МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва і архітектури

МОНІТОРИНГ ТА АУДИТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Методичні вказівки
до виконання практичних робіт
для студентів спеціальностей
125 «Кібербезпека»

Київ 2022

УДК 004.056.5(045)
М77

Укладачі: Ю.І. Хлапонін, д-р техн. наук, професор
О.В. Сєлюков, д-р техн. наук, професор

Рецензенти: Д.О. Гуменний, канд. техн. наук, доцент
С.В. Кондакова, канд. фіз.-мат. наук, доцент

Відповідальний за випуск Ю.І. Хлапонін, д-р техн. наук, професор

Затверджено на засіданні кафедри кібербезпеки та комп'ютерної інженерії протокол № 9 від 03 травня 2022 р.

В авторській редакції.

М77 **Моніторинг** та аудит інформаційно-комунікаційних систем: методичні вказівки / уклад.: Хлапонін Ю.І., Сєлюков О.В.. - Київ: КНУБА, 2022. – 52 с.

Містять зміст, порядок оформлення і вказівки до виконання практичних робіт.

Призначено для студентів спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології».

ЗМІСТ

ВСТУП

Мета викладання дисципліни –підготувати фахівців реагування на інциденти інформаційної безпеки, надати знання в сфері інцидентів мережевої безпеки, інцидентів, пов'язаних із шкідливим кодом, і в сфері загроз інсайдерських атак. В основі навчання лежать принципи і методи виявлення і реагування на загрози комп'ютерної безпеки.

Основне завдання курсу - дати студентам теоретичну та практичну підготовку з основ кібербезпеки, зокрема: тактику, методи та процедури, які використовуються кіберзлочинцями; принципи конфіденційності, цілісності і доступності, оскільки вони відносяться до станів даних і контрзаходів в області кібербезпеки; технології, продукти і процедури, які використовуються для захисту конфіденційності, цілісності та доступності; розуміння, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережі.

Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни “Кібербезпека”:

- знання та розуміння предметної області та розуміння професії;
- вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;
- здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки;
- здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;
- здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

Результати навчання:

- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;
- діяти на основі законодавчої та нормативно правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;
- розробляти моделі загроз та порушника;
- застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

Мета проведення лабораторних занять полягає у тому, щоб виробити у студентів практичні навички забезпечення безпеці в операційному середовищі Windows.

Завдання проведення лабораторних занять:

– вивчити перелік служб операційного середовища Windows;

– навчитись здійснювати моніторинг операційного середовища Windows;

– навчитись здійснювати перевірку програмного забезпечення ПЕОМ на наявність комп’ютерних вірусів;

– вміти переглядати журнал подій та системний журнал безпеки операційної системи Windows.

ЛАБОРАТОРНА РОБОТА № 1
Тема: Безпека у Windows

Мета: Розуміння та настроювання функцій служби "Безпека у Windows".

ТЕОРЕТИЧНІ ВІДОМОСТІ

Windows 10 та 11 і 11 Безпека у Windows є найновішим захистом від вірусів. Пристрій буде активно захищено з моменту початку Windows. Безпека у Windows постійно сканує зловмисні програми (зловмисні програми, віруси та загрози безпеці). Окрім цього захисту в реальному часі автоматично завантажуються оновлення, щоб пристрій залишався безпечним і захищеним від загроз.

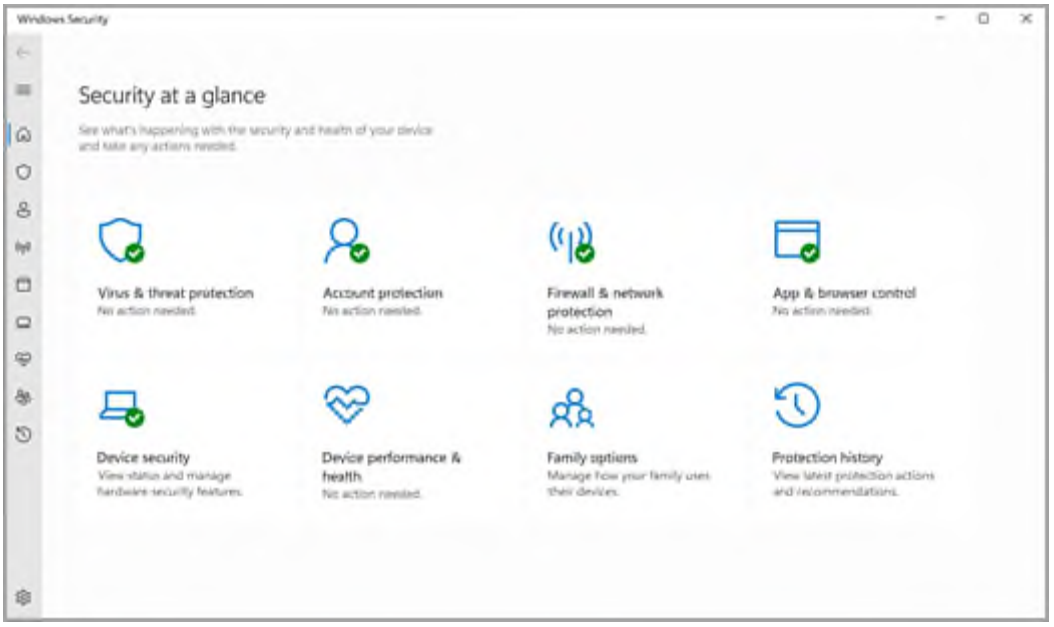

Рисунок 1.1. Важливі відомості про безпеку

Безпека у Windows вбудовано в Windows антивірусну програму, яка називається Антивірус для Microsoft Defender (у попередніх версіях Windows 10 Безпека у Windows називається Захисник Windows Центр безпеки, рис.1.1).

Якщо інстальоване й увімкнуто іншу антивірусну програму, Антивірус для Microsoft Defender вимкнеться автоматично. Якщо видалити іншу програму, Антивірус для Microsoft Defender знову ввімкнеться автоматично.

Розуміння та настроювання функцій служби "Безпека у Windows"

Безпека у Windows – це діалогове вікно для керування інструментами, які захищають ваш особистий пристрій (комп’ютер) і дані:

захист від вірусів і загроз – відстеження загроз пристрою, запуск перевірок і отримання оновлень із метою виявлення останніх загроз;

- захист облікових записів – доступ до параметрів входу й настройок

облікового запису, зокрема Windows Hello і динамічного блокування;

- брандмауер і захист мережі – керування настройками брандмауера та відстеження, що відбувається з вашими мережами та підключеннями до Інтернету;

- керування програмами та браузерами – оновлення параметрів Фільтр SmartScreen для Microsoft Defender, щоб захистити пристрій від потенційно небезпечних програм, файлів, сайтів і завантажень, та отримання доступу до функції запобігання експлойтам, що дозволяє налаштовувати настройки захисту для ваших пристроїв;

- безпека пристрою – зміна вбудованих параметрів безпеки, щоб захистити пристрій від атак зловмисного програмного забезпечення;

- продуктивність і справність пристрою – відомості про стан справності свого пристрою;

- родина – відстеження дій дітей в Інтернеті та пристроїв у вашій родині (колективі).

КЛЮЧОВІ ПИТАННЯ

1.Назвіть головні завдання, які виконує служба "Безпека у Windows".

2.Охарактеризуйте технології міжмережевих екранів.

3.Назвіть основні характеристики приватних мереж.

4. Яка залежність вразливості та атаки?

ДОМАШНЄ ЗАВДАННЯ

1. Перерахувати основи види вразливостей інформаційно-комунікаційних систем.

2. Перерахувати основи види інформаційних атак.

3. Перерахувати основи види засобів захисту інформації в інформаційно-комунікаційних системах.

ХІД РОБОТИ

Щоб налаштувати захист пристрою за допомогою цих функцій Безпека у Windows, натисніть кнопку Пуск > Настройки > Оновлення та захист > Безпека у Windows. Піктограми стану зазначають рівень безпеки: зеленим кольором свідчить про те, що наразі рекомендованих дій немає, жовтий колір означає, що для вас рекомендується безпечність, червоний – це попередження, що щось потребує негайної уваги. Подальші дії здійснити за однім з варіантів (табл.1), де кожний варіант відповідає номеру студента в списку групи.

За вибраним варіантом здійснити настроювання двох параметрів безпеки та зробити скрин-шоти результатів своїй роботи на кожному кроці.

Скласти звіт.

Таблиця 1

ВИХІДНІ ДАНИ ЗА ВАРІАНТАМИ

Варіант	***1-й параметр***	***2-й параметр***
1	Захист від вірусів і загроз	Параметри Антивірусу для Захисника Windows. Вимкнути періодичне сканування
2	Брандмауер і захист мережі	Мережа домену. Вимкнути захист комп’ютера під час використанні доменних мереж
3	Керування програмами та браузерами	Заблокувати перевірку програм та файлів
4	Захист від вірусів і загроз	Відкрити програму 360 Total Security. Антивірус. Здійснити вибіркову перевірку робочого столу комп’ютера
5	Брандмауер і захист мережі	Дозволити програмам обмінюватися даними через Брандмауер для Захисника Windows
6	Захист від вірусів і загроз	Настройка конфіденційності. Мовлення. Встановити параметр, який не дозволяє технологію онлайн-розпізнавання мовлення
7	Керування програмами та браузерами	Запобігання експлойтам. Настройки запобігання експлойтам. Вимкнути забезпечення випадковості виділення пам’яті
8	Захист від вірусів і загроз	Відкрити програму 360 Total Security. прискорення. Ввімкнути автоматичну оптимізацію розділу завантаження для прискорення завантаження комп’ютера
9	Брандмауер і захист мережі	Настоювання параметрів для кожного типу мережі. Вимкнути Брандмауер для Захисника Windows

Варіант	*1-й параметр*	*2-й параметр*
10	Захист від вірусів і загроз	Настройка конфіденційності. Загальні. Встановити параметр, який не дозволяє Windows відстежувати запуски програм для покращення меню «Пуск» і результатів пошуку
11	Брандмауер і захист мережі	Настойки сповіщень брандмауера. Керування сповіщеннями. Увімкнути отримання сповіщень щодо захисту облікового запису за всіма проблемами.
12	Захист від вірусів і загроз	Відкрити програму 360 Total Security. Здійснити повну перевірку комп’ютера
13	Брандмауер і захист мережі	Приватна мережа. Вимкнути захист комп’ютера під час використанні приватної мережі
14	Керування програмами та браузерами	Вимкнути фільтр захисту комп’ютера від шкідливих сайтів та навантажень
15	Захист від вірусів і загроз	Відкрити програму 360 Total Security. Очищення. Здійснити очищення плагинів та непотрібних файлів комп’ютера
16	Брандмауер і захист мережі	Настойки сповіщень брандмауера. Керування постачальниками. Увімкнути всі елементи захисту комп’ютера.
17	Захист від вірусів і загроз	Настройка конфіденційності. Загальні. Встановити параметр, який не дозволяє веб-сайтам отримувати доступ до списку мов

Варіант	***1-й параметр***	***2-й параметр***
18	Брандмауер і захист мережі	Загальнодоступна мережа. Заборонити вхідні підключення під час використання загальнодоступних мереж
19	Керування програмами та браузерами	Вимкнути фільтр SmartScreen для програм з MicrosoftStore
20	Захист від вірусів і загроз	Настройка конфіденційності. Загальні. Встановити параметр, який не дозволяє програмам використовувати код отримувача реклами

ЗМІСТ ЗВІТУ

1. Титульний лист (згідно Додатку А)
2. Виконане домашнє завдання.
3. Опис вихідних даних за варіантом.
4. Скрин-шоти результатів своїй роботи на кожному кроці.
5. Опис результатів роботи комп’ютера при вище встановлених параметрах.

ЛАБОРАТОРНА РОБОТА № 2

Тема: 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

На робочому столі комп'ютера за допомогою лівою кнопки миші активізувати ярлик **«Мой компьютер»,** далі натиснути на праву кнопку миші. У контекстному меню за допомогою лівої кнопки миші вибрати команду **«Управление»** (рис. 2.1).

