

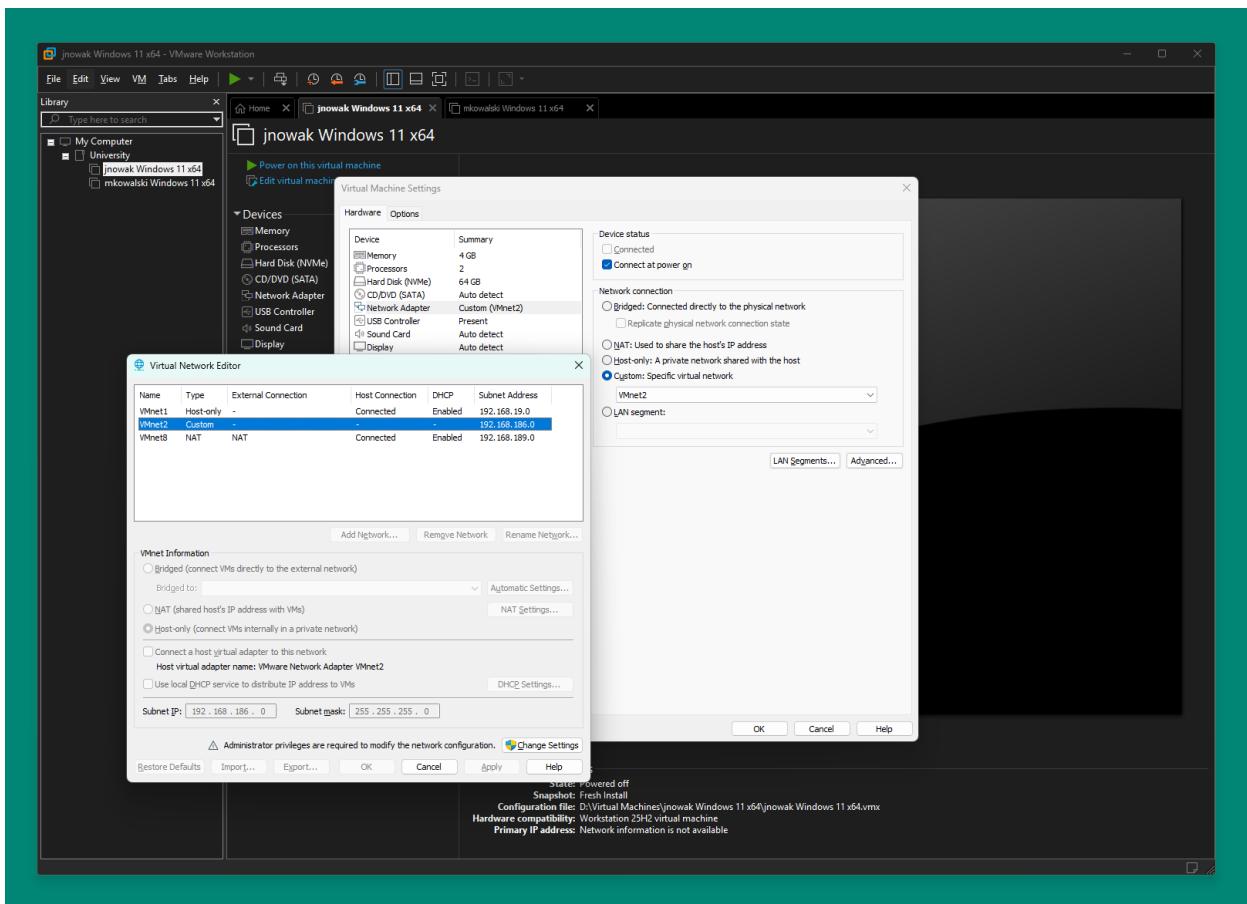
Bartosz Bieniek

gr. 7, st. 1, sem. 3, Informatyka RMS

## Przygotowanie środowiska.

Do wykonania zadań wykorzystałem maszynę wirtualną *jnowak* z systemem *Windows 11 Pro* oraz narzędzie do wirtualizacji *VMware Workstation*.

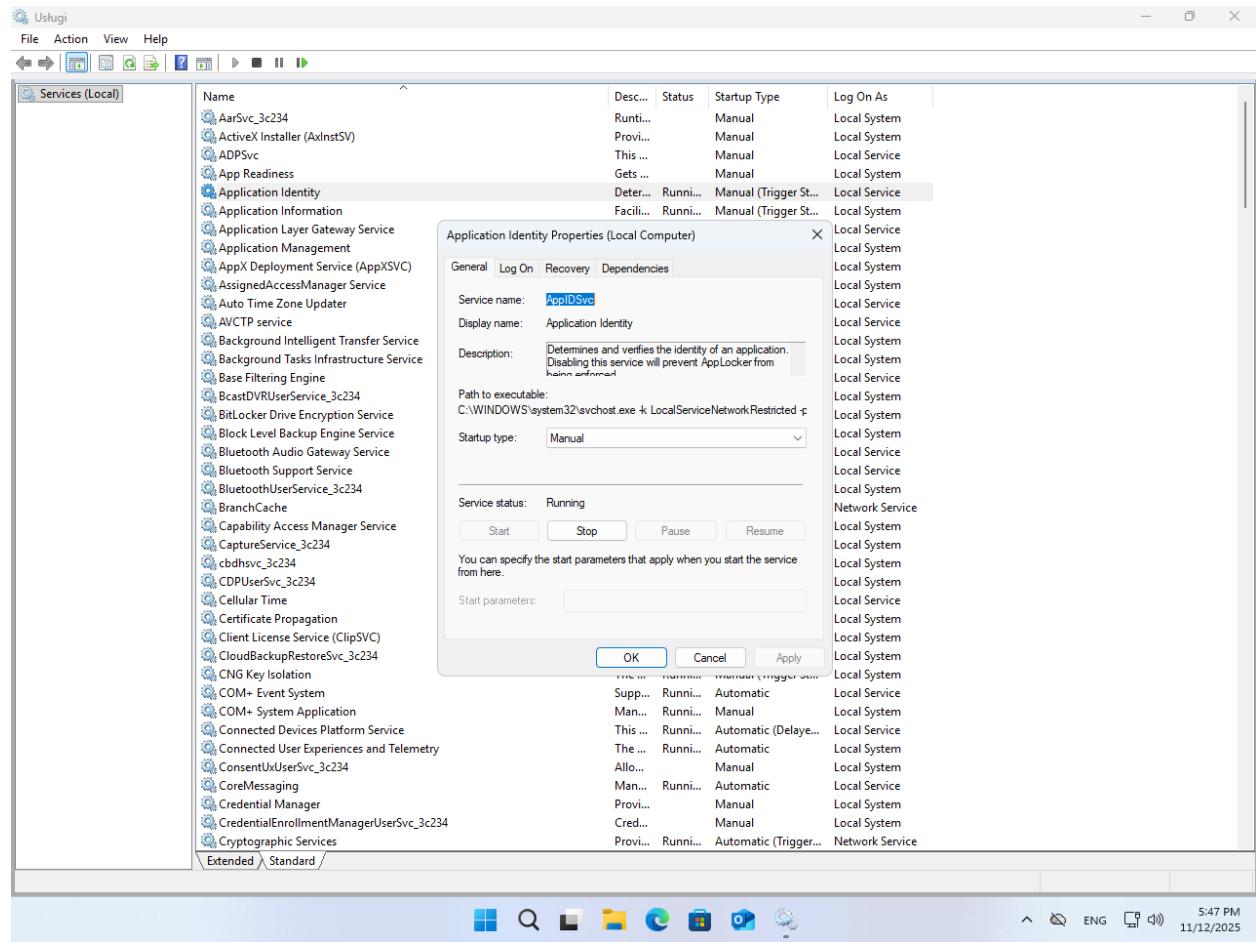
Aby podłączyć ją do sieci wewnętrznej (dostępnej tylko dla maszyn wirtualnych), utworzyłem w programie wirtualizacyjnym nową sieć w trybie „Host-only (connect VMs internally in a private network)” i odznaczyłem opcję “Connect a host virtual adapter to this network”. Następnie przeszedłem do ustawień maszyny wirtualnej i dołączylem ją do utworzonej sieci.



Zrzut ekranu 1 Tworzenie nowej sieci wewnętrznej. Dołączanie maszyny wirtualnej do sieci.

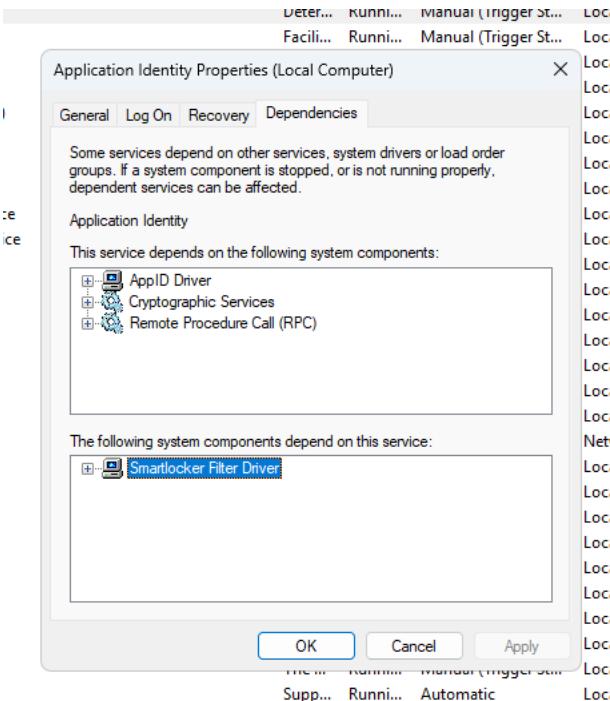
## Zadanie 1. Wyłączenie usługi App Identity (Tożsamość Aplikacji).

Usługi można włączać i wyłączać z poziomu programu *Usługi*.



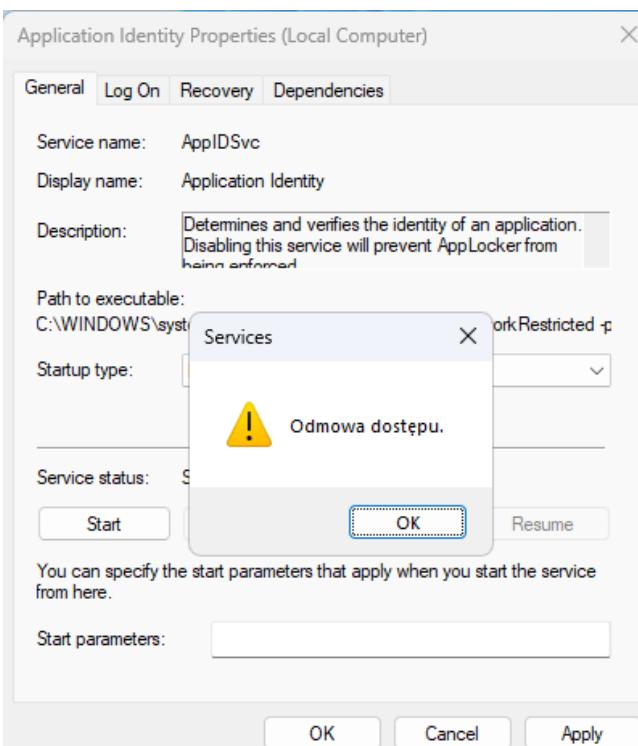
Zrzut ekranu 2 Program Usługi w systemie Windows 11. Szczegóły usługi App Identity (Tożsamość Aplikacji).

Wybierając konkretną usługę z listy możemy wyświetlić więcej informacji. W przypadku *App Identity*, możemy zobaczyć, że jest ona uruchamiana ręcznie i działa (choć nikt jej ręcznie nie uruchamiał). Wynika to z faktu, że uruchomiła się usługa zależna (*Smartlocker Filter Driver*), pociągając za sobą wszystkie usługi podległe.



