PC/DACS for Windows 95
Data Access Control System

SYSTEM BEZPIECZEŃSTWA
DLA KOMPUTERÓW OSOBISTYCH

PODRĘCZNIK ADMINISTRATORA

WERSJA DLA OSÓB TESTUJĄCYCH

Wersja ta zawiera przetłumaczone fragmenty oryginalnej dokumentacji. Nie wystarczy do pełnej skutecznej administracji systemem. Wystarczy jednak do zapoznania się z jego możliwościami. Głównym jej przeznaczeniem jest umożliwienie wszystkim zainteresowanym zapoznanie się z systemem PC/DACS for Windows 95 bez konieczności posługiwania się oryginalną dokumentacją. W związku z faktem, iż jest to jedynie częściowe tłumaczenie, pewne fragmenty i rozdziały oryginalnej dokumentacji nie są w ogóle dostępne. W razie pytań prosimy o kontakt z dystrybutorem - SAFE COMPUTING Sp. z o.o.

UWAGA!

Niniejszy podręcznik jest skrótową kompilacją oryginalnych podręczników *PC/DACS for Windows 95 Getting Started* oraz *PC/DACS for Windows 95 Administrator Reference Manual*. Będziemy wdzięczni za wszelkie uwagi i komentarze dotyczące niniejszego *Podręcznika Administratora*. Formularz uwag znajduje się na końcu niniejszego podręcznika.

Numer dokumentu: D95A9701

I - POMOC TECHNICZNA

Pomoc techniczna udzielana jest przez polskiego dystrybutora firmy MERGENT:

Email dla pomocy technicznej: support@safecomp.com
Tel/fax (0-22) 6198956, 6700756, 6700956
Adres: 03-733 Warszawa, ul. Targowa 34
Http://www.safecomp.com/

Udzielanie pomocy technicznej przez SAFE COMPUTING odbywa się na zasadach ujętych w dokumencie *Zasady udzielania pomocy technicznej przez SAFE COMPUTING Sp. z o.o.*

UWAGA! Jeśli zakupiłeś PC/DACS od dealera SAFE COMPUTING, jest on zobowiązany umową dealerską do udzielenia Ci pomocy technicznej. SAFE COMPUTING nie obsługuje ani nie udziela pomocy technicznej użytkownikom końcowym, którzy zakupili produkty u dealerów SAFE COMPUTING.

II - PC/DACS for Windows 95 - Uwagi wstępne (nie pomijaj tego rozdziału!)

1. Nie przystępuj do instalacji systemu PC/DACS, bez zapoznania się z tym podręcznikiem. Zanim rozpoczniesz instalację, przeczytaj ten podręcznik **co najmniej raz**. PC/DACS jest systemem rozbudowanym (pozwala m.in. na zaszyfrowanie różnych fragmentów twardego dysku) i próba zapoznania się z nim bez czytania dokumentacji może mieć skutek odwrotny do zamierzonego.
2. Jednym z ważniejszych elementów PC/DACS, zabezpieczającym przed najprostszą metodą obejścia PC/DACS (przez start z dyskietki systemowej) jest tzw. blokada twardego dysku (*Boot Protection*, w skrócie BP). BP jest również odpowiedzialna za niskopoziomowe szyfrowanie twardego dysku. Po instalacji PC/DACS blokada ta **nie jest domyślnie włączona**. Fakt ten ma dwie implikacje:

- aby system PC/DACS rzeczywiście chronił komputer w warunkach "bojowych", należy bezwzględnie włączyć blokadę twardego dysku,
- z drugiej strony, istnieje możliwość pełnego zapoznania się z całą administracją PC/DACS bez włączania blokady twardego dysku.
  Zalecamy więc, aby wstępnie zapoznać się z PC/DACS **bez włączania blokady twardego dysku**.

3. Blokada twardego dysku systemu PC/DACS for Windows 95 może być używana tylko na komputerach, gdzie istnieją wyłącznie partycje Windows 95 (lub "stara" partycja DOS z systemem operacyjnym Windows 95). Nie instaluj PC/DACS for Windows 95 na komputerze posiadającym inne partycje.
4. Nie instaluj PC/DACS for Windows 95 na komputerze pracującym pod kontrolą DOS/Windows 3.x. Do ochrony PC-tów pracujących pod kontrolą DOS/Windows 3.x służy system PC/DACS for DOS/Windows.
5. **NIGDY nie formatuj twardego dysku**, nawet w sytuacji, gdy włączyłeś blokadę twardego dysku, zapomniałeś hasła administratora i jesteś przekonany, że straciłeś całkowicie dostęp do twardego dysku. PC/DACS jest świetnie przygotowany na tego rodzaju sytuacje awaryjne. W przypadku licencji firmowych, sam administrator posiada narzędzia służące do rozwiązywania takich sytuacji awaryjnych. W przypadku pojedynczych egzemplarzy PC/DACS, jeśli znalazłeś się w sytuacji awaryjnej, skontaktuj się z twoim dostawcą PC/DACS. Powtórzymy to jeszcze raz: **nigdy w takiej sytuacji nie formatuj twardego dysku.**
6. Zawsze czytaj to, co jest napisane na ekranie PC/DACS, w którym się aktualnie znajdujesz. Jeśli pozwoliło na to miejsce, producent systemu umieścił na każdym ekranie PC/DACS instrukcje dotyczące tego ekranu. Jeśli są one dla ciebie niewystarczające, naciśnij `<F1>`, aby uzyskać pomoc dotyczącą bieżącego ekranu.

III - Witamy w gronie klientów firmy MERGENT

Witamy w gronie klientów firmy MERGENT (a company of Utimaco Safeware Group), światowego lidera w dziedzinie bezpieczeństwa komputerów osobistych. Już wiele lat temu założyciele firmy MERGENT zidentyfikowali tendencję do przesuwania się technologii przetwarzania danych w kierunku rozwiązań klient-serwer i rozpoznali zwiększone zagrożenia wynikające z przenoszenia przechowywania i przetwarzania danych z komputerów typu *mainframe* na komputery PC.

MERGENT był pierwsza firmą, która zaoferowała rozwiązanie problemu bezpieczeństwa komputerów PC, przeznaczone dla dużych instytucji. Jako pierwsza opracowała system bezpieczeństwa dla Windows, jako pierwsza wprowadziła na rynek system bezpieczeństwa dla OS/2 2.0 i jako pierwsza opracowała narzędzia do jednolitej implementacji polityki bezpieczeństwa oraz jednokrotnego logowania się (*single sign-on*).

Wszystkie produkty MERGENT opracowane są z myślą o zwiększeniu bezpieczeństwa i efektywności pracy w twojej instytucji. Głównym celem niniejszej dokumentacji jest przekazanie ci informacji o krokach, które musisz wykonać, aby efektywnie używać zakupionego produktu. Ponadto dokumentacja ta pozwoli ci podjąć prawidłowe decyzje implementacyjne oparte o twoje potrzeby, informując cię o problemach i procedurach implementacyjnych.

Rozwiązania problemów bezpieczeństwa oferowane przez firmę MERGENT

Linia produktów firmy MERGENT to szeroki zakres skalowalnych rozwiązań służących do ochrony zasobów informatycznych twojej instytucji.

Rozwiązania dla Wirtualnych Sieci Prywatnych (VPN-ów)
- Rozwiązania szyfrujące typu *end-to-end*
- Rozwiązania dla bezpiecznego uwierzytelniania
- MERGENT Gauntlet Internet Firewall
- Rozwiązania dla śledzenia działań użytkowników (audytu)

Rozwiązania implementacyjne i wspomagające administrację bezpieczeństwem oraz produktywność
- DOMAIN/DACS (system centralnego zarządzania stacjami roboczymi sieci LAN chronionymi PC/DACS for DOS/Windows)
- SSO/DACS (Single Sign-On / DACS) - system jednokrotnego logowania się w złożonym środowisku

Systemy bezpieczeństwa dla komputerów PC
- PC/DACS for DOS/Windows
- PC/DACS for Windows 95
- Safe Guard Desktop for OS/2
- (już wkrótce!) Safe Guard Advanced Security for Windows NT

Systemy bezpieczeństwa dla notebooków
- Safe Guard Easy for DOS & Windows

- Safe Guard Easy for OS/2
- Safe Guard Easy for Windows 95

Konsulting implementacyjny i pomoc techniczna
MERGENT i jego dystrybutorzy oferują szeroko rozumianą pomoc przed- i posprzedażną. Oferta pomocy zawiera konsultacje przy analizie potrzeb bezpieczeństwa instytucji, pomoc przy instalacji i implementacji produktów oraz pomoc techniczną dla użytkowników i administratorów produktów.

Umowy partnerskie firmy MERGENT

Umowy partnerskie zawierane przez MERGENT zapewniają szybki rozwój produktów i ich kompatybilność z najnowszymi systemami i trendami na rynku informatycznym. MERGENT jest partnerem następujących firm:

- Liderów rynku informatycznego: IBM, Hewlett Packard, Microsoft, Novell, Banyan, Security Dynamics.
- Liderów rynku konsultingowego: Arthur Andersen, Coopers & Lybrand, Deloitte & Touche, Price Waterhouse i Ernst & Young.
- MERGENT jest członkiem OURS (Open Users Recommended Solutions).

IV - Co znajdziesz w pakiecie PC/DACS for Windows 95?

Gratulacje! Właśnie otrzymałeś rozwiązanie twoich problemów bezpieczeństwa na platformę Windows 95. System PC/DACS pozwoli ci na pełne zabezpieczenie twojego komputera i stworzenie nieograniczonej liczby autoryzowanych użytkowników.

W pakiecie znajdziesz:

- Osiem dyskietek, w tym:
  - Pięć dyskietek instalacyjnych PC/DACS for Windows 95
  - Jedną dyskietkę *Boot Protection Unlock Disk* (deinstalacji blokady twardego dysku)
  - Jedną dyskietkę *Implementation Disk*
  - Jedną dyskietkę *Migration Disk*
- Dwa podręczniki: *PC/DACS for Windows 95 Getting Started* oraz *PC/DACS for Windows 95 Administrator Reference Manual*.

V - Co to jest PC/DACS for Windows 95?

PC/DACS for Windows 95 jest systemem bezpieczeństwa dla komputerów osobistych pracujących pod kontrolą Windows 95. PC/DACS kontroluje dostęp do komputera i jego lokalnych zasobów, dopuszczając do nich tylko autoryzowanych użytkowników.

PC/DACS for Windows 95 posiada bardzo wiele funkcji bezpieczeństwa (kontrola dostępu, szyfrowanie, audyt i inne), jednak dzięki łatwości administracji i połączeniu funkcjonalności z elastycznością, pozwala on na łatwe zaimplementowanie wybranych mechanizmów ochronnych, zgodnie z obowiązującą w instytucji polityką bezpieczeństwa.

PC/DACS for Windows 95 jest całkowicie przezroczysty dla autoryzowanych użytkowników i nie przeszkadza w ich codziennej pracy, niezależnie od ilości zainstalowanych i włączonych funkcji bezpieczeństwa.

VI - Jakie możliwości posiada PC/DACS for Windows 95?

Oto w największym skrócie możliwości i funkcje realizowane przez PC/DACS for Windows 95:

- **Kontrola dostępu do komputera.** Z komputera mogą korzystać tylko autoryzowani użytkownicy, którzy muszą zidentyfikować się względem PC/DACS porzez podanie identyfikatora i hasła, lub włożenie dyskietki logującej (stanowiącej odpowiednik karty identyfikacyjnej).
- **Kontrola dostępu do zasobów.** Dla każdego autoryzowanego użytkownika lub grupy użytkowników można zdefiniować dowolne zasady dostępu do dowolnych zasobów komputera (plików, folderów, dysków).
- **Time Out.** Funkcja ta chroni komputer, z którego w danym momencie nikt nie korzysta, porzez zablokowanie dostępu do ekranu, klawiatury i myszy. Funkcja ta włączana może być automatycznie - po określonym czasie braku aktywności - lub ręcznie.
- **Boot Protection - blokada twardego dysku i szyfrowanie.** Funkcja ta uniemożliwia dostęp do twardego dysku po starcie z dyskietki. Zapewnia też opcjonalnie niskopoziomowe szyfrowanie twardego dysku. Szyfrowanie odbywa się w locie - jest przezroczyste dla autoryzowanych użytkowników.
- **Szyfrowanie zasobów.** Funkcja ta pozwala szyfrować pliki o określonych rozszerzeniach, foldery i/lub dyskietki. Szyfrowanie odbywa się w locie - jest przezroczyste dla autoryzowanych użytkowników.
- **Ochrona przed wirusami.** Funkcja ta, w połączeniu z blokadą twardego dysku, zapewnia zabezpieczenie przed zawirusowaniem komputera.
- **Ochrona przed ponownym używaniem obiektów (Object Re-use).** Funkcja ta uniemożliwia odzyskanie skasowanych plików poprzez zamazanie obszaru dysku, w którym rezydował skasowany plik. Dodatkowo, Kosz Windows może być czyszczony automatycznie przy każdorazowym przelogowaniu użytkownika, aby uniknąć odzyskania plików przez nieautoryzowane osoby.
- **Zaufane aplikacje.** Funkcja ta pozwala na zdefiniowanie tzw. zaufanych aplikacji, co pozwala na przydzielenie praw do zasobów aplikacjom, a nie użytkownikom, co z kolei pozwala na udostępnienie zasobów użytkownikom tylko wtedy, gdy korzystają oni z tych zasobów z pośrednictwem określonych aplikacji.
- **Dodatkowe elementy kontroli dostępu.** Funkcja ta pozwala na gradacyjne kontrolowanie dostępu do stacji dyskietek, portów LPT i COM komputera oraz na kontrolę dostępu niskiego poziomu do dysku.
- **Audyt (dziennik działań).** PC/DACS umożliwia rejestrowanie wszystkich działań użytkowników i administratora.

VII - Informacja dla końcowego użytkownika komputera zabezpieczonego systemem PC/DACS

Następne dwie strony przeznaczone są dla końcowego, "zwykłego" użytkownika komputera PC, zabezpieczonego systemem PC/DACS for Windows 95. Zawarte są tu podstawowe informacje na temat PC/DACS for Windows 95 oraz informacje mające na celu ułatwienie pracy użytkownikowi. Prosimy wykonać odpowiednią ilość kserokopii następnych dwóch stron i przekazać je do końcowych użytkowników.

Przed wykonaniem kserokopii możesz zmodyfikować tekst tak, aby odpowiadał on standardom, zasadom oraz rozwiązaniom technicznym przyjętym w twojej instytucji.

UWAGA! Do przekazywania "zwykłym" użytkownikom przeznaczone są wyłącznie te (dwie) strony z niniejszego podręcznika. Wszelkie inne informacje przeznaczone sa wyłącznie dla administratora.

INFORMACJE DLA UŻYTKOWNIKA KOMPUTERA CHRONIONEGO SYSTEMEM BEZPIECZEŃSTWA PC/DACS

Co to jest system PC/DACS for Windows 95?
PC/DACS for Windows 95 jest to oprogramowanie zwane systemem bezpieczeństwa, mające na celu ochronę twojego komputera i przechowywanych w nim danych przed nieautoryzowanym dostępem. PC/DACS został zainstalowany i skonfigurowany na twoim komputerze przez administratora. Administrator skonfigurował PC/DACS tak, aby informacje w twoim komputerze były zabezpieczone przed intruzami, a jednocześnie byś mógł bez przeszkód wykonywać swoje codzienne obowiązki. Jeśli będziesz chciał zmienić cokolwiek w konfiguracji systemu bezpieczeństwa PC/DACS lub twojego komputera, będziesz musiał skontaktować się z administratorem.

