

Uprawnienia w systemie Windows

ZAGADNIENIA

- Rodzaje uprawnień występujące w systemie Windows
- Zarządzanie uprawnieniami do folderu
- Zarządzanie uprawnieniami specjalnymi do folderu
- Dziedziczenie uprawnień

Z każdym kontem są związane pewne **prawa** i **przywileje**, na których podstawie system podejmuje decyzję, czy zezwolić na wykonanie czynności, czy też zabronić jej wykonywania. Każdy użytkownik ma swój unikatowy **identyfikator (SID)**, który jest tworzony w momencie zakładania konta. Na podstawie **SID** (a nie nazwy logowania) są identyfikowani użytkownicy i jego prawa.

Ogólnie możliwości związane z kontem można podzielić na:

- **przywileje** – uprawnienia pozwalające na wykonanie określonych zadań administracyjnych, np. dodawanie stacji roboczych do domeny;
- **prawa logowania** – pozwalają użytkownikowi na zalogowanie się do systemu, np. prawo do logowania lokalnego;
- **uprawnienia wbudowane** – wstępnie zdefiniowane uprawnienia, przypisane grupom. Uprawnień tych nie możemy zmieniać, możemy je przekazać innym użytkownikom, dołączając ich do grupy mającej uprawnienie, np. prawo do tworzenia nowych kont;
- **prawa dostępu** – definiują operacje, które mogą być wykonane na zasobach sieciowych, np. prawo do tworzenia plików.

W warunkach szkolnych problem przyznania przywilejów i praw logowania będzie rozwiązany przez dołączenie wybranych użytkowników do grup wbudowanych, mających odpowiednie uprawnienia wbudowane. Przykładowo: jeżeli użytkownik *jankowski* powinien mieć prawo do tworzenia nowych kont sieciowych, to możemy dołączyć go do grupy *Administratorzy domeny*. W dużych sieciach, np. w firmach o skomplikowanej strukturze, mogą być tworzone nowe grupy i przyznawane bardziej szczegółowe przywileje i prawa.

W systemach z rodziny Windows Server uprawnienia zarówno na poziomie udostępniania zasobów, jak i na poziomie systemu plików NTFS bazują na **listach kontroli dostępu** (ang. *Access Control List* – ACL). Pozwalają one na bardzo szczegółowe zdefiniowanie uprawnień do poszczególnych obiektów (np. plików, folderów, udostępnień). Na poziomie systemu plików NTFS istnieje dużo bardzo szczegółowych uprawnień, które można przypisać. Poszczególne uprawnienia będą nazywane **uprawnieniami specjalnymi** lub **zaawansowanymi**. Aby ułatwić zarządzanie uprawnieniami specjalnymi, są one łączone w grupy, które tworzą **uprawnienia**. Innymi słowy, uprawnienie składa się z wielu uprawnień specjalnych. Wykaz tych uprawnień przedstawiono w tabeli 55.1. Uprawnienia specjalne (lewa kolumna) są przypisane do konkretnych grup uprawnień (górny wiersz).

Tabela 55.1. Tabela uprawnień NTFS

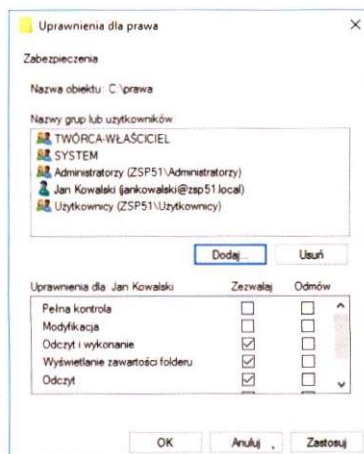
Uprawnienia specjalne	Pełna kontrola	Modyfikacja	Odczyt i wykonanie	Wyświetlanie zawartości folderu (tylko foldery)	Odczyt	Zapis
Przechodzenie przez folder / Wykonywanie pliku	X	X	X	X		
Wyświetlanie zawartości folderu / Odczyt danych	X	X	X	X	X	
Odczyt atrybutów	X	X	X	X	X	
Odczyt atrybutów rozszerzonych	X	X	X	X	X	
Tworzenie plików / Zapis danych	X	X	X			X
Tworzenie folderów / Dołączanie danych	X	X	X			X
Zapis atrybutów	X	X	X			X
Zapis atrybutów rozszerzonych	X	X	X			X
Usuwanie podfolderów i plików	X					
Usuwanie	X	X				
Odczyt uprawnień	X	X	X	X	X	X
Zmiana uprawnień	X					
Przejęcie na własność	X					

