МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
Кафедра кібербезпеки та DATA-технологій, факультет №6

МЕТОДИЧНІ МАТЕРІАЛИ

ДО ПРАКТИЧНИХ ЗАНЯТЬ

навчальної дисципліни «**Моніторинг та аудит кібербезпеки**»
обов'язкових компонент
освітньої програми другого (магістр) рівня вищої освіти

125 «Кібербезпека» (безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 22.12.2023 № 11

СХВАЛЕНО
Вченою радою факультету № 6
Протокол від 20.12.2023 № 11

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 21.12.2023 № 11

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій факультету № 6 *(протокол від 15.12.2023 №12)*

Розробник:
Доцент кафедри, к. т. н., доцент Хавіна І.П.

Рецензенти:
1. *Професор кафедри комп'ютерних наук та інформаційних технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» д. т. н., професор Малєєва О. В.*

2. *Професор кафедри інформаційних технологій та кібербезпеки ХНУВС, к.т.н., доцент Носов В. В.*

1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		Лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2							
Тема № 1. Аудит інформаційної безпеки	**16**	**2**		**4**		**10**	
Тема № 2. Внутрішній аудит СМІБ за вимогами ISO/IEC 27001 ТА ISO 19011	**18**	**4**		**4**		**10**	
Тема № 3. Комплексний аудит інформаційної безпеки	**20**	**4**		**6**		**10**	
Тема № 4. Менеджмент інцидентів інформаційної безпеки.	**20**	**4**		**6**		**10**	
Тема № 5. Функціонування груп реагування на інциденти інформаційної безпеки CERT/CSIRT.	**16**	**2**		**4**		**10**	
Всього по дисципліні	**90**	**16**		**24**		**50**	**Іспит**

2. Методичні вказівки до практичних занять

Практична робота № 1

Тема: Безпека у Windows.

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

Кількість годин: 4 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

Вступ.

1. Вивчення законодавчих вимог, методів та програмного додатку для реєстрації, зберігання та аналізу подій безпеки на базі ОС Windows.

- 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.

Література:

1. Матеріали лекції 1.
[1, с. 8 – 12, 16 - 19]
2. Нормативні документи [1].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

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

Стислі 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).

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. 1. Титульний лист.

2. Виконане 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.

Контрольні 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?

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна література

1. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.
2. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.
3. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. 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.

Допоміжна література

1. Метод формування параметрів функціональних обов'язків для оцінки загроз в соціотехнічних системах/ А. Корченко, С. Мацюк, О. Чобаль, О. Кручінін, Т. Паращук// Information Technology: Computer Science, Software Engineering and Cyber Security. – 2022. – №3. – С. 19-26.
2. Кількісна оцінка кіберзахищеності інформації / В. Хорошко Ю. Хохлачова, Н. Вишневська, О. Чобаль// Захист інформації. – 2023. – Т.25 (№2). – С. 70-76.
3. Стандарти систем управління ІБ серії ISO/IEC 27000. [Електронний ресурс]. Режим доступу: https://www.iso27001security.com/

Інформаційні ресурси в мережі Інтернет

1. https://www.netacad.com/
2. https://www.splunk.com/
3. https://portal.rangeforce.com/

Практична 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.

Кількість годин: 4 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

Вступ.

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

Література:

3. Матеріали лекції 2.

[1, с. 8 – 12, 16 - 19]

4. Нормативні документи [1].

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

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

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).

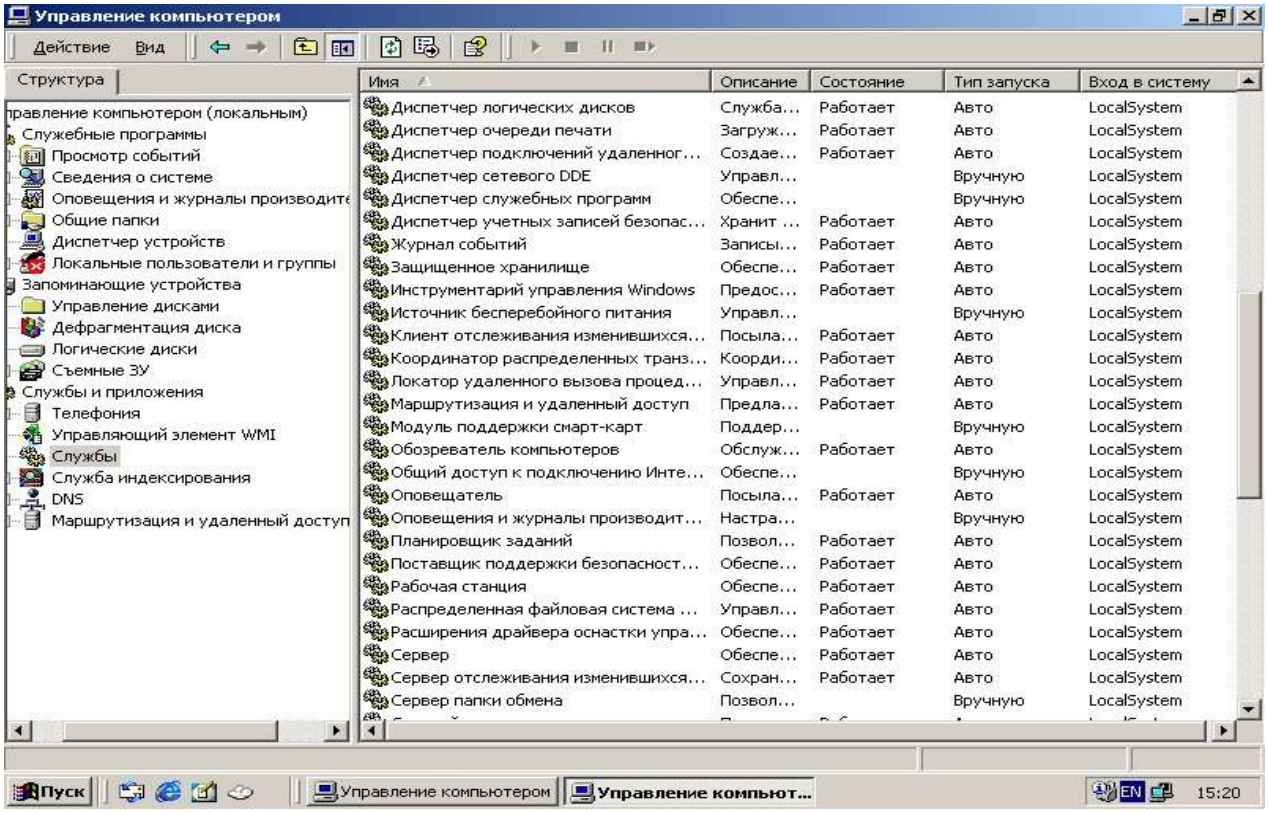

Рисунок 2.2. Виклик вікна «Службы»

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 сервері бази 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».**

