Elektroniczny klucz do PC, część 1

kit AVT-330

Każdy użytkownik PC-ta natknął się z pewnością na problem, w jaki sposób zabezpieczyć swój komputer przed dostępem osób niepowołanych? Za taką osobę autor uznał niegdyś swojego najmłodszego brata, który z ogromnym zacięciem (oczywiście niechcący) usuwał z dysku twardego efekty jego kilkudniowej pracy.... Ponieważ komputery bardzo skutecznie „trafiły pod strzechy", zabezpieczenie danych zgromadzonych na dysku twardym nabiera coraz większego znaczenia i to nie tylko w służbach specjalnych, ale także w codziennej pracy biurowej i w domu. Proponujemy dość nietypowe rozwiązanie tego problemu - nie trzeba już będzie ukrywać komputera w pancernej szafie, czy też zamykać dysku twardego na stalową kłódkę - zamiast tych drastycznych metod wystarczy zainstalować we wnętrzu komputera niewielką kartę i przypiąć sobie do kluczy breloczek z pastylką Touch Memory!

Od tego momentu po włączeniu komputera musimy się wylegitymować przed nim posiadaniem klucza-pastylki o odpowiednim numerze.

Najbardziej popularną metodą zabezpieczania komputera przed osobami niepowołanymi jest instalowanie haseł dostępu jako jedna z opcji BIOS-u. Metoda ta pomimo szeregu zalet ma jedną, dość istotną wadę - standardowe BIOS-y wyposażone są w hasła - klucze, które ustala producent płyty i przez to są one powszechnie znane. Bardzo często ich treść publikowana jest w dokumentacji udostępnianej odbiorcom, co czyni hasło zakładane indywidualnie praktycznie bezużytecznym.

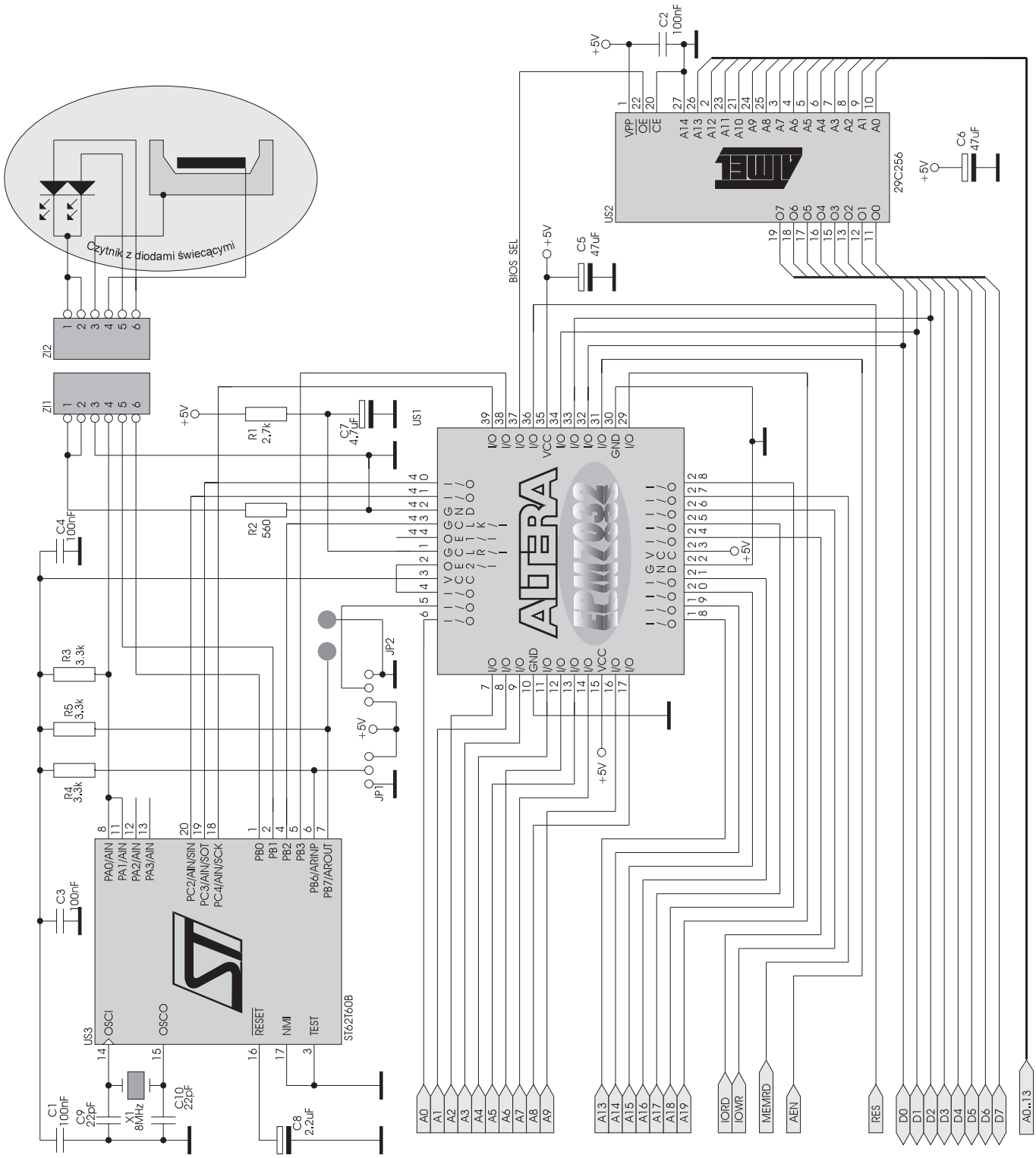
Innym spotykanym rozwiązaniem są programy typu Norton Disk Lock, które automatycznie uruchamiają się po włączeniu komputera, lecz ich wada jest podobna jak haseł w BIOS-ie. Między innymi, w Internecie są dostępne programy umożliwiające zdjęcie takiej blokady. Istnieje ponadto groźba powstania niebezpiecznych uszkodzeń struktury logicznej dysku w przypadku zainfekowania komputera wirusem modyfikującym FAT.

