Bezpieczeństwo systemów komputerowych i aplikacje użytkowe

3.1. Bezpieczeństwo systemu operacyjnego i ochrona danych
(Jacek Jędryczkowski – s.69-99)

Punkt przywracania systemu

Instalacja nowego oprogramowania, zawsze wiąże się z ryzykiem uszkodzenia systemu operacyjnego. W znacznej mierze można uniknąć tego niebezpieczeństwa tworząc wcześniej, tzw. **Punkt przywracania systemu**. Jest to miejsce (punkt umiejscowiony w czasie), do którego można cofnąć komputer.

Operacja ta powoduje cofnięcie zmian w obrębie najistotniejszych plików systemowych. Nie ma jednak wpływu na utworzone w międzyczasie dokumenty lub odebrane listy.

Tworzenie punktu przywracania systemu

Klika się: **Start / Pomoc i obsługa techniczna**, po chwili otworzy się okienko, w którym wybiera się opcję: **Cofnij zmiany dokonane w komputerze poprzez przywracanie systemu**. W tym momencie otworzy się okienko, w którym klika się: **Utwórz punkt przywracania / Dalej.** W kolejnym okienku, w polu **Opis punktu przywracania**, wpisuje się dowolną nazwę, a następnie klika na przycisku **Utwórz**. Po chwili pojawi się komunikat o utworzeniu nowego punktu przywracania.

W przypadku awarii systemu procedurę powtarza się, z tym tylko, że zamiast wybierać opcję **Utwórz punkt przywracania**, należy wybrać: **Przywróć mój komputer do wcześniejszego stanu / Dalej**.

Na planszy wyświetlonego wówczas kalendarza trzeba wybrać dzień, w którym został utworzony punkt przywracania oraz po prawej stronie kliknąć na nazwie punktu. Procedurę kończy się, klikając **Dalej / Dalej**. W tym momencie rozpoczyna się proces przywracania systemu. Po wieńczącym go restarcie, komputer uruchomi się bez aplikacji zainstalowanych po utworzeniu punktu przywracania.

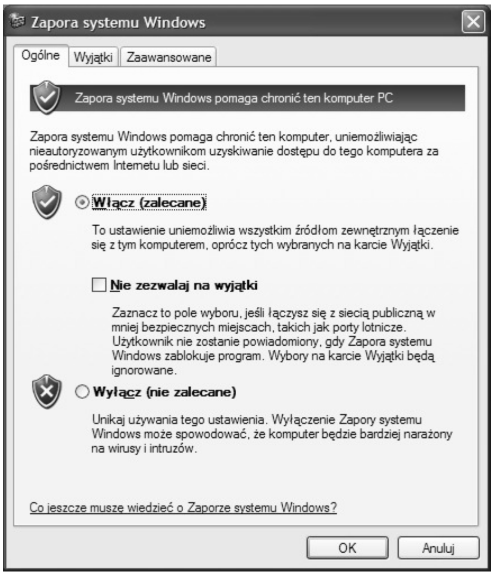
Zapora systemowa

Dbałość o sprawne i bezpieczne funkcjonowanie systemu operacyjnego wymaga kontroli ustawień w **Centrum zabezpieczeń** systemu operacyjnego Windows XP. W tym celu wybiera się: **Start / Ustawienia /Panel Sterowania**, a w nim klika dwukrotnie na ikonie **Centrum zabezpieczeń**. Otwarte zostanie w ten sposób okienko, w którym wszystkie trzy opcje (**Zapora, Aktualizacje automatyczne** oraz **Ochrona przed wirusami**) powinny być włączone.

Zapora jest mechanizmem systemowym ograniczającym swobodne komunikowanie się aplikacji działających pod kontrolą systemu Windows z nieznanymi miejscami w sieci Internet. W znacznej mierze blokuje także dostęp do komputera osobom niepowołanym. Samo uaktywnienie zapory nie jest efektywne, gdy są wyłączone **Aktualizacje automatyczne**. To one dostarczają poprawek dla wszystkich luk wykrytych w systemie zabezpieczeń.

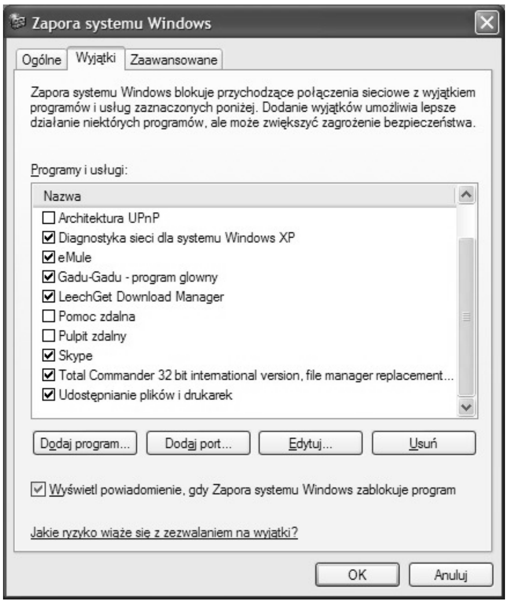
Rys. 1. Panel uaktywniający trzy podstawowe obszary zabezpieczeń systemu operacyjnego Windows XP

Zmiany ustawień zapory systemowej można wprowadzać wybierając: **Zapora systemu Windows** w sekcji **Zarządzaj ustawieniami zabezpieczeń dla** (rys 1). W ten sposób zostaje uaktywnione okienko (rys. 2), w którym decyduje się, czy zapora ma być aktywna (zakładka **Ogólne**).



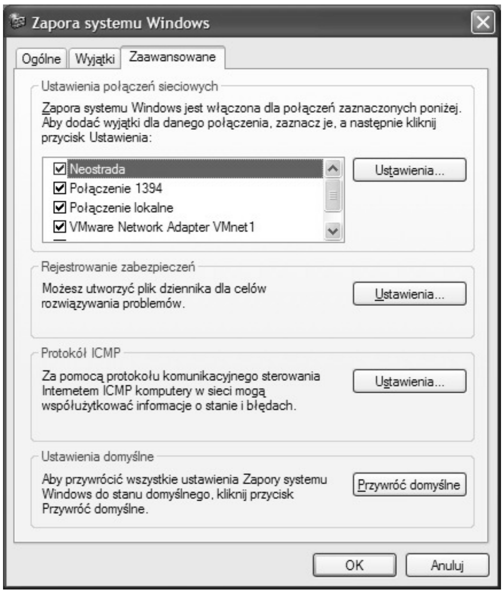
Rys. 2. Uaktywnianie zapory systemu Windows

Przechodząc na zakładkę **Wyjątki** (rys. 3), można zdecydować, które z aplikacji mają prawo samoczynnie kontaktować się z Internetem. Jest to szczególnie ważne, gdy instalując nowy program (np. klienta pocztowego) przez pomyłkę, na pytanie o reakcję zapory systemowej, wybierze się opcję blokowania.



Rys. 3. Korzystając z ustawień zapory systemowej można określić, które aplikacje mogą komunikować się z Internetem

Na zakładce **Zaawansowane** (rys. 4) wybiera się połączenia sieciowe chronione przez zaporę systemową.



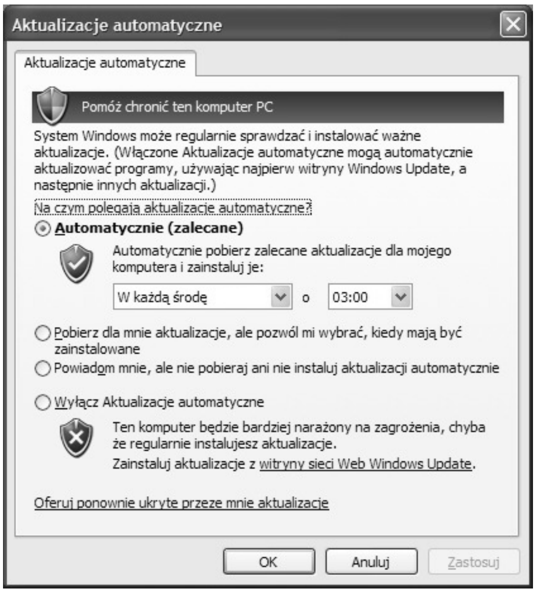
Rys. 4. Zapora systemowa może chronić połączenia sieciowe, np. dostęp do Internetu poprzez Neostradę

Nie wszystkich użytkowników satysfakcjonuje działanie zapory systemowej Windows XP. Niestety komercyjne zapory są stosunkowo drogie. Można jednak znaleźć wiele prostych i skutecznych rozwiązań. Dobrym przykładem jest darmowa zapora Ashampoo FireWall[1]. Jedną z jej zalet jest możliwość równoczesnej pracy wraz z zaporą systemową. Instalując inne zapory, okazuje się najczęściej, że wyłączają one oryginalną zaporę Windows XP.

Aktualizacje automatyczne i ochrona antywirusowa

Aktualizacje automatyczne

Jedną z najistotniejszych funkcji **Centrum zabezpieczeń** są **Aktualizacje automatyczne**. Ich uaktywnienie gwarantuje stałe unowocześnianie systemu operacyjnego, eliminowanie wszystkich luk w systemie zabezpieczeń oraz instalację nowych wersji aplikacji systemowych.



Rys. 5. Okienko ustawień aktualizacji automatycznych

Opcje aktualizacji ustawia się wybierając: **Aktualizacje automatyczne** (rys. 1) w sekcji **Zarządzaj ustawieniami zabezpieczeń dla** lub klikając w **Panelu sterowania** na ikonie **Aktualizacje automatyczne**. W ten sposób zostaje uaktywnione okienko (rys. 5), w którym wybiera się czy i kiedy komputer powinien być aktualizowany.

Alternatywy sposób aktualizacji systemu

Nielegalni użytkownicy systemu Windows XP bardzo często wyłączają aktualizacje automatyczne, obawiając się, iż zostanie zainstalowane oprogramowanie wyświetlające komunikaty o konieczności legalizacji oprogramowania. Użytkownicy ci oraz osoby

[1] http://www2.ashampoo.com/webcache/html/1/home_2.htm/

nieposiadające szybkiego dostępu do Internetu dokonują aktualizacji, stosując aplikację Autopatcher. Jest to zbiór wszystkich najnowszych poprawek i dodatków systemowych. Był on dostępny pod adresem http://autopatcher.com.pl/ lub w licznych czasopismach o tematyce komputerowej. Instalując ten pakiet w systemie Windows XP, następuje także aktualizacja przeglądarki Internet Explorer do wersji 7.0 oraz odtwarzacza Windows Media Player do wersji 11. W sierpniu 2007 roku Microsoft zażądał zamknięcia witryny Autopatchera.

Ochrona antywirusowa

System Windows XP nie posiada wbudowanego skanera antywirusowego. Aplikację taką należy samodzielnie zainstalować. Na rynku spotyka się szereg kosztownych aplikacji. Domowy użytkownik (najczęściej nie dotyczy to instytucji) może jednak skorzystać z wielu darmowych rozwiązań. Do najciekawszych należą:

AVG - http://www.avg.pl/produkt/pokaz/8/avg_anti_virus_free.html

Avast - http://www.avast.pl/

Partycje (dyski lokalne)

Kupując nowy dysk twardy otrzymuje się mechanizm nieprzygotowany do zapisu danych. Pierwszym krokiem, jaki należy wykonać jest podział dysku na części (partycje) o różnym przeznaczeniu. W systemie operacyjnym Windows może istnieć tylko jedna część, określana domyślnie jako dysk **C** (oznaczenia A i B tradycyjnie były zarezerwowane dla napędów dyskietek). Dysk C jest tzw. partycją systemową. Na niej znajduje się system operacyjny, tam umieszczony jest folder **Program Files**, wewnątrz którego lokują się komponenty wszystkich instalowanych programów.