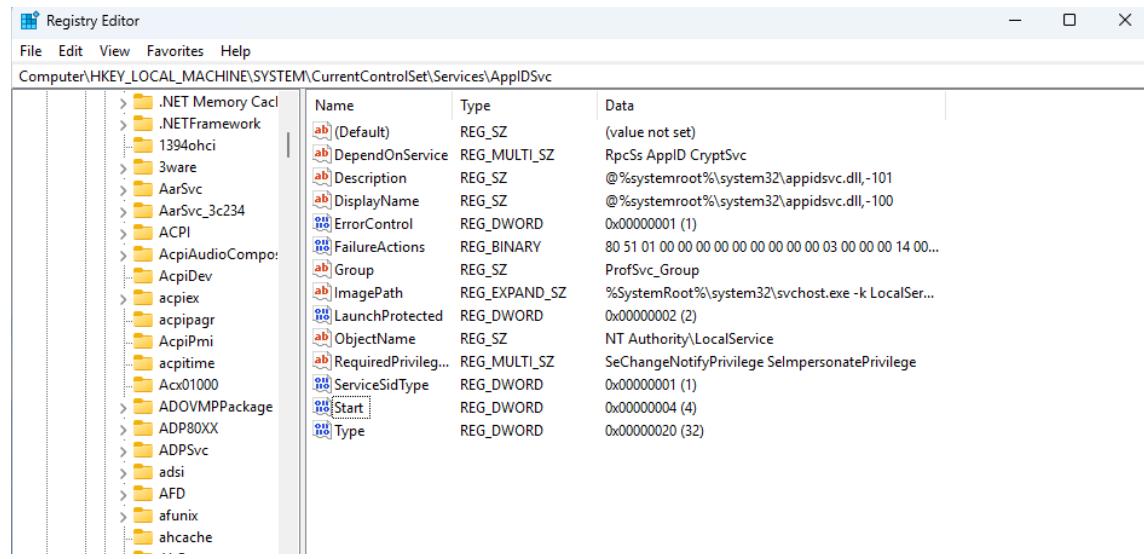
Zrzut ekranu 3 Zakładka z usługami zależnymi.

Aby wyłączyć usługę na stałe, należało by ustawić uruchamianie w zakładce „General” na „Wyłączony”. Usługa *App Identity* jest jednak zabezpieczona i próba jej wyłączenia generuje błąd „Odmowa dostępu”.



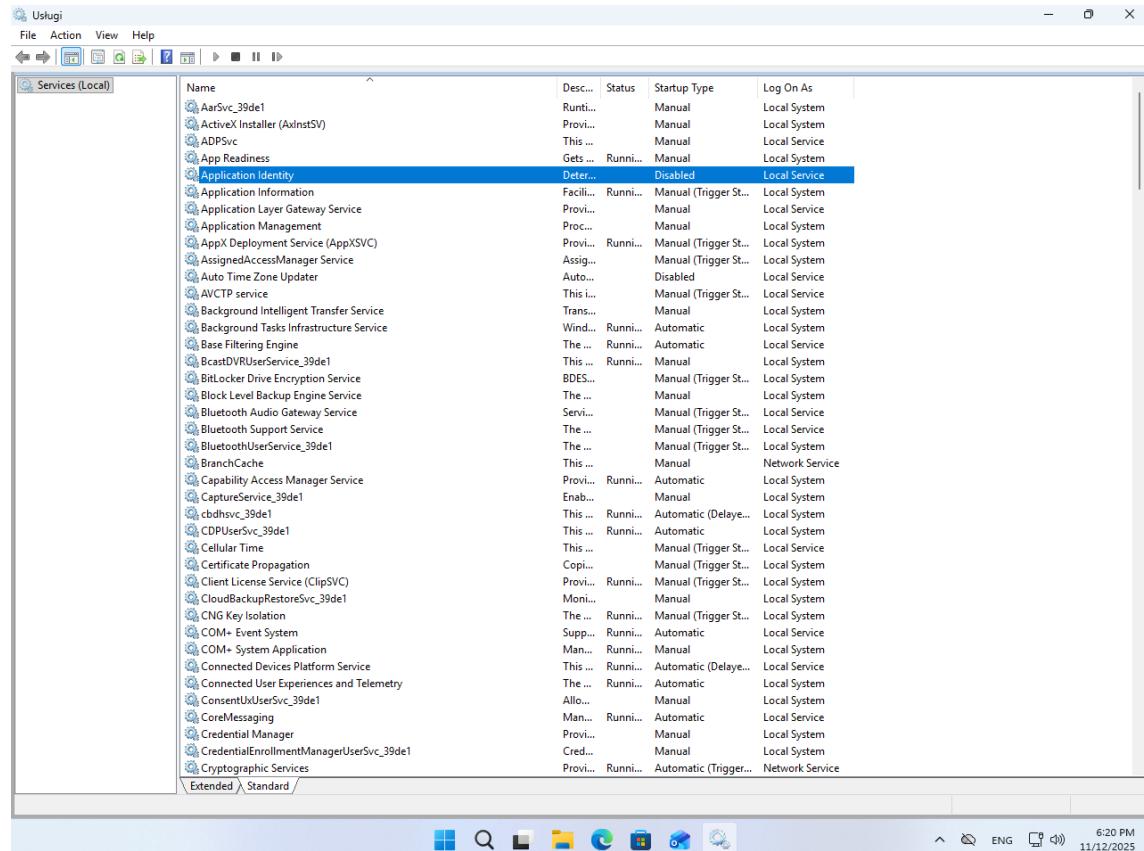
Zrzut ekranu 4 Odmowa dostępu przy próbie wyłączenia usługi *App Identity*.

Problem można jednak obejść, zmieniając ustawienia startu usługi z poziomu rejestru systemu. W kluczu `HKLM:\SYSTEM\CurrentControlSet\Services\AppIDSvc` należy ustawić wartość “Start” na 4, aby zapobiec włączaniu się usługi.



Zrzut ekranu 5 Wyłączenie uruchamiania się usługi App Identity z poziomu rejestru. Wartość „Start” ustawiona na 4.

Po restarcie systemu, usługa nie uruchamia się.

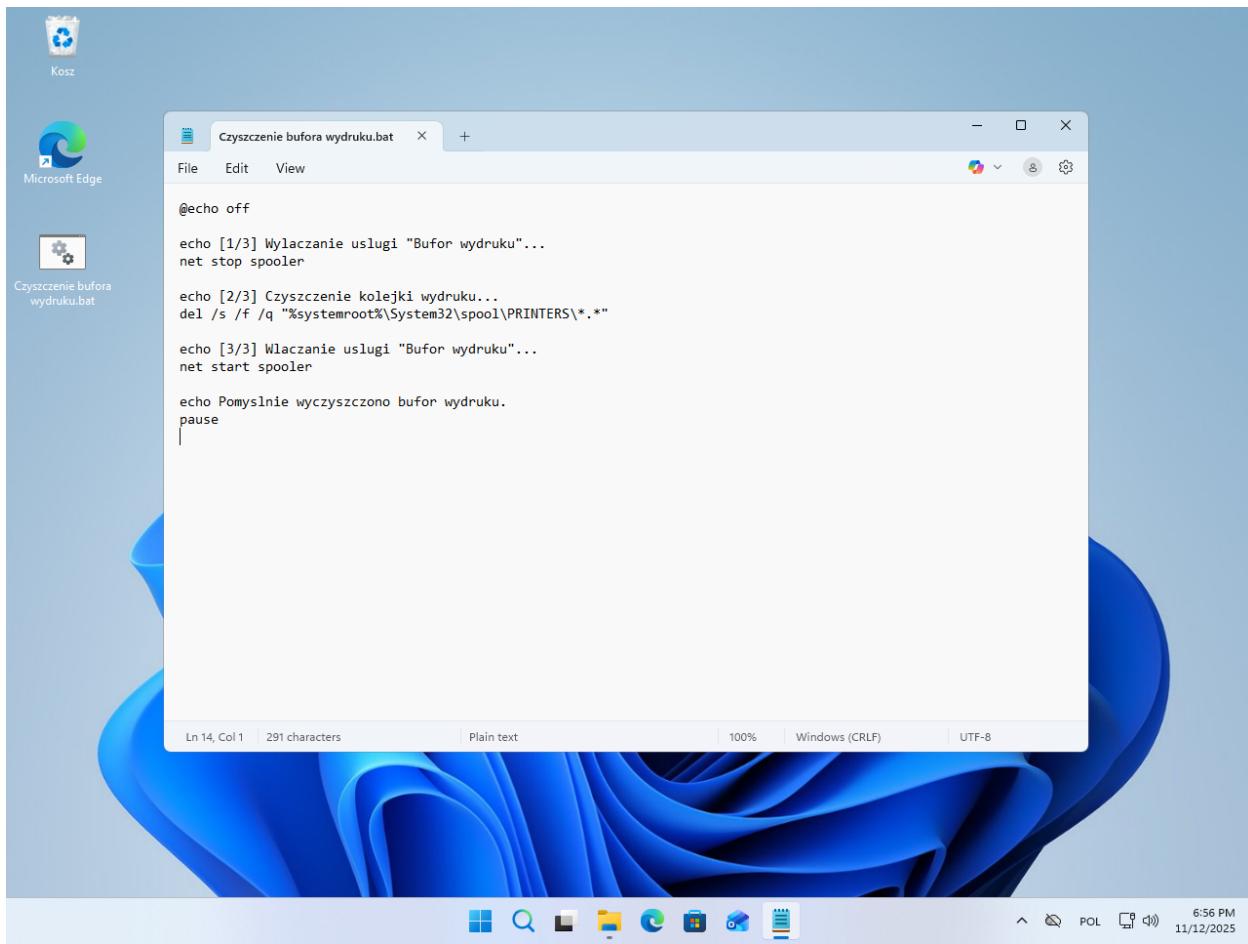


Zrzut ekranu 6 Wyłączona usługa App Identity.

## Zadanie 2. Zarządzanie usługami z poziomu wiersza poleceń (skryptów Batch).

Uruchomionymi usługami można zarządzać z poziomu wiersza poleceń przy pomocy programów (poleceń) `net` oraz `sc`. Dla przykładu, polecenia `net start <usługa>` oraz `net stop <usługa>` odpowiednio uruchamiają i stopują zadaną usługę.

Do automatyzacji bardziej złożonych zadań można utworzyć skrypty Batch, które umożliwiają wykonywanie wielu komend jedna po drugiej. Przykładowo można zrealizować zadanie polegające na restarcie usługi bufora wydruku („spooler”) i wyczyszczeniu kolejki wydruku. W tym celu utworzymy następujący skrypt.



```
Czyszczenie bufora wydruku.bat
File Edit View
@echo off
echo [1/3] Wyłączanie usługi "Bufor wydruku"...
net stop spooler
echo [2/3] Czyszczenie kolejki wydruku...
del /s /f /q "%systemroot%\System32\spool\PRINTERS\*.*"
echo [3/3] Włączanie usługi "Bufor wydruku"...
net start spooler
echo Pomyślnie wyczyszczono bufor wydruku.
pause
```

Ln 14, Col 1 291 characters Plain text 100% Windows (CRLF) UTF-8

6:56 PM 11/12/2025

Zrzut ekranu 7 Skrypt Batch restartujący usługę bufora wydruku i czyszczący niezrealizowane zadania wydruku.

