

# **Zasady bezpieczeństwa**

## **Polityka haseł**

# Efektywne stosowanie haseł

- Musimy zdać sobie sprawę jak ważne są silne hasła. Cały rozbudowany mechanizm bezpieczeństwa systemu Windows staje się bezradny w przypadku jeśli napastnik zaloguje się jako użytkownik o nieograniczonych możliwościach.
- Hasła są elementarnym narzędziem mającym na celu pomagać systemowi weryfikować użytkownika.

# Tworzenie silnych haseł



Typowym błędem użytkowników komputerów jest, że jako haseł używają imion, ulubionych nazwy, miejsca, dat.



## Najpopularniejsze hasła w 2015 roku:

- 123456
- password
- 12345678
- qwerty
- 12345
- 123456789
- football
- 1234
- 1234567
- baseball
- welcome
- 1234567890
- abc123
- 111111
- 1qaz2wsx
- dragon
- master
- monkey
- letmein
- login
- princess
- qwertyuiop
- solo
- passw0rd
- starwars

# Tworzenie silnych haseł

- Dodatkowo powinien być okresowo zmieniany i nikomu poza nami nie może być znany.



# Zemsta doskonała



# Zemsta doskonała

Możesz mi powiedzieć  
jakie jest nowe hasło?

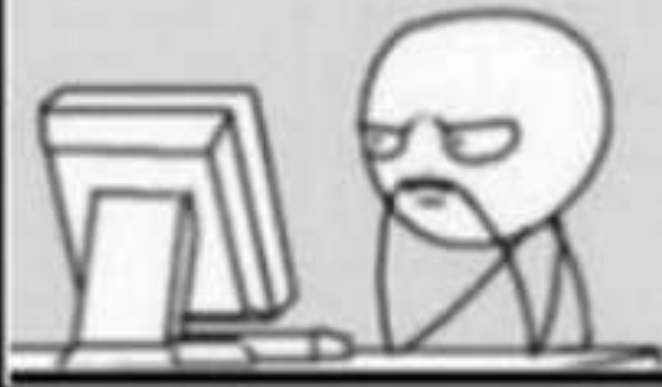
Data naszej  
pierwszej  
randki  
kochanie





# Zemsta doskonała

Godzine po namyślaniu



## Zemsta

Doskonała

# Tworzenie silnych haseł

- Do wykorzystania mamy dowolne znaki, także spacje. Stosowanie spacji w hasłach pomaga tworzyć długie frazy. Jednak nie należy używać spacji jako pierwszego lub ostatniego znaku, gdyż niektóre aplikacje obcinają te pozycje.

# Tworzenie silnych haseł

- Tworzenie hasła wykorzystując jakąś frazę:

"Juventus Turyn **wygrał z AC Milan 2-1**",  
tworzę hasło: "JT**wz**AM2-1".

Password:

\*\*\*\*\*

DEMOTYWATOR.PL

Przepraszamy, twoje hasło musi zawierać - przynajmniej jedną wielką literę, dwie cyfry, jakiś symbol, ukrytą wiadomość, tajemne zaklęcie, hieroglif egipski i włos jednorozca

Przyznaj, że też nienawidzisz, kiedy to się dzieje



*Hasła są jak majtki – należy je  
zmieniać często, nie zostawiać na  
widoku i nie pożyczać obcym.*

**GIODO**

# Tworzenie haseł konsola

**net user użytkownik hasło**

- Zamiast *hasło* możemy wpisać jedną z trzech wartości:

# Tworzenie haseł konsola

1) Ustalone hasło

```
WINDOWS\system32>net user kasia tajne
```

# Tworzenie haseł konsola

- 2) \* - System poprosi o wpisanie hasła,  
dobra opcja kiedy my tworzymy konto a  
użytkownik sam wpisuje sobie kod;

```
C:\WINDOWS\system32>net user kasia *  
Wpisz hasło dla użytkownika:  
Wpisz hasło ponownie w celu potwierdzenia:  
Polecenie zostało wykonane pomyślnie.
```



# Tworzenie haseł konsola

3) */random* - System sam wygeneruje 8-znakowe hasło i je wyświetli.

```
C:\WINDOWS\system32>net user kasia /random
Hasło dla kasia to: c$SpaLTf
Polecenie zostało wykonane pomyślnie.
```

# Klasyfikacja metod uwierzytelniania

- Użytkownicy mogą być uwierzytelniani na podstawie jednej lub kilku informacji pochodzących z następujących zbiorów:
- **Tego, co użytkownik wie** - tajny tekst np. hasło znane tylko użytkownikowi i systemowi.  
W procesie rejestracji jest ono wprowadzane przez użytkownika i sprawdzane przez system.

# Klasyfikacja metod uwierzytelniania

- **Tego, co użytkownik posiada** - klucz, plakietka, karta pomagające w weryfikacji użytkownika. W metodzie hasło-odzew (*challenge-response*) użytkownik dysponuje kartą wyświetlającą identyfikator liczbowy. Można stosować również metodę haseł jednorazowych.

# Klasyfikacja metod uwierzytelniania

- **Tego, kim użytkownik jest** (techniki biometryczne) –
- cechy fizyczne (odciski palców, odciski dłoni, wzorzec siatkówki) lub
- behawioralne (wzorzec głosu, podpis), które można zapamiętać i porównać.

# Zasady zabezpieczeń lokalnych przystawka secpol.msc

- Przystawka **secpol.msc** pozwala na zarządzanie zabezpieczeniami na komputerze. Pozwala m.in. na ustawianie zasad logowania i tworzenia haseł oraz na przypisywanie praw użytkownikom i grupom.

