вірусів, оновлення антивірусного програмного забезпечення.

2.7. Представити матеріали роботи для захисту викладачу.

ЗРАЗОК ЗВІТУ

Кількість об'єктів, які проскановані	Тривалість виконання операцій	Назва носія інформації, що перевірявся	База даних сигнатур	Версія бази даних сигнатур	Наявність загрози

Практичне заняття №4

(Перегляд журналів подій та системного журналу безпеки операційної системи Windows)

Метою практичної роботи є відпрацювання практичних завдань щодо порядку перегляду та перевірки вмісту подій, що виникають під час експлуатації загальносистемного та прикладного програмного забезпечення на ПЕОМ користувача та сервера начального класу за допомогою журналів подій та системного журналу безпеки операційної системи Windows.

Питання, що відпрацьовуються на занятті

1. Перегляд подій у журналах подій операційної системи.
2. Перевірка характеру подій у журналі безпеки операційної системи

Порядок виконання технологічних операцій:

1. Перегляд та перевірка характеру подій у журналах подій ОС.

1.1. Послідовно здійснити перегляд журналів подій операційної системи Windows на ПЕОМ слухача на сервері навчального класу. Для цього на робочу столі операційної системи ПЕОМ за допомогою лівої кнопки миші активізувати значок **«Мой копьютер»,** натиснути на праву кнопку миші, далі **«Управление»**, у вікні, що з'явиться, вибрати **«Просмотр событий»** та відповідний журнал подій:

на ПЕОМ користувачів (рис1):

- додатків;

- системи.

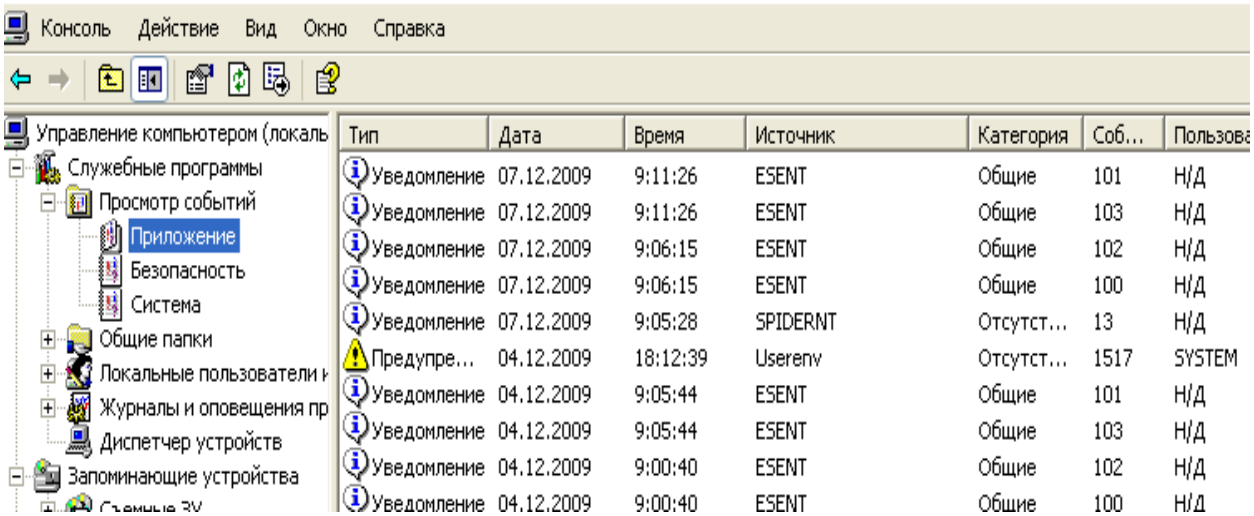


Рис.1. Вигляд вікна перегляду журналів подій на ПЕОМ

<u>на сервері навчального класу</u> <u>(рис.2.):</u>

- додатків;
- Directory Service;
- DNS Server;
- служба реплікації файлів;
- система

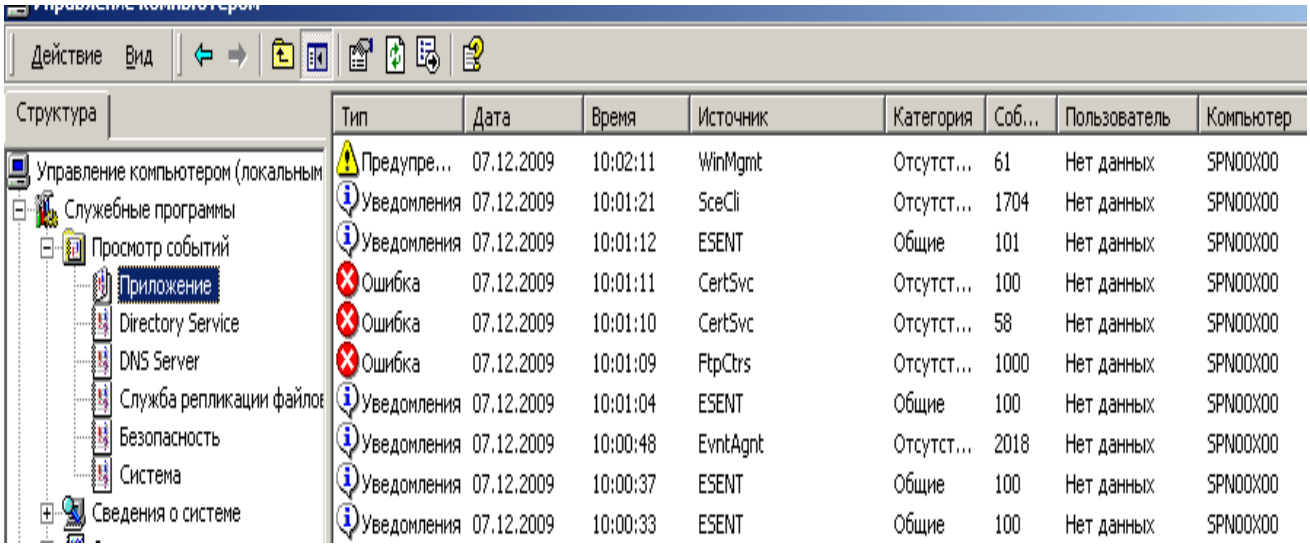


Рис.2. Вигляд вікна перегляду журналів подій на сервері та ПЕОМ

1.2. Перевірити записи у зазначених журналах та здійснити перегляд номерів повідомлень, які мають тип записи **«Ошибка»** або **«Предупреждение».** Для цього необхідно активізувати відповідний запис у журналі та два рази натиснути на ліву клавішу миші. У вікні, що з’явиться, здійснити перегляд вмісту повідомлення. (рис.3).