Na dysku C umieszczony jest folder **Documents and Settings** zawierający pliki użytkowników korzystających z jednego komputera. Każdy użytkownik posiada tam swój własny folder: **Moje dokumenty**, tam zapisana jest zawartość poszczególnych pulpitów oraz spersonalizowanych menu (tych, które widać po naciśnięciu przycisku **Start**).

Partycja systemowa w największym stopniu narażona jest na ataki wirusów oraz hakerów. Każdy system (szczególnie Windows) po pewnym czasie odmawia posłuszeństwa. Wtedy najlepiej nie mieć swoich efektów pracy (dokumentów, nagrań fotografii lub filmów) na dysku C (np. w folderze Moje dokumenty).

Najrozsądniejszym rozwiązaniem jest utworzenie na dysku twardym dwóch partycji: C – systemowej oraz D – przeznaczonej do przechowywania efektów własnej pracy oraz wszelkich zbiorów danych.

Twórcy Windowsa zamiast określenia *partycja* bardzo często stosują termin *dysk lokalny*.

Ważne dane przechowuje się na partycji D! Naprawdę istotne pliki dodatkowo należy zarchiwizować na płycie CD! Płyty CD już po dwóch latach mogą tracić dane!

System plików

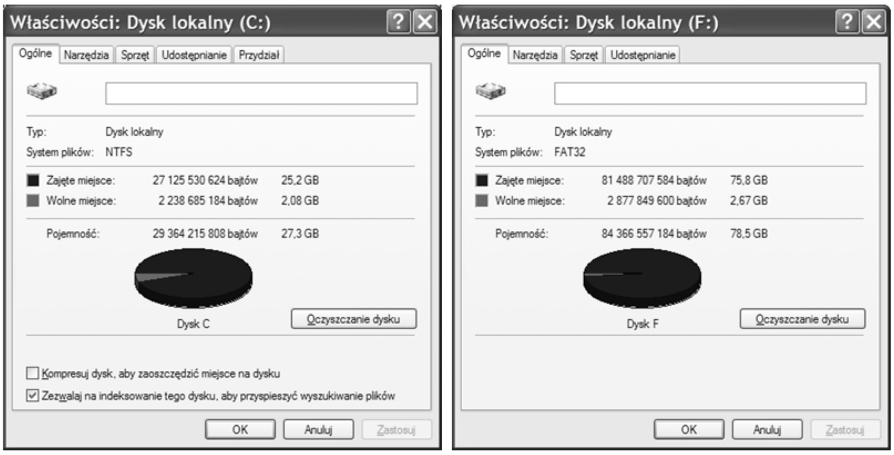
Partycjonowanie dysku twardego to dopiero pierwszy etap przygotowania dysku do pracy. Kolejnym krokiem jest wybór **systemu plików**. System plików to reguła, umowny sposób zapisu danych, często charakterystyczny tylko dla określonego systemu operacyjnego. System plików umożliwia szybkie odszukiwanie informacji na dysku, ich edytowanie, kasowanie oraz zapis.

We współczesnych systemach operacyjnych Windows stosuje się dwa rodzaje systemów plików. Starszy FAT32 może obsługiwać dyski twarde o pojemności do 120 gigabajtów, co dyskwalifikuje go w przypadku nowszych dysków. Maksymalna wielkość pliku to 4GB. Brakuje w nim zaawansowanych możliwości ochrony danych.

Najczęściej stosowanym systemem plików jest NTFS (New Technology File System), który zawiera Encrypting File System umożliwiający szyfrowanie plików systemowych (Windows XP Professional oraz Vista Business, nie jest dostępny w wersjach Home). W systemach domowych (Home) brak jest szyfrowania danych, ale istnieją inne sposoby ich ochrony. System plików NTFS pozwala na definiowanie praw dostępu do poszczególnym plików i folderów (Windows 2000, Windows XP Professional, Windows Server 2003 oraz Windows Vista z wyłączeniem wersji Home).

Sposób sprawdzania posiadanego systemu plików

Na pulpicie klika się **Mój Komputer**, a następnie na danej partycji (dysku lokalnym) prawym przyciskiem myszy i wybiera się **Właściwości**. Otwierają się wówczas okienka (rys. 6), w których można odczytać, iż w tym przypadku dysk lokalny C posiada system plików NTFS, a dysk F - FAT32.

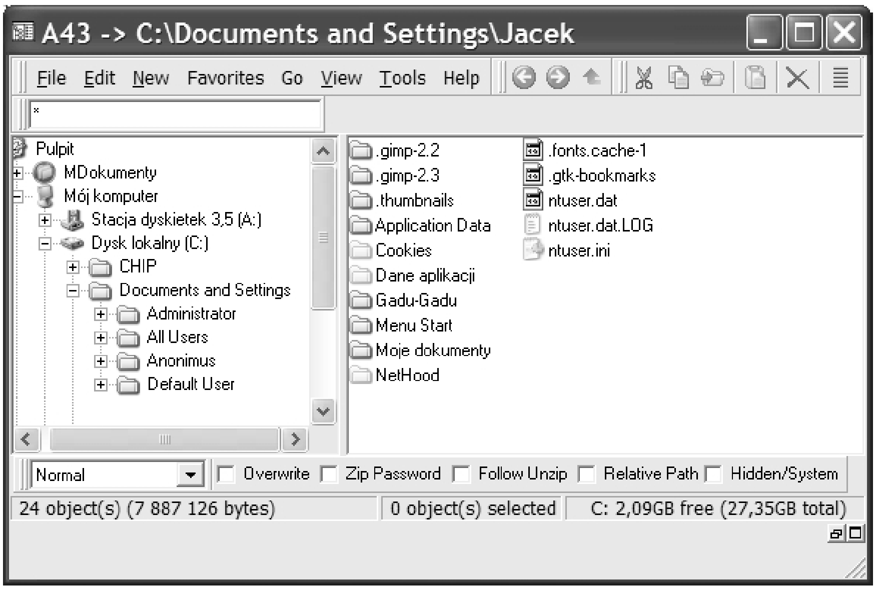


Rys. 6. Sprawdzanie zainstalowanego systemu plików

Odzyskiwanie danych

Podstawową niedogodnością systemu plików NTFS jest kłopotliwe odzyskiwanie danych z partycji C w przypadku awarii systemu operacyjnego. Przeciętny użytkownik może posłużyć się w takiej sytuacji botującą płytą CD (z takiej płyty, a nie z dysku twardego uruchamia się system operacyjny zapisany na płycie) zawierającą programem BartPE.

Po uruchomieniu komputera z tej płyty wystartuje okrojona wersja systemu operacyjnego Windows. Pozwoli jednak na uruchomienie menedżera plików **A43** (rys. 7) umożliwiającego przejrzenie zawartości partycji C i przeniesienie najważniejszych danych na partycję D.



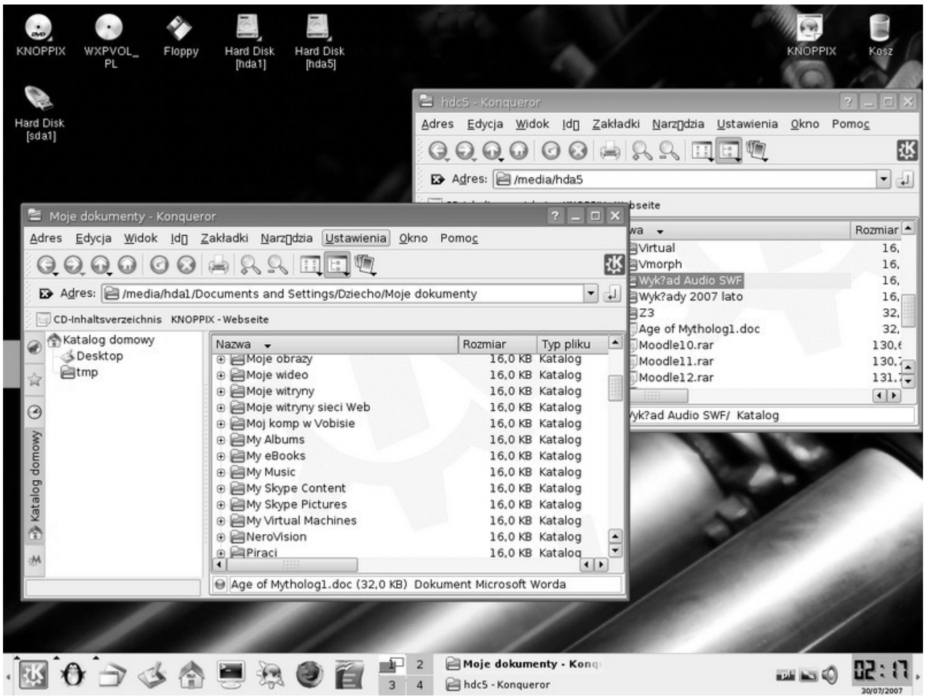
Rys. 7. Menedżer plików A43 dostępny na botującej płycie z systemem BartPE

Płyty tej niestety nie można kupić. Każdy legalny użytkownik Windowsa XP może ją sam sobie przygotować. Nie jest to proces skomplikowany. Jego opis można znaleźć w Internecie[2].

Niestety, jeśli płytę przygotuje się z polskiej wersji Windowsa (w odróżnieniu od angielskiej), to funkcjonalność tego narzędzia będzie znikoma. Nie będą dostępne nazwy plików i folderów na przeglądanych partycjach. Osoby kupujące notebooka często otrzymują dwie wersje językowe Windowsa. Istnieje więc możliwość utworzenia takiej płyty w sposób legalny.

Jeśli awaria nastąpiła w komputerze, na którym utworzone były partycje z systemem plików FAT32 lub NTFS (w ograniczonym zakresie), najprostszym rozwiązaniem może być wykorzystanie płyt z botującą wersją Linuxa, np. Knoppixa 5.0 (oraz wyższych). Po uruchomieniu komputera z włożoną do napędu płytą wystartuje w pełni sprawny system operacyjny umożliwiający prosty dostęp do wszystkich partycji (rys. 8).

Na partycjach FAT32 możliwe jest zapisywanie, więc także kopiowanie danych, np. z partycji C na D. W przypadku, gdy w komputerze są dostępne partycje NTFS, dane można skopiować tylko na pendrive lub dyskietkę.



Rys. 8. Pulpit Linuxa Knoppix 5.0.

[2] http://www.purepc.pl/node/549?pageNo=1
oraz http://www.chip.pl/arts/archiwum/n/articlear_142124.html (przejrzano 07.08.2007).

Ikony **Hard Disk [hda1]** oraz **Hard Disk [hda5]** odpowiadają partycjom C i D (ich zawartość jest widoczna w otwartych okienkach). Wszystkie ważne obiekty z partycji **C** można (w znany z Windowsa sposób) przeciągnąć na partycję **D,** jeśli na niej zastosowano system plików FAT32.

