Лабораторна робота - Налаштування Локальної політики безпеки Windows

# Вступ

У цій лабораторній роботі ви налаштуєте параметри локальної політики безпеки Windows. Локальна політика безпеки Windows призначена для налаштування широкого спектру параметрів безпеки автономних комп'ютерів, які не є частиною домену Active Directory. У цій роботі ви будете змінювати вимоги до пароля, активувати аудит, налаштовувати деякі права користувача та встановлювати деякі параметри безпеки. Далі ви скористаєтесь "Менеджером подій" для перегляду інформації, що реєструється.

# Рекомендоване обладнання

* Комп’ютер із встановленим Windows

**Примітка**: Процедура доступу до інструменту "Локальна політика безпеки" залежить від версії Windows. Але після відкривання інструменту. налаштування будуть однаковими для решти кроків у цій лабораторній роботі.

# Інструкції

## Аналіз вимог безпеки.

Для роботи філії клієнту необхідно мати шість автономних комп'ютерів з ОС Windows, налаштованих відповідно до діючої політики безпеки організації. Ці комп'ютери не входять у домен Active Directory. Політики необхідно налаштувати вручну на кожному комп’ютері.

Політика безпеки передбачає наступні вимоги:

* Довжина пароля повинна бути мінімум 8 символів
* Паролі змінюються кожні 90 днів
* Користувач може змінювати пароль один раз на день.
* Користувач повинен використовувати унікальний пароль щонайменше 8 разів підряд.
* Пароль повинен містити три з наступних чотирьох елементів:
* Як мінімум одну велику букву.
* Як мінімум одну маленьку букву.
* Як мінімум одну цифру.
* Як мінімум один символ.
* Після 5 невдалих спроб ввести пароль доступ користувача до комп'ютера блокується. Щоб знову спробувати ввійти у заблокований комп'ютер, користувач повинен зачекати 5 хвилин.
* Всі налаштування безпеки в "Політиці аудиту" повинні бути активовані.
* Після 30 хвилин бездіяльності відбувається автоматичний вихід користувача з системи. (тільки у Windows 8.1 та 8.0)
* Щоб відключити ноутбук від док-станції, користувачу необхідно ввійти в систему.
* Під час входу в систему користувачу повинно видаватись наступне текстове повідомлення:
* Заголовок: **Увага:**
* Текст: **Ваші дії контролюються. Цей комп'ютер призначений тільки для службового користування!**
* Користувачі повинні отримувати нагадування про зміну пароля за 7 днів до його закінчення.

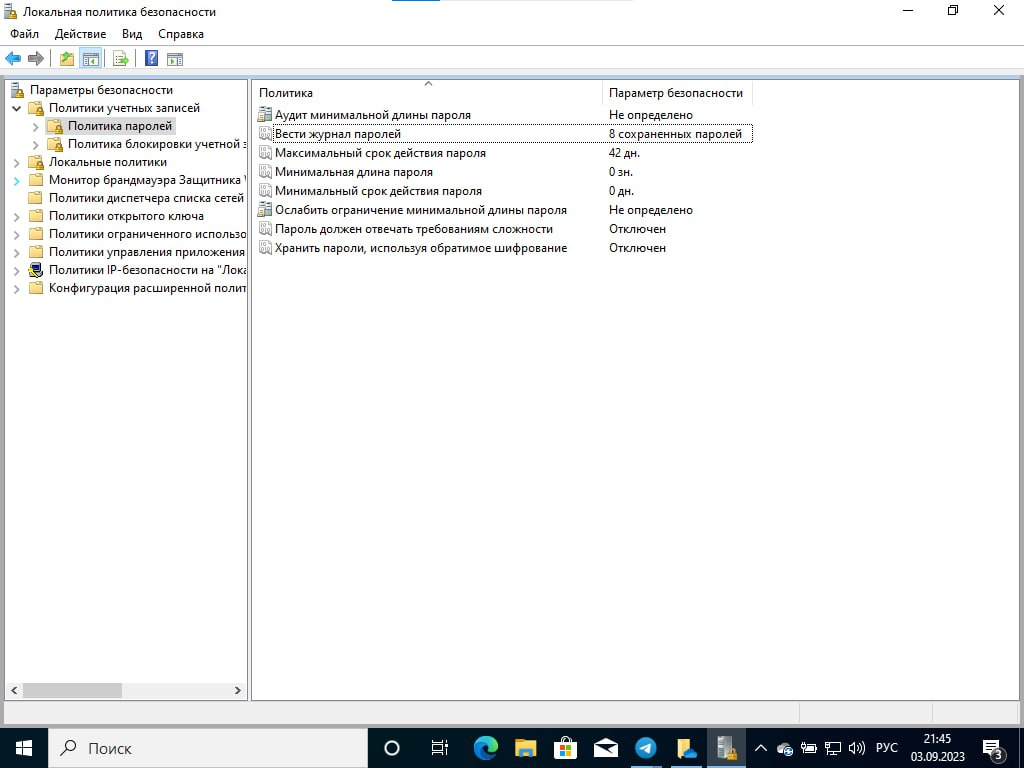
В інструменті **Локальна політика безпеки Windows** є доступними багато інших функцій, які не розглядаються у цьому курсі.