Co się zmieni w mojej pracy?
Jedyną zmianą w twojej codziennej pracy będzie konieczność podania identyfikatora i hasła podczas startu komputera. Po zainstalowaniu PC/DACS for Windows 95 nikt nie może skorzystać z twojego komputera bez podania swojego identyfikatora i hasła. Jeśli twój komputer ma więcej niż jednego użytkownika, każdy z użytkowników ma inny identyfikator i hasło. Swoje hasło uzyskasz od administratora. Administrator może dodać nowych lub usunąć istniejących użytkowników.

Twój identyfikator i hasło
Twój identyfikator i hasło stanowią "klucz" do twojego komputera (w fachowym języku mówi się, że "uwierzytelniają" cię względem systemu bezpieczeństwa). Hasło, które otrzymasz od administratora, jest jedynie tzw. "hasłem przekazania". Oznacza to, że po zalogowaniu się (wpisaniu identyfikatora i hasła) do systemu PC/DACS for Windows 95, będziesz musiał od razu to hasło zmienić - na dowolne, wybrane przez ciebie hasło. Wybierając hasło, pamiętaj, żeby nie wybrać hasła, które łatwo jest zgadnąć - np. imienia twojej żony, dziecka, daty urodzenia itp. Każdy, kto domyśli się, jakie masz hasło, może dostać się do twojego komputera i działać "na twoje konto". Nie powinieneś nigdzie w widocznym miejscu zapisywać swojego hasła, ani podawać go nikomu innemu. Wszyscy ci, którzy potrzebują skorzystać z twojego komputera, mają swoje własne hasła, a o ich prawie dostępu decyduje administrator. Administrator mógł nałożyć ograniczenia na treść twojego hasła, aby nie było ono zbyt proste do zgadnięcia. Mógł on np. określić minimalną ilość znaków dla hasła, zdecydować, że hasło ma zawierać 4 litry i 4 cyfry itp. Hasło, które wybierzesz dla siebie, będzie musiało być zgodne z tym standardem. Na wypadek, gdy zapomnisz hasła, administrator może ci nadać ponownie hasło przekazania.

Jak rozpocząć pracę z komputerem (zalogować się)?
Aby rozpocząć pracę, musisz zalogować się do komputera (podać swój identyfikator i hasło). Te dane wpisujesz do okna logującego PC/DACS. Okno logujące PC/DACS pojawia się gdy: włączysz komputer, zresetujesz komputer, wylogujesz się (zakończysz sesję pracy) z twojego komputera. Aby zalogować się, gdy pojawi się okno logujące PC/DACS:

1. Wpisz swój identyfikator w polu User ID. Naciśnij TAB, aby przejść do pola Password.
2. Wpisz swoje hasło w polu Password. Podczas pisania będą pojawiać się gwiazdki, tak, aby nikt nie podejrzał twojego hasła.
3. Naciśnij guzik Logon (znajdujący się w dolnej części okna logującego), aby zakończyć proces logowania się.

Time Out (blokada komputera po określonym czasie braku aktywności)
Time Out jest funkcją pozwalającą chronić twój komputer, gdy odejdziesz od niego na jakiś czas bez wylogowywania się. Po upływie określonego czasu od przerwania pracy system PC/DACS blokuje dostęp do komputera, tak, aby żaden intruz nie dostał się do twoich danych podczas gdy nie ma cię przy komputerze. Aby ponownie dostać się do komputera (przywrócić sesję pracy), będziesz musiał podać swoje hasło.

- **Blokada włącza się automatycznie**, gdy system wykryje brak aktywności z klawiatury lub myszy przez czas określony przez administratora.
- **Blokadę sesji możesz też i powinieneś włączyć ręcznie**, gdy chcesz na chwilę odejść od komputera. W tym celu wciśnij jednocześnie klawisze lewy Shift, prawy Shift i Alt (sekwencja ta mogła zostać zmieniona przez administratora). Możesz też włączyć blokadę sesji myszą. W tym celu kliknij prawym klawiszem myszy na logo (znaku) firmy MERGENT (producenta systemu PC/DACS). Znak ten to czerwony trójkąt w prawym dolnym rogu ekranu na pasku zadań Windows 95. Następnie wybierz opcję Time Out Now z menu, które się pokaże.

- **Aby powrócić do pracy z zablokowanej sesji**:

1. Podczas gdy sesja jest zablokowana, wciśnij dowolny klawisz lub użyj myszy. Pojawi się okno dialogowe z polem na wpisanie hasła.
2. Wpisz swoje hasło w polu Password. Podczas pisania będą pojawiać się gwiazdki, tak, aby nikt nie podejrzał twojego hasła.
3. Naciśnij <Enter> albo guzik OK, aby powrócić do swojej sesji.

Jak zmienić hasło?

Początkowa zmiana hasła przekazania

Pierwszy raz logujesz się do systemu z jednorazowym hasłem przekazania. Od razu po pierwszym zalogowaniu się, system PC/DACS wyświetli okno zmiany hasła.

1. Wpisz swoje nowe (wymyślone przez ciebie) hasło w polu New Password. Naciśnij <TAB>, aby przejść do pola Confirm new password.
2. W polu Confirm new password wpisz ponownie swoje nowe hasło, aby uniknąć pomyłki.
3. Naciśnij <Enter> albo guzik OK, aby zakończyć procedurę zmiany hasła. Odtąd do zalogowania się do komputera lub przywrócenia zablokowanej sesji musisz używać nowego hasła. Twój identyfikator pozostał bez zmian.

Zmiana hasła wykonywana przez użytkownika

W dowolnym momencie możesz zmienić swoje hasło. Możesz to zrobić np. gdy podejrzewasz, że ktoś domyśla się, jakie masz hasło. Hasło w PC/DACS zmienia się za pomocą standardowych narzędzi Windows 95.

1. Kliknij guzik Start na pasku zadań. Następnie kliknij Ustawienia, a potem Panel sterowania. Pojawi się Panel sterowania.
2. Kliknij podwójnie na ikonie Hasła.
3. Kliknij guzik Zmień inne hasła.
4. Z listy Wybierz hasło wybierz PC/DACS for Windows 95 Logon i naciśnij guzik Zmień. Pojawi się okno zmiany hasła.
5. Wpisz swoje stare i nowe hasło w odpowiednie pola i naciśnij OK. Odtąd do zalogowania się do komputera lub przywrócenia zablokowanej sesji musisz używać nowego hasła. Twój identyfikator pozostał bez zmian.

Jak zakończyć sesję pracy (wylogować się)?

Możesz zakończyć pracę poprzez zamknięcie systemu Windows 95, zgodnie z zasadami Windows 95, tj. poprzez wykonanie opcji Zamknij system z menu Start. Jeśli chcesz zakończyć sesję pracy bez zamykania systemu (ponieważ np. z komputera chce skorzystać inny użytkownik), to kliknij prawym klawiszem myszy na logo MERGENT-a na pasku zadań (czerwony trójkąt) i wybierz opcję Logoff Now z menu, które się pojawi.

Jak uzyskać pomoc?

Aby uzyskać pomoc w razie pytań lub problemów związanych z zainstalowaniem systemu bezpieczeństwa na twoim komputerze, skontaktuj się z administratorem. Dla ułatwienia, zanotuj sobie poniżej informacje, z kim należy się kontaktować:

Administrator:	
Telefon:	
Nr pokoju:	

Notatki:

VIII - Przygotowanie Windows 95

Przed przystąpieniem do instalacji PC/DACS for Windows 95 powinieneś sprawdzić niektóre opcje konfiguracyjne Windows 95.

Profile użytkowników

Windows 95 pozwala na skonfigurowanie komputera do jego użytkowania przez wielu użytkowników. Każdy z użytkowników może mieć własne ustawienia pulpitu. W przypadku konfiguracji z wieloma użytkownikami, Windows 95 zachowuje ustawienia pulpitu dla wszystkich użytkowników w profilu użytkownika. Aby przekonać się, jak skonfigurowany jest twój system, uruchom Panel Sterowania, w nim opcję Hasła, a w niej kliknij zakładkę Profile użytkownika. Jeśli wybrany jest guzik Użytkownicy mogą dostosować preferencje ..., to Windows 95 stworzy profil dla każdego użytkownika, który loguje się do Windows 95. Opcje Ustawienia profilu użytkownika pozwalają na dostosowanie pulpitu do własnych preferencji.

Aby przekonać się, czy twój komputer skonfigurowany jest do pracy z wieloma użytkownikami, możesz tez otworzyć Eksplorator i sprawdzić, czy istnieje podkatalog Profiles w katalogu Windows. Jeśli go nie ma, to twój komputer skonfigurowany jest do pracy z jednym użytkownikiem i możesz od razu przystąpić do instalacji PC/DACS.

Jeśli twój komputer jest skonfigurowany do pracy z wieloma użytkownikami, to aby zachować jednokrotne logowanie się, w PC/DACS będziesz musiał stworzyć użytkowników o identyfikatorach odpowiadających tym zdefiniowanym w Panelu Sterowania Windows 95. Zaleca się aby potem użytkownicy zsynchronizowali swoje hasła do pulpitu z hasłami do PC/DACS for Windows 95 poprzez zakładkę Zmień hasło opcji Hasła Panelu Sterowania.

IX - Synchronizacja haseł - uwagi wstępne

Synchronizacja hasła PC/DACS i hasła do pulpitu Windows

Sekwencja zmiany hasła przekazania (jednokrotnego hasła nadawanego przez administratora nowemu użytkownikowi) pozwala użytkownikowi od razu zsynchronizować jego hasło PC/DACS z hasłem do pulpitu Windows. Dzięki temu PC/DACS będzie mógł podawać automatycznie hasło użytkownika "dalej" do pulpitu i użytkownik będzie musiał logować się tylko raz, do PC/DACS. Pierwsze logowanie użytkownika, z jego hasłem przekazania, będzie składać się z następujących kroków:

1. Po pojawieniu się okna logującego PC/DACS użytkownik musi wprowadzić tam swój identyfikator i hasło przekazania, otrzymane od administratora, a następnie nacisnąć guzik Logon.
2. Po (opcjonalnym) pojawieniu się informacji o ostatnim logowaniu i usunięciu jej z ekranu poprzez naciśnięcie OK, użytkownik widzi okno dialogowe, w którym proszony jest o wpisanie swojego identyfikatora i hasła do pulpitu Windows 95. (PC/DACS zachowuje te informacje w swoiej bazie bezpieczeństwa. PC/DACS automatycznie poda te informacje "dalej" do pulpitu Windows 95 wtedy, gdy będzie to konieczne.)
3. Następnie Windows 95 poprosi o potwierdzenie hasła do pulpitu, jeśli jest to nowo zdefiniowany użytkownik pulpitu. Należy potwierdzić hasło do pulpitu poprzez jego ponowne wpisanie i naciśnięcie OK na tym oknie. (W zależności od konfiguracji sieci, użytkownik może być w tym momencie poproszony o zalogowanie się do domyślnej sieci.)
4. Po wykonaniu powyższych czynności PC/DACS wymusza na użytkowniku dokonanie zmiany jednorazowego hasła przekazania na nowe hasło. Należy wpisać swoje nowe hasło do PC/DACS. Powinno ono być takie samo, jak hasło do Windows 95. Należy je wpisać w obu polach i nacisnąć OK. Oczywiście nowe hasło do PC/DACS musi być zgodne z zasadami definiowania haseł, określonymi przez administratora. Jeśli PC/DACS zaakceptuje nowe hasło, proces logowania jest zakończony i pulpit Windows 95 staje się dostępny. Jeśli hasło nie zostało zaakceptowane, użytkownik zostanie poproszony o jego ponowne wybranie. **Jeśli hasło do PC/DACS jest zgodne z hasłem do pulpitu Windows 95, PC/DACS doda opcję "PC/DACS Logon" do opcji Hasła/Zmień inne hasła w Panelu Sterowania i hasło PC/DACS pozostanie zsynchronizowane z hasłem do pulpitu Windows 95.**

X - Wymagania sprzętowe i programowe

Aby móc używać PC/DACS for Windows 95, musisz mieć:
- komputer PC z procesorem 386DX lub nowszym,
- 6 MB RAM (zalecane 8 MB),
- kartę graficzną VGA lub lepszą,
- Windows 95,
- minimum 12 MB wolnej przestrzeni dyskowej.

Twój komputer musi dodatkowo spełniać wszystkie wymagania do prawidłowego działania Windows 95. Aby to zweryfikować, zapoznaj się ze swoją dokumentacją do Windows 95.

UWAGA! SAFE COMPUTING nie będzie udzielać pomocy technicznej użytkownikom, którzy zainstalowali PC/DACS for Windows 95 na komputerach nie spełniających powyższych wymagań.

XI - Jak to działa?

PC/DACS został skonstruowany tak, aby zapewnić skuteczną ochronę komputera bez wpływania na produktywność użytkowników komputera. Za pomocą PC/DACS możesz m. in.:

- kontrolować dla dowolnego użytkownika w dowolny sposób (odczyt, zapis itp.) dostęp do dowolnego foldera lub pliku w komputerze,
- grupować użytkowników i przypisywać im tzw. role, a następnie nadawać uprawnienia grupowo (rolom, a nie użytkownikom),
- grupować prawa i zasady dostępu w tzw. widoki, a następnie przypisywać użytkownikom i rolom widoki, a nie indywidualne prawa,
- prowadzić pełny dziennik działań (audyt) użytkowników i administratora,
- ustalić składnię i zasady zarządzania hasłami dostępu,
- użyć szyfrowania zasobów, aby zaszyfrować wskazane foldery lub dyski i chronić w nich poufne informacje,
- użyć blokady twardego dysku, aby uniemożliwić dostęp do komputera po starcie dyskietki i ew. zaszyfrować twardy dysk na niskim poziomie,
- ustalić dla użytkowników i ról dozwolone godziny i dni korzystania z komputera,
- użyć funkcji Time Out, aby zabezpieczyć komputery opuszczone przez użytkowników,
- użyć zaufanych aplikacji, aby przydzielić użytkownikom szerszy dostęp do zasobów tylko podczas pracy z dana aplikacją (np. backup),
- wyświetlić w oknie logującym PC/DACS dowolny tekst (np. ostrzeżenie o wyciągnięciu konsekwencji z prób nieautoryzowanego korzystania z komputera).

Użytkownicy, role i widoki tworzone podczas instalacji

UWAGA.

- Przez rolę rozumie się grupę użytkowników z tymi samymi uprawnieniami.
- Przez widok rozumie się nazwany zestaw praw dostępu do zasobów (listę zasad dostępu).

Podczas instalacji PC/DACS tworzy przede wszystkim konto administratora głównego z nieograniczonymi prawami. Dodatkowo, tworzone są dwa widoki: CONFIG CONTROL oraz SYSVIEW. Tworzone są też trzy role: Administrator, Support oraz User. Dodawany jest też jeden użytkownik specjalny, $LOGOFF.

Widok CONFIG CONTROL

Widok ten zezwala (użytkownikom i rolom, do których jest przypisany) na dostęp minimalny wystarczający na uruchomienie Windows 95 i PC/DACS. CONFIG CONTROL jest widokiem specjalnym, który jest przypisywany od razu wszystkim użytkownikom systemu.

