STACJA ROBOCZA

OSR-DG

DigiLab

Warszawa, 2004

Spółka z.o.o.

Al. Jerozolimskie 200
02-486 Warszawa
tel. (022) 863 21 50
fax. (022) 863 21 70
www.digilab.com.pl
e-mail: psi@digilab.com.pl

OPRACOWAŁ: **Marek Pokszan**

1. CHARAKTERYSTYKA OGÓLNA.

OSR-DG jest specjalizowaną stacją roboczą przeznaczoną do pracy systemach sieciowych lokalnych (LAN) i rozległych (WAN).

Komputer wyposażony jest w polskojęzyczny, wielozadaniowy system operacyjny Microsoft Windows 2000 Professional PL™ oraz narzędzia i aplikacje do obsługi zadań sieciowych.

Szczególną cechą stacji roboczej OSR-DG jest wbudowany czytnik specjalnej karty elektronicznej (chipowej), zwanej **Osobistym Identyfikatorem Cyfrowym** użytkownika. Czytnik ten jest współdziała ze specjalnym oprogramowaniem ***CartaGina***, rozszerzającym mechanizmy ochrony systemów operacyjnych z rodziny Windows NT.

Konstrukcja zastosowanego w OSR-DG mechanizmu identyfikacji użytkownika oraz zintegrowanego z systemem operacyjnym modułu zabezpieczeń oparta jest na wieloletnich doświadczeniach firmy DigiLab zdobytych przy licznych wdrożeniach specjalizowanych stacji dostepowych w sieciowych systemach Policji Państwowej i innych służb.

Zastosowanie w procesie identyfikacji użytkownika czytnika kart elektronicznych umożliwia stosowanie stacji OSR_DG w systemach wykorzystujących podpis elektroniczny.

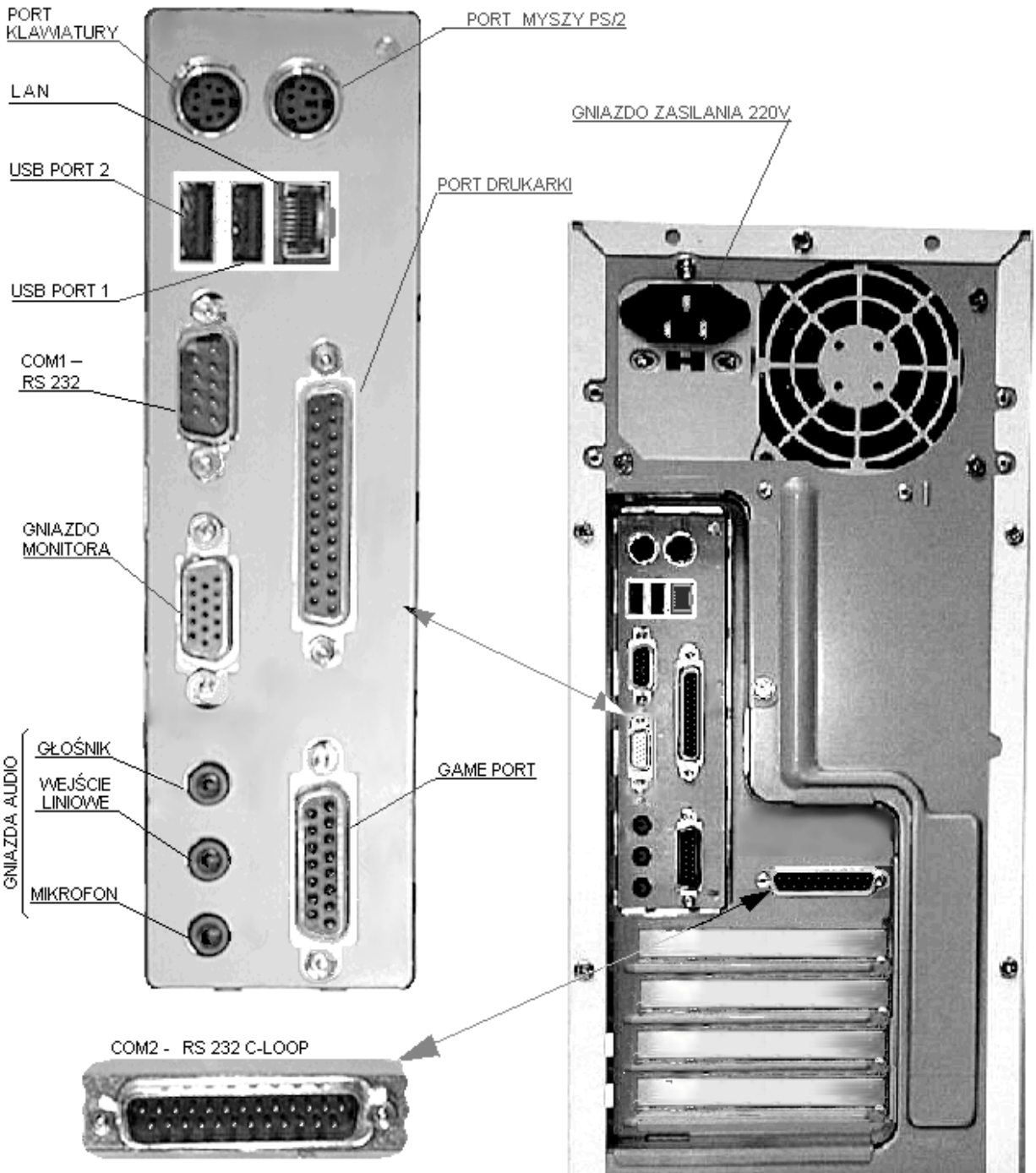
2. PARAMETRY TECHNICZNE OSR-DG.