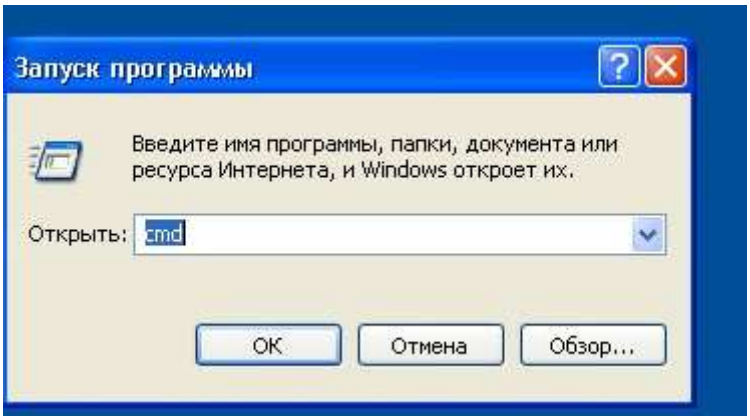

Рисунок 2.3. Запуск команди «**cmd»**

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

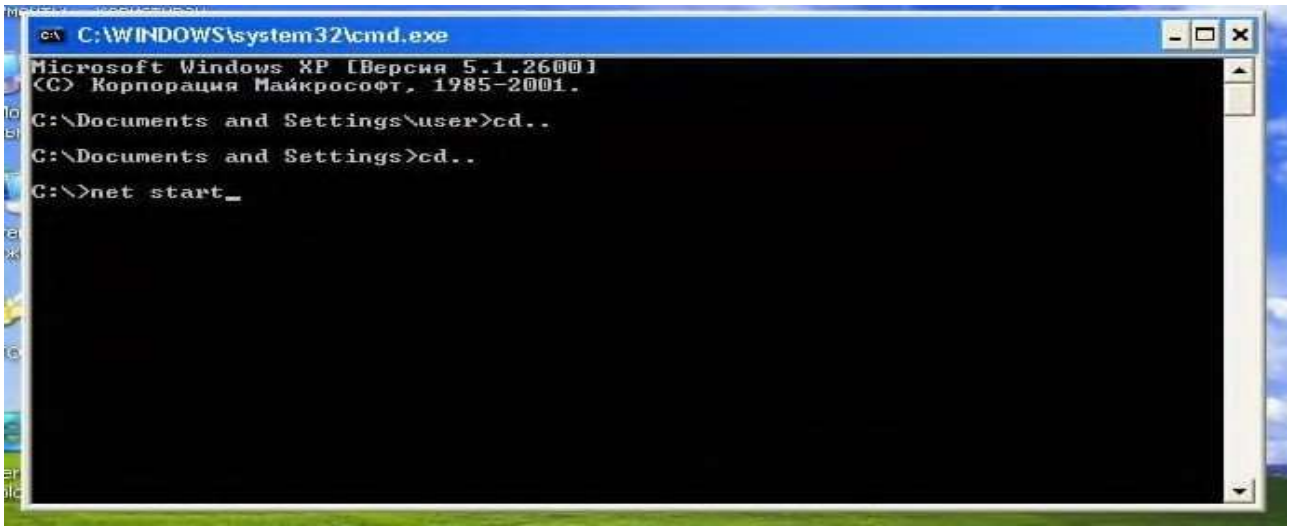

Рисунок 2.4. Запуск команди **«net start»**

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

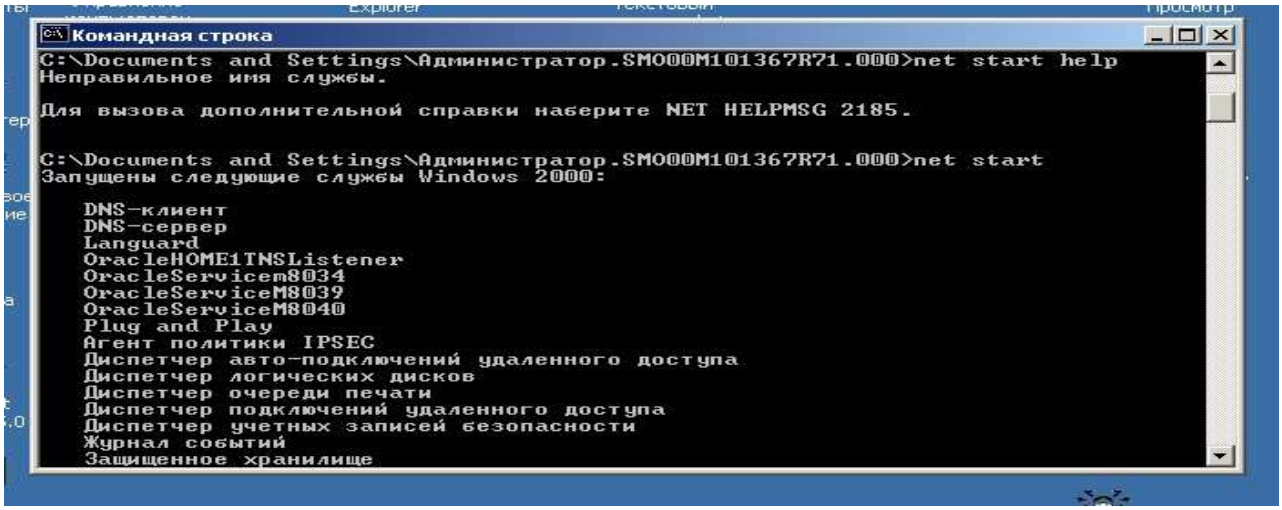

Рисунок 2.5. Вікно перегляду служб, що завантажені

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).

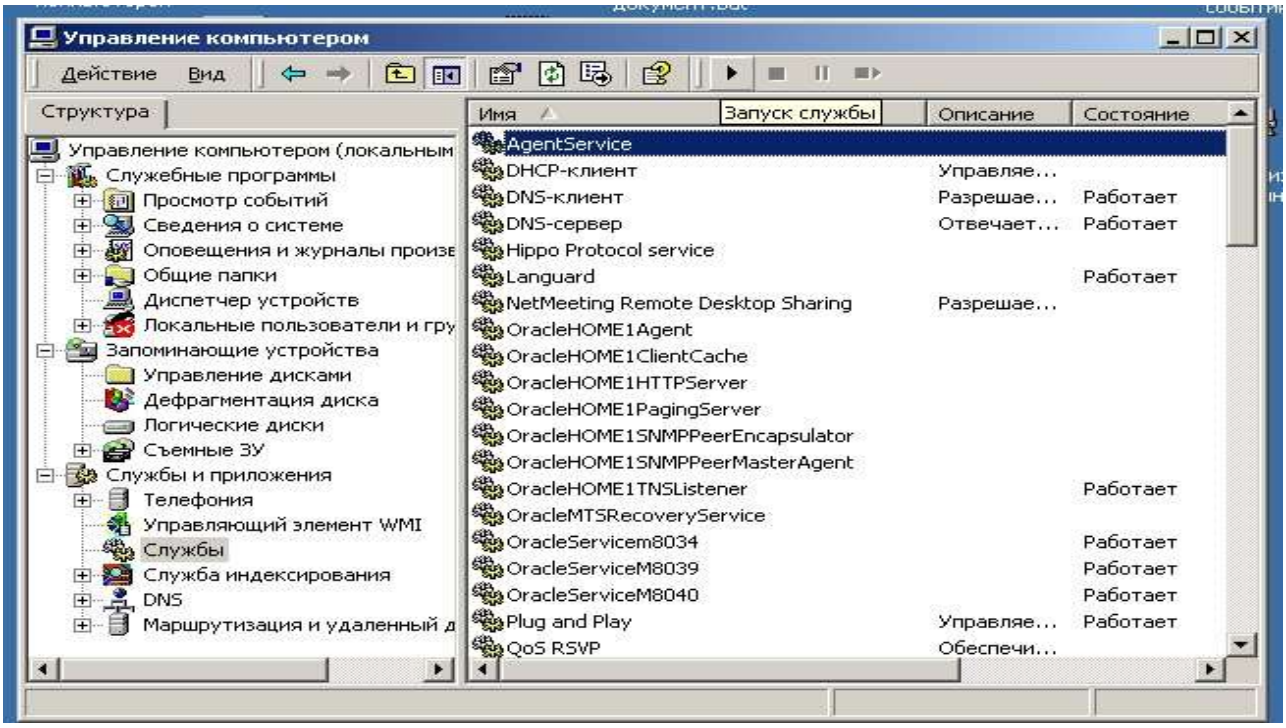

Рисунок 2.6. Порядок запуску служби

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

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

Послідовно на комп’ютері 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.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.

