# МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Національний університет “Львівська політехніка”**



**Інститут післядипломної освіти**

**ЗВІТ**

**Про виконання лабораторної роботи №4**

**«АУДИТ І НАЛАШТУВАННЯ БЕЗПЕКИ У WINDOWS 7»**

**з дисципліни «Основи системного адміністрування»**

Виконав:

слухач групи ПЗС-11

Гринчук Тарас

Прийняв:

доц. Яковина В.С.

« »\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 р.

∑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

ЛЬВІВ – 2014

**Мета роботи**: Ознайомлення зі структурою, принципом роботи та налаштуванням об’єкта групової політики на локальному комп’ютері під управлінням ОС Windows 7. Навчитись використовувати та створювати шаблони безпеки для ефективного налаштування та аналізу типових параметрів безпеки.

## 1. Хід роботи

1. Відкрити оснастку mmc "Групповая политика". Перейти в гілку "Политика аудита", включити аудит доступу до об’єктів. Після цього у властивостях безпеки об’єкту, за яким повинно проводитись спостереження (папки чи файлу), перейти у вкладку "Аудит" та увімкнути аудит для визначених суб’єктів безпеки та їх активності (наприклад видалення). (Переконатись, що без налаштування аудиту на об’єкті файлової системи записів в журнал не відбувається – п. 2.) Виконати умови аудиту (тобто дії над цим об’єктом та тим користувачем для яких налаштовано аудит).

