МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ „ЛЬВІВСЬКА ПОЛІТЕХНІКА”

НАЛАШТУВАННЯ БЕЗПЕКИ У WINDOWS 10

МЕТОДИЧНІ ВКАЗІВКИ
до виконання лабораторної роботи
з дисципліни „Основи системного адміністрування”
для студентів напряму 6.050103 «Програмна інженерія» та
спеціальності 121 „Інженерія програмного забезпечення”

Затверджено
на засіданні кафедри
програмного забезпечення
Протокол № 13 від 19.05.2016 р.

Львів – 2016

Налаштування безпеки у Windows 10.: Методичні вказівки до виконання лабораторної роботи з дисципліни „Основи системного адміністрування” для студентів напряму 6.050103 «Програмна інженерія» та спеціальності 121 „Інженерія програмного забезпечення” / Укл.: В.С. Яковина, Т.О. Муха, Р.Р. Шкраб – Львів: Видавництво Національного університету „Львівська політехніка”, 2016. – 27 с.

Укладачі Яковина В.С., доцент кафедри ПЗ
Муха Т.О., асистент кафедри ПЗ
Шкраб Р.Р., асистент кафедри ПЗ

Відповідальний за випуск Яковина В.С., завідувач кафедри ПЗ

Рецензенти Тушницький Р.Б., к.т.н., доцент кафедри ПЗ
Литвин В.В., д.т.н., завідувач кафедри ІСМ

Лабораторна робота № 4.

РЕАЛІЗАЦІЯ МЕХАНІЗМУ ГРУПОВИХ ПОЛІТИК У WINDOWS 10. АНАЛІЗ І НАЛАШТУВАННЯ БЕЗПЕКИ.

Мета роботи: Ознайомлення зі структурою, принципом роботи та налаштуванням об’єкта групової політики на локальному комп’ютері під управлінням ОС Windows 10. Навчитись використовувати та створювати шаблони безпеки для ефективного налаштування та аналізу типових параметрів безпеки.

Теоретичні відомості.

Групова політика – це технологія управління, що використовується для налаштування параметрів конфігурації робочих столів для груп комп’ютерів і користувачів. Групові політики можуть включати в себе параметри безпеки, параметри установки та підтримки програмного забезпечення і параметри для скриптів (сценаріїв), що управляють процесами завантаження і завершення роботи з системою. Групові політики зберігаються у вигляді об’єктів Group Policy (GPO), які, своєю чергою, зв’язуються з об’єктами Active Directory – сайтами, доменами чи організаційними одиницями (OU), крім того існує об’єкт локальної групової політики комп’ютера[1].

Численні параметри, що визначаються в рамках об'єкту групової політики, розділено на дві частини. Одна частина параметрів використовується для конфігурації комп'ютера (computer configuration), інша частина параметрів використовується для конфігурації середовища користувача (user configuration). Конфігурація комп'ютера припускає визначення значень для параметрів, що впливають на формування оточення будь-яких користувачів, що реєструються на заданому комп'ютері. Конфігурація середовища користувача дає можливість управляти процесом формування оточення конкретного користувача, незалежно від того, на якому комп'ютері він реєструється в мережі.

Незалежно від типу конфігурації, параметри групової політики організовані в спеціальні категорії (рис. 1). Кожна з категорій параметрів групової політики визначає окрему область оточення користувача. Доступні категорії параметрів перераховані в табл. 1. Перераховані в таблиці категорії параметрів надають адміністратору доступ до різних механізмів конфігурації

[1] GPO, який застосовується локально, зберігається в локальній папці комп’ютера %systemroot%\system32\GroupPolicy. Комп’ютер може мати тільки одну локальну групову політику.

робочих станцій. У свою чергу категорії параметрів групової політики організовані в три контейнери відповідно до свого призначення:

- **Software Settings** (Конфігурація програм). У контейнері розміщуються категорії параметрів групової політики, за допомогою яких можна управляти переліком додатків, доступних користувачам;
- **Windows Settings** (Конфігурація Windows). У контейнері розміщуються категорії параметрів групової політики, що визначають налаштування безпосередньо самої операційної системи. Вміст цього контейнера може бути різним, залежно від того, на якому рівні визначаються параметри групової політики (для користувача або комп'ютера);
- **Administrative Templates** (Адміністративні шаблони). Цей контейнер містить категорії параметрів групової політики, які встановлюють правила на основі системного реєстру[1].

Всі компоненти групової політики можна редагувати за допомогою Group Policy Editor.

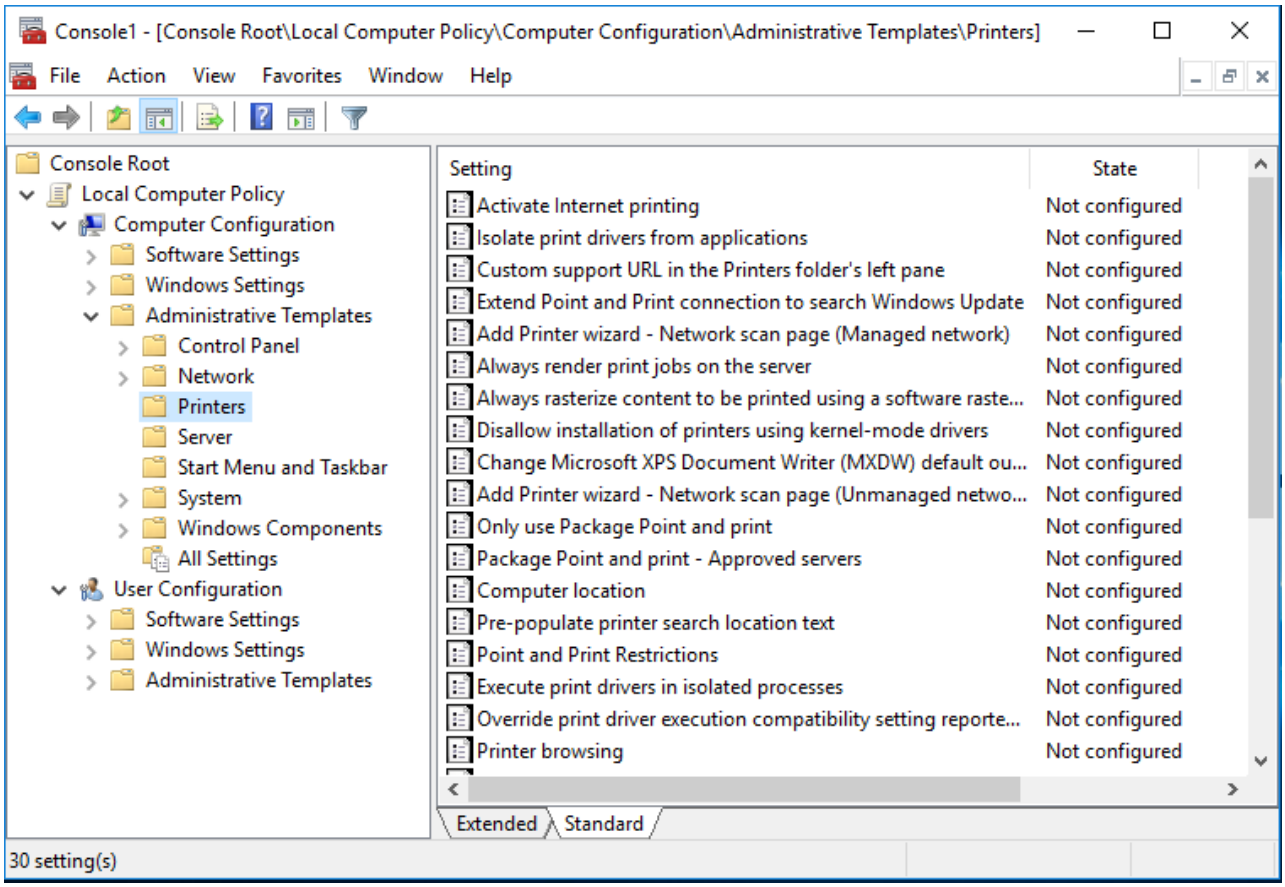

Рис. 1. Структура об'єкту групової політики.

[1] Адміністративний шаблон є текстовим файлом у форматі Unicode, який містить перелік ключів і параметрів реєстру. Такі файли мають розширення .adm і зберігаються в папці %SystemRoot%\inf.

Таблиця 1

Категорії параметрів групової політики

Категорія	Контейнер	Опис
Software Installation	Software Settings	Ця категорія параметрів використовується для централізованого управління додатками, доступними на певному комп'ютері, або для певного користувача. При цьому залежно від параметрів групової політики додатки можуть або встановлюватися примусово, або рекомендуватися для установки.
Remote Installation Service	Windows Settings	Ця категорія параметрів використовується для управління процесом віддаленої установки на клієнтському комп'ютері. Ця категорія параметрів доступна тільки у випадку конфігурації на рівні користувача.
Scripts	Windows Settings	Категорія використовується для визначення сценаріїв, які виконуватимуться при включенні/виключенні комп'ютера (Startup/Shutdown Scripts), або при реєстрації користувача в системі чи його виході з неї (Logon/Logoff Scripts).
Security Settings	Windows Settings	Параметри цієї категорії використовуються для управління налаштуваннями безпеки клієнтського комп'ютера. Крім групової політики, адміністратор може також використовувати інші механізми для управління налаштуваннями безпеки.
Folder Redirection	Windows Settings	За допомогою параметрів цієї категорії адміністратор може налаштовувати процес перенаправлення папок з призначеного для користувача профілю (таких, наприклад, як My Documents) на деякий мережний ресурс. Ця категорія параметрів доступна тільки для конфігурації користувача.
Internet Explorer Maintenance	Windows Settings	Параметри цієї категорії використовуються для налаштування браузера Internet Explorer. Ця категорія параметрів доступна тільки для конфігурації користувача.