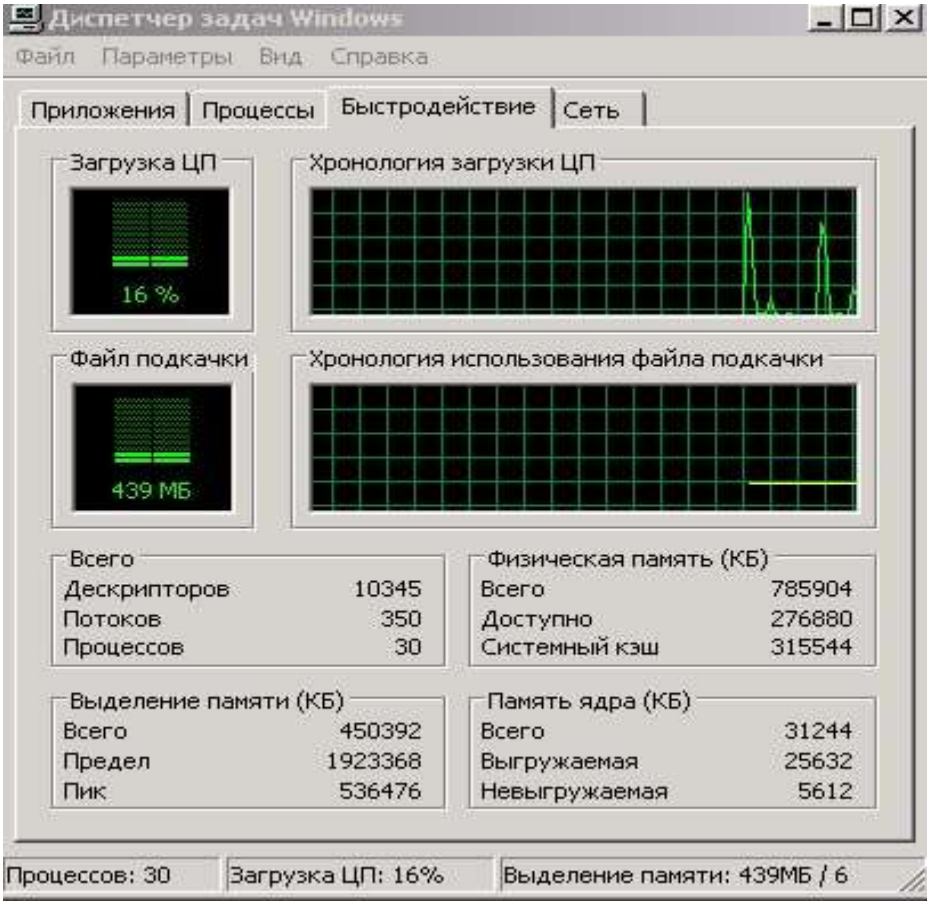

Рис.2.7. Від вікна Диспетчера задач Windows

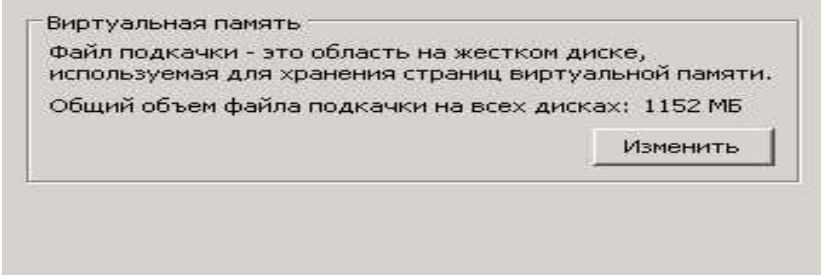

Рисунок 2.8. Визначення розміру файлу підкачки ОС Windows

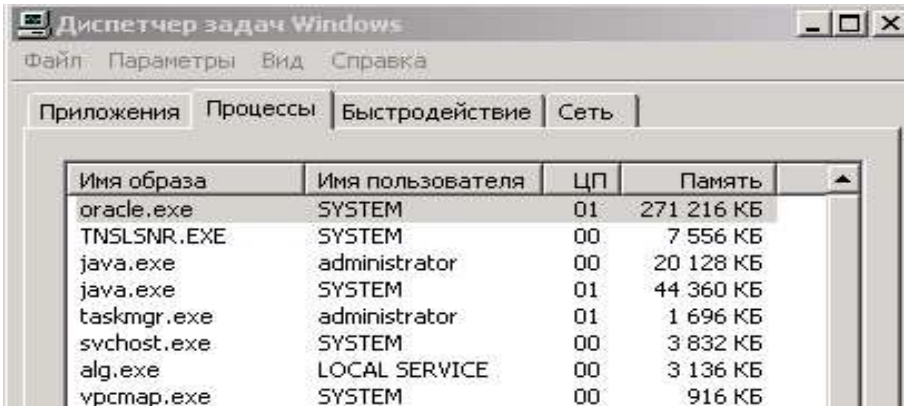

Рисунок 2.9. Від вікна щодо запущених процесів ОС Windows

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).