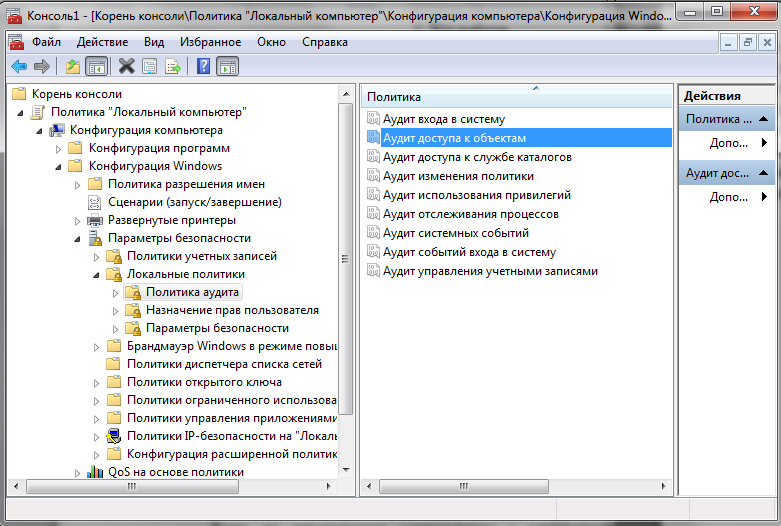


Рис. 1. Гілка політики аудиту в об’єкті групової політики

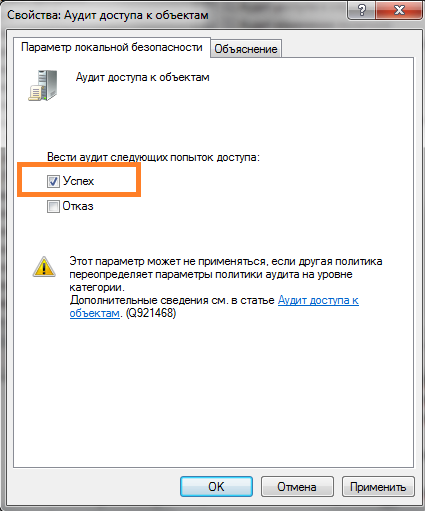


Рис. 2. Включення політики аудиту

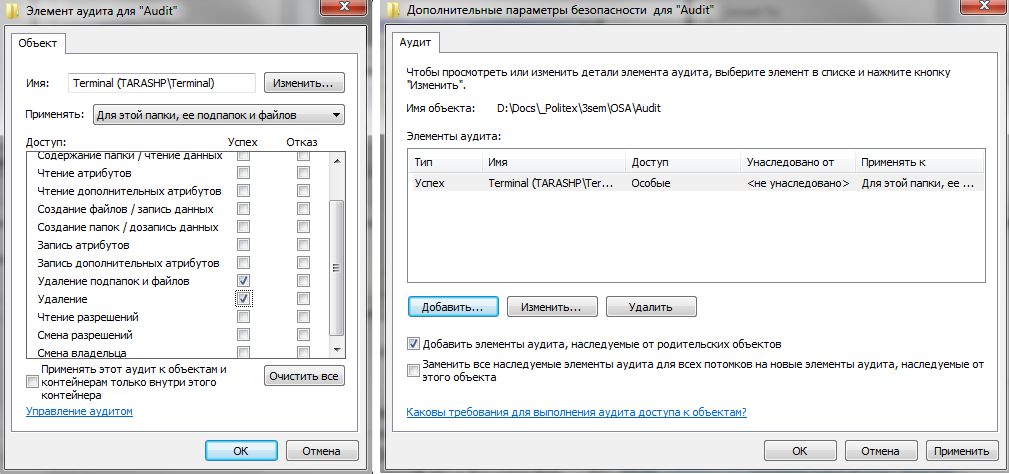


Рис. 3. Налаштування аудиту доступу до об’єктів на об’єктах файлової

системи

1. Відкрити оснастку mmc "Просмотр событий" та журнал "Безопасность" в ній. Знайти в журналі записи категорії "Доступ к объектам" та записи про дію, яку контролювалося. (Додаткові відомості про подію за номером її коду (ID) можна знайти на сайті Microsoft або в Resource Kit).

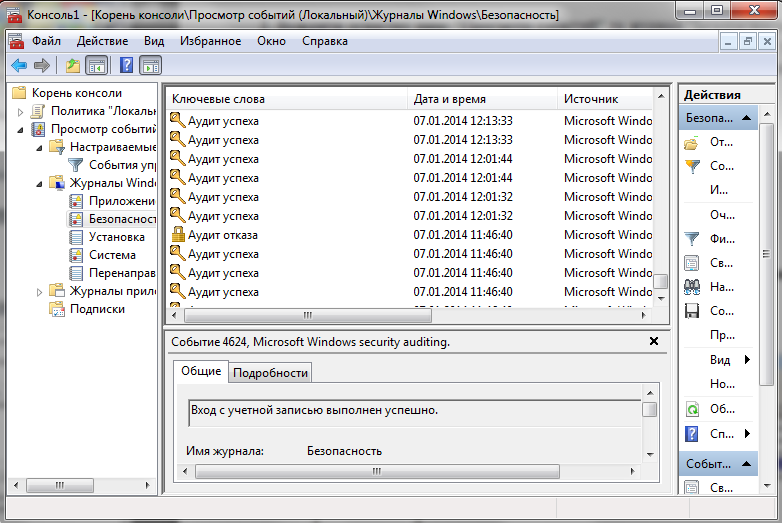


Рис. 4. Записи про події аудиту в журналі безпеки.

1. В політиках аудиту увімкнути аудит зміни політики та системних подій. Виконати умови аудиту (наприклад змінити системний час). В журналі безпеки відстежити записи про ці події. Увімкнути аудит управління обліковими записами користувачів; відключити обліковий запис існуючого користувача, створити нового користувача, задати пароль користувачу. В журналі безпеки відстежити записи про ці події. Увімкнути аудит входу в систему; вийти зі системи та зайти під іншим користувачем. В журналі безпеки знайти записи категорії "Вход/Выход" та відстежити записи про ці події.