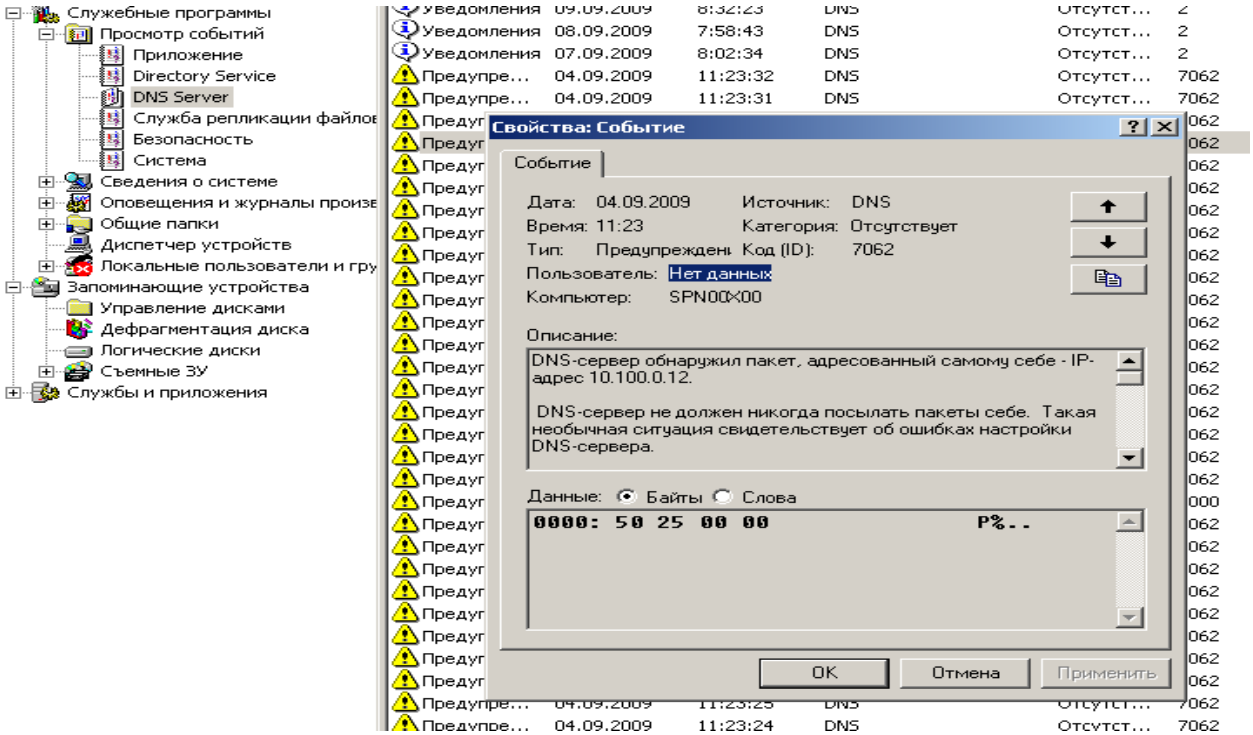


Рис.3. Перегляд вмісту події за допомогою журналу **DNS Server**

1.3. При появи помилок або попереджень з’ясувати причину їх появи та прийняти рішення щодо подальшого продовження роботи ПЕОМ та сервера.

2. Перевірка характеру подій у журналі безпеки ОС.

2.1. Перевірити встановлення та налаштування політик аудиту на мережевому сервері навчального класу. Для цього на панелі задач ОС контролера домену вузла натиснути на кнопку **«Пуск»,** далі **«Программы», «Администрирование», «Политека безпеки домена»,** вибрати **«Локальные политики»** та відкрити оснастку **«Політика аудиту».** Здійснити огляд встановлених параметрів аудиту (рис.4.)

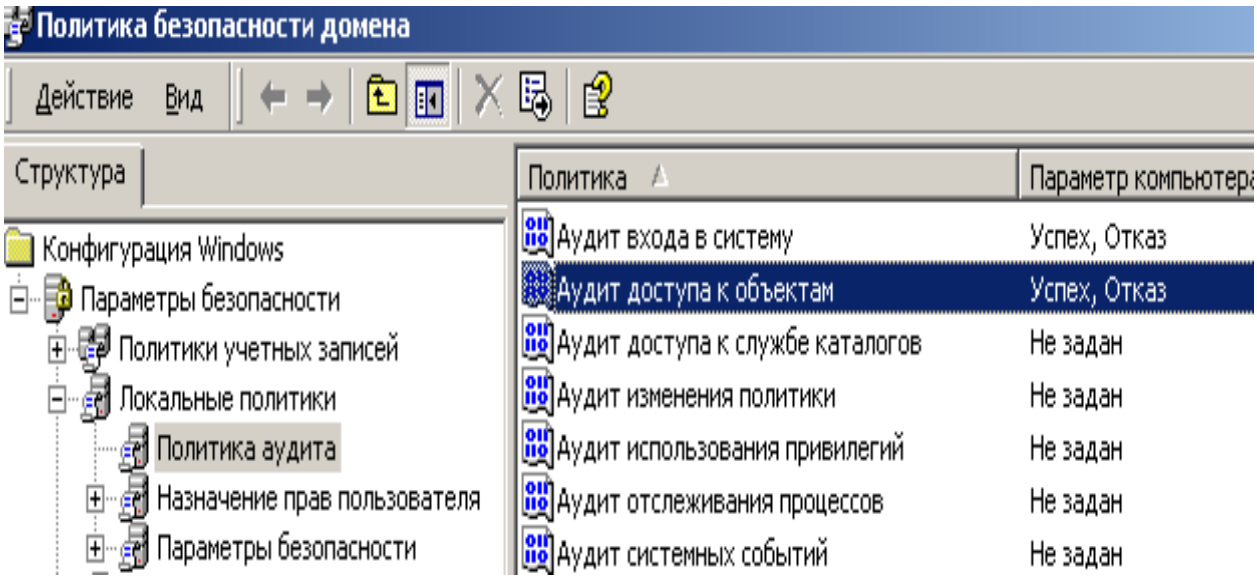


Рис.4. Перевірка налаштувань політик аудиту на сервері навчального класу

2.2. Послідовно виконати аналіз журналів безпеки ОС на робочих станціях АРМ користувачів та сервера бази даних вузла ДІС. Для цього на робочому столі операційної системи АРМ та сервера бази даних активізувати лівою кнопкою миші значок **«Мой копьютер»,** далі натиснути на праву кнопку миші, у контекстному меню вибрати **«Управление»** та натиснути на ліву кнопку миші, у вікні, що з'явиться вибрати **«Просмотр событий»** далі **«Безопасность»** (рис.5).