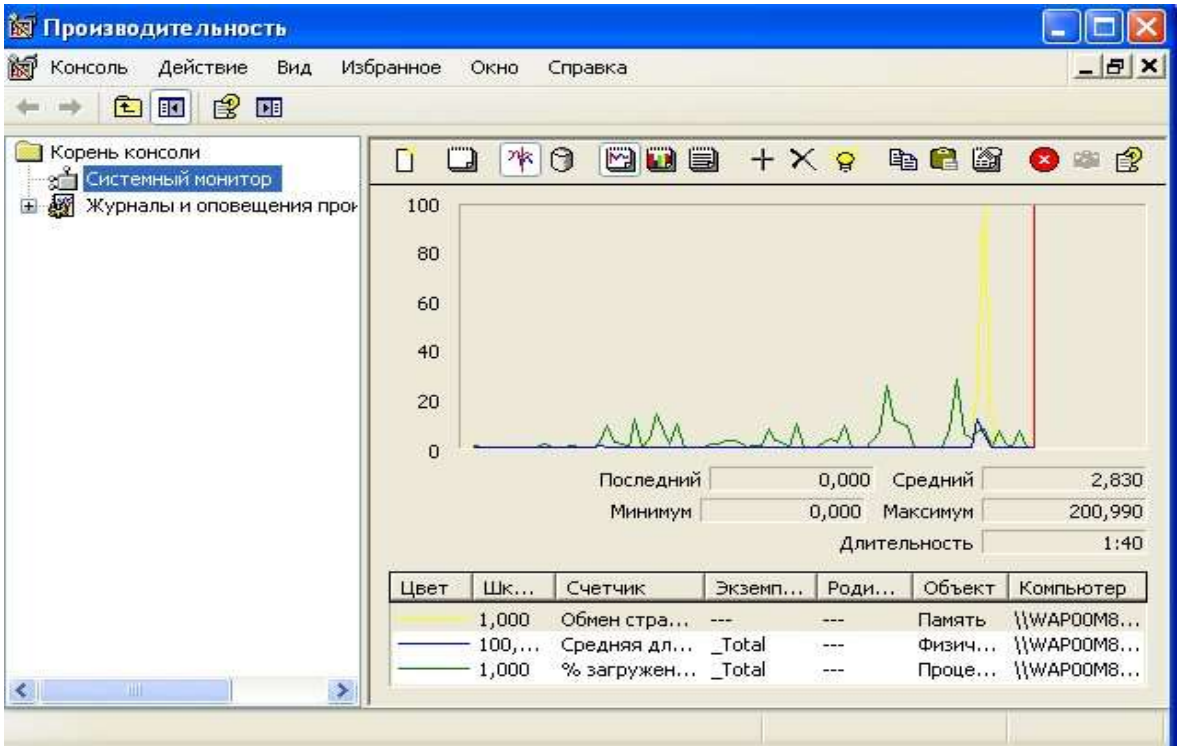

Рисунок 2.10. Активізація розділу **«Системный монитор»**

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).