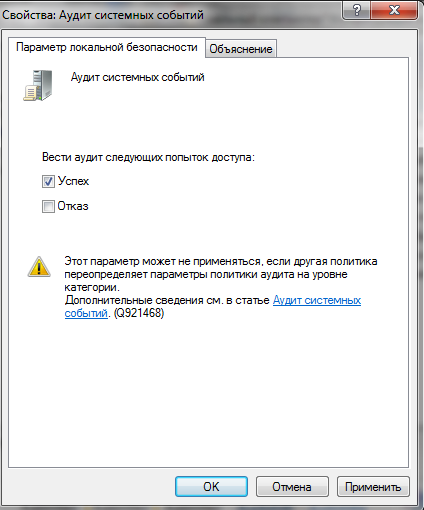


Рис. 5. Включення аудиту системних подій

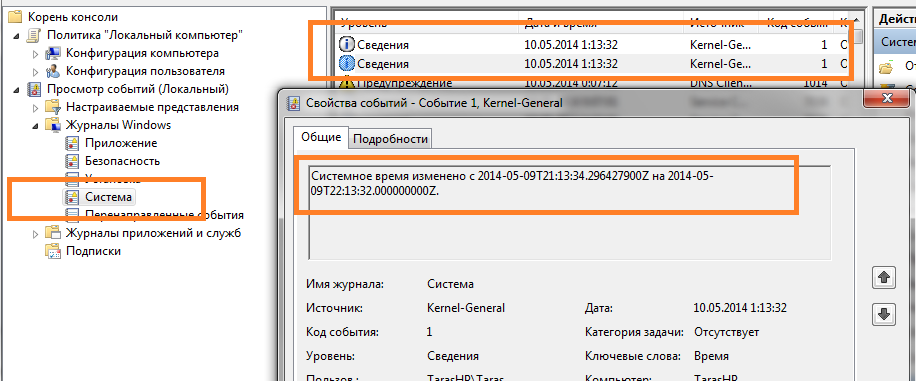


Рис. 6. Відстежуємо зміну системного часу

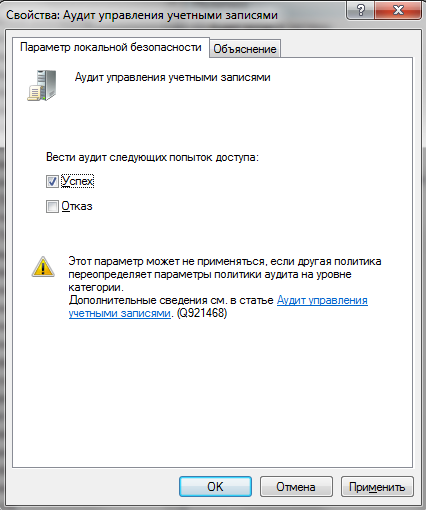
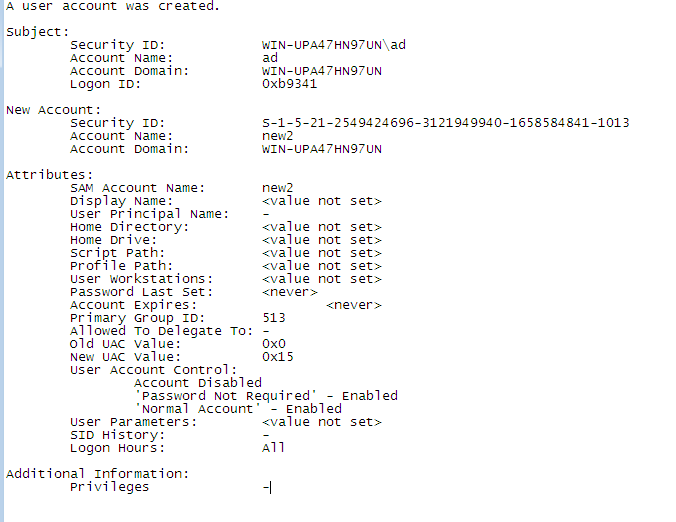
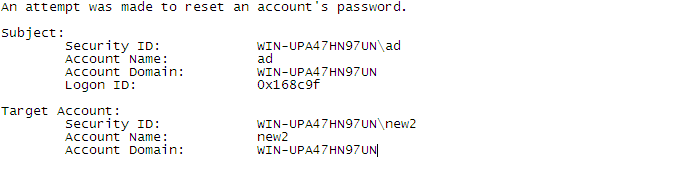


Рис. 7. Вмикаємо аудит управління обліковими записами користувачів.