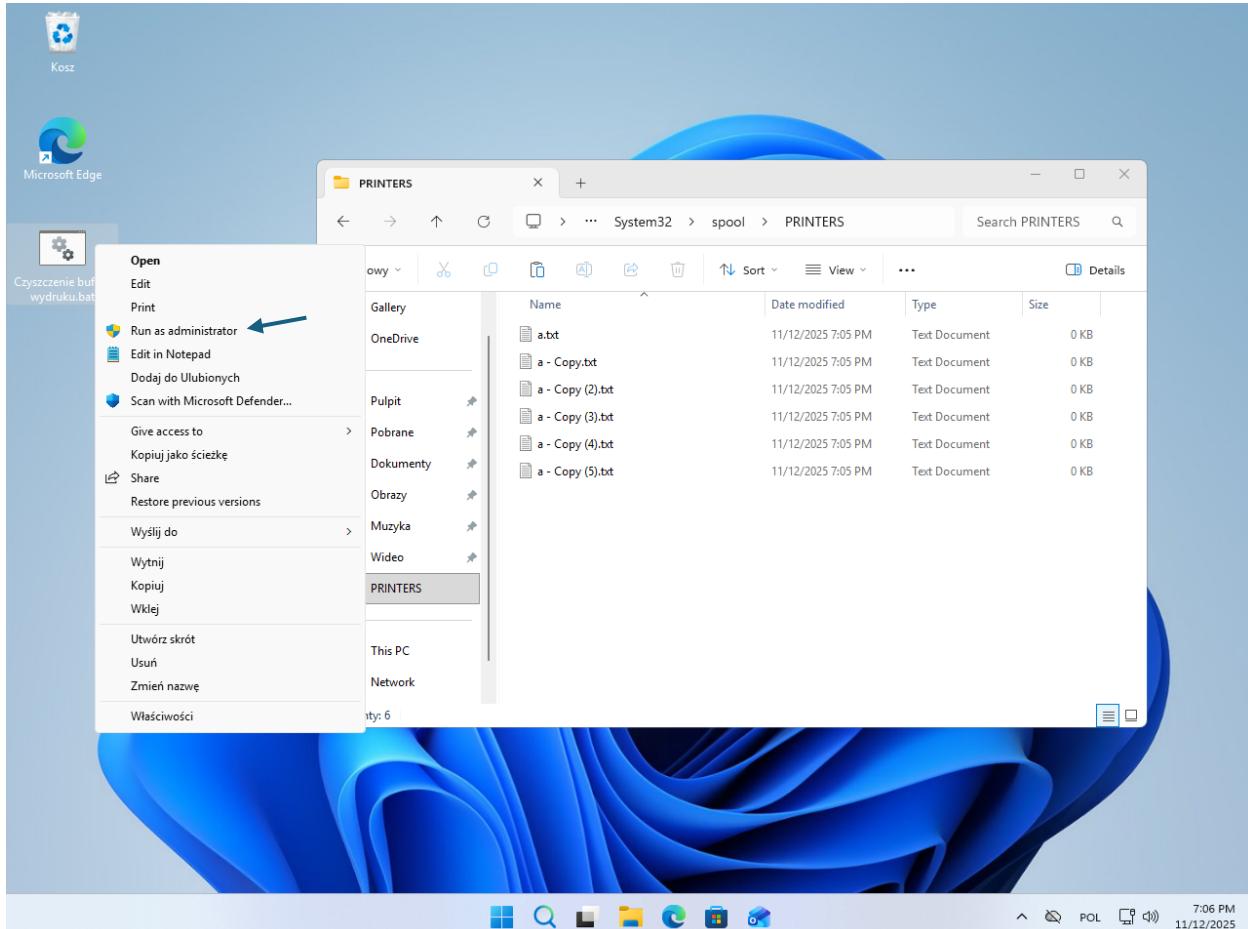
Do zarządzania usługą bufora wydruków konieczne są uprawnienia administratora, stąd konieczne jest uruchomienie skryptu jako administrator – w przeciwnym wypadku wyświetla się komunikaty o braku uprawnień.

```
C:\WINDOWS\system32\cmd. X + 
[1/3] Wyłączanie usługi "Bufor wydruku"...
System error 5 has occurred.

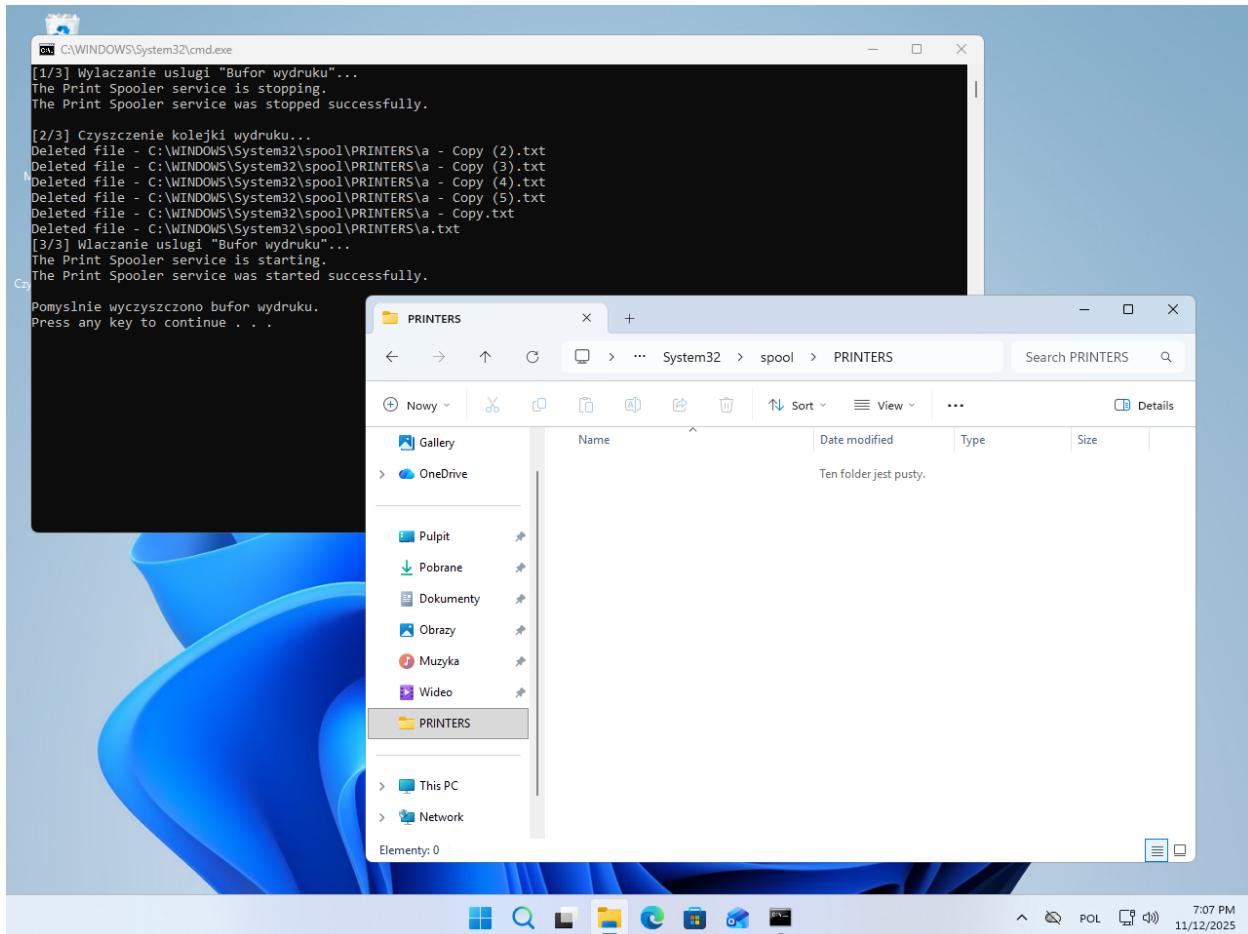
cro: Odmowa dostępu.
```

Zrzut ekranu 8 Błąd wyświetlany w przypadku uruchomienia skryptu bez uprawnień administratora.

Prześledźmy działanie skryptu we właściwych warunkach. W folderze z kolejką wydruku utworzyłem kilka plików, a następnie uruchomiłem plik .bat jako administrator.



Zrzut ekranu 9 Przykładowa zawartość w folderze z kolejką wydruku. Uruchamianie skryptu jako administrator.

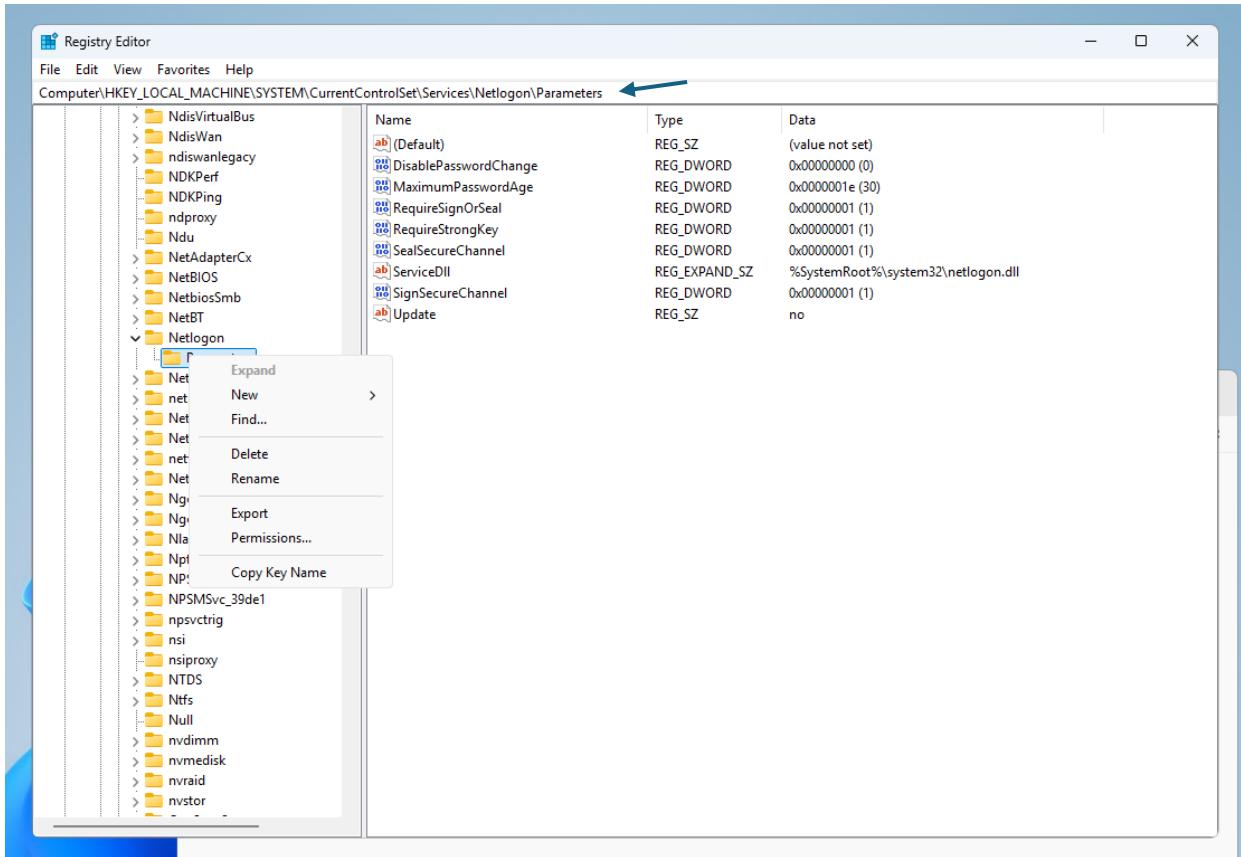


Zrzut ekranu 10 Efekt działania skryptu.

Jak widać, usługa bufora wydruku została zatrzymana, kolejka wydruku wyczyszczona (pliki z widocznego folderu zostały usunięte), po czym spooler został uruchomiony.

## Zadanie 3. Nanoszenie zmian w rejestrze – część 1.

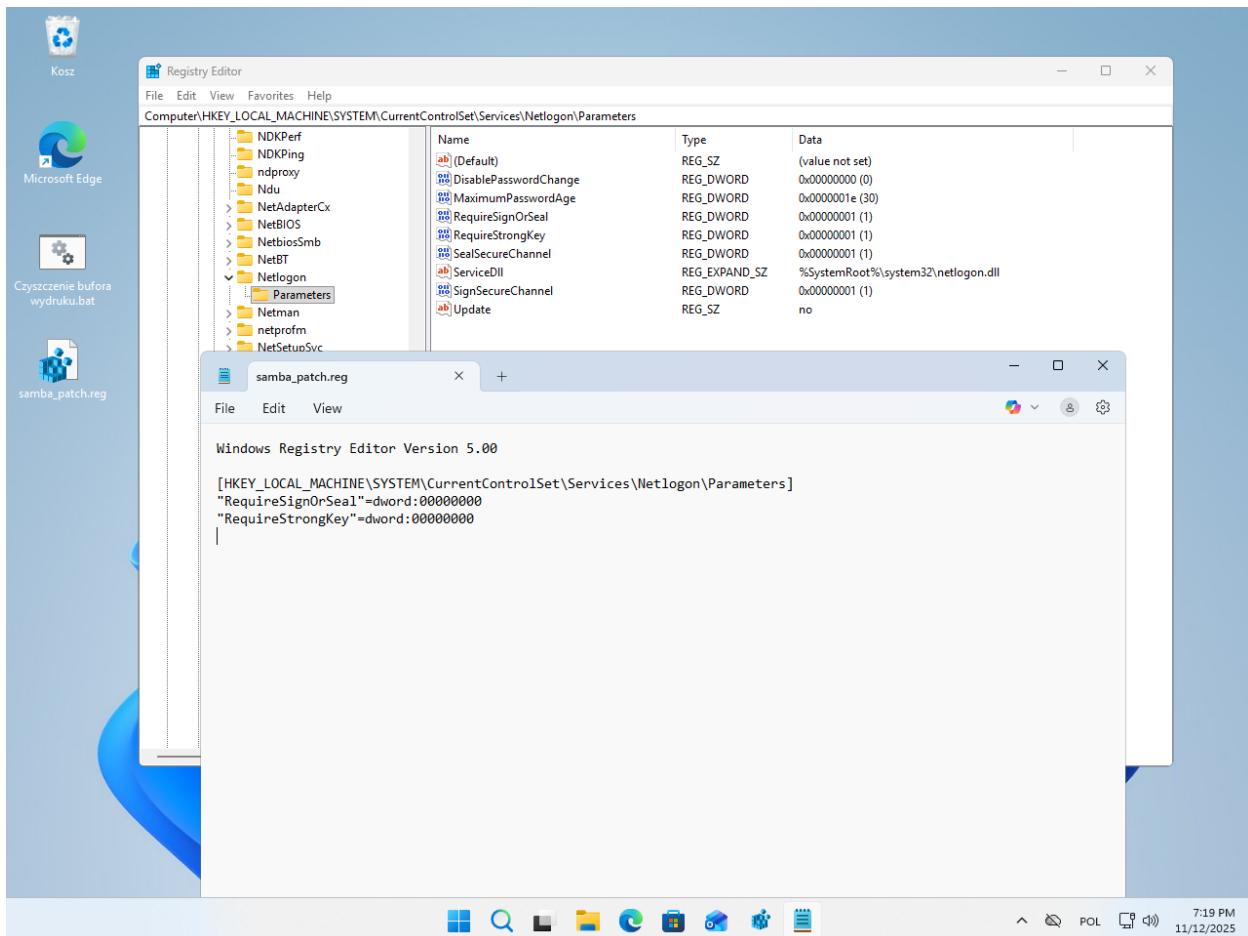
Zmiany w rejestrze najprościej jest nanieść przez program *Edytor rejestru*. W przypadku, gdy zajdzie konieczność edycji jakieś wartości, klucz można łatwo odszukać wpisując ścieżkę w górnym pasku programu.