Widok SYSVIEW

Widok ten zezwala na pełny dostęp do wszystkich folderów i plików w komputerze. Różnica pomiędzy prawami użytkownika z rolą Administrator a widokiem SYSVIEW polega na tym, że SYSVIEW nie daje możliwości konfigurowania PC/DACS ani jego deinstalacji.

Rola Administrator

Administrator jest rolą z pełnym dostępem do komputera i PC/DACS wraz z możliwością jego deinstalacji.

Rola SUPPORT

SUPPORT (Pomoc techniczna) jest rolą z pełnym systemowym dostępem do komputera. Funkcja Time Out jest ustawiona na 5 minut, czas logowania do systemu jest dowolny. Użytkownicy pełniący rolę SUPPORT mają pełne prawa instalacji, deinstalacji i aktualizacji PC/DACS.

Rola USER

User (użytkownik) jest rolą z domyślnie najmniejszymi uprawnieniami. Administrator może nadać tej roli większe uprawnienia w miarę potrzeb.

Prawo FCA (Full Configuration Access)

Jeśli przypiszesz prawo FCA (Pełne prawa konfiguracyjne) użytkownikowi, będzie miał on pełny dostęp do wszystkich plików systemowych Windows 95 i PC/DACS, z możliwością ich modyfikacji. Bez tego prawa, użytkownik jest ograniczony widokiem CONFIG CONTROL. (Prawo FCA można przypisać roli lub użytkownikowi w zakładce Access Control.)

Prawo FSA (Full System Access)
Jeśli przypiszesz prawo FSA (Pełny dostęp do systemu) użytkownikowi, będzie on miał nieograniczony dostęp do "nie-konfiguracyjnych" obszarów dysku. Bez tego prawa, użytkownik jest ograniczony prawami określonymi w widokach przypisanych temu użytkownikowi.

Uzytkownik specjalny $LOGOFF

PC/DACS używa użytkownika specjalnego $LOGOFF dla wszystkich działań i zdarzeń, które są wykonywane w systemie, gdy system jest aktywny, a nikt nie jest zalogowany (tzw. stan wylogowania). Np. wszystkie programy, które chcesz uruchomić przez opcję Run Services w Regedit muszą mieć wszystkie wystarczające prawa przypisane użytkownikowi $LOGOFF. Przykładem takiego programu może być program antywirusowy. Jeśli nie ustalisz dla niego odpowiednich praw (przypisując je do użytkownika $LOGOFF), to skaner ten nie uruchomi się, ponieważ nie będzie mógł odnaleźć swoich modułów, ponieważ PC/DACS nie zezwoli na dostęp do nich. W takiej sytuacji musisz nadać odpowiednie prawa użytkownikowi $LOGOFF. Pamiętaj jednak, że zmiany wprowadzone w konfiguracji użytkownika $LOGOFF stają się efektywne dopiero po restarcie systemu.

Hierarchia zasad dostępu

Hierarchia zasad dostępu PC/DACS mówi, że im bardziej specyficzna (przypisana konkretnemu użytkownikowi, roli) jest zasada dostępu, tym ma ona wyższy priorytet. Innymi słowy, w danym momencie dla danego zasobu stosowana będzie zasada dostępu najbardziej

bezpośrednio zastosowana. Załóżmy przykładowo, że PC/DACS został skonfigurowany tak, że żaden użytkownik nie może mieć dostępu do CONFIG.SYS. W późniejszym okresie dodawany jest jednak jakiś użytkownik, dla którego dostęp ten ma być zapewniony. W związku z tym przypisujesz dostęp do CONFIG.SYS tylko temu użytkownikowi. Następuje nałożenie praw domyślnych i nowo nadanego prawa, które spowoduje udostępnienie pliku CONFIG.SYS temu użytkownikowi, ponieważ konkretne prawo przypisane bezpośrednio użytkownikowi stoi wyżej w hierarchii niż prawa domyślne (grupowe).

Zasady dostępu przypisane bezpośrednio roli są ważniejsze niż zasady dziedziczone z widoku przypisanego tej roli. Zasady dostępu przypisane bezpośrednio do danego widoku użytkownika są ważniejsze niż zasady dziedziczone z roli tego użytkownika. Zasady dostępu przypisane bezpośrednio do użytkownika sa ważniejsze niż zasady dostępu dziedziczone z danego widoku użytkownika.

Przykład. Widok CONFIG CONTROL uniemożliwia dostęp do pliku C:\CONFIG.SYS. Jeśli jednak nadasz uprawnienia do tego pliku gdziekolwiek w PC/DACS, to uprawnienia te staną są ważniejsze niż uprawnienia z widoku CONFIG CONTROL.

Przykład. Załóżmy, że do jakiejś roli przypisałeś jedynie uprawniania Read i Open do danego zasobu. Następnie definiujesz użytkownika pełniącego ta rolę i przypisujesz do tego konkretnego użytkownika szersze prawa do tego zasobu: Read, Open i Write. Ostatecznie uzytkownik ten będzie miał właśnie te, szersze prawa, ponieważ są one przypisane bezpośrednio do niego.

XII - Strategia implementacyjna - jak przystosować PC/DACS do potrzeb bezpieczeństwa twojej firmy?

Definiowanie celów firmy (dla których ma być stosowany PC/DACS)

Aby jak najlepiej wykorzystać system PC/DACS musisz precyzyjnie zdefiniować cele, jakim ma służyć w twojej firmie. Cele te można podzielić na trzy kategorie: bezpieczeństwo, produktywność i administracja. Po zdefiniowaniu tych celów będziesz mógł przygotować strategię implementacji PC/DACS w twojej firmie.

PC/DACS jest elastycznym narzędziem, które pozwala na całkowite dostosowanie go do specyficznych potrzeb twoiej firmy. Pozwala on na łatwą i efektywną implementację polityki bezpieczeństwa funkcjonującej w twojej firmie. Nawet jeśli używasz PC/DACS do zabezpieczenia jednego komputera, warto zastanowić się teraz i zdefiniować swoją politykę bezpieczeństwa.

Cele bezpieczeństwa

PC/DACS for Windows 95 może pomóc ci w realizacji następujących celów bezpieczeństwa:
- zapobieganie nieautoryzowanemu dostępowi do informacji,
- zapobieganie nieautoryzowanemu dostępowi do Rejestru Windows 95,
- zapobieganie nieautoryzowanemu przepływowi informacji przez dyskietki i porty komputera,
- zapobieganie nieautoryzowanej instalacji, kasowaniu, kopiowaniu i aktualizowaniu oprogramowania,
- ochrona przed wirusami komputerowymi,
- ograniczenie dostępu do komputera do określonych dni i godzin,
- zapewnienie poufności wymiany informacji poprzez zaszyfrowanie wszystkich informacji kopiowanych na dyskietkę i wysyłanych modemem czy pocztą elektroniczną,
- wyświetlenie w oknie logującym PC/DACS ostrzeżenia przed złamaniem prawa,
- ograniczenie prób nieuprawnionego zalogowania się,
- określenie zasad zarządzania i składni haseł dostępu.

Cele produktywności

PC/DACS for Windows 95 może pomóc ci w realizacji następujących celów produktywności:
- dystrybucja PC/DACS for Windows 95 poprzez sieć,
- wykonywanie przez zwykłych użytkowników zadań wymagających większych uprawnień (np. backup),
- wykonywanie przez zwykłych użytkowników aktualizacji oprogramowania,
- zezwolenie na dostęp do komputera na prawach gościa.

Cele administracyjne

PC/DACS for Windows 95 może pomóc ci w realizacji następujących celów administracyjnych:

- rejestracja i generacja raportu ze zdarzeń administracyjnych (dodawanie i usuwanie użytkowników, generacja dyskietek logujących itp.) i prób nieautoryzowanego ich wykonania,
- rejestracja i generacja raportu ze zdarzeń tzw. ogólnych (zalogowanie, wylogowanie itp.) i prób nieautoryzowanego ich wykonania,
- rejestracja i generacja raportu ze zdarzeń plikowych (operacje na plikach i portach) i prób nieautoryzowanego ich wykonania.

Określenie potrzeb administrowanej przez ciebie grupy komputerów

Zdefiniowanie populacji użytkowników i ich podział na role; pojęcie widoku

W twojej firmie jest wielu potencjalnych użytkowników komputerów chronionych przez PC/DACS. Użytkownicy ci maja różne potrzeby względem komputerów; muszą oni wykonywać swoje obowiązki służbowe. Są grupy użytkowników mające bardzo podobne potrzeby, a więc wymagające podobnych uprawnień. Najczęściej sa to użytkownicy pełniący te same funkcje, czyli role. Dla celów PC/DACS użytkowników o podobnych uprawnieniach grupuje się właśnie w role. Oczywiście zyskuje się dzięki temu łatwość administracji, ponieważ nie trzeba przypisywać praw indywidualnym użytkownikom, lecz grupowo rolom.

Każda rola wymaga pewnego zestawu uprawnień, aby praca użytkowników pełniących tą rolę (należących do tej grupy) była możliwa i produktywna. Zestawy uprawnień przypisywane rolom (i/lub użytkownikom) nazywa się widokami (View). Do roli (i/lub użytkownika) można przypisać jeden lub więcej widoków. Różne role mogą mieć przypisane te same widoki.

Zdefiniowanie hierarchii użytkowników

Jako administrator masz nieograniczony dostęp (do danych oraz administracyjny) do komputerów chronionych PC/DACS w twojej firmie. Jest on niezbędny do wykonywania czynności administracyjnych i kontrolnych. Przy dużej ilości komputerów być może będziesz chciał zdefiniować dodatkowego administratora, o mniejszych uprawnieniach, tak, aby mógł on widzieć i konfigurować innych użytkowników i ich uprawnienia, lecz nie twoje. Być może będzie też potrzeba, aby kierownicy działów mogli sprawdzić, którzy użytkownicy mają dostęp do komputerów działu, lecz aby ci użytkownicy nie mogli wiedzieć, jacy kierownicy mogą ich kontrolować i mieć dostęp do ich komputerów. Tak więc po zdefiniowaniu populacji użytkowników i podziału ich na role, zdefiniować można również hierarchię ról, której odzwierciedlenie znajduje się w bazie bezpieczeństwa PC/DACS.

Określenie polityki bezpieczeństwa do zastosowania w PC/DACS

Polityka bezpieczeństwa jest zestawem podstawowych praw, które stosują się do każdego użytkownika w firmie. Zasady te określają podstawy definiowania i zarządzania hasłami, dostępu do komputerów, blokady twardego dysku, blokady komputera (Time Out), szyfrowania i audytu. Poprzez wprowadzenie określonych zasad do opcji Organizational Security i Global Security PC/DACS for Windows 95, implementujesz politykę bezpieczeństwa w PC/DACS for Windows 95. Polityka ta będzie dotyczyć wszystkich użytkowników. Każdy nowo dodany uzytkownik będzie jej również podlegać.

Definiowanie widoków (Views)

Widoki są zestawami praw dostępu do określonych zasobów. Widoki można przypisywać użytkownikom lub rolom. Dzięki temu nie trzeba przypisywać tych samych praw za każdym razem grupie lub użytkownikowi. Kiedy tworzysz widoki weź pod uwagę, że możesz przypisać więcej niż jeden widok użytkownikowi lub roli. Tak więc warto utworzyć różne widoki dla różnych aplikacji (np. Dostęp do Worda, Dostęp do Nortona itp.). Poprzez tworzenie różnych widoków możesz przypisać wspólny zestaw praw wielu różnym typom użytkowników. Rola może mieć przypisane wiele widoków; dzięki temu wszyscy użytkownicy przypisani do tej roli będą mieć uprawnienia zapisane w tych widokach.

Definiowanie ról (Roles)

Role są to grupy użytkowników odróżniane od siebie poprzez różne zestawy uprawnień im przypisane. Uprawnienia te są niezbędne użytkownikom przypisanym do roli w celu wykonania ich obowiązków służbowych. Ogólnie można powiedzieć, że role odpowiadają stanowiskom pracy (lub działom) i/lub funkcjom w hierarchii służbowej. Żądane uprawnienia przypisuje się do ról poprzez przypisanie im niezbędnych widoków.

Definiowanie zaufanych aplikacji

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Definiowanie użytkowników

Do definiowania użytkowników powinieneś przystąpić dopiero po zdefiniowania globalnych parametrów bezpieczeństwa, widoków, ról i ew. zaufanych aplikacji. Wtedy dodawanie nowych użytkowników do systemu będzie zadaniem bardzo prostym. Dodając użytkownika, przypisujesz mu od razu rolę, którą pełni. Automatycznie otrzymuje on wtedy zestaw uprawnień niezbędny do wykonywania jego zadań służbowych. Jeśli istnieje taka potrzeba, możesz dodać mu indywidualne uprawnienia, lub ograniczyć prawa wynikające z jego roli. Możesz także nadać mu indywidualne prawa do zaufanych aplikacji. Ten, jak i każdy następny uzytkownik będzie podlegał polityce bezpieczeństwa stworzonej i zaimplementowanej w PC/DACS.

XIII - Efektywne wykorzystanie PC/DACS (kroki implementacyjne)

Zanim rozpoczniesz instalację, zapoznaj się z poniższymi krokami, które zapewnią ci efektywne wykorzystanie PC/DACS w twojej firmie oraz oszczędzą twój czas jako administratora.

Po dokonaniu instalacji, PC/DACS powinien być konfigurowany w następującej kolejności:

1. **Ustalenie i wprowadzenie polityki bezpieczeństwa.** Globalne parametry bezpieczeństwa powinny być wprowadzone przed dodawaniem jakichkolwiek użytkowników, ról, czy widoków. Parametry sekcji Organizational Security powinny być definiowane przed parametrami Global Security.
2. **Utworzenie widoków.** Widoki są zestawami praw do zasobów. Użytkownicy, którzy nie mają praw do zasobów, nie widzą tych zasobów. Widoki znacznie ułatwiają administrację, a więc powinieneś kłaść nacisk na tworzenie widoków i przypisywanie ich użytkownikom i rolom, a nie na indywidualne przypisywanie praw użytkownikom. W zależności od potrzeb możesz stworzyć dowolną liczbę widoków dla danego komputera.
3. **Utworzenie ról.** Role określają typ użytkownika (grupują użytkowników). Użytkownicy przypisani do roli mają ten sam zestaw podstawowych uprawnień. Do roli przypisywane są widoki. Widoki te określają uprawnienia użytkowników pełniących ta rolę.
4. **Utworzenie zaufanych aplikacji.**
   (Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)
5. **Dodawanie użytkowników.** Podkreślmy, że dodawanie użytkowników jest ostatnim, a nie pierwszym krokiem implementacyjnym podczas konfigurowania PC/DACS. Dodając użytkownika w tym momencie możesz bowiem natychmiast nadać mu wszelkie niezbędne uprawnienia, po prostu przypisując go do danej roli.

Rozdział 1 - Instalacja PC/DACS for Windows 95

- Zanim rozpoczniesz instalację, upewnij się, że spełnione są wymagania programowe i sprzętowe wymienione na poprzedniej stronie.
- Wykonaj też kopie zapasowe dyskietek instalacyjnych PC/DACS for Windows 95 i schowaj je w bezpieczne miejsce.
- Podane niżej kroki instalacyjne zakładają, że znasz Windows 95.