Windows Components	Administrative Templates	У цій категорії представлені параметри, за допомогою яких адміністратор може здійснювати управління налаштуваннями Windows-компонентів, встановлених на системі, що налаштовується.
Start Menu and Taskbar	Administrative Templates	Параметри цієї категорії дозволяють адміністратору налаштовувати головне меню і панель завдань клієнтського комп'ютера (насамперед, обмежувати доступну функціональність). Ця категорія параметрів доступна тільки для конфігурації користувача.
Desktop	Administrative Templates	Параметри цієї категорії дозволяють адміністратору налаштовувати вигляд робочого столу клієнтського комп'ютера і його функціональність. Ця категорія параметрів доступна тільки для конфігурації користувача.
Control Panel	Administrative Templates	Параметри цієї категорії дозволяють адміністратору управляти відображенням окремих компонентів панелі управління на клієнтському комп'ютері. Ця категорія параметрів доступна тільки для конфігурації користувача.
Shared Folders	Administrative Templates	Параметри цієї категорії дозволяють управляти процесом публікації загальних папок. Ця категорія параметрів доступна тільки для конфігурації користувача.
Networks	Administrative Templates	Ця категорія параметрів використовується для управління конфігурацією мережних компонентів системи.
System	Administrative Templates	У даній категорії представлені параметри, що дозволяють управляти настройками реєстру, що впливають на поведінку системи в цілому
Printers	Administrative Templates	Параметри цієї категорії використовуються для управління процесом публікації принтерів. Ця категорія параметрів доступна тільки для конфігурації комп'ютера.

Побудова ієрархії об'єктів групової політики. Параметри, визначені в рамках об'єкту групової політики, впливають тільки на ті об'єкти каталога, до яких вони застосовані. Щоб визначити множину об'єктів каталога, що підпадають під дію того або іншого об'єкту групової політики, необхідно виконати прив'язку останнього до одного або декількох контейнерів каталога. Для будь-якого об'єкту групової політики (за винятком локальних)

дозволяється прив'язка до будь-якого з трьох класів об'єктів каталога – сайту, домена або підрозділу. Будь-які об'єкти, асоційовані з обліковими записами користувачів і комп'ютерів, що розташовуються всередині цих контейнерів, підпадають під дію прив'язаного об'єкту групової політики.

У випадку, коли в рамках дерева каталога є прив'язка декількох об'єктів групової політики, цілком можлива ситуація, коли деякі об'єкти каталога (або навіть всі) можуть підпадати під дію відразу декількох об'єктів групової політики. При цьому параметри, визначені в них, застосовуються до об'єктів каталога відповідно до певного порядку:

- спочатку застосовуються об'єкти групової політики, прив'язані до сайту, в якому знаходиться об'єкт каталога;
- після цього застосовуються об'єкти, прив'язані на рівні домена;
- останніми застосовуються об'єкти групової політики, прив'язані до організаційних одиниць.

Якщо є декілька вкладених організаційних одиниць, об'єкти групової політики застосовуються відповідно до рівнів вкладеності. В такому випадку йдеться про успадкування параметрів об'єктів вищого рівня групової політики (group policy inheritance).

Об'єкти групової політики, прив'язані до дочірніх контейнерів, можуть перевизначати параметри об'єктів групової політики, прив'язаних до об'єктів вищого рівня. В цьому випадку прийнято говорити про перевизначення (group policy overriding) параметрів об'єкту групової політики. При цьому успадковуються тільки ті параметри об'єктів групової політики, що були визначені для батьківського контейнера, але не визначені для дочірнього. Інакше значення параметрів, визначені в об'єкті групової політики, прив'язаному до об'єкту нижчого рівня групової політики, перевизначатимуть значення аналогічних параметрів об'єкту групової політики, прив'язаної до контейнера вищого рівня. Якщо деякий параметр об'єкту групової політики допускає безліч значень, значення параметра об'єкту групової політики батьківського контейнера доповнюють значення аналогічного параметра, визначеного в рамках об'єкту групової політики дочірнього контейнера.

Оснащення "Security Templates". За допомогою оснащення "Security Templates" можна створити політику безпеки для комп'ютера або мережі. Використовуючи це єдине оснащення, можна управляти всією безпекою системи. Оснащення "Security Templates" не надає нових параметрів безпеки, а просто впорядковує і надає зручний доступ до всіх наявних атрибутів безпеки для спрощення адміністрування.

При імпорті шаблону безпеки в об'єкт групової політики полегшується адміністрування домена, оскільки безпека настроюється для домена або підрозділу тільки один раз.

Щоб застосувати шаблон безпеки на локальному комп'ютері, можна використовувати засіб "Security Configuration and Analysis"

Шаблони безпеки можна використовувати, щоб визначити перелічені в табл. 2 елементи.

Таблиця 2

Елементи шаблонів безпеки

Область безпеки	**Опис**
Політики облікових записів	Політика паролів, політика блокування облікового запису і політика Kerberos
Локальні політики	Політика аудиту, призначення прав користувачів і параметри безпеки
Журнал подій	Параметри журналів подій додатків, системних подій і подій безпеки
Групи з обмеженим доступом	Участь в групах безпеки
Системні служби	Запуск і дозволи для системних служб
Реєстр	Дозволи для розділів реєстру
Файлова система	Дозволи для файлів і папок

Всі шаблони зберігаються в текстових файлах з розширенням .inf. Це дозволяє копіювати, вставляти, імпортувати і експортувати будь-які атрибути шаблону. У шаблоні безпеки можуть зберігатися всі атрибути безпеки, за виключенням політик безпеки IP і політик відкритого ключа.

Нові і готові шаблони

Можна створювати шаблони безпеки, що відповідають вимогам користувача, або використовувати готові шаблони. Перед зміною параметрів безпеки необхідно визначити параметри безпеки системи, що використовуються за умовчанням, а також їх призначення.

У Windows XP існувало декілька готових шаблонів, які рекомендується використовувати для захисту системи залежно від потреб конкретного користувача. Ці шаблони використовуються для виконання наступних дій:

- Відновлення параметрів за умовчанням (Setup security.inf);
- Впровадження середовища підвищеного захисту (Hisecws.inf);
- Впровадження середовища з нижчим рівнем захисту, але з більшою сумісністю (Compatws.inf);
- Захист кореневого каталога системи (Rootsec.inf);

Готові шаблони безпеки

Готові шаблони безпеки[1] є відправною точкою в створенні політик безпеки, які налаштовуються для задоволення вимог організації. Після налаштування готових шаблонів безпеки ці шаблони можна використовувати для зміни конфігурації одного комп'ютера або безлічі комп'ютерів[2]. Змінити конфігурацію комп'ютерів можна за допомогою оснащення "Security Configuration and Analysis", утиліти командного рядка Secedit.exe, а також за допомогою імпорту шаблону в оснащення "Local Computer Policy". Можна змінювати конфігурацію декількох комп'ютерів, імпортувавши шаблон в компонент "Security Configuration", що є розширенням оснащення "Group Policy". На основі шаблонів безпеки можна також виконувати аналіз можливих слабких місць безпеки і порушень політики системи за допомогою оснащення "Security Configuration and Analysis" За умовчанням готові шаблони безпеки збережені в розташуванні: %systemroot%\Security\Templates

- **Безпека за умовчанням (Setup security.inf)**

Шаблон Setup security.inf є шаблоном для конкретного комп'ютера і містить параметри безпеки, використовувані за умовчанням, які застосовуються під час установки операційної системи, включаючи дозволи для файлів кореневого каталога системного диска. Цей шаблон можна використовувати повністю або частково з метою аварійного відновлення. Шаблон Setup security.inf не можна застосовувати за допомогою оснащення "Групова політика".

- **Сумісний (Compatws.inf)**

Дозволи за умовчанням для робочих станцій і серверів спочатку створюються для їх локальних груп: "Administrators", "Power Users" і "Users". Члени групи "Administrators" володіють найбільшими правами тоді як члени групи "Users" – якнайменшими. З цієї причини можна значно підвищити безпеку, надійність і понизити загальну вартість володіння системою, якщо дотримуватися наступних правил:

- переконатися, що кінцеві користувачі є членами групи "Users";
- упровадити додатки, які можуть успішно запускатися і виконуватися членами групи "Users".

Особи, що мають права групи "Users", можуть успішно працювати із додатками, сертифікованими для Windows. Проте такі користувачі швидше за

[1] Ці шаблони призначені для комп'ютерів, на яких використовуються параметри безпеки за умовчанням. Іншими словами, будучи встановленими на комп'ютері, ці шаблони значно змінюють стандартні параметри безпеки. Але вони ***не*** встановлюють стандартні параметри безпеки, перш ніж змінити їх.

[2] Забезпечення безпеки неможливе в системах Windows XP Professional, встановлених на дисках з файловою системою FAT.

все не зможуть запускати не сертифіковані для Windows додатки. Якщо необхідно забезпечити підтримку не сертифікованих додатків, існують дві можливості:

- Всі члени групи "Users" повинні також бути членами групи "Power Users".
- Використовувати додаткові дозволи за умовчанням, створені для групи "Users".

Оскільки члени групи "Power Users" володіють успадкованими можливостями, такими як створення користувачів, груп, принтерів і загальних ресурсів, деякі адміністратори вважають за краще надати додаткові дозволи групі "Users", замість зарахування кінцевих користувачів в групу "Power Users". Для цих цілей служить "Сумісний" шаблон. За допомогою цього шаблону змінюються дозволи для файлів і реєстру, використовувані за умовчанням, створені для групи "Users", які відповідають вимогам більшості не сертифікованих застосувань. Крім того, оскільки після застосування сумісного шаблону користувачі не повинні приєднуватися до групи "Power Users", всі члени групи "Power Users" віддаляються.

Сумісний шаблон не слід застосовувати до комп'ютерів, які є контролерами домена. Наприклад, не слід імпортувати сумісний шаблон в стандартний домен або в об'єкт групової політики стандартного контролера домена.

- **Захист (Secure*.inf)**

У шаблоні "Security" визначаються параметри підвищеної безпеки. Найменш імовірно, що вони впливають на сумісність. Наприклад, в шаблоні "Захист" визначаються параметри надійних паролів, блокування і аудиту.

Крім цього, шаблоном "Захист" обмежується використання LAN Manager і протоколів перевірки достовірності NTLM шляхом налаштування клієнтів на відправку відповідей у форматі NTLMv2.

Шаблони безпеки також визначають додаткові обмеження для анонімних користувачів та включають підписування пакетів SMB на сервері, яке за умовчанням відключено для робочих станцій і серверів.