Zrzut ekranu 11 Okno programu Edytor rejestru.

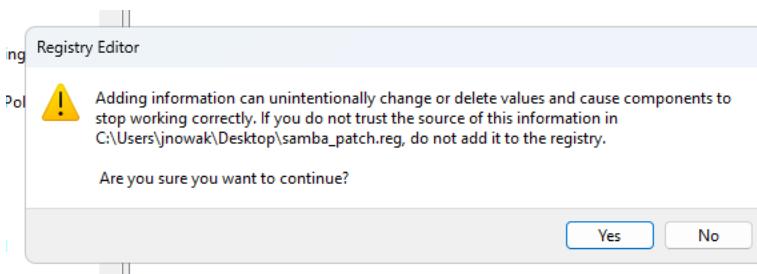
Przykładowo, aby rozwiązać problem z dołączeniem komputera do domeny utrzymywanej przez starszą wersję Samby, konieczne jest ustawnienie w kluczu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\parameters` wartości `RequireSignOrSeal` i `RequireStrongKey` na 0. Klikając dwukrotnie w daną pozycję na liście możemy zmienić jej wartość.

W przypadku, gdybyśmy na przykład chcieli nanieść identyczne zmiany w rejestrze na kilku komputerach, przydatna może okazać się opcja eksportu klucza. W tym celu należy kliknąć prawym przyciskiem myszy na klucz i wybrać „Export”. Tak wygenerowany plik (tak zwany „patch rejestrowy”) można edytować i pozostawić jedynie interesujące nas wartości, na przykład *RequireSignOrSeal* i *RequireStrongKey*.



Zrzut ekranu 12 Edycja patcha rejestrowego.

Aby z niego skorzystać, należy otworzyć wygenerowany plik .reg i potwierdzić chęć nанесения zmian.



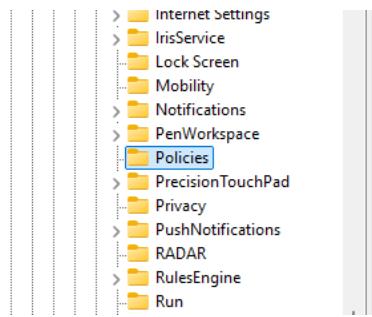
Zrzut ekranu 13 Komunikat potwierdzający chęć nанесienia zmian w rejestrze.

## Zadanie 4. Nanoszenie zmian w rejestrze – część 2. Zasady grup lokalnych.

Aplikacje nie mają obowiązku tworzyć w rejestrze wszystkich używanych przez siebie kluczy i inicjalizować wartości – dla brakujących wpisów wykorzystują wtedy najpewniej wartości domyślne.

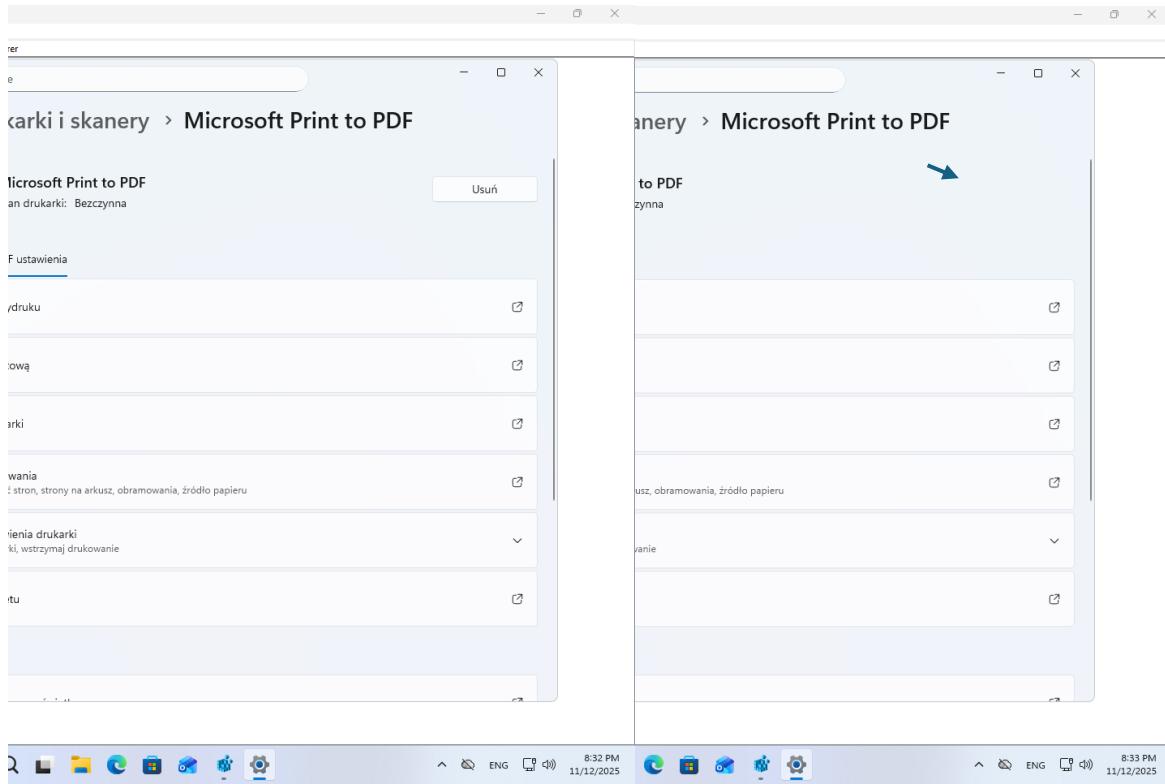
Jednym z przykładów nieistniejącego klucza jest ten odpowiedzialny za zablokowanie możliwości usuwania drukarek dla aktualnie zalogowanego użytkownika –

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer.`



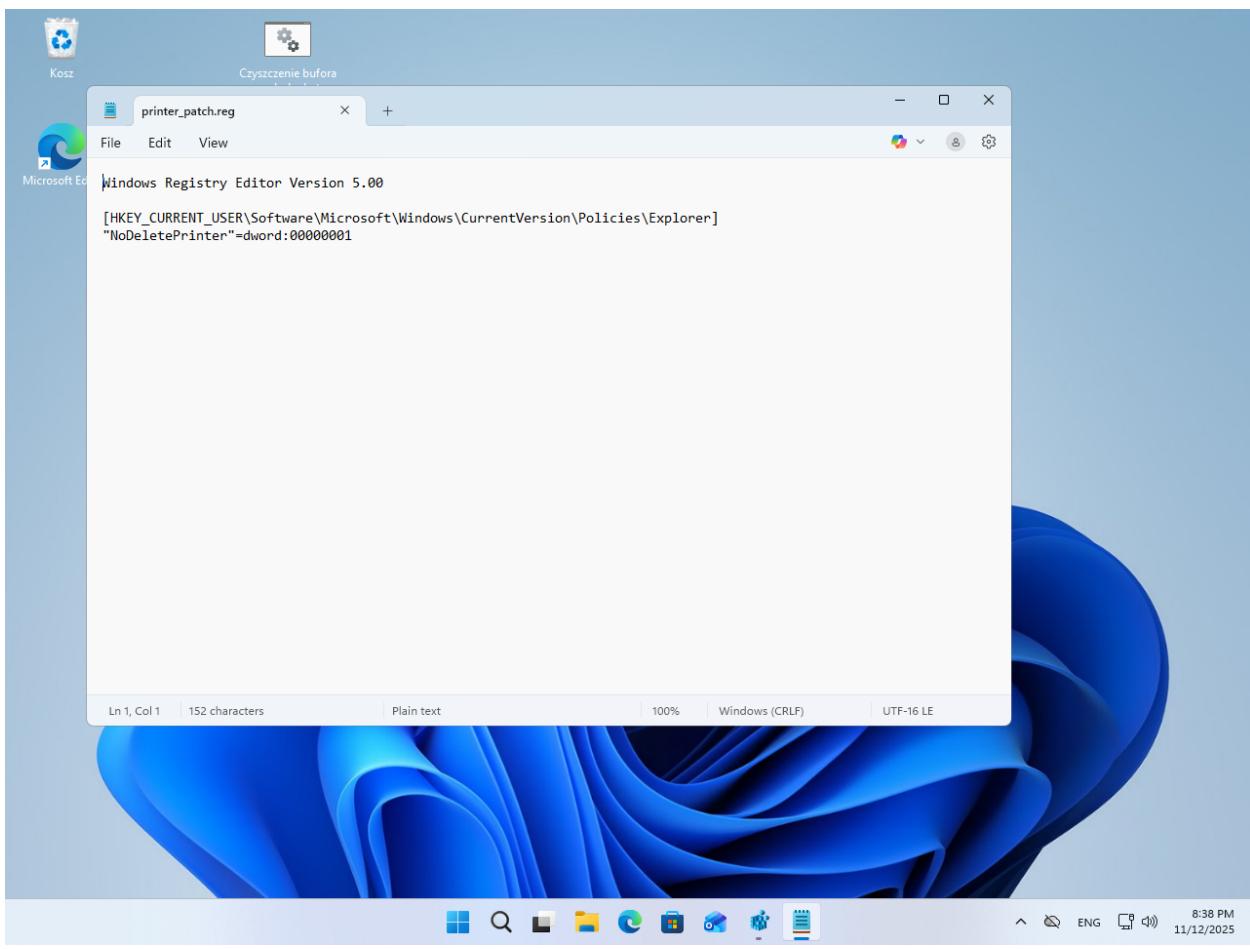
Zrzut ekranu 14 Nieistniejący klucz "Explorer".

Gdybyśmy jednak chcieli taką opcję skonfigurować, należy najpierw utworzyć klucz „Explorer” wewnętrz „Policies”, a następnie dodać do niego wpis „`NoDeletePrinter`” typu DWORD z wartością 1.



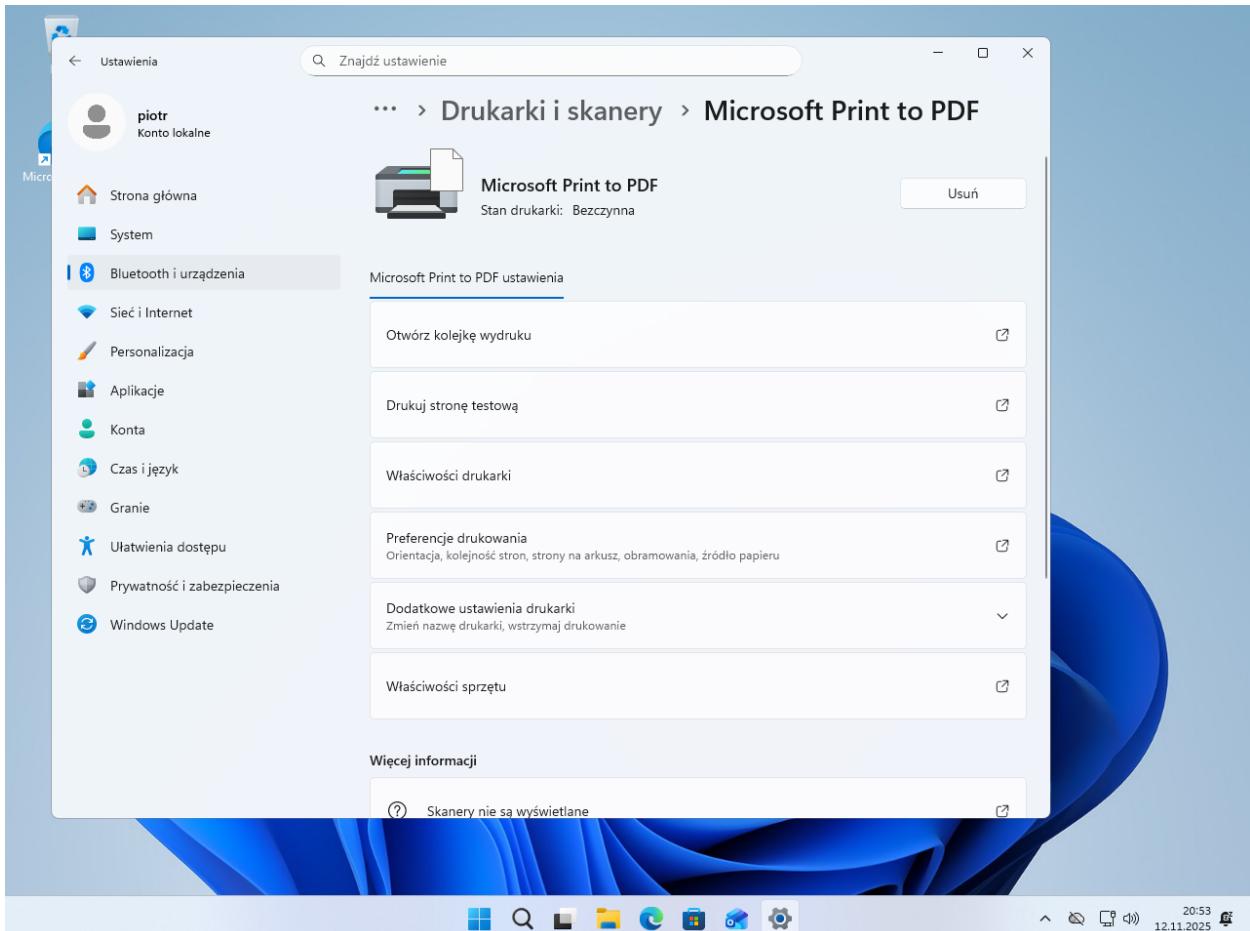
Zrzut ekranu 15 (Przed i po dodaniu wpisu w rejestrze) Ukryta w ustawieniach możliwość usuwania z systemu drukarek.