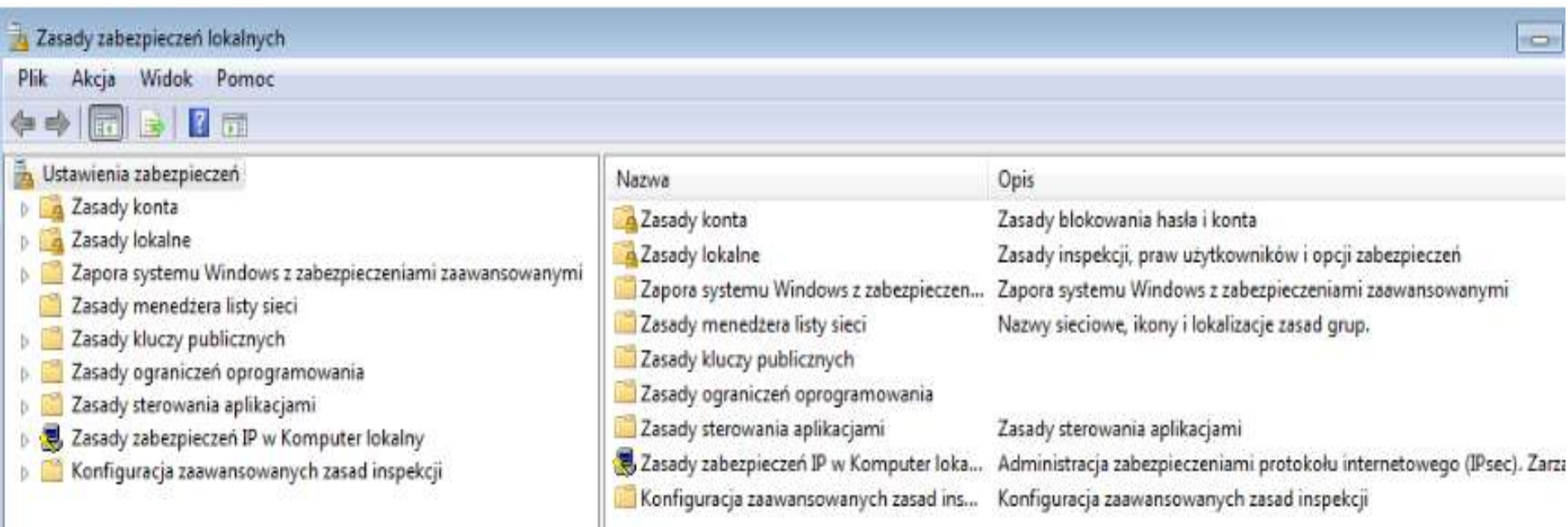
# Zasady zabezpieczeń lokalnych

## przystawka secpol.msc

- Przystawkę secpol.msc uruchamiamy za pomocą narzędzia uruchom ( akcesoria systemu)
- Lub przez konsolę wpisując polecenie secpol.msc

# Zasady zabezpieczeń lokalnych przystawka secpol.msc

## Główne okno przystawki



Ustawienia zabezpieczeń

- Zasady konta
- Zasady lokalne
- Zapora systemu Windows z zabezpieczeniami zaawansowanymi
- Zasady menedżera listy sieci
- Zasady kluczy publicznych
- Zasady ograniczeń oprogramowania
- Zasady sterowania aplikacjami
- Zasady zabezpieczeń IP w Komputer lokalny
- Konfiguracja zaawansowanych zasad inspekcji

Nazwa	Opis
Zasady konta	Zasady blokowania hasła i konta
Zasady lokalne	Zasady inspekcji, praw użytkowników i opcji zabezpieczeń
Zapora systemu Windows z zabezpieczeniami zaawansowanymi	Zapora systemu Windows z zabezpieczeniami zaawansowanymi
Zasady menedżera listy sieci	Nazwy sieciowe, ikony i lokalizacje zasad grup.
Zasady kluczy publicznych	
Zasady ograniczeń oprogramowania	
Zasady sterowania aplikacjami	Zasady sterowania aplikacjami
Zasady zabezpieczeń IP w Komputer lokalny	Administracja zabezpieczeniami protokołu internetowego (IPsec). Zarz...
Konfiguracja zaawansowanych zasad inspekcji	Konfiguracja zaawansowanych zasad inspekcji

# Zasady zabezpieczeń lokalnych przystawka secpol.msc

- W oknie **secpol.msc** widzimy listę folderów, których zawartość pozwala nam na administrowanie lokalnymi zabezpieczeniami komputera:
  - Zasady konta
  - Zasady lokalne
  - Zapora systemu Windows zabezpieczeniami zaawansowanymi