Podstawowa procedura instalacji PC/DACS for Windows 95

1. Naciśnij guzik Start.
2. Wybierz Ustawienia.
3. Wybierz Panel Sterowania.
4. Uruchom opcję Dodaj/Usuń Programy.
5. W oknie Właściwości: Dodaj/Usuń Programy wciśnij guzik Instaluj. Włóż do stacji dyskietek dyskietkę PC/DACS for Windows 95 Disk 1 - Setup.
6. W oknie Instaluj program z dyskietki lub dysku CD-ROM naciśnij guzik Dalej. Pojawi się pierwsze okno instalacji PC/DACS for Windows 95 z informacją o wersji PC/DACS for Windows 95.
7. Naciśnij guzik Dalej. Pojawi się okno z licencją oprogramowania.
8. Naciśnij guzik Tak, jeśli zgadzasz się z warunkami licencji. Pojawi się okno Choose Destinaton Location. Okno to pozwala na wybranie dysku docelowego, na którym będzie zainstalowany PC/DACS. Jeśli masz tylko jeden dysk twardy, PC/DACS poinformuje cię, że wybrał go jako domyślny. Naciśnij OK, aby zaakceptować wybór dysku domyślnego.
9. Naciśnij guzik Dalej. Pojawi się okno Setup Type (Rodzaj instalacji). Możesz wybrać jeden z trzech rodzajów instalacji:

- Typical (Typowy) - program zostanie zainstalowany ze wszystkimi opcjami. Dla większości użytkowników zaleca się ten typ instalacji.
- Compact (Ograniczony) - program zostanie zainstalowany wyłącznie z funkcją kontroli dostępu do komputera (logowania się) i Time Out.
- Custom (Definiowalny) - program zostanie zainstalowany z opcjami wybranymi przez użytkownika. Ta opcja zalecana jest wyłącznie dla osób dobrze znających PC/DACS for Windows 95.

10. Wybierz rodzaj instalacji i naciśnij guzik Dalej. Pojawi się okno Drive Table (Tablicy dysków). Jest to lista urządzeń dyskowych wykrytych przez PC/DACS. Na podstawie tej listy PC/DACS będzie implementować mechanizmy kontroli dostępu (jeśli na tej liście nie ma dysku, który chcesz chronić - np. dysku wyjmowalnego - to musisz go dodać, by był chroniony). Możesz dodać dysk do tablicy dysków używając guzika Add; możesz zmienić rodzaj dysku guzikiem Change możesz też usunąć dysk z tablicy dysków PC/DACS guzikiem Delete. (Konfiguracja tablicy dysków jest również dostępna z poziomu programu administracyjnego PC/DACS.)
11. Jeśli zawartość tablicy dysków jest właściwa, naciśnij guzik Dalej. Pojawi się okno Select Database Option (Wybór opcji dla bazy bezpieczeństwa). Okno to pozwala ci na wybranie w jaki sposób zostanie utworzona baza bezpieczeństwa PC/DACS (zestaw informacji o prawach i profilach użytkowników i systemu), Możesz:

- utworzyć nową bazę bezpieczeństwa PC/DACS (Generate a new PC/DACS database) - wybierz tą opcję, jeśli instalujesz PC/DACS po raz pierwszy na tym komputerze,

- użyć istniejącej bazy bezpieczeństwa PC/DACS (Use an existing PC/DACS database) - wybierz tą opcję, jeśli masz do dyspozycji gotową, prekonfigurowaną bazę bezpieczeństwa PC/DACS for Windows 95,
- zaimportować bazę bezpieczeństwa z PC/DACS 3.x (Migrate PC/DACS 3.x database) - wybierz tą opcję, jeśli masz do dyspozycji przygotowaną do importu (uprzednio wyeksportowaną) bazę bezpieczeństwa systemu PC/DACS for DOS/Windows.

Dla większości użytkowników zalecana jest opcja pierwsza, wybrana domyślnie.

12. Po wybraniu żądanej opcji dotyczącej bazy bezpieczeństwa PC/DACS, wciśnij guzik Dalej. Jeśli wybrałeś jakąkolwiek opcję wymagająca użycia istniejącej bazy bezpieczeństwa, to będziesz musiał wskazać jej lokalizację. Po jej wskazaniu (lub od razu po wybraniu pierwszej, domyślnej opcji) ukaże się okno Administrator Information, w którym zdefiniujesz identyfikator i hasło głównego administratora tego komputera.
13. W polu User ID wpisz identyfikator administratora (będzie to najprawdopodobniej jednocześnie twój identyfikator), w polu Password hasło, a polu Name swoje imię i nazwisko. Po wpisaniu wymaganych informacji, wciśnij guzik Dalej. Pojawi się okno weryfikacji hasła głównego administratora.
14. Wpisz ponownie swoje hasło i wciśnij guzik Dalej. Ukaże się okno Logon/Time Out Scheme (wyboru schematu logowania). Do dyspozycji masz dwie (lub trzy - patrz niżej) opcje. Możesz wybrać wszystkie trzy na raz. Oto dostępne opcje:

- PC/DACS Logon/Time Out Dialogs - standardowe logowanie do PC/DACS za pomocą identyfikatora i hasła,
- SecurID Logon/TIme Out dialogs - logowanie za pomocą systemu SecurID (oddzielny produkt innego dostawcy, z którym MERGENT zapewnia kompatybilność); opcji tej należy używać, gdy wraz z PC/DACS na komputerze zainstalowany jest system SecurID,
- Challenge/Response Dialogs - logowanie awaryjne za pomocą schematu challenge-response (wyzwanie-odpowiedź); opcji tej należy użyć, aby zapewnić użytkownikom możliwość logowania się w sytuacjach awaryjnych (np. gdy zapomnieli hasła).

15. Wybierz żądane schematy logowania (**dla większości użytkowników zalecane jest zaznaczenie opcji pierwszej i trzeciej**).
16. Wciśnij guzik Dalej. Pojawi się okno Current Settings (bieżące ustawienia), w którym program instalacyjny informuje o wybranych przez ciebie opcjach, z którymi zostanie zainstalowany PC/DACS for Windows 95.
17. Jeśli ustawienia te odpowiadają ci, wciśnij guzik Dalej. Rozpocznie się instalacja PC/DACS for Windows 95.
18. Podczas dalszej części procesu instalacji postępuj zgodnie z instrukcjami na ekranie. Będziesz proszony o wkładanie do stacji kolejnych dyskietek.
19. Na zakończenie instalacji zostaniesz poproszony o wyjęcie ostatniej dyskietki ze stacji, po czym nastąpi restart komputera.
20. Po zrestartowaniu komputera ukaże się okno logujące PC/DACS. Zaloguj się do PC/DACS swoim identyfikatorem i hasłem (głównego administratora), zdefiniowanym podczas instalacji.

UWAGA.

- **Po zakończeniu instalacji moduł blokady twardego dysku jest zainstalowany, lecz nie włączony. Aby w pełni chronić komputer (uniemożliwić dostęp do twardego dysku po starcie z dyskietki, zaszyfrować twardy dysk) należy włączyć blokadę twardego dysku. Włączanie blokady twardego dysku opisane jest w rozdziale Globalne parametry bezpieczeństwa.**

- **Jeśli jednak planujesz jedynie zapoznanie się z możliwościami PC/DACS i administracją tym systemem, to jest to w pełni wykonalne bez konieczności włączania blokady twardego dysku.**

Alternatywna procedura instalacji PC/DACS for Windows 95

Instalacja poprzez opcję Uruchom.
1. Włóż do stacji dyskietkę PC/DACS for Windows 95 Disk 1 - Setup.
2. Kliknij guzik Start.
3. Wybierz opcję Uruchom.
4. W polu Otwórz wpisz `A:SETUP` i naciśnij guzik OK. Postępuj daje zgodnie z krokami 7 i dalszymi powyżej, aż do zakończenia instalacji poprzez restart komputera.

UWAGA.
- **Po zakończeniu instalacji moduł blokady twardego dysku jest zainstalowany, lecz nie włączony. Aby w pełni chronić komputer (uniemożliwić dostęp do twardego dysku po starcie z dyskietki, zaszyfrować twardy dysk) należy włączyć blokadę twardego dysku. Włączanie blokady twardego dysku opisane jest w rozdziale Globalne parametry bezpieczeństwa.**
- **Jeśli jednak planujesz jedynie zapoznanie się z możliwościami PC/DACS i administracją tym systemem, to jest to w pełni wykonalne bez konieczności włączania blokady twardego dysku.**

Jakie zmiany wprowadza PC/DACS for Windows 95 do pulpitu Windows 95?

Poprawej stronie na pasku zadań pojawia się logo firmy MERGENT - czerwony trójkącik. Służy on do logowania i wylogowywania się, włączania funkcji Time Out oraz do uruchamiania programu administracyjnego.

Jak wylogować się z systemu?

Procedury logowania i wylogowywania się są opisane w Rozdziale 9 - Logowanie i wylogowywanie się z PC/DACS.

Program administracyjny PC/DACS for Windows 95

System PC/DACS startuje wraz z system operacyjnym Windows 95 i od razu chroni Twój komputer. Zastosowane opcje ochrony są zależne od konfiguracji dokonanej przez administratora. Jako minimum, PC/DACS nie dopuszcza do użycia komputera bez zalogowania się, tj podania identyfikatora i hasła.

Interfejsem administratora PC/DACS jest moduł Standalone Administration Services (nazywany dalej programem administracyjnym PC/DACS). W tym programie ustala się wszelkie parametry bezpieczeństwa i uprawnienia dla użytkowników komputera chronionego przez PC/DACS. Program administracyjny PC/DACS możesz uruchomić na dwa sposoby:

Uruchamianie programu administracyjnego przez logo MERGENTa

1. Kliknij podwójnie na logo MERGENTa (czerwony trójkąt) po prawej stronie na pasku zadań. Pojawi się okno programu administracyjnego - Standalone Administration Services.

Uruchamianie programu administracyjnego przez menu Start

1. Kliknij guzik Start, potem opcję Programy. W liście programów znajdziesz PC/DACS for Windows 95.
2. Kliknij tą opcję, a potem wybierz i kliknij PC/DACS Administration. (Druga opcja - Audit Log Viewer - uruchamia moduł PC/DACS służący do przeglądania i drukowania dziennika działań użytkowników.)

Rozdział 2 - Globalne parametry bezpieczeństwa

Uwagi ogólne

- System PC/DACS chroni komputer zgodnie z parametrami ustalonymi przez administratora. Wszystkie zasady ochrony (zawarte w tzw. polityce bezpieczeństwa instytucji) muszą być prowadzone do bazy bezpieczeństwa PC/DACS (poprzez program administracyjny), aby stały się aktywne i skuteczne. Jest to zadanie administratora systemu.
- PC/DACS działa na zasadzie "co nie jest dozwolone, jest zabronione". Oznacza to, że każdy nowo zdefiniowany w systemie uzytkownik ma minimalne prawa, umożliwiające jedynie uruchomienie Windows 95 i PC/DACS. Dostęp do każdego potrzebnego mu zasobu jest nadawany przez administratora.
- W systemie PC/DACS rozróżnia się zasady obowiązujące wszystkich użytkowników (tzw. globalne) i dotyczące konkretnych użytkowników i grup.

Globalne parametry bezpieczeństwa - wprowadzenie

Globalne parametry bezpieczeństwa (GSP, Global Security Parameters), pozwalają na ustalenie podstawowych zasad bezpieczeństwa, dotyczących wszystkich administratorów, użytkowników, widoków i ról danego komputera (pojęcia widoku i roli zostaną wyjaśnione poniżej).

Globalne parametry bezpieczeństwa dzielą się na dwie grupy - Bezpieczeństwo organizacyjne (Organizational Security) i Bezpieczeństwo globalne (Global Security).

Parametry bezpieczeństwa organizacyjnego

Bezpieczeństwo organizacyjne określa wszelkie zasady definiowania i posługiwania się hasłami w instytucji (organizacji) oraz zasady rejestrowania czynności administracyjnych wykonanych przez administratora PC/DACS. Zasady definiowania haseł (ograniczenia - Password Restrictions - i wyłączenia - Exclusions) pozwalają na ścisłe zdefiniowanie, jak mogą wyglądać hasła definiowane i używane przez użytkowników (w systemie PC/DACS hasła użytkowników definiowane są przez nich samych). Gwarantuje to używanie haseł, które są bezpieczne, tj. trudne do odgadnięcia i złamania. Możesz także definiować minimalną i maksymalną długość hasła oraz okres ważności hasła, który wymusza jego cykliczne zmiany. Wszystkie te możliwości zapewniają bezpieczne środowisko pracy i skuteczną kontrolę dostępu. Poniżej opisane są dokładnie procedury modyfikacji parametrów bezpieczeństwa organizacyjnego.

Ekran parametrów bezpieczeństwa organizacyjnego

Aby dostać się do ekranu parametrów bezpieczeństwa organizacyjnego uruchom program administracyjny. Wybierz Organizational Security z menu Manage. Ukaże się okno Organizational Security. Okno to składa się z trzech zakładek. Poniżej objaśnione są zawartości tych zakładek.

Zakładka Password (Hasło)

UWAGA. PC/DACS dopuszcza spacje w hasłach.

Objaśnienia pól liczbowych:

- Number of Expired Passwords (liczba wygasłych haseł). Hasła, które wygasły, przechowywane są w liście wygasłych haseł. Kiedy użytkownik definiuje nowe hasło, PC/DACS sprawdza je z tą listą aby upewnić się, że nie używa on hasła już kiedyś użytego. To pole liczbowe pozwala na ustalenie ile wygasłych haseł PC/DACS będzie przechowywać. Możesz wprowadzić wartości od 0 do 12. Jeśli wprowadzisz 0, użytkownicy będą mogli wpisywać swoje stare hasło za każdym razem, gdy nastąpi wygaśnięcie hasła. Spowoduje to, że ich hasła będą mogły pozostać bez zmian.
- Number of Days to Expiration (liczba dni do wygaśnięcia). Pole to pozwala ustalić okres ważności hasła. Ustala się go w dniach, od 0 do 365 dni. Np. dzięki wpisaniu w tym polu 30, a w powyższym 12 hasło użytkownika będzie musiało ulec zmianie co miesiąc i nie powtórzy się w ciągu całego roku kalendarzowego.
- Minimum Length. Pole to pozwala ustalić minimalną długość hasła. Wartość domyślna: 5.
- Maximum Length. Pole to pozwala ustalić maksymalną długość hasła. Wartość domyślna: 15.

Objaśnienia pól wyboru:

- Allow Password same as User ID. Jeśli zaznaczysz to pole wyboru, hasła użytkowników będą mogły być takie same, jak ich identyfikatory. Pozostawienie tego pola wyboru pustego spowoduje, że hasła użytkowników będą musiały być różne od ich identyfikatorów.
- Allow Password as a Palindrome. Jeśli zaznaczysz to pole wyboru, hasła użytkowników będą mogły być palindromami, tj słowami czytanymi tak samo "do przodu", jak i "do tyłu". Pozostawienie tego pola wyboru pustego spowoduje, że hasła użytkowników nie będą mogły być palindromami.
- Allow Password as an Anagram of user ID. Jeśli zaznaczysz to pole wyboru, hasła użytkowników będą mgły być anagramami identyfikatorów użytkowników, tj składać się z tych samych znaków, co identyfikator, lecz przestawionych w dowolnej kolejności. Pozostawienie tego pola wyboru pustego spowoduje, że hasła użytkowników nie będą mogły być anagramami identyfikatorów.

