



Prawa dostępu w systemach operacyjnych

- [Wprowadzenie](#)
- [Przeczytaj](#)
- [Prezentacja multimedialna](#)
- [Sprawdź się](#)
- [Dla nauczyciela](#)



Źródło: Glenn Carstens-Peters, domena publiczna.

Jednym z podstawowych zadań, jakie możemy realizować w systemie operacyjnym, jest dostęp do plików i folderów. W wielu przypadkach z jednego komputera lub usług zainstalowanych na danym komputerze korzysta wielu użytkowników. Należy zatem zdefiniować i skonfigurować uprawnienia dostępu do poszczególnych zasobów dla użytkowników lub grup użytkowników pracujących na danym systemie. Każdy system operacyjny wyposażony jest w mechanizmy pozwalające definiować uprawnienia do plików i folderów w łatwy i prosty sposób.

Twoje cele

- Poznasz podstawowe uprawnienia użytkowników względem plików i folderów.
- Dowiesz się, jakie zasady obowiązują podczas definiowania uprawnień.
- Nauczysz się definiować uprawnienia do plików i folderów systemie Windows 10.

Przeczytaj

Definiowanie uprawnień do plików i folderów to jedna z **podstawowych funkcjonalności** nowoczesnych systemów operacyjnych. Dzięki temu, gdy z komputera korzysta wielu użytkowników (np. w szkole), możemy ustalać różne poziomy dostępu i uprawnień do zasobów danego komputera dla poszczególnych użytkowników oraz grup użytkowników.

Taki mechanizm pozwala określać zarówno do jakich plików i katalogów dany użytkownik **ma dostęp** w ogóle, do jakich **nie ma dostępu**, a także co może z danym zasobem lub w ramach danego zasobu robić (tworzyć pliki, zmieniać dane w plikach, itp).

Uprawnienia w systemie Windows

W systemach Windows powszechnie stosowany jest **system plików** o nazwie **NTFS**. **System plików określa metody i sposoby przechowywania plików na dysku twardym komputera**. Dodatkowo NTFS pozwala na **określanie uprawnień do poszczególnych folderów i plików** zapisanych w pamięci komputera względem poszczególnych użytkowników systemu.

Mechanizm ten w systemie plików NTFS nazywany jest **listą kontroli dostępu** (ang. **ACL** – *Access Control List*).

Ważne!

Listy kontroli dostępu to nic innego jak **zbiór uprawnień danego użytkownika do określonego pliku i/lub katalogu definiujący co dany użytkownik może z zasobem, do którego posiada określone uprawnienia zrobić**, to znaczy, czy może go wyświetlać, zmieniać, tworzyć nowe pliki w danym katalogu lub też czy mamy zabroniony dostęp do danego katalogu.

W systemie **NTFS** stosuje się dwie grupy uprawnień:

- **podstawowe,**
- **zaawansowane.**

Do podstawowych uprawnień do folderów i plików zaliczamy:

- **Zapis** – to uprawnienie pozwala (lub zabrania) na tworzenie plików i folderów, zapis danych do plików oraz ich modyfikacje, a także określanie atrybutów.
- **Odczyt** – to uprawnienie pozwala (lub zabrania) odczytywać dane oraz atrybuty z plików, nie pozwala natomiast na zapis do pliku.
- **Odczyt i wykonanie** – to uprawnienie pozwala (lub zabrania) wyświetlać zawartość oraz uprawnienia do folderu, odczytywać dane i uprawnienia do pliku, a także

uruchamiać programy zapisane w folderze oraz przechodzić przez folder.

- **Wyświetlenie zawartości folderu** – to uprawnienie również pozwala (lub zabrania) wyświetlać zawartość oraz uprawnienia, ale tylko w odniesieniu do folderów. W przypadku plików to uprawnienie nie pojawia się na liście uprawnień.
- **Modyfikacja** – to uprawnienie pozwala (lub zabrania) użytkownikowi wykonywać wszystkie możliwe operacje poza usuwaniem plików i podkatalogów, bez możliwości zmiany ich uprawnień i przejmowania na własność.
- **Pełna kontrola** – to uprawnienie pozwala (lub zabrania) na wykonywanie wszystkich operacji na folderze i pliku, łącznie z usuwaniem plików i podkatalogów w danym folderze, włącznie ze zmianą uprawnień i przejściem własności.