Poniżej opisane zostały elementy decydujące o specyfice stacji roboczej OSR-DG:

- komputer – jako zespół sprzętowy,
- system specjalnych zabezpieczeń .

2.1 KOMPUTER

❑ Procesor:	Intel: Pentium P-4 min. 1,6 GHz
❑ Chipset:	Intel 845G
❑ Pamięć operacyjna:	256MB, DDR min. 266MHz
❑ Pamięć masowa:	1 HDD (min. 40 GB / UDMA66), 1 FDD (3.5''), 1 CDROM 48x
❑ Sterownik obrazu:	Direct AGP, 1÷20MB RAM / przydzielane dynamicznie
❑ Monitor:	kolorowy, CRT 17'' (opcja LCD 15"), TCO 95, 1280x1024 / 60 Hz
❑ Interfejs drukarki:	1, Centronics (ECP)
❑ Interfejsy magistrali:	PCI–1 wolny wewnętrzny slot,
❑ Interfejs szeregowy COM1:	RS 232 C (Złącze DB-9/P)
❑ Interfejs szeregowy COM2:	RS 232 z pętlą prądową 20mA (opcja)
❑ Interfej USB:	2 x USB2.0,
❑ Interfejs sieciowy:	1, Fast Ethernet 10/100 MHz, (opcja: konwerter 10 Base 2)
❑ Klawiatura:	EPC, złącze PS/2, standard ' Windows' - 106 klawiszy
❑ Mysz:	przewodowa - PS/2
❑ Zasilanie:	Sieć jednofazowa, uziemiona (3-przewodowa), napięcie 220V / 50Hz
❑ Obudowa i zasilacz:	Mini Tower, standard ATX / Micro-ATX.
❑ Szyfrator danych (OPCJA):	wewnętrzny - ISA, GAMA –P lub DELTA-3



Stacja robocza - widok od tyłu.

2.2 WYMOGI EKSPLOATACYJNE SPRZĘTU

a) Wszystkie urządzenia współpracujące zestawu OSR-DG muszą być **zasilane z tej samej fazy oraz wspólnie zerowane.**

b) Gniazda sieciowe 220V (±10%) / 50 Hz zasilające elementy zestawu powinny zawierać **zerowanie (bolec ochronny**).

c) Sprzęt powinien przebywać w pomieszczeniu o temperaturze +15...+35 st. C, wilgotności względnej 8%...80% mierzonej w temp. 20 st. C.

d) Po transporcie w warunkach odbiegających od zalecanych do eksploatacji sprzęt przed włączeniem powinien zostać odstawiony w pomieszczeniu, w którym będzie użytkowany, na czas potrzebny do **dostosowania swojej temperatury do temperatury otoczenia**.

