2.9.1. Uprawnienia do plików i katalogów w systemie Linux

W systemie Linuks użytkownik, który nie jest administratorem, ma dostęp tylko do niektórych plików. Dzięki temu nikt nie może na przykład zmodyfikować plików należących do innego użytkownika. Do każdego pliku jest przypisany *identyfikator właściciela* **u** (*user*) – użytkownika, który stworzył ten plik, oraz *grupy* **g** (*group*) – czyli zbioru użytkowników, którzy mają do tego pliku uprawnienia, w przeciwieństwie do *pozostałych* **o** (*others*). Uprawnienia można określać dla wszystkich użytkowników **a** (*all*).

Istnieją trzy podstawowe prawa dostępu do pliku:

- **r** (*read*) – prawo do *odczytu*,
- **w** (*write*) – prawo do *zapisu*,
- **x** (*execute*) – prawo do *uruchomienia*, jeśli plik jest programem.

Prawa te nadaje się niezależnie właścicielowi pliku, grupie, do której plik należy, i pozostałym użytkownikom. Aby dowiedzieć się, jakie uprawnienia są przypisane poszczególnym plikom, używa się polecenia: *ls –l*.

Każdy plik i katalog w systemie Linux ma 10 bitów protekcji w formacie drwxrwxrwx, gdzie:

- **bit 1** – to identyfikacja rodzaju zbioru:
  - **– d** (*directory*) to katalog,
  - **– –** to plik,
  - **– l** (*link*) – to link do pliku,
- **bity 2–4** – to uprawnienia właściciela pliku,
- **bity 5–7** – to uprawnienia grupy, do której należy właściciel,
- **bity 8–10** – to uprawnienia pozostałych użytkowników.

Jeżeli na bitach 2–10 występuje litera, oznacza to ustawione uprawnienie, natomiast kreska oznacza brak uprawnienia.

Administrowanie uprawnieniami jest możliwe za pomocą polecenia *chmod*, np. użycie polecenia *sudo chmod ugo+w plik.txt* powoduje dodanie (+) prawa do zapisu w (*write*) dla pliku o nazwie plik.txt właścicielowi u (*user*), użytkownikom należącym do tej samej grupy co właściciel pliku g (*group*) oraz dodanie prawa do zapisu pliku wszystkim pozostałym użytkownikom o (*others*).

Każde z praw dostępu ma przypisany odpowiedni parametr cyfrowy:

- **r** – prawo do odczytu – 4,
- **w** – prawo do zapisu – 2,
- **x** – prawo do uruchomienia – 1,
- **– –** brak praw dostępu – 0.

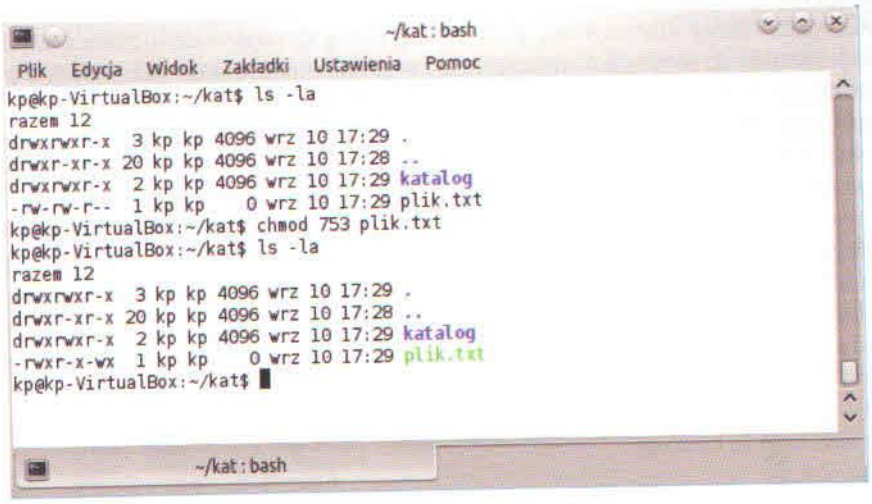
Po dodaniu odpowiednich parametrów zestaw trzech praw można przedstawić za pomocą jednej cyfry.

Oto możliwe kombinacje:

- **– – –** 0 brak praw,
- **– – x** 1 prawo do uruchomienia,
- **–w–** 2 prawo do zapisu,
- **–wx** 3 prawo do zapisu i wykonania,

- r-- 4 prawo do odczytu,
- r-x 5 prawo do odczytu i uruchomienia,
- rw- 6 prawo do odczytu i zapisu,
- rwx 7 prawo do odczytu, zapisu i uruchomienia.

Do zmiany uprawnień można wykorzystać również polecenie *chmod* oraz uprawnienia zapisane jako 3-cyfrowa liczba. Cyfry od lewej oznaczają uprawnienia dla właściciela, grupy i pozostałych użytkowników. Aby ustawić uprawnienia, należy wpisać polecenie: *chmod 750 plik.txt*. Przypisane zostaną uprawnienia 7 dla właściciela (rwx), 5 dla grupy (r-x), 0 dla pozostałych użytkowników (---).



Rys. 23.2. Wyświetlanie uprawnień do zasobów

Właścicielem każdego pliku i katalogu jest użytkownik, który ten zbiór utworzył. Przenieść własność zbioru na innego użytkownika może tylko administrator lub użytkownik posiadający odpowiednie uprawnienia. Do zmiany właściciela w systemie Linux używa się polecenia *chown*.

Uwaga!
Zmiana właściciela zbioru może spowodować zmianę uprawnień przypisanych użytkownikom do danego zbioru.