## Відкрити інструмент "Локальна політика безпеки Windows"

* + 1. Для доступу до інструменту Локальна політика безпеки в Windows 10, можна використати наступні два шляхи:

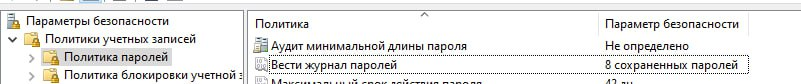
**Адміністрування > Локальна політика безпеки (Local Security Policy)**

Або **Пошук > secpol.msc** і потім натиснути на **secpol**.

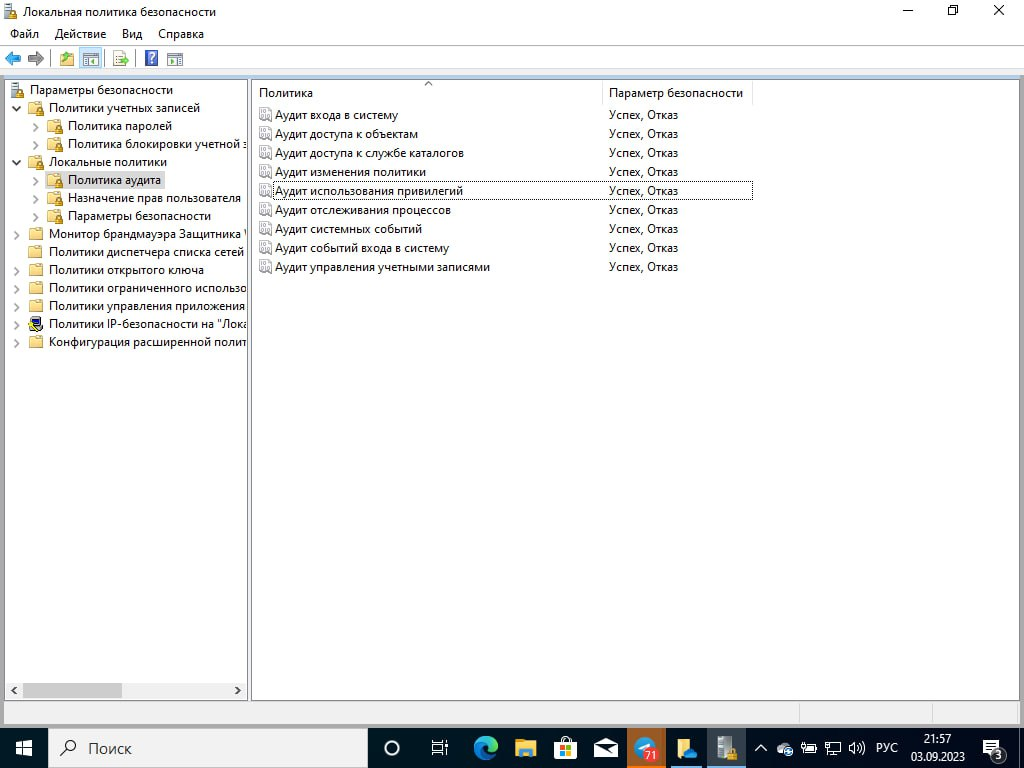
* + 1. Відкриється вікно **Локальна політика безпеки Windows** (Локальна політика безпеки). В цій лабораторній роботі розглядаються **Політики облікових записів** (Account Policies) та **Локальні політики** (Local Policies), що виділені на рисунку нижче. Інші **Налаштування безпеки** в межах цього курсу не розглядаються.
    2. 