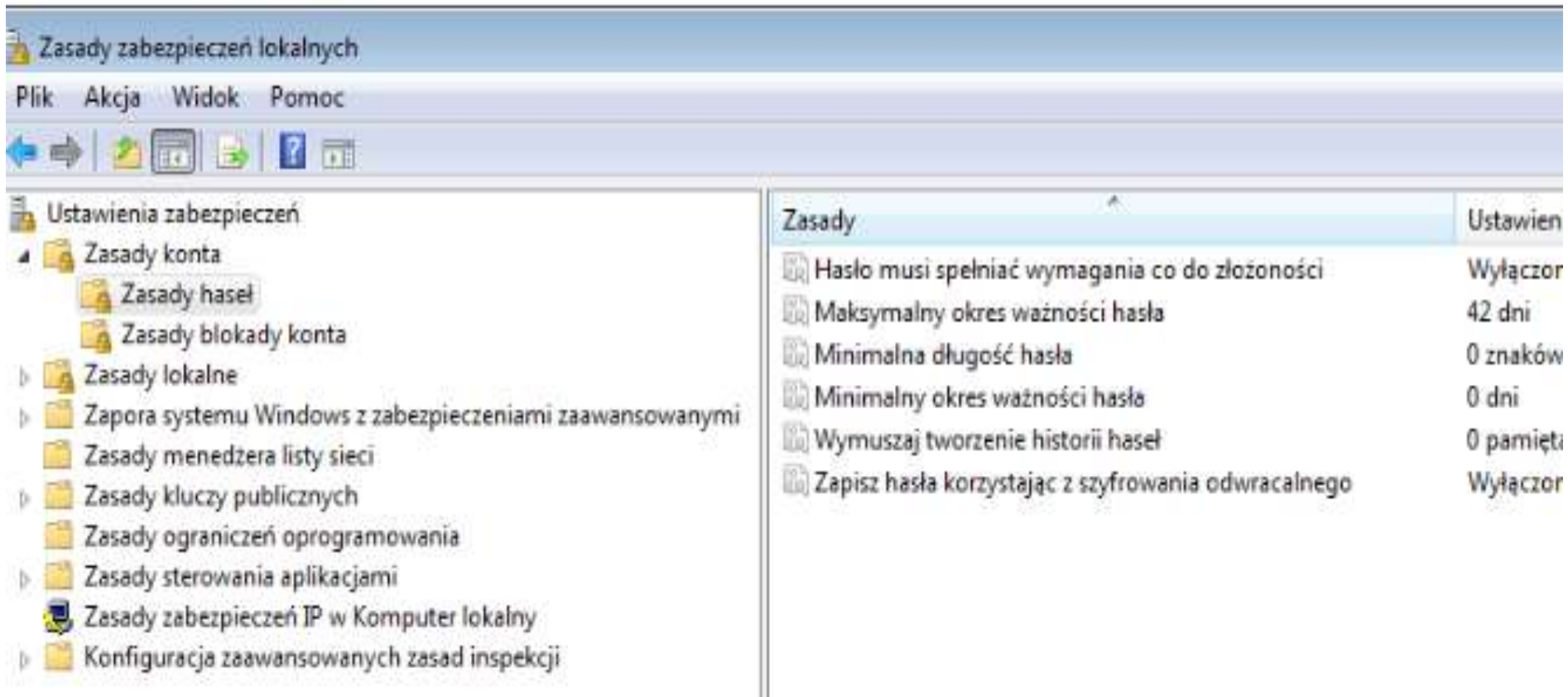


# Zasady zabezpieczeń lokalnych

## przystawka secpol.msc

- Zasady menedżera listy sieci
- Zasady kluczy publicznych
- Zasady ograniczeń oprogramowania
- Zasady sterowania aplikacjami(program AppLocker)
- Zasady zabezpieczeń IP w Komputer lokalny
- Konfiguracja zaawansowanych zasad inspekcji

# Zasady konta

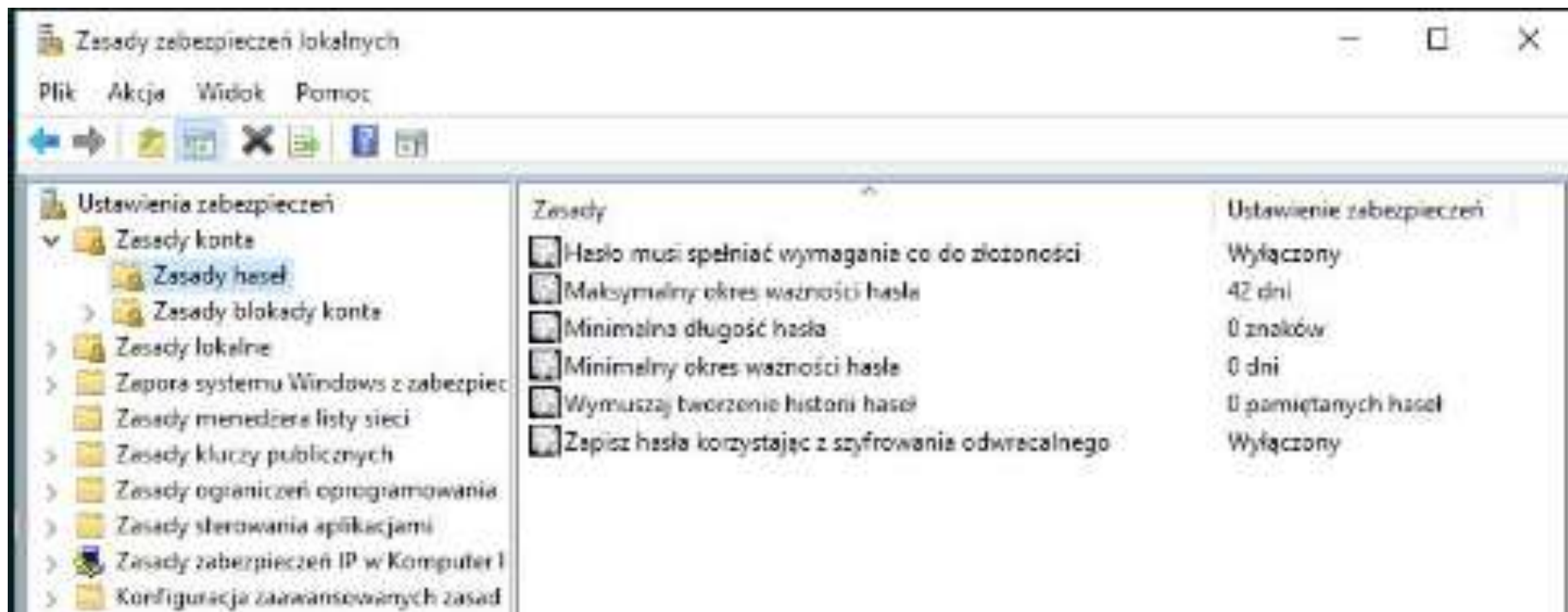


The screenshot displays the Windows Local Security Policy console. The left pane shows the tree view with 'Zasady konta' (Account Policies) selected. The right pane shows a list of account policies with their current settings.

Zasady	Ustawien
Hasło musi spełniać wymagania co do złożoności	Wyłączor
Maksymalny okres ważności hasła	42 dni
Minimalna długość hasła	0 znaków
Minimalny okres ważności hasła	0 dni
Wymuszaj tworzenie historii haseł	0 pamięt
Zapisz hasła korzystając z szyfrowania odwracalnego	Wyłączor