Zakładka Restrictions/Exclusions (Ograniczenia/wyłączenia)

Zakładka ta pozwala zdefiniować składnię (maskę) hasła i wykluczyć wskazane konkretne słowa i maski z użycia jako hasła. Można np. zdefiniować, że hasła używane w instytucji muszą składać się z 3 cyfr, 3 liter i 2 znaków specjalnych w określonej kolejności oraz, że niedopuszczalne jest wybranie jako hasła słowa DACS oraz PC/DACS.

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Zakładka Audit Administration (Audyt czynności administracyjnych)

Zakładka ta pozwala na zdefiniowanie, jakie czynności administracyjne mają być rejestrowane w dzienniku działań (Audit Log). Pozwala to na śledzenie zmian w konfiguracji systemu bezpieczeństwa, dokonywanych przez administratora i uprawnionych użytkowników. Wystarczy zaznaczyć wybrane zdarzenia (te, które mają być rejestrowane), poprzez zaznaczenie pola wyboru przy nazwie zdarzenia.

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Parametry bezpieczeństwa globalnego

Parametry bezpieczeństwa globalnego pozwalają zdefiniować:
- tekst pojawiający się w oknie logowania PC/DACS,
- sposób reakcji systemu na próbę nieprawidłowego zalogowania się,
- które foldery mają być szyfrowane i w jaki sposób,
- parametry blokady twardego dysku, w tym szyfrowania dysku na niskim poziomie,
- parametry audytu (rejestracji) działań użytkowników.

Ekran parametrów bezpieczeństwa globalnego

Aby dostać się do ekranu parametrów bezpieczeństwa globalnego Uruchom program administracyjny. Wybierz Global Security z menu Manage. Ukaże się okno Global Security. Okno to składa się z ośmiu zakładek. Poniżej objaśnione są zawartości tych zakładek.

Zakładka System Access (Dostęp do systemu)

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Zakładka Personalization Text (Własny tekst na ekranie logującym)

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Zakładka Audit SecurID (Audyt systemu SecurID)

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Zakładka Audit File (Audyt operacji plikowych)

Zakładka ta pozwala na zdefiniowanie, jakie czynności administratorów i użytkowników na poziomie systemu operacyjnego i plików mają być rejestrowane przez system. Rejestrowane mogą być wszystkie operacje dotyczące plików i folderów oraz dostęp do portów COM i LPT. Dziennik działań użytkowników można potem przeglądać (wybiórczo lub w całości) za pomocą modułu Audit Log Viewer. Zakładka Audit File zawiera dokładną listę operacji (zdarzeń), które mogą być rejestrowane przez PC/DACS.

Wybór operacji plikowych do rejestracji w dzienniku

1. Kliknij zakładkę Audit File w oknie Global Security.
2. Zaznacz pola wyboru przy wszystkich zdarzeniach (kolumna Operations), które chcesz rejestrować. Jeśli chcesz rejestrować również próby wykonania operacji bez autoryzacji (próby pogwałcenia praw nadanych użytkownikom), zaznacz pola wyboru w kolumnie Violations przy wszystkich operacjach, których próby niedozwolonego wykonania chcesz rejestrować. Jeśli chcesz rejestrować wszystkie zdarzenia z tej zakładki, kliknij pole wyboru Audit All.
3. Kliknij OK, aby zakończyć wybór zdarzeń do rejestracji.

Zakładka Audit General (Audyt operacji podstawowych)

Zakładka Audit General pozwala na rejestrację logowania się użytkowników, wylogowywania się, zmiany haseł użytkowników i wywoływania funkcji Time Out. Kolumna Violations jest, jak wyżej, odpowiedzialna za próby wykonania tych operacji w sposób nieautoryzowany.

Wybór operacji podstawowych do rejestracji w dzienniku

1. Kliknij zakładkę Audit General w oknie Global Security.
2. Zaznacz pola wyboru przy wszystkich zdarzeniach (kolumna Operations), które chcesz rejestrować. Jeśli chcesz rejestrować również próby wykonania operacji bez autoryzacji (np. próby nieprawidłowego logowania się, próby pogwałcenia praw nadanych użytkownikom), zaznacz pola wyboru w kolumnie Violations przy wszystkich operacjach, których próby niedozwolonego wykonania chcesz rejestrować. Jeśli chcesz rejestrować wszystkie zdarzenia z tej zakładki, kliknij pole wyboru Audit All.
3. Kliknij OK, aby zakończyć wybór zdarzeń do rejestracji.

Zakładka Resource Encryption (Szyfrowanie zasobów)

PC/DACS pozwala na zdefiniowanie dowolnego dysku (w tym stacji dyskietek) oraz foldera (z lub bez podfolderów, ze wszystkimi plikami lub według maski) jako zasobu zaszyfrowanego. Pliki z zasobów zaszyfrowanych mogą być kopiowane na dyskietki w formie zaszyfrowanej; dzięki temu możesz chronić swoje kopie zapasowe, jak i wymieniać informacje z innymi użytkownikami PC/DACS bez obawy o utratę ich poufności.

Szyfrowanie zasobów jest jedną z dwu możliwości szyfrowania realizowanych przez PC/DACS. Druga to szyfrowanie całych dysków lub wybranych partycji na niskim poziomie. Szyfrowanie dysków realizowane jest przez moduł blokady twardego dysku (Boot Protection). Oba rodzaje szyfrowania mogą ze sobą współistnieć. Oznacza to, że dysk może być zaszyfrowany na niskim poziomie za pomocą modułu blokady twardego dysku, a jednocześnie dodatkowo zaszyfrowane mogą być wybrane foldery.

Szyfrowanie zasobów jest całkowicie przezroczyste dla autoryzowanego użytkownika. Może on nawet nie wiedzieć, że dany folder jest zaszyfrowany. PC/DACS deszyfruje informacje w momencie, gdy następuje jej odczyt z nośnika, i szyfruje ją ponownie, gdy dostęp do zasobu jest zakończony. Tak więc na nośniku magnetycznym informacja jest zawsze zaszyfrowana i bezpieczna. Takie szyfrowanie nazywa się też szyfrowaniem "w locie" lub on-line.

Zasoby, które mają być szyfrowane w locie, definiuje się przez zasady szyfrowania (Encryption rules). Zasady te określają sam zasób i sposób jego szyfrowania (np. klucz). Foldery, które mają być szyfrowane, muszą być puste w momencie definiowania ich jako zasobu zaszyfrowanego. Foldery, które mają być usunięte z listy zaszyfrowanych zasobów, muszą być przedtem opróżnione. Sposób i miejsce definiowania zasad szyfrowania omówione sa poniżej.

Używanie przełącznika szyfrowania (Resource Encryption Passthru)

Gdy plik jest przenoszony (lub kopiowany) przez autoryzowanego użytkownika z obszaru zaszyfrowanego do niezaszyfrowanego, następuje jego automatyczna deszyfracja, zgodnie z zasada działania szyfrowania on-line. Tzw. przełącznik szyfrowania pozwala na pozostawienie pliku w jego zaszyfrowanej postaci podczas przenoszenia (lub kopiowania) pliku z zasobu zaszyfrowanego do obszaru niezaszyfrowanego. Przełącznik szyfrowania może być szczególnie przydatny gdy trzeba np.:

- skopiować plik w zaszyfrowanej postaci na dyskietkę,
- skopiować plik w zaszyfrowanej postaci do katalogu poczty elektronicznej, skąd plik ten może być przesłany do odbiorcy bez obawy utraty jego poufności.

Używanie przełącznika szyfrowania z poziomu Eksploratora

Standardowo gdy korzystasz z Eksploratora i kopiujesz lub przenosisz plik z obszaru niezaszyfrowanego do obszaru zaszyfrowanego, PC/DACS automatycznie szyfruje plik. I podobnie, gdy Eksploratorem kopiujesz lub przenosisz plik z obszaru zaszyfrowanego do obszaru niezaszyfrowanego, PC/DACS automatycznie deszyfruje plik. PC/DACS dodaje do Eksploratora przełącznik szyfrowania, który pozwala ci kontrolować, czy przenoszony lub kopiowany plik ma być szyfrowany/deszyfrowany, czy nie. Aby użyć przełącznika szyfrowania z poziomu Eksploratora, użyj do kopiowania lub przeniesienia pliki prawego, zamiast lewego klawisza myszy. Gdy opuścisz plik, pojawi się menu z opcjami przełącznika szyfrowania. Wybierz żądana opcję i kliknij na niej myszą, a PC/DACS wykona operację zgodnie z niżej podanym opisem poszczególnych opcji (w danym momencie w menu wyświetlone będą tylko dwie z czterech opcji):

- Move No Encrypt Here (Przenieś tu bez szyfrowania) - przeniesienie pliku do zaszyfrowanego katalogu bez jego szyfrowania. Tą opcję musisz wybrać, gdy przenosisz do zaszyfrowanego katalogu plik, który jest już zaszyfrowany (ponieważ dwukrotne zaszyfrowanie pliku spowoduje, że stanie się on bezużyteczny),
- Copy No Encrypt Here (Kopiuj tu bez szyfrowania) - kopiowanie pliku do zaszyfrowanego katalogu bez jego szyfrowania. Tą opcję musisz wybrać, gdy kopiujesz do zaszyfrowanego katalogu plik, który jest już zaszyfrowany (ponieważ dwukrotne zaszyfrowanie pliku spowoduje, że stanie się on bezużyteczny),
- Move Encrypted Here (Przenieś tu zaszyfrowany) - przeniesienie pliku z zaszyfrowanego katalogu bez jego deszyfrowania (plik pozostaje w postaci zaszyfrowanej). Ta opcja jest przydatna, gdy istnieje potrzeba ochrony plików przenoszonych na inny dysk, dyskietkę, lub przesyłanych pocztą elektroniczną. Przeniesiony plik może być odczytany tylko przez użytkownika z tymi samymi zasadami szyfrowania.
- Copy Encrypted Here (Skopiuj tu zaszyfrowany) - skopiowanie pliku z zaszyfrowanego katalogu bez jego deszyfrowania (plik pozostaje w postaci zaszyfrowanej). Ta opcja jest przydatna, gdy istnieje potrzeba ochrony plików kopiowanych na inny dysk, dyskietkę,

lub przesyłanych pocztą elektroniczną. Skopiowany plik może być odczytany tylko przez użytkownika z tymi samymi zasadami szyfrowania.

Używanie przełącznika szyfrowania z poziomu linii komend

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Podgląd właściwości zaszyfrowanego pliku z poziomu Eksploratora

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Jak utworzyć zaszyfrowany katalog (zdefiniować zasady szyfrowania)?

UWAGA. Jeśli dysk, dla którego definiowana jest zasada szyfrowania, jest zdefiniowany jako "Use Volume Label" w oknie Manage Drives, to musi on być dostępny w momencie definiowania lub usuwania zasady szyfrowania. Problem ten dotyczy zwykle dysków wyjmowalnych (twardych, dyskietek).

1. W zakładce Resource Encryption wybierz folder do zaszyfrowania jedną z dwu poniższych metod:

- w liście Folders kliknij na znaku +, aby rozwinąć listę folderów dla danego dysku. Kliknij żądany katalog. Nie może on zawierać żadnych plików typu podanego w polu Expression (maska plików). Jeśli nie podajesz maski plików (pole Expression jest puste), PC/DACS przyjmuje domyślnie *.*. Jeśli zaznaczyłeś pole wyboru All Subdirectories (Wszystkie podkatalogi), to również żaden z podkatalogów nie może zawierać plików zdefiniowanych przez maskę Expression.
- w polu Folder Name wpisz nazwę żądanego katalogu. Katalog ten nie musi istnieć na dysku; jeśli go nie ma, zostanie utworzony przez PC/DACS. Jeśli wpisany katalog istnieje, to nie może on zawierać żadnych plików typu podanego w polu Expression (maska plików). Jeśli nie podajesz maski plików (pole Expression jest puste), PC/DACS przyjmuje domyślnie *.*. Jeśli zaznaczyłeś pole wyboru All Subdirectories (Wszystkie podkatalogi), to również żaden z podkatalogów nie może zawierać plików zdefiniowanych przez maskę Expression.

2. Algorytm i klucz szyfrujący. Przejdź do listy rozwijalnej Encryption Algorithm (algorytm szyfrowania) i wybierz żądany typ algorytmu. Dostępne są następujące algorytmy (opracowane przez firmę MERGENT):

- Standard - standardowy algorytm szyfrowania PC/DACS.
- Bi-Crypt 1 i 2 - algorytmy silniejsze (lecz wolniejsze) od algorytmu Standard,
- Tri-Crypt 1..4 - algorytmy najsilniejsze.
  Pole Key (Klucz) i uwagi dotyczące klucza szyfrującego. Jeśli wybierzesz algorytm Standard, pole Key może pozostać puste. Jeśli wybierzesz inny algorytm, musisz również zdefiniować klucz. Zdefiniowanie własnego klucza zapewni ci całkowitą prywatność - ktokolwiek, kto wszedłby w posiadanie twoich zaszyfrowanych informacji, musiałby nie tylko zastosować ten sam algorytm, ale również znać twój klucz. Dzięki możliwości wprowadzenia własnego klucza jest również możliwa bezpieczna wymiana informacji pomiędzy dwoma lub więcej użytkownikami, lub tworzenie zamkniętych grup użytkowników (w tym zamkniętego obiegu zaszyfrowanych dyskietek). Klucz wpisuje się jako ciąg znaków w pole Key; może on mieć od 1 do 16 znaków. Nie musisz

zapamiętywać swojego klucza, ponieważ nie będziesz go na codzień używać - szyfrowanie i deszyfracja odbywa się w locie.
3. Jeśli chcesz szyfrować również wszystkie podkatalogi katalogu wskazanego w Folder Name, kliknij pole wyboru All Subdirectories.
4. Po zakończeniu ustalania parametrów (zasady) szyfrowania, kliknij guzik Add, aby dodać zdefiniowaną zasadę szyfrowania do listy Encrypted Folders (zaszyfrowane foldery). (Jeśli zażądałeś użycia własnego klucza, zostaniesz poproszony o jego podanie.)
5. Powtórz kroki 1-4 dla każdego zasobu, który chcesz zaszyfrować. Na zakończenie definiowania zaszyfrowanych zasobów naciśnij OK.
6. Pojawi się informacja: "A logoff must occur before the resource encryption rules will take effect" (należy się wylogować, aby wprowadzone zasady szyfrowania zaczęły działać). Kliknij OK na oknie dialogowym i wyloguj się z PC/DACS, po czym zaloguj się ponownie.

Zakładka BP Encryption (Blokada twardego dysku)

Blokada twardego dysku (Boot Protection, w skrócie BP) jest bardzo ważnym modułem PC/DACS. Dzięki niej dostęp do twardego dysku (dysków) jest niemożliwy po starcie komputera z dyskietki. Daje ona też możliwość zaszyfrowania dysku na niskim poziomie.

Blokada twardego dysku nie jest włączona po instalacji PC/DACS. W celu uzyskania całkowitej ochrony komputera, należy ją włączyć. Sposób włączenia i konfiguracji blokady twardego dysku jest opisany poniżej.

Przed włączeniem blokady twardego dysku zaleca się sprawdzenie go narzędziem typu ScanDisk.

Jak włączyć i skonfigurować blokadę twardego dysku?