W przypadku partycji NTFS można skorzystać z przenośnej pamięci pendrive. Jeśli do portu USB włoży się pendrive, to na pulpicie samoczynnie pojawi się jego ikona - tu **Hard Disk [sda1]**. Na nośnik ten można swobodnie kopiować pliki i foldery z partycji NTFS (Knoppix 5.0).

Microsoft nigdy nie udostępnił specyfikacji NTFS, dlatego twórcy różnych wersji Linuxa podjęli samodzielną próbę stworzenia narzędzi pozwalających korzystać z tej partycji. Opracowano dwa sterowniki. W wersji 2.4 - istnieje możliwość zapisu na partycji NTFS, ale prawdopodobieństwo zniszczenia systemu plików i utraty danych jest bardzo duże.

Bezpieczniejszy jest sterownik 2.5.11 - nie obsługuje on zapisu ale pozwala na przeglądanie zasobów i kopiowanie danych z partycji NTFS, np. na pendrive. Nie każdy Linux ma możliwość odczytu partycji NTFS, ale zawsze można tę funkcję dodać. Nie jest to jednak proste zadanie dla użytkowników Windowsa.

Jednym ze sposobów dotarcia do danych znajdujących się na dysku z uszkodzonym systemem operacyjnym, jest przełożenie go do innego komputera pracującego pod kontrolą identycznego systemu.

Wszystkie powyższe zabiegi są niepotrzebne, gdy ważne pliki, prace i wszelkie informacje przechowuje się na partycji D!

Obraz partycji

W sytuacji, gdy nauczyciel opiekuje się pracownią komputerową lub system operacyjny wraz z niezbędnymi aplikacjami instaluje się nawet kilka dni, należy pomyśleć o sporządzeniu, tzw. obrazu partycji. Jest to plik, najczęściej skompresowany, który zawiera wszystko, co zainstalowano na partycji C. Obraz ten przechowuje się na partycji D lub osobnej płycie CD lub DVD.

Obraz partycji wykonuje się, gdy już zostanie zainstalowany i przetestowany nowy system operacyjny wraz z dodatkowymi aplikacjami. W przypadku awarii systemu, jego odtworzenie z pliku obrazu zajmuje zaledwie kilka minut.

Istnieje wiele darmowych aplikacji do tworzenia obrazu dysku oraz późniejszego odtwarzania systemu. Jednak najpopularniejszy jest komercyjny **Symantec Norton Ghost.**

Może być instalowany w systemie Windows lub uruchamiany z botującej dyskietki lub płyty CD. Opis działania programu można znaleźć na stronach internetowych[3].

Dodawanie konta użytkownika
Logowanie do systemu Windows XP

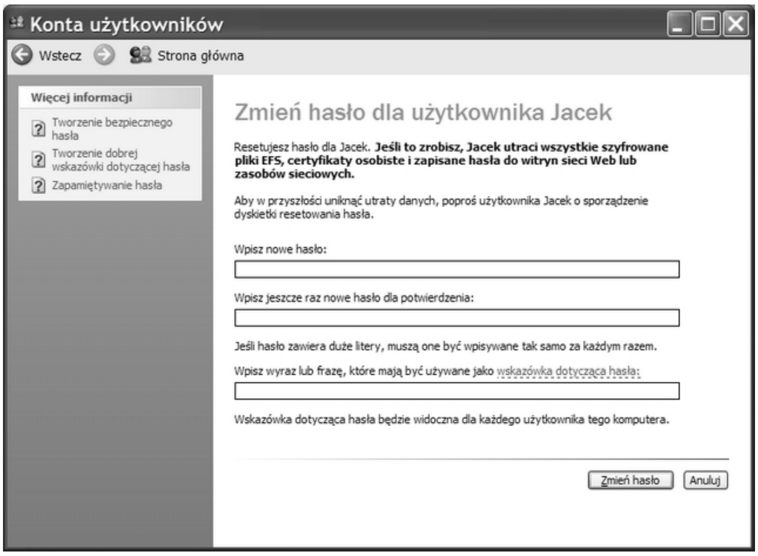
Zakładanie konta użytkownika lub modyfikacja parametrów konta

Wybiera się: **Start / Ustawienia / Panel sterowania**, tam klika na ikonie **Konta użytkowników**. Otwarte zostanie okienko, w którym są widoczne istniejące konta. Jeśli konto jest chronione hasłem, obok jego ikony znajduje się odpowiednia informacja. Tutaj osoba z prawami administratora może zakładać i modyfikować istniejące konta.

W celu dodania nowego użytkownika klika się: **Utwórz nowe konto**. W tym momencie otwiera się nowe okienko. W polu **Wpisz nazwę nowego konta** można wprowadzić, np. imię użytkownika, a następnie kliknąć na przycisku **Dalej**. Otwiera się wówczas kolejne okienko, w którym określa się, czy użytkownik ma mieć pełne prawa, czy też z ograniczeniami (np. brak możliwości instalacji programów). Po dokonaniu wyboru klika się: **Utwórz konto**.

W tym momencie pojawia się pierwsze okienko, ale uzupełnione o ikonę nowego konta. Klikając na niej uaktywnia się okienko **Co chcesz zmienić w koncie użytkownika**. Wybierając **Zmień obraz**, można wskazać dowolną fotografię lub grafikę o niewielkich wymiarach (zalecane zdjęcie użytkownika). Klikając: **Utwórz hasło** – następuje przełączenie do okienka **Zmień hasło dla użytkownika** (rys.9).

[3] http://www.cdrinfo.pl/cdr/artykuly/ghost/nghost.php3
lub http://pccentre.pl/modules.php?op=modload&name=News&file
=article&sid=13438&pagenum=2&mode=thread&order=0&thold=0, (przejrzano 07.08.2007).



Rys. 9. Wprowadzenie lub zmiana hasła użytkownika

W okienku tym należy dwukrotnie podać wymyślone hasło oraz frazę, która umożliwi jego przypomnienie. Na końcu klika się **Zmień hasło**.

Teraz można pozamykać wszystkie okienka. Ponowne uruchomienie Windowsa będzie wiązało się z wyświetleniem ekranu logowania (widoczne obrazki i nazwy użytkowników). Klikniecie na nazwie użytkownika skutkuje uaktywnieniem paska, na którym wpisuje się własne hasło. Po tej operacji użytkownik uzyskuje dostęp do systemu operacyjnego.

Każdy logujący się otrzymuje swój własny **Pulpit** oraz swoje własne **Moje dokumenty**. Należy pamiętać, że jeżeli nie zabezpieczy się dostępu do prywatnych danych, to każdy inny użytkownik komputera będzie mógł przeglądać dowolne zasoby, korzystając ze ścieżek dostępu: **C:\ Documents and Settings \ Nazwa użytkownika \ Pulpit** lub **C:\ Documents and Settings \ Nazwa użytkownika \ Moje dokumenty**.

Zmiana aktywnego użytkownika może odbywać się na dwa sposoby. Klika się: **Start / Wyloguj / Nazwa użytkownika** - pojawi się okienko **Wylogowywanie z systemu Windows**. Tutaj określa się, czy aktywny użytkownik ma skończyć pracę z komputerem bez wyłączania komputera - **Wyloguj**, czy przerywa pracę tylko na chwilę, pozwalając skorzystać z komputera innemu użytkownikowi - **Przełącz użytkownika**. Oba wybory skutkują wyświetleniem ekranu logowania.

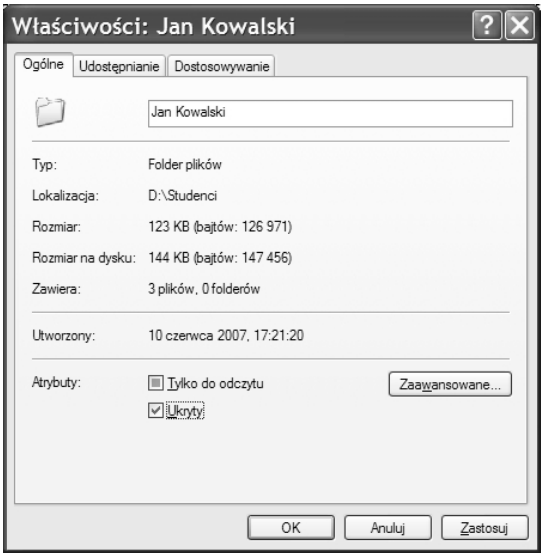
Opisany powyżej sposób uaktywniania ekranu logowania jest bardzo czasochłonny. Jeśli należy szybko przełączyć użytkownika lub odchodzi się od komputera i trzeba zablokować do niego dostęp, należy: na klawiaturze przytrzymać **symbol Windows** i raz nacisnąć przycisk z literą **L**.

Blokowanie dostępu do informacji poufnych

Ukrywanie plików i folderów

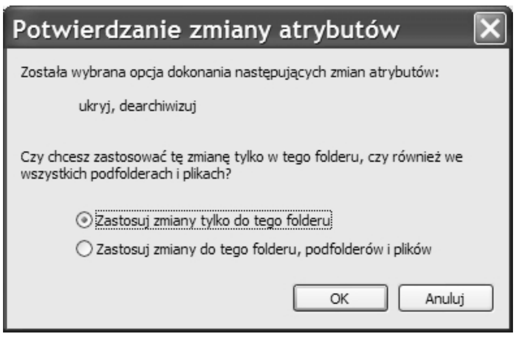
W systemie operacyjnym Windows istnieje bardzo prosty (ale łatwy do obejścia) sposób ukrywania plików i folderów.

Klika się prawym przyciskiem myszy na folderze zawierającym pliki przeznaczone do ukrycia. Wybiera się **Właściwości** i zaznacza się opcję **Ukryty** (rys. 10).



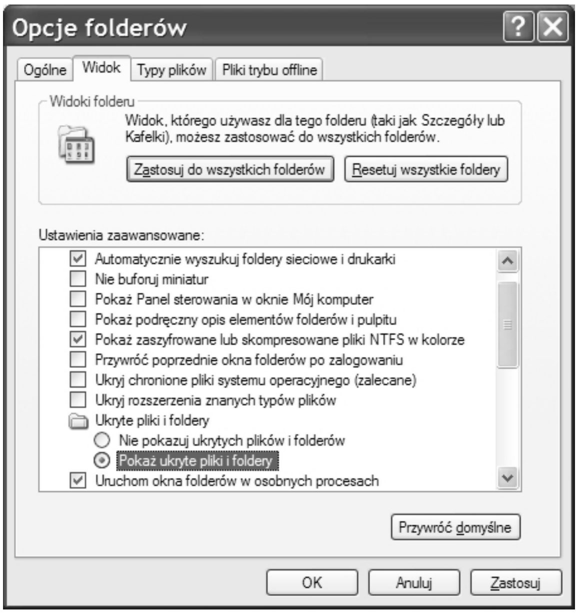
Rys. 10. Okienko właściwości folderu

W otwartym wówczas okienku (rys. 11) określa się, czy ukryty ma zostać tylko folder, czy także wszystkie obiekty w nim zawarte. W praktyce wystarczy opcja pierwsza. Skoro nie widać folderu, to tym bardziej obiektów wewnątrz.



Rys. 11. Zmiana atrybutów plików i folderów

Niestety bardzo łatwo można odszukać ukryte w ten sposób obiekty. Wystarczy w dowolnym otwartym okienku, np. **Mój komputer** wybrać na pasku menu: **Narzędzia / Opcje folderów /** oraz zakładkę **Widok** (rys. 12), a następnie wybrać: **Pokaż ukryte pliki i foldery / Zastosuj / OK**.