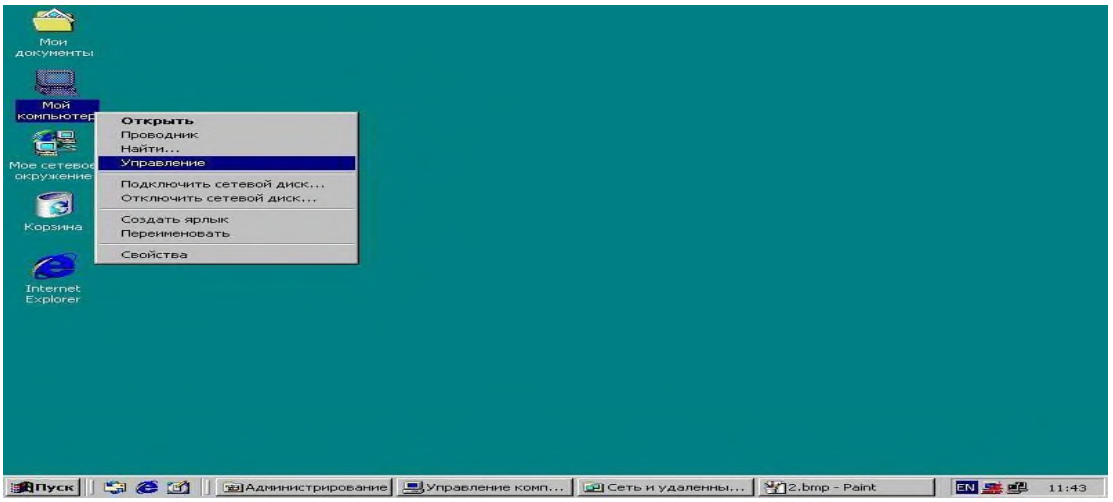

Рисунок 2.1. Виклик вікна «Управління комп'ютером»

У вікні «**Управление компьютером**» за допомогою лівої кнопки миші активізувати розділ **«Службы и приложения»**, далі **«Службы»** (рис.2.2).

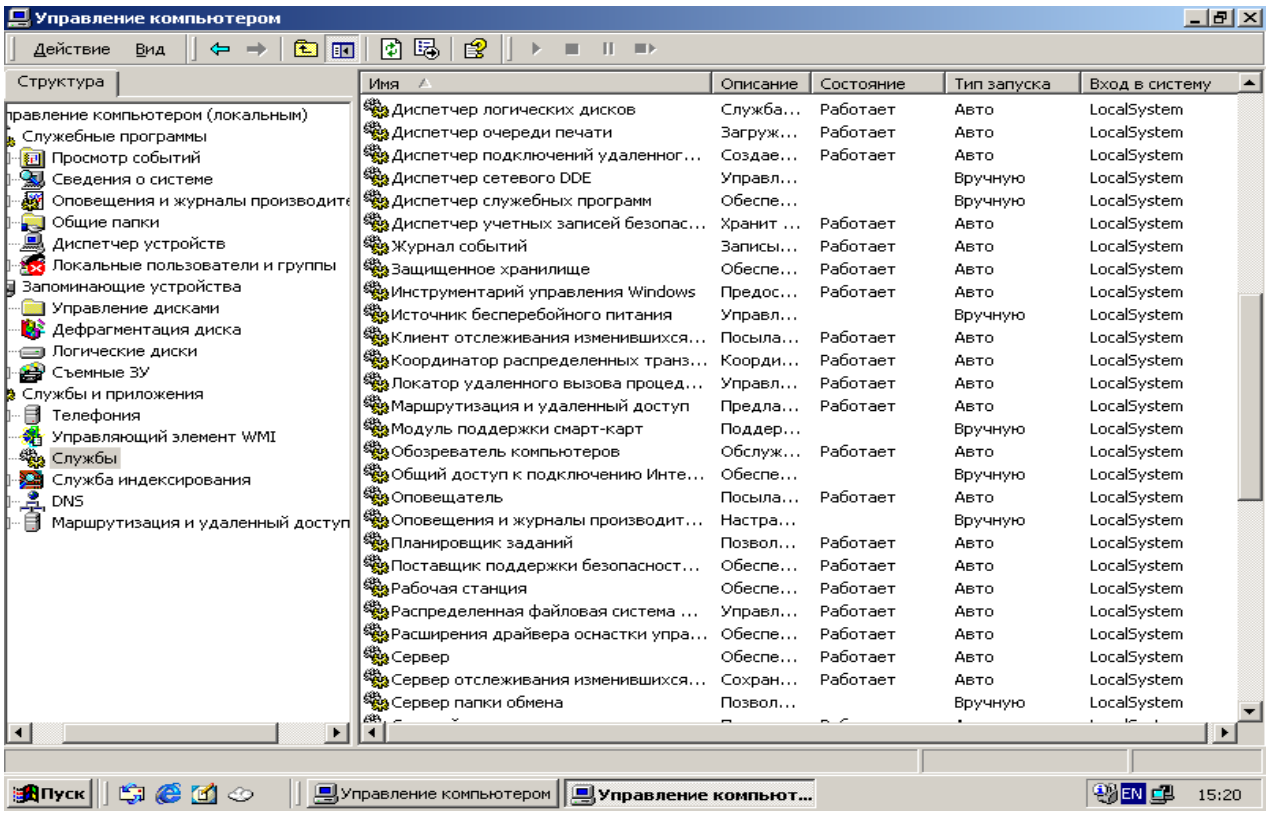

Рисунок 2.2. Виклик вікна «Службы»

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.

У разі необхідності можливо перевірити наявність та стан запуску служб за допомогою командного рядку операційної системи. Для цього на серверібази даних вузла натиснути на кнопку **«Пуск»** панелі задач ОС, далі вибрати команду **«Выполнить»** та ввести у командному рядку команду «**cmd**» (рис.2.3) далі **«ОК»**.

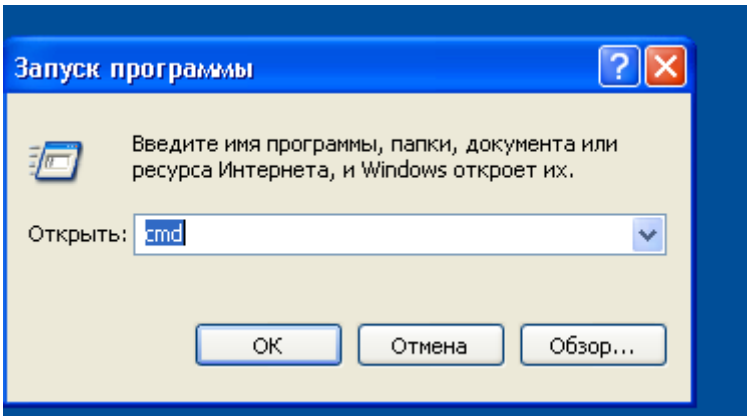

Рисунок 2.3. Запуск команди «**cmd**»

У вікні, що з’явиться (рис. 2.4), ввести в командному рядку команду **«netstart»**.

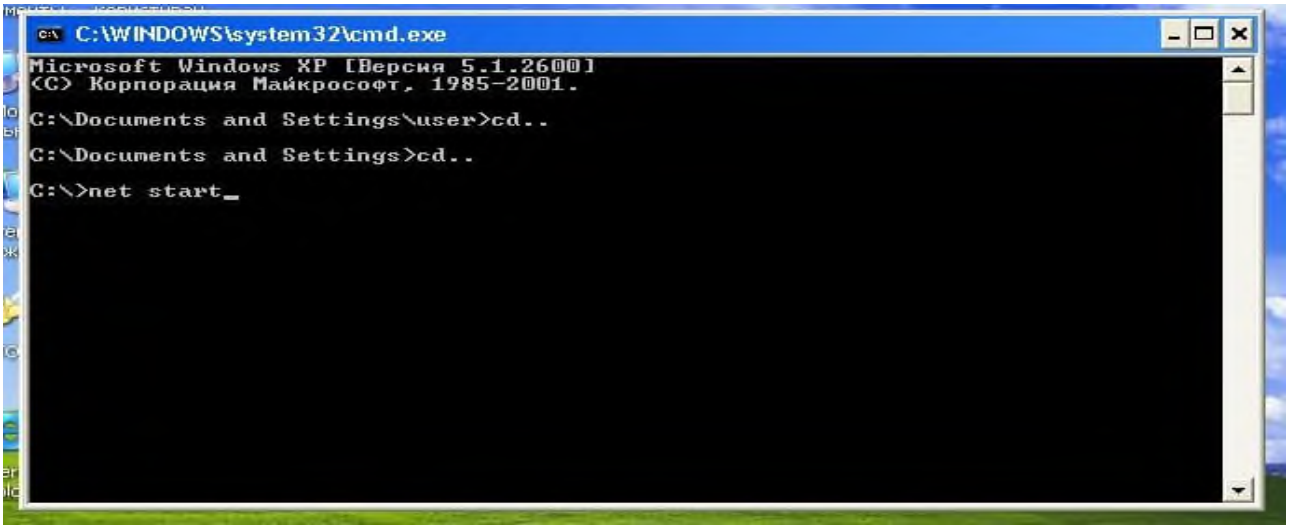

Рисунок 2.4. Запуск команди **«net start»**

Виконати перегляд служб, які завантажені та знаходяться у працездатному стані (рис. 2.5).

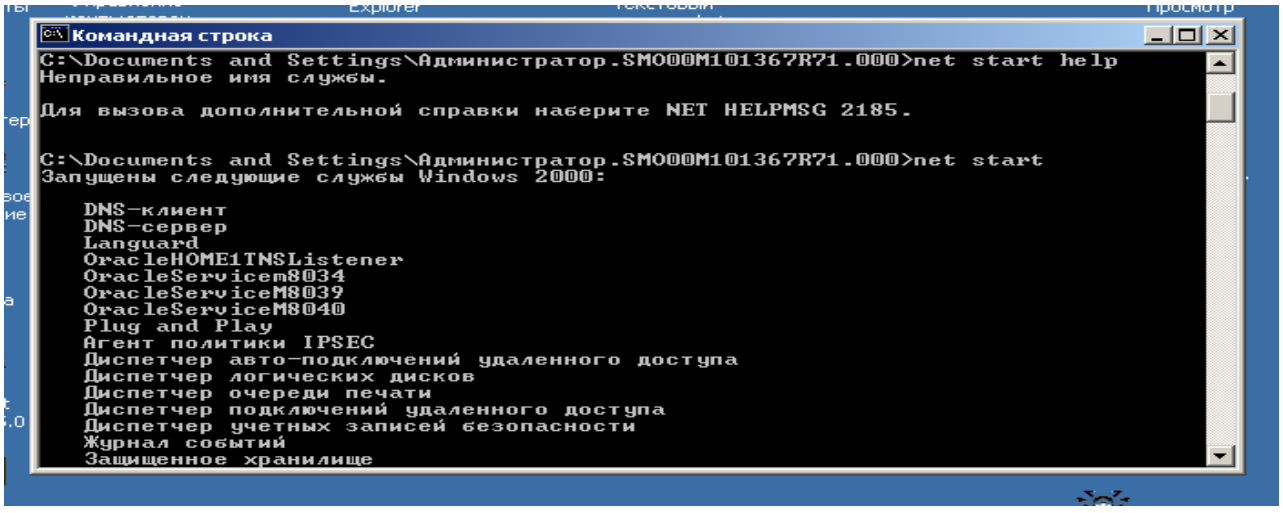

Рисунок 2.5. Вікно перегляду служб, що завантажені

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.2.6).