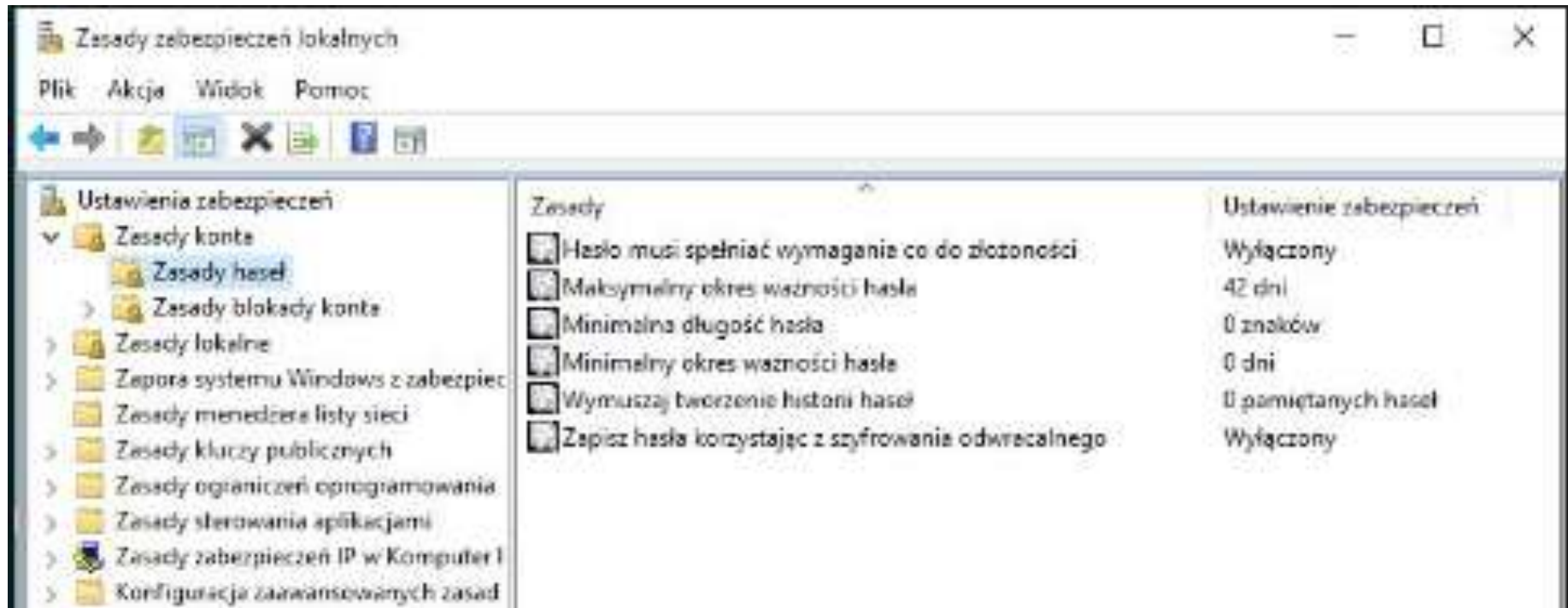
# Ustanawianie i wymuszanie zasad haseł

- Aby przejść do zasad dotyczących haseł wszystkich kont otwieramy węzeł **Ustawienia zabezpieczeń\Zasady konta\Zasady haseł**.



# Ustanawianie i wymuszanie zasad haseł

- Mamy do dyspozycji listę następujących zasad (otwieramy je klikając wybraną dwukrotnie):



# Ustanawianie i wymuszanie zasad haseł

- **Wymuszaj tworzenie historii haseł.**  
Windows tworzy listę dotychczasowych haseł (maksymalnie 24), dzięki której może kontrolować, aby użytkownik nie zmieniał hasła na takie, które już wcześniej stosował.

# Ustanawianie i wymuszanie zasad haseł

- Jeśli korzystamy z tej funkcji powinniśmy też ustawić minimalny okres ważności hasła. W ten sposób nie pozwolimy na to, aby użytkownik mógł zmieniać sobie wielokrotnie hasło, a następnie znowu podać takie, jakie miał dotychczas.

# Ustanawianie i wymuszanie zasad haseł

- **Maksymalny okres ważności hasła.** Ustawiamy tu okres ważności konta (maksymalnie 999 dni). Aby dla wybranego konta wyłączyć tę funkcję, należy w przystawce **Użytkownicy i grupy lokalne** otworzyć właściwości konta i zaznaczyć **Hasło nigdy nie wygasa**.

# Ustanawianie i wymuszanie zasad haseł

- **Minimalny okres ważności konta.** Czyli liczba dni (maksymalnie 999), po upływie których hasło może być zmienione.



# Ustanawianie i wymuszanie zasad haseł

- **Minimalna długość hasła.** Maksymalnie 14 znaków.
- Zmiana tego ustawienia nie wpływa na dotychczasowe hasła.

# Ustanawianie i wymuszanie zasad haseł

- **Hasła muszą spełniać wymagania co do złożoności.**
- Włączenie zasady oznacza: hasła muszą mieć przynajmniej 6 znaków, muszą zawierać małe, duże litery, cyfry i symbole, nie mogą zawierać części nazwiska ani nazwy użytkownika.
- Zmiana nie wpływa na dotychczasowe hasła.

# Ustanawianie i wymuszanie zasad haseł

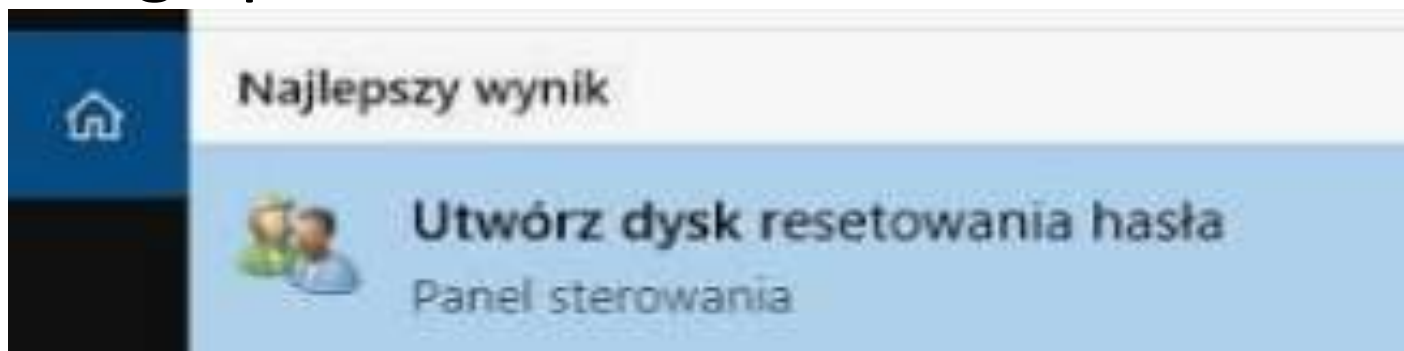
- **Zapisz hasła dla wszystkich użytkowników w domenie, korzystając z szyfrowania odwracalnego.**
- Włączenie powoduje zapisywanie haseł otwartym tekstem, a nie w postaci zaszyfrowanej. Stosuje się to bardzo rzadko, jedynie w celu uzyskania kompatybilności ze starszymi aplikacjami.