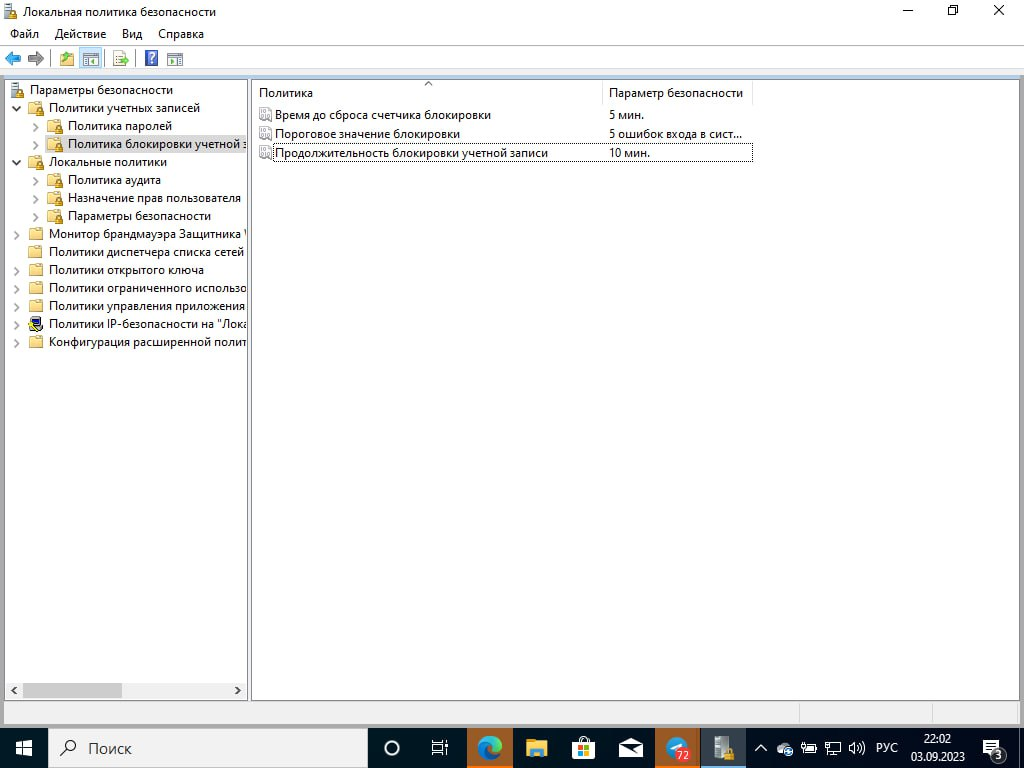
## Задайте налаштування безпеки, що відносяться до Політики паролів (Password Policy).