e) Sprzęt nie powinien podlegać wstrząsom i wibracjom, pracować w pobliżu silnych pól magnetycznych lub być narażony na jakiekolwiek wyładowania elektrostatyczne a także powinien być zabezpieczony przed nadmiernym nasłonecznieniem.

f) Sprzęt powinien być eksploatowany w pomieszczeniach o niewielkim stopniu zapylenia.

g) **Wszelkich odłączeń i przełączeń pomiędzy elementami zestawu należy dokonywać tylko po odłączeniu przewodu sieci zasilającej.** Zaleca się, by osoba manipulująca przy złączach, **przed odłączeniem** przewodu zasilającego pozbyła się nagromadzonego na sobie elektrycznego ładunku statycznego – dotykając ręką do **metalicznej** części obudowy (ściany tylnej) OSR-DG.

3. INSTALACJA STACJI ROBOCZEJ

Miejsce instalacji terminala powinno być tak wybrane, aby zapewnić prawidłowe chłodzenie w trakcie eksploatacji. Komputer powinien znajdować się w takiej odległości od gniazda sieciowego, by przewód zasilający nie był naprężony (praktycznie - nie większej niż 2 m).

Aby przygotować stację roboczą do pracy, należy wykonać następujące czynności : wyjąć komputer, monitor i klawiaturę z opakowania transportowego, sprawdzić kompletność, sprawdzić czy nie wystąpiły uszkodzenia transportowe, podłączyć kable: monitora, klawiatury i komunikacyjne do odpowiednich złącz znajdujących się z tyłu komputera. Podłączyć kable zasilające monitora i komputera do gniazd.

3.1 PIERWSZE URUCHOMIENIE

- Włączyć zasilanie monitora przy pomocy włącznika sieciowego umieszczonego na maskownicy ekranu monitora (z przodu).
- Włożyć **O**sobisty **I**dentyfikator **C**yfrowy (klucz) do otworu czytnika w panelu czołowym modułu komputera.
- Włączyć zasilanie modułu komputera przy pomocy włącznika sieciowego umieszczonego w panelu przednim.

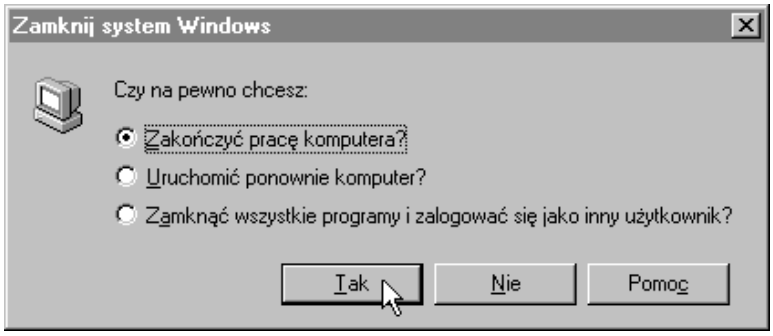
Po upływie kilku sekund od włączenia zasilania gotowość do pracy zgłasza BIOS komputera[1] a następnie system operacyjny. Ładowanie systemu operacyjnego wraz z interfejsem użytkownika może trwać dość długo. Odbywa się ono automatycznie i w warunkach normalnej eksploatacji **nie należy w ten proces ingerować** do czasu wyświetlenia charakterystycznego okienka z wezwaniem do zalogowania stacji roboczej i podania hasła użytkownika.

3.2 WYŁĄCZANIE

Przed wyłączeniem komputera należy **zamknąć wszystkie aplikacje** oraz **system operacyjny**[2].

Zamknięcie systemu - przykład nawigacji myszką na „pasku zadań" i „Menu Start**":**

Po kliknięciu myszką w tym miejscu, pojawia się okno dialogowe:



[1] Podczas startu BIOS wyświetlane jest firmowe logo OSR-DG .
[2] Istnieje kilka sposobów. Wszystkie opisane są w podręczniku systemu Windows NT ™.

Bezwzględnie należy odczekać na pojawienie się komunikatu zezwalającego na **RESTART** (!).
Po pojawieniu się takiego komunikatu **nie naciskać żadnych klawiszy** w klawiaturze ani w myszce lecz należy wcisnąć na panelu czołowym okrągły 'POWER' i przytrzymać go przez co najmniej 4 sekundy[3].