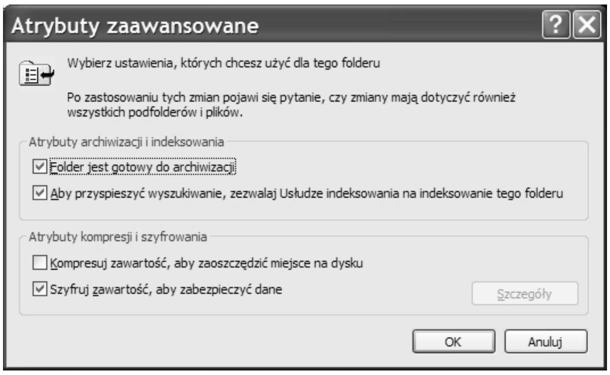


Rys. 12. Dokonując zmian w okienku *Opcje folderów*, można sprawić, że pojawią się wszystkie ukryte obiekty

Szyfrowanie plików

W Windows XP Professional (tylko na partycji NTFS) istnieje niezwykle skuteczna metoda szyfrowania plików. Jest ona przydatna, gdy z komputera korzysta kilku użytkowników posiadających własne konta chronione hasłem. Osoba, która zaloguje się do komputera nie będzie mogła przeglądać cudzych zasobów. Zabezpieczenie to nie chroni danych, gdy ktoś obcy będzie korzystał z konta użytkownika, który zapomniał się wylogować.

W celu zaszyfrowania plików klika się prawym przyciskiem myszy na folderze, w którym się znajdują. Następnie wybiera się **Właściwości**, wtedy otworzy się okienko (rys. 10), w którym klika się **Zaawansowane**. W ten sposób otwarte zostanie kolejne okienko **Atrybuty zaawansowane** (rys. 13), w nim zaznacza się opcję **Szyfruj zawartość, aby zabezpieczyć dane** i klika **OK**.



Rys. 13. Windows XP Professional - szyfrowanie danych na partycji NTFS

Od tej pory nazwy zaszyfrowanych plików będą zapisane zieloną czcionką, jeśli w okienku - (rys. 12) wybierze się taką opcję. Dla użytkownika komputera praca z takimi plikami nie zmienia się w widoczny sposób. Jednak żaden inny zalogowany użytkownik nie będzie miał dostępu do zaszyfrowanych plików, nikt poprzez sieć nie skopiuje ich ani nie odczyta.

Dużą ostrożnością musi wykazać się osoba zabezpieczająca w ten sposób poufne dane. Podczas kopiowania plików na partycje FAT32, na pendrive lub kompresując WinRarem, traci się szyfrowanie. Wszystkie dane stają się dostępne dla osób niepowołanych.

Istnieje groźba utraty dostępu do zabezpieczonych w ten sposób danych, jeśli nie wykona się niezaszyfrowanej kopii, np. na płycie CD. Gdy awarii ulegnie system operacyjny, a następnie zostanie zainstalowany ponownie, to praktycznie nie ma już możliwości ich odzyskania. Można próbować korzystać z pewnych programów, np. Aefsdr, ale bez gwarancji sukcesu. Chcąc uniknąć takiej sytuacji (tylko zaawansowani użytkownicy), można wyeksportować swój certyfikat oraz utworzyć Agenta odzyskiwania[4].

Ten niezwykle sprawny system szyfrowania niesie ze sobą niebezpieczeństwo utraty dostępu do danych i całkowicie nie chroni ich w sytuacji, gdy odejdzie się od komputera, a osoba niepowołana usiądzie i zacznie przeglądać zasoby pozostawione bez nadzoru.

Należy pamiętać, aby odchodząc od komputera, na klawiaturze przytrzymać symbol Windowsa i wcisnąć przycisk L (kombinacja ta włącza ekran logowania).

Szyfrowanie plików i folderów z zastosowaniem programu WinRar[5]

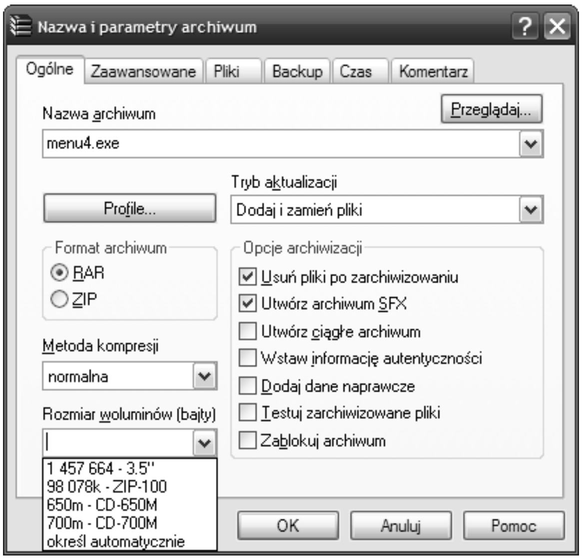
Dowolny folder wraz z zawartymi w nim plikami można skompresować z zastosowaniem programu WinRar. Takie archiwum może być chronione hasłem. W celu

[4] http://www.enter.pl/archiwum/tekst2.asp?p=/archiwum/ent2004/07/enter_art_nstr_119889.html, (przejrzano. 10.08.2007).
[5] Program można pobrać na stronie: http://www.winrar.pl/.

utworzenia archiwum klika się na wybranym folderze prawym przyciskiem myszy. Należy wskazać opcję **Dodaj do archiwum**.

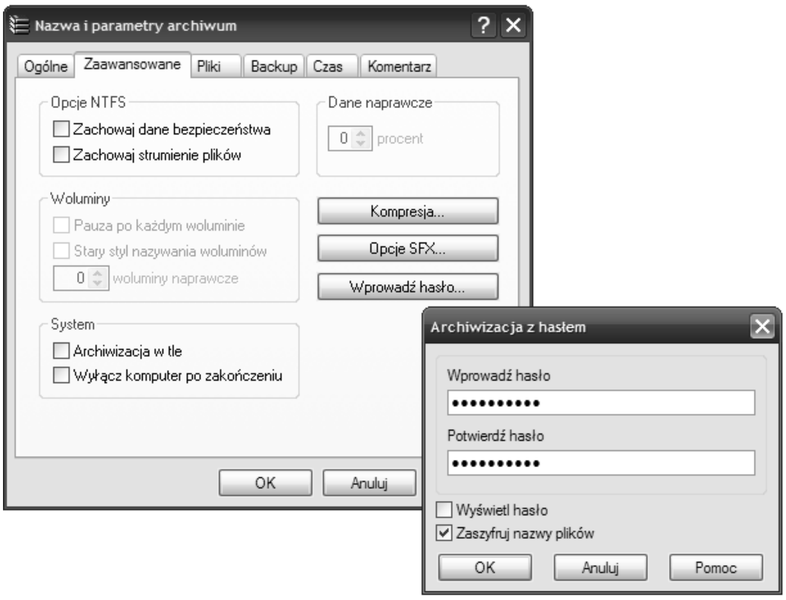
W okienku **Nazwa i parametry archiwum**, na zakładce **Ogólne** (rys. 14) można wybrać:

- **Usuń pliki po zarchiwizowaniu** (pozostaje tylko archiwum, oryginalny obiekt zostaje skasowany),
- **Utwórz archiwum SFX** (niezbędne, jeśli archiwum ma być rozpakowywane w komputerze bez zainstalowanego WinRara),
- **Rozmiar woluminów** (jeśli dane nie mieszczą się na jednym nośniku, archiwum może zostać podzielone na kilka części).



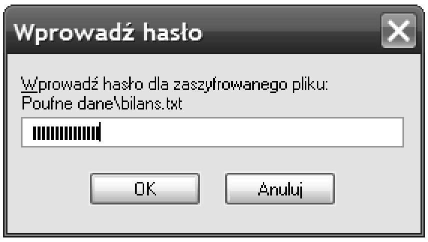
Rys.14. Interfejs programu WinRar, zakładka *Ogólne*

Po określeniu podstawowych parametrów archiwum, należy przejść na zakładkę **Zaawansowane** (rys.15). Kliknięcie na przycisku **Wprowadź hasło** uaktywni okienko **Archiwizacja z hasłem**. Hasło należy wprowadzić dwukrotnie i ewentualnie wybrać opcję **Zaszyfruj nazwy plików**. Wymyślone hasło powinno: być długie (najlepiej kilkanaście znaków), zawierać wielkie i małe litery oraz znaki specjalne (np. @#$%^). Istnieje wiele programów do odnajdywania haseł WinRara. Zastosowanie się do powyższych zaleceń może sprawić, że złamanie hasła może wymagać miesięcy, a nawet lat nieprzerwanej pracy komputera.



Rys.15. Interfejs programu WinRar, zakładka *Zaawansowane*

Uaktywnienie zaszyfrowanego pliku archiwum wiąże się z wyświetleniem okienka (rys. 16), w którym należy wprowadzić hasło niezbędne do rozpakowania pliku.



Rys.16. Rozpakowanie zaszyfrowanego archiwum wymaga uprzedniego podania hasła

Wyszukiwanie i likwidacja ukrytych kont użytkowników

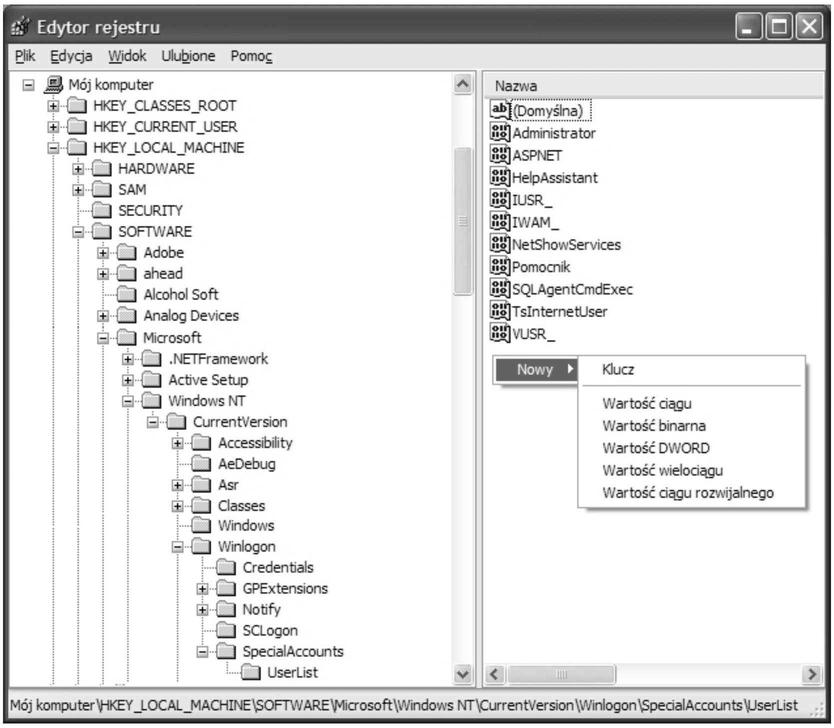
Ukrywanie konta użytkownika

Jeśli uczniowie będą mieli tylko przez chwilę dostęp do aktywnego konta z prawami administratora, to może zachodzić obawa, że stworzyli sobie niewidoczne podczas logowania konto, z którego mogą w sposób niekontrolowany korzystać z zasobów komputera.