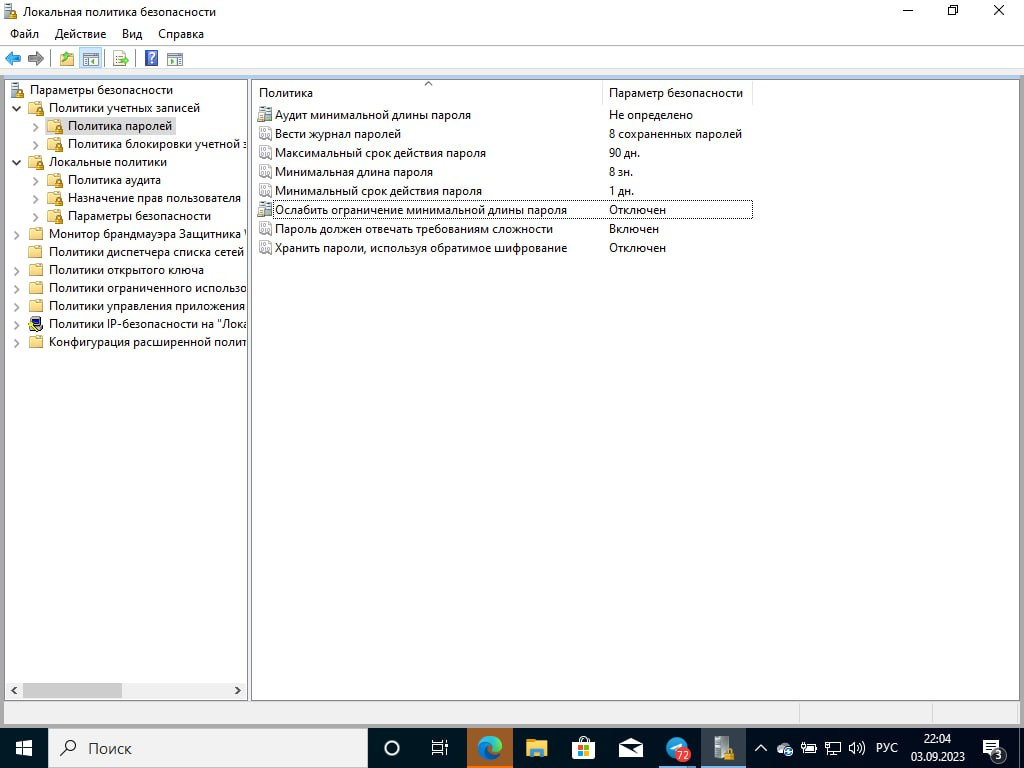
Перші шість вимог політики безпеки компанії налаштовуються в розділі **Політики облікових записів** служби **Локальна політика безпеки**.

* + 1. Натисніть стрілку вниз, щоб розгорнути **Політики облікових записів** та виберіть пункт **Політика паролів**. На правій панелі відображаються шість політик та їх налаштування безпеки за замовчуванням.
    2. Перша політика, **Вести журнал паролів** (Enforce password history), задає кількість унікальних паролів, які повинен задати користувач, поки йому не буде дозволено використовувати попередній пароль повторно. У відповідності з політикою безпеки для організації, що описана в кроці 1, для цієї політики повинно бути задано налаштування безпеки **8**. Двічі клікніть **Вести журнал паролів** щоб відкрити вікно **Властивості:Вести журнал паролів** (Enforce password history Properties). Задайте значення **8**.
    3. 
    4. У відповідності до вимог політики безпеки організації, що описані у кроці 1 задайте необхідні параметри **Локальної політики безпеки** для інших налаштувань безпеки в **Політиці паролів**.

| **Політика** | **Настройки безпеки** |
| --- | --- |
| Вести журнал паролів (Enforce password history) | 8 |
| Максимальний вік пароля (Maximum password age) | 42 дн. |
| Мінімальний вік пароля (Minimum password age) | 0 дн. |
| Мінімальна довжина пароля (Minimum password length) | 0 зн. |
| Пароль повинен відповідати вимогам до складності (Password must meet complexity requirements) | Вимкнено |
| Зберігайти паролі, використовуючи оборотне шифрування (Store passwords using reversible encryption) | Вимкнено |







**Примітка**: Налаштування безпеки **Зберігати паролі, використовуючи оборотне шифрування** повинно бути завжди вимкнено. Зберігання паролів за допомогою оборотного шифрування по суті є тим самим, що і зберігання версій паролі в у відкритому тексті. З цієї причини цю політику ніколи не слід активувати, якщо вимоги програми не переважають над необхідністю захисту інформації про пароль.

* + 1. Відкрийте кожну з політик і задайте значення, що вказані у таблиці вище.

## Налаштування параметрів безпеки, що відносяться до "Політики блокування облікових записів" (Account Lockout Policy).

* + 1. Скільки спроб входу дозволено користувачу у відповідності з політикою безпеки, що описана на кроці 1, перед тим як обліковий запис буде заблоковано?

Запишіть тут свою відповідь.

**Користувачу дається 5 спроб, після чого доступ до облікового запису буде заблоковано.**

* + 1. Скільки часу повинен почекати користувач перед тим, як знову спробувати увійти в систему?