Najbardziej skutecznym sposobem zabezpieczenia dysku twardego wydaje się być sprzętowe szyfrowanie zawartości tego dysku, co jest rozwiązaniem dość kosztownym i nie zawsze akceptowanym przez nowoczesne systemy operacyjne (Windows 95, OS/2). Problemem stają się także opóźnienia wprowadzane przez kartę szyfrującą podczas zapisu i odczytu, ponieważ obniża się wydajność działania programów operujących na danych zgromadzonych na dysku twardym.

Proponowane przez nas rozwiązanie pozbawione jest wymienionych dotychczas wad, posiada

Parametry i cechy charakterystyczne karty - klucza

- ✓ 8-bitowa karta w standardzie ISA;
- ✓ wbudowany własny BIOS, lokowany pod adresem: D8000h;
- ✓ karta zajmuje jeden dwukierunkowy port I/O, lokowany pod adresem: 31Fh;
- ✓ możliwość obsługi dwóch kluczy DS1990 lub dowolnych innych układów rodziny Touch Memory lub iButton;
- ✓ numery kluczy (64-bitowe) zapamiętywane są w pamięci nieulotnej EEPROM;
- ✓ zasilanie karty: 5V/200mA (ze slotu ISA);
- ✓ możliwość wymiany numerów kluczy przy pomocy dołączonego oprogramowania;
- ✓ możliwość włączenia i wyłączenia zabezpieczenia przy pomocy dołączonego oprogramowania;
- ✓ możliwość zmiany języka (polski/angielski) w jakim wyświetlane są komunikaty BIOS-a;
- ✓ możliwość skasowania kluczy w pamięci EEPROM w trybie awaryjnym (wymaga rozebrania komputera);
- ✓ możliwość zmiany trybu pracy diody sygnalizacyjnej;
- ✓ łatwość instalacji i użytkowania;
- ✓ łatwa konfiguracja trybu pracy.



Rys. 1. Schemat elektryczny układu.

za to nieco inne - nie zabezpiecza komputera po zdemontowaniu karty-klucza i nie szyfruje zawartości dysku twardego, przez co nie gwarantuje tajności trzymanych na nim informacji. Jest za to łatwe w obsłudze i w typowych zastosowaniach biurowych i domowych (gdzie rzadko grasują zawodowi włamywacze komputerowi) praktycznie uniemożliwia korzystanie z komputera przez osoby nieuprawnione.

Rolę klucza uruchamiającego komputer spełnia znana doskonale Czytelnikom EP pastylka Touch Memory firmy Dallas. Głowica czytnika instalowana jest na przedniej części obudowy komputera.