Każde z wymienionych uprawnień może mieć 3 statusy:

- **Zezwalaj** (ang. *allow*) – ten status określa czy użytkownik lub grupa użytkowników ma przydzielone prawo do wykonywania określonej czynności.
- **Odmów** (ang. *deny*) – ten status informuje czy określony użytkownik lub grupa użytkowników ma odebrane prawo do wykonywania określonej czynności.
- **Nieprzydzielone** (nieokreślone) – oznacza, że nie określono statusu zezwalaj ani odmów dla poszczególnych uprawnień.

Wymienione uprawnienia są wystarczające w większości sytuacji i scenariuszy. Czasami jednak bywa tak, że administrator systemu chce uszczegółowić uprawnienia jeszcze bardziej. W takiej sytuacji można zastosować uprawnienia zaawansowane, do których zaliczyć możemy:

- **Przechodzenie poprzez folder** – to uprawnienie pozwala na dostęp do pliku w sytuacji, gdy użytkownik nie posiada uprawnień do katalogu przechowującego ten plik, ale posiada je do samego pliku.
- **Wykonanie** – to uprawnienie pozwala na uruchamianie pliku zawierającego kod programu. Prawo to stosuje się jedynie do plików.
- **Odczyt atrybutów** – to uprawnienie pozwala na przeglądanie atrybutów pliku lub folderu.
- **Odczyt atrybutów rozszerzonych** – to uprawnienie pozwala na przeglądanie rozszerzonych atrybutów pliku bądź folderu. Do rozszerzonych atrybutów należy zaliczyć kompresję i szyfrowanie.
- **Tworzenie plików/Zapis danych** – to uprawnienie pozwala na tworzenie plików wewnątrz folderu oraz na dokonywanie zmian w plikach i nadpisywania ich zawartości.
- **Tworzenie folderów/Dołączanie danych** – to uprawnienie pozwala na tworzenie podkatalogów wewnątrz folderu, a także na dopisywanie nowych danych do plików.
- **Zapis atrybutów** – to uprawnienie pozwala na zmianę atrybutów pliku lub folderu.

- **Zapis rozszerzonych atrybutów** – to uprawnienie pozwala na zmianę atrybutów rozszerzonych pliku lub folderu.
- **Usuwanie podfolderów i plików** – to uprawnienie pozwala na usuwanie znajdujących się w folderze plików oraz podfolderów.
- **Usuwanie** – to uprawnienie pozwala na usuwanie plików i katalogów.
- **Odczyt uprawnień** – to uprawnienie pozwala na odczyt uprawnień zastosowanych do plików lub folderów.
- **Zmiana uprawnień** – to uprawnienie pozwala na zmianę uprawnień zastosowanych do plików lub folderów, takich jak: Pełna kontrola, Zapis, Odczyt.
- **Przejęcie na własność** – to uprawnienie pozwala na przejęcie pliku lub folderu na własność.

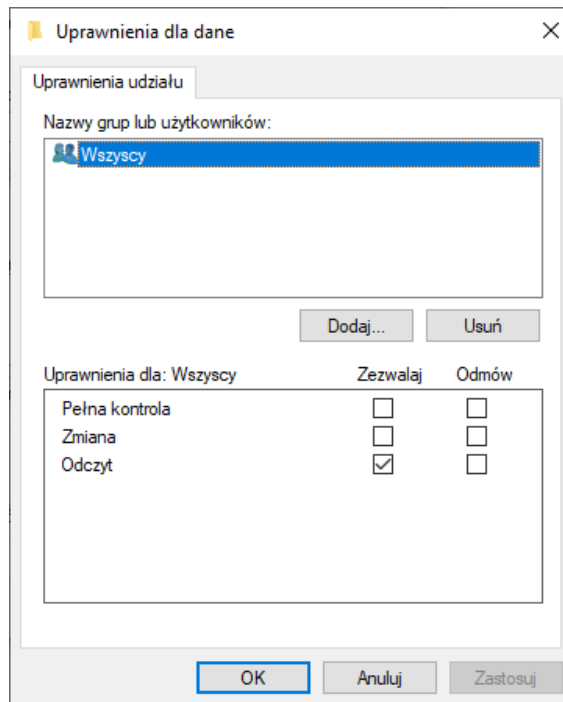
Ważne!