- **Підвищений захист (hisec*.inf)**

Група шаблонів підвищеного захисту включає шаблони, що накладають додаткові обмеження на рівні шифрування і підпису, необхідні для перевірки достовірності і для даних, що передаються по безпечним каналам між клієнтами SMB і серверами. Наприклад, тоді як параметри шаблонів безпеки визначають відмову серверів від відповідей LAN Manager, параметри шаблонів підвищеного захисту визначають відмову серверів як від відповідей LAN Manager, так і від відповідей NTLM. Шаблон захисту включає підписання

пакетів SMB на сервері, а для шаблону підвищеного захисту таке підписання є необхідним. Для шаблонів підвищеного захисту є необхідним надійне кодування і підпис для даних, що передаються по безпечному каналу між доменом і членом домена і між двома доменами, між якими встановлені довірчі відносини.

Крім обмежень на використання протоколів LAN Manager і вимог шифрування і підпису даних SMB і потоку даних безпечного каналу шаблони підвищеного захисту також обмежують використання кешованих даних входу в систему, таких як дані, збережені за допомогою Winlogon і засобу "Збереження імен користувачів і паролів".

Крім цього, в шаблоні Hisecws параметри групи обмеженого доступу використовуються для виконання наступних дій:

- Видалення всіх членів групи "Power Users".
- Перевірка того, що тільки адміністратори домена і локальні облікові записи адміністратора є членами локальної групи "Administrators".

Шаблоном Hisecws визначаються ці обмеження для груп при виконанні тільки сертифікованих для Windows 2000 додатків. При роботі тільки з сертифікованими додатками ані небезпечні сумісні шаблони, ані небезпечна група "Power Users" не є необхідними. Користувачі можуть успішно працювати з сертифікованими додатками в безпечному контексті звичного користувача, який визначається параметрами безпеки за умовчанням файлової системи і реєстру.

- **Безпека системного кореневого каталога (Rootsec.inf)**

Шаблоном Rootsec.inf визначаються нові дозволи для кореневого каталога Windows 10. За умовчанням ці дозволи визначаються шаблоном Rootsec.inf для кореневого каталога системного диска. Цей шаблон можна використовувати, щоб повторно застосувати дозволи для кореневого каталога, якщо вони були випадково змінені. Шаблон також може бути змінений для застосування цих дозволів для кореневого каталога до інших томів. Шаблоном не перевизначаються явні дозволи, визначені для всіх дочірніх об'єктів. Шаблоном розповсюджуються тільки успадковані дочірніми об'єктами дозволи.

- **Відсутність SID користувача серверу терміналів (Notssid.inf)**

Стандартні таблиці управління доступом до файлової системи і реєстру, розташовані на серверах, надають дозволи для SID (Secuity ID) сервера терміналів. SID сервера терміналів використовується, тільки якщо цей сервер запущений в режимі сумісності додатків. Якщо сервер терміналів не використовується, цей шаблон може бути застосований для видалення непотрібних SID сервера терміналів з файлової системи і реєстру. Проте

видалення запису управління доступом для SID сервера терміналів з файлової системи і реєстру не підвищує безпеку системи. Замість видалення SID сервера терміналів слід запустити сервер терміналів в режимі повної безпеки. При роботі в режимі повної безпеки SID сервера терміналів не використовується.

Щоб імпортувати[1] шаблон безпеки:

1. Відкрийте оснащення "Security Configuration and Analysis". У дереві консолі клацніть правою кнопкою миші вузол "Security Configuration and Analysis"
2. і виберіть команду "Import Template".
3. (Необов'язково) Для видалення з бази даних від всіх збережених раніше шаблонів встановіть відмітку "Clear this database before importing".
4. Клацніть файл шаблону і натисніть кнопку "Open".
5. Повторіть попередній крок для всіх шаблонів, для яких вимагається виконати злиття з базою даних.

Щоб виконати аналіз безпеки системи:

1. Відкрийте оснащення "Security Configuration and Analysis"
2. У дереві консолі клацніть правою кнопкою миші вузол " Security Configuration and Analysis " і виберіть команду "Open database".
3. У діалоговому вікні "Open database" даних виконайте одну з наступних дій:
   - щоб створити нову базу даних, введіть ім'я в полі "Name file" і натисніть кнопку "Open";
   - щоб відкрити існуючу базу даних, виберіть базу даних і натисніть кнопку "Open".
4. Якщо створюється нова база даних, в діалоговому вікні "Import Template " виберіть шаблон і натисніть кнопку "Open".
5. У області відомостей клацніть правою кнопкою миші вузол " Security Configuration and Analysis " і виберіть команду "Analyze Computer".
6. Виконайте одну з наступних дій:
   - для використання стандартного журналу в групі "The path of the log file errors" натисніть кнопку "OK";
   - для вибору іншого журналу введіть в полі " The path of the log file errors " допустимі шлях і ім'я файлу.

[1] Імпорт шаблонів в особисту базу даних впливає тільки на базу даних аналізу і не змінює параметри системи.

Щоб налаштувати безпеку системи:

1. Відкрийте оснащення **"Security Configuration and Analysis"**
2. У дереві консолі клацніть правою кнопкою миші вузол **"Security Configuration and Analysis"** і виберіть команду "**Open database**".
3. У діалоговому вікні "**Open database**" виконайте одну з наступних дій:
   - щоб створити нову базу даних, введіть ім'я в полі "**Name file**" і натисніть кнопку "**Open**";
   - щоб відкрити існуючу базу даних, виберіть базу даних і натисніть кнопку "**Open**".
4. Якщо створюється нова база даних, в діалоговому вікні "**Import Template**" виберіть шаблон і натисніть кнопку "**Open**".
5. У дереві консолі клацніть правою кнопкою миші вузол **"Security Configuration and Analysis"** і виберіть команду "**Configure Computer**".
6. Виконайте одну з наступних дій:
   - для використання стандартного журналу в групі **"The path of the log file errors"** натисніть кнопку "**OK**";
   - для вибору іншого журналу введіть в полі **"The path of the log file errors"** допустимі шлях і ім'я файлу.

Завдання до виконання роботи

1. Відкрити оснастку mmc "Group Policy". Перейти в гілку "Password Policy" (рис. 2), задати мінімальну довжину пароля (рис. 3). Після цього спробувати змінити власний пароль на такий, довжина якого менша за вказану в політиці, переконатись в неможливості такої дії (рис. 4). Повторити такі дії з параметрами "Password must meet complexity requirements" та "Store passwords using reversible encryption".

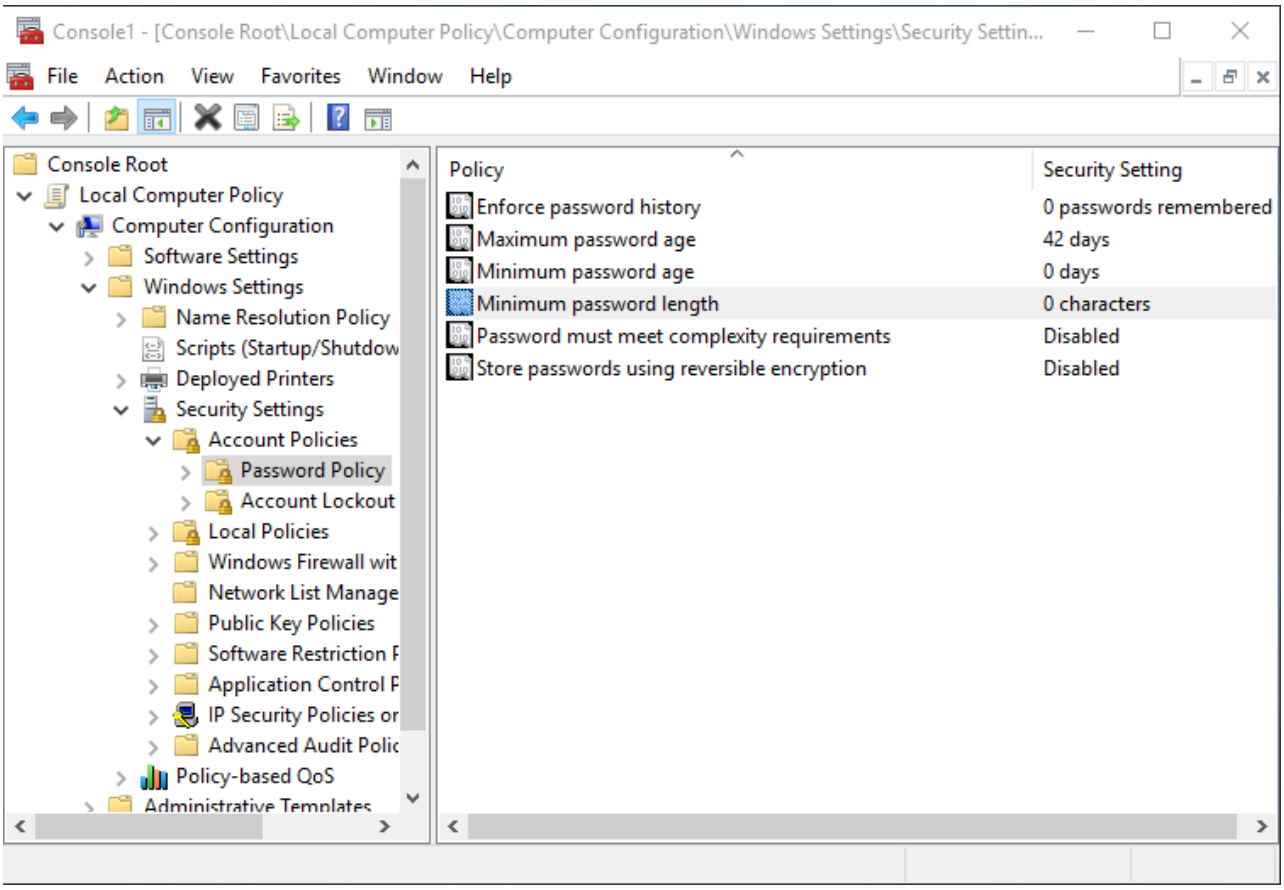

Рис. 2. Оснащення "Group Policy".