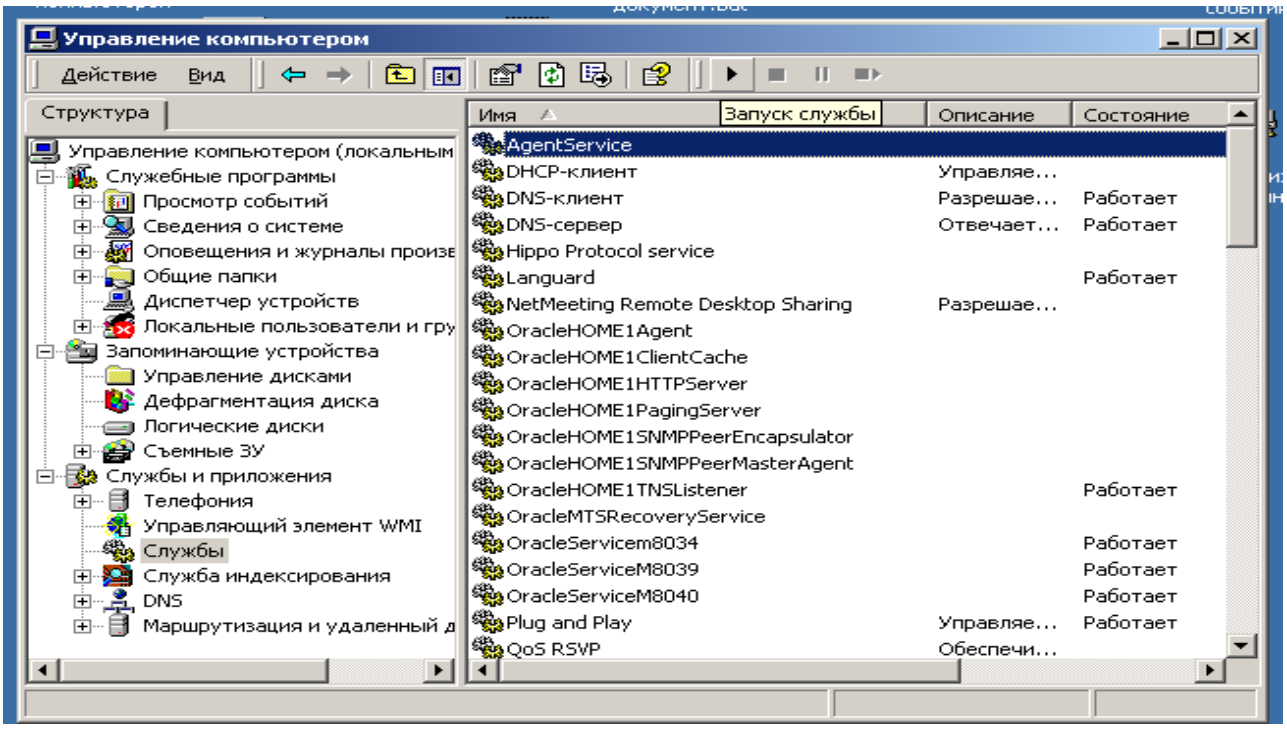

Рисунок 2.6. Порядок запуску служби

За результатами робіт зробити остаточний висновок щодо наявності тастану працездатності програмних служб ОС ПЕОМ.

2. Моніторинг завантаженості операційної системи Windows. Контроль за станом пам’яті ПЕОМ

Послідовно на комп’ютері перевірити параметрипам’яті ОС, а саме:

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

Для цього запустити програмне забезпечення «**Диспетчер задач Windows»** та протягом 20-30 хвилин здійснити аналіз параметрів пам’яті, які використовує операційна система (рис.2.1).

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.2.1).

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.2.2). На прикладі роботи ПЕОМ видно, що розмір файлу підкачки складає **1152** Мб, що приблизно в **1,5 рази більше** розміру встановленої фізичної пам'яті.

Визначити розмір пам'яті, що використовують програми (процеси), які запущені на ПЕОМ користувача (рис.2.3).

Для цього у вікні «**Диспетчера задач»** необхідно активізувати закладку

«Процессы» (рис.2.3) 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.

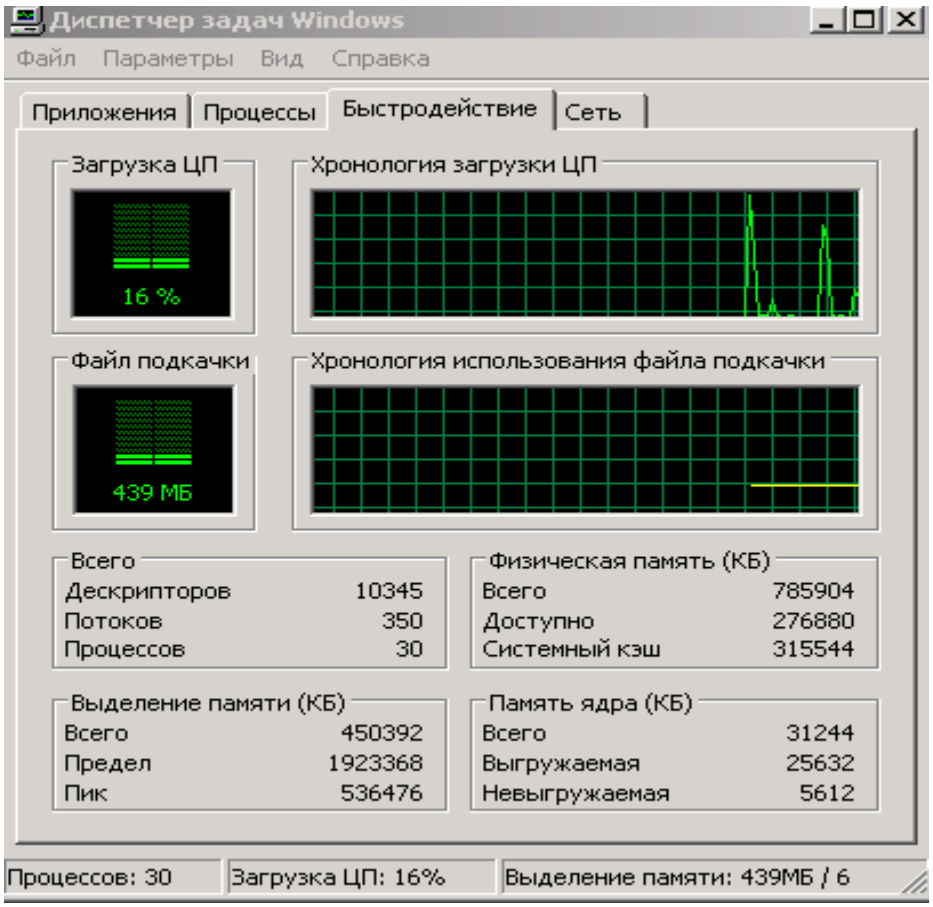

Рис.2.7. Від вікна Диспетчера задач Windows

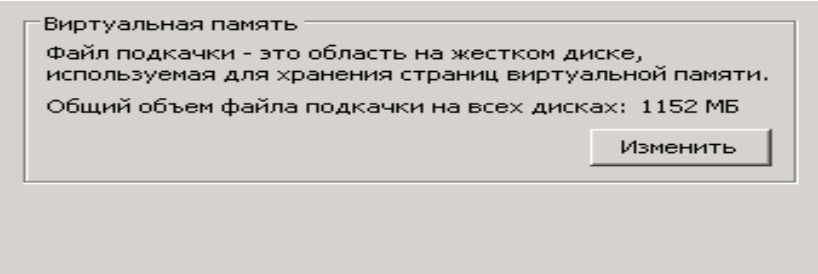

Рисунок 2.8. Визначення розміру файлу підкачки ОС Windows

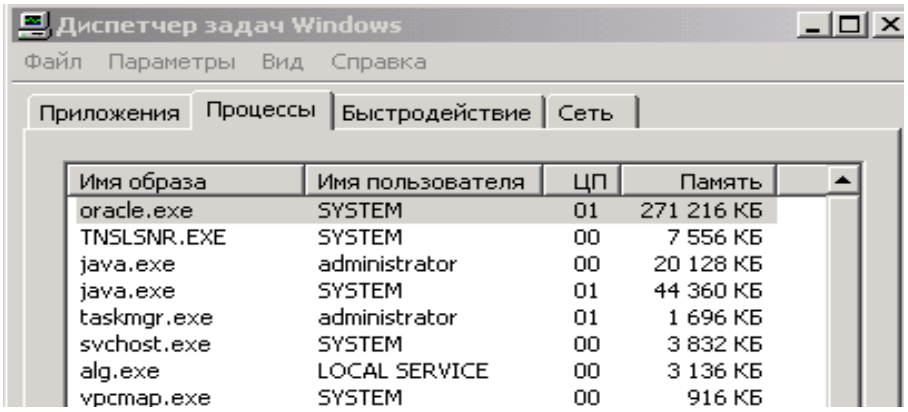

Рисунок 2.9. Від вікна щодо запущених процесів ОС Windows

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

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 комп’ютерів учбового класу розмір файлу підкачки складає **785*1,5 = 1177Мб**, що приблизно співпадає з існуючим його розміром **(1152 Мб).**

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

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.2.10).

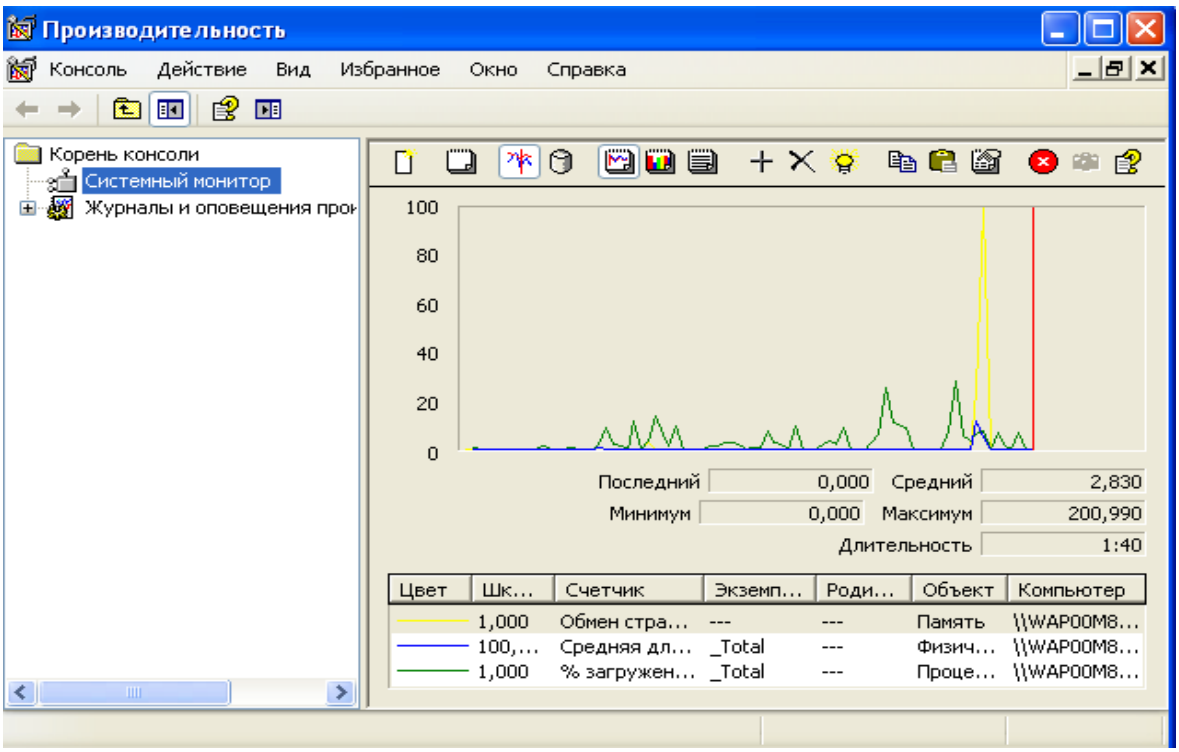

Рисунок 2.10. Активізація розділу **«Системный монитор»**

На панелі інструментів вікна **«Системный монитор»** 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.2.11).