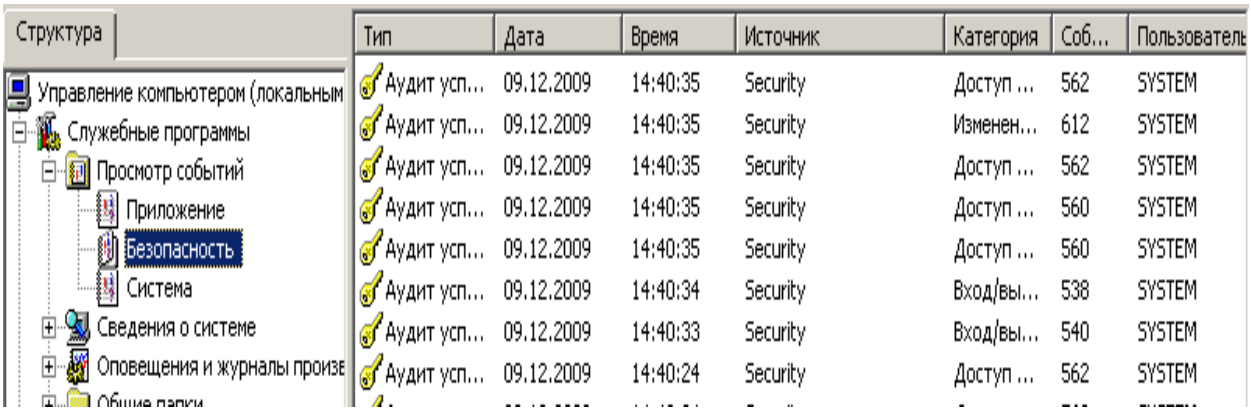


Рис.5. Перегляд типу подій в журналі безпеки ОС

2.3. Згідно п. 1.2. виконати аналіз вмісту повідомлень, які відображені у журналі безпеки АРМ користувача (рис.6), особливо щодо подій, які зазначені у таблиці.

Таблиця - Номера подій журналу безпеки ОС, які потребують перегляду та контролю

№ події	Короткий зміст (мовою операційної системи)
528	Успешный вход в систему
529	Отказ входа в систему. Неизвестное имя пользователя
530	Пользователь пытался войти в систему в недозволенное ему время
531	Учетная зпись пользователя заблокирована
532	Учетная запись пользователя просрочена или устарел пароль пользователя.
533	Пользователь ограничен входом лишь на некоторые рабочие станции, а он пытается войти в систему с другого компьютера
534	Попытка запуска службы с использованием учетной записи пользователя, не имеющей права на запуск служб
537	Отказ по неизвестной причине
538	Выход пользователя из системы
540	Успешный сетевой вход в систему
560	Фиксирует открытия объекта пользователем
562	Фиксирует закрытия объекта пользователем
628	Задание пароля учетной записи
642	Изменение учетной записи
644	Блокировка учетной записи пользователя в домени

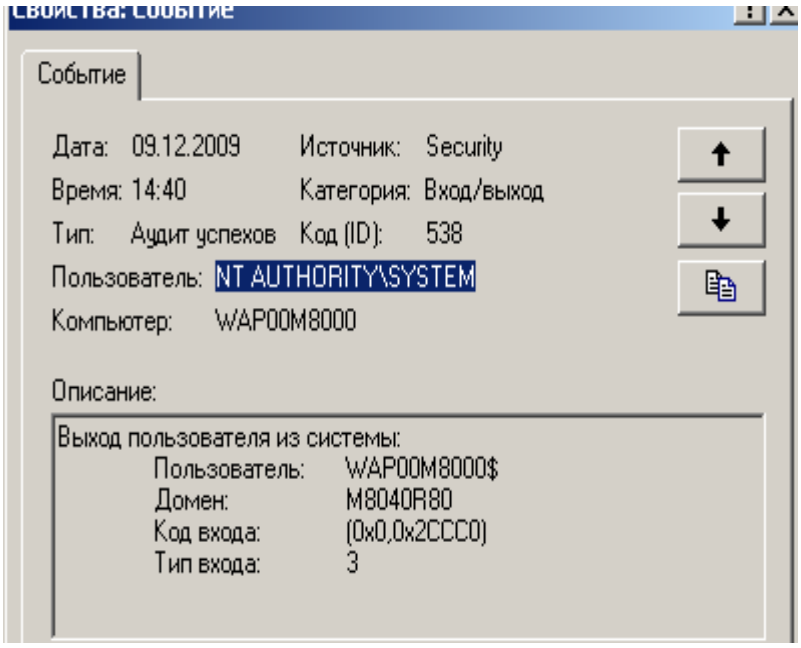


Рис.6. Перегляд події в журналі безпеки АРМ користувача

2.4. Перевірити записи в журналі безпеки ОС АРМ користувачів щодо подій, пов’язаних з реєстрацією користувача на АРМ, а саме, визначити номер типу входу користувача в систему.

В журналі безпеки зазначені події фіксуються наступними порядковими номерами:

2 – відповідає інтерактивному входу в систему з консолі, наприклад за допомогою монітору або клавіатури;

3 – підключення до системи за допомогою мережевого ресурсу;

4 – вказує на запуск командного файлу;

5 – фіксує запуск служби з зазначенням облікової записі користувача

6 – підключення користувача здійснюється за допомогою Proxy Server

7 – користувач здійснював розблокування робочої станції.