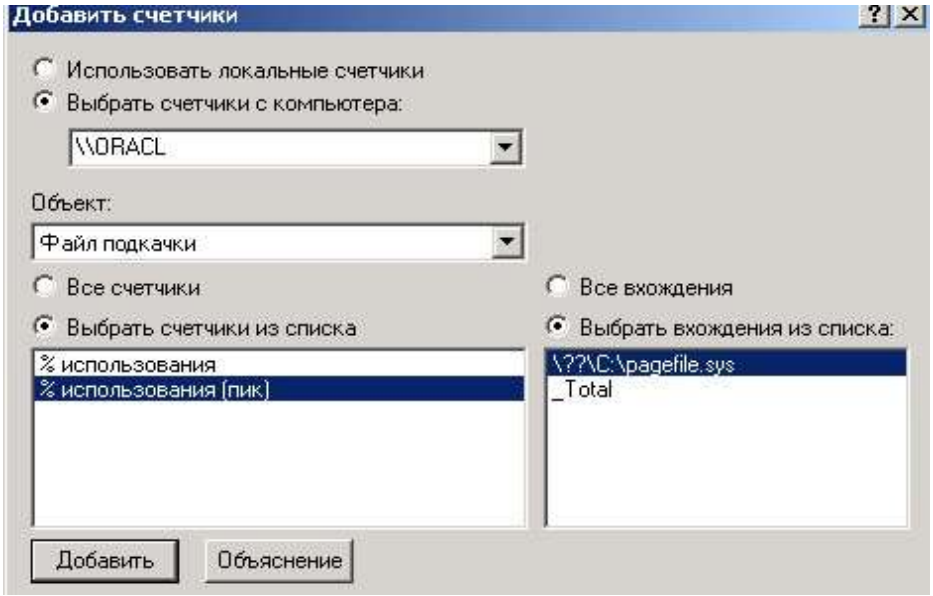

Рисунок 2.11. Вибір лічильник**а «% использования»**

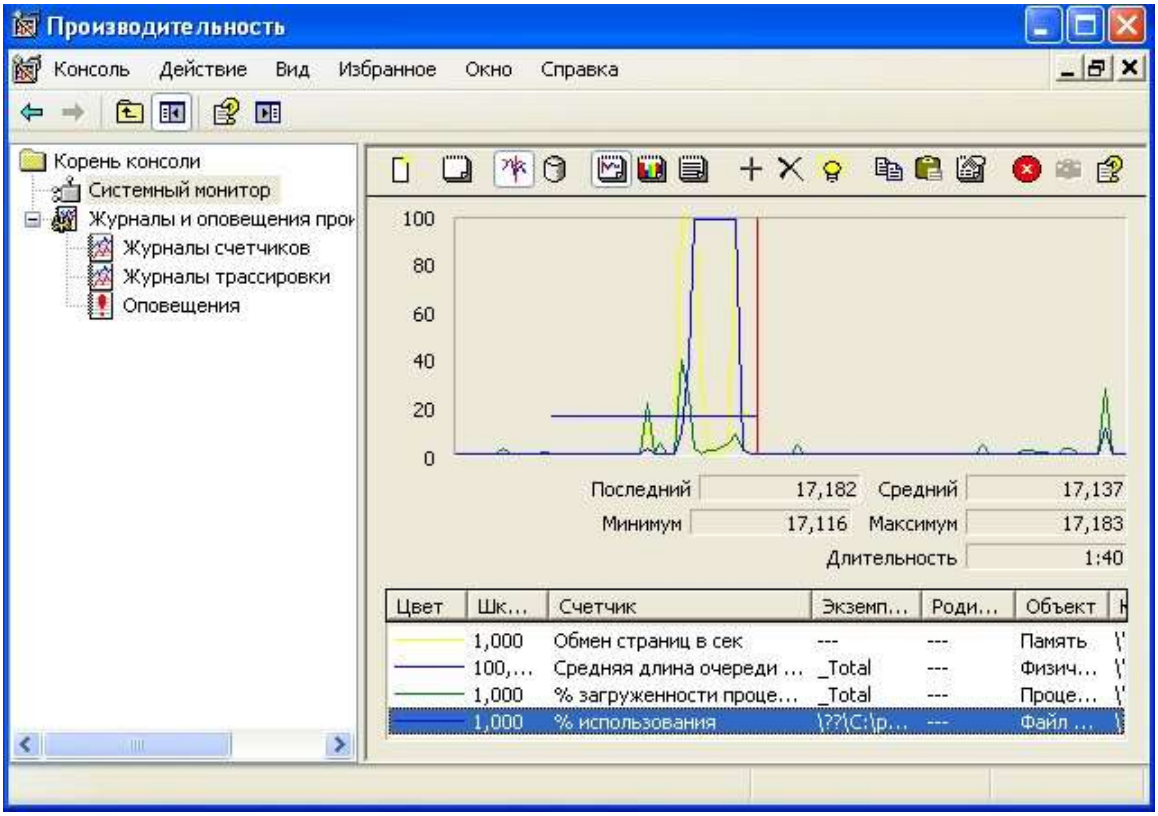

Рисунок 2.12. Активізація лічильника **«% использования»**

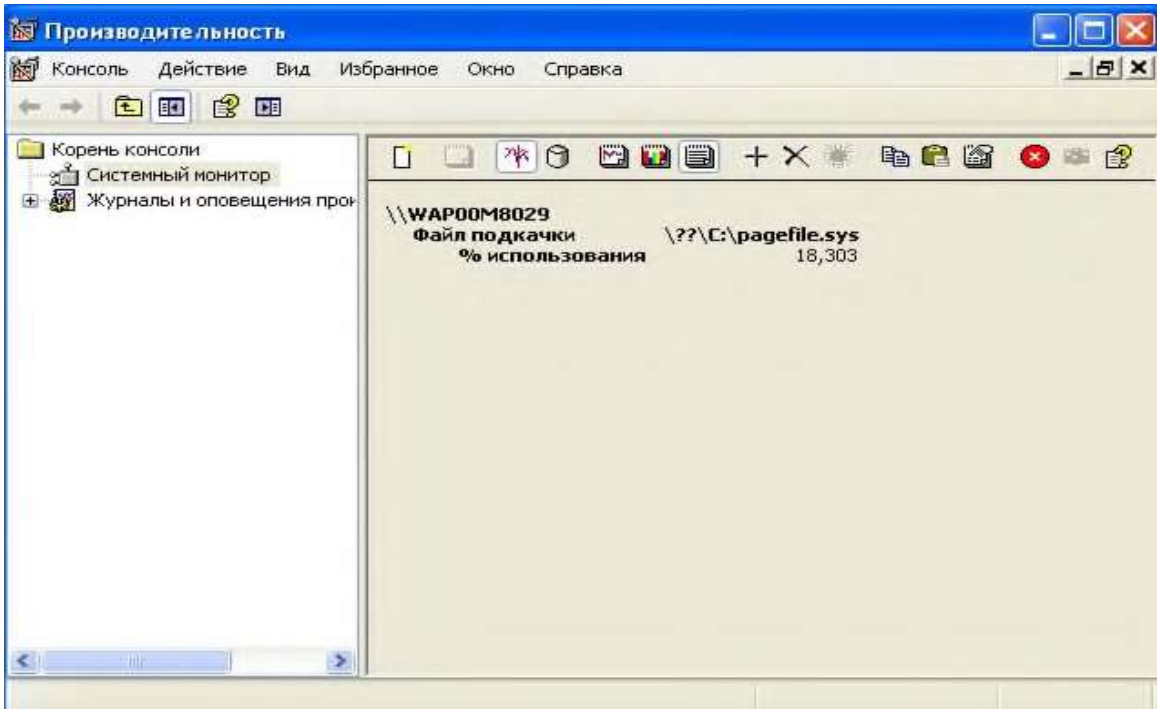

Рисунок 2.13. Перегляд звіту

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

Контрольні питання

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

4.Охарактеризуйте технології міжмережевих екранів.

3.Назвіть основні характеристики приватних мереж.

4. Яка залежність вразливості та атаки?

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна література

4. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.
5. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.
6. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. 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.

Допоміжна література

4. Метод формування параметрів функціональних обов'язків для оцінки загроз в соціотехнічних системах/ А. Корченко, С. Мацюк, О. Чобаль, О. Кручінін, Т. Паращук// Information Technology: Computer Science, Software Engineering and Cyber Security. – 2022. – №3. – С. 19-26.
5. Кількісна оцінка кіберзахищеності інформації / В. Хорошко Ю. Хохлачова, Н. Вишневська, О. Чобаль// Захист інформації. – 2023. – Т.25 (№2). – С. 70-76.
6. Стандарти систем управління ІБ серії ISO/IEC 27000. [Електронний ресурс]. Режим доступу: https://www.iso27001security.com/

Інформаційні ресурси в мережі Інтернет

4. https://www.netacad.com/
5. https://www.splunk.com/
6. https://portal.rangeforce.com/

Практична 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.

Кількість годин: 4 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

Вступ.

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

Література:

1.Матеріали лекції 3.
[3, с. 8 – 12, 16 - 19]
2. Нормативні документи.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

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 кожний процес окремо (рис.3.1).

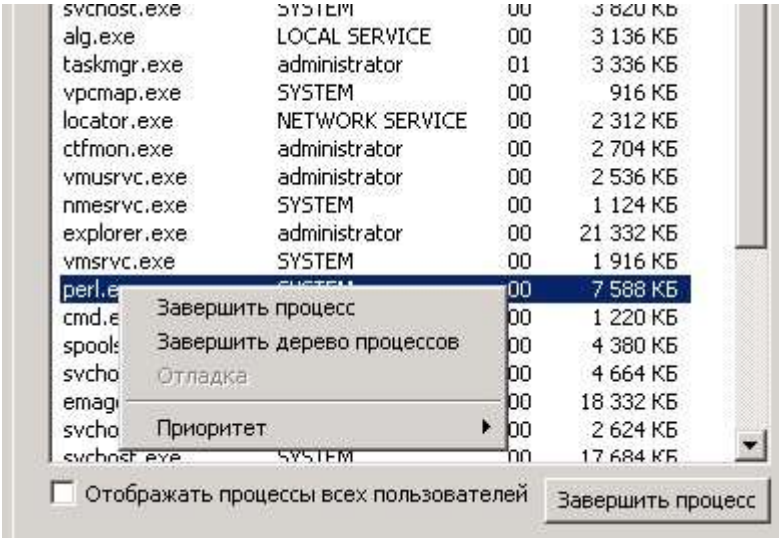

Рис.3.1. Відключення процесів, що заважають роботі ОС

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, що з'явиться набрати команду **msconfig.exe** (рис.2). У вікні, що з'явиться активізувати закладку **«Атозагрузка»** (рис.3.2).

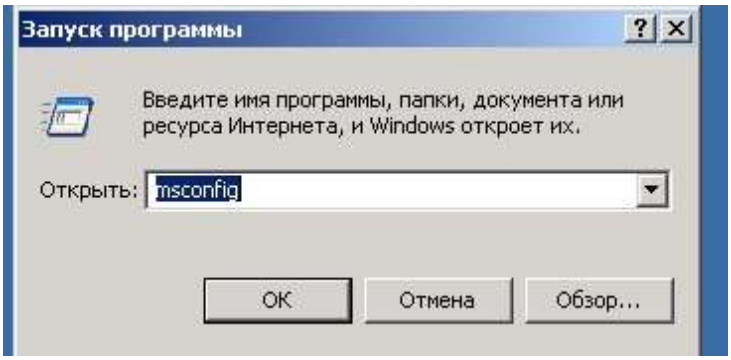

Рисунок 3.2. Запуск команди **msconfig.exe**

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.

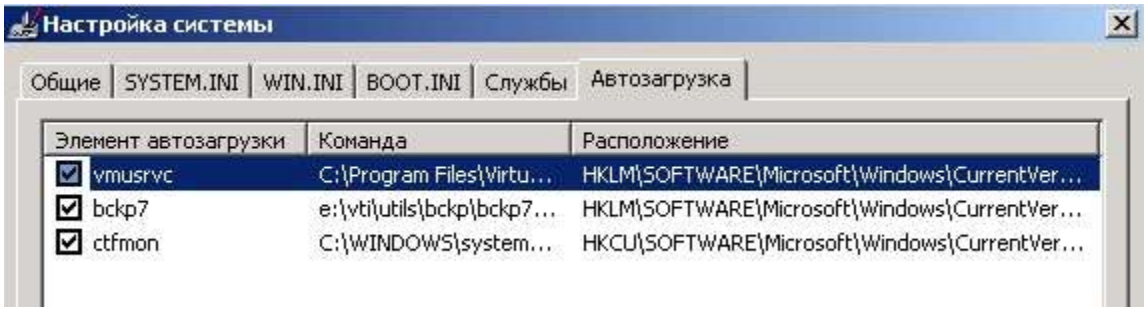

Рисунок 3.3. Відключення автозавантаження програм ОС

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: Commit Limit	Величина, яка визначає кількість віртуальної пам’яті система може надати без збільшення розміру файлу підкачки		
Process: % Processor Time	Ступень використання процесора заданим процесом		

Контрольні питання

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

6.Охарактеризуйте технології міжмережевих екранів.