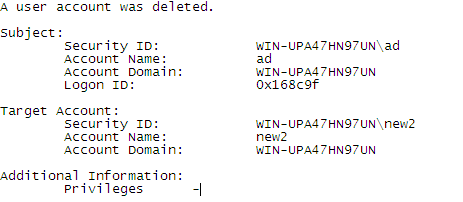
Після створення нового користувача в журналі буде запис:



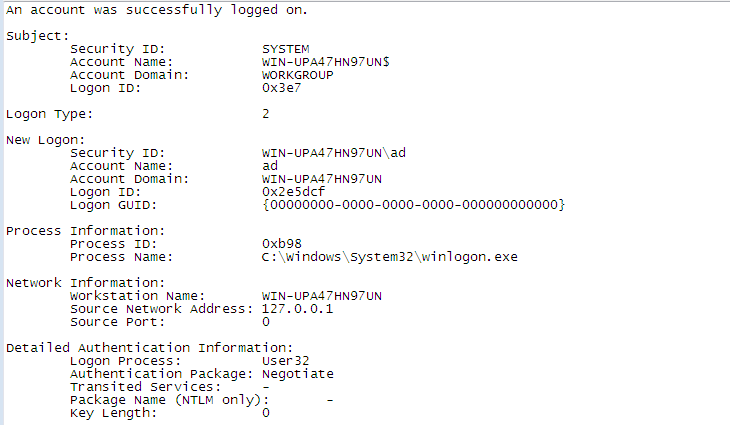
Після зміни паролю обліковому запису new2 в журналі отримуємо такий запис:



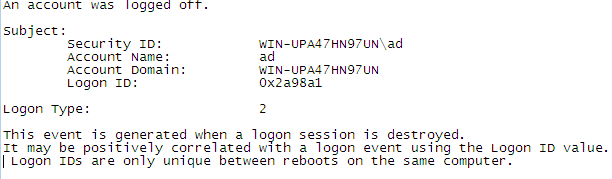
Видаливши обліковий запис отримаємо наступний запис:



При вході користувача в систему робиться такий запис:



При виході користувача з системи робиться такий запис:



1. В контекстному меню журналу безпеки вибрати пункт "Свойства". Задати якнайменший розмір журналу та політику "Не затирать события". Після цього в редакторі об’єкту групової політики (гілка "Параметры безопасности") включити параметр політики "Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности". Заповнити журнал аудиту увімкнувши політики та виконавши достатню кількість дій, що підлягають аудиту. Якщо це виконувалось користувачем з адміністративними повноваженнями, спробувати увійти в систему як звичайний користувач. Переконатись у неможливості входу в систему через переповненість журналу аудиту. Увійти як адміністратор; вимкнути увесь аудит. В контекстному меню журналу безпеки вибрати пункт "Стереть все события" для очищення журналу. Чи усі події вдалося видалити? Чи з’явились нові записи?

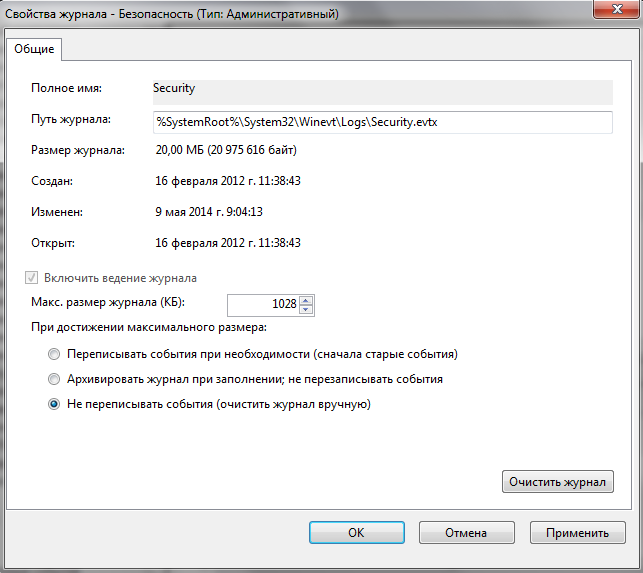


Рис. 8. Задаємо найменший розмір журналу та політику "Не затирать события".

