

## T: Zasady grup w systemie Windows.

### Zadanie1:

Wyjaśnij następujące pojęcia: GPO (Group Policy Objects), GPOE (Group Policy Objects Editor) oraz GPM (Group Policy Management).

Zasady grupy (ang. Group Policies) to obiekty zawierające zbiory ustawień konfiguracyjnych systemu. Zasady te obejmują ustawienia dla komputera oraz dla użytkownika. Dzięki zasadom grup można skonfigurować elementy systemu Windows począwszy od instalacji oprogramowania przez konfigurację środowiska użytkownika po zaawansowane opcje zabezpieczeń. Ustawienia zasad grup są przechowywane w obiektach GPO (ang. Group Policy Object). Obiekty GPO mogą być lokalne dla komputera lub domenowe, przechowywane w usłudze Active Directory. Jeżeli komputer należy do grupy roboczej dotyczą go wyłącznie ustawienia lokalnych zasad grup, natomiast, gdy należy do domeny, na konfigurację komputera wpływają również obiekty GPO stworzone przez administratora domeny. Wszystkie zasady grupy zostały podzielone na dwie zasadnicze części Konfiguracja komputera i Konfiguracja użytkownika. Pierwsze ustawienia dotyczą parametrów komputera, które są ładowane podczas startu systemu jeszcze przed logowaniem użytkownika. Drugie dotyczą ustawień specyficznych dla użytkownika i są ładowane w momencie logowania do systemu.

Przystawka Zasady grupy dostępna w systemie Microsoft® Windows 2003 Server służy do zarządzania następującymi funkcjami:

- Instalacja oprogramowania,
- Szablony administracyjne,
- Przekierowanie folderu,
- Usługi instalacji zdalnej,
- Ustawienia zabezpieczeń,
- Skrypty (uruchamiania/zamykania i logowania/wylogowania),
- Konserwacja programu Internet Explorer.

Przystawka Zasady grupy pozwala zdefiniować ustawienia zasad, które będą stosowane do komputerów lub użytkowników.

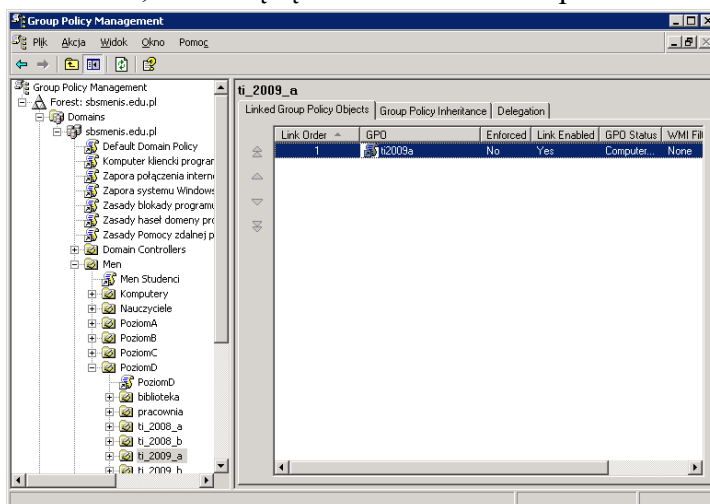
### Konsole administracyjne:

- Edytor Zasad grupy (gpedit.msc),
- Zasady zabezpieczeń lokalnych (secpol.msc),
- Wynikowy zestaw zasad (rsop.msc),
- Zarządzanie zasadami grup (Group Policy Management – na kontrolerze domeny).

Zasady zabezpieczeń można edytować za pomocą konsoli administracyjnej **Zasady grupy** (gpedit.msc) lub otwierając pustą konsolę **mmc.exe** i dołączając do niej przystawkę **Edytor obiektów zasad grupy**.

Przystawka pozwala zdefiniować ustawienia zasad, które będą stosowane do komputerów lub użytkowników. Dostępne ustawienia w konsoli Zasady grupy można dodawać bądź usuwać poprzez tzw. **Szablony administracyjne**. Aktualnie wykorzystywane w konsoli szablony administracyjne zapisane są w postaci plików z rozszerzeniem **\*.adm** znajdujących się w katalogu %Systemroot%\System32\GroupPolicy\Adm. Szablony administracyjne, które możemy dodać do konsoli Zasady grupy znajdują się w systemie w katalogu %Systemroot%\inf lub możemy pobrać je bezpłatnie ze stron internetowych firmy Microsoft.

W celu wprowadzenia zasad dla użytkowników komputera należy zalogować się jako administrator i wprowadzić odpowiednie ustawienia zasad zabezpieczeń. Następnie każdy z użytkowników, którego mają dotyczyć wprowadzone zmiany powinien zostać zalogowany w systemie. Lokalne zasady zabezpieczeń zapisane są w pliku %Systemroot%\System32\GroupPolicy\User\Registry.pol dla użytkownika oraz w pliku %Systemroot%\System32\GroupPolicy\Machine\Registry.pol dla komputera. Jeżeli chcemy, aby ograniczenia nie dotyczyły administratora należy po przeprowadzeniu aktualizacji zasad dla użytkowników (logowanie)