Należy pamiętać, że w OSR-DG podobnie jak we wszystkich maszynach klasy ATX po tak zwanym wyłączeniu zasilania (klawiszem 'POWER') płyta główna i niektóre intrerfejsy pozostają pod napięciem. **Tylko odłączenie kabla sieciowego fizycznie wyłącza zasilanie OSR-DG.**

4. KONSERWACJA BIEŻĄCA.

Zalecenia codzienne:

- oczyścić klawiaturę z pyłu i kurzu,
- przetrzeć ekran kineskopu przy pomocy ściereczki flanelowej,
- używać wyłącznie specjalnych substancji czyszczących przeznaczonych dla sprzętu komputerowego (zabrania się stosowania rozpuszczalników takich ,jak spirytus, aceton, benzyna).

Przynajmniej raz na pół roku czyścić napędy FDD i CD za pomocą dostępnych na rynku dyskietek czyszczących, zgodnie z załączoną do nich instrukcją.

Uwaga: Należy pamiętać, że w komputerze znajdują się **napięcia niebezpieczne** (220V) i mimo istniejących zabezpieczeń (osłon) należy zachować szczególną ostrożność przy manipulacji w ich pobliżu.

Naprawy:

Wszystkie komponenty stacji roboczej OSR-DG są zaplombowane. Zabrania się jakiejkolwiek ingerencji w jej wnętrze poza autoryzowanym serwisem.

[3] W razie krótkotrwałego wciśnięcia, komputer ponownie wystartuje – jak po 'RESET'.

5. OSOBISTY IDENTYFIKATOR CYFROWY

5.1 Składniki

Osobisty Identyfikator Cyfrowy (skr. **OIC**) - karta elektroniczna (chipowa), zawierająca unikatowy identyfikator użytkownika.

Czytnik – Czytnik Identyfikatora Cyfrowego (**CIC**) - urządzenie wbudowane na stałe do wnętrza OSR-DG, odczytujące identyfikator użytkownika z karty OIC włożonej do gniazda w przedniej ścianie obudowy komputera.

5.2 Współpraca OSR-DG z czytnikiem identyfikatora.

a) Aby uruchomić OSR-DG należy włożyć OIC do gniazda. W przypadku braku klucza, OSR-DG zatrzyma się po włączeniu na teście POST do czasu włożenia klucza.

b) Czytnik wczytuje numer pierwszego klucza włożonego do gniazda po włączeniu zasilania lub restarcie OSR-DG, po czym umożliwia normalną pracę pod kontrolą systemu operacyjnego.

c) Każdorazowe wyjęcie karty OIC z gniazda powoduje zablokowanie OSR-DG (zgaszenie ekranu, zablokowanie klawiatury i myszy oraz zablokowanie dostępu poprzez sieć). Ten stan jest sygnalizowany miganiem zielonej diody umieszczonej na obudowie OSR-DG.

d) Możliwości odblokowania OSR-DG:

- **włożenie tej samej karty OIC,** co przy starcie – OSR-DG samoczynnie powraca do stanu z przed wyjęcia karty
- **włożenie innej karty OIC** i naciśnięcie przycisku RESET na obudowie komputera – następuje samoczynny sprzętowy restart OSR-DG ze wszystkimi tego konsekwencjami dla systemu Windows 2000[4]. Następnie OSR-DG rozpoczyna normalną pracę wczytując z OIC identyfikator nowego użytkownika.

[4] taka metoda restartu OSR-DG nie jest prawidłowa, ponieważ nie została poprzedzona wylogowaniem z sesji terminalowych oraz zamknięciem systemu operacyjnego Windows NT ™.

e) Wyjęciu OIC z czytnika towarzyszy przełączenie OSR-DG w stan uśpienia: klawiatura i mysz pozostają zablokowane, a monitor ma wykasowaną zawartość ekranu i jest zdalnie wyłączony;

6 ZABEZPIECZENIA

6.1 ZABEZPIECZENIA TECHNICZNE

- Wszystkie funkcje blokowania OSR-DG realizowane są przez czytnik kart OIC wewnętrznie i nie ma możliwości ich wyłączenia.
- Dostęp do setup BIOS-u w OSR-DG jest zablokowany poprzez hasło.
- Zablokowana jest możliwość zmiany kodu BIOS-u komputera OSR-DG.
- Zablokowana jest możliwość załadowania systemu operacyjnego z innego źródła niż dysk **HDD0**
  Wszelkie uszkodzenia wymagające ponownej instalacji systemu operacyjnego wymagają znajomości haseł.
- Plik wymiany (Pagefile.sys) jest usuwany z dysku każdorazowo przy zamykaniu systemu.
- Obudowa OSR-DG jest plombowana mechanicznie w sposób uniemożliwiający samowolny dostęp do wnętrza.