Uprawnienia można **nadawać** – Zezwalaj (ang. *Allow*) lub **odbierać** – Odmów (ang. *Deny*). Zaznaczenie pola **Zezwalaj** nadaje użytkownikowi (grupie) dane uprawnienia (rys. 55.1). Uprawnienia każdego użytkownika do danego obiektu są sumą uprawnień wynikających z praw, jakie ma dany użytkownik, oraz wynikających z praw, jakie mają grupy, do których on przynależy. Zaznaczenie **Odmawiaj** ma zastosowanie wtedy, gdy chcemy zabrać użytkownikowi prawo do danego obiektu, mimo posiadania przez niego praw wynikających z jego przynależności do danej grupy użytkowników. Odmowa uprawnienia jest ważniejsza niż zezwolenie. Stosujemy ją, gdy chcemy stworzyć wyjątek. Załóżmy, że *jankowalski* jest członkiem grupy *uczniowie*. Jeżeli nadamy uprawnienie (**Zezwalaj**) do folderu grupie *uczniowie*, to z faktu przynależności do niej otrzyma uprawnienie również *jankowalski*. Jeżeli odmówimy uprawnienia (**Odmów**) użytkownikowi *jankowalski*, to nie będzie on miał uprawnienia, mimo że powinien je mieć z racji przynależności do grupy *uczniowie*.

PRZYKŁAD 55.1**Zarządzanie uprawnieniami do folderu**

Aby zmieniać lub przeglądać uprawnienia do folderu, należy:

1. Kliknąć prawym przyciskiem myszy folder, którego uprawnienia będą modyfikowane, i z menu kontekstowego wybrać **Właściwości**, a następnie zakładkę **Zabezpieczenia**.
2. Kliknąć przycisk **Edytuj**, a następnie przycisk **Dodaj**, aby dodać użytkownika lub grupę do listy uprawnionych (jeżeli użytkownik jest na liście, wystarczy go wskazać i przejść do punktu 5.).
3. Wprowadzić nazwę użytkownika, który ma być dodany do listy uprawnionych.
4. Wskazać kursorem użytkownika, którego uprawnienia będą modyfikowane.
5. Zaznaczyć uprawnienia (**Zezwalaj** lub **Odmów**), które mają być zmodyfikowane, i kliknąć przycisk **Zastosuj**.