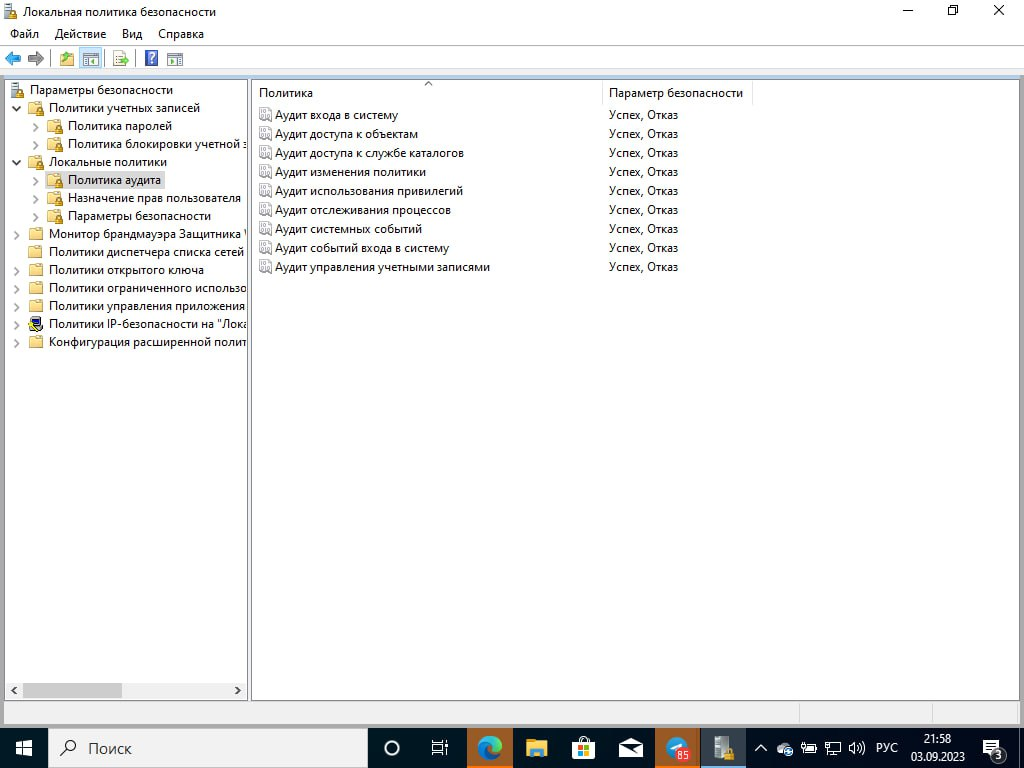
Запишіть тут свою відповідь.

**Користувач повинен почекати 5 хвилин, перед тим, як знову зможе спробувати увійти в систему.**

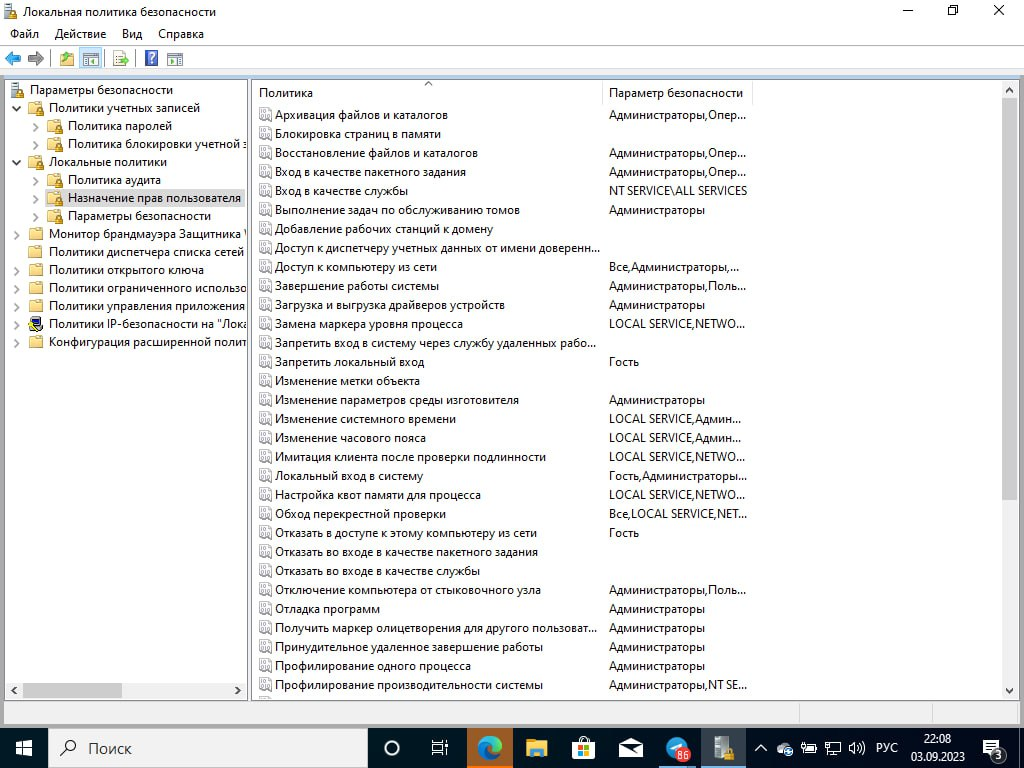
* + 1. Використайте налаштування у **Локальні політики безпеки**,що мають відношення до **Політики блокування облікових записів**  щоб налаштувати необхідні політики.