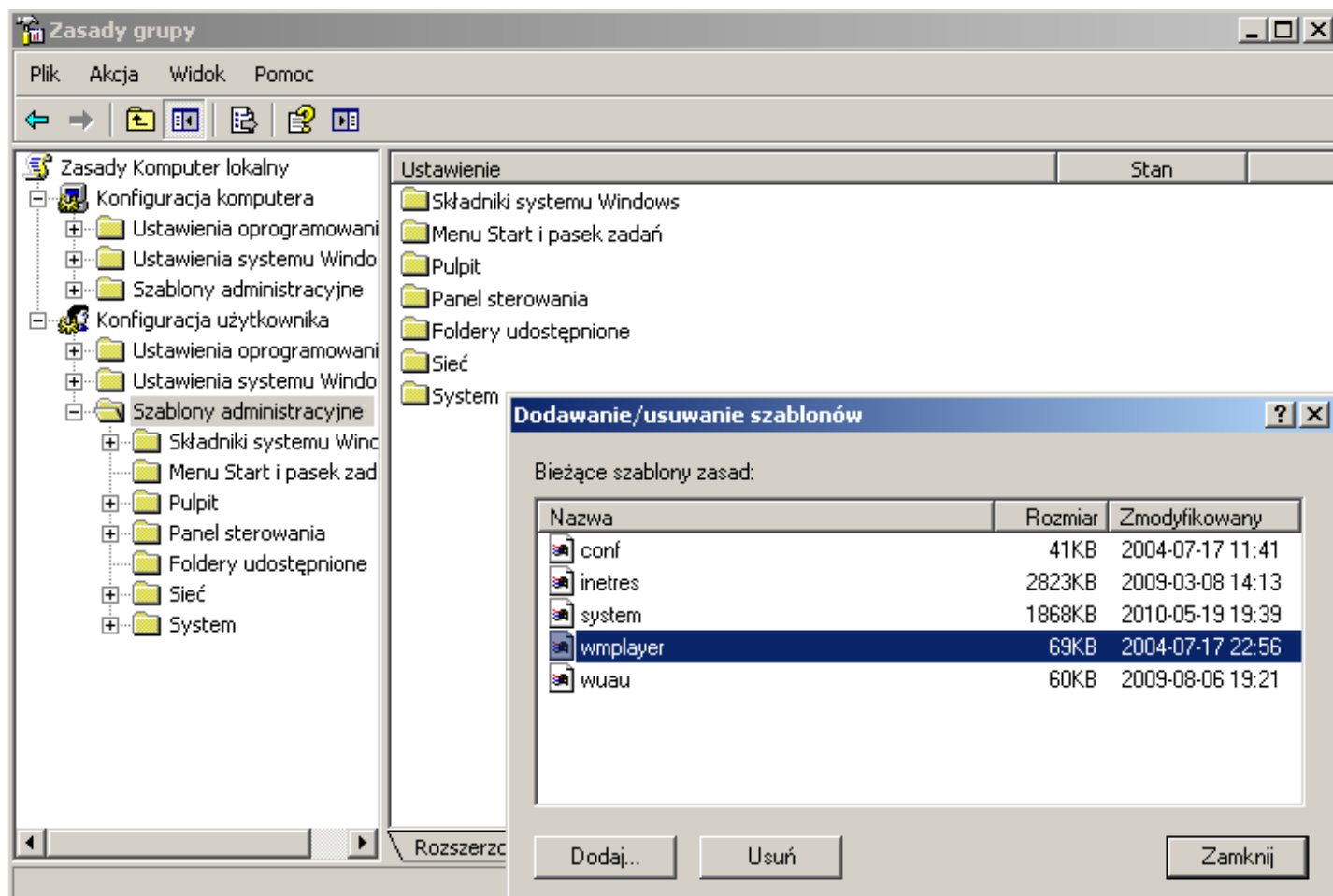


zalogować się na konto administratora, skopiować plik registry.pol, powrócić do edytora zasad zabezpieczeń i cofnąć ograniczenia, zamknąć edytor zasad grup i skopiowanym wcześniej plikiem zastąpić nowy registry.pol (po zamknięciu konsoli powstał nowy plik).

W przypadku problemów z zabezpieczeniami (np. niepoprawna konfiguracja) można przywrócić ustawienia domyślne zasad grup. W tym celu należy usunąć istniejący plik registry.pol lub zmienić jego nazwę i ponownie uruchomić komputer. System ochrony plików spowoduje przywrócenie domyślnego pliku registry.pol.

Przy użyciu przystawki Zasady grupy można wykonywać następujące czynności:

- **Zarządzać zasadami opartymi na rejestrze**, za pomocą Szablonów administracyjnych. Przystawka Zasady grupy tworzy plik zawierający ustawienia rejestru, które są zapisywane w części User lub Local Machine bazy danych rejestru. Ustawienia profilu użytkownika właściwe dla użytkownika, który loguje się na danej stacji roboczej lub serwerze, są zapisywane w rejestrze w kluczu HKEY\_CURRENT\_USER (HKCU), a ustawienia właściwe dla komputera są zapisywane w kluczu HKEY\_LOCAL\_MACHINE (HKLM).
- **Przypisywać skrypty**. Znajdują się tu takie skrypty, jak uruchamianie komputera, zamykanie komputera oraz operacje logowania i wylogowywania.
- **Przekierowywać foldery**. Można przekierować foldery, takie jak Moje dokumenty i Moje obrazy, z folderu Documents and Settings na komputerze lokalnym do lokalizacji sieciowych.
- **Zarządzać aplikacjami**. Używając rozszerzenia Instalacja oprogramowania przystawki Zasady grupy, można przypisywać, publikować, aktualizować lub naprawiać aplikacje.
- **Określać opcje zabezpieczeń**.