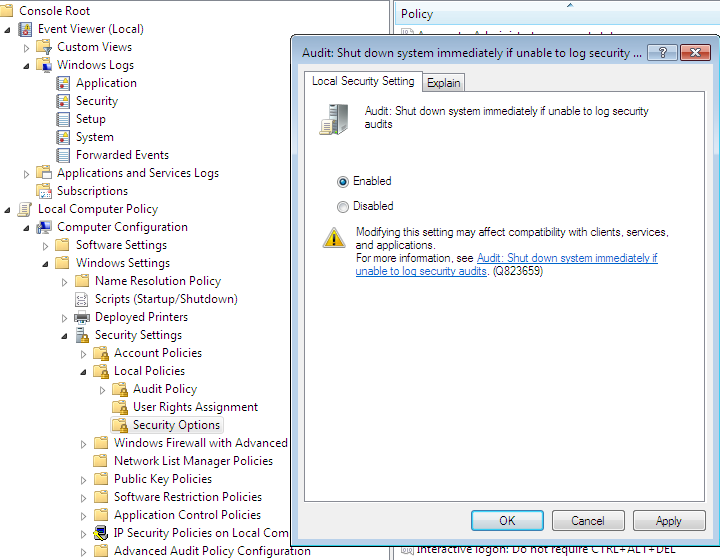


Рис. 9. Включення параметру політики "Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности"

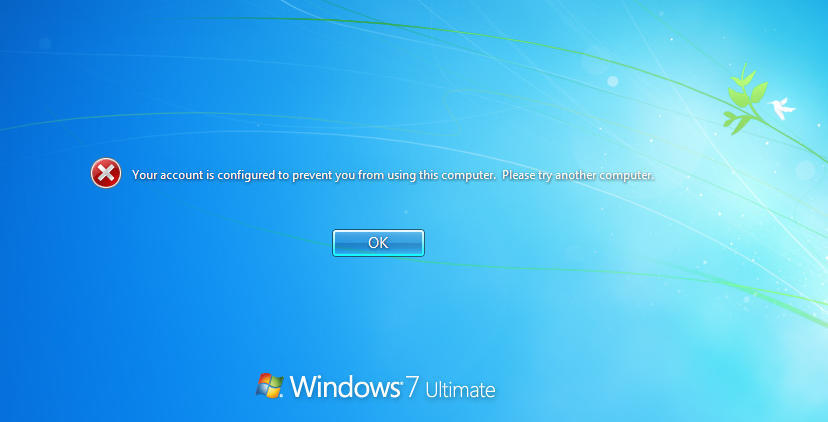


Рис. 10. Вхід під звичайним користувачем

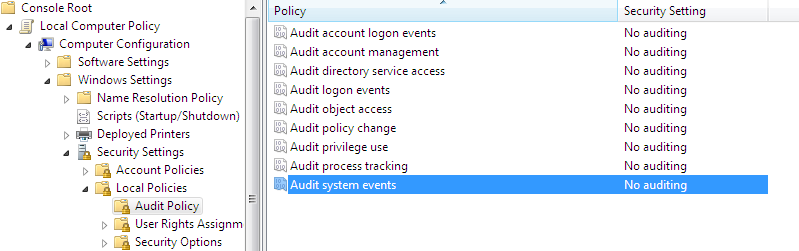


Рис. 11. Вимкнення аудиту під адміністратором

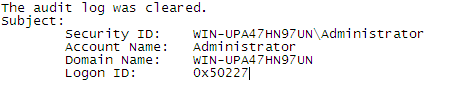


Рис. 12. Запис в журналі, що аудит було вимкнено

## ВИСНОВКИ

Виконавши дану роботу я ознайомився зі структурою, принципом роботи та налаштуванням об’єкта групової політики на локальному комп’ютері та навчився використовувати та створювати шаблони безпеки для ефективного налаштування та аналізу типових параметрів безпеки.