1. Wybierz Global Security z menu Manage.
2. Kliknij zakładkę BP Encryption. W głównym oknie zakładki ukaże się drzewo dysków twojego komputera. Każdy dysk fizyczny ukazany jest w nim jako korzeń; dla każdego logicznego dysku (partycji) odchodzą gałęzie. Każdy dysk logiczny jest oznaczony jako n:vvv sss, gdzie n jest literą dysku, vvv jego etykietą, a sss opisuje rozmiar partycji w MB.
3. Wybierz poprzez kliknięcie dysk, dla którego chcesz włączyć blokadę twardego dysku. Następnie kliknij pole wyboru Boot Protect, aby zabezpieczyć ten dysk.

- Blokadę twardego dysku włącza się dla dysków fizycznych. Szyfrowanie dysków włącza się dla partycji. W związku z tym, gdy poruszasz się po drzewie dysków, różne opcje kontrolne zakładki BP Encryption stają się dostępne lub zacienione.
- Pierwszy dysk fizyczny musi być zabezpieczony (blokada twardego dysku włączona) zanim zabezpieczane będą następne dyski. Zanim zaszyfrowana zostanie partycja na danym dysku, dysk ten musi być zabezpieczony (blokada twardego dysku włączona).

- Kiedy włączasz blokadę twardego dysku na twoim komputerze możesz i powinieneś stworzyć zapis (plik), zawierający informacje służące do odblokowania twojego komputera. Zapis ten nazywany jest WIF (Workstation Identification File - Plik

identyfikacyjny komputera). Zapis ten służy do odblokowania twardego dysku zarówno procedurą tzw. Internal - wewnętrzną (poprzez menu programu administracyjnego PC/DACS), jak i External - zewnętrzną. Procedury te są objaśnione w dalszych rozdziałach podręcznika. Plik WIF jest ściśle związany z danym komputerem i może służyć jedynie do odblokowania dysku w tym komputerze. Pamiętaj, aby dyskietkę WIF (dyskietkę zawierającą plik WIF) przechowywać w bezpiecznym miejscu, chronioną przed osobami niepowołanym!

4. Jeśli jeszcze nie zdefiniowałeś opcji dotyczących zewnętrznej metody wyłączania blokady twardego dysku (w tym dyskietki WIF), system przypomni ci o tym komunikatem. Kliknij Yes i zostaniesz automatycznie przeniesiony do zakładki BP External Unlock.

- PC/DACS oferuje dwa mechanizmy autoryzacji zewnętrznego zdejmowania blokady twardego dysku. Jest to dyskietka z plikiem WIF (opatrzonym ew. hasłem) oraz tzw. hasło odblokowania twardego dysku (Hard Drive External Unlock Password). Dyskietka WIF omówiona została wyżej. Hasło odblokowania twardego dysku jest to hasło zapisywane w postaci zaszyfrowanej bezpośrednio na twardy dysk. Wystarczy ono do przeprowadzenia procedury zewnętrznego odblokowania twardego dysku bez konieczności posiadania dyskietki WIF. **Zaleca się jednak stosowania dyskietki WIF dla pełnego bezpieczeństwa!**

5. Aby ustalić hasło odblokowania twardego dysku, kliknij pole wyboru Password Protect.
6. Kliknij guzik Set Password, aby ustalić hasło odblokowania twardego dysku dla tego komputera. Pojawi się ono dialogowe Set Password.
7. Wpisz wybrane przez siebie hasło w pole Password i potwierdź je w polu Retype. (Może to być dowolne hasło, nie musi być w żaden sposób związane z twoim hasłem logowania.) Hasło odblokowania zostanie zapisane na twardy dysk.

- UWAGA! Zapamiętaj podane hasło! Jeśli zdecydujesz się nie korzystać z dyskietki WIF, to jeśli zapomnisz hasła odblokowania, jedyne pozostałe metody zewnętrznego odblokowania twardego dysku to: procedura Challenge/Response (wyzwanie/odpowiedź) lub specjalna dyskietka odblokowująca (Master Unlock Disk). **Zaleca się więc stosowanie dyskietki WIF dla pełnego bezpieczeństwa!**

8. Kliknij OK, aby potwierdzić hasło.
9. Aby utworzyć dyskietkę WIF, zaznacz pole wyboru Create on BP/Encrypt.

- Możesz opcjonalnie dodać hasło do pliku WIF. W tym celu Kliknij guzik Set Password, aby ustalić hasło dla pliku WIF dla tego komputera. Pojawi się ono dialogowe Set Password. Wpisz wybrane przez siebie hasło w pole Password i potwierdź je w polu Retype. (Może to być dowolne hasło, nie musi być w żaden sposób związane z twoim hasłem logowania.) Hasło zostanie zapisane do pliku WIF na dyskietkę.
- UWAGA! Zapamiętaj podane hasło! Jeśli zapomnisz hasła do pliku WIF, jedyne pozostałe metody zewnętrznego odblokowania twardego dysku to: procedura Challenge/Response (wyzwanie/odpowiedź) lub specjalna dyskietka odblokowująca (Master Unlock Disk).

10. Wybierz dysk i ścieżkę dla pliku WIF. Może to być wyłącznie stacja dyskietek lub dysk sieciowy. (Najczęściej będzie to stacja A:.)
11. Włóż czystą, sformatowaną, niezabezpieczoną przed zapisem i sprawdzoną (nie zawierającą złych sektorów) dyskietkę do wybranej stacji dyskietek. W tym momencie zakończyłeś procedurę przygotowania do ew. zewnętrznego odblokowania twardego dysku. Jesteś gotowy do włączenia blokady twardego dysku.
12. Powróć do zakładki blokady twardego dysku (BP Encryption).
13. Wybierz myszą lub kursorem dysk, który chcesz zablokować i zaznacz odpowiadające mu pole wyboru Boot Protect (zablokuj dysk).
14. Ustal żądane opcje blokady twardego dysku, zgodnie z poniższym opisem.

Opcje szyfrowania (sekcja Encrypt)
Sekcja Encrypt (Szyfrowanie) pozwala na wybranie sposobu, w jaki ma być zaszyfrowany na niskim poziomie twardy dysk przez moduł blokady twardego dysku. Dopuszczalne opcje to:

- None (Brak) - brak szyfrowania, jedynie włączenie blokady twardego dysku (twardy dysk niewidoczny po starcie z dyskietki),
- System Area (Obszary systemowe) - zaszyfrowane zostaną obszary systemowe, tj. sektor startowy DOS, FAT i katalog główny.
- Partition (Partycja) - zaszyfrowane zostaną wskazane partycje. Zapobiega to próbom dostępu do informacji na niskim poziomie oraz utraty poufności informacji na danej partycji np. w przypadku kradzieży komputera, czy przekazania dysku do serwisu. Uniemożliwia też próby wyłączenia (obejścia) blokady twardego dysku poprzez użycie programów "ratujących" twardy dysk. Zaszyfrowana będzie cała zawartość partycji.
- Full Disk (Cały dysk) - zaszyfrowany zostanie cały fizyczny twardy dysk, niezależnie od jego podziału na partycje. Jest to najlepsze zabezpieczenie poufności informacji.

Opcje odtwarzania na wypadek awarii (lista rozwijalna Recovery)
Jeśli podczas szyfrowania wystąpi jakiś problem, np. awaria zasilania, wystąpić może ryzyko utraty danych. Jako administrator PC/DACS możesz jednak kontrolować stopień ryzyka związany z sytuacjami awaryjnymi podczas szyfrowania twardego dysku. Lista rozwijalna Recovery (odtwarzanie awaryjne) pozwala ci wybrać opcje odtworzenia danych na wypadek sytuacji awaryjnej. Dostępne sa następujące opcje odtwarzania:

- No Recovery (Brak odtwarzania) - włączenie tej opcji spowoduje aktualizowanie informacji o blokadzie twardego dysku dopiero na zakończenie procesu szyfrowania. W związku z tym w razie awarii możesz utracić wszystkie dane. Z drugiej strony jednak, wybranie tej opcji powoduje, że proces szyfrowania jest najszybszy.
- Normal (Zwykłe) - włączenie tej opcji spowoduje aktualizowanie informacji o blokadzie twardego dysku co 10 ścieżek podczas procesu szyfrowania. Dzięki temu w razie awarii stracisz tylko taką ilość ścieżek, która została zaszyfrowana od ostatniej aktualizacji.
- Best Recovery (Najdokładniejsze) - włączenie tej opcji spowoduje aktualizowanie informacji o blokadzie twardego dysku co 1 ścieżkę podczas procesu szyfrowania. Dzięki temu w razie awarii utracisz tylko 1 ścieżkę informacji. Z drugiej strony jednak, wybranie tej opcji powoduje, że proces szyfrowania jest najwolniejszy.

Przywrócenie wartości domyślnych (guzik Reset)
Wciśnięcie tego guzika spowoduje przywrócenie wszystkich zmian dokonanych w ustawieniach blokady twardego dysku. Operację tą należy potwierdzić wciskając guzik Yes na oknie dialogowym, które pojawi się po wciśnięciu guzika Reset.

15. Po wybraniu wszystkich żądanych opcji w zakładce BP Encryption, wciśnij guzik OK, aby rozpocząć proces włączania blokady twardego dysku (i ew. szyfrowania). Okno stanu wyświetlać będzie postęp tego procesu.
- Proces włączania blokady możesz przerwać, wciskając guzik Interrupt. Przerwanie procesu może być konieczne np. gdy wiadomo jest, że w niedługim czasie może nastąpić zanik lub awaria napięcia (burza, wyczerpywanie się baterii w notebooku itp.).
- **UWAGA! Nie próbuj przerywać procesu włączania blokady twardego dysku poprzez reset komputera!** Grozi to utratą danych.

16. Jeśli blokada twardego dysku nie była wcześniej włączana, twój komputer zostanie zrestartowany na zakończenie tego procesu.

Jak wyłączyć blokadę twardego dysku?

Istnieje wiele opcji wyłączania blokady twardego dysku. Są one opisane w Rozdziale 11.

Rozdział 3 - Widoki

Widoki są to (posiadające nazwy) zestawy praw do zasobów. Widoki ułatwiają administrację ponieważ pozwalają nadawać użytkownikom i rolom prawa grupowo (cały zestaw praw naraz), a nie pojedynczo. Aby widok stał się aktywny dla danego użytkownika czy roli, należy go do tej roli przypisać. (Widoków nie przypisuje się administratorom, ponieważ oni mają nieograniczony dostęp do komputera.)

Przykład. Można utworzyć widok o nazwie Dostęp do Worda, który będzie zawierać wszelkie niezbędne uprawnienia (zestaw praw) do uruchomienia i korzystania z tego edytora. Użytkownikom i rolom, które mają korzystać z Worda nie trzeba potem przydzielać indywidualnych (pojedynczych) praw, a wystarczy przypisać im ten widok.

Przykład. Załóżmy, ze w twojej firmie ABC użytkownicy mogą mieć pełny dostęp do zasobów komputera z wyjątkiem katalogu C:\KADRY. Aby zrealizować to założenie należy utworzyć widok np. o nazwie Dostęp w ABC. Widok ten powinien zawierać dwie zasady dostępu. Pierwsza z nich powinna zezwalać na pełny dostęp do całego twardego dysku (tj. C:\ *.* z podkatalogami plus zezwolenie na pełny dostęp). Druga z nich powinna odcinać dostęp do C:\KADRY (tj. C:\KADRY plus brak zezwolenia na jakikolwiek dostęp). Stworzenie takiego widoku i przypisanie go do odpowiednich ról (najprawdopodobniej do roli User) zrealizuje założoną zasadę bezpieczeństwa. Zwróć uwagę, że nadanie pełnych praw do twardego dysku nadal nie umożliwia modyfikacji plików konfiguracyjnych, ponieważ chronione są one domyślnym widokiem CONFIG CONTROL.

Tworzenie widoków

Podczas instalacji tworzony jest widok systemowy CONFIG CONTROL. Zawiera on prawa dostępu działające dla każdego użytkownika systemu, który nie ma przypisanego prawa FCA. Możesz modyfikować prawa widoku CONFIG CONTROL dla każdego widoku, który tworzysz, lub modyfikować sam widok CONFIG CONTROL. UWAGA. Nie możesz modyfikować systemowych zasad dostępu w tym widoku.

Gdy tworzysz nowy widok, w oknie View Properties (Właściwości widoku) w sekcji Rules masz do dyspozycji dwa pola wyboru: User i System. gdy tworzysz nowy widok, musisz wybrać pole wyboru User. Pole System jest bowiem używane tylko do przeglądania systemowych zasad dostępu zapisanych w widoku CONFIG CONTROL.

Przeglądanie zasad dostępu w widoku CONFIG CONTROL

1. W oknie administracyjnym PC/DACS naciśnij guzik View (Widok). Ukaże się lista widoków zdefiniowanych w systemie.
2. Kliknij podwójnie na widoku CONFIG CONTROL. Pojawi się okno właściwości tego widoku.
3. Kliknij pole wyboru System. Pojawi się lista systemowych zasad dostępu.

Tworzenie nowego widoku

1. W oknie administracyjnym PC/DACS naciśnij guzik View (Widok). Ukaże się lista widoków zdefiniowanych w systemie.
2. Z menu File wybierz opcję New. Pojawi się okno właściwości nowo definiowanego widoku.
3. Przejdź do pola Name i wpisz nazwę tworzonego widoku. Nazwa może zawierać spacje.
4. Teraz rozpoczniesz definiowanie listy zasad dostępu, które składać się będą na ten widok. Na początek rozwiń listę Drives (Dyski) i wybierz dysk, dla którego będziesz definiować zasadę dostępu.
5. Przejdź do listy Folders (Foldery) rozwiń drzewo folderów dla wybranego dysku. Kliknij folder, którego dotyczyć będzie aktualnie definiowana zasada dostępu.
6. W liście Files (Pliki) ukażą się pliki znajdujące się wybranym folderze. Możesz wybrać typ plików, które mają być pokazywane poprzez wybranie odpowiedniej opcji z listy rozwijalnej List Files of Type (Wyświetl pliki typu). Jeśli chcesz stworzyć widok dla foldera, wybierz All Files (wszystkie pliki). Jeśli chcesz dodać konkretne pliki, kliknij na wybranym folderze, a następnie na wybranym pliku w liście Files.
7. Kliknij podwójnie plik lub folder, którego ma dotyczyć zasada dostępu dodawana do widoku. Pojawi się okno dialogowe Rights (Prawa), zawierające wszystkie opcje dotyczące praw nadawanych wybranemu folderowi (lub plikowi).

- Zaznaczenie pola wyboru Read/Execute spowoduje nadanie prawa do odczytu/wykonania pliku/plików/foldera w podanej ścieżce.
- Zaznaczenie pola wyboru Write spowoduje nadanie prawa do zapisu do pliku/plików/foldera w podanej ścieżce.
- Zaznaczenie pola wyboru Search spowoduje nadanie prawa do przeglądania zawartości pliku/plików/foldera w podanej ścieżce.
- Zaznaczenie pola wyboru Open spowoduje nadanie prawa do otwierania pliku/plików/foldera w podanej ścieżce.
- Zaznaczenie pola wyboru Delete spowoduje nadanie prawa do kasowania pliku/plików/foldera w podanej ścieżce.
- Zaznaczenie pola wyboru Create spowoduje nadanie prawa do tworzenia pliku/plików/foldera w podanej ścieżce.
- Zaznaczenie pola wyboru Modify spowoduje nadanie prawa do modyfikacji nazwy i atrybutów pliku/plików/foldera w podanej ścieżce.
- Zaznaczenie pola wyboru Administrate spowoduje nadanie prawa do tworzenia i usuwania podfolderów w podanej ścieżce.
- Guziki znajdujące się po lewej stronie pól wyboru dotyczących praw ułatwiają nadawanie najczęściej stosowanych kombinacji praw. Naciśnięcie guzika All spowoduje nadanie pełnych praw.
- Naciśnięcie guzika None spowoduje usunięcie wszystkich praw.
- Naciśnięcie guzika ROS spowoduje nadanie praw do czytania, otwierania i przeglądania.
- Naciśnięcie guzika RWOS spowoduje nadanie praw do czytania, zapisywania, otwierania i przeglądania.