Za pomocą przystawki **Ustawienia zabezpieczeń** można modyfikować zasady zabezpieczeń jednostki organizacyjnej, domeny lub lokacji z dowolnego komputera dołączonego do domeny. Ustawienia zabezpieczeń pozwalają administratorowi zabezpieczeń modyfikować ustawienia zabezpieczeń przypisane do obiektu zasad grupy.

Konto komputera powinno być dodane do właściwości zabezpieczeń obiektu GPO tworzonego do sprzężenia zwrotnego. Aby to zrobić, wykonaj następujące kroki:

1. Zaznacz obiekt GPO utworzony do sprzężenia zwrotnego, a następnie kliknij polecenie **Właściwości**.
2. Kliknij kartę **Zabezpieczenia**, a następnie kliknij przycisk **Dodaj**.
3. W oknie dialogowym **Wybieranie: Użytkownicy, Komputery lub Grupy** zaznacz konto komputera, a następnie kliknij przycisk **OK**.
4. Kliknij konto komputera w polu **Nazwy grupy lub użytkownika**.
5. W polu **Uprawnienia dla nazwa komputera** kliknij, aby zaznaczyć pola wyboru **Odczyt** i **Stosowanie zasad grupy** w kolumnie **Zezwalaj**.
6. Kliknij przycisk **OK** dwa razy, aby zamknąć i zapisać ustawienia zasad.

### Aby utworzyć nowy obiekt zasad grupy

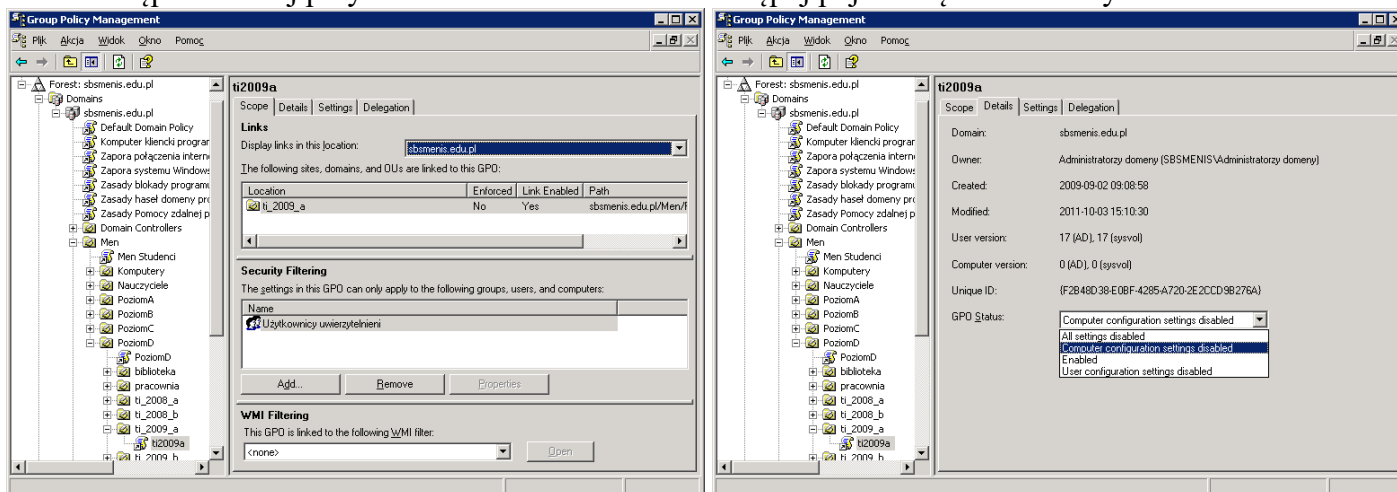
1. Wykonaj jedną z następujących czynności:
  - Aby utworzyć obiekt zasad grupy połączony z domeną lub jednostką organizacyjną, otwórz przystawkę Użytkownicy i komputery usługi Active Directory.
  - Aby utworzyć obiekt zasad grupy połączony z lokacją, otwórz przystawkę Lokacje i usługi Active Directory.
2. W drzewie konsoli kliknij prawym przyciskiem myszy lokację, domenę lub jednostkę organizacyjną, z którą ma być połączony nowy obiekt zasad grupy. Obiekt zasad grupy będzie przechowywany w domenie bieżącej, czyli w domenie, w której znajduje się kontroler domeny wykorzystywany przez przystawkę Użytkownicy i komputery usługi Active Directory lub przystawkę Lokacje i usługi Active Directory.
3. Kliknij polecenie **Właściwości**, a następnie kliknij kartę **Zasady grupy**.
4. Kliknij opcję **Nowy**, wpisz nazwę obiektu zasad grupy, a następnie kliknij przycisk **Zamknij**.