**Підказка**: В першу чергу вам необхідно задати **Порогове значення блокування** (Account lockout threshold).

## Налаштування параметрів безпеки, що мають стосунок до "Політики аудиту" (Audit Policy).

* + 1. У вікні інструменту "Локальна політика безпеки" розгорніть меню "Локальні політики" і виберіть "Політики аудиту".
    2. Двічі клікніть на стрічці **Аудит подій входу в систему** (Audit account logon events), щоб відкрити вікно **Властивості** (Properties). Відкрийте вкладку **Пояснення** (Explain), щоб прочитати інформацію про це налаштування безпеки.
    3. Відкрийте вкладку **Параметр локальної безпеки** (Local Security Setting), і встановіть прапорці на пунктах  **Успіх** (Success) та **Невдача** (Failure). Натисніть **OK** щоб закрити вікно **Властивості** і застосувати налаштування безпеки.
    4. Змініть інші налаштування безпеки, що мають відношення до **Політики аудиту**. Відкрийте вкладку **Пояснення**, щоб прочитати інформацію про кожне з налаштувань. Відкрийте графіки на пунктах **Успіх** і **Невдача** у кожному вікні **Властивості** (Properties).
    5. 

## Налаштування додаткових параметрів безпеки у розділі "Локальні політики"

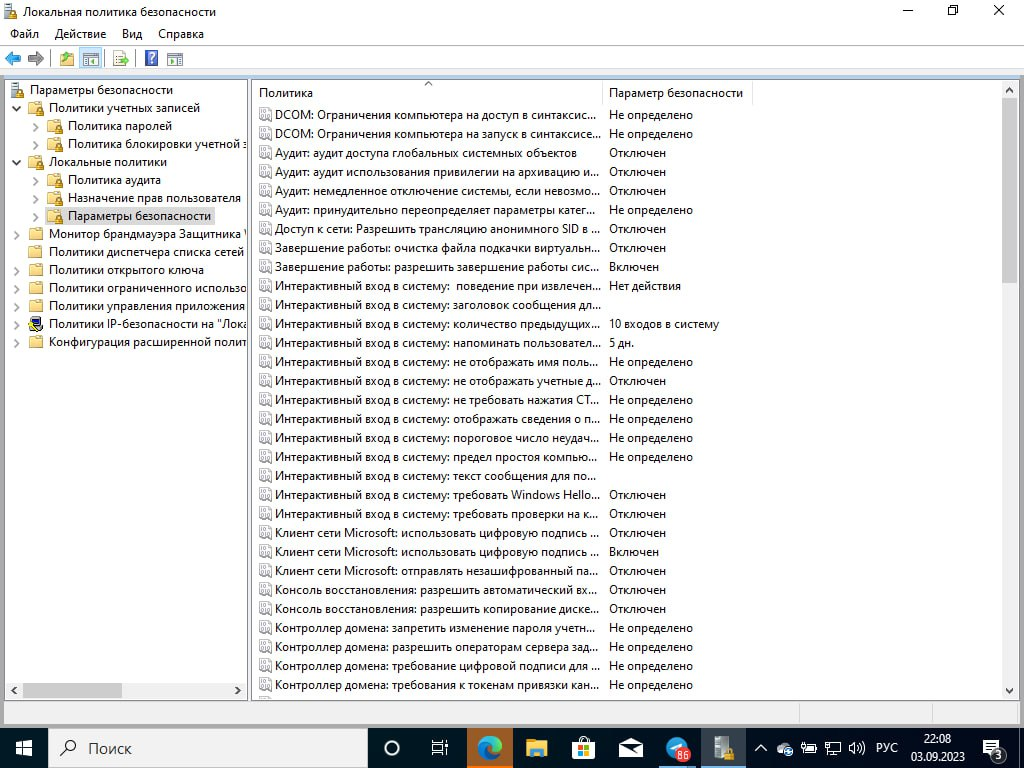
* + 1. У розділі "Локальні політики" інструменту "Локальні політики безпеки", натисніть "Призначення прав користувачів" (User Rights Assignment) та перевірте налаштування безпеки.
    2. Хоча, для дотримання вимог політики безпеки, жодних налаштувань змінювати не потрібно, перегляньте налаштування, що задані за замовчуванням.
    3. 