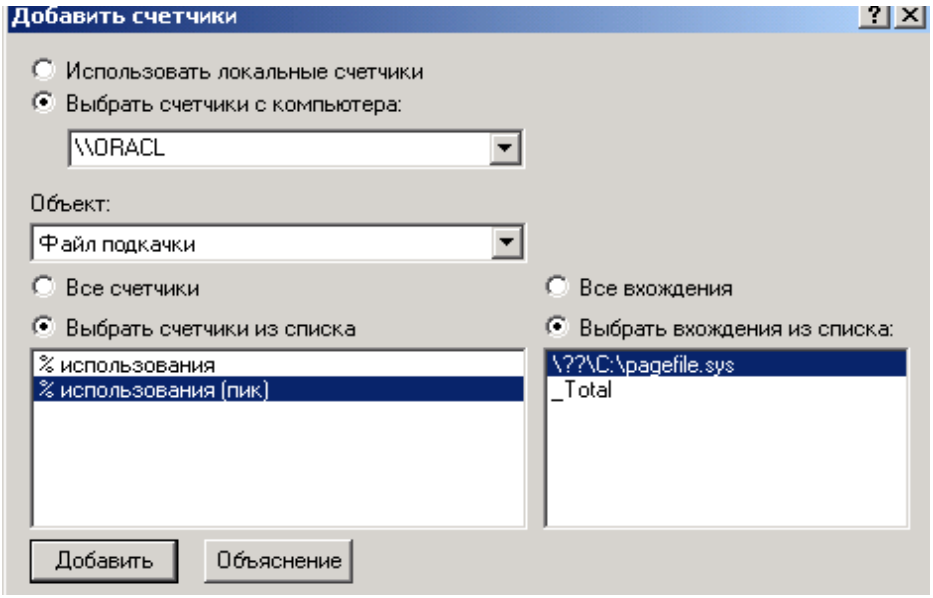

Рисунок 2.11. Вибір лічильника **«% использования»**

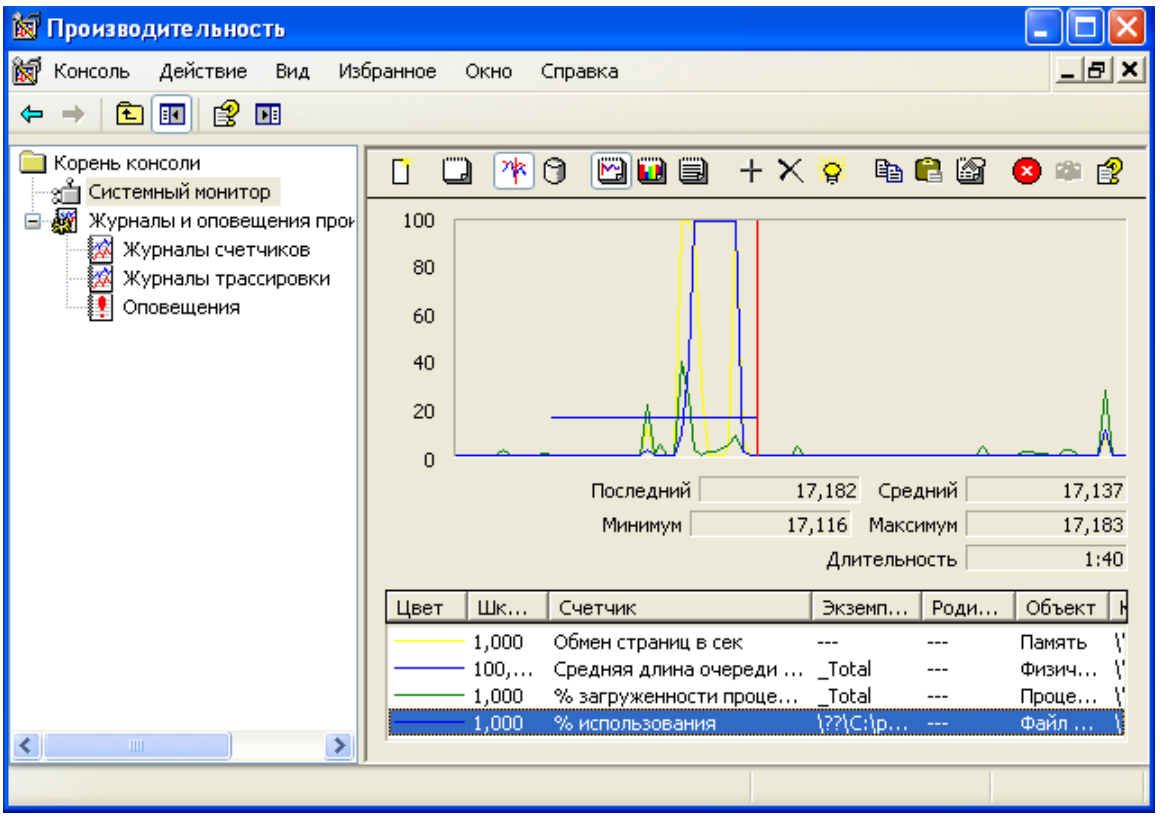

Рисунок 2.12. Активізація лічильника **«% использования»**

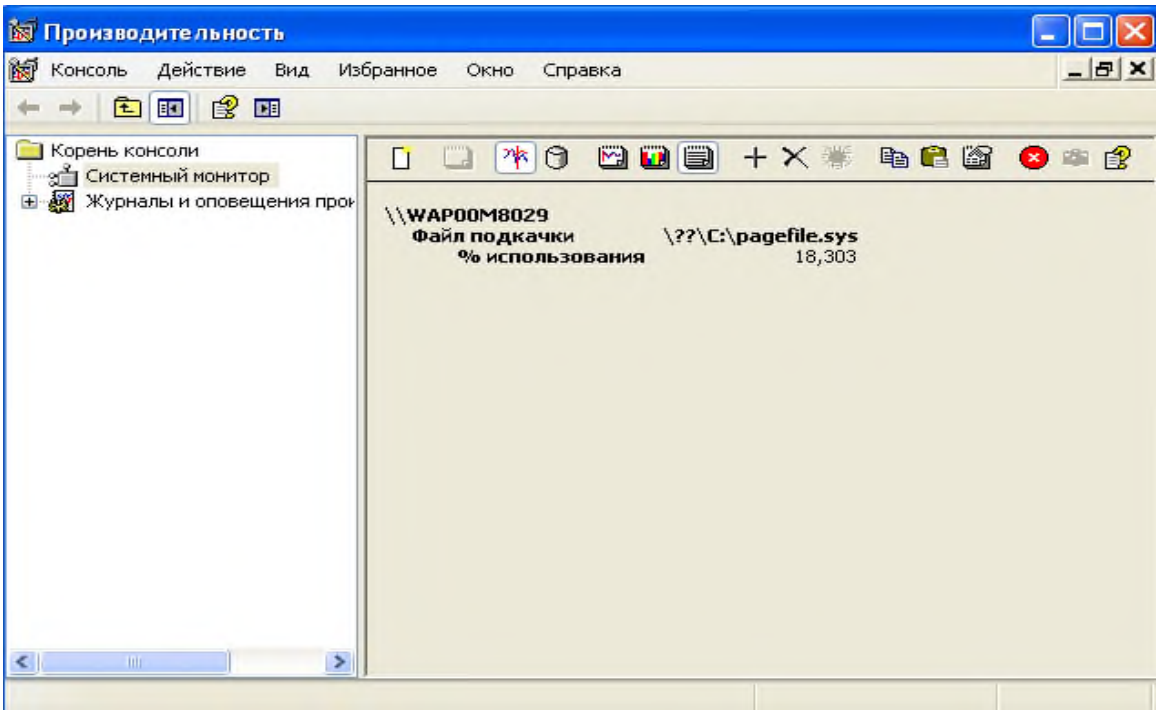

Рисунок 2.13. Перегляд звіту

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

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

ЛАБОРАТОРНА РОБОТА № 3

Тема: 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

ХІД РОБОТИ

3.1. Контроль за станом завантаженості процесора на ПЕОМ

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.

Виконати перевірку загальної завантаженості процесора за допомогою вікна **«Диспетчер 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 кожнийпроцес окремо (рис.3.1).

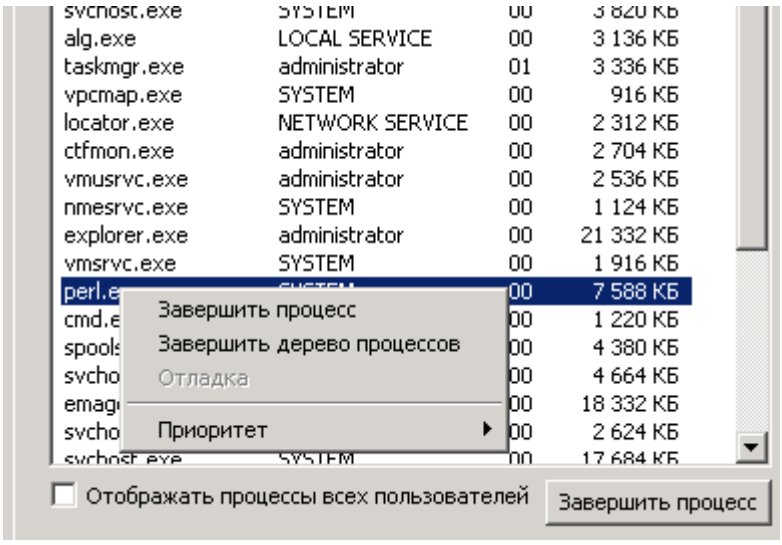

Рис.3.1. Відключення процесів, що заважають роботі ОС

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

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.3.1).

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

Натиснути на кнопку **«Пуск»** панелі задач ОС на ПЕОМ користувача, далі необхідно вибрати кнопку **«Выполнить»**, у вікні, щоз'явиться набрати команду **msconfig.exe** (рис.2). У вікні, що з'явиться активізувати закладку **«Атозагрузка»** (рис.3.2).

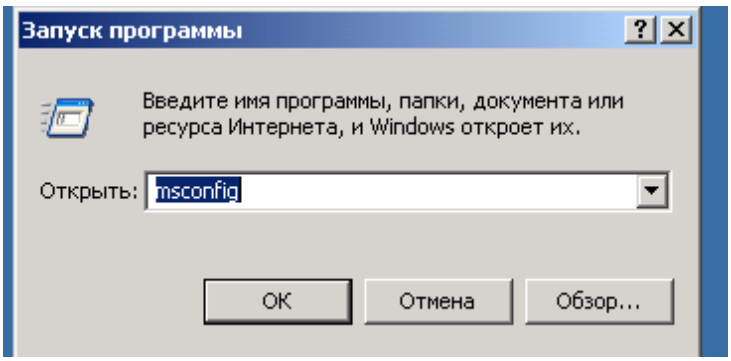

Рисунок 3.2. Запуск команди **msconfig.exe**

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. 3.2).

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

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.

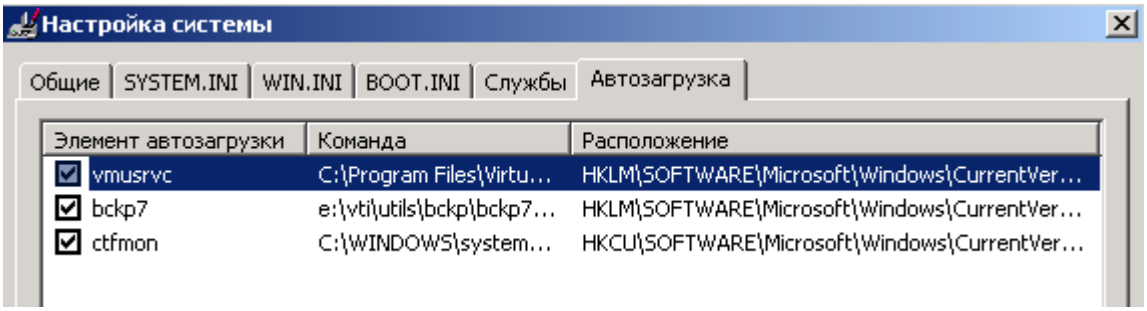

Рисунок 3.3. Відключення автозавантаження програм ОС

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 3.1

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 (Пам’ять: Байт віртуальної пам’яті)	Загальний розмір віртуальної пам’яті, яку на даний час займають всі процеси користувачів
Memory: Commit Limit (Пам’ять: Межа віртуальної пам’яті	Величина, яка визначає кількість віртуальної пам’яті система може надати без збільшення розміру файлу підкачки.
Process: % Processor Time (Процес: % завантаженості процесора)	Ступень використання процесора заданим процесом

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

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

За результатами робіт підготувати звіт щодо завантаженості параметрів операційної системи ЕОМ 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: CommitLimit	Величина, яка визначає кількість віртуальної пам’яті система може надати без збільшення розміру файлу підкачки		
Process: % Processor Time	Ступень використання процесора заданим процесом		

ЛАБОРАТОРНА РОБОТА № 4

Тема: Перевірка програмного забезпечення ПЕОМ на наявність комп'ютерних вірусів

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

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:

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

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.