Właściciel pliku lub folderu (użytkownik, który go utworzył) może zawsze zmienić jego uprawnienia, niezależnie od tego, jakie uprawnienia nadał dla katalogu lub pliku administrator systemu.

Uprawnienia sieciowe

W przypadku zasobów, które udostępnione są w sieci lokalnej z wykorzystaniem [protokołu SMB](#), wyróżnia się tylko trzy rodzaje uprawnień.

- **Odczyt** – jest to rodzaj uprawnienia, które nadawane jest wszystkim użytkownikom w momencie udostępniania katalogu w sieci lokalnej. Pozwala przeglądać foldery, odczytywać pliki i uruchamiać programy zapisane w katalogach.
- **Zmiana** – pozwala użytkownikowi na odczyt danych i możliwość tworzenia plików i katalogów, a także dokonywania zmian w plikach.
- **Pełna kontrola** – pozwala na pełną kontrolę danych, w tym odczyt i zapis.



Okno nadawania uprawnień na poziomie sieci lokalnej

Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Słownik

uprawnienia efektywne

suma uprawnień użytkownika uwzględniająca jego uprawnienia oraz uprawnienia grupy do której należy

protokół SMB

protokół sieci komputerowych pozwalający udostępniać pliki i foldery w sieci lokalnej

Prezentacja multimedialna

Polecenie 1

Zapoznaj się z prezentacją.

Zasady dotyczące stosowania uprawnień NTFS

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/P114b541x>

1

Stosując uprawnienia NTFS w systemach Windows, pamiętać należy o trzech **ważnych** zasadach.

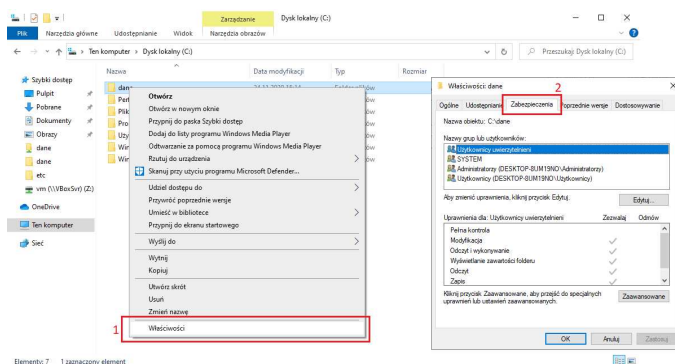
1. Uprawnienia NTFS są **dziedziczone**. To znaczy, że jeśli do katalogu XYZ użytkownik **x1** ma uprawnienia tylko do odczytu, to takie same uprawnienia będzie miał do wszystkich zasobów zapisanych w tym katalogu (chyba, że dziedziczenie zostanie wyłączone).
2. Uprawnienia NTFS są **kumulowane** (sumowane). To znaczy, że jeśli użytkownik **x1** należy do grupy **gx1**, to jego uprawnienia efektywne są sumą uprawnień jego oraz grupy, do której należy.
3. **Odmowa uprawnienia jest ważniejsza niż zezwolenie** (ma wyższy priorytet). To znaczy, że jeśli użytkownik **x1** jest członkiem grupy **gx1**, której zabroniono dostępu do określonego zasobu, to nie będzie on miał takiego dostępu, nawet jeśli na poziomie jego konta uprawnienia na dostęp zezwalają.

2

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/P114b541x>

Na dysku twardym komputera znajduje się katalog o nazwie dane, a z tego komputera korzysta dwóch użytkowników: Adam i Roman. Roman ma mieć pełny dostęp do katalogu ze wszystkimi uprawnieniami, Adam natomiast może tylko wyświetlać zawartość plików i katalogów zapisanych w folderze dane.