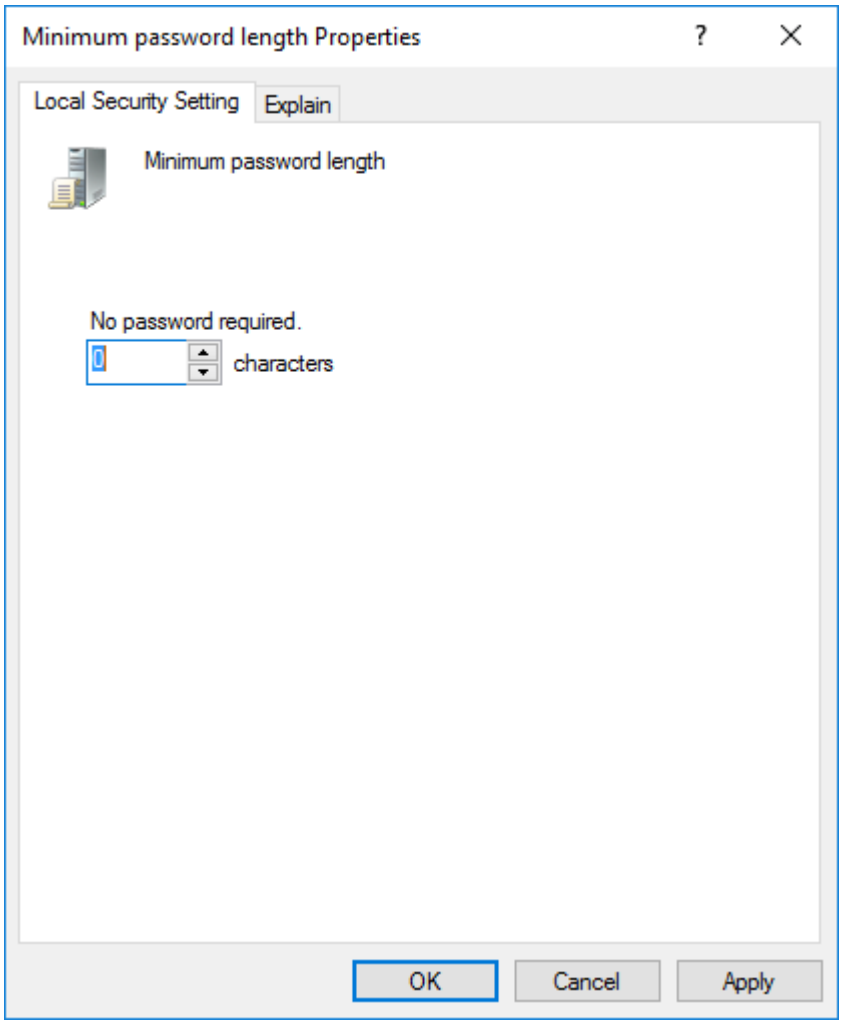

Рис. 3. Властивості параметру безпеки.

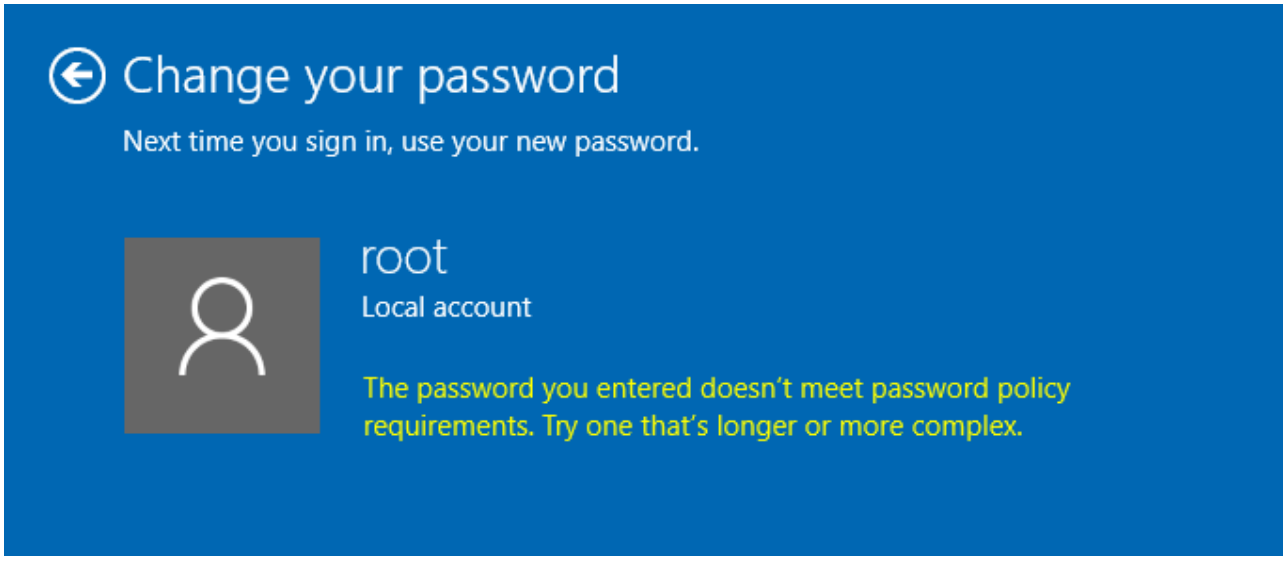

Рис. 4. Повідомлення системи про невідповідність параметру значенню політики.

2. Перейти в гілку "Account lockout threshold" (рис. 2), задати граничне значення блокування (рис. 5). Після цього спробувати декілька разів зайти в систему з неправильним вводом пароля – переконатись у спрацюванні блокування (рис. 6). Увійти в систему як адміністратор – зняти блокування вручну з оснастки "Local Users and Groups" у властивостях заблокованого облікового запису (рис. 7).

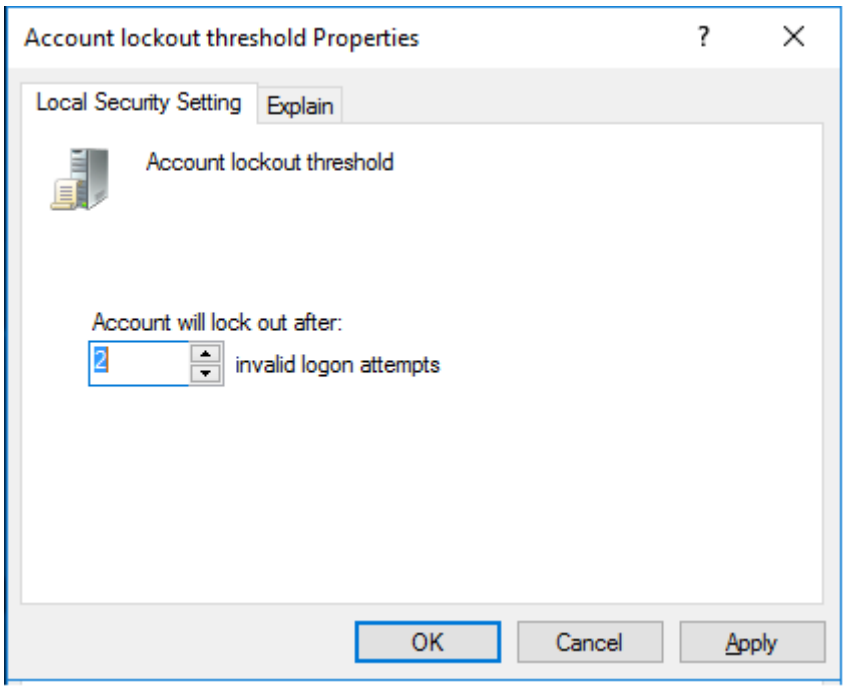

Рис. 5. Встановлення граничного значення блокування облікового запису.

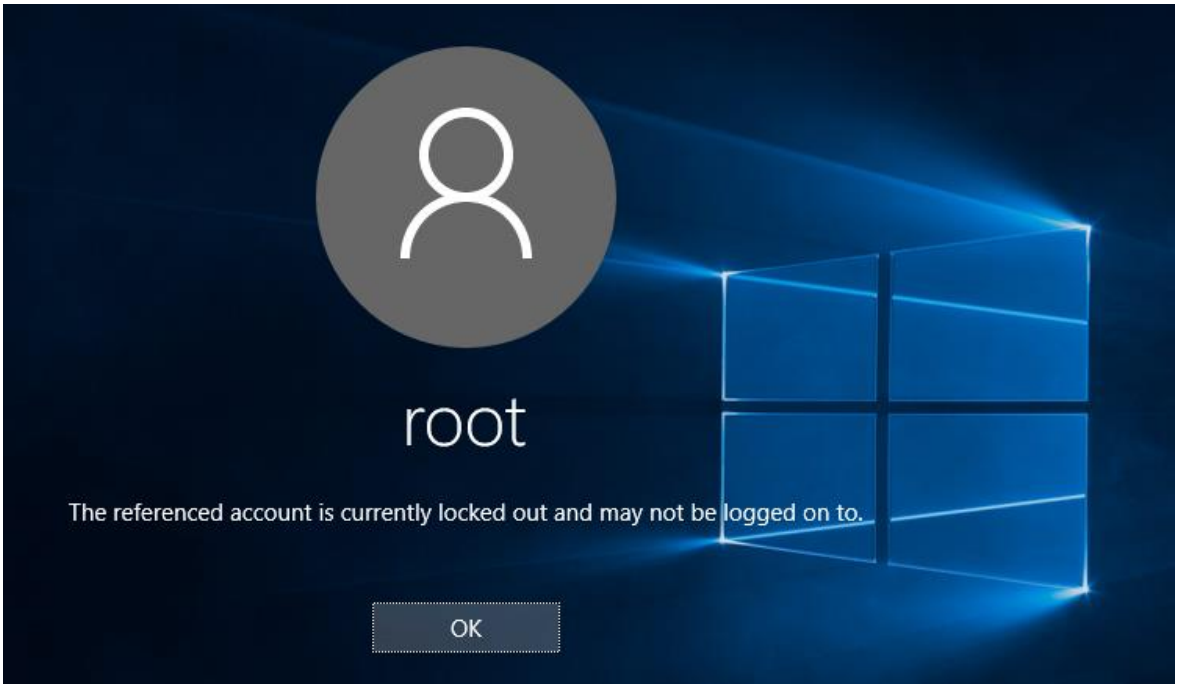

Рис. 6. Повідомлення системи про блокування облікового запису.