# Odzyskiwanie zapomnianego hasła


- Jeśli często zmieniamy hasła, które są długie i skomplikowane, to wysoce prawdopodobne jest to, że kiedyś możemy zapomnieć o jednym z nich. Najrozsądniej jest zabezpieczyć się przed takim przypadkiem, tworząc **dysk resetowania hasła**.
- Dzięki niej możemy zalogować się do systemu, nie znając hasła. Możemy ją utworzyć tylko dla naszego lokalnego profilu.

# dysk resetowania hasła

- Z dysku możemy skorzystać w momencie, gdy zapomnimy hasła do naszego profilu, wybierając stosowną opcję podczas operacji logowania. Należy jednak pamiętać, aby nie udostępniać stworzonego dysku osobom trzecim, gdyż dzięki niemu mogą one dostać się do naszego profilu.



Podłączamy przygotowany pendrive do komputera, a następnie przechodzimy do opcji ***Utwórz dysk resetowania hasła***


 Konta użytkowników

← → ▾ ↑  > Panel sterowania > Konta użytkowników > Konta użytkowników

Strona główna Panelu sterowania

Zarządzaj powiadzczeniami


**Utwórz dysk resetowania hasła**


 Skonfiguruj zaawansowane właściwości profilu użytkownika

Zmień moje zmienne środowiskowe

Wprowadź zmiany w koncie użytkownika

Wprowadź zmiany na moim koncie w ustawieniach komputera

 Zmień swoją nazwę konta

 Zmień typ swojego konta

 Zarządzaj innym kontem

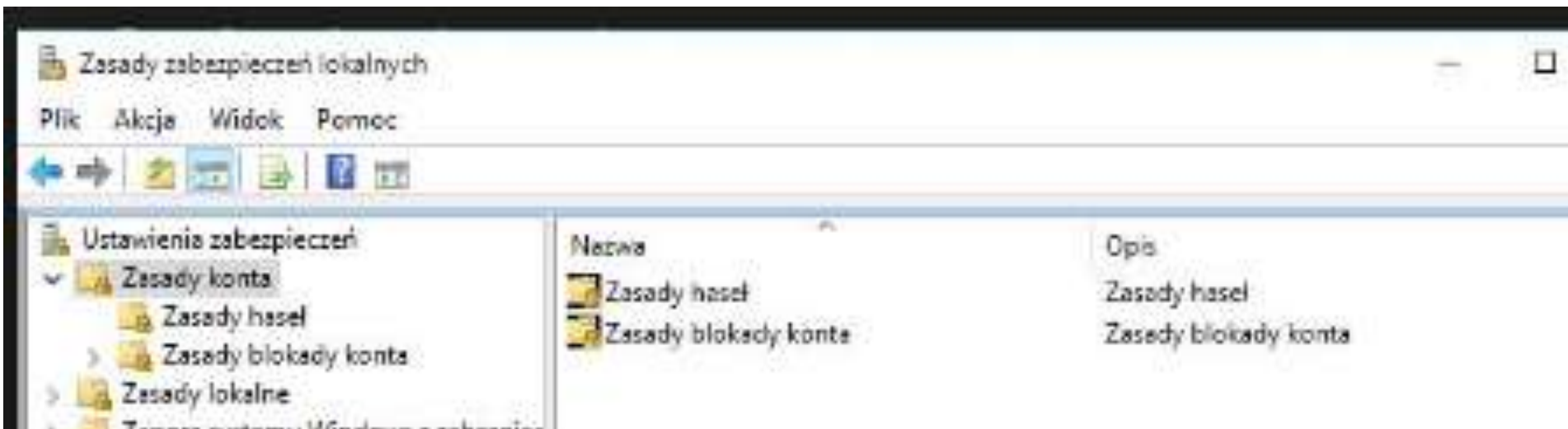
 Zmień ustawienia funkcji Kontrola konta użytkownika