6.2 ZABEZPIECZENIA SYSTEMOWE

- ***CartaGina*** **– Opis działania systemu wspomagania autoryzacji użytkowników stacji roboczych na platformie Windows 2000**

Firma DigiLab jest wieloletnim, doświadczonym producentem sprzętowych identyfikatorów użytkownika stosowanych w odpowiedzialnych systemach informatycznych. System *CartaGina* został opracowany przy współpracy z firmą EMG-Systems. Każda karta OIC ma swój własny, niepowtarzalny kod, co w połączeniu ze standardowym mechanizmem autoryzacji zaimplementowanym przez Microsoft™ w systemie operacyjnym Windows 2000 pozwala uzyskać bardzo wysoki poziom bezpieczeństwa. *CartaGina* zapewnia obecnie następującą funkcjonalność:

- podczas uruchamiania systemu operacyjnego, każdy autentyczność użytkownika jest weryfikowana nie tylko za pomocą standardowej procedury autoryzacyjnej (podanie nazwy konta oraz aktualnego hasła), lecz także na podstawie zaszyfrowanych danych z odczytanych z karty elektronicznej zawierającej unikatowy identyfikator przypisany do konta użytkownika;
- podczas pracy obecność karty OIC w gnieździe jest stale monitorowana, jej wyjęcie powoduje natychmiastowe zablokowanie stacji roboczej;
- ponowne umieszczenie w gnieździe tej samej karty OIC natychmiast odblokowuje system operacyjny; użytkownik uzyskuje dostęp do swoich aplikacji dokładnie w takim stanie jak przed blokadą;
- w dalszym ciągu można zablokować komputer w standardowy sposób (sekwencja Ctrl+Alt+Del i “zablokuj stację roboczą”) – w takiej sytuacji wyjęcie karty OIC powoduje “podwójną” blokadę – aby powrócić do pracy trzeba zarówno ponownie umieścić kartę w gnieździe, jak i podać hasło;

- gdy komputer został zablokowany, użycie innego (ale autoryzowanego na danej stacji roboczej) karty OIC o równym lub wyższym priorytecie powoduje wymuszone wylogowanie aktualnego użytkownika, a system pozwala na rozpoczęcie pracy przez nowego operatora (dysponującego kontem oraz właściwym OIC);
- specjalna aplikacja administracyjna pozwala na utworzenie i modyfikowanie bazy danych użytkowników;
- administracja kartami OIC polega na przypisaniu wybranym użytkownikom systemu (uprzednio zdefiniowanym za pomocą Menadżera użytkowników) kodów identyfikacyjnych, którymi mogą się oni posługiwać; dowolnie wybrani operatorzy mogą mieć uprawnienia administracyjne, można również zdefiniować hierarchię uprawnień (tylko OIC o równym lub wyższym priorytecie może wymusić wylogowywanie użytkownika, który opuścił stację roboczą i zablokował ją w ten sposób).

- **KeyEdit – Opis działania aplikacji administracyjnej.**

Do ustalania uprawnień poszczególnych OIC przewidziany jest program administracyjny o nazwie KeyEdit. Można go użyć, jeżeli spełnione są następujące warunki:

- na stacji roboczej zainstalowany jest system *CartaGina*;
- bieżący użytkownik ma uprawnienia administracyjne (zarówno z punktu widzenia Windows NT jak i systemu *CartaGina*);

Standardowo bezpośrednio po zainstalowaniu *CartaGina*, operator o nazwie “administrator” ma przypisany bazowy klucz danego systemu z uprawnieniami do administracji kluczami.

System *CartaGina* bazuje na liście lokalnych użytkowników danej stacji roboczej (zdefiniowanych zwykle dzięki wbudowanemu programowi “Menadżer użytkowników”). Każde konto, które nie jest aktualnie zablokowane, może mieć przypisany co najwyżej jeden OIC, którego obecność w gnieździe jest wymagana podczas logowania się i później podczas pracy z Windows NT. Użytkownicy, którzy nie mają zarejestrowanych OIC, nie mogą się zalogować.