8. Jeśli nadawane przez ciebie prawa dotyczą katalogu, możesz dodatkowo zdecydować, czy mają one dotyczyć wszystkich plików w danym katalogu, czy wskazanej maski plików. W tym celu wybierz odpowiednią opcję w sekcji Expression (Maska plików): Defined Expression (Określona maska) lub All Files (Wszystkie pliki). Jeśli wybrałeś opcję Expression musisz wpisać maskę plików (np. *.doc, *. dbf) w polu tekstowym Expression.

9. Zdefiniowane przez ciebie dla danego foldera prawa możesz zastosować również do wszystkich podfolderów. W tym celu zaznacz pole wyboru All Directories (Wszystkie katalogi).
10. Po zakończaniu definiowania praw do wybranego zasobu, kliknij OK, aby powrócić do okna definicji widoku. Zdefiniowane przez ciebie prawa do danego zasobu pojawią się w liście Rules.
11. Jeśli chcesz dodawać następne zasoby wraz z prawami do tego widoku, wykonaj ponownie kroki 4-10. Po zakończeniu budowania listy zasobów i praw dla danego widoku możesz wcisnąć Another (Następny), aby zdefiniować następny widok, albo wcisnąć OK, aby zakończyć definiowanie widoku i powrócić do głównego okna administracyjnego. Zdefiniowany przez ciebie widok zostanie zachowany i będzie wyświetlany w liście widoków w głównym oknie administracyjnym. Możesz go od teraz przypisywać do ról i użytkowników.

Edycja widoku

1. W głównym oknie administracyjnym kliknij guzik View. Pojawi się lista widoków zdefiniowanych w systemie.
2. Kliknij podwójnie na widoku, który chcesz zmodyfikować. Pojawi się okno właściwości widoku. Lista Rules zawiera zasoby tego widoku i przypisane im prawa. (Podczas edycji guzik Another nie jest widoczny.)
3. Kliknij podwójnie na zasobie, który chcesz zmodyfikować, rozpocznij dopisywanie nowych zasobów do widoku zgodnie z opisaną wyżej procedurą (lub kliknij guzik Delete, aby usunąć zasób z widoku).
4. Po zakończeniu modyfikacji listy zasobów kliknij OK, aby powrócić do okna właściwości widoku.
5. Po zakończeniu modyfikacji widoku, kliknij OK w oknie właściwości widoku, aby zachować zmiany.

Rozdział 4 - Role

Wprowadzenie

Role odpowiadają grupom użytkowników o podobnych uprawnieniach. Każdy użytkownik systemu PC/DACS for Windows 95 musi być przypisany do roli. Jego rola będzie najczęściej wynikać z jego funkcji służbowej. Dzięki rolom istnieje możliwość łatwego, grupowego nadawania atrybutów użytkownikom. Jeśli atrybut nadany zostanie roli, to automatycznie otrzymują go wszyscy użytkownicy pełniący tą rolę.

Przykład. Załóżmy, że dla pracowników działu sprzedaży stworzona została w systemie PC/DACS for Windows 95 rola Handlowiec. Rola ta zawiera dostęp do wszelkich niezbędnych aplikacji i danych potrzebnych do racy handlowca w firmie, w tym np. do arkusza kalkulacyjnego, bazy danych i edytora tekstu. Kiedy do zespołu handlowców dołącza nowa osoba, nie ma potrzeby indywidualnego nadawania jej uprawnień do tych narzędzi pracy. Wystarczy, że administrator przypisze ją do roli Handlowiec, a uprawnienia zaczną działać automatycznie. Podobnie, gdy np. do użycia wejdzie oprogramowanie faksowe, nie ma potrzeby indywidualnego nadawania uprawnień do tego oprogramowania każdemu handlowcowi. Wystarczy, że uprawnienia te nada się roli Handlowiec (zalecaną metodą widoku), a wszyscy handlowcy automatycznie zyskają te uprawnienia.

Role zdefiniowane w systemie pojawiają się po naciśnięciu guzika Role w głównym oknie administracyjnym.

Praca z rolami

Jak dodać nową rolę?

1. Wciśnij guzik Role w głównym oknie administracyjnym. Pojawi się lista już utworzonych ról.
2. Wybierz New z menu File. Pojawi się okno właściwości roli (Role Properties).
3. Wpisz nazwę roli w polu Name. Wpisz opcjonalną datę ważności roli w polu Expiration Date.
4. Wciśnij guzik Security, aby przejść do profilu bezpieczeństwa roli i zmodyfikuj wszystkie żądane opcje bezpieczeństwa (rozłożone na zakładki opisane poniżej). Po zakończeniu wprowadzania modyfikacji wciśnij OK, aby powrócić do profilu bezpieczeństwa roli.
5. Kliknij guzik OK, aby dodać rolę do listy ról zdefiniowanych w systemie, lub wciśnij guzik Another (Następna), aby utworzyć następną rolę.

Jak zmodyfikować profil bezpieczeństwa istniejącej roli?

1. Wciśnij guzik Role w głównym oknie administracyjnym. Pojawi się lista już utworzonych ról.
2. Kliknij podwójnie na wybranej roli. Pojawi się okno właściwości roli (Role Properties).
3. Wciśnij guzik Security, aby przejść do profilu bezpieczeństwa roli i zmodyfikuj wszystkie żądane opcje bezpieczeństwa (rozłożone na zakładki opisane poniżej). Po zakończeniu wprowadzania modyfikacji wciśnij OK, aby powrócić do profilu bezpieczeństwa roli.
4. Kliknij guzik OK, aby zapamiętać modyfikacje wprowadzone do roli.

Blokowanie atrybutów bezpieczeństwa

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Zakładki profilu bezpieczeństwa

UWAGA.

- **Niżej opisane atrybuty definiuje się w sposób identyczny dla ról i użytkowników.**
- **Pamiętaj, że jeśli modyfikujesz którykolwiek z poniższych atrybutów dla roli, to zmiana ta dotyczyć będzie wszystkich użytkowników pełniących tą rolę.**
- **Jeśli natomiast modyfikujesz którykolwiek z poniższych atrybutów dla użytkownika (patrz rozdział dotyczący użytkowników), to zmiana ta dotyczyć będzie tylko tego użytkownika, którego profil bezpieczeństwa modyfikujesz.**

Zakładka Logon Times (Godziny pracy)

W zakładce tej definiuje się dopuszczalne dni i godziny logowania się użytkowników. Lista Allowed Logon zawiera dopuszczalne dni i godziny logowania się. Guziki Add, Change i Delete służą odpowiednio do dodawania, edycji i usuwania pozycji z listy Allowed Logon.

Zakładka Access Control (Kontrola dostępu)

W tej zakładce definiuje się różne atrybuty kontroli dostępu.

Grupa Sector Level I/O (Dostęp niskiego poziomu)

W tej grupie pól wyboru definiuje się sposób, w jaki PC/DACS obsługuje żądania obsługi przerwań dyskowych BIOS dla dysków z aktywną pełną kontrolą dostępu (parametry ochrony dysków modyfikuje się w oknie Manage Drives). Opcja ta zapobiega użyciu narzędzi typu Disk Editor czy Disk Doctor w celu obejścia PC/DACS. (Użytkownicy z atrybutem FSA mają pełne prawa do dostępu niskiego poziomu.) Dostępne są następujące opcje:

- Read (Odczyt) - bezpośredni dostęp do sektorów tylko do odczytu,
- All (Pełny) - bezpośredni dostęp do sektorów do odczytu i zapisu (zezwala również na formatowanie),
- None (Brak) - brak bezpośredniego dostępu do sektorów.

Grupa Floppy Access (Dostęp do dyskietek)

W tej grupie pól wyboru definiuje się dostęp do dysków z kontrolą dostępu na poziomie zapis/odczyt (generalnie są to dyskietki; parametry ochrony dysków modyfikuje się w oknie Manage Drives). Wymienione niżej dostępne opcje odnoszą się zarówno do dostępu na poziomie plików, jak i na poziomów sektorów:

- Read (Odczyt) - zezwala na odczyt ze stacji dyskietek,
- All (Pełny) - zezwala na odczyt i zapis na stację dyskietek,
- None (Brak) - opcja domyślna; uniemożliwia jakikolwiek dostęp do stacji dyskietek,

- Write (Zapis) - zezwala wyłącznie na zapis na stację dyskietek.

Grupa Port (Kontrola portów)

W tej grupie pól wyboru definiuje się prawa dostępu do portów LPT i COM komputera:
- Zaznaczenie pola wyboru przy żądanym porcie umożliwia dostęp do tego portu,
- Wyczyszczenie pola wyboru przy żądanym porcie blokuje dostęp do tego portu.

Dodatkowe opcje kontroli dostępu

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Zakładka Administration (Administracja)

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Zakładka Access Rules

Zakładka Access Rules umożliwia na bezpośrednie nadanie roli (lub użytkownikowi) praw dostępu do zasobów, bez konieczności stosowania widoków. Zanim przystąpisz do nadawania praw dostępu do zasobów bezpośrednio roli lub użytkownikowi, weź pod uwagę następujące zalecenia:
- zaleca się stosowanie widoków w celu nadawania uprawnień do zasobów; widoki znacznie ułatwiają administrację systemem i pozwalają na centralizację kontroli nad prawami dostępu,
- jeśli nie możesz lub nie chcesz korzystać z widoku, aby nadać żądane prawa dostępu, to zaleca się nadawanie ich rolom, a nie bezpośrednio użytkownikom.

Pola wyboru Attached oraz Inherited

Po prawej stronie listy Rules znajdują się dwa pola wyboru: Attached (Dołączone) i Inherited (Dziedziczone). Wybierz pole Attached, jeśli chcesz modyfikować zasady dostępu przypisane bezpośrednio do roli/użytkownika. Guzik Inherited dotyczy wyłącznie użytkowników. Wybierz Inherited, jeśli chcesz zobaczyć zasady dostępu dziedziczone przez użytkownika z jego roli.

Nadawanie roli/użytkownikowi praw do zasobów

Prawa dostępu nadaje się roli w identyczny sposób, jak przy tworzeniu widoku (patrz sekcja Tworzenie nowego widoku - listy Rules, Files, Folders, List File of Type i Drives są tam opisane).

Zakładka Virus (Ochrona antywirusowa)

PC/DACS potrafi aktywnie bronić się zarówno przed wirusami sektorów startowych, jak i przed wirusami plikowymi. (PC/DACS stosuje własne mechanizmy ochronne - nie jest skanerem antywirusowym, lecz może być używany w połączeniu z takim oprogramowaniem.) Zakładka Virus służy do konfiguracji ochrony przed wirusami plikowymi.

Wirusy plikowe atakują pliki wykonywalne. Zarażenie polega na uruchomieniu zawirusowanego programu - gdy kod wirusa w takim programie staje się aktywny, zaraża inne pliki poprzez skopiowanie się do nich. Wymagany jest więc zapis do pliku wykonywalnego. Dzięki pełnej kontroli, jaką daje PC/DACS nad systemem operacyjnym, istnieje możliwość zabezpieczenia plików o zdefiniowanych rozszerzeniach przed zapisem, co uniemożliwi ich zawirusowanie.

Ochrona antywirusowa PC/DACS działa na całym obszarze dysku dostępnym dla danego użytkownika/roli. Oznacza to, że nawet jeśli użytkownik ma do dyspozycji folder z plikami wykonywalnymi, do którego ma prawo zapisu, to jeśli ochrona antywirusowa jest aktywna, to wszystkie pliki wykonywalne (o zdefiniowanych rozszerzeniach) w tym katalogu będą zabezpieczone przed zapisem.

Jak zabezpieczyć określone typy plików przed wirusami (przed zapisem)?

1. W zakładce Virus zaznacz pole wyboru Enable Virus Prevention (włącz ochronę antywirusową).
2. Kliknij w pole Current; wpisz tam rozszerzenie plików, które chcesz chronić (np. DLL).
3. Naciśnij guzik Add. Wpisane przez ciebie rozszerzenie pojawi się w liście Extension List (Lista rozszerzeń). Pliki o rozszerzeniach wymienionych w tej liście będą chronione przed zapisem (dla danej roli/użytkownika).
4. Po zakończeniu tworzenia listy rozszerzeń chronionych pików, kliknij OK, aby zachować zmiany.

Jak usunąć zabezpieczenie przed zapisem z określonego typu plików?

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Jak zmienić wybrane rozszerzenie z listy rozszerzeń chronionych plików?

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Zakładka Installation (Instalacja)

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Zakładka Views (Widoki)

Zakładka Views służy do przypisywania widoków do roli/użytkownika. Przypisując widok do roli, nadajesz tej roli wszystkie uprawnienia do zasobów, które wynikają z przypisywanego widoku. Po wybraniu zakładki Views wyświetla się lista wszystkich widoków zdefiniowanych w systemie. Widoki wybrane (podświetlone) są aktywne.

Jak przypisać widok do roli/użytkownika?

1. W zakładce Views podświetl myszą wszystkie widoki, który chcesz przypisać do aktualnie modyfikowanej roli/użytkownika.
2. Naciśnij OK, aby zachować wprowadzone zmiany. Od momentu następnego zalogowania się użytkownika, wybrane przez ciebie widoki będą aktywne.

Jak usunąć przypisanie widoku do roli/użytkownika?

1. W zakładce Views usuń myszą podświetlenie wszystkich widoków, które chcesz "zdjąć" z aktualnie modyfikowanej roli/użytkownika.
2. Naciśnij OK, aby zachować wprowadzone zmiany. Od momentu następnego zalogowania się użytkownika aktywne będą już tylko te widoki, które pozostały podświetlone w liście widoków.

Rozdział 5 - Zaufane aplikacje

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Rozdział 6 - Użytkownicy

Uzytkownik jest osobą, której przydziela się dostęp do komputera chronionego przez PC/DACS. Dostęp przydzielany jest przez administratora; polega to na stworzeniu tzw. konta użytkownika w systemie.

Tworzenie użytkowników w systemie

Dodanie nowego użytkownika związane jest z przypisaniem go do roli. Nie można zdefiniować nowego użytkownika nie przypisując go do jednej z ról zdefiniowanych w systemie. Przypisanie użytkownika do roli powoduje automatyczne nadanie mu wszystkich uprawnień, ograniczeń i widoków przypisanych do tej roli. W dużej mierze to właśnie rola definiuje uprawnienia użytkownika. Jeśli istnieje potrzeba modyfikacji uprawnień wynikających z roli, to można tego dokonać, modyfikując uprawnienia dla wybranego (i tylko tego) użytkownika.

Jak stworzyć nowego użytkownika?