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 кольору програми **Kaspersky Antivirus**.

Рисунок 4.1. Перевірка наявності та активності роботи **Kaspersky Antivirus**

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.4.2), далі натиснути ліву кнопку миші та переглянути головне вікно програми Антивирус Касперского (рис.4.2).

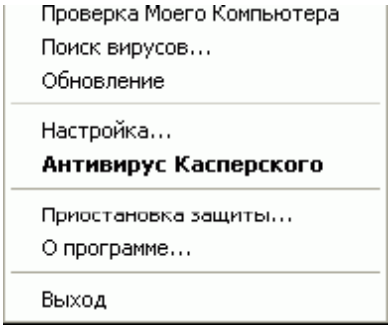

Рис.4.2. Вид вікна контекстного меню **«Kaspersky Antivirus»**

Здійснити перевірку змінних носіїв інформації на наявність комп'ютерних вірусів. Для цього у вікні програми **Kaspersky Antivirus** необхідно натиснути на кнопку **«Поиск вирусов»** (рис.4.3)**.**

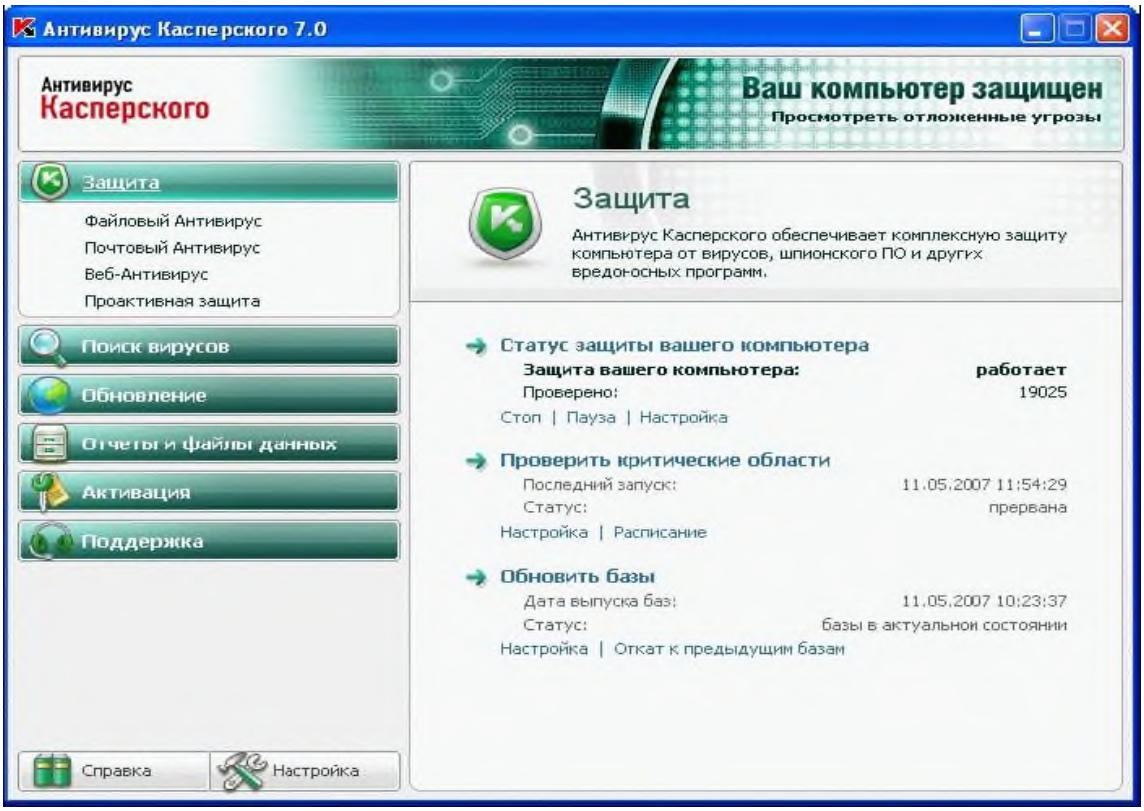

Рисунок 4.3. Від головного вікна програми «**Kaspersky Antivirus»**

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.4.4). У разі необхідності необхідно виконати перевірку наявності вірусів на ПЕОМ (жорсткі диски, поштові скриньки).

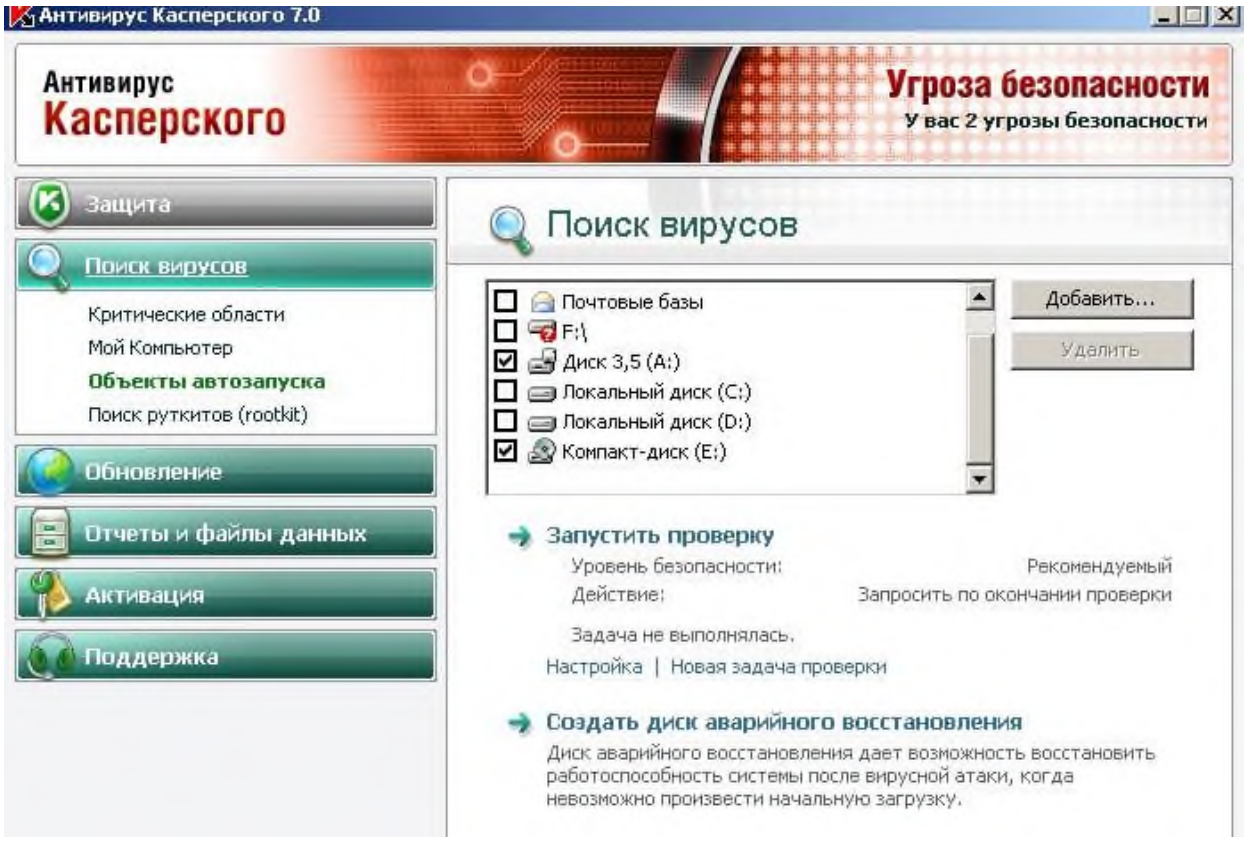

Рисунок 4.4. Запуск перевірки об’єктів на наявність комп’ютерних вірусів

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

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.4.5).

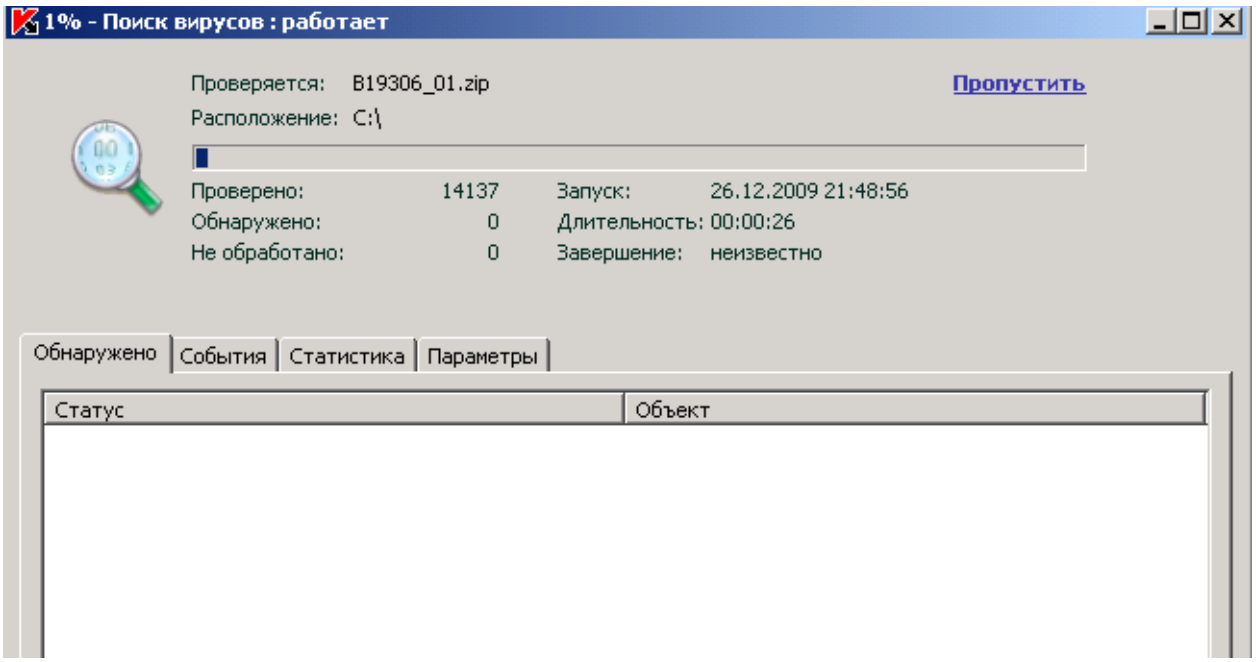

Рисунок 4.5. Стан перевірки носія з інформації на ПЕОМ

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.4.6.).