3

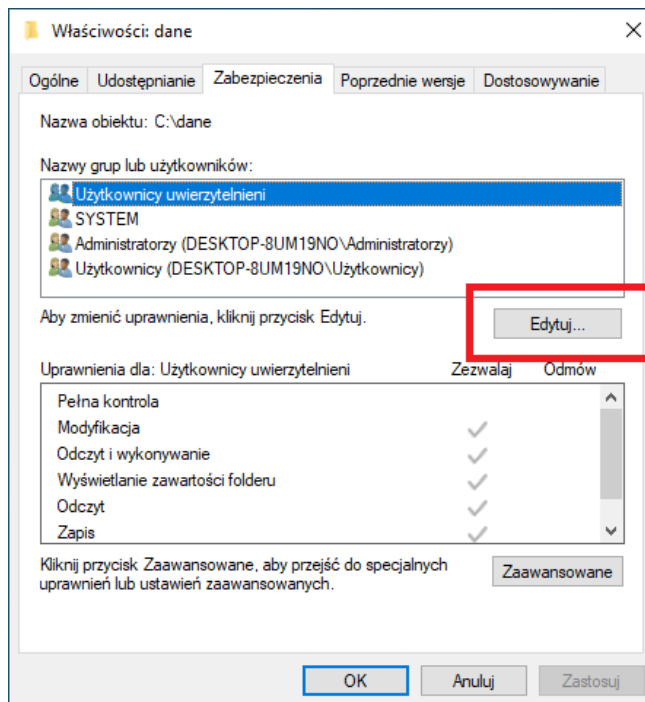
Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/P114b541x>

Uruchamiamy edytor uprawnień, klikając PPM w katalog dane i dalej Właściwości, a następnie zakładka Zabezpieczenia.

4

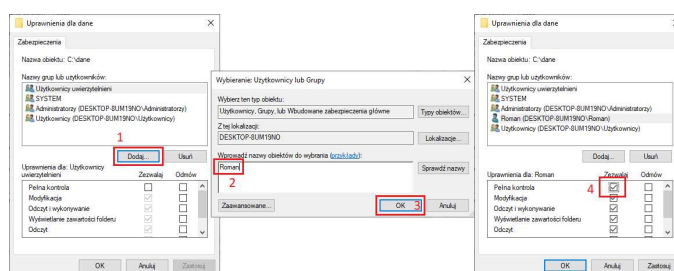


Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/P114b541x>

Edytujemy uprawnienia dla katalogu klikając Edytuj . . .



Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

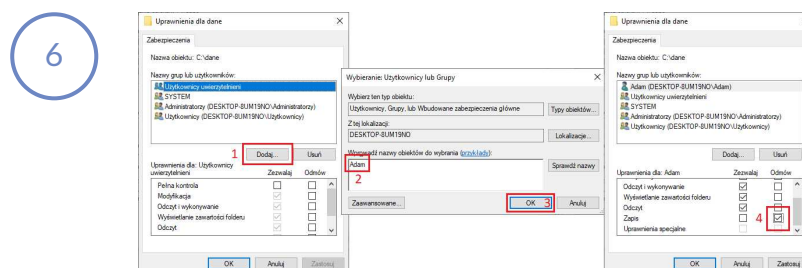
Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/P114b541x>

Klikamy Doda j . . . (1) | wprowadzamy nazwę użytkownika Roman (2) | klikamy OK (3) | określamy uprawnienia (4). Wystarczy zaznaczyć Zezwala j dla uprawnienia Pełna

5

kontrola, pozostałe uprawnienia zaznaczone zostaną automatycznie.



Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Materiał audio dostępny pod adresem:

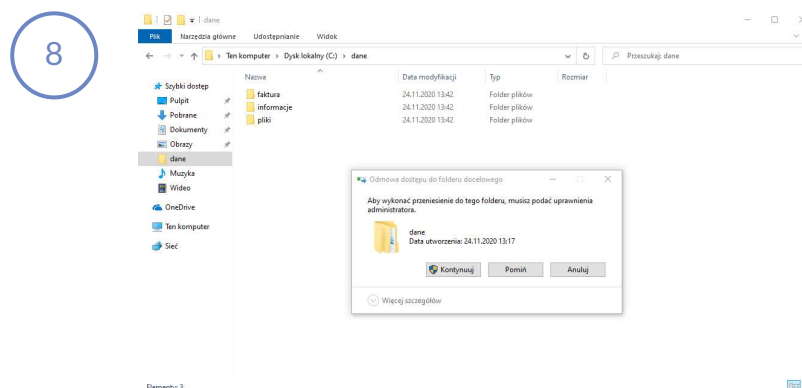
<https://zpe.gov.pl/b/P114b541x>

Ponownie klikamy Dodaj . . . (1) |
wprowadzamy nazwę użytkownika Adam (2) |
klikamy OK (3) | zaznaczamy Odmów dla
uprawnienia Zapis (4).

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/P114b541x>

Zapisujemy zmiany i zamykamy wszystkie okna.



Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Materiał audio dostępny pod adresem:

<https://zpe.gov.pl/b/P114b541x>

Test poprawności konfiguracji. Użytkownik Adam nie może tworzyć zasobu w katalogu dane. Przy próbie przekopiowania folderu lub jego utworzenie pojawia się komunikat odmawiający wykonania operacji.

Źródło: Contentplus.pl Sp. z o.o., licencja: CC BY-SA 3.0.

Sprawdź się

Pokaż ćwiczenia:   

Ćwiczenie 1



Wskaż, czym jest SMB.

- ☐ system plików
- ☐ nazwa usługi systemowej umożliwiającej nadawanie uprawnień w systemie Windows
- ☐ protokół sieciowy umożliwiający udostępnianie plików w lokalnych sieciach komputerowych
- ☐ rodzaj zabezpieczeń dostępu

Ćwiczenie 2



Uzupełnij zdanie.

Uprawnienia są , co oznacza, że jeśli użytkownik x1 należy do grupy gx1, to jego uprawnienia są uprawnień jego oraz .

SMB

ACL

domyślne

NTFS

efektywne

grupy, do której należy

innych użytkowników systemu

sumą

kumulowane

iloczynem

Ćwiczenie 3



Wskaż, na co nie pozwala uprawnienie modyfikacja.

- ☐ usuwanie pliku
- ☐ utworzenie pliku
- ☐ odczyt z pliku
- ☐ zapis do pliku
- ☐ przejęcie na własność pliku

Ćwiczenie 4



Połącz w pary podstawowe uprawnienia NTFS oraz ich opisy.

Odczyt i wykonanie

pozwała na wykonywanie wszystkich operacji na folderze i pliku

Modyfikacja

pozwała odczytywać dane oraz atrybuty z plików

Odczyt

pozawala na tworzenie plików i folderów, zapis danych do plików oraz ich modyfikacje

Zapis

pozwała wykonywać wszystkie możliwe operacje poza usuwaniem plików i podkatalogów, bez możliwości zmiany ich uprawnień oraz przejmowania na własność

Wyświetlenie zawartości folderu

pozwała wyświetlać zawartość folderu, odczytywać dane z pliku, oraz uruchamiać programy zapisane w folderze

Pełna kontrola

pozwała wyświetlać zawartość oraz uprawnienia w odniesieniu do folderu

Ćwiczenie 5



Wskaż, jakie atrybuty pliku uznaje się za rozszerzone.

☐ plik skompresowany

☐ plik zaszyfrowany

☐ plik ukryty

☐ plik systemowy

☐ plik archiwalny

Ćwiczenie 6



Uzupełnij zdanie.

pliku lub (użytkownik, który go utworzył) może zawsze zmienić jego , niezależnie od tego, jakie uprawnienia nadał dla katalogu lub pliku administrator systemu.

komputera

status

Właściciel

uprawnienia

możliwości

dokumentu

Moderator

folderu

Użytkownik

Ćwiczenie 7



Wskaż, które zdanie dotyczące uprawnień NTFS jest nieprawdziwe.