# Zasady zabezpieczeń lokalnych narzędzie przystawka secpol.msc

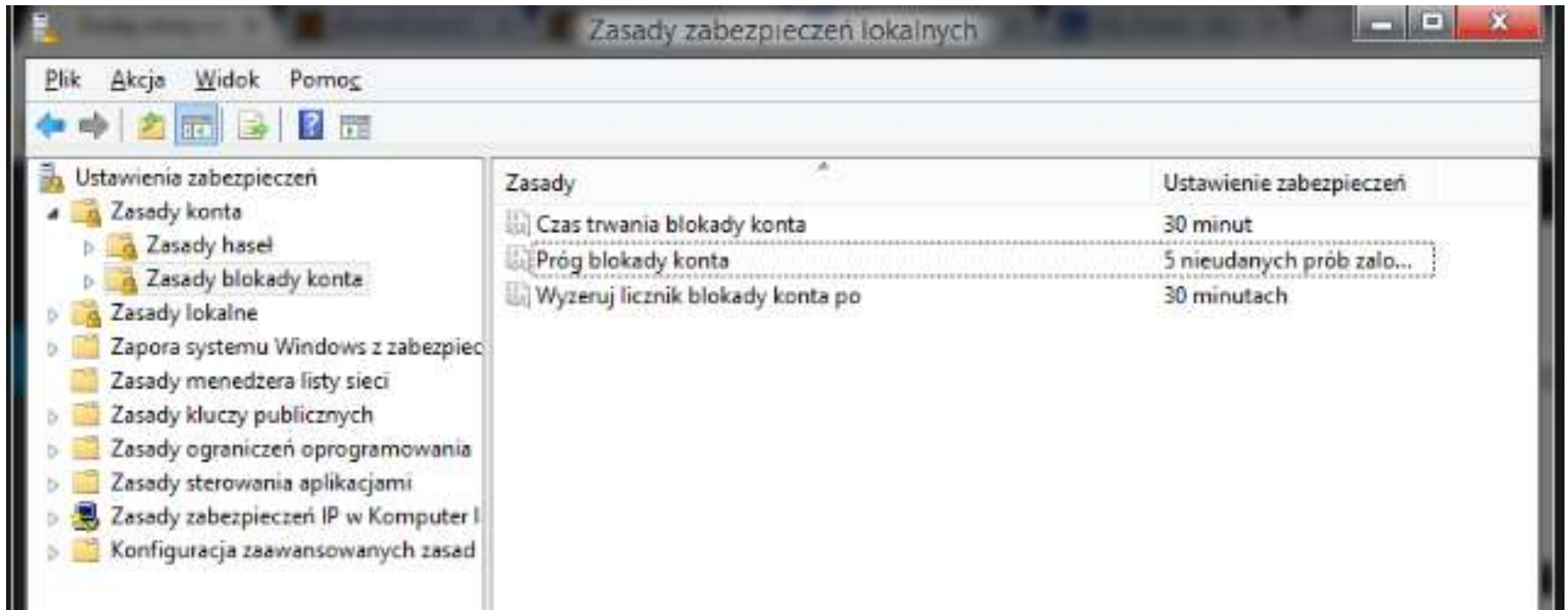
- Skutecznym **zabezpieczeniem** przed użytkownikiem czy programem usiłującym się włamać do systemu przez podawanie kolejno różnych haseł jest ustawienie **zasad blokady kont**.

# Zasady zabezpieczeń lokalnych narzędzie przystawka secpol.msc





# Otwieramy węzeł **Ustawienia zabezpieczeń**\**Zasady konta**\**Zasady blokady konta**



# Zasady blokady kont

- **Czas trwania blokady konta.** Liczba wyznaczająca czas zablokowania użytkownika. Wartość 0 oznacza zablokowanie konta na zawsze (do czasu odblokowania go przez administratora). Maksymalna wartość to 9999 minut, czyli około 69 dni.

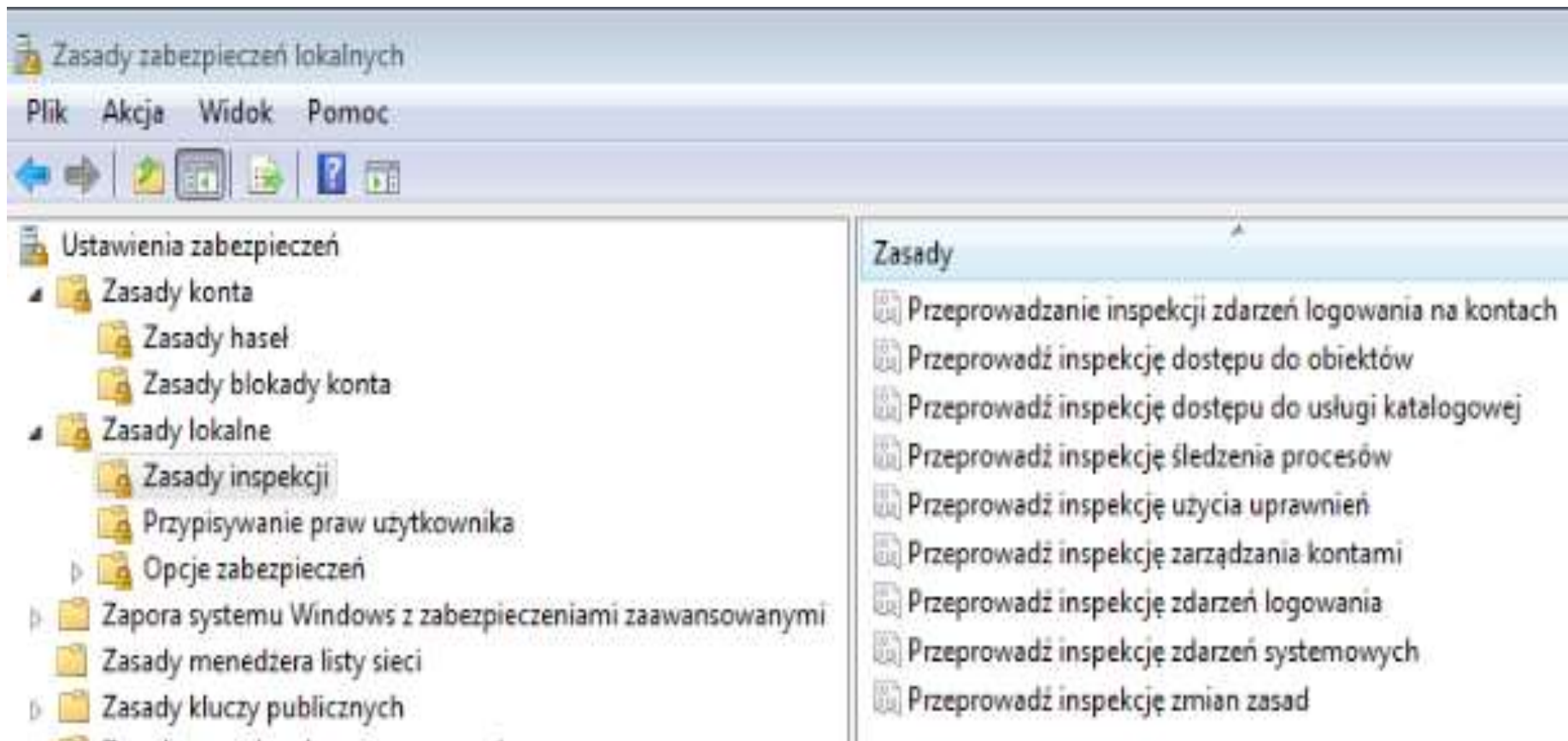
# Zasady blokady kont

- **Próg blokady konta.** Liczba (od 1 do 999) wyznaczająca limit nieudanych logowań w ustalonym okresie czasu, którego przekroczenie powoduje zablokowanie konta.