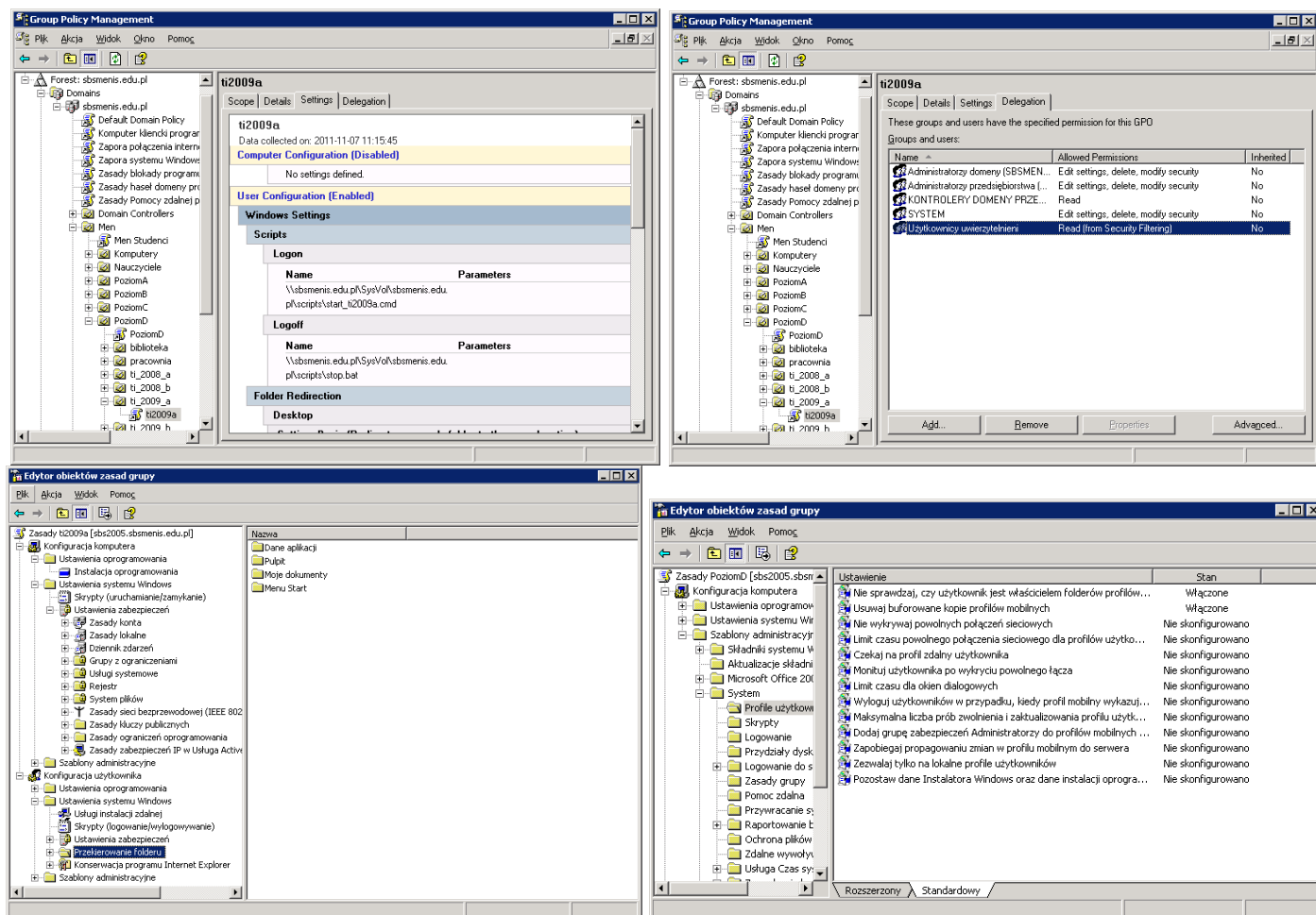
### Aby zablokować dziedziczenie zasad

1. Aby zablokować dziedziczenie zasad w domenie lub jednostce organizacyjnej, otwórz przystawkę **Użytkownicy i komputery usługi Active Directory**.
2. W drzewie konsoli kliknij prawym przyciskiem myszy **domenę** lub **jednostkę organizacyjną**, w której chcesz zablokować dziedziczenie zasad grupy, a następnie kliknij polecenie **Właściwości**.
3. Kliknij kartę **Zasady grupy**, zaznacz pole wyboru **Zablokuj dziedziczenie zasad**, a następnie kliknij przycisk **OK**. Jest to opcja zalecana i jest ona wybrana domyślnie.

### Aby zapobiec zastąpieniu obiektu zasad grupy

1. Właściwości jednostki => Karta **Zasady grupy** => Na liście Łącza obiektu zasad grupy kliknij prawym przyciskiem myszy łącze obiektu zasad grupy, które chcesz wymusić, kliknij polecenie **Nie zastępuj**, a następnie kliknij przycisk **OK**. W kolumnie **Nie zastępuj** pojawi się znacznik wyboru.