Якщо під час аналізу були виявлені спроби несанкціонованого доступу (реєстрації) користувачів на ПЕОМ (**події №№529, 530, 537**, тип входу **2,3**), необхідно ретельно проаналізувати зазначені події та прийняти заходи щодо недопущення несанкціонованого доступу до ресурсів ПЕОМ.(рис.7)

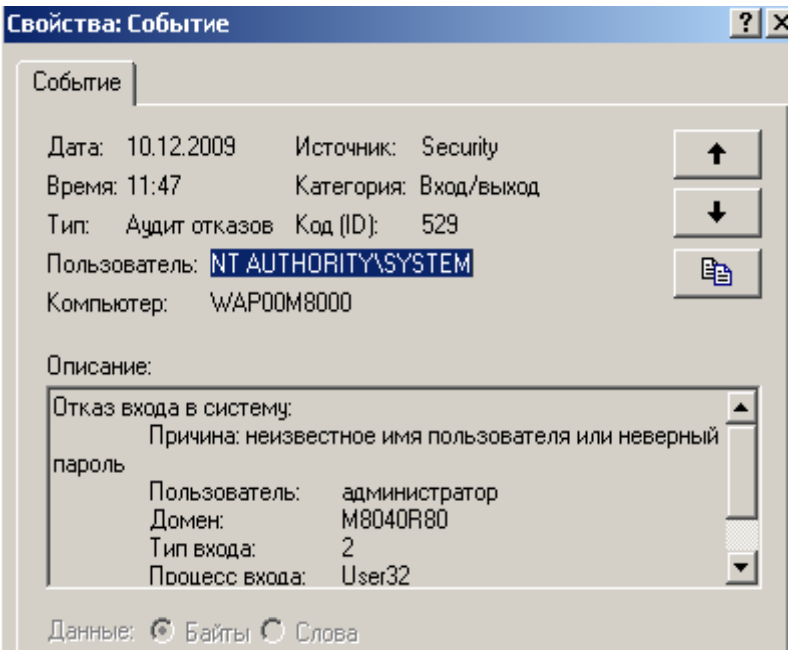


Рис.7. Перегляд події в журналі безпеки щодо спроби несанкціонованого доступу на ПЕОМ користувача

2.5. Здійснити аналіз подій журналу безпеки щодо доступу користувача до об’єктів системи (події за номерами **560** та **562** рис. 8.). До таких об’єктів відносяться виконавчі файли загальносистемного та прикладного програмного забезпечення (програмне забезпечення ПЕОМ, клієнтське програмне забезпечення СКБД, Microsoft Office тощо).

За результатами розгляду проаналізувати коректність доступу користувачів до зазначеного програмного забезпечення.

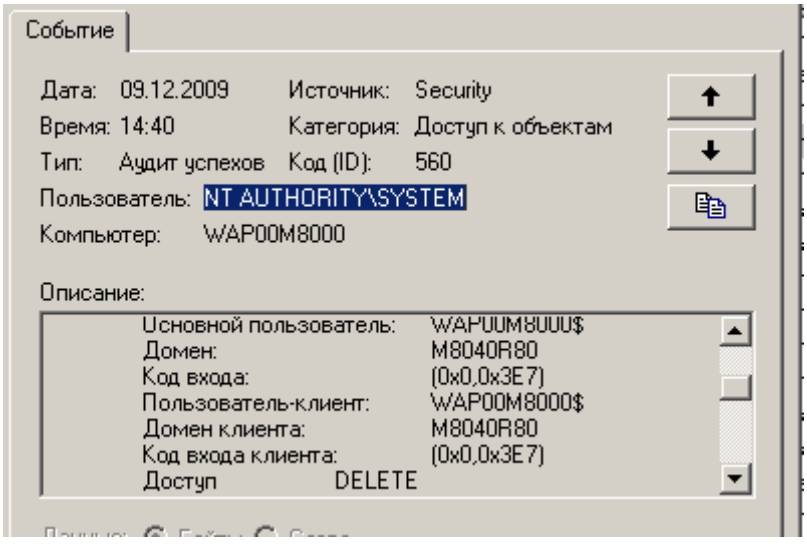


Рис.8. Перегляд події в журналі безпеки щодо доступу до прикладного програмного забезпечення АРМ користувача

3.15.3. Перевірка налаштувань журналів подій та безпеки ОС на ПЕОМ та сервері

3.1. На АРМ користувача або сервера вузла ДІС відрити вікно **«Управление компьютером»,** за допомогою лівої кнопки миші вибрати розділ **«Просмотр событий»,** далі активізувати необхідний журнал подій ОС, натиснути на праву кнопку миші та у контекстному меню вибрати команду **«Свойства»** (рис.9).

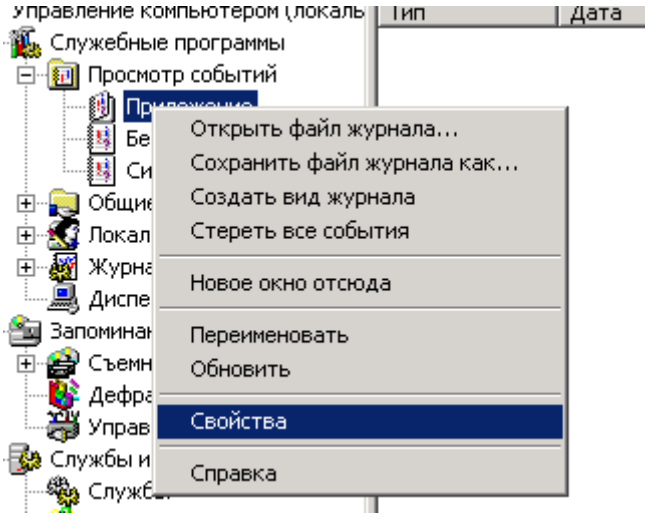


Рис.9. Вибір вікна властивостей журналу подій

3.2. Перевірити значення конфігураційних параметрів журналу, а саме, його максимальний розмір та правило записи у журнал при його заповненні **(затирать события старее 7 дней)**. За допомогою кнопки **«Очистить журнал»** здійснити видалення його повідомлень (рис.10).