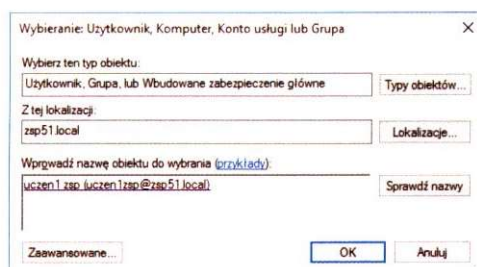


Rys. 55.1. Uprawnienia użytkownika do folderu

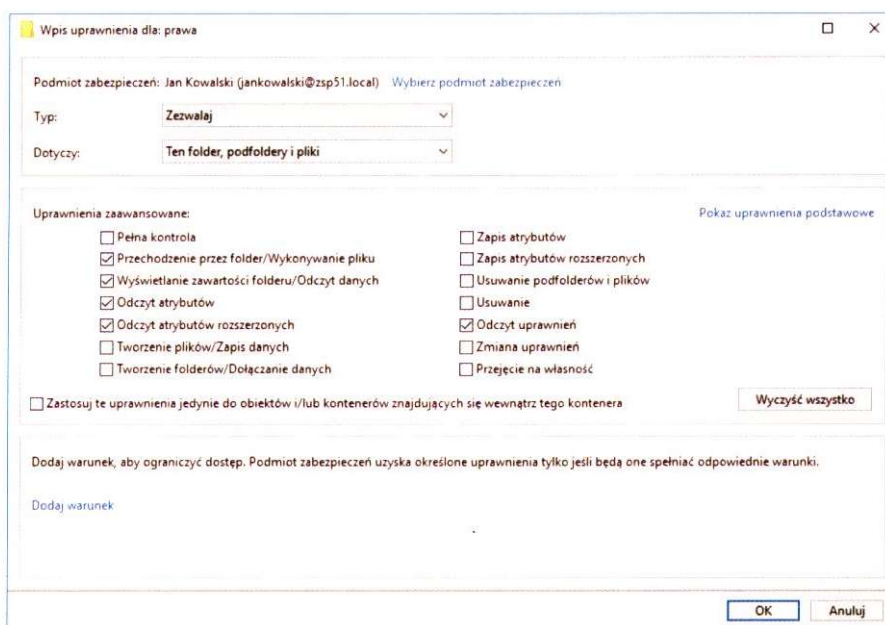
PRZYKŁAD 55.2**Zarządzanie uprawnieniami specjalnymi do folderu**

Aby zmienić lub przeglądać uprawnienia specjalne do folderu, należy:

1. Kliknąć prawym przyciskiem myszy folder, którego uprawnienia będą modyfikowane, i z menu kontekstowego wybrać **Właściwości**, a następnie zakładkę **Zabezpieczenia**.
2. Kliknąć przycisk **Zaawansowane**.
3. W zakładce **Uprawnienia**, jeżeli użytkownik jest na liście, to wystarczy go wskazać i przejść do punktu 5.
4. Kliknąć przycisk **Dodaj**. Kliknąć odnośnik **Wybierz podmiot zabezpieczeń** i wprowadzić nazwę użytkownika, który ma być dodany do listy uprawnionych (rys. 55.2). Kliknąć przycisk **OK**.
5. Wskazać myszą użytkownika, którego uprawnienia będą modyfikowane, i kliknąć przycisk **Edytuj**.
6. Kliknąć odnośnik **Pokaż uprawnienia zaawansowane**.
7. W polu **Typ** wskazać typ uprawnień (**Zezwalaj** lub **Odmów**), które mają być zmodyfikowane, i kliknąć przycisk **OK** (rys. 55.3).