# Zasady blokady kont

- **Wyzeruj licznik blokady konta po.** Liczba (od 0 do 99999 minut) wyznaczająca okres, w ciągu którego obowiązuje limit nieudanych prób logowania. Jeśli ustalimy 10 minut oznacza to, że po tym okresie liczba prób jest zerowana i odliczanie zaczyna się od początku.

# Zasady lokalne



# Zasady lokalne

- Opcje zasad lokalnych dzielą się na trzy podfoldery:
  - Zasady inspekcji
  - Przypisywanie praw użytkownika
  - Opcje zabezpieczeń

# Zasady inspekcji

- Zasady inspekcji pozwalają na inspekcjonowanie konkretnych zdarzeń na komputerze i powiadamianie, gdy zakończą się powodzeniem lub niepowodzeniem.
- Aby zmienić ustawienia zasady należy nacisnąć prawym przyciskiem myszy na zasadę, otworzyć okno *Właściwości* i wybrać interesujące nas ustawienia.

# Zasady inspekcji

The image shows a Windows Security Policies console window titled "Zasady zabezpieczeń lokalnych". The left pane displays a tree view of security policies, with "Zasady inspekcji" selected under "Zasady lokalne". The right pane lists several inspection policies, with "Przeprowadź inspekcję użycia uprawnień" highlighted. A foreground dialog box titled "Właściwości: Przeprowadź inspekcję użycia uprawnień" is open, showing the policy name and a list of options to inspect: "Sukces" and "Niepowodzenie".

**Zasady**

- Przeprowadzanie inspekcji zdarzeń logowania na kontach
- Przeprowadź inspekcję dostępu do obiektów
- Przeprowadź inspekcję dostępu do usługi katalogowej
- Przeprowadź inspekcję śledzenia procesów
- Przeprowadź inspekcję użycia uprawnień**
- Przeprowadź inspekcję zarządzania kontami

**Właściwości: Przeprowadź inspekcję użycia uprawnień**

Ustawianie zabezpieczeń lokalnych Wyjaśnienie

Przeprowadź inspekcję użycia uprawnień

Dokonuj inspekcji tych prób:

- Sukces
- Niepowodzenie



# Przypisywanie praw użytkownika

- Sekcja Przypisywanie praw użytkownika pozwala na nadawanie lub odmawianie określonym użytkownikom lub grupom określonych praw.

# Przypisywanie praw użytkownika

The screenshot shows the Windows Security Policies console. The left pane displays a tree view of security settings, with 'Przypisywanie praw użytkownika' (Assign User Rights) selected under 'Zasady lokalne' (Local Policies). The right pane shows a list of policies with their assigned users.

Zasady	Ustawienie
Blokuj strony w pamięci	
Debuguj programy	Administrat
Dodaj stacje robocze do domeny	
Dostosuj przydziały pamięci dla procesów	USŁUGA LO
Działanie jako część systemu operacyjnego	
Generuj inspekcje zabezpieczeń	USŁUGA LO
Logowanie w trybie usługi	NT SERVICE
Logowanie w trybie wsadowym	Administrat
Ładuj i zwalnij sterowniki urządzeń	Administrat
Modyfikuj etykietę obiektu	
Modyfikuj wartości środowiskowe oprogramowania układo...	Administrat
Obejdź sprawdzanie przy przechodzeniu	Wszyscy,US
Odmawiaj logowania za pomocą usług pulpitu zdalnego	
Odmowa dostępu do tego komputera z sieci	Gość
Odmowa logowania lokalnego	HomeGroup
Odmowa logowania w trybie usługi	

# Przypisywanie praw użytkownika

- Aby dodać lub usunąć użytkowników lub grupy z danej zasady należy nacisnąć prawym przyciskiem myszy na zasadę, otworzyć okno *Właściwości*, a następnie użyć opcji *Dodaj użytkownika lub grupę* lub *Usuń*.