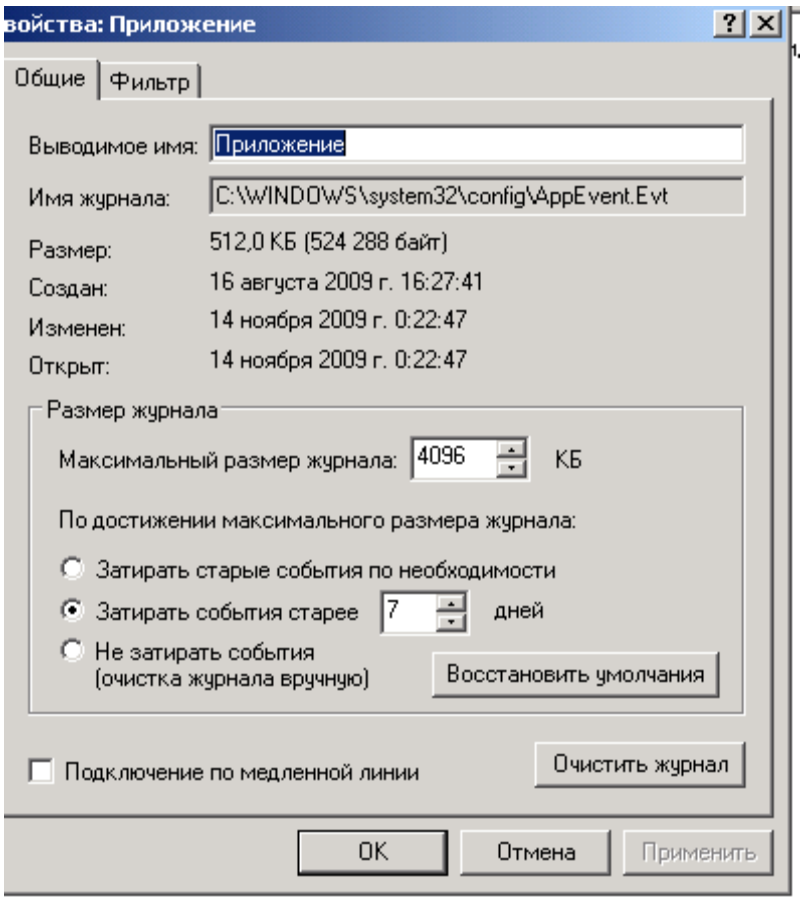


Рис.10 Від вікна налаштувань журналу повідомлень ОС

3.3. За результатами робіт підготувати звіт на надати його для захисту викладачу.

ЗРАЗОК ЗВІТУ

Назва журналу ОС	Опис наявних попереджень	Опис наявних критичних помилок	Номер подій журналу безпеки	Короткий зміст події журналу безпеки

Назва журналу ОС	Встановлений розмір журналу	Адреса розміщення журналу на дисках ПЕОМ

Практичне заняття №5

(Перевірка функціонування та величини завантаження локальної мережі, швидкості та активності мережевого серверу)

Метою заняття є виконання технологічних операцій з перевірки функціонування та величини завантаження локальної мережі, швидкості та активності роботи мережевого серверу (контролеру домену).

Перевірка функціонування та завантаженості локальної мережі пов'язана перш за все з перевіркою величини завантаження мережевого серверу вузла (контролеру домену), його програмних складових (Active Directory) та апаратних засобів, що потребують моніторингу та аналізу.

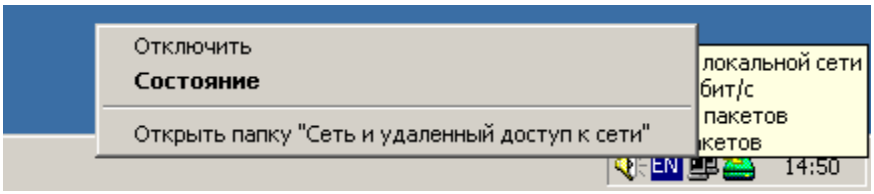
Питання, що відпрацьовуються на занятті

1. Перевірка функціонування та величини завантаження локальної мережі.
2. Перевірка величини завантаження мережного сервера за допомогою програмного забезпечення Performance Monitor.
3. Моніторинг роботи Active Directory мережевого сервера вузла ДІС.

Порядок виконання технологічних операцій:

1. Перевірка функціонування та величини завантаження локальної мережі

1.1. Визначити максимальну кількість активних сеансів на контролері домену вузла та здійснити перевірку функціонування локальної мережі та величини її завантаження. Для цього на панелі задач операційної системи Windows контролера домену вузла ДІС вибрати іконку підключення до локальної мережі та натиснути на праву кнопку миші, далі у контекстному меню вибрати команду **«Состояние».** У вікні, що з'явиться, переглянути стан працездатності мережі, тривалість передачі та кількості отриманих та переданих пакетів (рис.1).



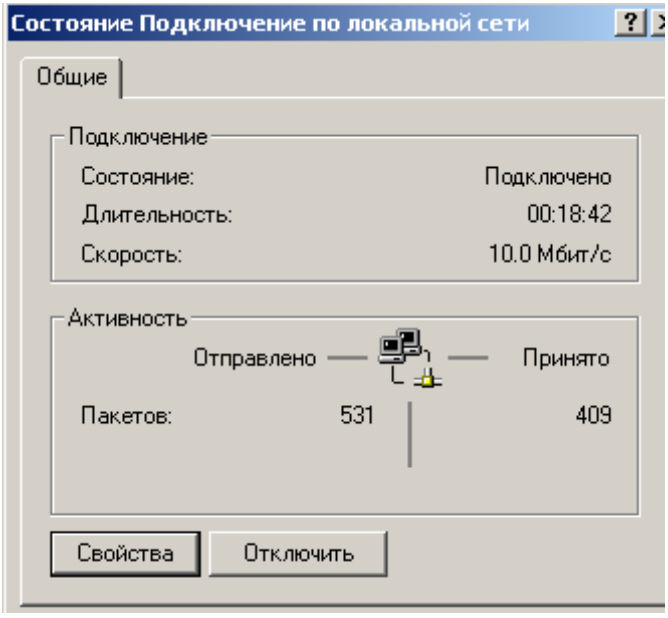


Рис.1. Перевірка стану працездатності локальної мережі мережевого серверу

1.2. Запустити на контролері домену вузла ДІС **«Диспетчер задач»** та здійснити вибір закладки **«Сеть»** (рис.2). Перевірити стан працездатності мережевого адаптера сервера шляхом визначення відсотка завантаження мережі та швидкості надсилання та отримання мережевих пакетів.

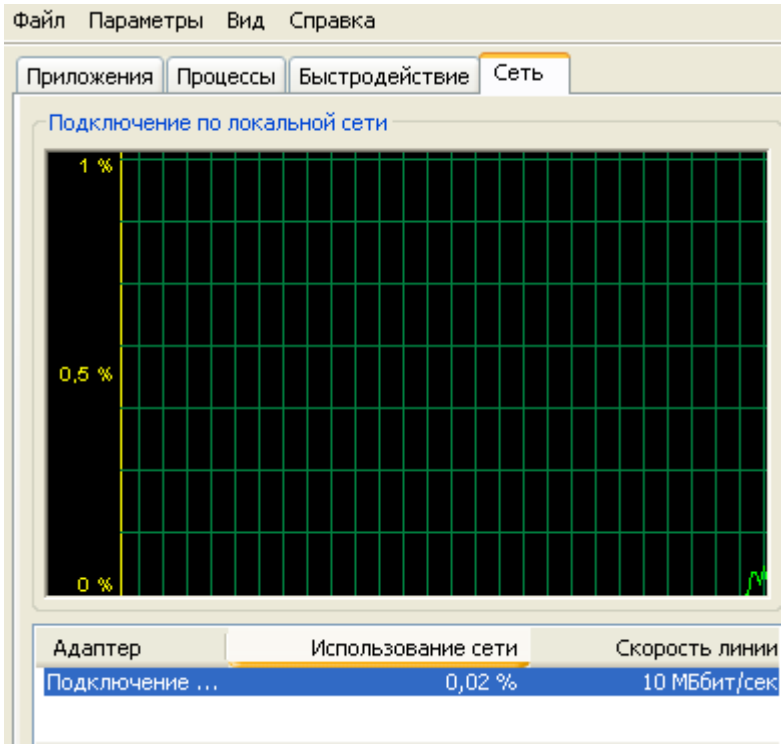


Рис.2. Від вікна «Диспетчер задач»