Nieświadomy niczego rodzic lub opiekun pracowni będzie nadal uruchamiał komputer, wpisując hasło lub podając hasło do konta z ograniczeniami. Dzieci jednak będą posiadały pełną i nieograniczoną kontrolę.

Ukryte konto tworzy się z poziomu profilu administratora. W pierwszej kolejności należy utworzyć zwykłe konto z prawami administratora. Nie należy się na nie logować.

Ukrywanie konta odbywa się poprzez wprowadzenie zmian w rejestrze systemowym. Dostęp do rejestru uzyskuje się, wybierając: **Start / Uruchom**. W okienku **Uruchamianie** należy wpisać **regedit** i kliknąć **OK**. Uaktywnione zostanie okienko **Edytora rejestru** (rys. 16).



Rys.16. *Edytor rejestru* systemu operacyjnego Windows XP

W lewym panelu, klikając na małych kwadracikach ze znakiem „+”, przechodzi się do następującej gałęzi rejestru:

HEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon \ SpecialAccounts \ UserList

Rozwinięcie **UserList** spowoduje wyświetlenie zbioru elementów widocznych w prawym panelu (rys. 16). Jest wśród nich konto głównego **Administratora** systemu (odpowiednik konta root w Linuksie), które przy normalnych ustawieniach nie jest widoczne na ekranie logowania.

Kontrolując wpisy w powyższym okienku (prawy panel) można stwierdzić,

czy pojawiły się ukryte konta!

W prawym panelu klika się prawym przyciskiem myszy i wybiera: **Nowy / Wartość DWORD**.

Pojawi się nowy wpis **Nowa wartość #1**. Klika się na nim prawym przyciskiem myszy i wybiera **Zmień nazwę**. Teraz należy dokładnie wpisać nazwę nowego konta użytkownika (tego, które ma zostać ukryte).

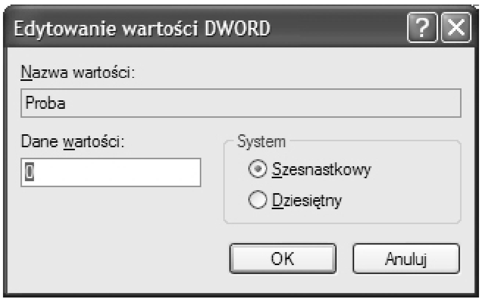
Na utworzonym w ten sposób obiekcie (tutaj konto **Proba**) klika się ponownie prawym przyciskiem myszy i wybiera **Modyfikuj**.

Otwarte zostanie okienko (rys. 17), w którym w polu **Dane wartości** można wpisać **0** lub **1**, gdzie:

0 - na ekranie logowania nie widać nowego użytkownika,

1 - na ekranie logowania użytkownik jest widoczny.

Po wpisaniu wartości **0** klika się **OK**. Od tego momentu nie widać użytkownika na ekranie logowania.



Rys.17. Edytor rejestru systemu operacyjnego Windows XP – edytowanie wartości DWORD

Ukryty użytkownik musi korzystać z tradycyjnego ekranu logowania systemu Windows. Gdy pojawia się ekran powitalny z nazwami użytkowników, należy: trzymając wciśnięte jednocześnie przyciski: **Alt** i **Ctrl**, dwukrotnie nacisnąć przycisk **Delete**. Pojawi się wówczas okienko (rys. 18), w którym trzeba ręcznie wpisać nazwę użytkownika oraz hasło, a następnie kliknąć **OK**.

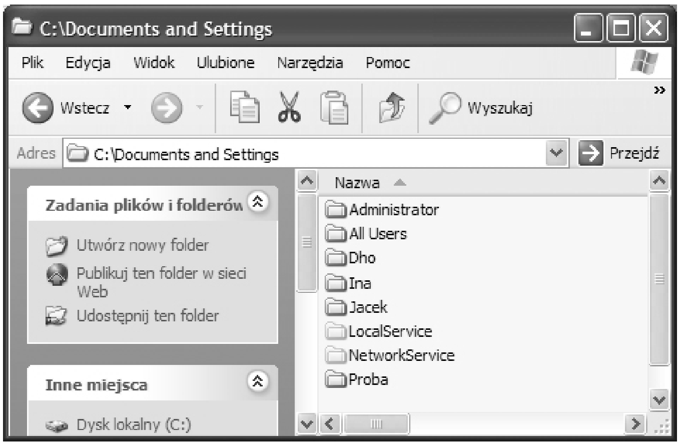
Rys.18. Tradycyjne okienko logowania systemu Windows

Kasowanie ukrytego konta użytkownika

W polu **Dane wartości** (rys. 17) wpisuje się wartość **1** i klika się **OK**. Następnie w okienku (rys. 16) klika się prawym przyciskiem myszy na nazwie ukrytego konta i wybiera **Usuń**. Teraz zamyka się okienko **Edytora rejestru**.

Ukryte do tej pory konto użytkownika będzie już widoczne podczas logowania. Kolejnym krokiem jest przejście do Panelu sterowania: **Start / Ustawienia / Panel sterowania**. Tam klika się dwukrotnie na ikonie **Konta użytkowników**, następnie na nazwie konta, które ma zostać skasowane, w otwartym wówczas okienku wybiera się **Usuń**.

Najprostszym sposobem stwierdzenia, czy w komputerze pojawiły się nowe konta, jest przejście do następującej lokalizacji: **C:\ Dokuments and Settings**. W otwartym okienku (rys. 19) widoczne są foldery z nazwami użytkowników. Oczywiście inspekcji tej należy dokonywać, gdy aktywne jest wyświetlanie ukrytych plików i folderów. W dowolnym folderze wybiera się: **Narzędzia / Opcje folderów /** teraz zakładka **Widok**, a następnie wybrać **Pokaż ukryte pliki i foldery / Zastosuj / OK**.



Rys.19. Zawartość folderu *Dokuments and Settings*, to konta użytkowników systemu operacyjnego Windows XP

Uwaga! Jeśli w **Panelu sterowania** dokona się zmiany nazwy użytkownika, to zmiana ta będzie widoczna na ekranie logowania. Jednak w lokalizacji **C:\ Dokuments and Settings** wszystkie pliki użytkownika będą nadal zawarte w folderze, którego nazwa jest pierwotną nazwą konta użytkownika. Chcąc zatem ukryć (lub odnaleźć) konto użytkownika w **Edytorze rejestru**, należy brać pod uwagę jego pierwotną nazwę.

Foldery prywatne

Foldery prywatne - dostępne są wyłącznie dla tworzącego je, zalogowanego użytkownika. W systemie operacyjnym (na partycjach NTFS) **Windows XP Home Edition** oraz **Windows XP Professional** (z włączoną opcją: **Użyj prostego udostępniania plików**) możliwe jest utworzenie folderów prywatnych.

Foldery te mogą znajdować się wyłącznie w obrębie lokalizacji: **C:\ Documents and Settings** czyli, np. **Pulpit** lub **Moje dokumenty**.

Włączanie opcji prostego udostępniania plików: **Mój komputer /** w pasku menu **Narzędzia / Opcje folderów /** zakładka **Widok /** zaznacza się **Użyj prostego udostępniania plików**.

Tworzenie folderu prywatnego

Należy kliknąć prawym przyciskiem myszy na folderze (musi znajdować się na **Pulpicie** lub w **Moich dokumentach**), wybrać **Właściwości** i w otwartym okienku (rys. 20) zakładkę **Udostępnianie**. Teraz zaznacza się opcję **Uczyń ten folder folderem prywatnym**.

Od tego momentu do zawartości tego folderu ma dostęp wyłącznie osoba logująca się na konto, na którym został utworzony folder prywatny.

Rys. 20. Tworzenie folderów prywatnych

Dostęp do cudzego folderu prywatnego

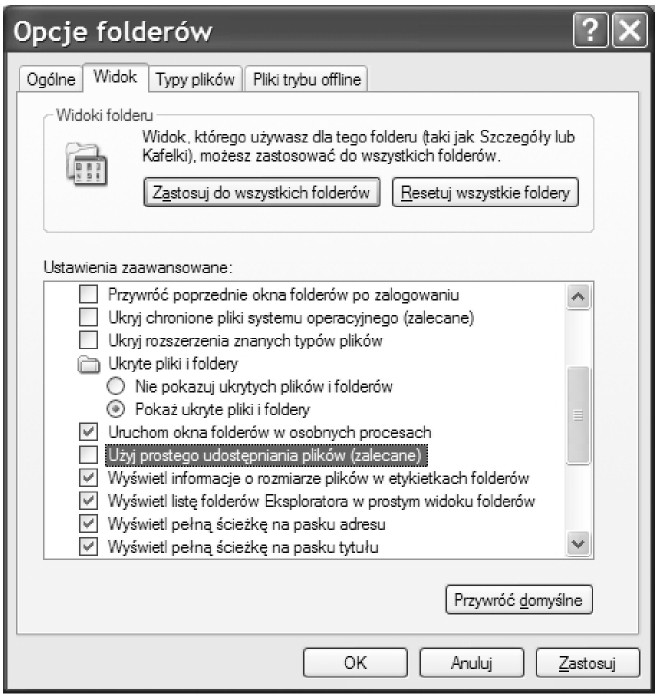
W systemie Windows XP Home Edition jest to rozwiązanie stosunkowo bezpieczne. Żaden użytkownik logujący się na swoim koncie nie ma dostępu do folderów prywatnych pozostałych użytkowników.

Należy pamiętać, że jeśli właściciel folderu prywatnego przenosi go w inne miejsce (oprócz **Pulpitu** i **Moich dokumentów**), to folder ten przestaje być folderem prywatnym (każdy ma do niego dostęp).

W systemie operacyjnym Windows XP Professional bardzo łatwo można obejść takie zabezpieczenie, dlatego że Windows XP Home Edition nie szyfruje plików.

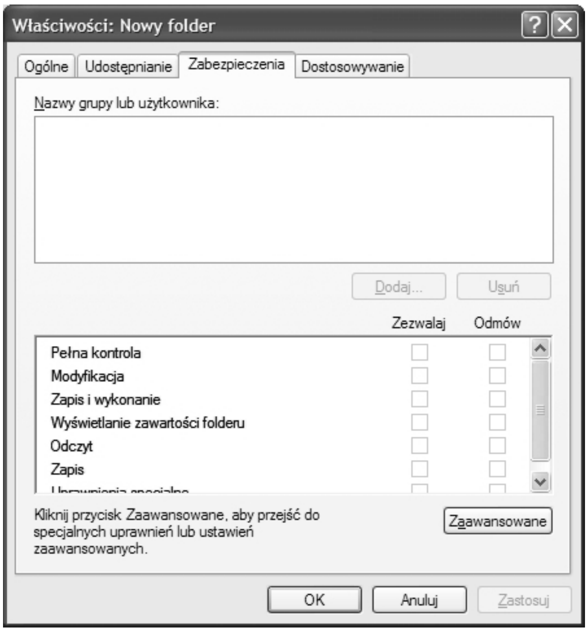
Poniżej omówiony zostanie sposób, w jaki można uzyskać dostęp do folderu prywatnego w Windows XP Professional. Należy pamiętać, że sposobu tego należy korzystać wyłącznie w przypadku awarii systemu, gdy zachodzi potrzeba odzyskania danych.