## Zadanie2:

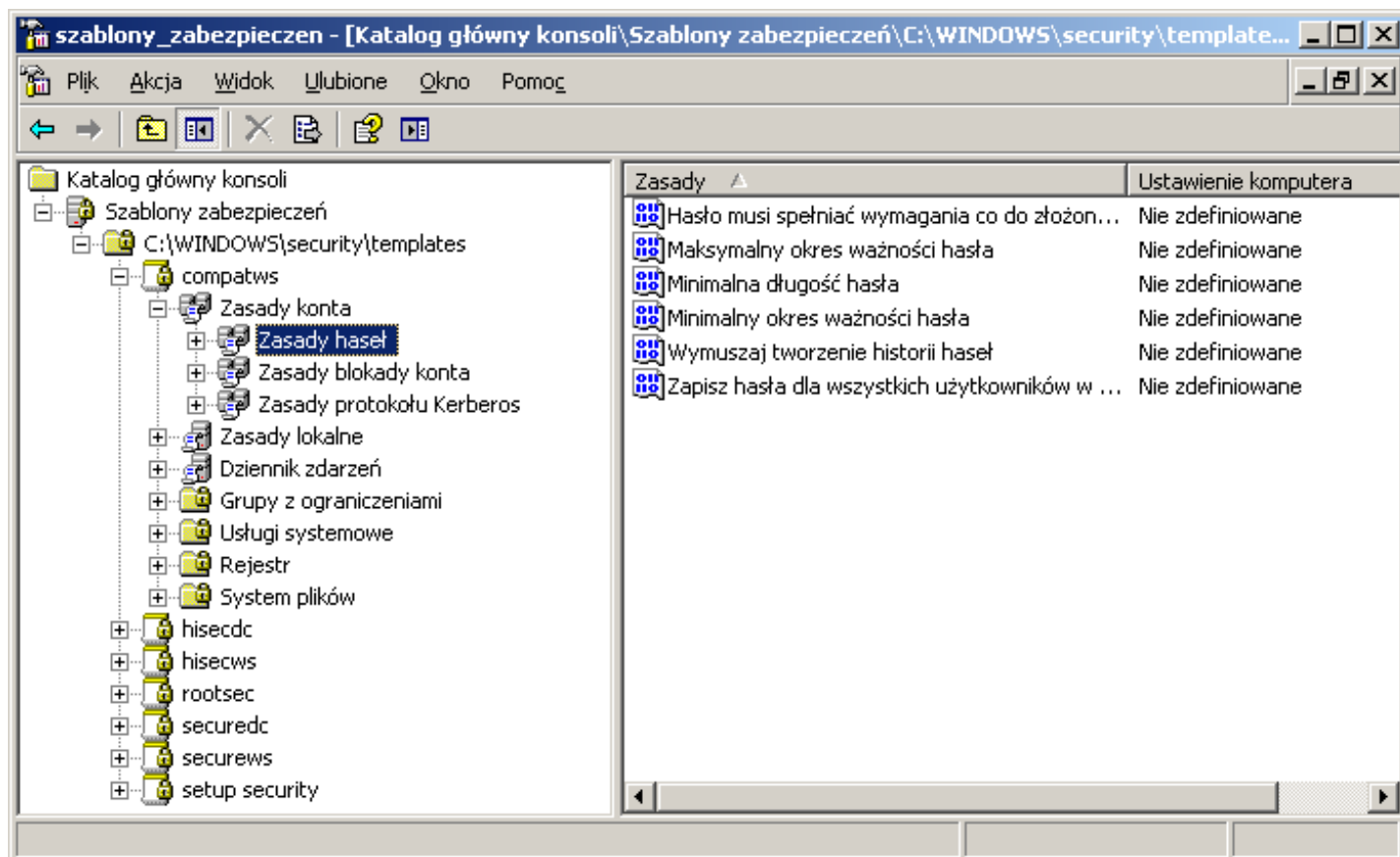
Utwórz dokument w programie MS Word, w którym wymienisz i uzasadnisz dziesięć ustawień zabezpieczeń dostępnych w edytorze Zasad grupy (gpedit.msc) w systemie MS Windows XP Professional, które twoim zdaniem warto wprowadzić dla użytkowników pracujących w domenie Windows. Ustawienia należy ograniczyć do kategorii Szablonów administracyjnych dostępnych w Ustawieniach użytkownika. Pracę zachowaj pod nazwą \$nazwisko\_zabezpieczenia.doc na dysku h: w katalogu asso lub prześlij pocztą elektroniczną do nauczyciela na adres [greszata@zs9elektronik.pl](mailto:greszata@zs9elektronik.pl).

Dopuszcza się możliwość utworzenia do powyższego zadania prezentacji w programie MS PowerPoint. W prezentacji należy zamieścić następujące elementy:

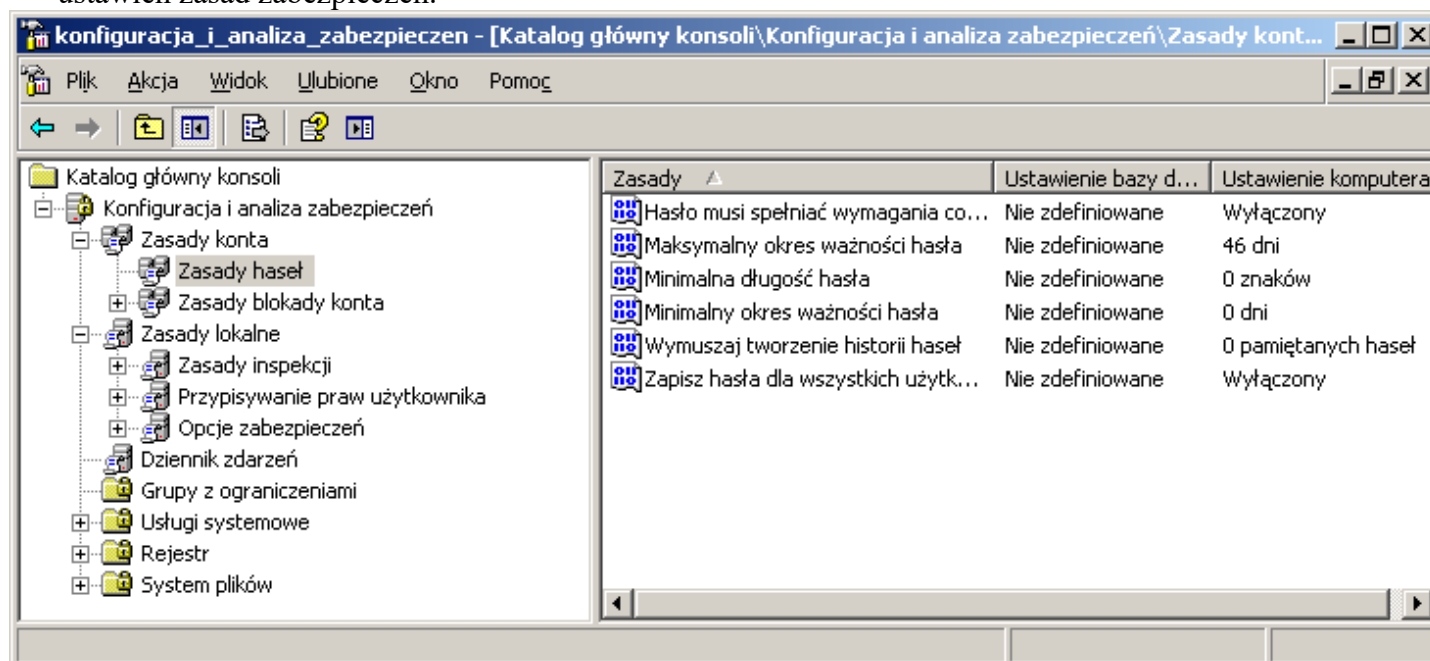
- slajd tytułowy,
- slajd wyjaśniający zagadnienie zasad zabezpieczeń i edytora Zasad grupy,
- slajdy z poszczególnymi ustawieniami zabezpieczeń zawierające odpowiednio dopasowany zrzut ekranowy z danym ustawieniem i uzasadnieniem zastosowania danego ustawienia w domenie,
- slajd zakończeniowy.

Wyróżniamy następujące narzędzia zasad zabezpieczeń:

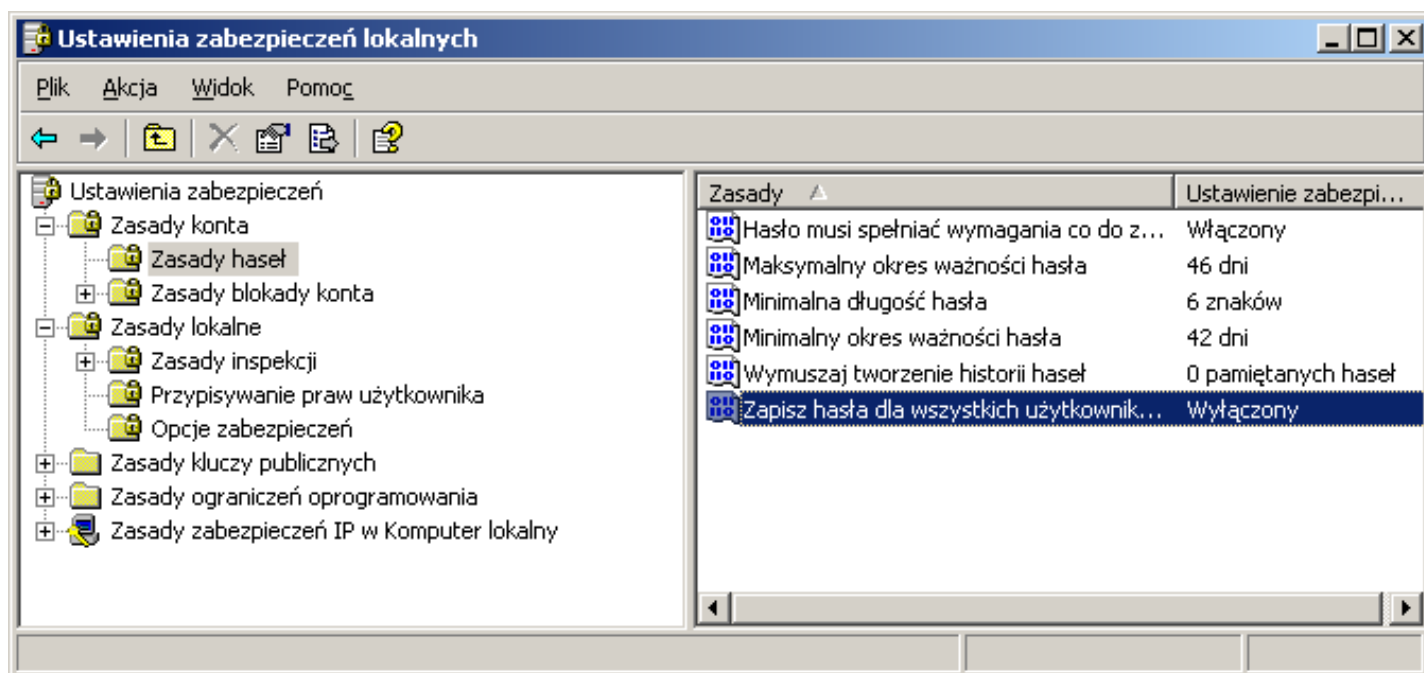
- **Szablony zabezpieczeń** - W szablonie można zdefiniować zasady zabezpieczeń. Szablony można stosować do obiektu zasad grupy lub do zabezpieczeń komputera lokalnego. Przykładowe ustawienia zabezpieczeń zdefiniowane są w szablonach zabezpieczeń zapisanych w katalogu %Systemroot%\Security\Templates.