Opis układu

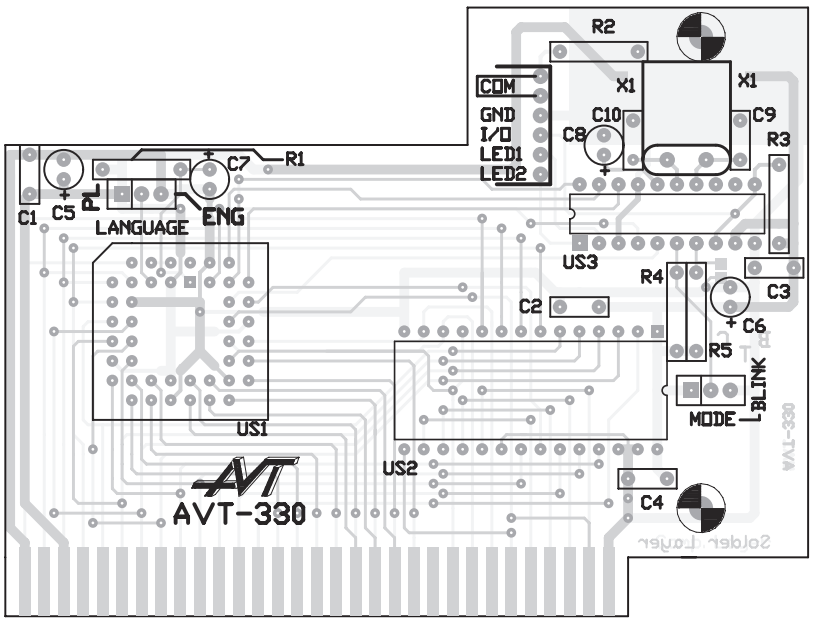
Schemat elektryczny karty zabezpieczającej przedstawiono na **rys.1**. Jest to urządzenie o niezwykle prostej konstrukcji sprzętowej, co udało się uzyskać dzięki zastosowaniu trzech układów programowanych: struktury CPLD (US1 - MAX7032 firmy Altera), pamięci EPROM (US2 - w modelu

zastosowano EEPROM AT29C256) i mikrokontrolera z wewnętrzną pamięcią programu (US3 - ST62T60).

W pamięci US2 znajduje się program, którego obecność jest automatycznie wykrywana przez BIOS komputera PC. Po przeprowadzeniu testów i zainicjowaniu podstawowych modułów komputera (w tym karty graficznej) sterowanie jest przekazywane do BIOS-u karty-klucza. Program ten blokuje pracę komputera do czasu zgłoszenia przez procesor US3 faktu wykrycia przyłożenia do czytnika klucza o numerze zgodnym z jednym ze wzorców. Czas oczekiwania na przyłożenie klucza jest ograniczony przez program do ok. 40 sek. Oczekiwanie na przyłożenie klucza jest sygnalizowane przy pomocy paska o zmieniającej się długości, który wskazuje upływ czasu.

Układ US1 realizuje na karcie dość złożone zadania:
- spełnia rolę dekodera adresowego dla rejestru 31Fh;
- spełnia rolę dekodera adresowego dla pamięci EPROM z zapisanym BIOS-em;
- spełnia rolę rejestru konfiguracyjnego i portu weryfikacji (obydwa te elementy umożliwiają wymianę informacji pomiędzy procesorem komputera i mikrokontrolerem US3);
- spełnia rolę automatu kontrolującego protokół wymiany informacji pomiędzy programem zapisanym w BIOS-ie a procesorem US3. Zaprojektowano 8-stanowy automat synchroniczny gwarantujący niemal 100% utajnienie sposobu wymiany informacji pomiędzy procesorem komputera i mikrokontrolerem US3.

Aplikacja układu US3 jest zbliżona do rozwiązania zastosowanego w zestawie AVT-294. Identyczne są w obydwu układach procedury odczytu pastylek DS1990, a także sposób wyliczania sumy kontrolnej i zapobiegania możliwości wczytania klucza o numerze seryjnym 0. Zupełnie odmienne są natomiast procedury zgłaszania otoczeniu wykrycia poprawnego klucza, zastosowano ponadto bardzo złożoną procedurę wymiany informacji z otoczeniem (BIOS-em karty). Wymiana informacji pomiędzy procesorem i automatem „zaszytym" w strukturze US1 odbywa się szeregowo poprzez linie I/O US3 oznaczone PC.2, PC.3 i PC.4.



Rys. 2. Rozmieszczenie elementów na płytce.