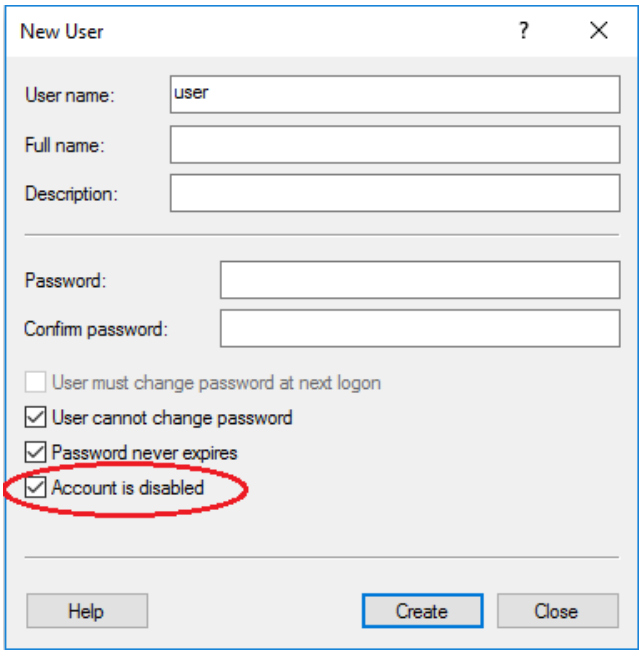

Рис. 7. Властивості заблокованого облікового запису.

3. Налаштування привілеїв користувачів. Перейти в гілку "Local Policies | User Rights Assignment" (рис. 8), задати привілей на вимкнення комп'ютера тільки для групи адміністраторів (рис. 9). Увійти до системи як користувач без адміністративних привілеїв; переконатись, що пункт "Shut down" зник з меню "Start", крім того завершення роботи системи з командного рядка теж неможливе (рис. 10).

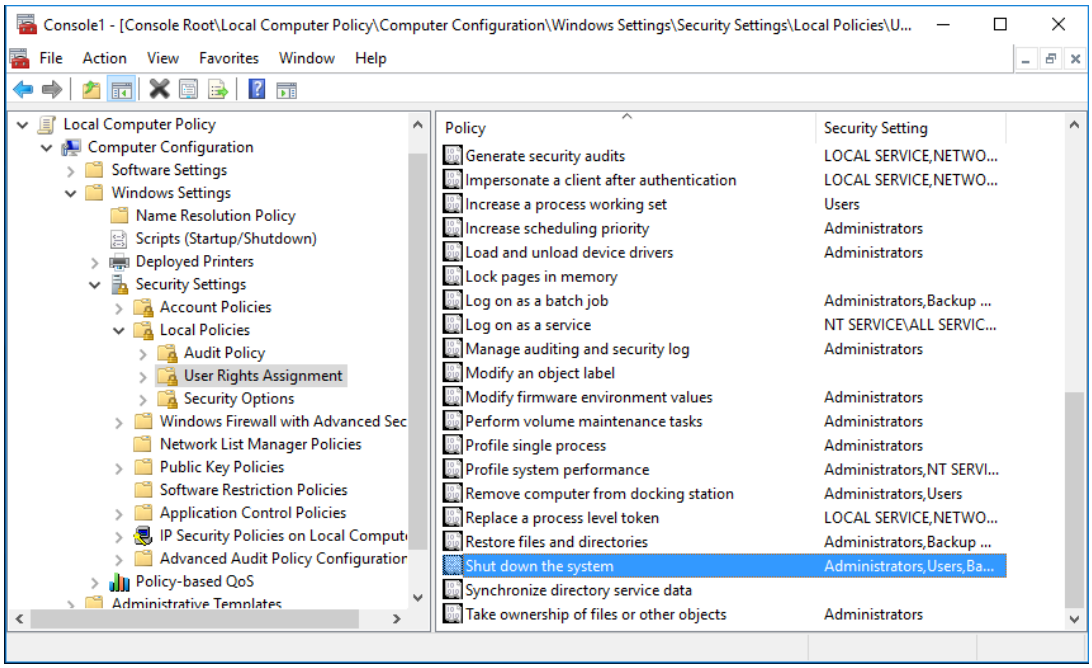

Рис. 8. Призначення прав користувачів за допомогою групової політики.

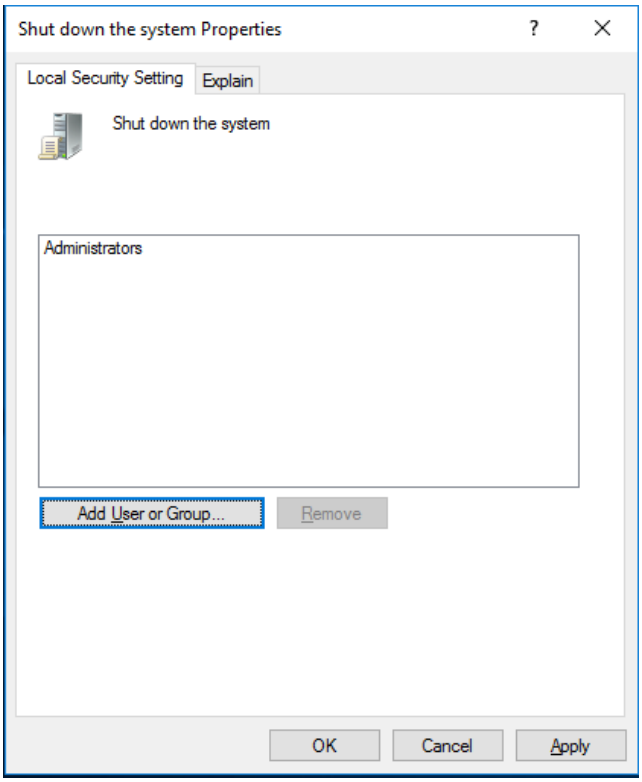

Рис. 9. Властивості параметру прав користувачів на завершення роботи системи.

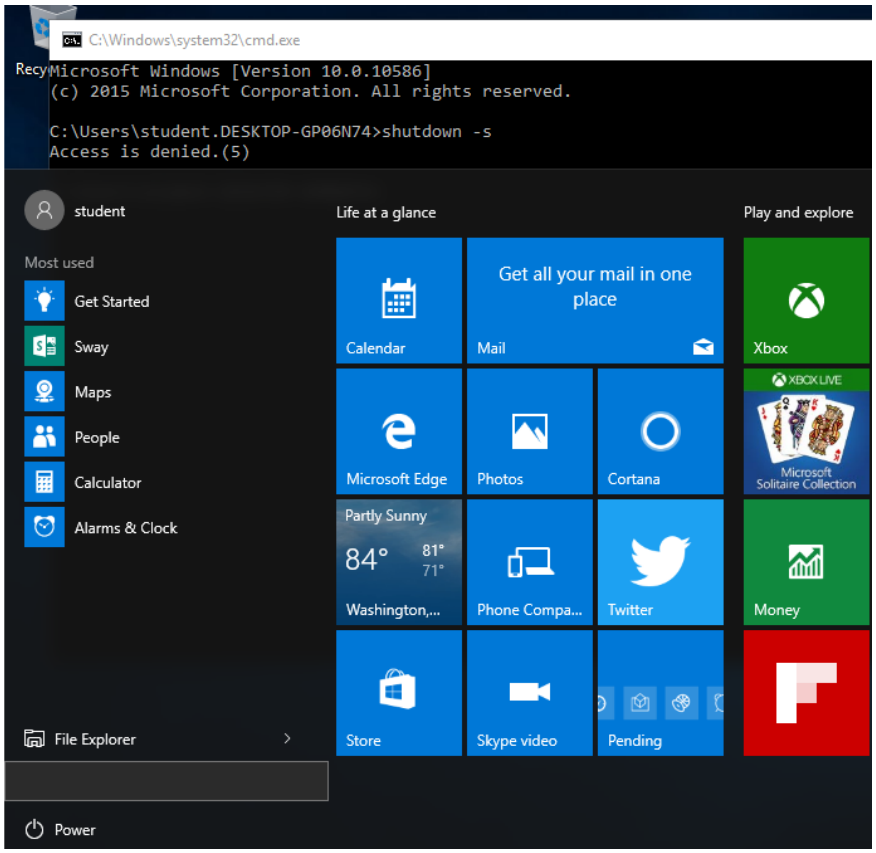

Рис. 10. Результат виконання політики стосовно заборони користувачу завершення роботи системи.

4. Оглянути вміст гілки "Administrative Templates" як для частини "Computer Configuration", так і "User Configuration". В гілці "Control Panel | Display" увімкнути політику видалення значка "Display" з панелі управління (рис. 11). Спробувати змінити параметри екрану (рис. 12). Переконатись, що політики діють на усіх користувачів локальної системи.