Jak widać, opcja usuwania drukarek zniknęła z ustawień. Aby było tę zmianę łatwiej rozpowszechniać, można utworzyć w identyczny jak w poprzednim zadaniu sposób „patch rejestrowy”. W tym celu należy prawym przyciskiem myszy kliknąć na klucz w rejestrze i wybrać opcję „Export”.



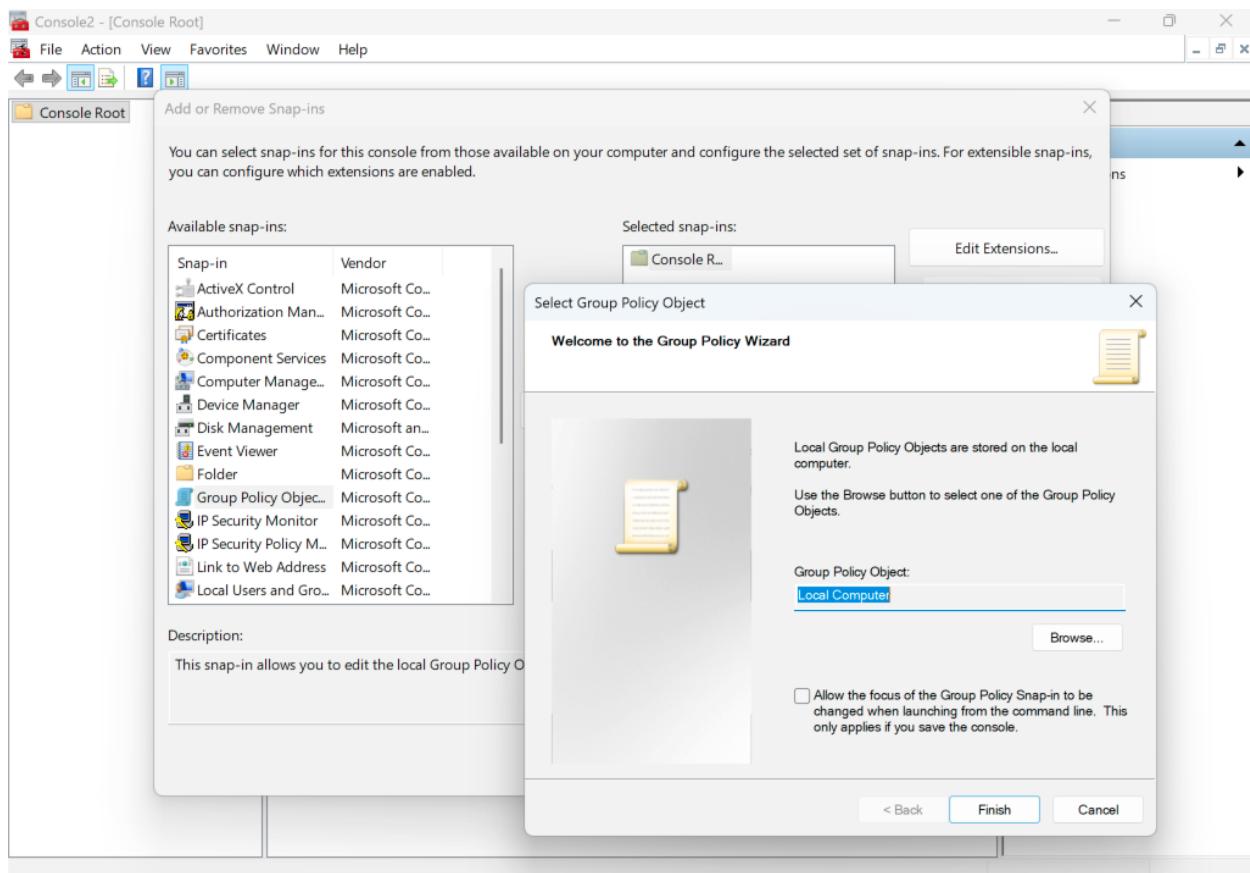
Zrzut ekranu 16 Patch rejestrowy wyłączający możliwość dodawania drukarek dla aktualnie zalogowanego użytkownika.

Tak wprowadzone w rejestrze zmiany dotyczą jednak tylko aktualnie zalogowanego użytkownika. Możemy to sprawdzić tworząc nowe konto na komputerze i przechodząc do ustawień.



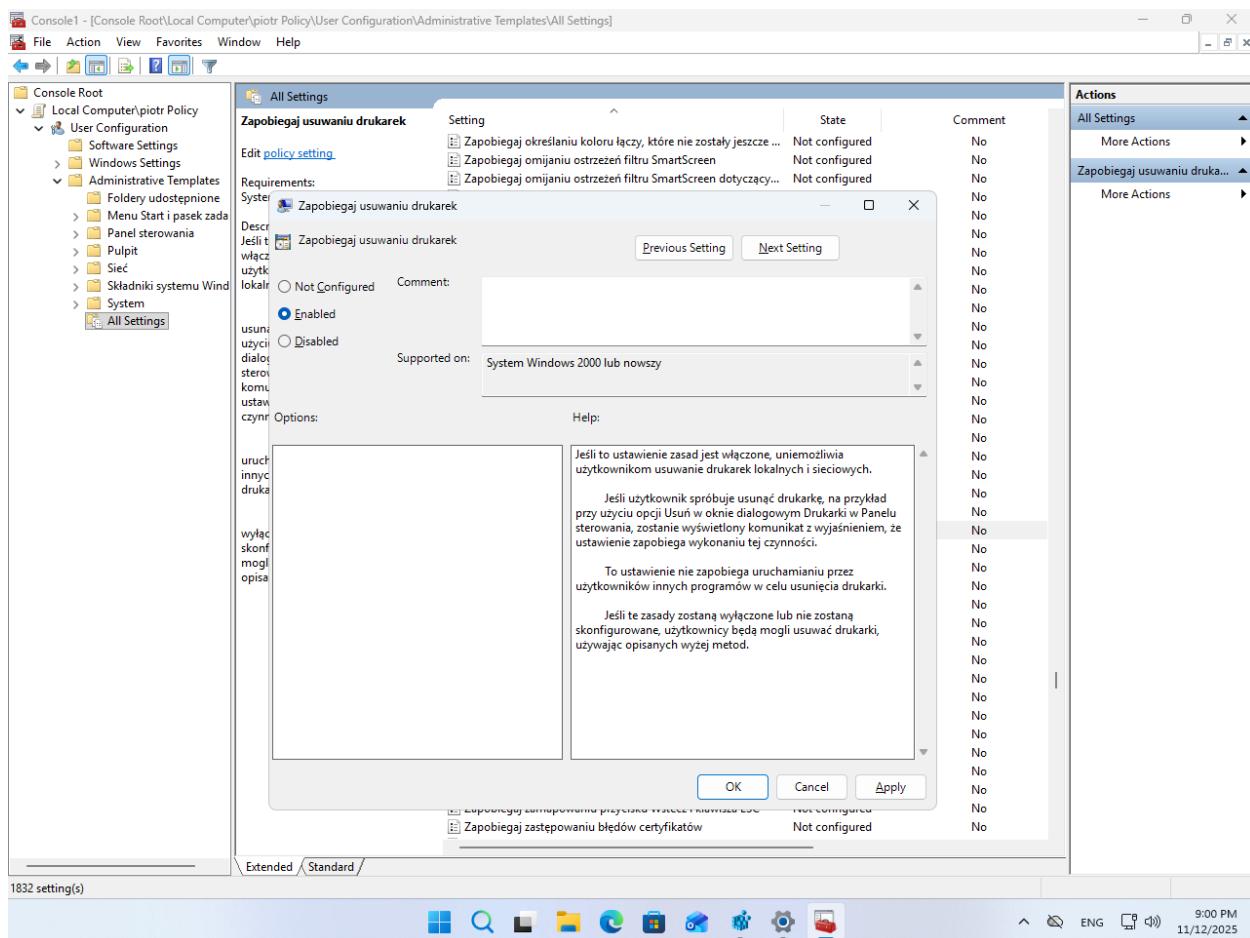
Zrzut ekranu 17 Widoczna opcja usuwania drukarek dla innego użytkownika komputera.

Aby to zmienić, z konta administratora systemu można przejść do programu *Microsoft Management Console* i utworzyć nową zasadę grup lokalnych.



Zrzut ekranu 18 Program Microsoft Management Console. Dodawanie wtyczki do zarządzania zasadami grup lokalnych.

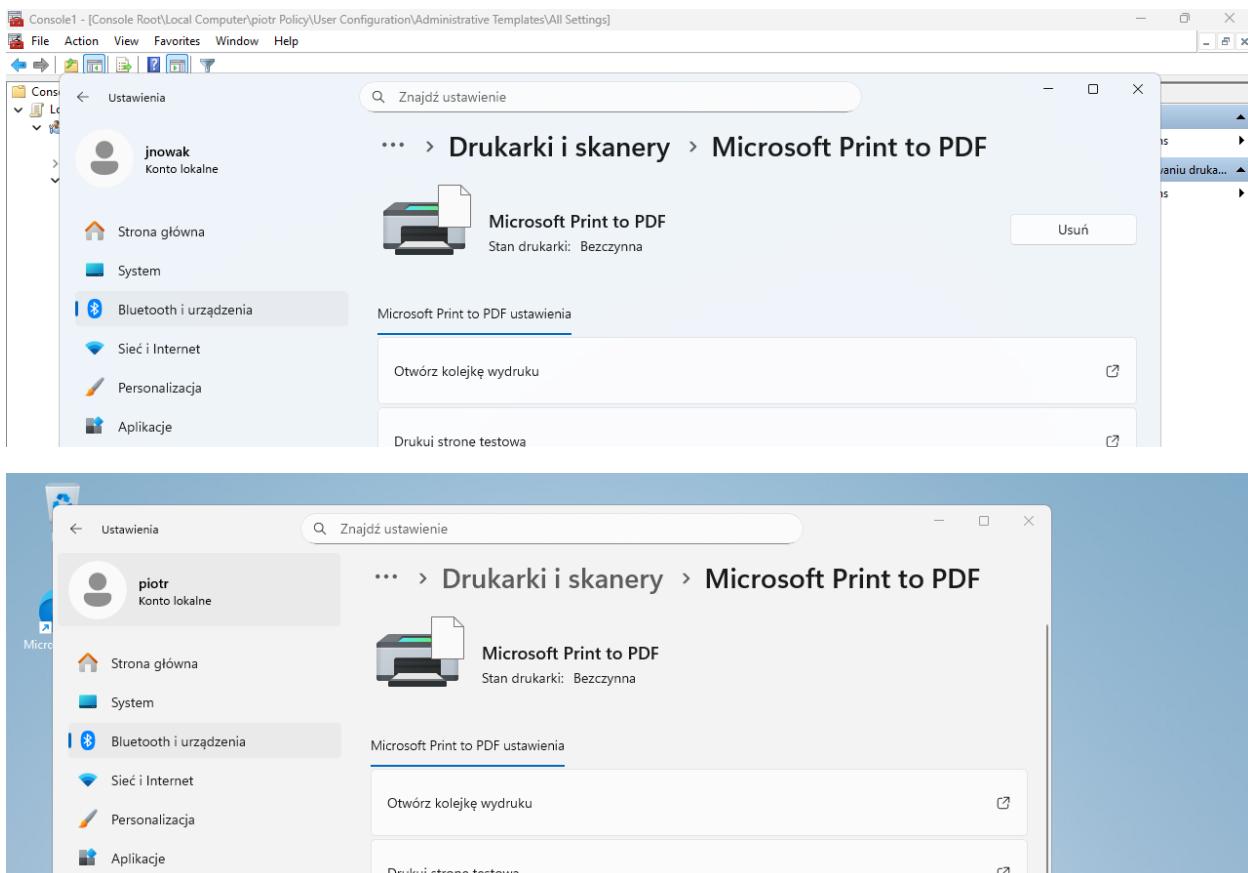
W tym celu z górnego menu programu wybieramy opcję „File” → „Add or Remove Snap-ins” i dodajemy wtyczkę „Group Policy Object”. W okienku konfiguratora klikamy na „Browse...”, a następnie wskazujemy kogo ma się ona dotyczyć – na przykład konta użytkownika *piotr*.