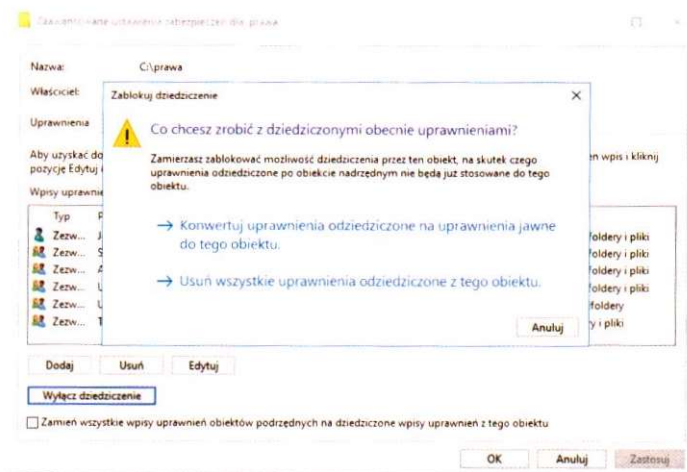
Rys. 55.2. Wybór podmiotu zabezpieczeń



Rys. 55.3. Uprawnienia zaawansowane użytkownika do folderu

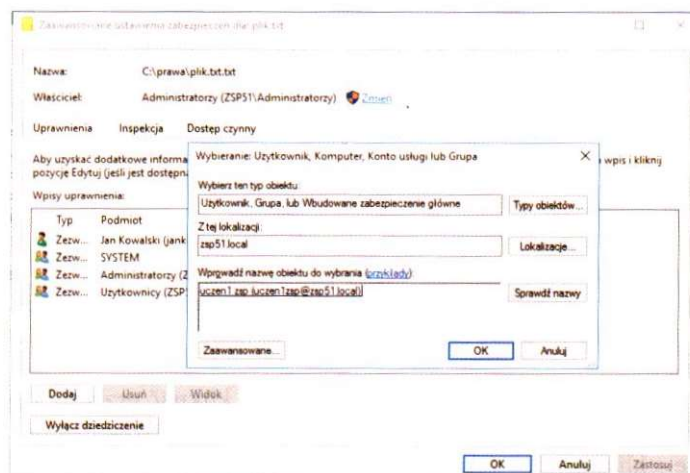
Jedną z ważniejszych zalet mechanizmu uprawnień jest możliwość dziedziczenia uprawnień. **Dziedziczenie** uprawnień pozwala, aby np. wszystkie pliki czy podfoldery dziedziczyły uprawnienia z folderu nadrzędnego. Jeśli podczas przeglądania uprawnień dla obiektu pola wyboru uprawnień **Zezwalaj** i **Odmów** są zaciemnione, oznacza to, że obiekt odziedziczył uprawnienia z obiektu nadrzędnego. Istnieją trzy sposoby wprowadzania zmian w uprawnieniach dziedziczonych:

- **jawne wprowadzenie zmian w obiekcie nadrzędnym** – obiekt podrzędny odziedziczy zmienione uprawnienia;
- **jawne wprowadzenie zmian w obiekcie**, np. zaznaczenie uprawnienia **Zezwalaj**, aby zastąpić dziedziczone uprawnienie **Odmów**;
- **wyłączenie dziedziczenia** – kliknąć przycisk **Wyłącz dziedziczenie** i wybrać sposób postępowania z dziedziczonymi obecnie uprawnieniami (rys. 55.4). Następnie wprowadzić zmiany w uprawnieniach – obiekt nie będzie już dziedziczył uprawnień po obiekcie nadrzędnym. Kliknąć przycisk **OK**.



Rys. 55.4. Wyłączanie dziedziczenia uprawnień

Każdy obiekt, np. plik, ma swojego **właściciela**. Domyślnie jest nim ten, kto obiekt stworzył. Bez względu na uprawnienia właściciel zawsze może zmienić prawa ustawione dla swojego obiektu, a w szczególności zabrać sobie samemu prawa do niego. Wtedy nie ma możliwości np. odczytania danego pliku, jeżeli wcześniej nie przywróci sobie praw. Zmiany właściciela pliku można dokonać w oknie **Zaawansowane ustawienia zabezpieczeń** (rys. 55.5). Należy kliknąć odnośnik **Zmień** i wskazać nowego właściciela.



Rys. 55.5. Zmiana właściciela pliku

SPRAWDŹ SWOJĄ WIEDZĘ

1. Wymień rodzaje uprawnień występujących w systemie Windows.
2. Co to są uprawnienia specjalne do folderu? Jak nimi zarządzać?
3. Wypisz uprawnienia specjalne, które składają się na prawo zapisywania w folderze.
4. Na czym polega mechanizm dziedziczenia uprawnień? Podaj przykłady.
5. Do czego służy odmowa uprawnienia (**Odmów**)? Podaj przykłady wykorzystania.

Udostępnianie zasobów i przypisywanie uprawnień do udostępnianych zasobów

ZAGADNIENIA

- Uprawnienia nadawane do udostępnianych zasobów
- Udostępnianie folderów i przypisywanie do nich uprawnień

Jeśli udostępniamy zasób w sieci, możemy każdemu użytkownikowi lub grupie przydzielić uprawnienia:

- **pełna kontrola** – użytkownik ma pełne prawa – może tworzyć nowe pliki, odczytywać, modyfikować, zapisywać i usuwać już istniejące oraz zmieniać uprawnienia i przejmować je na własność;
- **zmiana** – użytkownik ma te same uprawnienia co pełna kontrola poza prawem do zmiany uprawnień i przejmowania na własność, czyli może tworzyć nowe pliki, odczytywać, modyfikować, zapisywać i usuwać już istniejące;
- **odczyt** – użytkownik ma prawo do odczytywania plików (w tym ich uruchamiania), nie może tworzyć nowych plików i usuwać ani modyfikować już istniejących.