☐ Odmowa uprawnienia nie ma większego priorytetu niż zezwolenie.

☐ Właścicielem pliku jest użytkownik, który go utworzył.

☐ Uprawnienia NTFS można przypisywać zarówno do plików, jak i katalogów.

☐ Uprawnienie modyfikacja nie pozwala na usuwanie plików.

Ćwiczenie 8



Wskaż, ile jest możliwych do ustawienia uprawnień na poziomie sieciowym (jest ich mniej niż w przypadku uprawnień NTFS).

☐ 1

☐ 3

☐ 4

☐ 5

Dla nauczyciela

Autor: Damian Stelmach

Przedmiot: Informatyka

Temat: Prawa dostępu w systemach operacyjnych

Grupa docelowa:

Szkoła ponadpodstawowa, liceum ogólnokształcące, technikum, zakres podstawowy

Podstawa programowa:

Cele kształcenia – wymagania ogólne

III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi, w tym: znajomość zasad działania urządzeń cyfrowych i sieci komputerowych oraz wykonywania obliczeń i programów.

Treści nauczania – wymagania szczegółowe

III. Posługiwanie się komputerem, urządzeniami cyfrowymi i sieciami komputerowymi.

Zakres podstawowy. Uczeń:

3) rozwiązuje problemy korzystając z różnych systemów operacyjnych;

Kształtowane kompetencje kluczowe:

- kompetencje cyfrowe;
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się;
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii.

Cele operacyjne (językiem ucznia):

- Poznasz podstawowe uprawnienia użytkowników względem plików i folderów.
- Dowiesz się, jakie zasady obowiązują podczas definiowania uprawnień.
- Nauczysz się definiować uprawnienia do plików i folderów systemie Windows 10.

Strategie nauczania:

- konstruktywizm;
- konektywizm.

Metody i techniki nauczania:

- dyskusja;
- rozmowa nauczająca z wykorzystaniem multimediu i ćwiczeń interaktywnych;
- metody aktywizujące.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami, słuchawkami i dostępem do internetu;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda.

Przebieg lekcji

Przed lekcją:

1. **Przygotowanie do zajęć.** Nauczyciel loguje się na platformie i udostępnia e-materiał: „Prawa dostępu w systemach operacyjnych”. Uczniowie mają zapoznać się z treściami w sekcji „Przeczytaj”.

Faza wstępna:

1. Nauczyciel inicjuje rozmowę wprowadzającą w temat lekcji. Przedstawia cele zajęć oraz kryteria sukcesu.
2. **Rozpoznanie wiedzy uczniów.** Uczniowie tworzą pytania dotyczące tematu zajęć, na które odpowiedzą w trakcie lekcji.

Faza realizacyjna:

1. Uczniowie analizują przykład z sekcji „Przeczytaj” i powtarzają zaprezentowane rozwiązanie na swoim komputerze.
2. **Praca z multimediu.** Nauczyciel wyświetla zawartość sekcji „Film edukacyjny”. Uczniowie wspólnie zapoznają się z treścią zawartego w niej multimediu. Zapisują ewentualne problemy i pytania. Po czym następuje dyskusja, w trakcie której nauczyciel wyjaśnia niezrozumiałe treści.
3. **Ćwiczenie umiejętności.** Uczniowie wykonują ćwiczenia nr 1-8 z sekcji „Sprawdź się”. Nauczyciel sprawdza poprawność wykonanych zadań, omawiając je wraz z uczniami.

Faza podsumowująca:

1. Nauczyciel zadaje pytania podsumowujące, np.
 - czym są uprawnienia efektywne?
 - do czego służy protokół SMB?
 - wymień kilka podstawowych uprawnień do folderów i plików,
 - czym są listy kontroli dostępu?

Praca domowa:

1. Uczniowie charakteryzują różnice, jakie występują w zarządzaniu prawami dostępu w różnych systemach operacyjnych.

Wskazówki metodyczne:

- Treści w sekcji „Przeczytaj” można wykorzystać jako podsumowanie i utrwalenie wiedzy uczniów.