Zrzut ekranu 19 Konfiguracja blokady możliwości usuwania drukarek w zasadach grup lokalnych.

W kolejnym kroku odszukujemy „Zapobiegaj usuwaniu drukarek” na liście zasad lokalnych dla konta *piotr* i zapisujemy zmiany.

Aby potwierdzić poprawność wprowadzonych zmian, zaczniemy od usunięcia z rejestru ręczne wprowadzonego wpisu dotyczącego blokady usuwania drukarek dla konta *jnowak* (administratora systemu). Następnie na obydwu kontach sprawdzimy widoczność przycisku w ustawieniach.



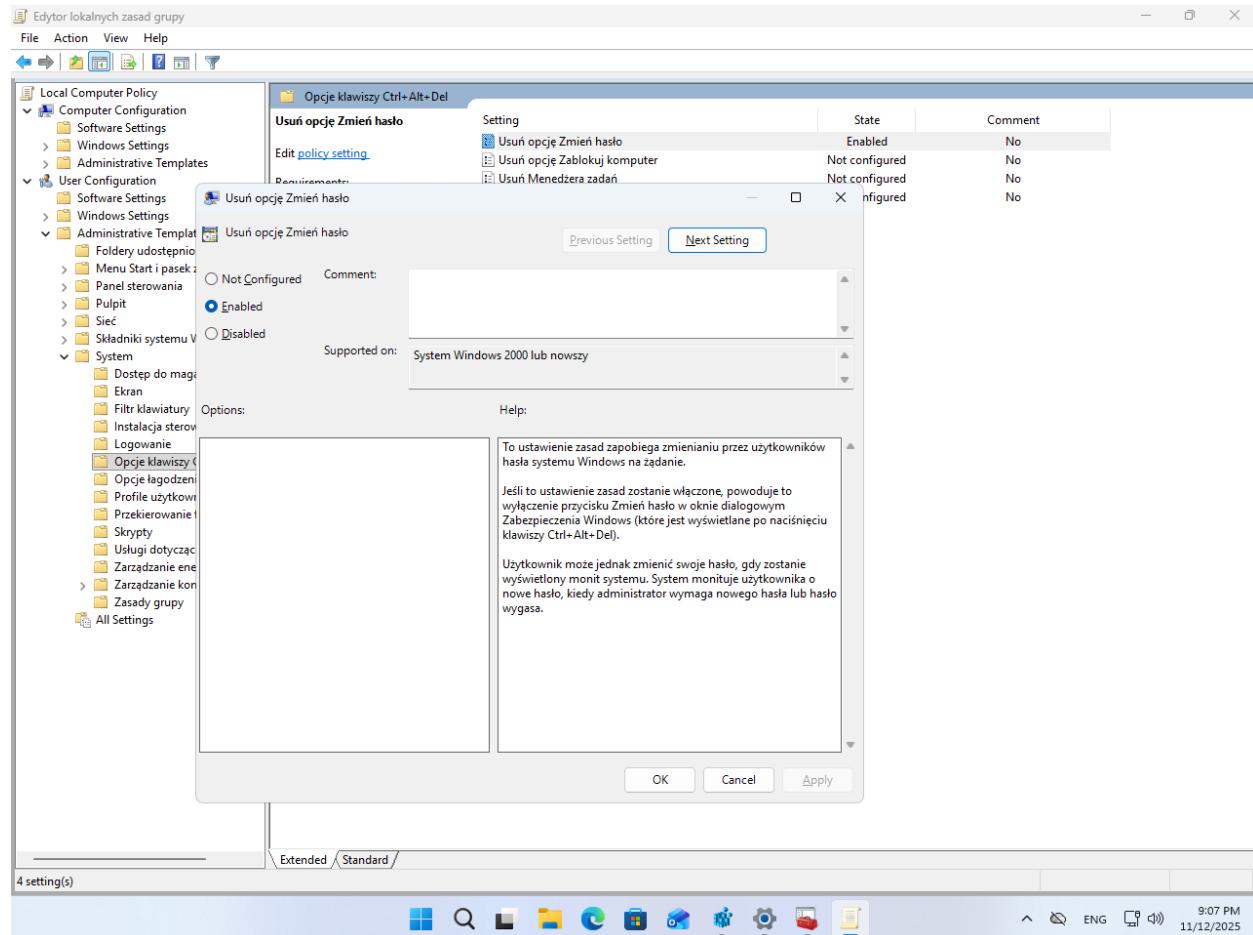
Zrzut ekranu 20 Przycisk do usuwania drukarek ukryty wyłącznie na koncie piotr.

Zgodnie z przewidywaniami, opcja usuwania drukarek jest teraz niedostępna wyłącznie dla użytkownika **piotr**.

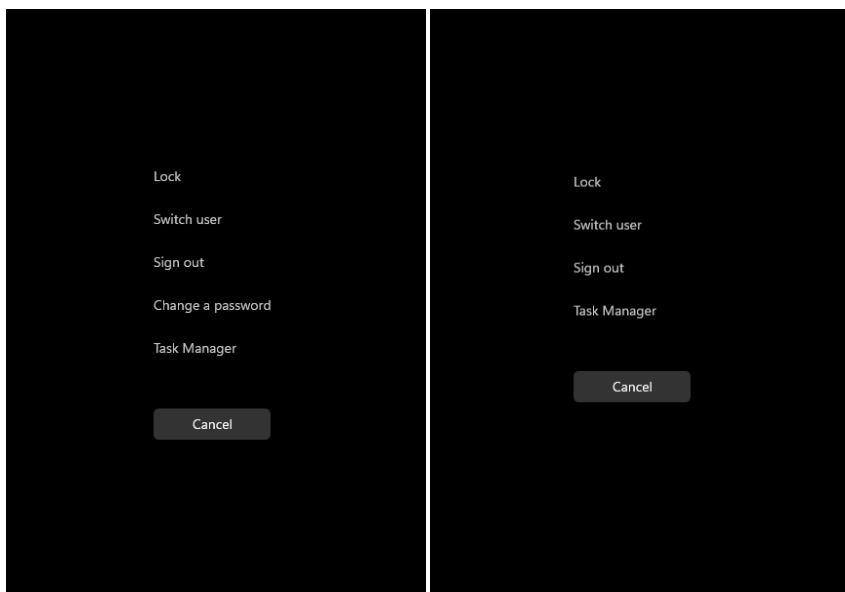
## Zadanie 5. Zasady grup lokalnych.

Wykorzystany w poprzednim zadaniu mechanizm grup lokalnych można też zastosować na przykład do konfiguracji opcji wyświetlnych w menu zabezpieczeń w systemie Windows (wywoływanego kombinacją klawiszy „CTRL+ALT+DELETE”).

Aby ukryć opcję „Zmień hasło” dla aktualnie zalogowanego użytkownika, należy uruchomić aplikację „Edit group policy” i przejść do *User Configuration* → *Administrative Templates* → *System* → *Ctrl+Alt+Delete Options* i włączyć opcję „Remove Change password”.



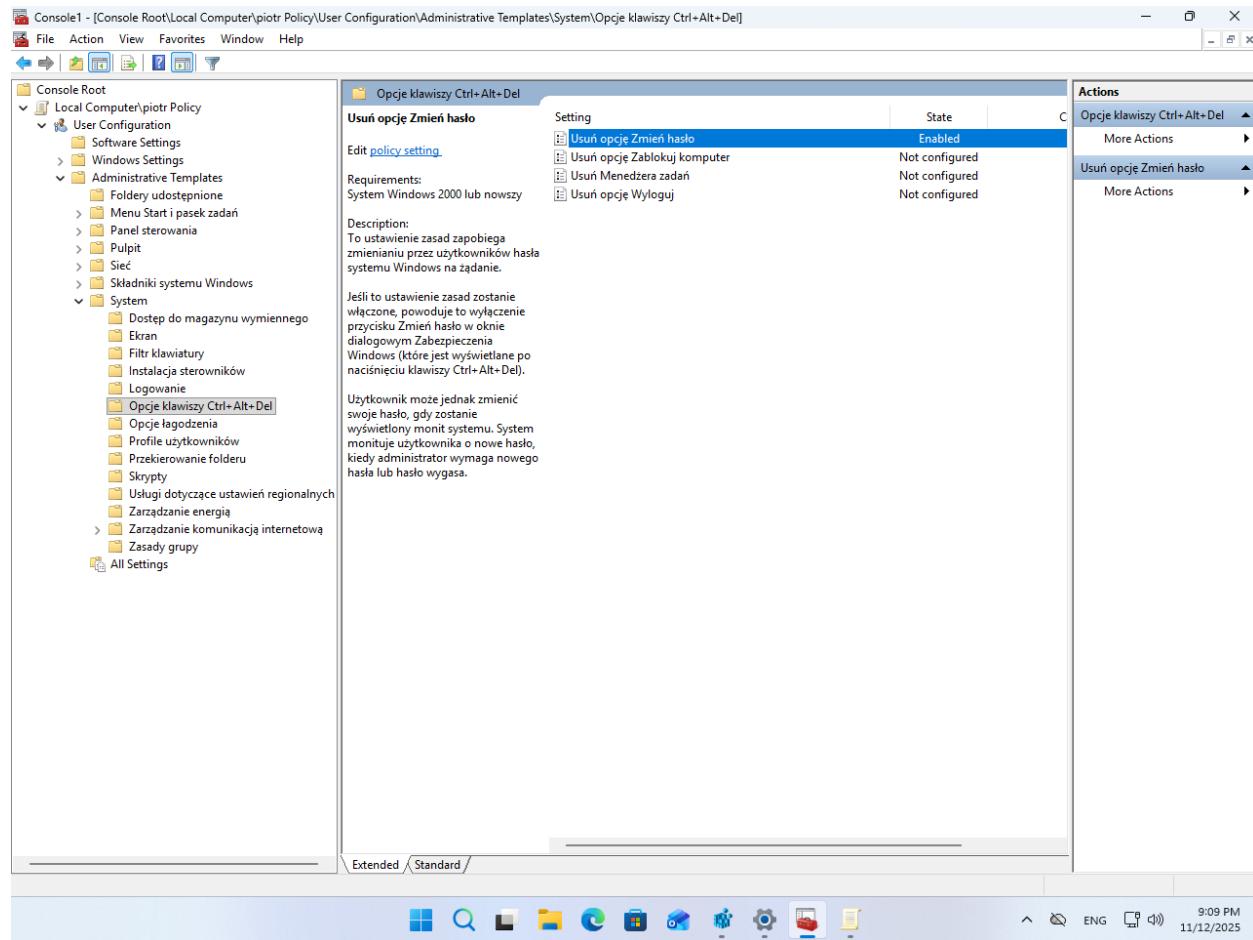
Zrzut ekranu 21 Zasada usuwająca opcję zmiany hasła z ekranu zabezpieczeń systemu Windows.