Uprawnienia do udostępnionego zasobu sieciowego, np. folderu, są wypadkową wynikającą z uprawnień nadanych na poziomie udostępniania udziału oraz na poziomie systemu plików NTFS. Oznacza to, że zawsze zostaną zastosowane bardziej rygorystyczne uprawnienia.

PRZYKŁAD 56.1

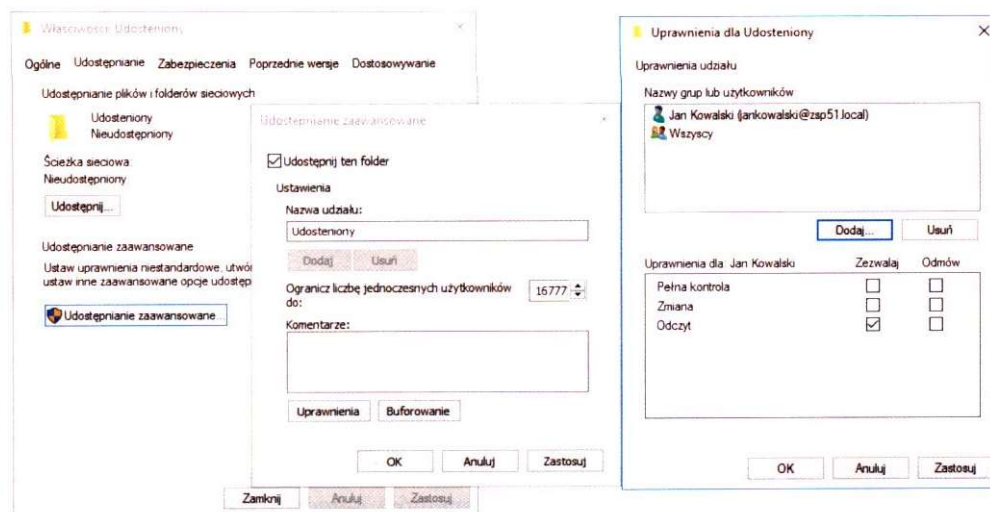
Udostępnianie folderu

Aby udostępnić folder w sieci, należy:

1. Kliknąć prawym przyciskiem myszy folder i wybrać **Właściwości**.
2. Wybrać zakładkę **Udostępnianie** i kliknąć przycisk **Udostępnianie zaawansowane**.
3. Zaznaczyć opcję **Udostępnij ten folder** i kliknąć przycisk **Uprawnienia**.
4. W oknie **Uprawnienia dla** (rys. 56.1) wskazać użytkownika (jeżeli nie ma go na liście – kliknąć przycisk **Dodaj** i dodać użytkownika do listy).
5. Zaznaczyć uprawnienia (**Zezwalaj** lub **Odmów**), które mają być zmodyfikowane, i kliknąć przycisk **OK** (rys. 56.1).

! UWAGA

Nie zapomnij o nadaniu uprawnień w systemie NTFS. Jeżeli użytkownik nie otrzyma uprawnień do pliku, to pomimo udostępnienia zasobów będzie on niedostępny.



Rys. 56.1. Uprawnienia do udostępnianego zasobu

SPRAWDŹ SWOJE UMIEJĘTNOŚCI

1. Utwórz folder Pliki. Udostępnij go w sieci. Przydziel uprawnienia:
 - uczniom wszystkich klas i grup – tylko możliwość odczytywania plików;
 - nauczycielom – możliwość odczytywania i zapisywania;
 - kontu nauczyciel1 – pełne prawa do folderu.

W folderze Pliki każdy z pięciu nauczycieli ma folder prywatny, np. **nauczyciel1** – nikt poza nim nie może mieć żadnych uprawnień do tego folderu.