Do wejścia PB.6 dołączony został jumper, który umożliwia ustalenie, czy czerwona dioda LED, zintegrowana z głowicą czytnika, ma być włączona (migać) po przejściu do stanu czuwania, czy też ma pozostać zgaszona. Wejście PB.7 umożliwia awaryjne wyzerowanie pamięci EEPROM US3, dzięki czemu po zgubieniu obydwu kluczy istnieje możliwość dalszego wykorzystania karty, bez konieczności wymiany procesora.

Jumper JP2 służy do ustalenia języka, w jakim będą wyświetlane komunikaty BIOS-u. Do wyboru przewidziano wersję angielską i polską.

Jak wspomniano wcześniej we wnętrzu układu US1 znajduje się 8-stanowy automat synchroniczny. Do poprawnej pracy wymaga on zerowania po włączeniu zasilania. Zadanie to realizują elementy R1, C7. Podobną rolę (lecz dla procesora US3) odgrywa kondensator C8.

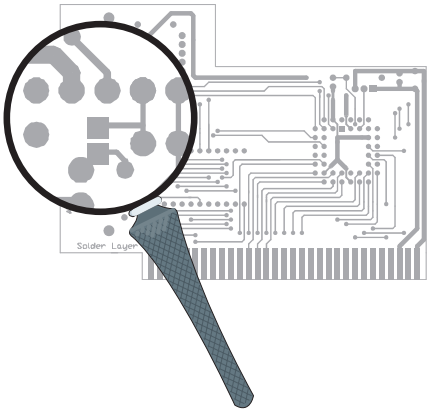
Głowica czytnika jest dołączona do karty przy pomocy 6-stykowego złącza kątowego Zl1, Zl2. Rezystor R3 „podciąga" stan logiczny szyny transmisyjnej do poziomu logicznej „1". Zastosowano rezystor o wartości nieco mniejszej niż w dotychczasowych aplikacjach. Okazało się to konieczne w przypadku stosowania długich kabli łączących głowicę czytnika z płytką. Nieco dłuższe kable trzeba stosować w obudowach typu big-tower oraz obudowach dużych serwerów sieciowych.

Montaż i uruchomienie układu

Płytka drukowana urządzenia została zaprojektowana jako dwustronna z metalizacją, co ogromnie podniosło komfort montażu i uruchomienia układu. Złącze krawędziowe karty pokryto warstwą złota, które zapobiega pokrywaniu się powierzchni styku korozyjnymi nalotami, przez co rezystancja styku jest mała i nie zmienia się w czasie.

Do wykonania poprawnego montażu karty niezbędna jest dobrej jakości lutownica ze standardową grzałką. Lutownica transformatorowa może spowodować uszkodzenie ścieżek na płytce drukowanej i nie gwarantuje dobrej jakości lutu. Zalecane jest stosowanie stopu cyny z rdzeniem z kalafonii, który bardzo ułatwia wykonanie poprawnych lutów. Zastosowanie się do powyższych uwag może zapobiec rozczarowaniom, gdyż pomimo stosunkowo prostej konstrukcji montaż układu wymaga precyzji.

Rozmieszczenie elementów przedstawiono na **rys.2**. Widok ścieżek na obydwu stronach płyt-



Rys. 3. Umiejscowienie punktów zerowania pamięci.

ki drukowanej przedstawiono na wkładce wewnątrz numeru.

Montaż rozpoczynamy od wlutowania w płytkę rezystorów i podstawek pod układy scalone. Układ US1 wymaga zastosowania specjalnej podstawki dla układów PLCC.

Następnie montujemy kondensatory, jumpery i kwarc. Kwarc powinien być wlutowany równolegle do powierzchni płytki, a jego obudowa dolutowana do pocynowanego pola pod spodem. Przed przylutowaniem obudowy kwarce należy przykręcić do płytki wspornik śledzia, stanowiącego jedyny element konstrukcji mechanicznej. Podczas lutowania obudowy kwarcu należy uważać, aby zbyt długo jej nie podgrzewać, gdyż może to spowodować uszkodzenie płytki rezonującej.

Na końcu montujemy w płytce złącze kątowe Zl1. Kabel łączący głowicę czytnika z płytką należy zaopatrzyć w komplementarną końcówkę złącza Zl1 (oznaczona jako Zl2). Na tym kończymy montaż i możemy rozpocząć procedurę uruchamiania.

Przed włożeniem karty do komputera należy ponownie skontrolować jakość i poprawność montażu elementów na płytce. Warto także sprawdzić, czy na złączu krawędziowym nie ma zwarć pomiędzy poszczególnymi wyprowadzeniami.