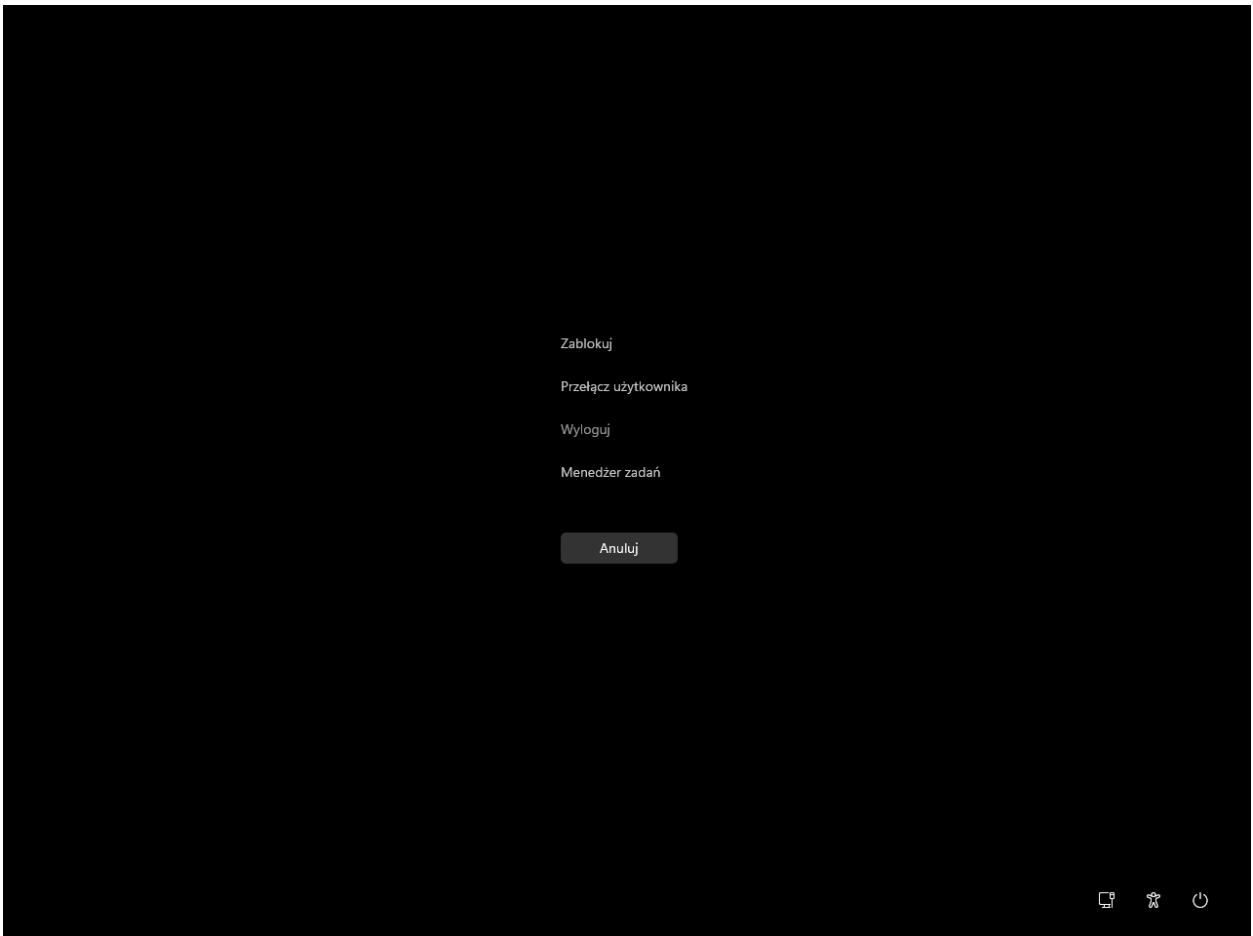
Zrzut ekranu 22 (Przed i po włączeniu zasady ukrywającej opcję zmiany hasła) Ukryta opcja zmiany hasła w menu zabezpieczeń systemu Windows.

Zasada ta została aktywowana jedynie dla aktualnie zalogowanego użytkownika, dlatego *piotr* dalej widzi ją z poziomu menu zabezpieczeń systemu. Aby to zmienić, ponownie wykorzystamy aplikację *Microsoft Management Console* z przystawką zarządzającą zasadami grup lokalnych – a konkretniej zasadami lokalnymi dla konta *piotr*.

Tutaj ponownie odszukujemy opcji pod wyżej wskazaną ścieżką i włączamy blokadę zmiany hasła.



Zrzut ekranu 23 Usunięcie opcji zmiany hasła dla użytkownika *piotr* z poziomu aplikacji *Microsoft Management Console*.

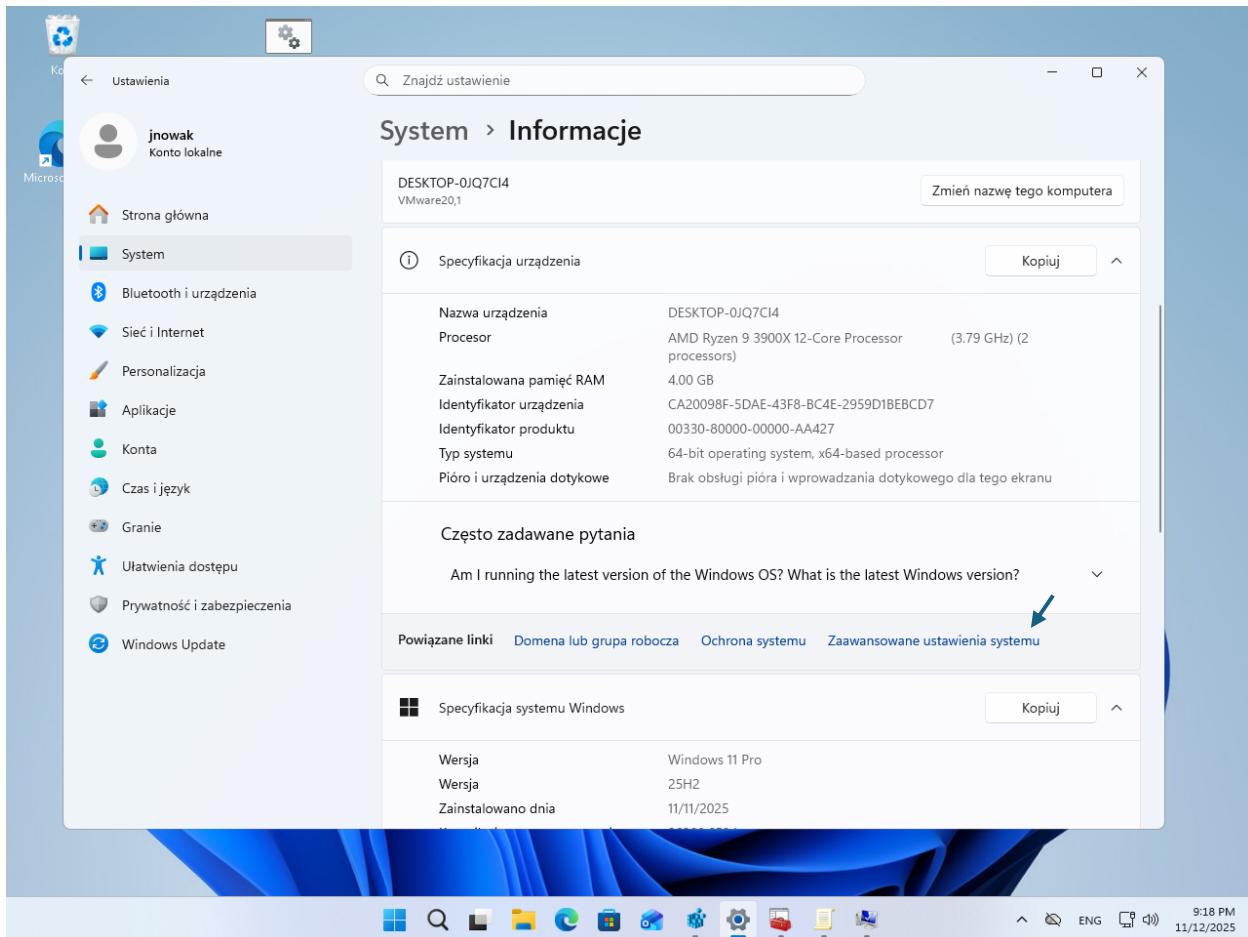


Zrzut ekranu 24 Ekran zabezpieczeń systemu widoczny z poziomu konta użytkownika *piotr*.

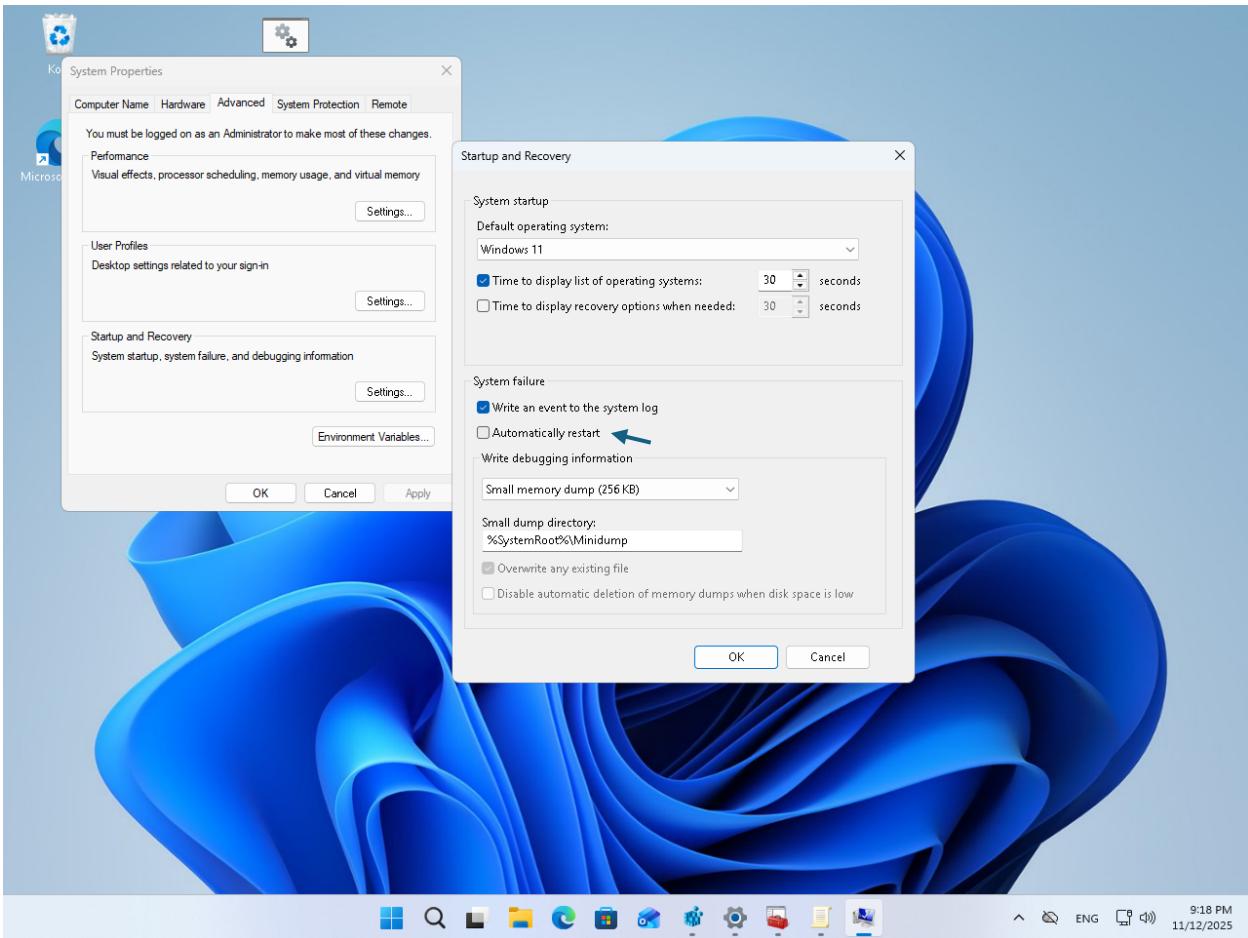
Jak widać, użytkownikowi *piotr* zniknęła opcja zmiany hasła.

## Zadanie 6. Właściwości systemu.

System Windows domyślnie restartuje się po wystąpieniu błędu krytycznego, co utrudnia przepisanie przyczyny wystąpienia problemu. Aby wyświetlić błąd i zapobiec automatycznemu ponownemu uruchomieniu komputera, należy przejść do ustawień systemu, a następnie przejść do „System” → „Information” → „Advanced system settings” → „Advanced” i w grupie „Startup and Recovery” wybrać „Settings”, a na koniec w grupie „System failure” odznaczyć opcję „Automatically restart”.



Zrzut ekranu 25 Przejście do zaawansowanych ustawień systemu z aplikacji Ustawienia.