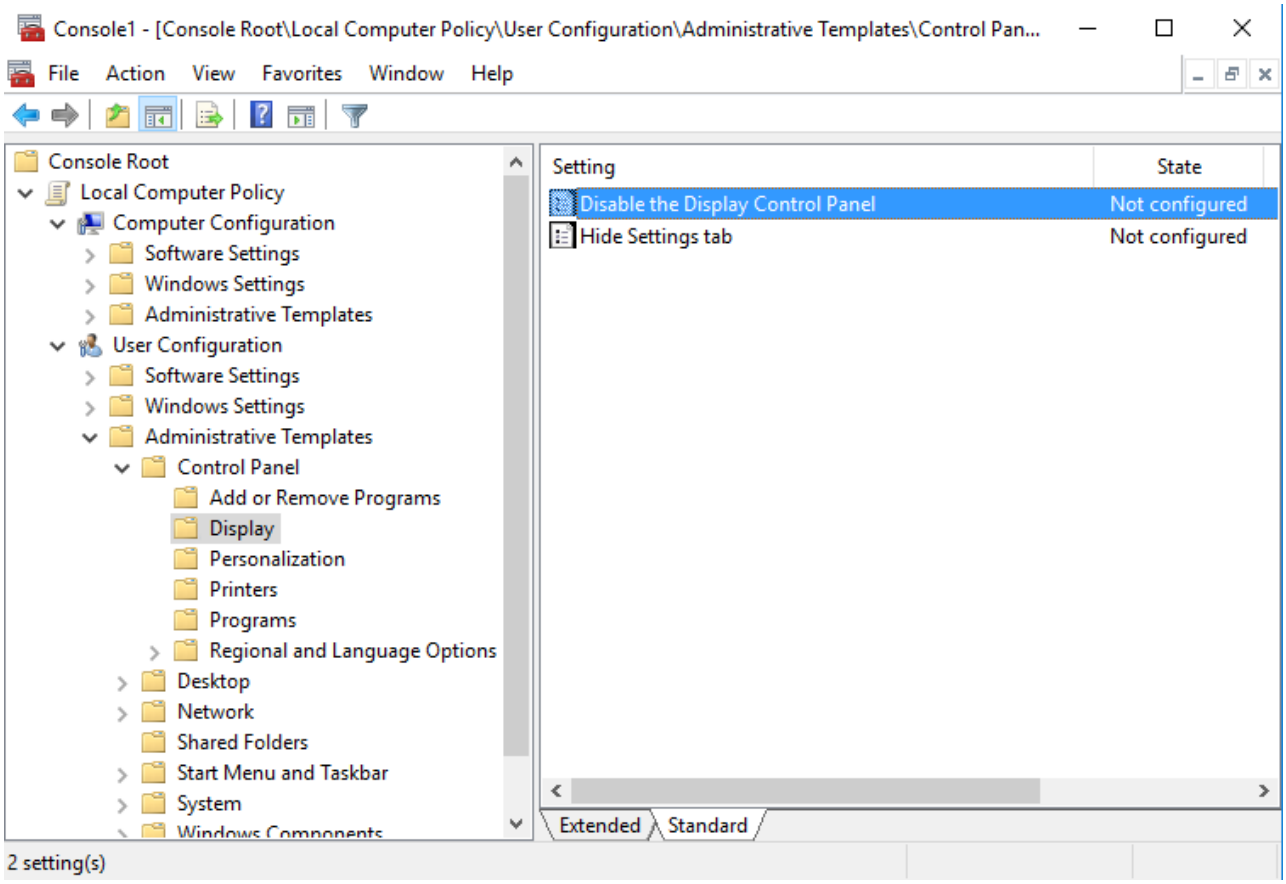

Рис. 11. Налаштування адміністративних шаблонів.

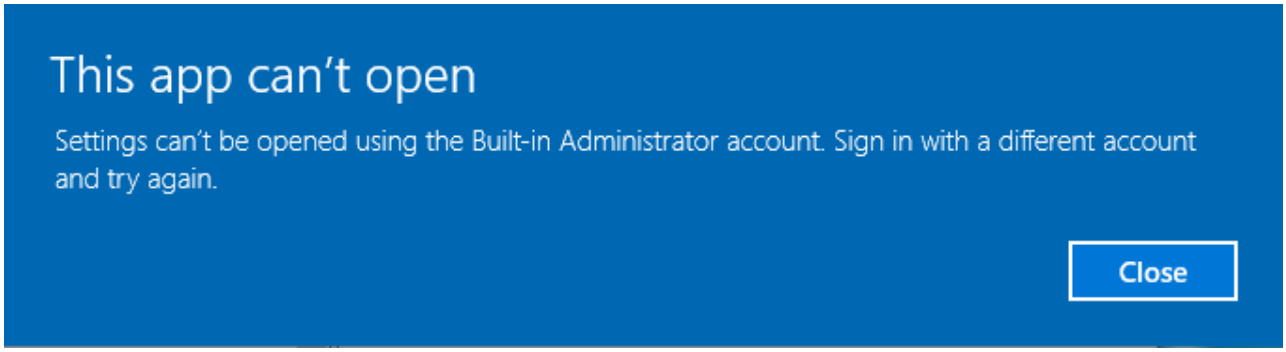

Рис. 12. Повідомлення системи щодо заборони виконання певних налаштувань робочого середовища.

5. Перейти в гілку "Software Restriction Policies" (рис. 13). Створити нову політику. Не змінюючи політики за замовчуванням створити нове правило (правила), що забороняє виконання програм з будь-якого тому крім "C:" (при потребі створити логічні диски або розділи) – рис. 14, 15. Спробувати виконати будь-який файл з цього тому (рис. 16). Створити нове правило для хешу програми, яке дозволить виконувати саме цей вказаний файл (рис. 17). Спробувати запустити на виконання цей файл. Для яких потреб можуть використовуватись правила такого типу?

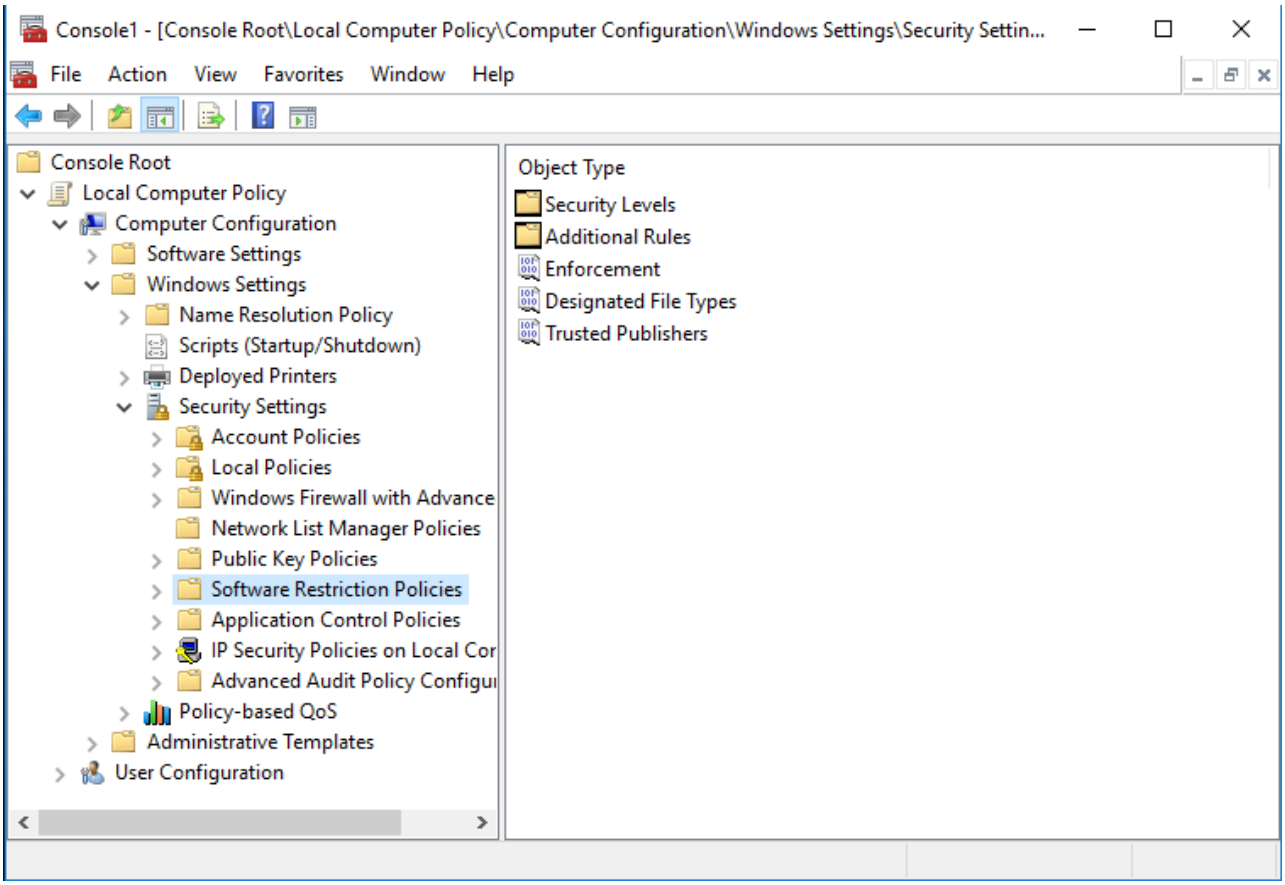

Рис. 13. Загальний вигляд гілки обмеженого використання програм.

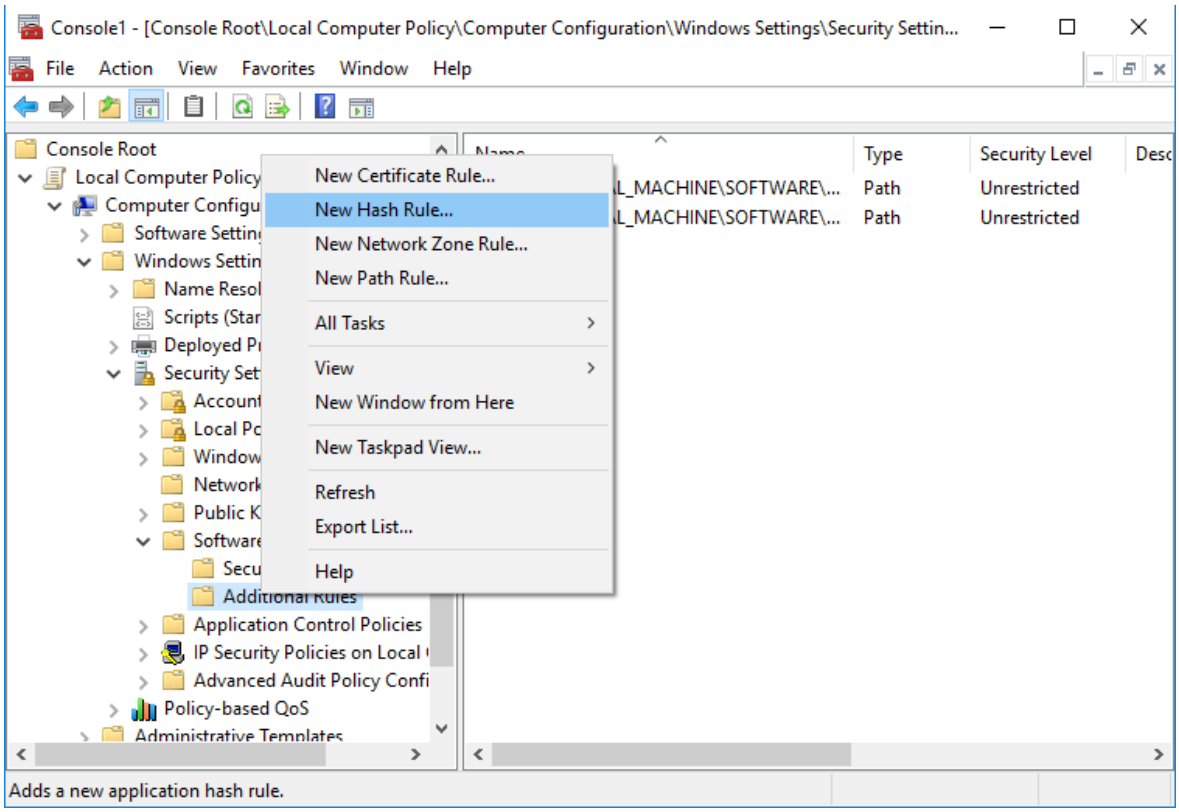

Рис. 14. Створення правил обмеженого використання програм.