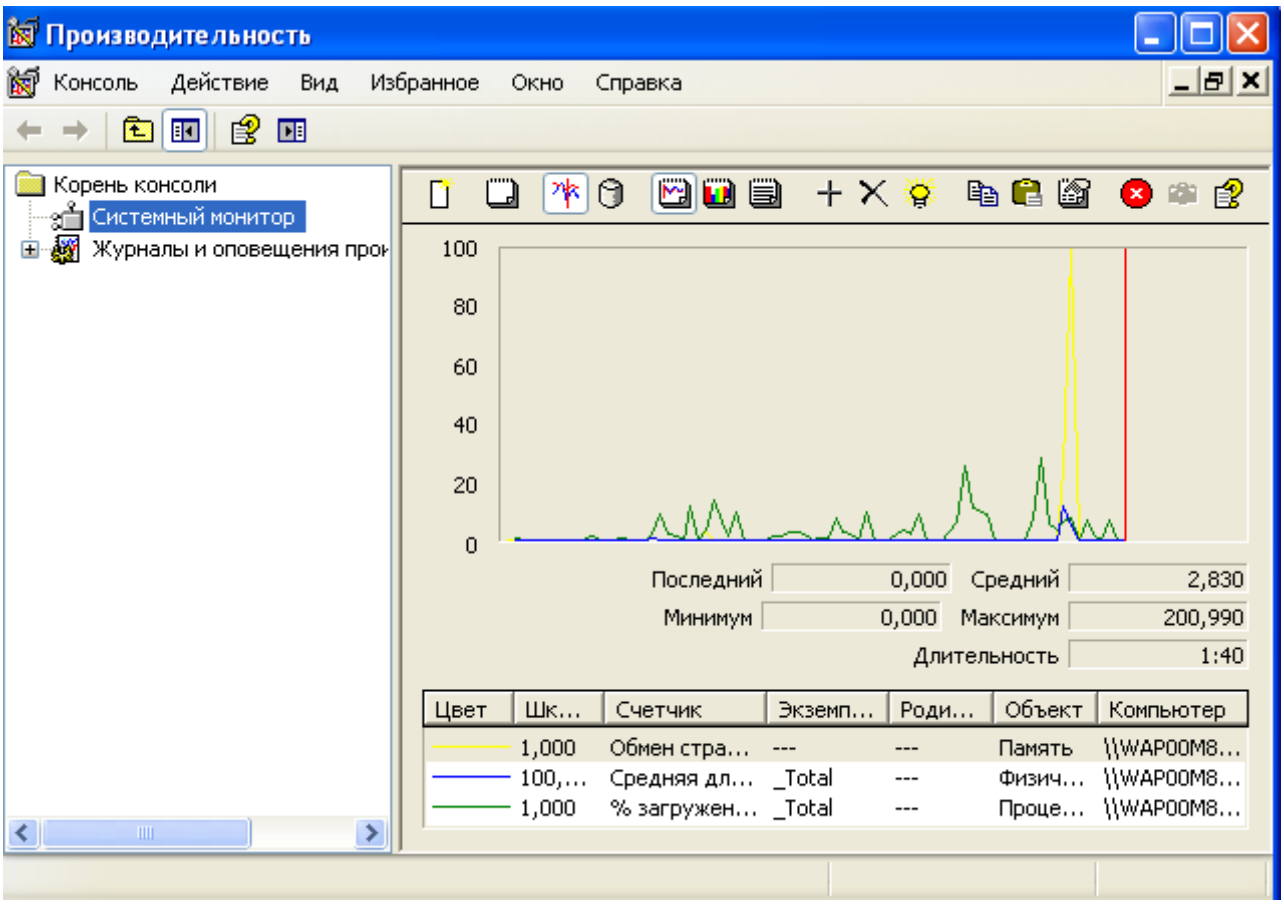
Примітка: Якщо протягом експлуатації мережевого серверу виникають випадки зупинки надсилання та отримання мережних пакетів або погіршення продуктивності серверу, здійснити додаткові заходи з перевірки стану завантаження мережі за допомогою програмного забезпечення Performance Monitor.

2. Перевірка величини завантаження мережного сервера за допомогою програмного забезпечення Performance Monitor.

2.1. На панелі задач операційної системи мережевого сервера користувача вузла натиснути на кнопку **«Пуск»**, далі **«Настройка», «Панель управления», «Администрирование»,** вибрати **«Производительность».** У вікні **«Производительность»**, активізувати розділ **«Системный монитор»**(рис.3).

2.2. На панелі задач вікна **«Производительность»** натиснути на кнопку **«Добавить»,** яка має позначення **«+» та у вікні, що з'явиться, у розділі «Объект»** вибрати **лічильник «Network Interface - мережевий інтерфейс»** Ретельно перевірити частоту, з якою здійснюється отримання та відправлення пакетів через мережевий інтерфейс.(рис.4).

2.3. За допомогою лічильника **Server/Work Item Shortage** виконати перевірку обробки сервером мережевих запитів. Зазначений лічильник відслідковує дані щодо черги мережних запитів від користувачів. Якщо сервер перевантажений, то запит від користувачів може бути відкладений (рис.5.).