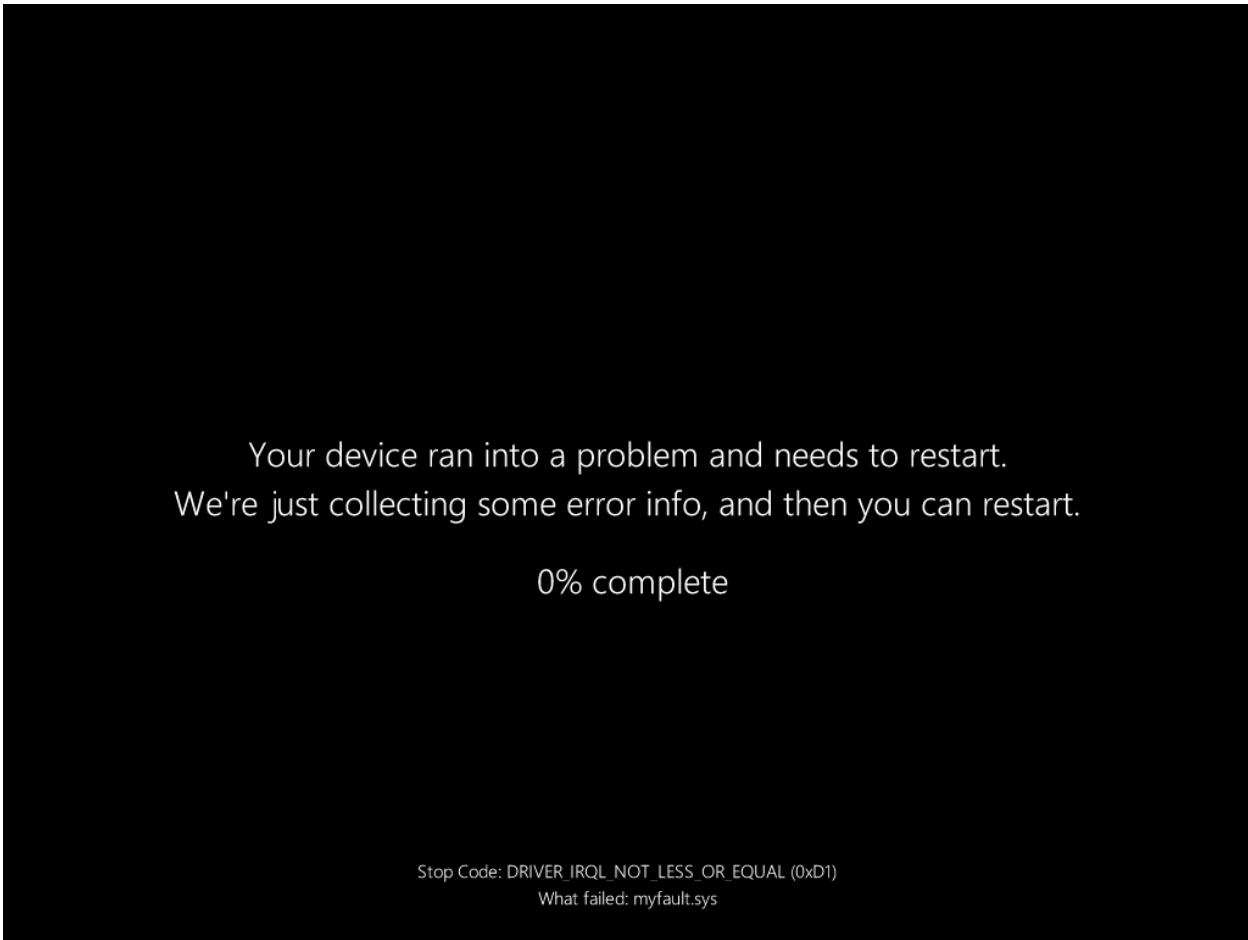


Zrzut ekranu 26 Wyłączenie automatycznego restartu komputera po wystąpieniu błędu krytycznego.

Aby przetestować działanie ustawienia, można skorzystać z programu *NotMyFault*, autorstwa Marka Russinovicha, pochodzącego z zestawu dodatkowych narzędzi systemowych *Sysinternals*.

<https://learn.microsoft.com/en-us/sysinternals/downloads/notmyfault>

Po otwarciu aplikacji i wcisnięciu przycisku „Crash”, system generuje informacje o błędzie krytycznym.



Zrzut ekranu 27 Ekran z informacjami o błędzie krytycznym.

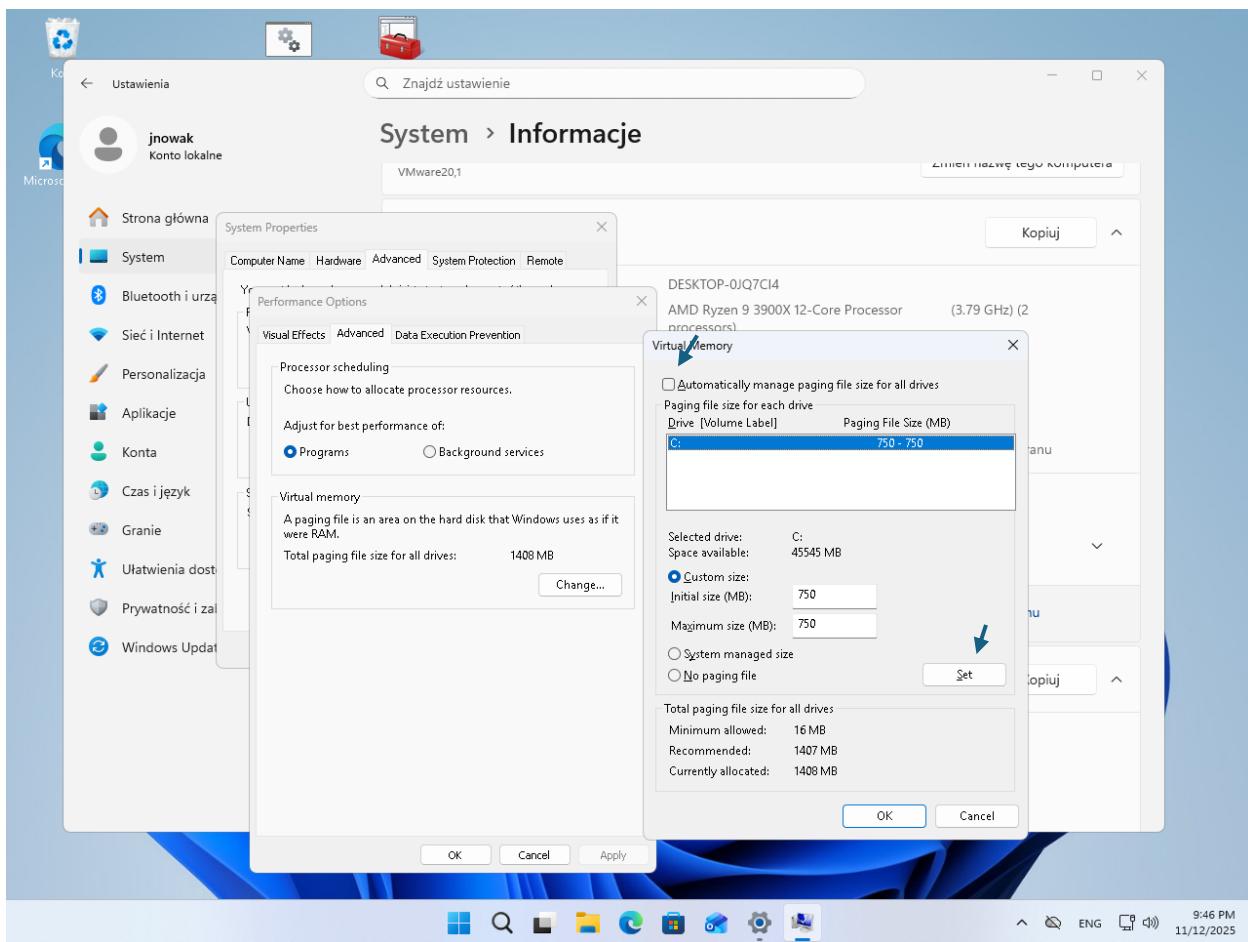
Na ekranie zostały wypisane szczegóły problemu, a po zebraniu informacji o błędzie, system się nie zrestartował.

## Zadanie 7. Ustawienia pliku stronicowania.

Plik stronicowania umożliwia „zwiększenie” ilości posiadanej pamięci RAM. Dane które nie są w danej chwili potrzebne w pamięci tymczasowej, mogą zostać zapisane na dysku komputera. Dzięki temu stan nieaktywnych aplikacji nie jest tracony, a działające programy mają do dyspozycji więcej pamięci RAM.

Taki mechanizm wymaga jednak przydzielenia na dysku określonej ilości miejsca (określenie wielkości pliku stronicowania). Domyślnie, system Windows sam dobiera jego wielkość, ale można ją skonfigurować ręcznie. W tym celu należy wejść do ustawień zaawansowanych systemu (Ustawienia → „System” → „Information” → „Advanced system settings” → „Advanced”), a następnie w grupie „Performance” wybrać „Settings” → zakładka „Advanced” i w grupie „Virtual memory” kliknąć przycisk „Change...”.

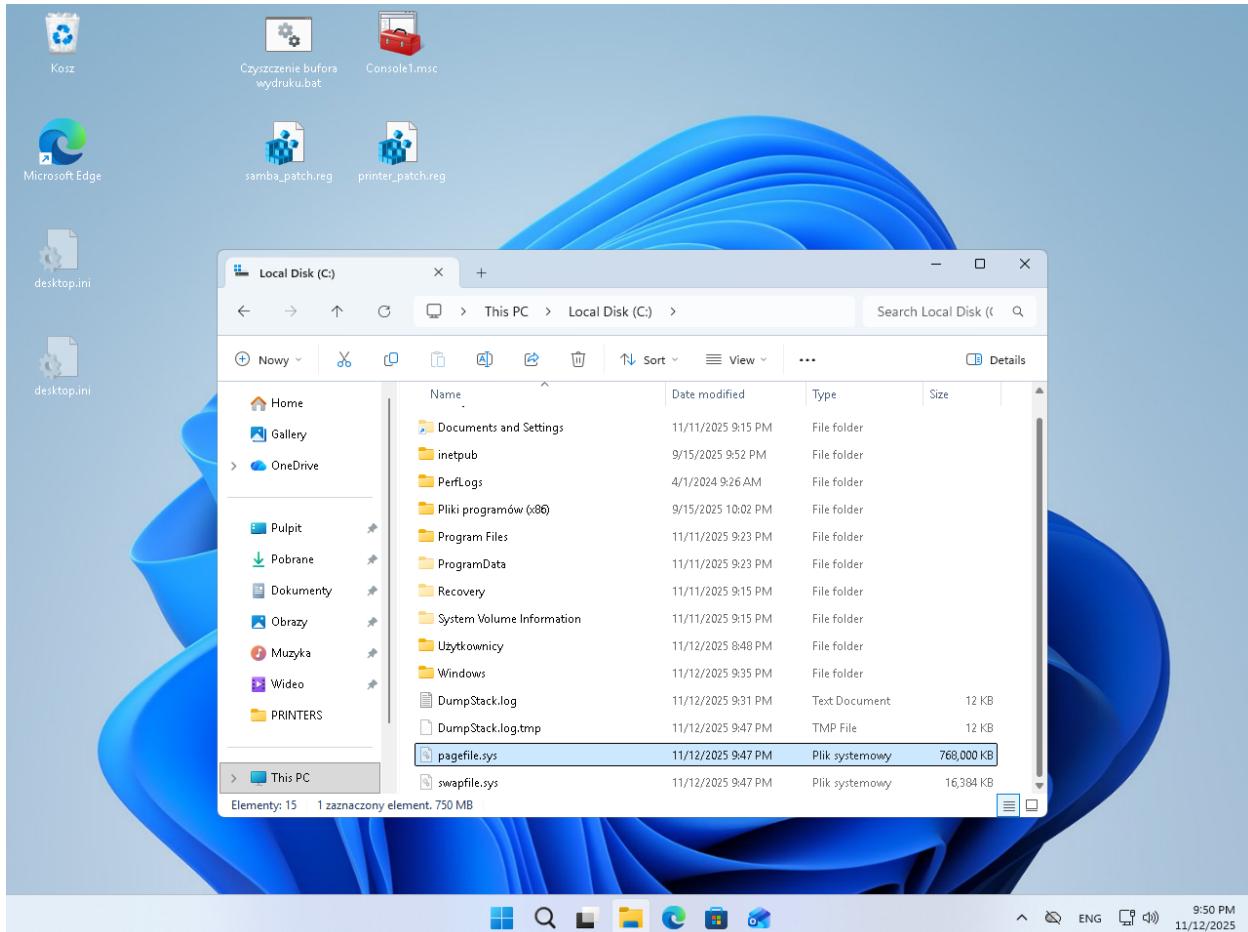
Po odznaczeniu „Automatically manage page file size for all drives” i zaznaczeniu „Custom size” można ręcznie skonfigurować ustawienia pliku stronicowania, a następnie zapisać je przyciskiem „Set”.



Zrzut ekranu 28 Zmiana wielkości pliku stronicowania.

Do wprowadzenia zmian konieczne jest ponowne uruchomienie komputera, co należy uczynić.

Zmiany można potwierdzić włączając w Eksploratorze plików wyświetlanie zasobów systemowych i sprawdzając wielkość pliku *pagefile.sys*.



Zrzut ekranu 29 Sprawdzenie wielkości pliku stronicowania.

Jak widać, plik stronicowania ma rozmiar około 750 MB, zgodnie z tym co ustaliliśmy przed chwilą. Niewielka niezgodność wielkości wynika prawdopodobnie ze sposobu w jaki system Windows zarządza tym zasobem.