W takiej sytuacji, dysk z uszkodzonym systemem operacyjnym Windows XP Home Edition, podpina się do komputera pracującego pod kontrolą systemu Windows XP Professional. Po uruchomieniu komputera, w dowolnym otwartym okienku, np. **Mój komputer** wybiera się na pasku menu: **Narzędzia / Opcje folderów.** W otwartym okienku (rys. 21) przechodzi na zakładkę **Widok,** a następnie zabiera zaznaczenie przy opcji **Użyj prostego udostępniania plików**, teraz klika się: **Zastosuj** i **OK**.



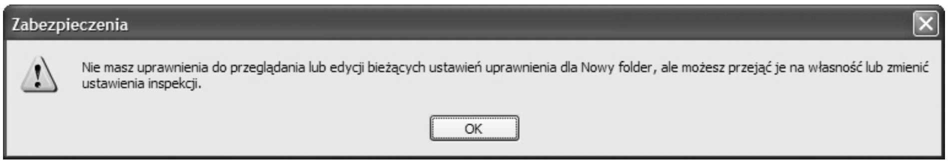
Rys. 21. Włączanie opcji – *Użyj prostego udostępniania plików*

Należy na odpowiedniej partycji znaleźć folder **Documents and Settings**, wewnątrz nazwę użytkownika, którego folder zamierza się przejąć. Tam odszukuje się foldery **Moje dokumenty** lub **Pulpit**, a następnie określony folder prywatny. Klika się na nim prawym przyciskiem, w otwartym w ten sposób okienku (rys. 22) przechodzi na zakładkę **Zabezpieczenia**.



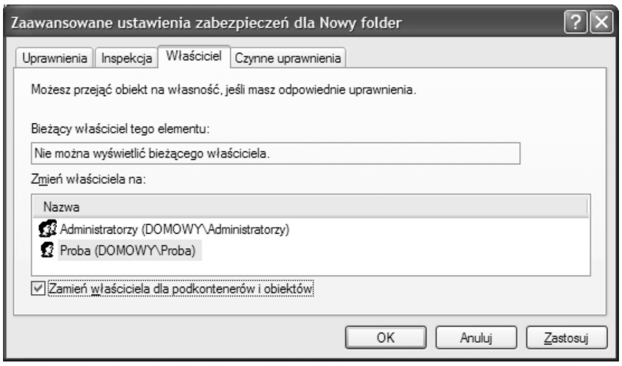
Rys. 22. Przejmowanie praw do cudzego folderu prywatnego

Wówczas pojawia się komunikat o braku praw do przeglądania zawartości danego folderu i możliwości przejęcia tych praw (rys. 23) - klika się wówczas **OK**. Na zakładce **Zabezpieczenia** wybiera się **Zaawansowane** (rys. 22).



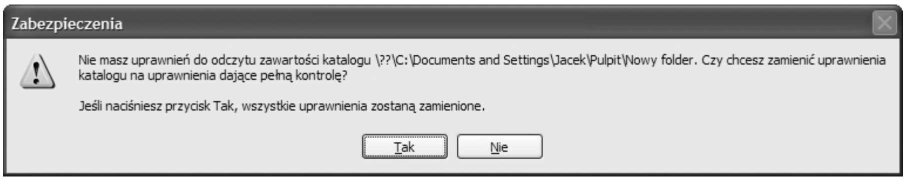
Rys. 23. Komunikat o możliwości przejęcia praw do zawartości cudzego folderu

W ten sposób otwarte zostaje kolejne okienko (rys. 24), w którym na zakładce **Właściciel** zaznacza się nazwę konta, z którego następuje próba przejęcia uprawnień. Poniżej wybiera się: **Zmień właściciela dla podkontenerów i obiektów / Zastosuj**.



Rys. 24. Wybór użytkownika, który przejmuje prawa do cudzego folderu

Pojawi się okienko (rys. 25) z prośbą o potwierdzenie chęci przejęcia pełnej kontroli nad cudzymi danymi. Po wyrażeniu zgody można już przeglądać zawartość takiego folderu.



Rys. 25. Ostatnie potwierdzenie przed przejęciem praw dostępu do cudzego folderu

Rozwiązania tego należy używać wyłącznie do odzyskiwania danych! Jeśli w ten sposób potraktuje się czyjś folder prywatny, to legalny użytkownik straci możliwość dostępu do zawartych w nim danych. Oczywiście powtarzając powyższą procedurę, może on odzyskać dostęp. Odczyta ponadto nazwę użytkownika, który przeglądał jego pliki.

Powyższy przykład można przećwiczyć także na jednym komputerze pracującym pod kontrolą systemu operacyjnego Windows XP Professional. Jeden użytkownik tworzy folder prywatny z aktywną opcją **Użyj prostego udostępniania plików,** a drugi na swoim profilu po dezaktywacji opcji **Użyj prostego udostępniania plików,** postępuje w podany powyżej sposób i przejmuje prawa do folderu.

Blokowanie dostępu do aplikacji oraz wybranych lokalizacji w systemie Windows XP Professional

Blokowanie dostępu do aplikacji

Mając pod opieką komputery w szkolnej pracowni, należy pamiętać o zablokowaniu dostępu do aplikacji, które mogą utrudniać prawidłowy przebieg zajęć lub stanowić potencjalne zagrożenie. Na przykład program Winamp umożliwia oglądanie pornograficznych stacji telewizyjnych, korzystając z komunikatora Gadu-Gadu, można rozsyłać SMS'y z pogróżkami itd.

Blokowanie dostępu do aplikacji bez stosowania dodatkowego oprogramowania jest możliwe tylko w systemie Windows XP Professional (nie dotyczy wersji Home Edition), pod warunkiem, że aplikacja, którą zamierza się zablokować, jest zapisana na partycji z systemem plików NTFS.

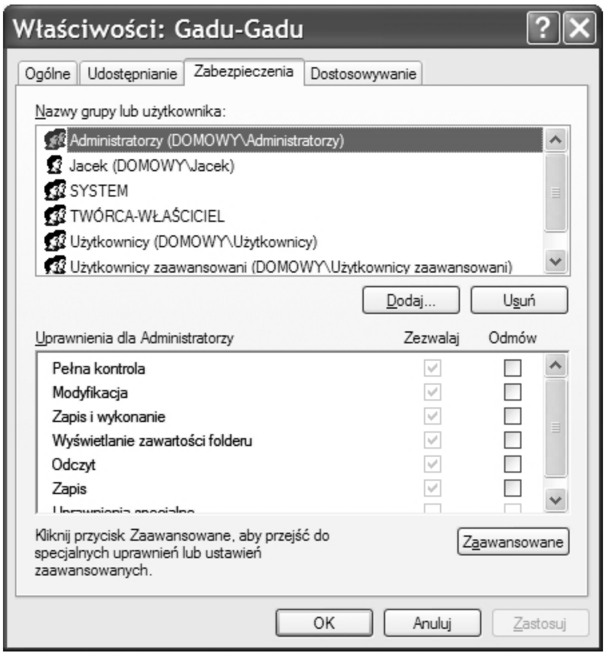
Komputer, w którym planuje się wprowadzenie ograniczeń, musi mieć przynajmniej dwóch użytkowników: konto administratora chronione hasłem oraz konto z ograniczeniami (niekoniecznie chronione hasłem).

Konto ucznia, na którym planuje się ograniczyć dostęp do wybranych aplikacji, musi być „kontem z ograniczeniami”. W **Panelu sterowania**, po uaktywnieniu ikony **Konta użytkowników**, wybiera się użytkownika (tutaj konto „Proba”), któremu zostaną ograniczone prawa dostępu. Uaktywnione zostanie wtedy okienko, w którym klika się na opcji **Zmień typ konta**. W kolejnym, otwartym automatycznie, okienku klika się w polu **Ograniczone**, a następnie na przycisku **Zmień typ konta**.

Dalsze działania są możliwe, gdy jest wyłączone proste udostępnianie plików. W dowolnym otwartym okienku, np. **Mój komputer** wybiera się na pasku menu: **Narzędzia / Opcje folderów.** W otwartym okienku przechodzi się na zakładkę **Widok,** a następnie zabiera się zaznaczenie przy opcji **Użyj prostego udostępniania plików**, a następnie: **Zastosuj / OK**.

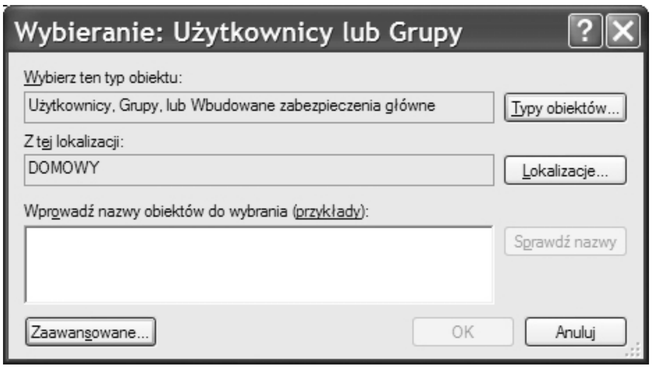
Przykład 1. - Blokowanie dostępu do komunikatora Gadu-Gadu

Będąc zalogowanym na koncie administratora, należy przejść na partycję **C**, do folderu **Program Files** i odnaleźć folder **Gadu-Gadu**. Teraz trzeba kliknąć na nim prawym przyciskiem myszy i wybrać **Właściwości**. W otwartym w ten sposób okienku należy przejść na zakładkę **Zabezpieczenia** i kliknąć na przycisku **Dodaj** (rys. 26).



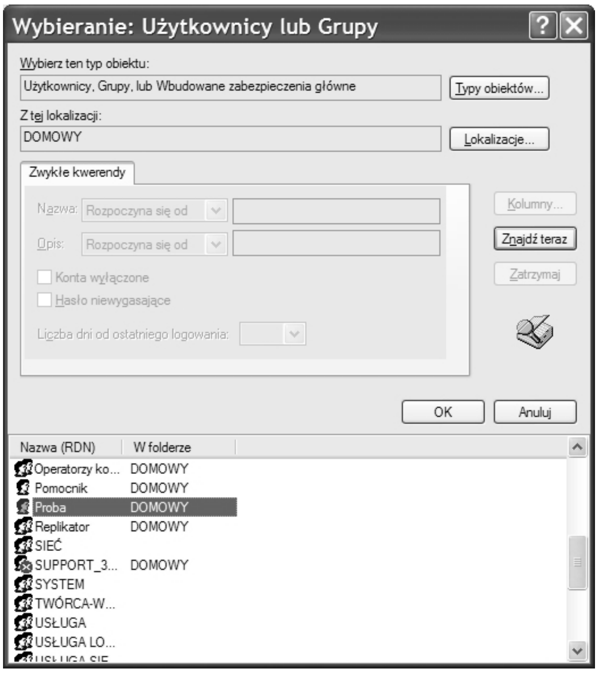
Rys. 26. Ograniczanie dostępu wybranej aplikacji

W ten sposób otworzy się kolejne okienko (rys.27), w którym należy wybrać **Zaawansowane**.