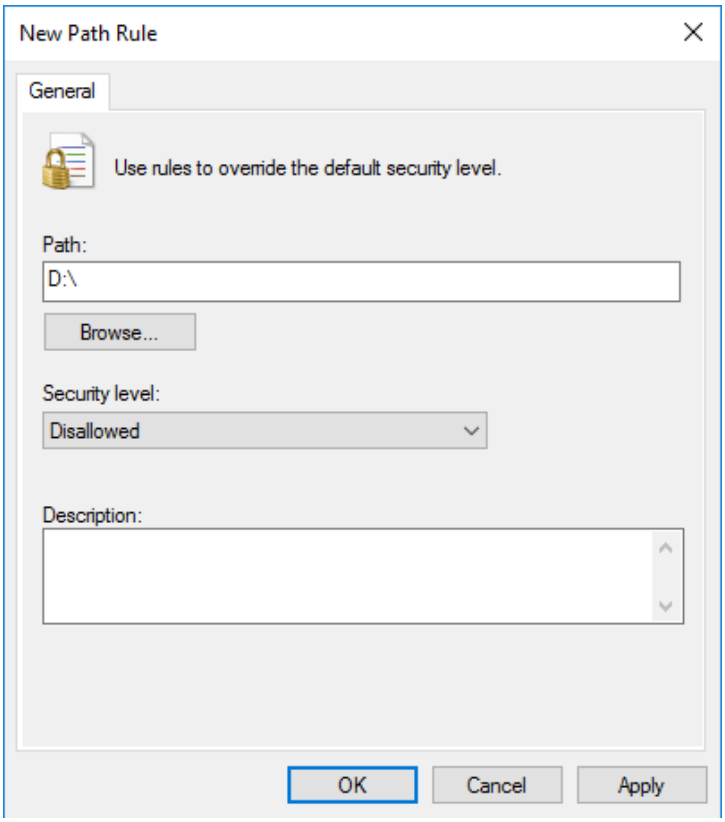

Рис. 15. Властивості правила обмеженого використання програм.

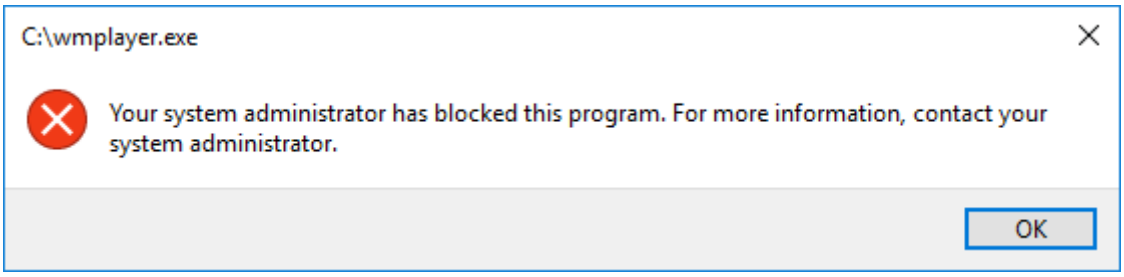

Рис. 16. Повідомлення системи про заборону виконання програми.

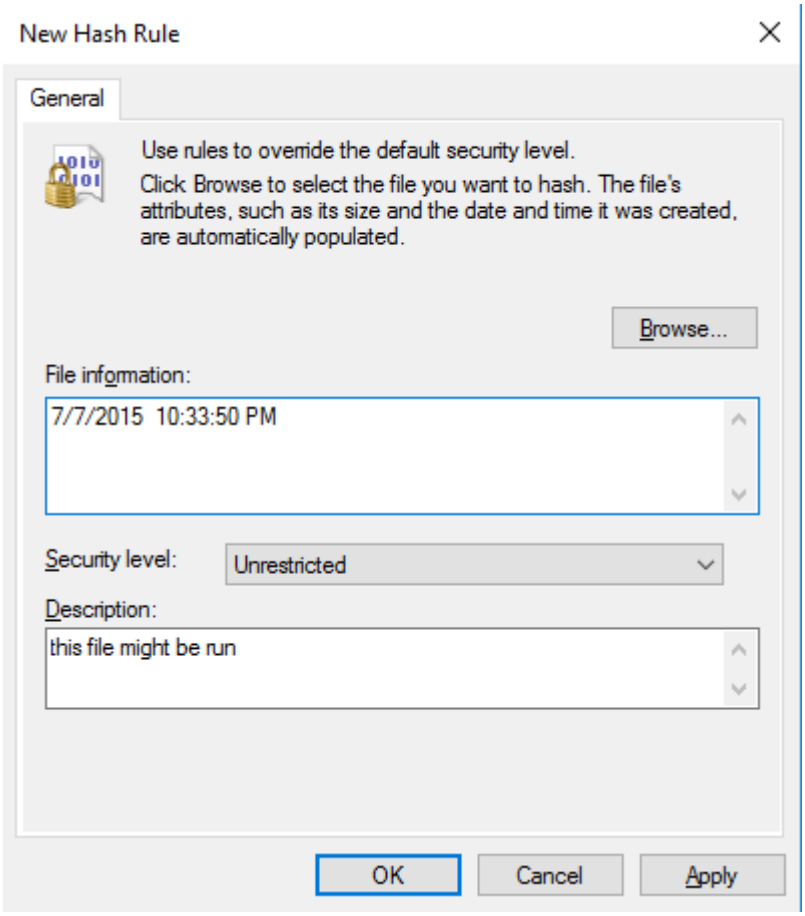

Рис. 17. Створення правила для хеша.

6. Відкрити оснастку mmc "Security Configuration and Analysis" (рис. 18). Створити нову базу даних, яка буде відображати стан налаштування політик комп’ютера за певним шаблоном.

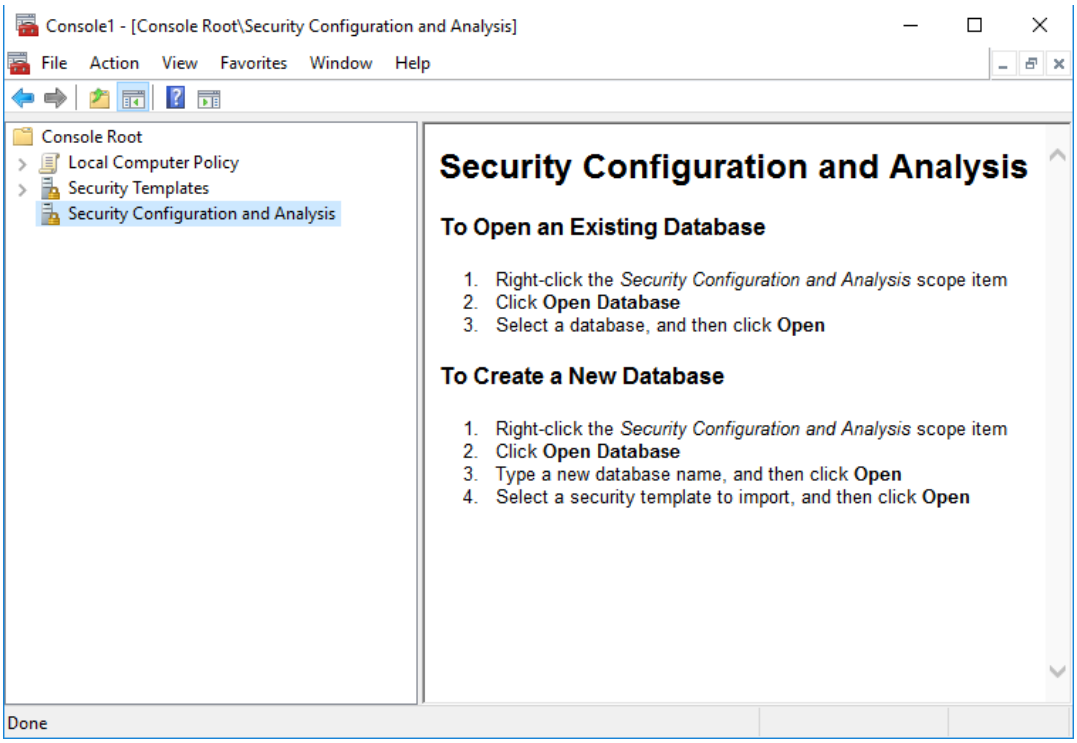

Рис. 18. Оснащення "Security Configuration and Analysis".

Власні шаблони створюються за допомогою оснастки "Security Templates" (рис. 19). Проаналізувати параметри безпеки комп'ютера (рис. 20). Результати аналізу відображаються як порівняння параметрів комп'ютера з параметрами шаблону (створеної бази даних) – рис. 21. Базу даних можна редагувати в цьому ж вікні, а потім вибрати пункт контекстного меню "Save" та, при потребі, експортувати відредагований шаблон безпеки.