3.Назвіть основні характеристики приватних мереж.

4. Яка залежність вразливості та атаки?

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна література

7. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.
8. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.
9. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. 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.

Допоміжна література

7. Метод формування параметрів функціональних обов'язків для оцінки загроз в соціотехнічних системах/ А. Корченко, С. Мацюк, О. Чобаль, О. Кручінін, Т. Паращук// Information Technology: Computer Science, Software Engineering and Cyber Security. – 2022. – №3. – С. 19-26.
8. Кількісна оцінка кіберзахищеності інформації / В. Хорошко Ю. Хохлачова, Н. Вишневська, О. Чобаль// Захист інформації. – 2023. – Т.25 (№2). – С. 70-76.
9. Стандарти систем управління ІБ серії ISO/IEC 27000. [Електронний ресурс]. Режим доступу: https://www.iso27001security.com/

Інформаційні ресурси в мережі Інтернет

7. https://www.netacad.com/
8. https://www.splunk.com/
9. https://portal.rangeforce.com/

Практична робота № 4

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

Метою заняття 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.

Кількість годин: 4 год.

Місце проведення: комп'ютерний клас.

Навчальні питання:

Вступ.

1. Перевірку інформації, яка надається для завантаження на ПЕОМ сервер, щодо наявності комп'ютерних вірусів.
2. Здійснення оновлення антивірусних баз.

Література:

1. [4, с. 8 – 12, 16 - 19]

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

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 ВАШОГО антивірусного програмного забезпечення .

.

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 просканові	Тривалість виконання операцій	Назва носія інформації, що перевірявся	База даних сигнатур	Версія бази даних сигнатур	Наявність загрози

Контрольні питання

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

8.Охарактеризуйте технології міжмережевих екранів.

3.Назвіть основні характеристики приватних мереж.

4. Яка залежність вразливості та атаки?

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна література

10. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.
11. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.
12. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. 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.

Допоміжна література

10. Метод формування параметрів функціональних обов'язків для оцінки загроз в соціотехнічних системах/ А. Корченко, С. Мацюк, О. Чобаль, О. Кручінін, Т. Паращук// Information Technology: Computer Science, Software Engineering and Cyber Security. – 2022. – №3. – С. 19-26.
11. Кількісна оцінка кіберзахищеності інформації / В. Хорошко Ю. Хохлачова, Н. Вишневська, О. Чобаль// Захист інформації. – 2023. – Т.25 (№2). – С. 70-76.
12. Стандарти систем управління ІБ серії ISO/IEC 27000. [Електронний ресурс]. Режим доступу: https://www.iso27001security.com/

Інформаційні ресурси в мережі Інтернет

10. https://www.netacad.com/
11. https://www.splunk.com/
12. https://portal.rangeforce.com/

Практична 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.

Кількість годин: 4 год.
Місце проведення: комп'ютерний клас.

Навчальні питання:

Вступ.

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

Література:

1. Матеріали лекції 5.
[3, с. 8 – 12, 16 - 19]

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Зробити огляд завдання і визначити порядок його виконання. Надати посилання на відповідні презентації.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору. У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ХІД РОБОТИ

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»**, у вікні, що з'явиться, вибрати **«Просмотр событий»** та відповідний журнал подій:

на ПЕОМ користувачів (рис.5.1):

- додатків; - системи.

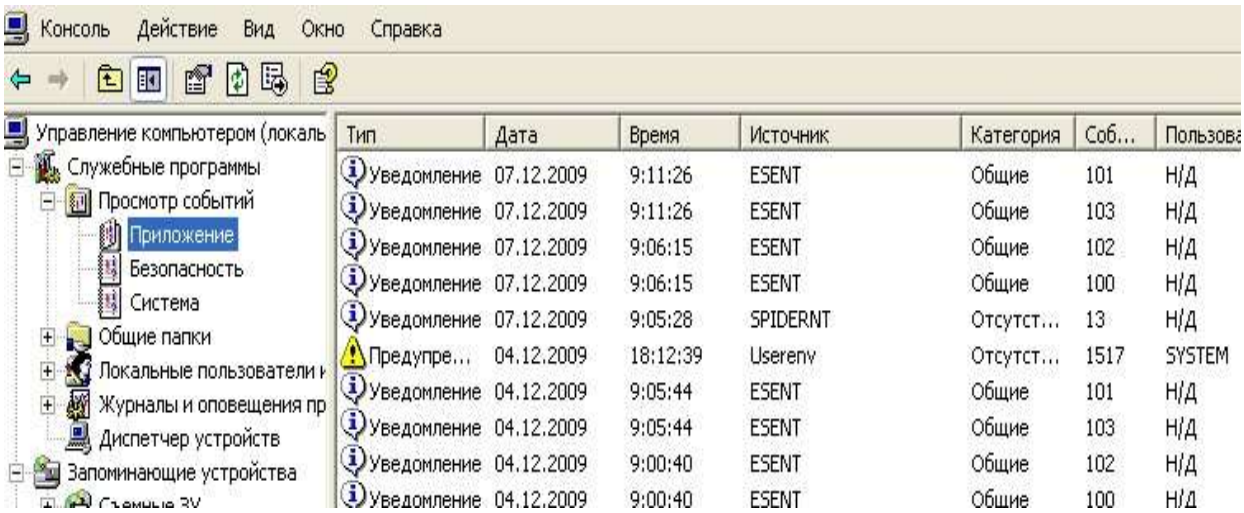

Рисунок 5.1. Вигляд вікна перегляду журналів подій на ПЕОМ

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).