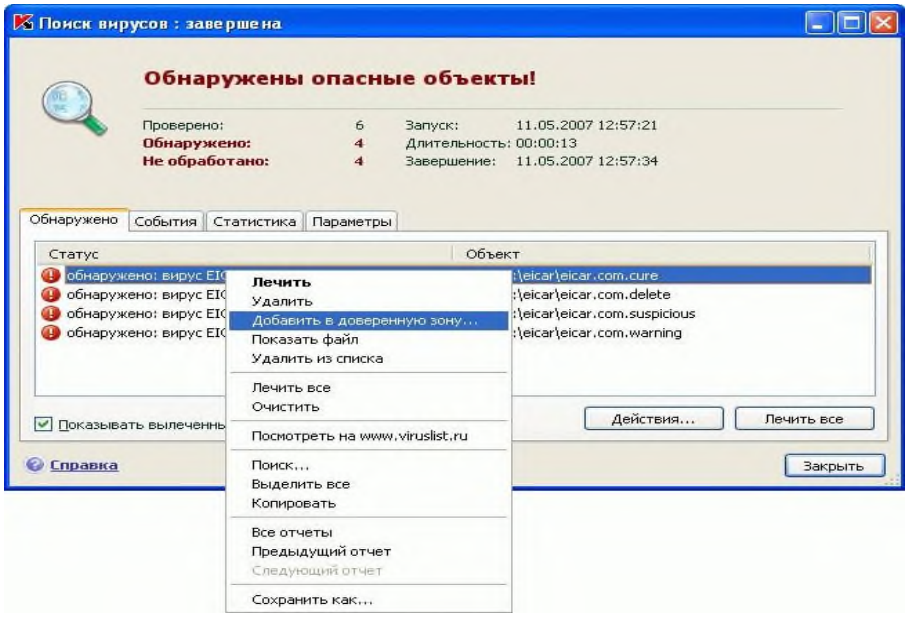

Рисунок 4.6. Дії під час виявлення комп'ютерних вірусів на ПЕОМ

4.2. Технологія актуалізації антивірусних баз на ПЕОМ

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_26112022** де **26112022** – дата оновлення.

Здійснити копіювання порцій оновлення на логічний диск ПЕОМ за адресою **E:\kav_upd_26112022** 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 каталогпотребує віддалення.

Для виконання оновлення запустити програму Kaspersky Antivirus та у головному вікні програми натиснути на кнопку «Обновление». На правій половині вікна «Обновление» перевірити дату випуску баз, кількість записів в базах та їх статус, після чого натиснути на кнопку «Настройка» (рис.4.7).

Рисунок 4.7. Від вікна **«Обновление»** програми **Kaspersky Antivirus**

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_26112022 та натиснути на кнопку «ОК» (рис.4.8).

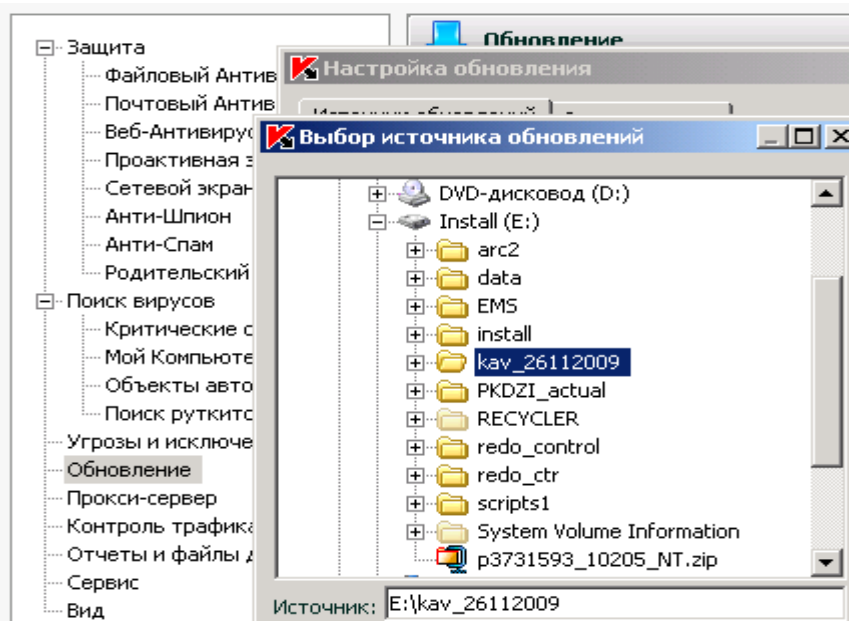

Рисунок 4.8. Вибір каталогу з порціями оновлень антивірусних баз

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.

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

Представити матеріали роботи для захисту викладачу.

ЗРАЗОК ЗВІТУ

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

ЛАБОРАТОРНА РОБОТА № 5
Тема: 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:

5.1. Перегляд та перевірка характеру подій у журналах подій ОС

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 компьютер»,** натиснути на праву кнопку миші, далі **«Управление»**, увікні, що з'явиться, вибрати **«Просмотр событий»** та відповідний журнал подій:

на ПЕОМ користувачів (рис.5.1):

- додатків;
- системи.

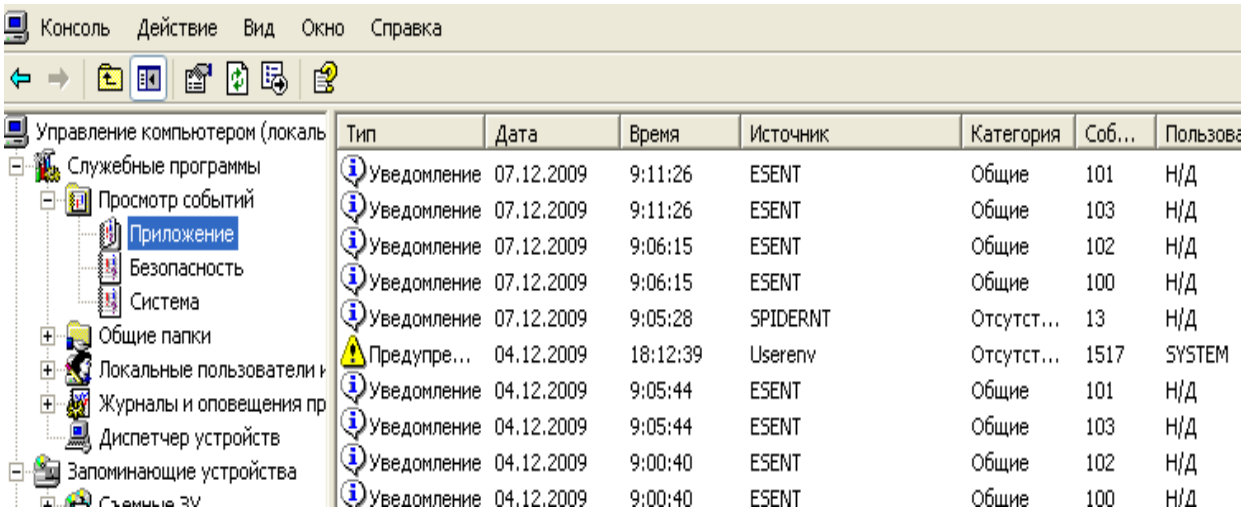

Рисунок 5.1. Вигляд вікна перегляду журналів подій на ПЕОМ

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.5.2).

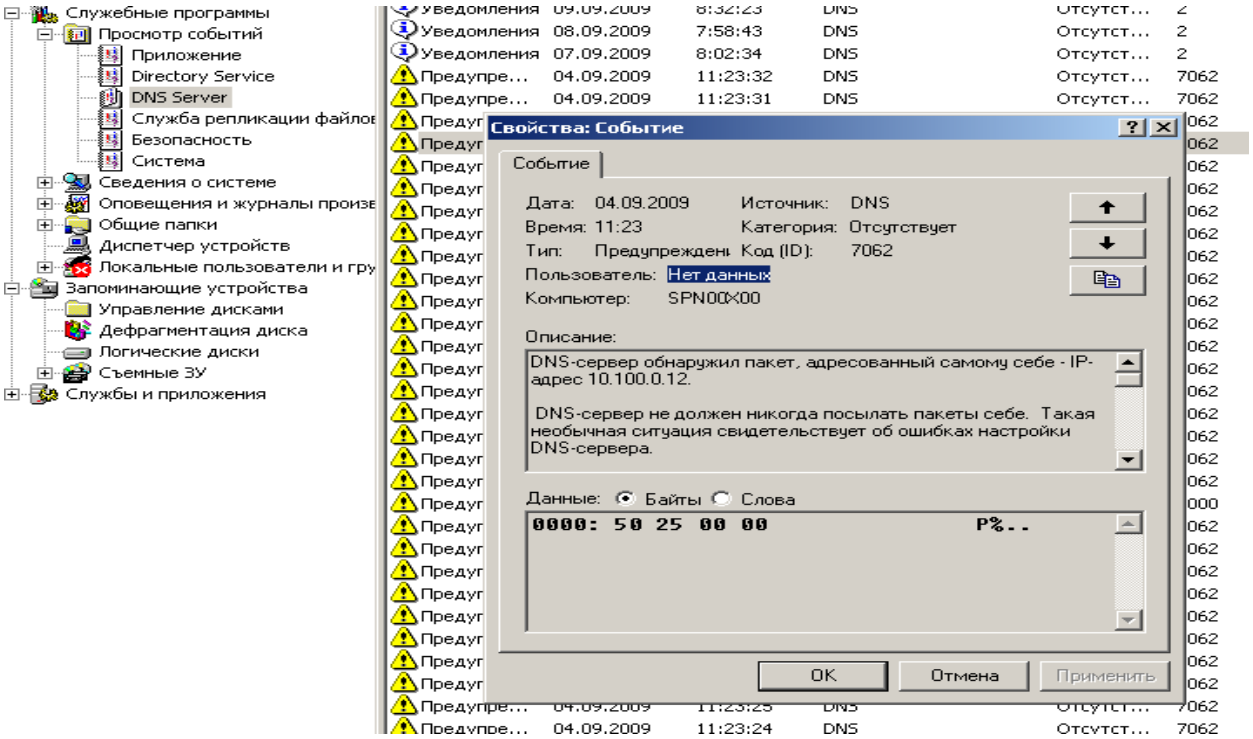

Рисунок 5.2. Перегляд вмісту події за допомогою журналу **DNS Server**

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

5.2. Перевірка характеру подій у журналі безпеки ОС

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», «Политика безопасности домена»,** вибрати **«Локальные политики»** та відкрити оснастку **«Політика аудиту».** Здійснити огляд встановлених параметрів аудиту (рис.5.3).

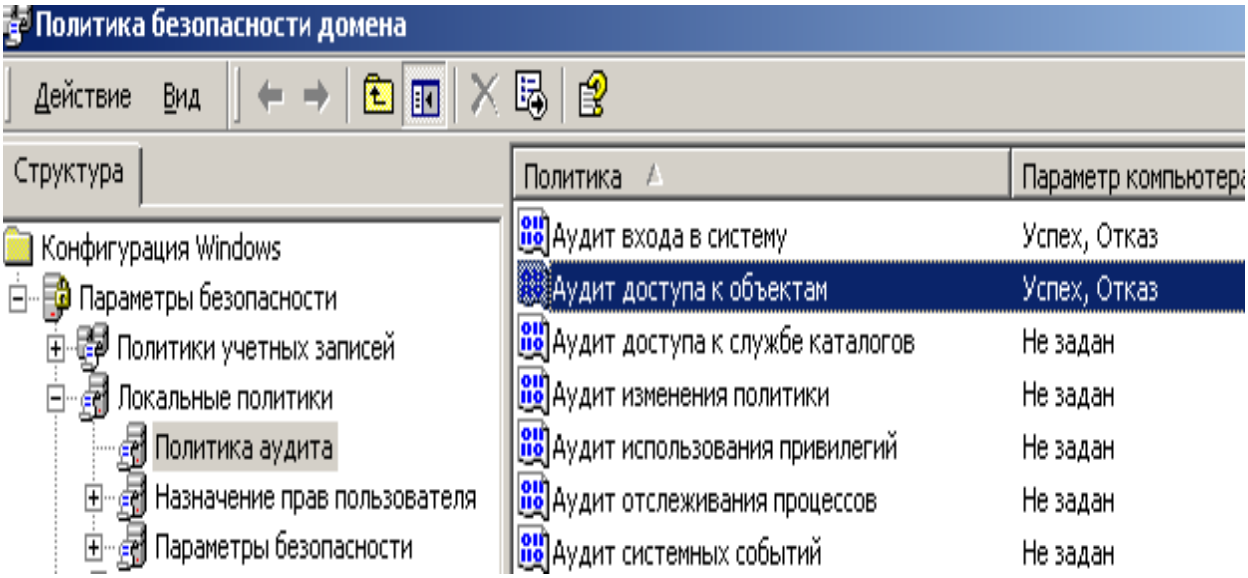

Рисунок 5.3. Перевірка налаштувань політик аудиту на сервері навчального класу

Послідовно виконати аналіз журналів безпеки ОС на ЕОМ користувачів. Для цього на робочому столі операційної системи ЕОМ активізувати лівою кнопкою миші значок **«Мой компьютер»,** 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.5.4).