- **Konfiguracja i analiza zabezpieczeń** - Tego narzędzia można używać do konfigurowania komputera za pomocą szablonu zabezpieczeń lub do porównywania aktualnych ustawień komputera z ustawieniami zdefiniowanymi w szablonie zabezpieczeń. Niezbędne bazy danych lub szablony zabezpieczeń znajdziemy w katalogu: c:\Windows\security. Przystawka konfiguracja i analiza zabezpieczeń umożliwia przywrócenie ustawień zasad zabezpieczeń.



- **Zasady zabezpieczeń lokalnych** - Tego narzędzia można używać do edytowania poszczególnych ustawień zabezpieczeń na komputerze lokalnym. Lokalne zasady zabezpieczeń zapisane są w pliku %Systemroot%\System32\GroupPolicy\User\Registry.pol dla użytkownika oraz w pliku %Systemroot%\System32\GroupPolicy\Machine\Registry.pol dla komputera.



Za pomocą konsoli Zasady zabezpieczeń lokalnych (ang. Local security policy) użytkownik z uprawnieniami administratora może dowolnie skonfigurować zasady bezpieczeństwa komputera lokalnego. Zostały one podzielone na następujące grupy:

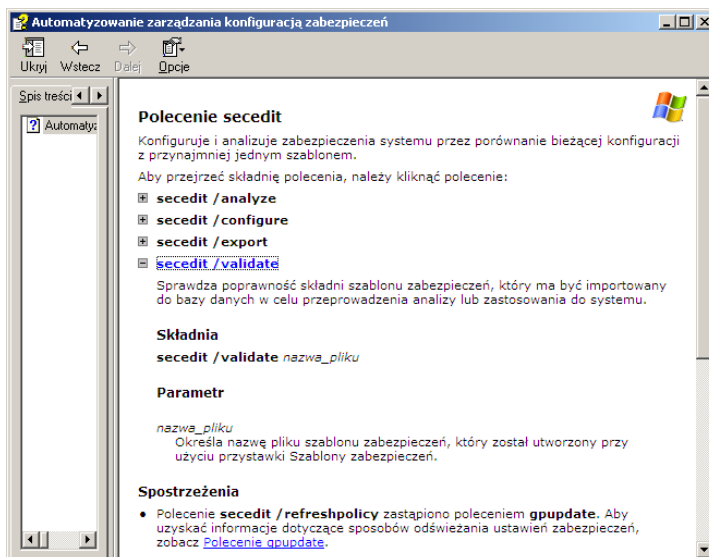
- Zasady konta – ustawienia blokowania konta oraz zasady haseł.
  - Zasady lokalne – obejmujące zasady inspekcji, opcje zabezpieczeń i przypisywanie praw użytkownika.
  - Zasady kluczy publicznych – ustawienia szyfrowania plików.
  - Zasady ograniczeń oprogramowania,
  - Zasady zabezpieczeń IP.
- **Polecenie secedit** - Tego narzędzia można używać do automatyzowania zadań związanych z konfiguracją i analizą zabezpieczeń systemu przez porównanie bieżącej konfiguracji z szablonami zabezpieczeń za pomocą wiersza poleceń.

secedit /?

```
secedit /configure /DB Nazwa_pliku /CFG
"%windir%\Security\Templates\Setup security.inf"
[/overwrite][/areasObszar1 Obszar2...]
[/logŚcieżka_dziennika] [/quiet]
```

**Porada:** Do działań administracyjnych warto przygotować globalną konsolę administracyjną (za pomocą konsoli **mmc**). Taka konsola powinna zawierać następujące przystawki:

- .NET Framework Configuration,
- Dzienniki wydajności i alerty,
- Group Policy Management,
- Konfiguracja i analiza zabezpieczeń,
- Menedżer autoryzacji,
- Monitor sieci bezprzewodowej,
- Pulpity zdalne,
- Rozproszony system plików (DFS),
- Szablony zabezpieczeń,
- Przystawki do zarządzania Active Directory,
- Urząd certyfikacji,



- Usługi składowe,
- Wynikowy zestaw zasad.