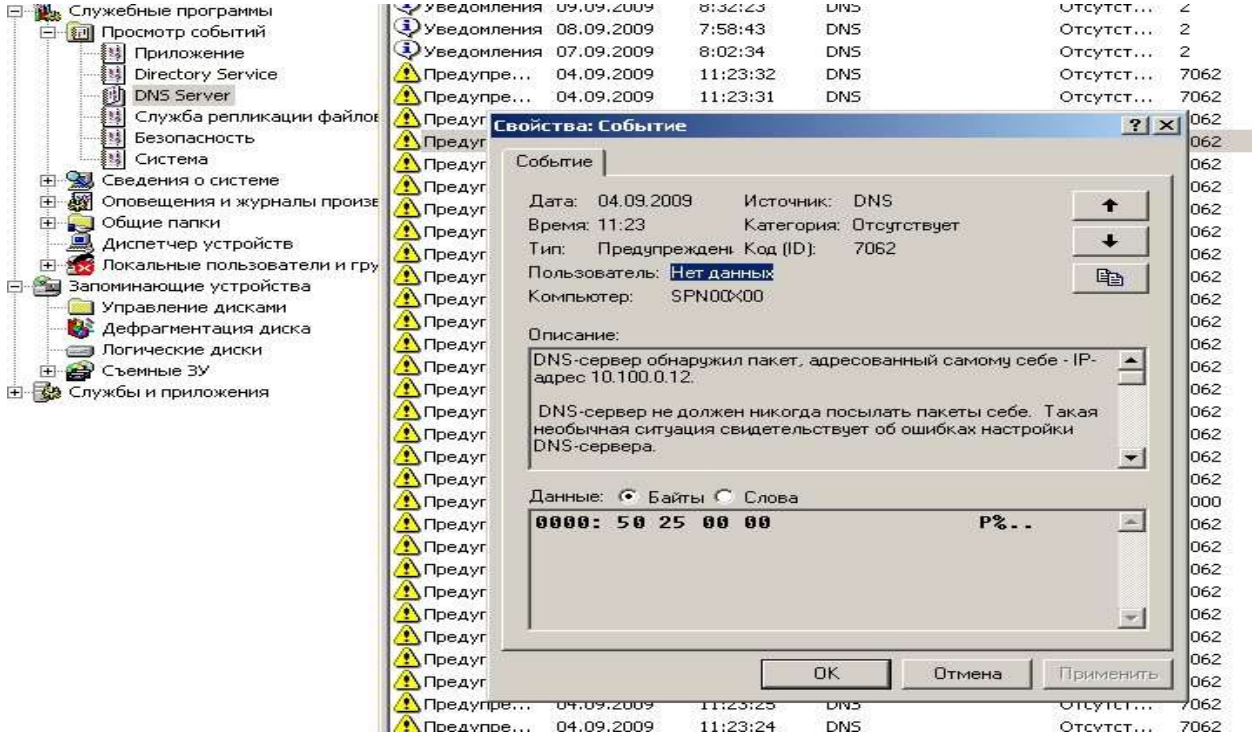

Рисунок 5.2. Перегляд вмісту події за допомогою журналу **DNS Server**

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).

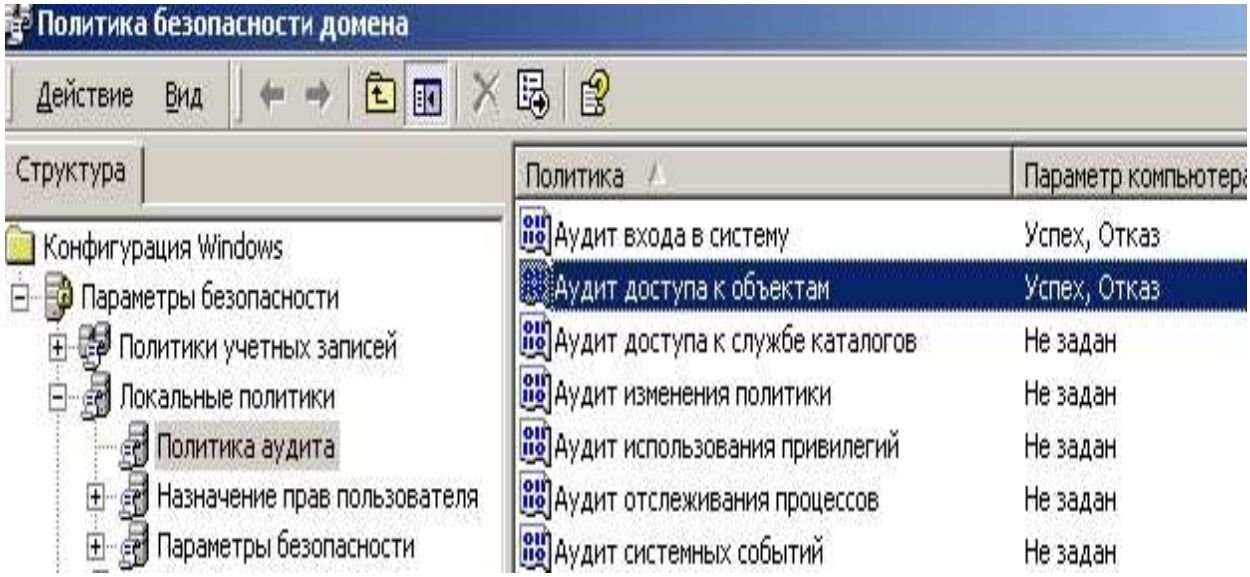

Рисунок 5.3. Перевірка налаштувань політик аудиту на сервері навчального класу

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).

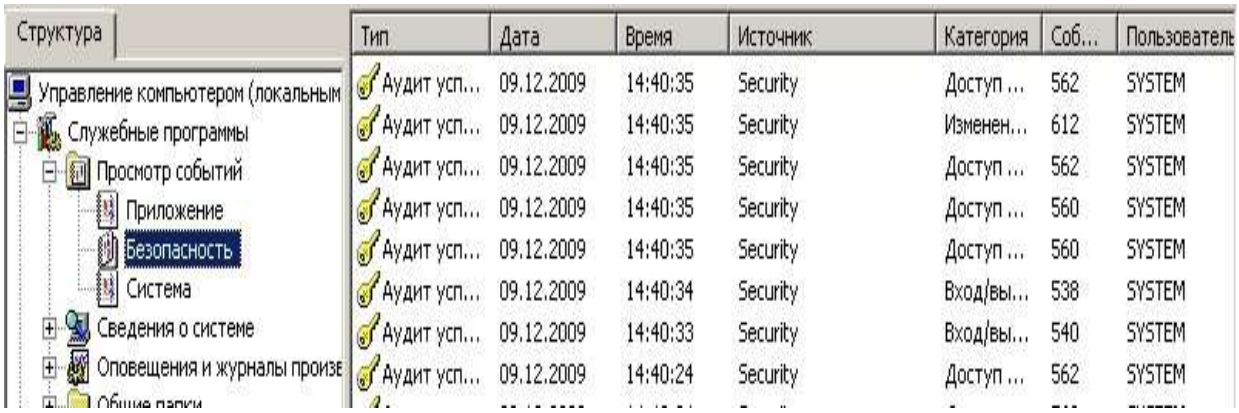

Рисунок 5.4. Перегляд типу подій в журналі безпеки ОС

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 та контролю

№ 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).

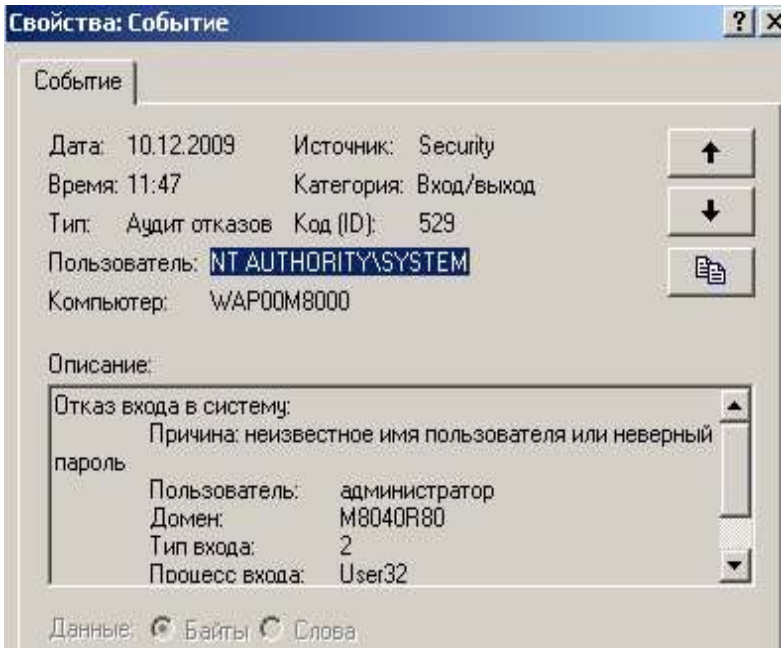

Рисунок 5.6. Перегляд події в журналі безпеки щодо спроби несанкціонованого доступу на ПЕОМ користувача

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.