#### Запитання:

Чи порекомендували б ви які-небудь зміни? Чому?

Запишіть тут свою відповідь.

**Як на мене, там нічого змінювати не треба, особливо таким користувачам, як я, за замовчуванням там все виставлено зручно.**

* + 1. В розділі "Локальні політики" інструменту "Локальна політика безпеки", відкрийте пункт "Налаштування безпеки" (Security Options) та перевірте налаштування безпеки.
    2. 
    3. Для інших вимог політики безпеки, що описані у кроці 1, вкажіть у таблиці нижче, політики та налаштування безпеки, які необхідно змінити в **Налаштуваннях безпеки**. Перша стрічка вже заповнена.

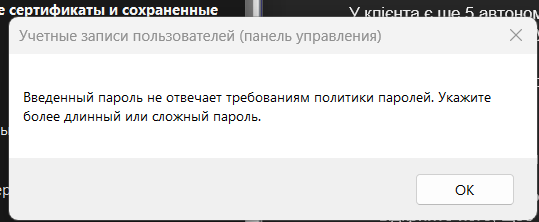
| **Політика** | **Налаштування безпеки** |
| --- | --- |
| Інтерактивний вхід в систему: Межа простою комп'ютера | 1800 секунд |
|  | * Заголовок: **Увага:** * Текст: **Ваші дії контролюються. Цей комп'ютер призначений тільки для службового користування!** |
| Интерактивный вход в систему: напоминать пользователям об истечении действия пароля. | 7 дн. |
| Интерактивный вход в систему: пороговое число неудачных попыток входа | 5 |
| Интерактивный вход в систему: не отображать имя пользователя при входе в систему | Включен |

## Перевірка налаштувань політики безпеки паролів.

Перевірте параметри, що мають відношення до політики безпеки паролів. Для цього спробуйте змінити пароль. Спробуйте задати новий пароль, який не відповідає вимогам довжини чи складності.

**Панель керування> Облікові записи користувача > Внести зміни до свого облікового запису в налаштуваннях ПК > Варіанти входу**, і натисніть **Змінити** під опцією **Пароль**.

Ви одержали повідомлення про те, що ваш новий пароль не відповідає вимогам політики паролів.



## Експорт та імпорт параметрів політики безпеки.

У клієнта є ще 5 автономних комп'ютерів, які повинні відповідати однаковим вимогам політики безпеки. Замість того, щоб вручну задавати налаштування кожного з комп'ютерів, експортуйте налаштування комп'ютера.

* + 1. На панелі меню в інструменті "Локальна політика безпеки", виберіть Дія > Експорт політики... (Export policy...)
    2. Виберіть ім'я файла **.inf** і місце для його зберігання.
    3. Скопіюйте файл політики безпеки **.inf** на флеш-накопичувач. Перенесіть флеш-накопичувач до другого комп'ютера. Вставте флеш-накопичувач, відкрийте **Локальна політика безпеки**, та натисніть **Дія > Імпорт політики... (Import Policy...)** Знайдіть на флеш-накопичувачі файл **.inf** і відкрийте його, щоб поміняти політику безпеки на цьому комп'ютері.

Кінець документа