1. W głównym oknie administracyjnym kliknij guzik User.
2. Z menu File wybierz New. Pojawi się okno właściwości użytkownika (User Properties).
3. Wypełnij pola tekstowe zgodnie z potrzebami. Musisz wypełnić co najmniej pola User ID (identyfikator), Password (hasło; uwaga - jest to jednorazowe hasło przekazania) oraz Name (imię i nazwisko użytkownika).
4. Kliknij guzik Advanced (Zaawansowane), aby wprowadzić dodatkowe systemowe informacje o użytkowniku.
5. Jeśli jako metodę logowania wybrałeś SecurID, to zaznacz pole wyboru SecurID Defined.
6. Kliknij zakładkę Win95.
7. Zaznacz pole wyboru Define Windows 95 ID (Zdefiniuj identyfikator dla Windows 95).
8. W polu Windows 95 User ID (Identyfikator użytkownika w Windows 95) wpisz identyfikator użytkownika, którego używa on do logowania się do Windows 95. W polu Password wpisz hasło, którego używa on do logowania się do Windows 95.

- UWAGA. Czynność ta pozwala systemowi PC/DACS for Windows 95 zsynchronizować identyfikator i hasło użytkownika z identyfikatorem i hasłem użytkownika używanym w Windows 95. Podane w tej zakładce hasło jest podawane do Windows 95 przez PC/DACS po zalogowaniu się użytkownika. Identyfikatory i hasła do PC/DACS i do Windows 95 mogą, lecz nie muszą być takie same. Jeśli użytkownik uprzednio logował się do Windows 95, to jego identyfikator i hasło powinny być wpisane właśnie w tej zakładce. Jeśli nie wypełni się pól tej zakładki, użytkownik będzie poproszony o podanie swojego identyfikatora i hasła do pulpitu Windows 95 po pierwszym prawidłowym logowaniu się do PC/DACS.
- Patrz też rozdział wstępny IX.

9. Kliknij zakładkę Personal Information (Informacje o użytkowniku).
10. Wypełnij pola tekstowe. Wypełnienie informacji jest tu opcjonalne. W polu adresu możesz np. zapisać nr pokoju itp. Nową linię rozpoczyna się wciskając Ctrl-Enter.
11. Na zakończenie wciśnij guzik OK, aby zapisać wszystkie wprowadzone zaawansowane informacje o użytkowniku. Powrócisz do okna właściwości użytkownika.
12. Z okna właściwości użytkownika wciśnij guzik Security, aby przejść do ekranu z profilem bezpieczeństwa użytkownika.

- **Zakładki profilu bezpieczeństwa użytkownika są identyczne, jak zakładki profilu bezpieczeństwa roli i są objaśnione w rozdziale dotyczącym ról. Jeśli chcesz teraz przystąpić do modyfikacji profilu bezpieczeństwa użytkownika, powróć do rozdziału o rolach, gdzie znajdziesz niezbędne opisy.**

13. Teraz skonfiguruj opcje logowania dla użytkownika. Opcje te opisane są niżej w sekcji Opcje logowania.

Atrybuty dziedziczone

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Zakładka Logon/Logoff (opcje logowania)

Jako administrator PC/DACS musisz określić, w jaki sposób uzytkownik będzie mógł logować się do komputera oraz wylogowywać się. Zakładka Logon/Logoff okna profilu bezpieczeństwa użytkownika (okno Security) służy do konfigurowania metod logowania użytkowników.

Zakładka Logon/Logoff pojawia się od razu po naciśnięciu guzika Security na ekranie użytkownika.

Grupa Logon Method (Sposób logowania się)

Grupa Logon Method zawiera cztery pola wyboru, określające metodę logowania się użytkowników do PC/DACS:

- Screen (Standardowe) - poprzez identyfikator i hasło,
- Floppy (Dyskietka) - poprzez dyskietkę logującą; bez identyfikatora ani hasła,
- All (Dowolne) - oboma powyższymi metodami,
- None (Brak) - brak możliwości logowania się dla tego użytkownika. Ta opcja jest przydatna, gdy trzeba czasowo "odciąć" użytkownika od komputera lub wymusić na nim zalogowanie się jako uzytkownik specjalny $GUEST. Opcja None jest dobrym wyborem, gdy dany użytkownik będzie używany tylko jako projekt. Użytkownik może zalogować się z widokiem z projektu, ale nie jako projekt.

Grupa Logon Password Changes (Zmiany hasła)

Grupa Logon Password Changes zawiera cztery pola wyboru, określające metodę zmiany hasła użytkownika:

- User (Użytkownik) - zezwala użytkownikowi na zmianę hasła w dowolnym momencie,
- System (System) - zezwala tylko na zmiany hasła wymuszane przez system,
- All (Dowolne) - opcja domyślna, zezwala na dowolne zmiany hasła,
- None (Brak) - nie zezwala na żadne zmiany hasła.

Pole wyboru Rename User On Next Use

To pole wyboru (Zmień nazw użytkownika przy następnym użyciu) spowoduje wymuszenie przy następnym logowaniu użytkownika zmianę jego identyfikatora i hasła.

Pole wyboru Reboot System on Logoff

To pole wyboru (Zresetuj system przy wylogowaniu) spowoduje zamknięcie i restart systemu po każdym wylogowaniu się użytkownika.

Pozostałe zakładki profilu bezpieczeństwa użytkownika

Pozostałe zakładki profilu bezpieczeństwa użytkownika są identyczne, jak zakładki profilu bezpieczeństwa roli i są objaśnione w rozdziale dotyczącym ról. Jeśli chcesz teraz przystąpić do modyfikacji profilu bezpieczeństwa użytkownika, powróć do rozdziału o rolach, gdzie znajdziesz niezbędne opisy.

Zapamiętanie nowego użytkownika

1. Po zakończeniu wprowadzania modyfikacji do profilu bezpieczeństwa użytkownika, wciśnij guzik OK. Powrócisz do ekranu użytkownika.
2. Jeśli chcesz stworzyć następnego użytkownika, wciśnij guzik Another (Następny). Jeśli chcesz teraz dodać tylko jednego użytkownika, wciśnij OK. Powrócisz do głównego okna administracyjnego.
3. Uzytkownik został dodany i od tego momentu można już logować się do PC/DACS z jego identyfikatorem. Przekaż użytkownikowi jego identyfikator oraz zdefiniowane przez ciebie jednorazowe hasło przekazania, tak aby użytkownik mógł zalogować się do PC/DACS, zmienić sobie hasło i rozpocząć pracę.

Tworzenie projektów

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Rozdział 7 - Zarządzanie zaawansowanymi opcjami konfiguracyjnymi PC/DACS

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Rozdział 8 - Generacja raportów z dziennika działań

PC/DACS potrafi skutecznie rejestrować działalność użytkowników i administratora w systemie. Zdarzenia i operacje, które mają być rejestrowane wybiera się podczas konfiguracji globalnych parametrów bezpieczeństwa (patrz sekcja Parametry bezpieczeństwa globalnego).

PC/DACS pozwala na efektywne przeglądanie i drukowanie dziennika działań. Do tego celu służy osobny moduł PC/DACS Audit Log Viewer.

PC/DACS Audit Log Viewer uruchamia się z menu Start/Programy/PC/DACS for Windows 95. Po uruchomieniu modułu PC/DACS Audit Log Viewer, należy wybrać opcję Options z menu Report, ustawić wszystkie żądane opcje w oknie PC/DACS Audit Report Options i nacisnąć guzik Generate Report w tym samym oknie.

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Rozdział 9 - Logowanie i wylogowywanie się z systemu PC/DACS

Konfiguracja opcji logowania

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Logowanie się do systemu

Okno logowania PC/DACS pojawia się zawsze wtedy, gdy startujesz/restartujesz swój komputer. Pojawia się też wtedy, gdy wylogujesz się z systemu bez restartu komputera. Po pojawieniu się okna logującego, musisz zalogować się do systemu, aby rozpocząć pracę.

1. W polu User ID wpisz swój identyfikator. Ewentualne błędy popraw standardowymi klawiszami edycyjnymi. Naciśnij <TAB>, aby przejść do pola Password (nie naciskaj <Enter>, naciśnięcie klawisza <Enter> jest równoznaczne z naciśnięciem guzika Logon).
2. W polu Password wpisz swoje hasło. Ewentualne błędy popraw standardowymi klawiszami edycyjnymi. Znaki hasła nie będą wyświetlać się na ekranie.
3. Naciśnij guzik Logon lub naciśnij <Enter>. Jeśli jest to twoje pierwsze logowanie jako użytkownik PC/DACS, pojawi się okno, w którym będziesz musiał podać swój identyfikator i hasło do pulpitu Windows 95. Te dane zostaną podane przez PC/DACS do pulpitu Windows 95 po zalogowaniu się użytkownika do PC/DACS.

- Informacje o synchronizacji haseł znajdziesz w rozdziale wstępnym IX i Rozdziale 6 - Użytkownicy.
- Guzik Change Password służy do zmiany hasła; guzik Shutdown pozwala na zamknięcie systemu z poziomu okna logującego.

4. Wpisz swój identyfikator i hasło do pulpitu Windows 95, lub zaakceptuj wartości domyślne, wciskając OK.
5. Pojawi się (opcjonalne) okno z informacją o ostatnim logowaniu się na to konto. Okno to ma na celu poinformowanie (w celu weryfikacji), kiedy nastąpiło ostatnie logowanie na to konto i czy nie było prób nieautoryzowanego zalogowania się.
6. Kliknij OK na oknie informacyjnym. Jeśli jest to twoje pierwsze logowanie się, będziesz teraz poproszony o zmianę hasła przekazania, które otrzymałeś od administratora. Zmiana hasła zakończy proces logowania.

- Informacje o synchronizacji haseł znajdziesz w rozdziale wstępnym IX i Rozdziale 6 - Użytkownicy.

Wylogowywanie się z systemu

UWAGA. Zastosowanie dowolnej z poniższych procedur spowoduje zakończenie wszystkich połączeń sieciowych. Ponowne zalogowanie do sieci będzie możliwe (i, w zależności od konfiguracji, zostanie wykonane automatycznie) po ponownym zalogowaniu się do PC/DACS.

Wylogowywanie się poprzez logo MERGENT-a

1. Kliknij prawym klawiszem myszy czerwone logo MERGENT-a na pasku zadań.

2. Z menu wybierz opcję Logoff Now (Wyloguj teraz), aby zakończyć proces wylogowania się.

Wylogowywanie się standardowa metodą Windows 95

1. Z menu Start wybierz opcję Zamknij system.
2. Z dostępnych opcji w oknie Zamknij system wybierz żądaną opcję. Możesz np. zalogować się jako inny użytkownik bez zamykania systemu, co da taki sam efekt, jak opisana wyżej procedura wylogowania przez ikonę MERGENT-a.
3. Wciśnij guzik Tak, aby zakończyć proces wylogowania się.

Logowanie się za pomocą schematu Challenge/Response (wyzwanie/odpowiedź)

Jeśli uzytkownik zapomni hasła, znajduje się zwykle w trudnej sytuacji. Szczególnie niebezpieczna jest taka sytuacja, gdy użytkownik znajduje się w miejscu, gdzie nie może poprosić administratora o odwiedzenie go i zresetowanie jego hasła. PC/DACS jest dobrze zabezpieczony przed takimi sytuacjami i pozwala skutecznie je rozwiązywać, bez konieczności wykonywania czynności przez administratora bezpośrednio przy komputerze użytkownika. Jednocześnie dzięki zastosowaniu metod kryptograficznych, nie jest w żaden sposób naruszone bezpieczeństwo systemu.

Do przydzielenia dostępu i umożliwienia zmiany hasła użytkownikowi, który zapomniał swojego hasła, służy logowanie się za pomocą schematu Challenge/Response. Polega on na generacji przez użytkownika w oknie logującym specjalnej, jednorazowej i losowej liczby-wyzwania (Challenge), podaniu tej liczby przez telefon administratorowi, a następnie wpisaniu w oknie logującym otrzymanej od administratora liczby-odpowiedzi (Response).

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Rozdział 10 - Time Out (blokada komputera po określonym czasie)

Time Out jest funkcją PC/DACS pozwalającą na zablokowanie komputera, do którego jest zalogowany uzytkownik, lecz opuścił on swoje stanowisko pracy. Zabezpiecza to przed skorzystaniem z "niepilnowanego", włączonego komputera przez osoby niepowołane. Time Out może włączać się automatycznie po określonym czasie, lub może być inicjowany przez użytkownika.

Opcje Time Out można konfigurować grupowo - dla ról, lub indywidualnie, dla użytkowników. Dokonuje się tego w zakładce Time Out profilu bezpieczeństwa użytkownika lub roli.

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Rozdział 11 - Wyłączanie blokady twardego dysku

W każdej chwili możesz wyłączyć włączoną blokadę twardego dysku. Możesz dokonać tego metodą tzw. wewnętrzną (Internal) poprzez zakładkę BP Encryption globalnego profilu bezpieczeństwa, lub metodami zewnętrznymi (po starcie komputera z dyskietki).

Wewnętrzne (standardowe) wyłączanie blokady twardego dysku

1. Uruchom program administracyjny PC/DACS.
2. Wybierz opcję Global Security z menu Manage.
3. Kliknij zakładkę BP Encryption.
4. Wybierz dysk, dla którego chcesz wyłączyć blokadę.
5. Wyłącz blokadę poprzez wyczyszczenie pola wyboru Boot Protect. PC/DACS przystąpi do zdejmowania blokady i będzie cię informować na bieżąco o stanie tej czynności.

- W systemach z więcej niż jednym twardym dyskiem, zdjęcie blokady z pierwszego dysku spowoduje automatyczne zdjęcie blokady z wszystkich kolejnych dysków fizycznych.

Wyłączanie blokady twardego dysku z użyciem dyskietki odblokowującej

(Szczegółowy opis tej opcji/funkcji znajdzie się w pełnym tłumaczeniu podręcznika administratora.)

Rozdział 12- Deinstalacja PC/DACS

UWAGA. Przed deinstalacją PC/DACS musisz usunąć wszystkie zaszyfrowane katalogi. Pamiętaj o skopiowaniu ważnych informacji z tych katalogów do katalogów niezaszyfrowanych!

1. Z menu Start wybierz opcję Ustawienia.
2. Uruchom Panel Sterowania.
3. Kliknij podwójnie ikonę Dodaj/Usuń Programy.
4. W liście zainstalowanych programów kliknij PC/DACS for Windows 95.
5. Wciśnij guzik Dodaj/Usuń, który rozpocznie procedurę automatycznej deinstalacji PC/DACS.
6. Postępuj zgodnie ze wskazówkami na ekranie.
7. Po zakończeniu deinstalacji nastąpi restart komputera. Od tego momentu twój komputer nie jest już chroniony.

FORMULARZ UWAG I KOMENTARZY DO PODRĘCZNIKA

Tytuł podręcznika:	*PC/DACS for Windows 95 - Podręcznik administratora: wersja dla osób testujących*
Numer dokumentu:	*D95A9701*
Data otrzymania:	
Forma (plik, wydruk):	

UWAGI:

Formularz uwag jest anonimowy. Jeśli jednak chcesz, abyśmy skontaktowali się z Tobą w sprawie powyższych uwag, lub nadesłali poprawioną wersję podręcznika, zostaw nam swoje dane kontaktowe.

Imię i nazwisko:
Telefon:
Email:

FORMULARZ TEN WYŚLIJ NA

FAX: (0-22) 6198956, 6700756, 6700956

LUB EMAIL: info@safecomp.com
LUB POCZTĄ: SAFE COMPUTING Sp. z o.o., 03-733 Warszawa, ul. Targowa 34

Dziękujemy za poświęcenie czasu na przekazanie nam Twoich uwag!

SPIS TREŚCI