# Przypisywanie praw użytkownika

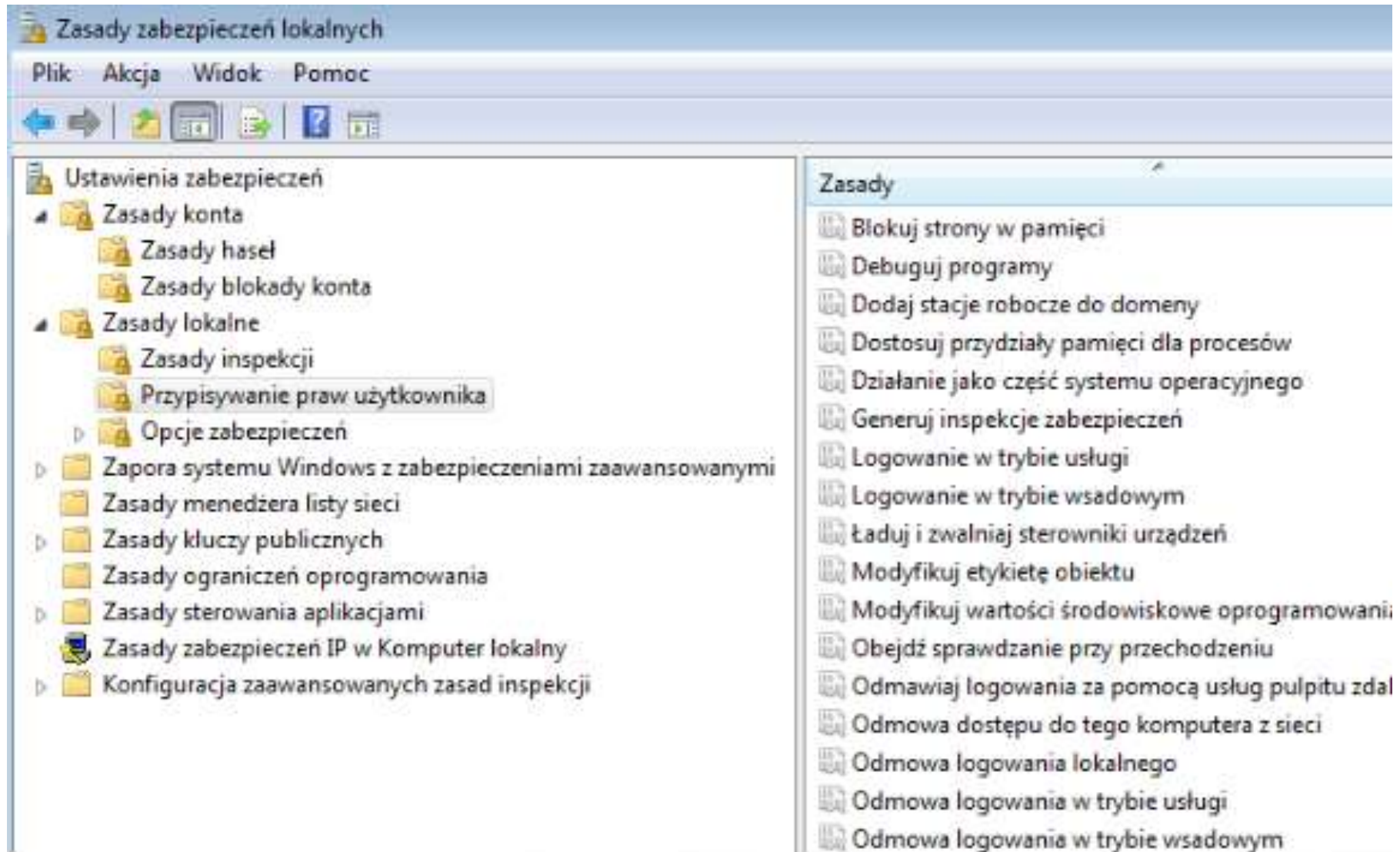
The image shows a Windows Security Policies console window titled "Zasady zabezpieczeń lokalnych". The left pane displays a tree view of security policies, with "Przypisywanie praw użytkownika" selected under "Zasady lokalne". The right pane lists several policies, including "Blokuj strony w pamięci", "Debuguj programy", "Dodaj stacje robocze do domeny", "Dostosuj przydziały pamięci dla procesów", "Działanie jako część systemu operacyjnego", and "Generuj inspekcje zabezpieczeń".

An "Właściwości: Zamknij system" dialog box is open in the foreground. It shows the policy name "Zamknij system" and a list of users and groups that can be assigned the policy: "Administratorzy", "Operatorzy kopii zapasowych", and "Użytkownicy". The dialog includes buttons for "Dodaj użytkownika lub grupę...", "Usuń", and "Wyjaśnienie".

# Opcje zabezpieczeń

- Zakładka Opcje zabezpieczeń zawiera spis zasad warunkujących stopień zabezpieczeń komputera. Aby dokonać modyfikacji w zasadzie musimy kliknąć na nią prawym przyciskiem myszy, wybrać pozycję **Właściwości** i dokonać odpowiednich zmian w oknie ustawień zasady.

# Opcje zabezpieczeń



# Zarządzanie kontami poprzez **NET ACCOUNTS**

- **NET ACCOUNTS** uaktualnia bazę kont użytkowników i zmienia hasło oraz wymagania logowania dla wszystkich kont.
- Użyte bez opcji, **NET ACCOUNTS** wyświetla bieżące ustawienia hasła i ograniczeń logowania oraz informacje o domenie.

# Zarządzanie kontami poprzez NET ACCOUNTS

```
net help accounts
```

Składnia tego polecenia jest następująca:

```
NET ACCOUNTS
```

```
[/FORCELOGOFF:{minuty | NO}] [/MINPWLEN:długość]  
    [/MAXPWAGE:{dni | UNLIMITED}] [/MINPWAGE:dni]  
    [/UNIQUEPW:liczba] [/DOMAIN]
```



# /FORCELOGOFF:{minuty | NO}

Ustawia liczbę minut, przez które użytkownik może być zalogowany przed wymuszeniem wylogowania wskutek wygaśnięcia konta lub ważności godzin logowania. NO, wartość domyślna, zapobiega wymuszaniu wylogowania.

```
net accounts /forcelogoff:5
```

# **/MINPWLEN : długość**

Ustawia minimalną liczbę znaków w haśle.

Zakres długości hasła wynosi od 0 do 14 znaków;  
wartość domyślna to 6 znaków.

```
net accounts /MINPWLEN:9
```

# `/MAXPWAGE : {dni | UNLIMITED}`

Ustawia maksymalną liczbę dni ważności hasła. UNLIMITED ustala nieograniczony czas ważności hasła. Wartość `/MAXPWAGE` nie może być mniejsza od wartości `/MINPWAGE`. Zakres wynosi od 1 do 999; domyślnie wartość się nie zmienia.

```
net accounts /MAXPWAGE:Unlimited
```

## **/MINPWAGE : dni**

Ustawia minimalną liczbę dni, które muszą minąć, zanim użytkownik może zmienić hasło. Wartość 0 ustawia brak tego ograniczenia. Zakres wynosi od 0 do 999; wartość domyślna to 0 dni. Wartość /MINPWAGE nie może być większa od wartości /MAXPWAGE.

```
net accounts /MINPWAGE:5
```

# /UNIQUEPW:liczba

Wymaga, aby hasło użytkownika było unikatowe, poprzez określoną liczbę zmian hasła. Największa wartość to 24.

```
net accounts /UNIQUEPW:4
```

# /DOMAIN

Wykonuje operacje na kontrolerze domeny w bieżącej domenie. W innym wypadku operacje te są dokonywane na komputerze lokalnym.

```
net accounts /DOMAIN
```

# Wyświetlenie ustawień kont

```
net accounts
```

```
Po jakim czasie od wygaśnięcia czasu wymuszać wylogowanie?:      Nigdy
Minimalny okres ważności hasła (dni):                               0
Maksymalny okres ważności hasła (dni):                             42
Minimalna długość hasła:                                           0
Długość zapamiętywanej historii haseł:                             Brak
Próg blokady:                                                       Nigdy
Czas trwania blokady (minuty):                                       30
Okno obserwowania blokady (minuty):                                 30
Rola komputera:
```