System przewiduje aktualnie cztery poziomy uprawnień OIC: administracyjny, wysoki, średni oraz niski. Uprawnienia administracyjne mogą być nadane tylko kontom administratorów (z punktu widzenia Windows NT). Pozostałe poziomy uprawnień mogą być przydzielane dowolnie i nie mają związku z przynależnością do grup użytkowników Windows NT. Aktualnie poziomy uprawnień *CartaGina*-a (poza administrowaniem kartami OIC) decydują tylko o możliwości – lub nie – zalogowania się na komputerze zablokowanym po wyjęciu karty z gniazda: system dopuszcza “siłowe” wylogowanie bieżącego użytkownika (tzn. tego który zablokował Windows NT) tylko w przypadku użycia OIC o równym lub wyższym priorytecie.

Obsługa KeyEdit-a jest bardzo prosta: po uruchomieniu program dezaktywuje proces śledzący obecność karty w gnieździe, aby umożliwić manipulację identyfikatorami. Program przegląda i porównuje bazy danych użytkowników i kart. W przypadku znalezienia kart, których użytkownicy zostali usunięci z systemu, pojawia się stosowny komunikat, a

zdezaktualizowane wpisy zostaną usunięte (podczas zapisywania aktualnej bazy). Następnie na ekranie pojawia się okno programu, zawierające cztery elementy: listę użytkowników oraz trzy przyciski: “Przypisz klucz”, “Usuń przypisanie” i “Koniec”. Lista użytkowników składa się z trzech kolumn: “Użytkownik / konto”, zawierającej nazwy użytkowników systemu; “Klucz”, gdzie może być wpis “Tak” lub “Nie”, informujący o stanie przypisania lub nie klucza do użytkownika oraz “Poziom uprawnień” – poziomy uprawnień opisano powyżej (jeżeli konto nie ma swojego klucza, w tej kolumnie znajduje się tekst: “[-]”). Poszczególni użytkownicy mogą być wyróżnieni kolorem czerwonym, co oznacza możliwość przypisania im uprawnień administracyjnych, zaś konta wyłączone zaznaczone są kolorem szarym. W oknie z listą operatorów można przemieszczać kursor-podświetlenie, wybierając linię odpowiadającą operatora, którego parametry mają ulec zmianie. Przesunięcie kursora na daną pozycję powoduje odpowiednią aktywację lub dezaktywację przycisków. Każdemu aktywnemu użytkownikowi można przypisać nowy identyfikator OIC, zaś każdy użytkownik z kartą OIC (również aktualnie nieaktywny) może mieć usunięte przypisanie. Usunięcie przypisania jest natychmiastowe, natomiast przypisanie identyfikatora wymaga włożenia do gniazda odpowiedniej karty.

Nie jest możliwe przypisanie jednego OIC więcej niż jednemu użytkownikowi. Po prawidłowym przypisaniu identyfikatora do konta, otrzymuje ono domyślnie poziom uprawnień “średni”, można je następnie dowolnie zmienić.

Po zakończeniu edycji przypisań i uprawnień OIC operator wybiera przycisk “Koniec”. Program zadaje pytanie, czy zapisać aktualny stan bazy danych (odpowiedź “nie” spowoduje rezygnację z wprowadzonych zmian). Na tym etapie można jeszcze wrócić do programu i dokonać kolejnych poprawek. Program **wymaga, aby przynajmniej jeden operator miał uprawnienia do administrowania bazą OIC** – w przeciwnym przypadku nie byłoby możliwe ponowne użycie KeyEdit-a.

Zamykając sesję administracyjną, program ponownie aktywuje śledzenie kart i – jeżeli w gnieździe znajduje się inny OICz niż przypisany do bieżącego operatora – blokuje stację roboczą. Wystarczy wówczas włożyć do gniazda właściwą kartę, aby móc kontynuować normalną pracę.

9. WSPARCIE TECHNICZNE

DigiLab Sp. z o.o.

tel.: (+48 22) 8632150
fax.: (+48 22) 8632170
e-mail: psi@digilab.com.pl