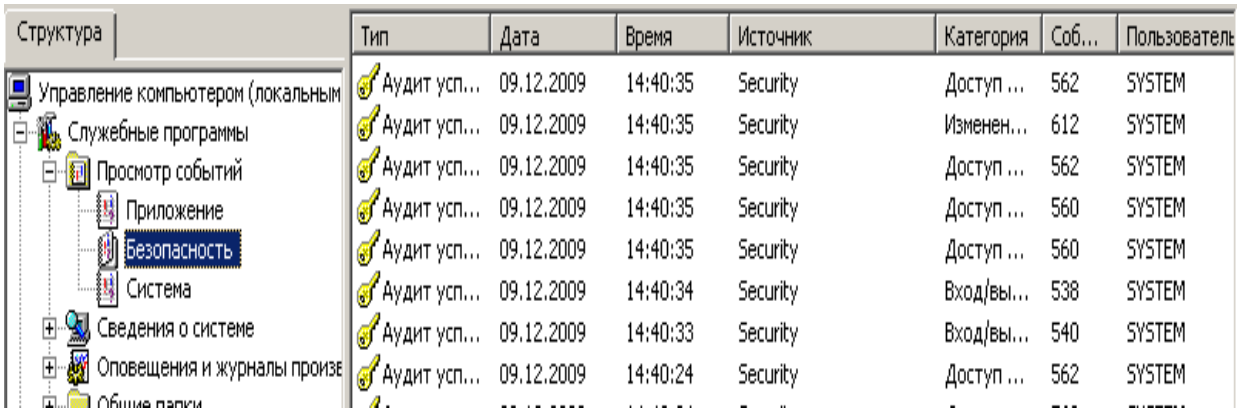

Рисунок 5.4. Перегляд типу подій в журналі безпеки ОС

Згідно п. 1.2. виконати аналіз вмісту повідомлень, які відображені у журналі безпеки ЕОМ користувача (рис.5.5), особливо щодо подій, які зазначені у таблиці.

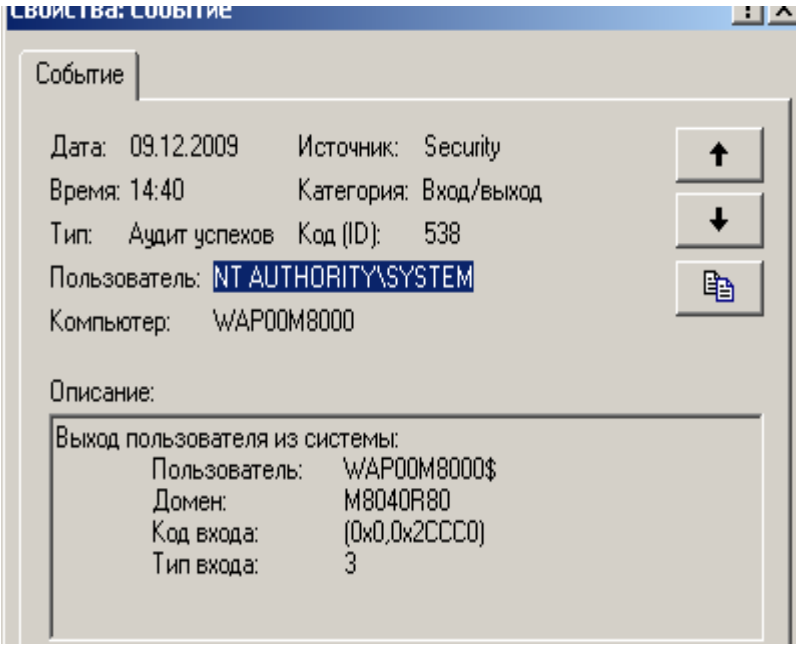

Рисунок 5.5. Перегляд події в журналі безпеки АРМ користувача

Таблиця 4.1

Номера подій журналу безпеки ОС, які потребують перегляду таконтролю

№ події	**Короткий зміст (мовою операційної системи)**
528	Успішний вхід до системи
529	Відмова входу до системи. Невідоме ім'я користувача
530	Користувач намагався увійти в систему
531	недозволений йому час
532	Обліковий запис користувача заблоковано
533	Обліковий запис користувача прострочений або застарілий
534	пароль користувача.
537	Користувач обмежений входом лише на деякі робочі станції, а він намагається увійти до системи з іншого
538	комп'ютера
540	Спроба запуску служби за допомогою облікового
560	записи користувача, який не має права на запуск служб
562	Відмова з невідомої причини
628	Вихід користувача із системи
642	Успішний мережевий вхід до системи
644	Фіксує відкриття об'єкта користувачем

Перевірити записи в журналі безпеки ОС ЕОМ користувачів щодо подій, пов’язаних з реєстрацією користувача на ЕОМ, 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.5.6).

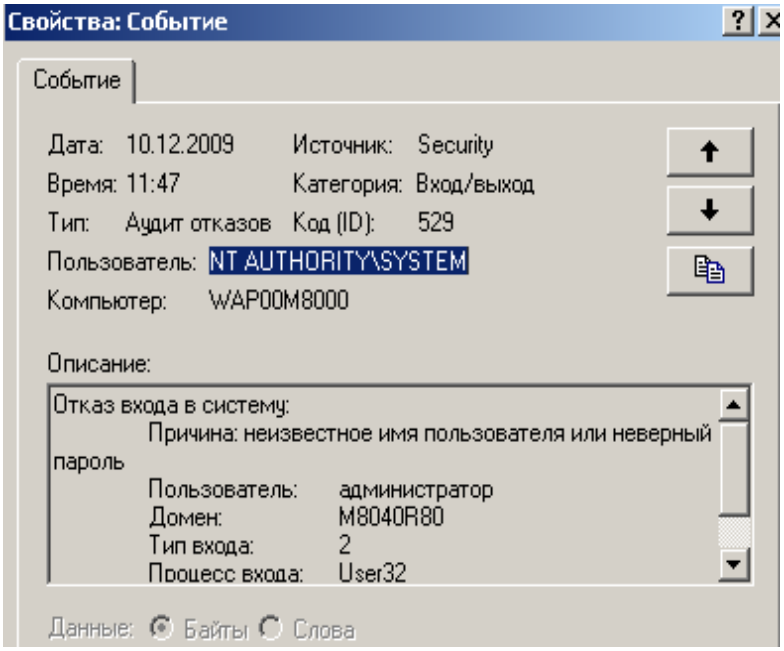

Рисунок 5.6. Перегляд події в журналі безпеки щодо спроби несанкціонованого доступу на ПЕОМ користувача

Здійснити аналіз подій журналу безпеки щодо доступу користувача до об’єктів системи (події за номерами **560** та **562,** рис.5.7). 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.

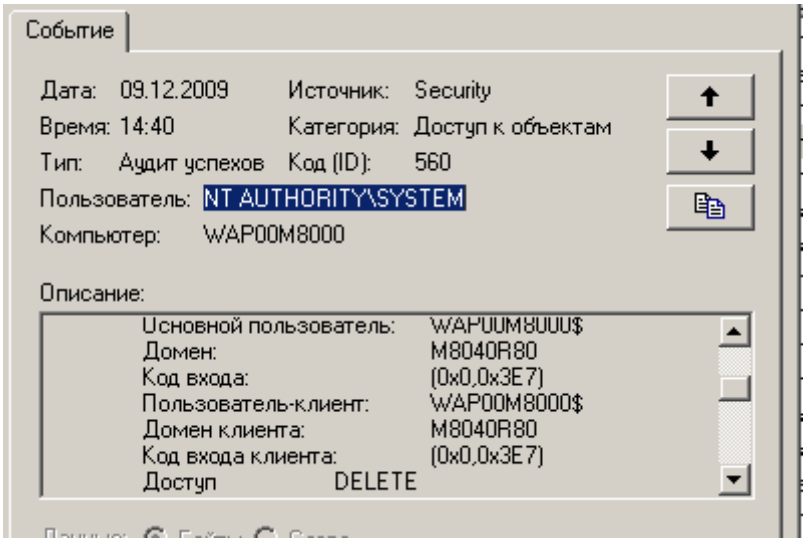

Рисунок 5.7. Перегляд події в журналі безпеки щодо доступу до прикладного програмного забезпечення АРМ користувача

5.3. Перевірка налаштувань журналів подій та безпеки ОС на ПЕОМ

На АРМ користувача або сервера вузла ДІС відрити вікно **«Управлениекомпьютером»,** 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.5.8).

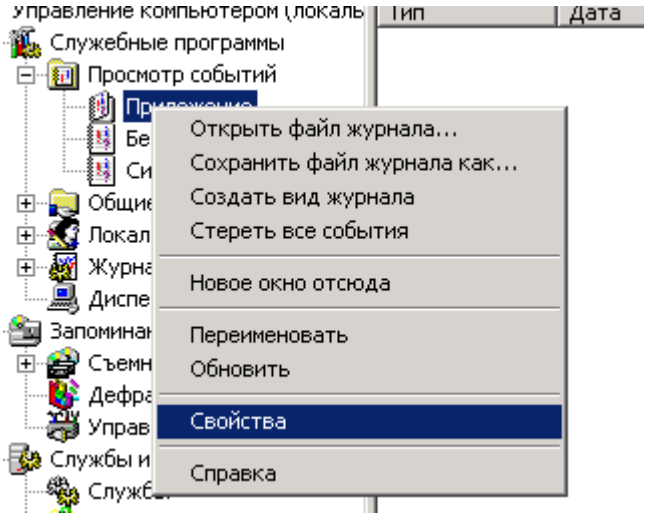

Рисунок 5.8. Вибір вікна властивостей журналу подій

Перевірити значення конфігураційних параметрів журналу, а саме, його максимальний розмір та правило записи у журнал при його заповненні **(затирати події старіші за 7 днів)**. За допомогою кнопки **«Очистить журнал»** здійснити видалення його повідомлень (рис.5.9).