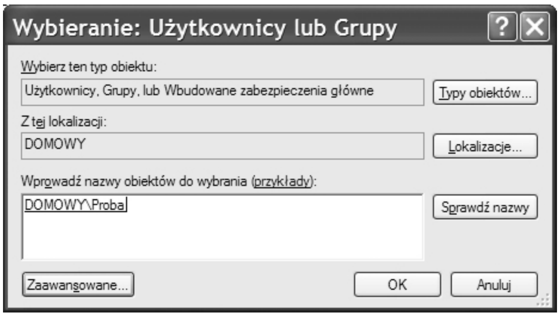
Rys. 27. Kliknięcie na przycisku *Zaawansowane* pozwala wybrać użytkowników, którym zostaną ograniczone prawa dostępu do wybranych aplikacji

Otworzy się wówczas okienko (rys. 28), w którym wybiera się **Znajdź teraz**. W dolnej części okienka odszukuje się użytkownika, któremu należy odebrać prawa do korzystania z programu Gadu-Gadu. Klika się na jego nazwie (musi podświetlić się na niebiesko) i naciska **OK**.



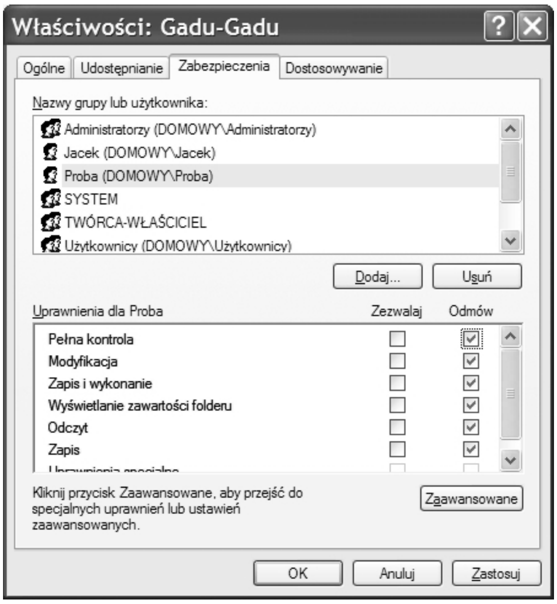
Rys. 28. Wybór użytkownika, któremu odbiera się prawa do korzystania z wybranej aplikacji

Okienko to zamknie się, a w okienku (rys. 27) pojawi się nazwa użytkownika, któremu ogranicza się prawa dostępu (rys. 29).



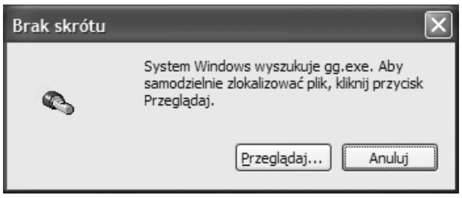
Rys. 29 W polu *Wprowadź nazwy obiektów do wybrania* pojawiła się nazwa użytkownika, któremu zostaną odebrane prawa dostępu do określonej aplikacji

Po kliknięciu **OK** wraca się do okienka znanego już z rysunku numer 26 (rys. 30), w którego górnej części jest już widoczna nazwa dodanego użytkownika (tutaj **Proba**). Klika się na tej nazwie i zabiera wszystkie zaznaczenia z kolumny **Zezwalaj** oraz zaznacza się wszystkie opcje w kolumnie **Odmów**.



Rys. 30. Wszelkie uprawnienia z kolumny *Zezwalaj* zostały zastąpione odmowami

Klikając **Zastosuj**, potwierdza wolę wprowadzenia ograniczeń. Teraz można już wylogować się z konta administratora. Po zalogowaniu na konto ucznia (z ograniczeniami) należy dokonać próby uruchomienia programu Gadu-Gadu. Na ekranie powinien pojawić się komunikat o braku możliwości znalezienia wymaganych plików (rys. 31). Uczniowie stracili dostęp do komunikatora. Oczywiście program ten działa bez zmian na każdym innym koncie tego komputera.



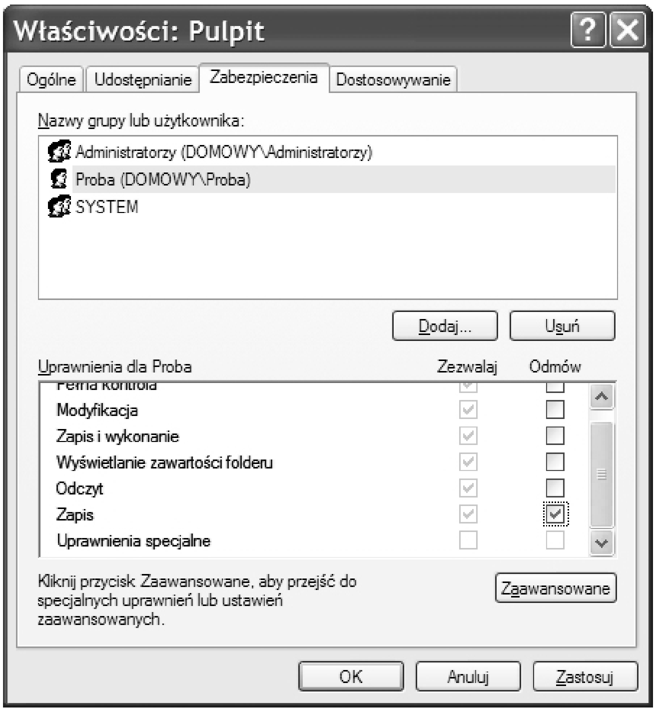
Rys. 31. Komunikat potwierdzający brak uprawnień do wybranej aplikacji

Przykład 2. - Blokowanie możliwości zapisu na pulpicie
(lub w każdym innym miejscu na partycji NTFS)

W pracowni, w której nie wprowadzono blokady zapisu na pulpicie, po kilku godzinach zajęć panuje straszny bałagan. Wskazane jest zatem zablokowanie dostępu do tej lokalizacji.

Należy postępować analogicznie jak w przypadku blokowania dostępu do Gadu-Gadu. Zamiast klikania prawym przyciskiem na folderze Gadu-Gadu (opis nad rysunkiem nr 26), wykonuje się tę operację na folderze **Pulpit**. Folder ten można znaleźć w następującej lokalizacji: **C:\ Documents and Settings \ Nazwa użytkownika,** któremu odbiera się uprawnienia **\ Pulpit**.

Różnica w procedurze postępowania pojawia się w momencie wyboru dostępnych uprawnień (rys. 32). W kolumnie **Odmów** zaznacza się opcję **Zapis**.



Rys. 32. Ograniczając prawa zapisu na *Pulpicie*, w kolumnie *Odmów* zaznacza się wyłącznie opcję *Zapis*

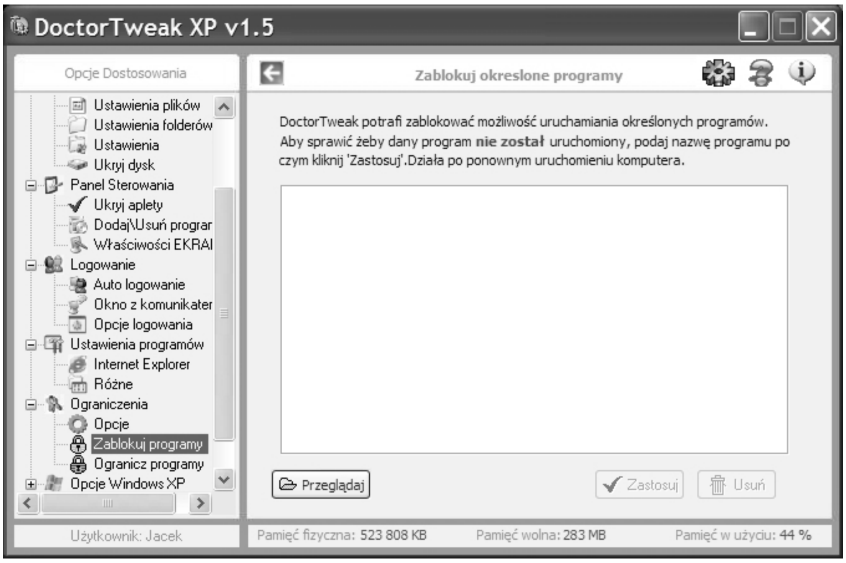
Po wprowadzeniu zmian należy wylogować się z konta administratora i zalogować na konto ucznia (z ograniczeniami). Wszelkie próby zapisu na pulpicie zakończą się komunikatem o braku dostępu do tej lokalizacji (rys.33).

Rys. 33. Komunikat o braku uprawnień do zapisywania na *Pulpicie*

W obu opisanych przykładach przywrócenie uprawnień jest możliwe wyłącznie z poziomu konta administratora. W okienkach (rys. 30 i 32) należy odtworzyć pierwotny układ zaznaczonych opcji. Warto zatem przed dokonaniem zmian sporządzić odpowiednie notatki.

Kontrola dostępu z poziomu aplikacji zabezpieczających
(także w Windows Home Edition)

W systemie Windows Home Edition omówione powyżej rozwiązania są niedostępne. Można jednak zastosować szereg aplikacji, które umożliwią uzyskanie podobnych efektów. Do ciekawych przykładów należy darmowy program **DoctorTweak XP**[6] (rys. 34) dostępny w polskiej wersji językowej.



Rys. 34. Istnieją aplikacje umożliwiające wprowadzanie ograniczeń dostępu do wybranych aplikacji także w systemie Windows Home Edition

Programy, które nie powinny pojawiać się w szkolnej pracowni

Szczególnie istotną kwestią jest blokowanie dostępu do aplikacji służących do nielegalnego pobierania plików z Internetu. Aplikacje tego typu bazują na technologii P2P. Pobierane filmy, muzyka lub oprogramowanie są zapisywane na dyskach twardych. Stamtąd ich fragmenty trafiają do innych osób ściągających ten sam plik. Pobieranie dowolnych danych z Internetu nie jest w Polsce zakazane, jednak dalsza dystrybucja, czyli to, co dzieje się w przypadku programów P2P, jest ścigane jak paserstwo.

Użytkownicy sieci poradzili sobie i z tym problemem. Pojawiły się aplikacje P2M (Per2Mail). Pliki umieszczane są w dużych darmowych skrzynkach pocztowych. Podczas bardzo szybkiego pobierania plików, żadne ich fragmenty nie trafiają do osób trzecich.

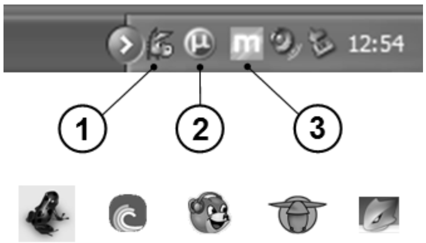
Nauczyciele oraz rodzice mając na uwadze możliwe konsekwencje, powinni umieć rozpoznać tego typu aplikacje w komputerach szkolnych i domowych. Poniżej znajdują się są ikony niebezpiecznych programów (rys. 35).

1. eMule - popularny program P2P,

[6] Autorem programu jest Marcin Ficowski (http://www.ficsite.ltd.pl/).

2. uTorrent - program P2P (program trudny do zablokowania przez administratorów sieci),
3. MoorHunt - program P2M.

Pod rysunkiem zamieszczone są ikony analogicznych programów: Azureus, BitTorrent, BearShare, eDonkey, BitSpirit.