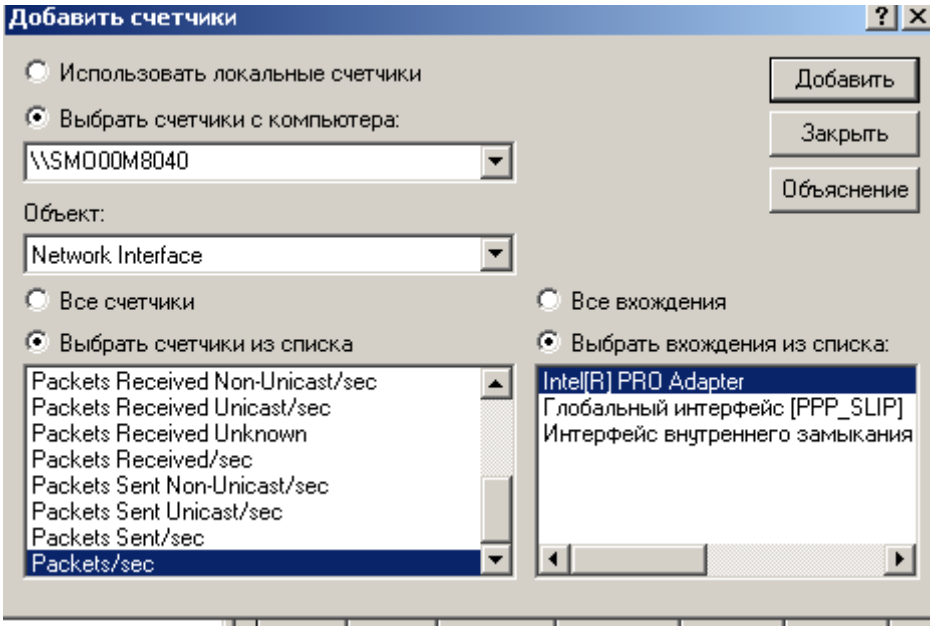


Рис.4. Вибір лічильників для розрахунку трафіка локальної мережі вузла ДІС

2.4. Здійснити аналіз мережевої активності компонентів серверу Redirector, за допомогою лічильника **Network Errors** (рис.6) та **Current Commands,** где: **Network Errors** – активність виникнення мережевих помилок, **Current Commands** – визначає кількість команд, які знаходяться у черзі до **Redirector.**

Якщо число більше, ніж одна команда на один мережевий адаптер, то **Redirector** може бути вузьким містом у системі. Це виникає у зв'язку з появою суттєвих мережевих помилок. Поява таких помилок свідчить про необхідність проведення додаткових досліджень. Для з'ясування причин низької продуктивності необхідно використовувати журнал повідомлень ОС сервера **Event Log.**

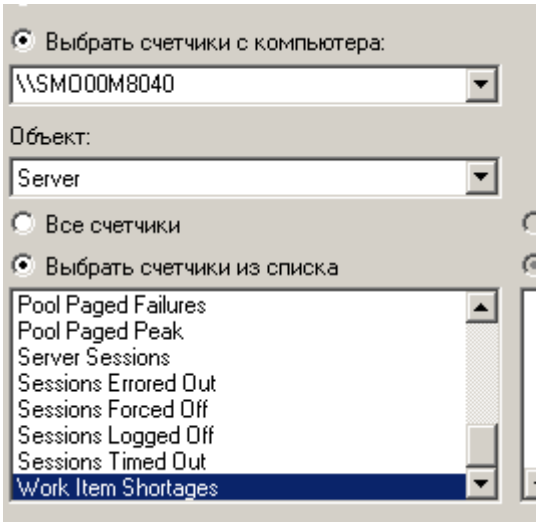


Рис.5. Вибір лічильник сервера Work Item Shortage

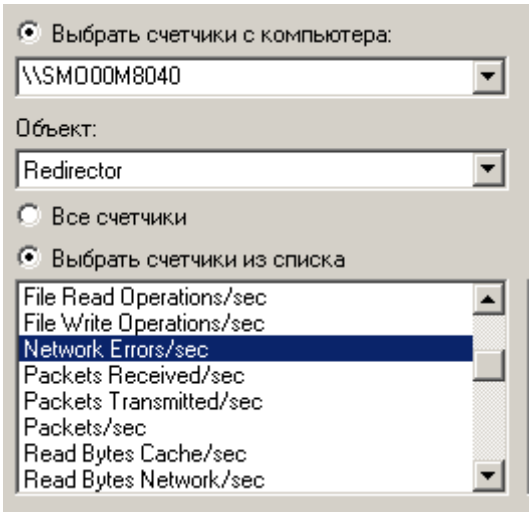


Рис.6. Вибір лічильник Network Errors

2.5. Виконати перевірку завантаженості локальної мережі вузла, а саме, продуктивності обміну файлами між мережевим сервером та ПКДЗІ вузла ДІС. Для цього необхідно запустити програмне забезпечення **Performance Monitor** та додати лічильники **Reads Denied/sec и Writes Denied/sec** для аналізу завантаженості локальної мережі вузла. Якщо під час аналізу виявлено не нульові

лічильників **Reads Denied/sec и Writes Denied/sec,** це свідчіть про те, що сервера вузла, з якими здійснюється обмін, мають проблеми оперативної пам'яті. (рис.6).

2.6. За допомогою лічильників **Pool Nonpaged Failures** та **Pool Paged Failures**. перевірити кількість фізичної пам'яті мережевого сервера (рис.8). Любі значення лічильників свідчать про те, у що мережевого сервера недостатньо фізичної пам'яті.

2.7. Після закінчення робіт здійснити заходи з **віддалення лічильників.** Для цього у вікні **«Системный мониторинг»** на правій половині вікна активізувати лівою кнопкою миші необхідний лічильник**,** далі натиснути на кнопку **«Удалить»,** яка має позначення **«Х»,** після чого **необхідно р**етельно перевірити стан відключення лічильників та зателефонувати фахівцям Центрального апарата Департамента ІТ – аутсорсінгу про закінчення робіт.