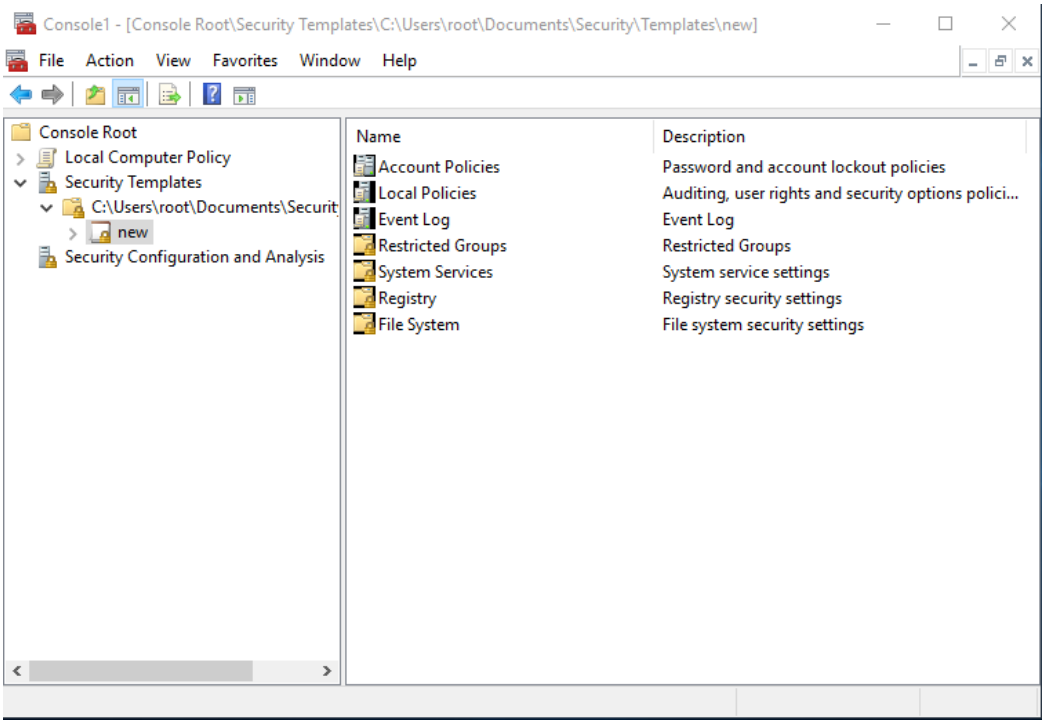

Рис. 19 Створення власних шаблонів.

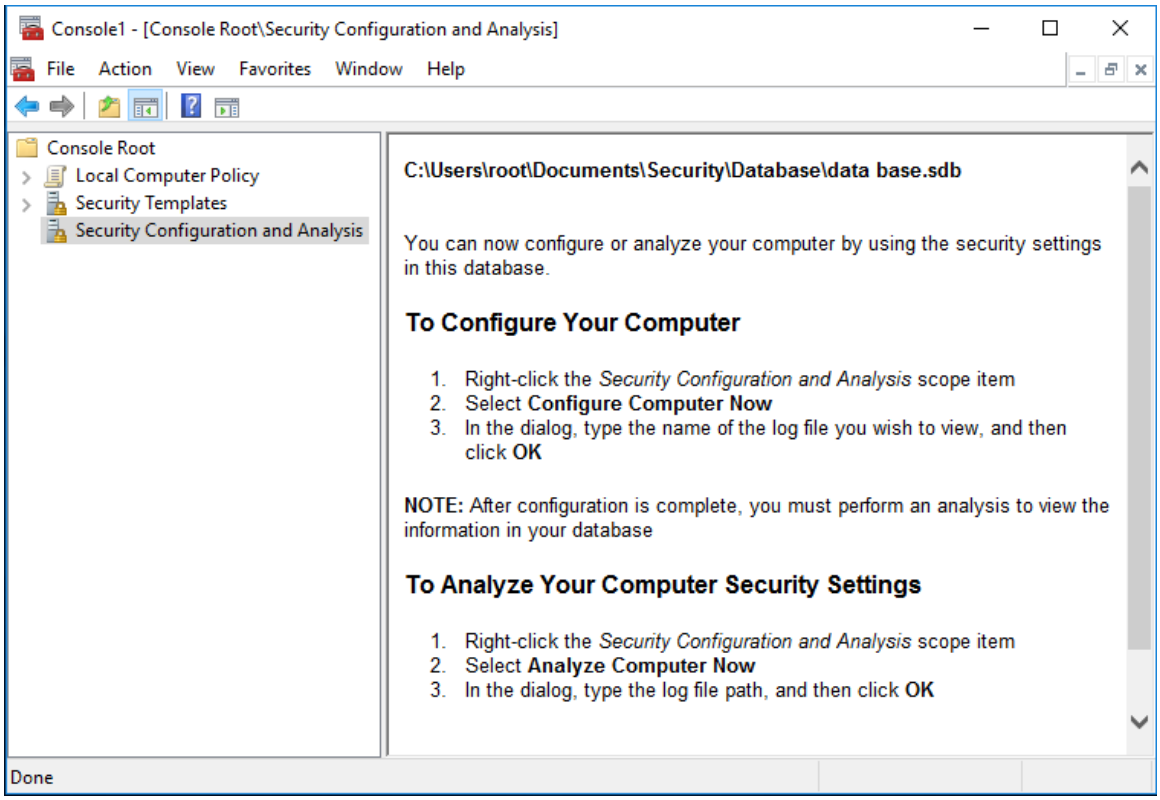

Рис. 20. Використання оснащення "Security Configuration and Analysis".

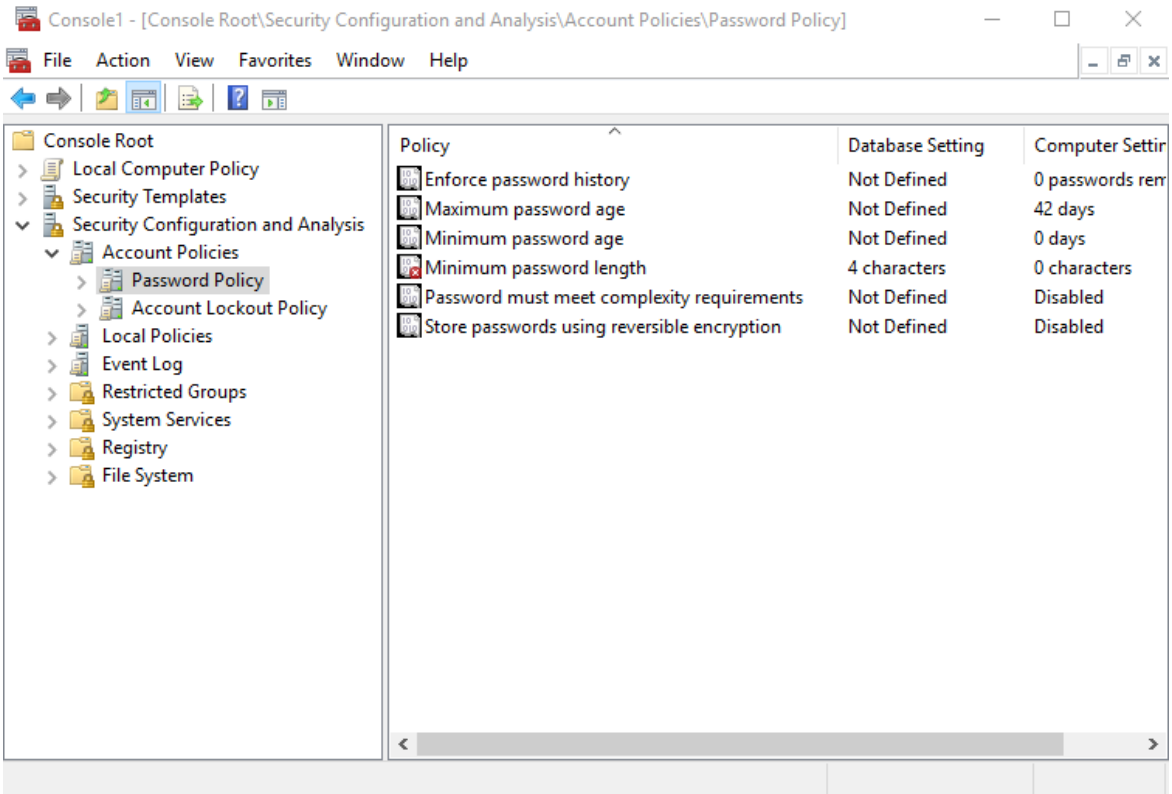

Рис. 21. Результат аналізу безпеки системи.

Налаштувати комп’ютер за певним, власним, шаблоном безпеки (привести у відповідність параметри бази даних і поточні налаштування комп’ютера), виконавши необхідні дії (рис. 20).

У звіті до лабораторної роботи описати та пояснити отримані результати.

Контрольні запитання.

1. Призначення групових політик.
2. Чим відрізняються гілки політики "Computer Configuration" та "User Configuration"?
3. Хто має привілей брати об’єкти у власність?
4. Порядок застосування групових політик в Active Directory.
5. Для чого використовуються шаблони безпеки?
6. Чи можна (і як) за допомогою політик бути впевненим у відсутності модифікацій програмного забезпечення після його встановлення на комп’ютер?

СПИСОК ЛІТЕРАТУРИ

1. **Microsoft Corporation** Microsoft Windows XP. Учебный курс MCSA/MCSE. – М.: Издательско-торговый дом "Русская Редакция", 2003. – 1008 стр.
2. **Ed Bott** Introduction Windows 10 for IT Professionals. – Published by Microsoft Press. A Division of Microsoft Corporation One Microsoft Way Redmond, Washington, 2015. – 115 p.
3. **Microsoft Corporation** Microsoft Windows 2000 Active Directory Services. Учебный курс MCSE. – М.: Издательско-торговый дом «Русская редакция», 2004. – 608 с.
4. **Руссинович М.**, **Соломон Д.** Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. – М.: Издательско-торговый дом «Русская редакция»; СПб.: Питер, 2005. – 992 с.
5. **Вишневский А**. Windows Server 2003. Для профессионалов. – СПб.: Питер, 2004. – 767 с.
6. **К. Айвенс** Microsoft Windows Server 2003. Полное руководство. – М.: Издательство "СП ЭКОМ", 2004.– 896 с.

НАВЧАЛЬНЕ ВИДАННЯ

НАЛАШТУВАННЯ БЕЗПЕКИ У WINDOWS 10

МЕТОДИЧНІ ВКАЗІВКИ
до виконання лабораторної роботи
з дисципліни „Основи системного адміністрування ”
для студентів напряму 6.050103 «Програмна інженерія» та
спеціальності 121 „Інженерія програмного забезпечення ”

Укладачі Яковина В.С., доцент кафедри ПЗ
Муха Т.О., асистент кафедри ПЗ
Шкраб Р.Р., асистент кафедри ПЗ

Редактор

Комп’ютерне верстання