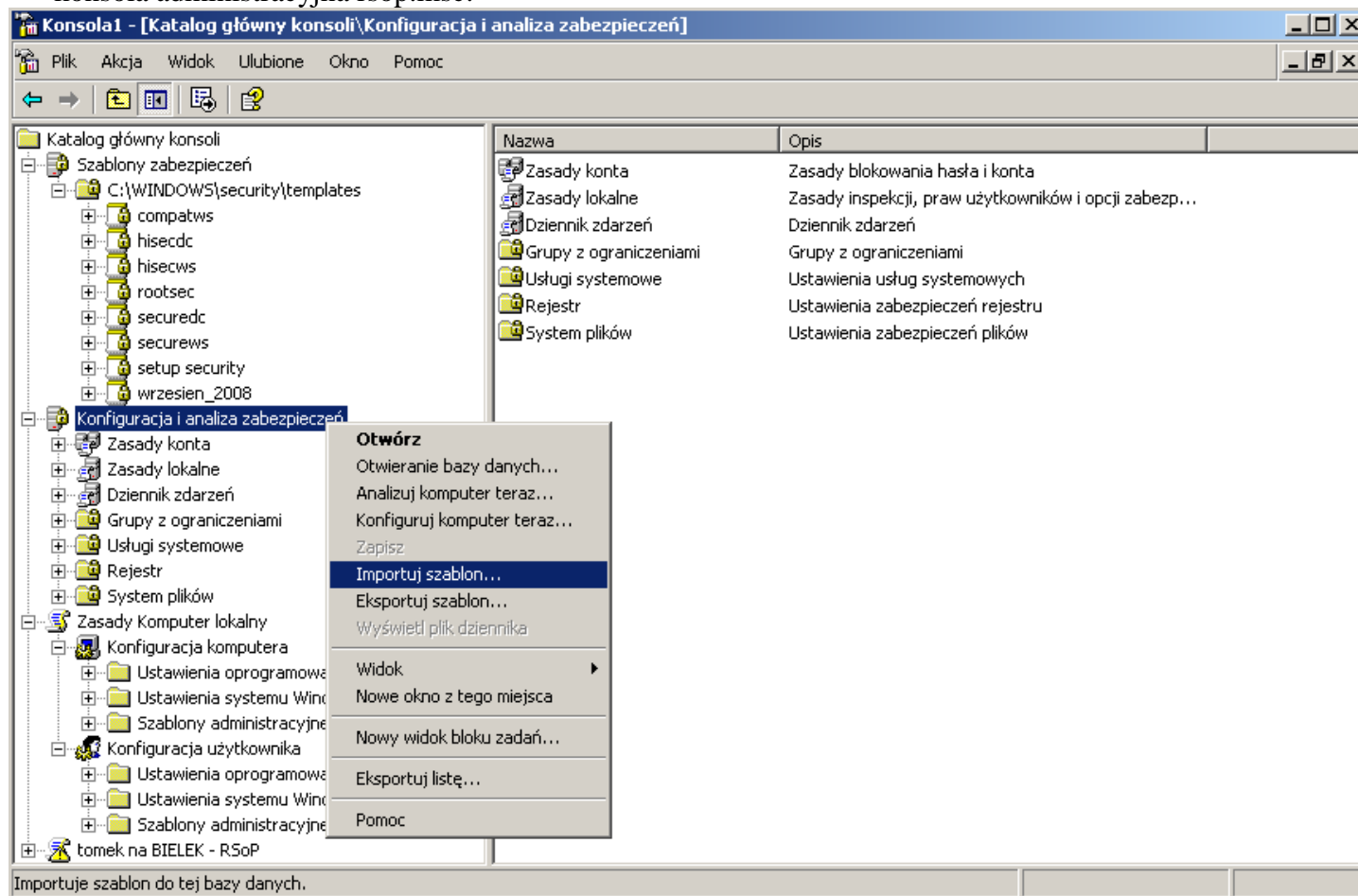
W celu przygotowania konsoli należy wykonać:

```
Start => Uruchom => mmc /a %SystemRoot%\system32\compmgmt.msc
```

Spowoduje to uruchomienie konsoli Zarządzanie komputerem w trybie do edycji. Nową konsolę zapisujemy pod nową nazwą w katalogu c:\Toolkit.

Polecenia do samodzielnego przeanalizowania:

- **gpupdate /force**,
- **gpreult /user login**,
- konsola administracyjne **gpedit.msc**,
- konsola administracyjna **rsop.msc**.



Zadanie3:

Wykorzystując maszynę wirtualną z systemem Windows 2016 Server oraz narzędzie Edytor zasad grupy przeprowadź konfigurację systemu Windows wg następujących wytycznych:

- ustaw tapetę pulpitu na dowolny plik graficzny z katalogu systemowego Web,
- ukryj ustawienia myszy w Panelu sterowania,
- zablokuj przenoszenie usuniętych plików do kosza,
- zabroń uruchamiania wiersza poleceń (cmd.exe),
- wymuszaj uruchamianie notatnika podczas logowania użytkowników do systemu,
- usuń polecenie Uruchom z menu Start.
- **wyłącz zapórę Windows Defender dla wszystkich profili sieciowych,**
- **zastosuj domyślny awatar dla kont użytkowników,**
- **uruchamiaj skrypt c:\start.cmd podczas uruchamiania komputera,**
- **wymuszaj stosowania limitu przydziałów dyskowych dla wszystkich użytkowników,**
- **nie wymagaj naciśnięcia klawiszy Ctrl + Alt + Del podczas logowania do systemu,**
- **nie zezwalaj na zapisywanie plików w usłudze OneDrive.**

Z wykonanych działań wykonaj zrzuty ekranowe, zapisz je oraz krótko opisz w pliku pod nazwą **\$nazwisko\_\$klasa\_\$gr\_gpedit.docx**. Utworzony plik prześlij pocztą elektroniczną do nauczyciela w postaci załącznika na adres [greszata@zs9elektronik.pl](mailto:greszata@zs9elektronik.pl).