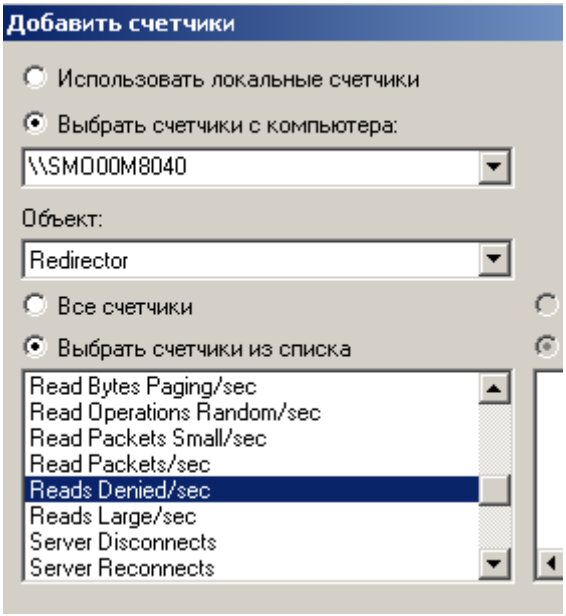


Рис.7. Від вікна лічильника Reads Denied

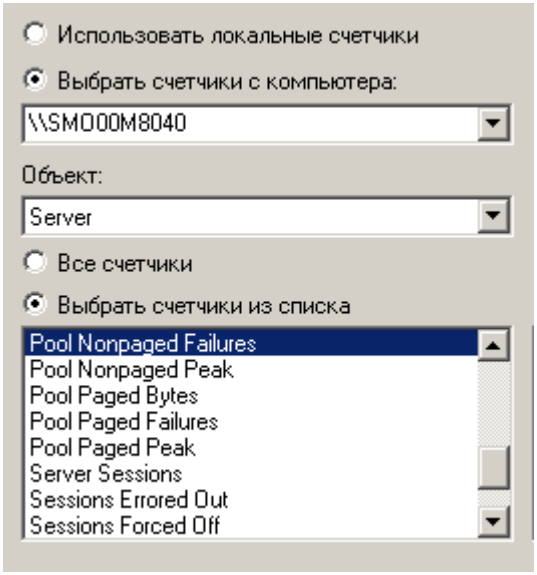


Рис.8. Від вікна лічильника Pool Nonpaged Failures

3. Моніторинг роботи Active Directory мережевого сервера вузла ДІС.

3.1. Ретельно прочитати та вивчити матеріали практичної роботи що надаються та отримати дозвіл на їх виконання.

3.2. На панелі задач операційної системи мережевого сервера користувача вузла натиснути на кнопку **«Пуск»**, далі **«Настройка», «Панель управления», «Администрирование»,** вибрати **«Производительность».** У вікні **«Производительность»**, активізувати розділ **«Системный монитор»**. Послідовно за допомогою лічильників, які наведені у таблиці, виконати технологічні операції з моніторингу роботи Active Directory мережевого сервера вузла.

3.3. За результатами робіт підготувати звіт щодо повноти виконання технологічних операцій з моніторингу мережного сервера

3.4. Представити матеріали роботи для захисту викладачу.

3.5. Після закінчення робіт здійснити заходи з **віддалення лічильників.** Для цього у вікні **«Системный мониторинг»** на правій половині вікна активізувати лівою кнопкою миші необхідний лічильник**,** далі натиснути на кнопку **«Удалить»,** яка має позначення **«Х»,** після чого **необхідно р**етельно перевірити стан відключення лічильників.

ЗРАЗОК ЗВІТУ

№ з.п.	Назва лічильника (мовою операційної системи, що встановлена на вузлі	Пояснення (мовою операційної системи, що встановлена на вузлі)	Значення параметра, що отримане під час аналізу
1	NTDS/DS Search sub-operations/sec	использование ресурсов системы	
2	% Processor Time	Указывает процент времени работы процессора службой Active Directory. Увеличение значения указывает на то, что новое приложение обращается к этому контроллеру домена, или что больше клиентов было добавлено к сети**.**	
3	NTDS/ LDAP Client Sessions	LDAP сеансы клиентов. Указывает текущее количество клиентов, связанных с контроллером домена. Его увеличение указывает на то, что другие машины не выполняют свою работу, перегружая этот контроллер домена.	
4	Процесс/ Private Bytes	Личные байты. Отслеживает объем памяти, используемой контроллерами домена.	

5	Процесс/ Virtual Bytes	Виртуальные байты. Используется для определения того, что Active Directory выполняется при нехватке виртуального адресного пространства памяти, что указывает на утечку памяти	
6	NTDS/DRA Inbound Bytes Compressed	DRA входящие сжатые байты (Между сайтами после сжатия/секунды). Указывает количество реплицируемых данных. Изменение значения этого счетчика указывает на изменение топологии репликации или на то, что существенные данные были добавлены или изменены в Active Directory.	
7	NTDS/DRA Outbound Bytes Not Compressed	Исходящие несжатые DRA байты. Указывает количество реплицируемых данных, выходящих из этого контроллера домена.	
8	NTDS/NTLM Authentications	Указывает количество клиентов в секунду, которые аутентифицируются на контроллере домена.	
9	Memory	Высокая степень ошибок страницы указывает на недостаточную физическую пам'ять.	
10	Physical Disk /Current DiskQueue	Отслеживает объемы файлов Ntds.dit и .log. Указывает, что имеется отставание дисковых запросов ввода/ вывода.	
11	Processor% DPC Time	Указывает отложенную работу, из-за занятости контроллера домена	

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАНЯТТЬ

1. Електронні та друковані інформаційні ресурси, диски.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Рэнд Моримото, Майкл Ноэл, Омар Драуби, Росс Мистри, Крис Амарис - Microsoft Windows Server 2012 R2. Полное руководство//СПб Питер 2015 – 1455 с.
2. Т. Адельштайн, Б. Любанович. Системное администрирование Linux. //СПб:Питер, 2014. -288 с.
3. Душан Петкович. MS SQL Server 2012. Руковоство для начинающих, //СПб Питер -2012 – 743 с.
4. Колісніченко Д.Н. Linux – сервер своїми руками. СПб: //Наука и Техника, 2014 – 678 с.
5. Кен Хендерсон. Профессиональное руководство по SQL Server. //Структура и реализация, 2012 – 1064 с.
6. Бруй В.В., Карлов С.В. Linux-сервер: пошаговіе инструкции инсталяции и настройки.//Москва.: Изд-во СИП РИАб 2012. – 572 с.
7. И.Ф. Астахова. SQL в примерах и задачах.// Учебное пособие, 2012 – 176 с.
8. Сетевые средства Linux М.В. Кульгин Коммутация и маршрутизация IP/IPX трафика. //М.: КомпьютерПресс, -2010. –320 с.
9. Д. Энсор. Oracle. Проектирование баз даних, 1999 – 557 с.
10. А.И. Бражук. Сетевые средства Linux//http://www.intuit.ru/department/os/netapplinux.
11. Н.Н. Васин Построение сетей на базе коммутаторов и маршрутизаторов // http://www.intuit.ru/department/network/netbsr/
12. С.В. Гончарук. Администрирование ОС Linux http://www.intuit.ru/department/os/linuxadmin/3/linuxadmin_3.html
13. Н.Н. Васин. Построение сетей на базе коммутаторов и маршрутизаторов // http://www.intuit.ru/department/network/netbsr/