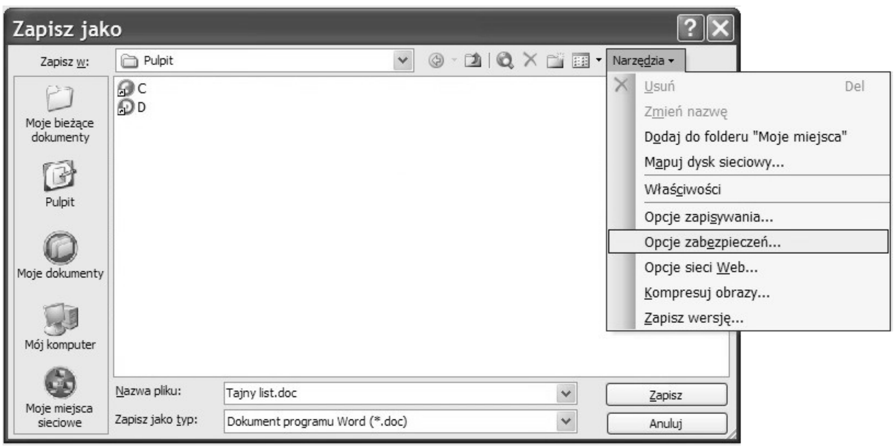
Rys. 35. Programy służące do nielegalnego pobierania plików z Internetu

Pakiety biurowe -zabezpieczanie dokumentów hasłem

MS Word (podobnie, np. MS Power Point)

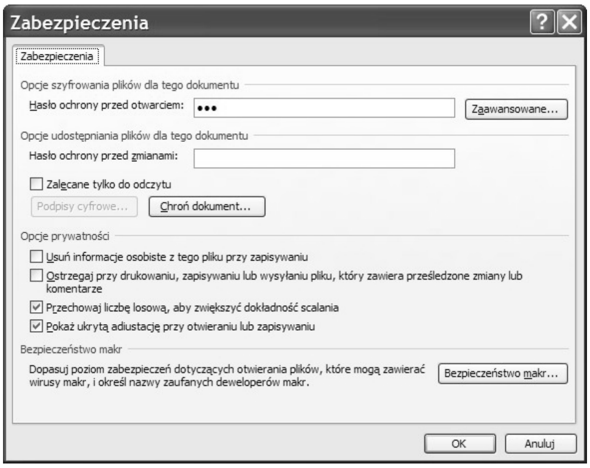
Zapisując dokument Worda wybiera się: **Plik / Zapisz jako**. Wówczas zostanie otwarte okienko (rys. 36), w którym wpisuje się nazwę pliku oraz jego lokalizację (tutaj - Pulpit). Zanim kliknie się na przycisku **Zapisz**, wybiera się: **Narzędzia**, a następnie **Opcje zabezpieczeń**

W Excelu zamiast **Opcji zabezpieczeń** należy wybrać się **Opcje ogólne** (pozostałe kroki są bardzo zbliżone).



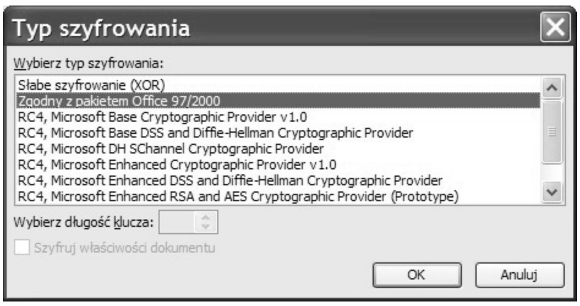
Rys. 36. Microsoft Word – zapisywanie dokumentu zabezpieczonego hasłem

Otwarte zostanie w ten sposób okienko **Zabezpieczenia** (rys. 37). Tu w polu **Hasło ochrony przed otwarciem,** należy wpisać wymyślone przez siebie hasło (im dłuższe, złożone z liter dużych i małych oraz cyfr, tym trudniejsze do złamania).



Rys. 37. Microsoft Word – wprowadzanie hasła ochrony przed otwarciem

Klikając na przycisku **Zaawansowane,** otwiera się dodatkowe okienko **Typ szyfrowania** (rys. 38). Tu można wybrać słabe szyfrowanie (zgodne z pakietem Office 97/2000). Dokument taki będzie można otworzyć w starszych wersjach MS Office. Jeśli istotne jest mocne szyfrowanie (dostępne w MS Office 2003 i wyższych), należy wybrać inny typ szyfrowania.

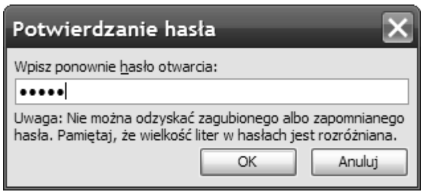


Rys. 38. Microsoft Word – szyfrowanie zgodne z pakietem Office 97/2000

Każdy typ szyfrowania udostępnia, tzw. klucz - im dłuższy tym szyfrowanie mocniejsze (rys. 39).

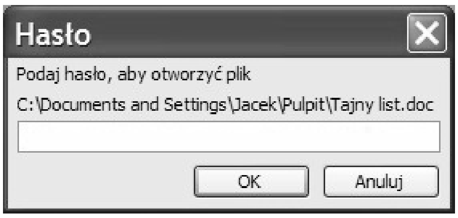
Rys. 39. Microsoft Word – możliwość wyboru „mocniejszego" szyfrowania

Po wybraniu typu szyfrowania klika się **OK**, następnie w okienku (rys. 37) ponownie **OK**. Wtedy otwarte zostanie okienko (rys. 40), w którym należy wpisać hasło. Hasła zawsze są maskowane w postaci czarnych kropek. Nie ma zatem możliwości kontrolowania poprawności jego zapisu. Jeśli hasło zostanie wpisane dwukrotnie, oznacza to, iż nie popełniono błędu literowego oraz, że zostało poprawnie zapamiętane.



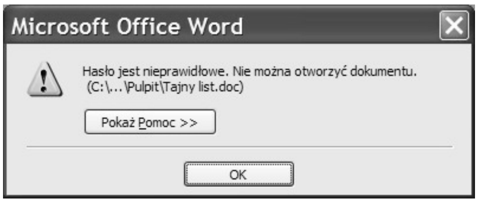
Rys. 40. Procedura podwójnego wpisywania hasła zabezpieczającego dokument

Jeśli zapisany w ten sposób plik zostanie zamknięty i nastąpi próba jego otwarcia, to pojawi się wówczas okienko (rys. 41), w którym należy podać poprawne hasło.



Rys. 41. Otwarcie zabezpieczonego dokumentu wymaga podania hasła

W przypadku podania błędnego hasła, pojawi się okienko (rys. 42) informujące o pomyłc. Dokument nie zostanie otwarty.

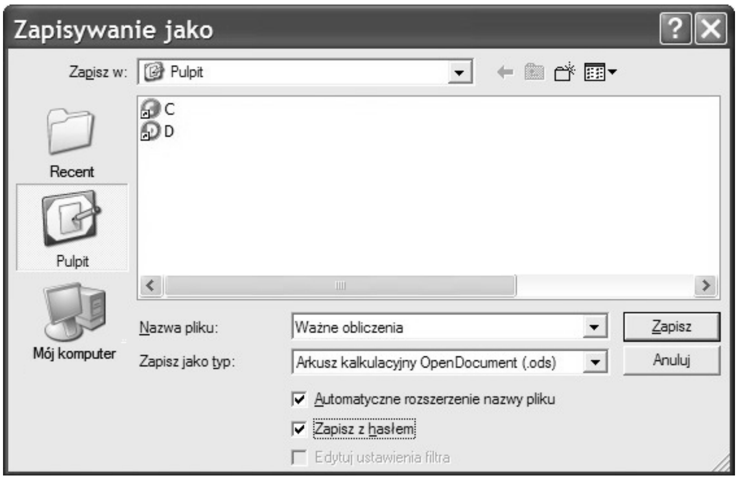


Rys. 42. Komunikat o błędnie wpisanym haśle

Pakiet Open Office (wszystkie aplikacje)

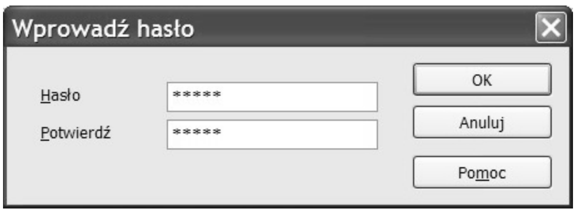
Zapisując dokumenty pakietu Open Office, wybiera się: **Plik / Zapisz jako**. Wówczas otwarte zostanie okienko (rys. 43), w którym wpisuje się nazwę pliku oraz jego lokalizację (tutaj - Pulpit).

Tam zaznacza się opcję: **Zapisz z hasłem**. Teraz należy kliknąć na przycisku **Zapisz**.



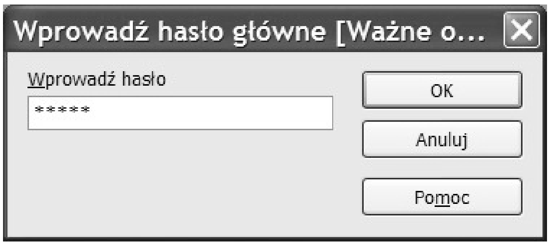
Rys. 43. Szyfrowanie dokumentów tworzonych z zastosowaniem aplikacji pakietu OpenOffice

Otwarte zostanie wówczas okienko (rys. 44), w którym dwukrotnie wpisuje się wymyślone przez siebie hasło. Musi to być przynajmniej 5 znaków. Jeśli liczba znaków będzie mniejsza, przycisk **OK** nie uaktywni się.



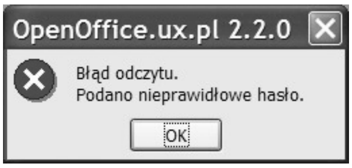
Rys. 44. Szyfrowanie aplikacji pakietu OpenOffice – hasło powinno mieć przynajmniej 5 znaków

Jeśli zapisany w ten sposób plik zostanie zamknięty i nastąpi próba ponownego otwarcia, pojawi się wówczas okienko (rys. 45). Należy podać w nim poprawne hasło.



Rys. 45. Pakiet OpenOffice – otwarcie zaszyfrowanego dokumentu wymaga podania odpowiedniego hasła

W przypadku podania błędnego hasła, pojawi się okienko (rys. 46). Dokument nie zostanie otwarty.



Rys. 46. Pakiet OpenOffice – komunikat o błędnie wpisanym haśle

Blokowanie dostępu do określonych treści w Internecie
Blokowanie aplikacji internetowych

Opieka nad komputerami, z których korzystają uczniowie, stawia przed nauczycielem obowiązek filtrowania treści, do jakich mogą oni dotrzeć z jego pomocą. Na rynku istnieje szereg aplikacji filtrujących. Ministerstwo Edukacji zaleca do wszystkich szkół darmowy program Beniamin, który można pobrać ze strony: http://www.beniamin.pl/pobierz.html/.

Program ten oprócz blokowania dostępu do stron, na których pojawiają się zdefiniowane w programie słowa (czarna lista) umożliwia blokowanie dostępu do wszelkich aplikacji łączących się z Internetem. Rodzice nie mają świadomości, iż nawet pozornie niewinny program do słuchania muzyki Winamp (lub inne łączące się z telewizją internetową) umożliwia bardzo łatwy dostęp do przekazów pornograficznych.

Osoba instalująca program musi wymyślić i wpisać hasło. Jego ponowne wpisanie czasowo dezaktywuje program, przywracając komputerowi pełen dostęp do Internetu.

Dokładny opis programu znajduje się na stronie: http://www.beniamin.pl/funkcje.html/.