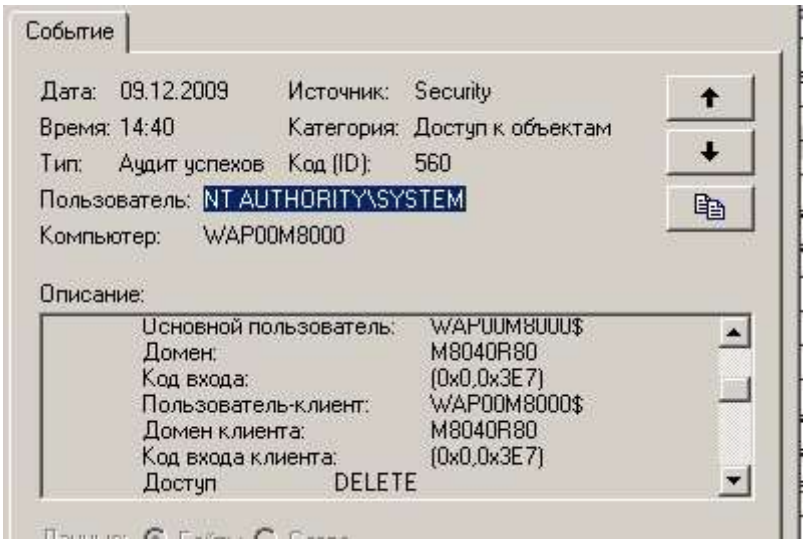

Рисунок 5.7. Перегляд події в журналі безпеки щодо доступу до прикладного програмного забезпечення АРМ користувача

5.3. Перевірка налаштувань журналів подій та безпеки ОС на ПЕОМ

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

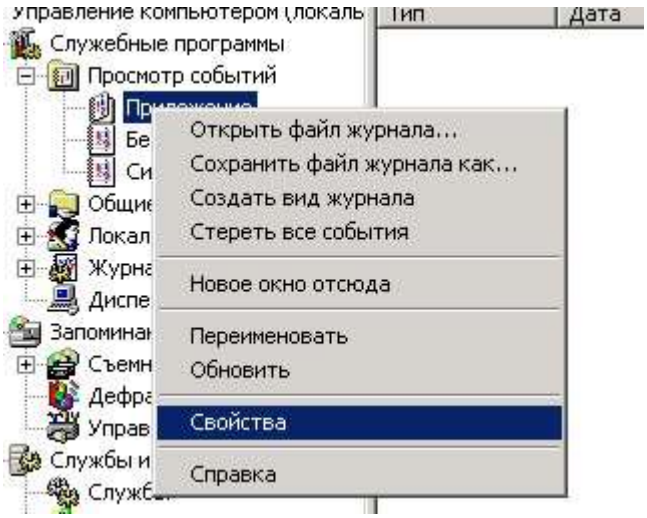

Рисунок 5.8. Вибір вікна властивостей журналу подій

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).

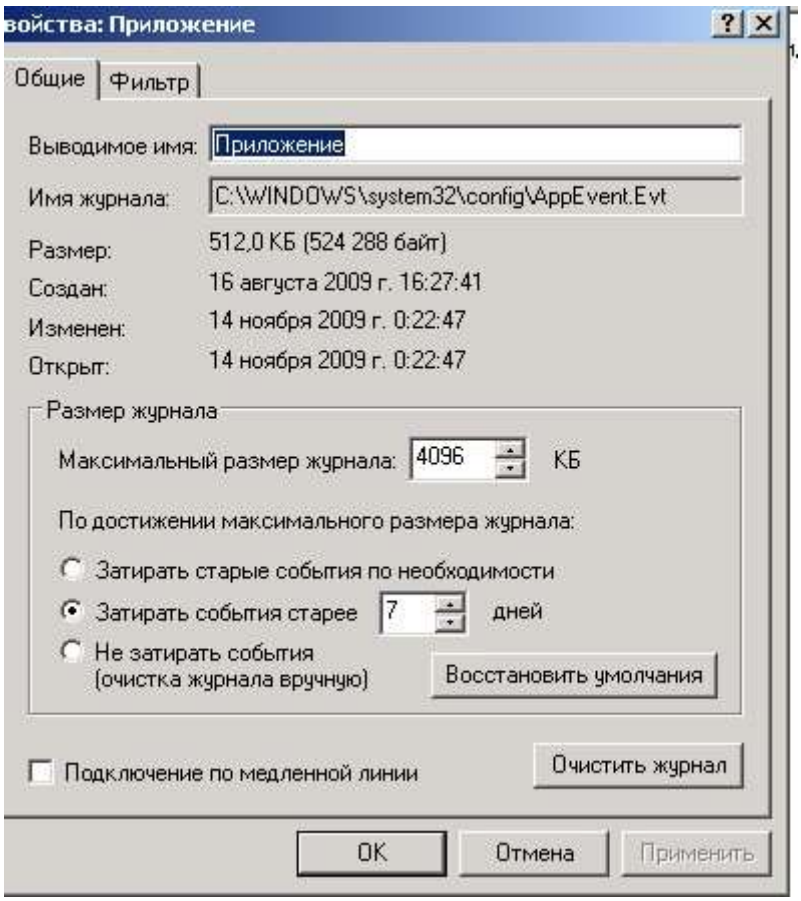

Рисунок 5.9. Від вікна налаштувань журналу повідомлень ОС

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

Контрольні питання

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

10. Охарактеризуйте технології міжмережевих екранів.

3.Назвіть основні характеристики приватних мереж.

4. Яка залежність вразливості та атаки?

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, додаткова), інформаційні та навчальні ресурси в Інтернеті

Основна література

13. Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки // О.Г. Корченко, С.О. Гнатюк, С.В. Казмірчук, В.М. Панченко, С.В. Мельник. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 193 с.
14. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. – 408 с.
15. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. 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.

Допоміжна література

13. Метод формування параметрів функціональних обов'язків для оцінки загроз в соціотехнічних системах/ А. Корченко, С. Мацюк, О. Чобаль, О. Кручінін, Т. Паращук// Information Technology: Computer Science, Software Engineering and Cyber Security. – 2022. – №3. – С. 19-26.
14. Кількісна оцінка кіберзахищеності інформації / В. Хорошко Ю. Хохлачова, Н. Вишневська, О. Чобаль// Захист інформації. – 2023. – Т.25 (№2). – С. 70-76.
15. Стандарти систем управління ІБ серії ISO/IEC 27000. [Електронний ресурс]. Режим доступу: https://www.iso27001security.com/

Інформаційні ресурси в мережі Інтернет

13. https://www.netacad.com/
14. https://www.splunk.com/
15. https://portal.rangeforce.com/