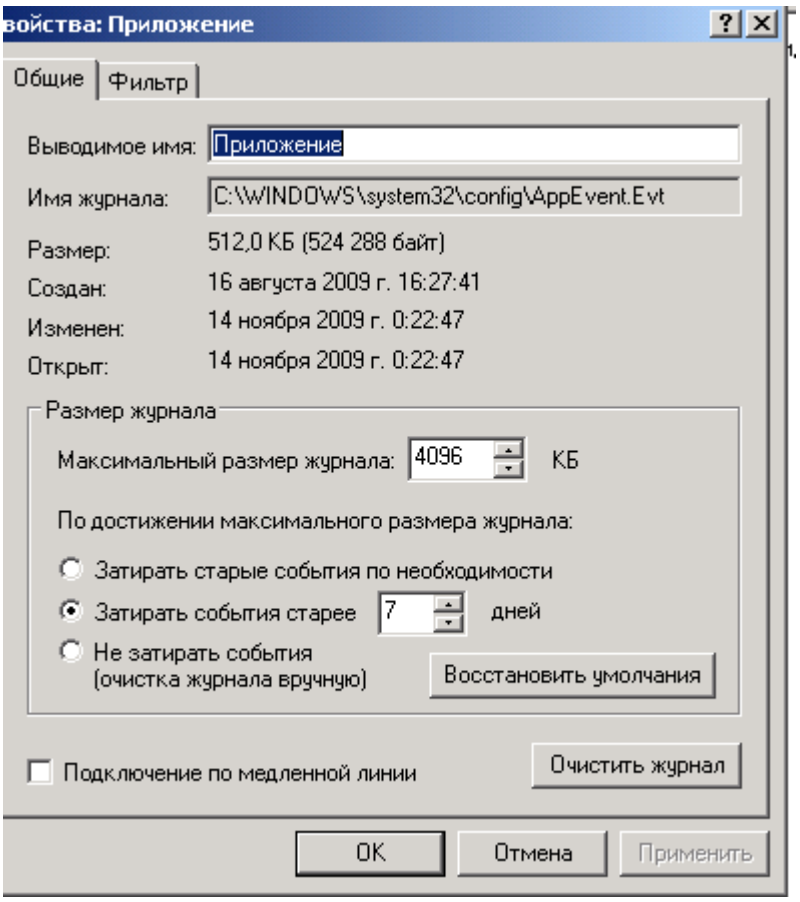

Рисунок 5.9. Від вікна налаштувань журналу повідомлень ОС

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

ЗРАЗОК ЗВІТУ

Таблиця 5.1

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

Таблиця 5.2

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

Рекомендована література

Основна література:

1. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.

2. Інформаційна безпека в комп'ютерних мережах : навч. посіб. — Кропивницький: Видавець Лисенко В. Ф., 2020. — 295 с.

3. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.).

4. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.

5. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 1 – Комплекси засобів захисту інформації від НСД: навч. посіб. / М.В. Захарченко, В.Г. Кононович, В.Й. Кільдішев, Д.В. Голев // За ред. ак. МАІ М.В. Захарченка.– Одеса: ОНАЗ ім. О.С. Попова, 2011. – 168 с.

6. Захарченко М.В. Інформаційна безпека інформаційно-комунікаційних систем. Захист інформації від НСД у каналах зв'язку: навч. посіб. / М.В. Захарченко, В.В. Топалов, М.С. Русляченко // За ред. чл.-кор. МАЗ В.Г. Кононовича. – Одеса: ОНАЗ ім. О.С. Попова, 2014. – 228 с.

7. 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.

8. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія. - Київ, ЦП «Компринт», 2019 – 361 с.

9. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

10. Чунарьова А.В. Сучасні методи аудиту та моніторингу в задачах захисту інформації // Проблеми інформатизації та управління. – К.: НАУ, 3(43), 2013.

Додаткова література:

1. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99. – Київ: ДСТСЗІ СБ України, 1999. – 16 с.

2. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 2.2–004–99. – Київ: ДСТСЗІ СБ України, 1999. – 55 с.

3. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.2–005–99. – Київ: ДСТСЗІ СБ України, 1999. – 23 с.

4. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–003–99. – Київ: ДСТСЗІ СБ України, 1999. – 26 с.

5. Антонюк А., Жора В. Моделювання доступу та каналів витоку в інформаційних системах / Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. - №3. – С.156-160.

6. Антонюк А.А. О выборе профиля защищенности // Проблемы программирования, 2001, №2, С.26-29.

7. Антонюк А.О., Жора В.В. Загрози інформації і канали витоку // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2001, №2, С.22-23.

8. Антонюк А.А. Теоретические и прикладные аспекты защиты информации в автоматизированных системах // Проблемы программирования, 2002, № 3-4, С.55-59.

9. Антонюк А.О. Політика безпеки в захищених автоматизованих системах // Наукові записки НаУКМА. - Київ: НаУКМА, 2003, т. 21, с.19-22.

10.Антонюк А.О. Основи захисту інформації в автома-тизованих системах. Навчальний посібник.- К: Видавничій дім «КМ Академія», 2003, с.244.

11.Антонюк А.А. О функциях защиты информации // Проблемы программирования, 2005, № 4, с.51-55.

12.Антонюк А.О., Жора В.В Використання доказового методу для проектування та оцінки рівня захищеності інформаційно-телекомунікаційної системи // Проблемы программирования, 2007, № 3, с.88-96.

13.Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: «ТИД «ДС», 2002. – 688 с.

ДОДАТОК А

Приклад оформлення лабораторної роботи

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

Кафедра кібербезпеки та комп'ютерної інженерії

ЛАБОРАТОРНА РОБОТА

з Моніторинг та аудит інформаційно-комунікаційних систем

На тему : Безпека у Windows

Варіант № 10

Студента 4 курсу КСМ-41 групи
Анастасії ЛИСЕНКО

Керівник проф. Сєлюков О.В.

Національна шкала_____

Кількість балів : _____ Оцінка : ECTS _____

ЗМІСТ

ВСТУП

мета роботи;
короткі теоретичні відомості;
методи досліджень

завдання;
опис усіх етапів виконання роботи;
опис отриманих результатів

ВИСНОВКИ

чому навчився;
оцінка результатів

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Wikipedia. – URL: https://uk.wikipedia.org/wiki/Microsoft_Office (дата звернення 16.10.2022)
2. Wikipedia. – URL: https://uk.wikipedia.org/wiki/Microsoft_Word (дата звернення 19.10.2022)
3. Wikipedia. – URL: https://uk.wikipedia.org/wiki/Microsoft_Excel (дата звернення 13.10.2022)
4. Wikipedia.-URL: https://uk.wikipedia.org/wiki/Microsoft_PowerPoint (дата звернення 22.10.2022)
5. Wikipedia. – URL: https://uk.wikipedia.org/wiki/MATLAB (дата звернення 06.10.2022)

ДОДАТОК Б

Приклади оформлення бібліографічного опису

1. 1. Алефіренко М.Ф. Теоретичні питання фразеології. Харків : Вища школа, 1987. 135 с.
2. Шейко В. М., Кушнаренко Н. М. Організація та методика науково-дослідницької діяльності : підручник. Вид. 6-те, переробл. і допов. Київ : Знання, 2008. 310 с.
3. Кузнєцов М. А., Фоменко К. І., Кузнецов 0.1. Психічні стани студентів у процесі навчально- пізнавальної діяльності : монографія. Харків: ХНПУ, 2015. 338 с.
4. Формування здорового способу життя молоді: навч.-метод. посіб. для працівників соц. служб для сім'ї, дітей та молоді / Т. В. Бондар, О. Г. Карпенко, Д. М. Дикова-Фаворська та ін. Київ: Укр. ін-т соц. дослідж., 2005. 115 с.
5. Дахно І. І., Алієва-Барановська В. М. Право інтелектуальної власності: навч. посіб. / за ред. 1.1. Дахна. Київ : ЦУЛ, 2015. 560 с.
6. Українська мова : енциклопедія / ред. кол. В.М.Русанівський, 0.0.Тараненко та ін. Київ : "Укр.енциклопедія", 2004. 832 с.
7. Новицкий О. М. Сочинения : в 4 т. / ред. изд. : Н. Г. Мозговая, А. Г. Волков; авт. вступ, ст. Н. Г. Мозговая. Киев ; Мелитополь : НПУ им. М. Драгоманова ; МГПУ им. Б. Хмельницкого, 2017. Т. 1. 382 с.
8. Дудоладова О. В. Динаміка мовної репрезентації тендера в англійському публіцистичному дискурсі (друга пол. XX ст.-поч. XXI ст.) : автореф. дис. ... канд. філол. наук : спец. 10.02.04. Харків, 2003. 20 с.
9. Кагановська О. М. Текстові концепти художньої прози : когнітивна та комунікативна динаміка (на матеріалі французької романістики середини XX сторіччя) : дис. ... д-ра філол. наук : спец. 10.02.05. Київ: КНЛУ, 2003. 383 с.
10. Про затвердження Вимог до оформлення дисертації: наказ Міністерства освіти і науки від 12.01.2017 р. № 40. Офіційний вісник України. 2017. №20. С. 136-141.
11. Наукове товариство ім. Шевченка. Львів, наук, б-ка ім. В. Стефаника НАН України. Ф. 1. Оп. 1. Спр. 78. Арк. 1-7.
12. Люмінісцентний матеріал: пат. 25742 Україна : МПК6 С09К11/00, О01Т1/28, 021Н3/00. № 200701472; заявл. 12.02.07; опубл. 27.08.07, Бюл. № 13. 4 с.
13. Шиляев Б. А., Воєводин В. Н. Расчетьі параметров радиационного

повреждения материалов нейтронами источника ННЦ ХФТИ / А1ЧЬ ША с подкритической сборкой, управляемой ускорителем электронов. Харьков : ННЦ ХФТИ, 2006. 19с.: ил., табл. (Препринт. НАН Украиньї, Нац. науч. Центр “Харьк. физ.-техн. ин-т”; ХФТИ 2006-4).

14. ДСТУ 3582:2013. Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила (180 4:1984, ИЕ0; 180 832:1994, КЕС)). [На заміну ДСТУ3582-97; чинний від 2013-08-22]. Вид. офіц. Київ: Мінекономрозвитку України, 2014. 15 с. (Інформація та документація).
15. Історико-правова спадщина України : кат. вист. / Харків, держ. наук, б-ка ім. В. Г. Короленка; уклад.: Л. І. Романова, 0. В. Земляніщина. Харків, 1996. 64 с.
16. Чернівецький національний університет імені Юрія Федьковича в незалежній Україні: бібліогр. покажи. / уклад. : Н. М. Загородна та ін.; наук. ред. Т. В. Марусик ; відп. за вип. М. Б. Зушман. Чернівці : Чернівецький національний університет, 2015. 512 с. (До 140-річчя від дня заснування).
17. Гетьман А. П. Екологічна політика держави: конституцшно-правовии аспект. Тридцать лет с зкологическим правом : избранньїе труди. Харьков, 2013. С. 205-212.
18. Епик Е. А. Гендерньій аспект оценочньїх сентенций. Сучасні проблеми та перспективи дослідження романських і германських мов і літератур : зб. тез. конф. Донецьк : ДонНУ, 2004. С. 125-127.
19. Корнилова Е. Н. Французская литература : справ.- библиогр. указ. Н. Новгород : МКУК ЦБС Московскош района : ЦРБ им. Пушкина, 2015. С. 54—55.
20. Круковський В. І. Концепти суб’єктивність / об’єктивність, модалізація / модальність та засоби їх вираження в мові та мовленні: питання теорії (на матеріалі французької мови). Філологія. Педагогіка. Психологія : наук. вісн. каф. ЮНЕСКО КНЛУ. гол. ред.
21. Круковський В. І. Концепт, термін, дефініція і спеціалізований дискурс. Проблеми семантики, прагматики та когнітивної лінгвістики : зб. наук. пр. Вип. 24. Київ : Логос, 2013. С. 188-199.
22. Глазова О. П. Вивчення неологізмів. 2013. URL :http://elibrary.kubg.edu.ua/ 26/1 /O_Glazova _ 10_IP.pdf (дата звернення: 11.09.2022).
23. Bolhken B. The Idiom Experience. ETC. : A Review of General Semantics. Vol. 53, N0. 2, 2006. URL: https://www.questia.com/library/journal/1G1 - 19726532/the- idioms-experience (дата звернення 07.08.2022).

ДЛЯ НОТАТОК

Навчально-методичне видання

МОНІТОРИНГ ТА АУДИТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Методичні вказівки
до виконання практичних робіт
для студентів спеціальностей
125 «Кібербезпека»

Укладачі: **Хлапонін** Юрій Іванович
Сєлюков Олександр Васильович

Комп'ютерне верстання *М.М. Власенко*

Підписано до друку 05.05.2022 Формат 60 х 84 1/ 16
Ум. друк. арк. 2,79. Обл.-вид. арк. 1,12.
Електронний документ. Вид № 59/ІІІ-17.

Видавець і виготовлювач
Київський національний університет будівництва і архітектури

Повітрофлотський проспект, 31, Київ, Україна, 03680
Свідоцтво про внесення до Державного реєстру суб'єктів
видавничої справи ДК № 808 від 13.02.2002 р.