Kartę wkładamy do komputera po wyłączeniu jego zasilania! Warto także pamiętać o tym, aby po wyłączeniu zasilania odczekać kilkanaście sekund przed ponownym jego włączeniem. Zapobiegniemy w ten sposób możliwości uszkodzenia przetwornicy impulsowej, które może wystąpić w wyniku udaru wywołanego stanem nieustalonym.

Po włączeniu zasilania na ekranie wyświetlony zostanie komunikat o nie zainicjowanej pamięci kluczy. Inicjalizacja tej pamięci polega na przytknięciu do głowicy czytnika kolejno dwóch kluczy. Należy cały czas obserwować ekran monitora, ponieważ BIOS wyświetla odpowiednie komunikaty, które ułatwiają obsługę karty.

Uruchomienie karty sprowadza się w zasadzie tylko do wymienionych powyżej czynności. Jeżeli montaż został wykonany poprawnie i z zastosowaniem sprawnych elementów, to nie powinny wystąpić żadne trudności.

Uwagi końcowe

Ponieważ trudno wykluczyć możliwość zagubienia przez właściciela komputera klucza (pastylki) do niego, przewidziana została możliwość awaryjnego wykasowania z pamięci EEPROM (zaimplementowanej w układzie US3) znacznika ważności kluczy.

Kasowanie kluczy odbywa się poprzez zwarcie dwóch niewielkich pól na powierzchni płytki drukowanej, których umiejscowienie przedstawiono na **rys.3**. Zwarcie tych pól wymaga ingerencji we wnętrze komputera, co z reguły wzbudza zainteresowanie otoczenia, utrudniając nielegalne wykonanie tej czynności.

W egzemplarzu modelowym jako pamięć BIOS-u (US2) zastosowano układ z matrycą reprogramowlaną EEPROM, co znacznie ułatwiło prace konstrukcyjne. W skład kitu AVT-330 wchodzą zaprogramowane pamięci EPROM, które charakteryzuje znacznie niższa cena.

Przed ostatecznym zainstalowaniem karty we wnętrzu komputera należy ustawić przy pomocy jumperów JP1 i JP2 język, w jakim będą wyświetlane komunikaty (JP2) i tryb pracy diody LED po wyłączeniu zabezpieczenia. W położeniu JP1 oznaczonym „BLINK“ czerwona dioda LED zapala się na krótki czas, sygnalizując fakt dezaktywacji klucza. Jeżeli ktoś uzna to za zbyt denerwujące, jest możliwe wyłączenie tej diody poprzez zmianę położenia jumpera.

Program sterujący pracą procesora US3 zawiera proste, lecz skuteczne procedury autotestowania jednostki centralnej, co zapobiega jej niepoprawnej pracy.

W przypadku wykorzystywania karty w środowisku sprzyjającemu indukowaniu się ładunków elektrycznych, warto zastosować jako dodatkowe zabezpieczenie wejścia procesora US3 transil o napięciu przebicia 6.8..10V i mocy gaszenia 600W..1500W, włączony równolegle pomiędzy wejście czytnika i masę układu.

Piotr Zbysiński, AVT

W kolejnym numerze opublikujemy opis programu sterującego pracą procesora na karcie.

Autor zastrzega sobie prawo do modyfikacji programu zawartego w BIOS-ie, przy czym parametry użytkowe nie ulegną pogorszeniu.

Aktualizowane wersje BIOS-a do kitu AVT-330 będą dostępne (w miarę ich opracowywania) poprzez Internet, pod adresem www.atm.com.pl/~avt/ep (link „Nasze konto FTP“).

WYKAZ ELEMENTÓW

Rezystory
R1: 2,7kΩ
R2: 560Ω
R3, R4, R5: 3,3kΩ
Kondensatory
C1, C2, C3, C4: 100nF
C5, C6: 47µF/16V
C7: 4.7µF/16V
C8: 2.2µF/16V
C9, C10: 22pF
Półprzewodniki
US1: EPM7032LC44 (EPM7064LC44) zaprogramowany
US2: 27C256-15, 29C256-15 (Atmel) lub szybsza, zaprogramowana
US3: ST62T60B zaprogramowany
Różne
X1: 8MHz
Zl1, Zl2: złącze kpl.
JP1, JP2: Jumpery 1x3
Uklady DS1990: 2 szt.
Czytnik z wbudowanymi diodami LED
Śledź z uchwytami
Dyskietka z oprogramowaniem dla DOS AVT-330.