"Strażnik" klawiatury

AVT-867

W artykule prezentujemy niezwykłe urządzenie, którego zadaniem jest umożliwienie i jednocześnie maksymalne uproszczenie zabezpieczania oprogramowania przed nieuprawnionym rozpowszechnianiem. Tak więc za pomocą krótkiego programu, niewielkiej płytki i pastylki Dallasa, chroniony program staje się praktycznie niekopiowalny bez licencji.

Jak działa klawiatura?

Nie sposób napisać dłuższego, a nawet krótszego tekstu bez porządnej klawiatury (o czym piszący te słowa przekonał się wielokrotnie). Nawet w najnowocześniejszych komputerkach nareczных - *palmtopach* - prawie pozbawionych klawiszy, klawiatura - a przynajmniej jej rysunek - pojawia się na czułych na dotyk wyświetlaczach. Może kiedyś będzie można podyktować tekst komputerowi, jednak nie wiadomo, czy operator będzie wolał nadwerężyć gardło, czy palce. W każdym razie, klawiatura była obecna w tej czy innej formie - od zarania epoki komputerowej, chociaż czasami w dziwnej dla dzisiejszego użytkownika formie.

Klawiatura współczesnych komputerów osobistych nie jest tylko zwykłą „deską" z przyciskami. Wynika to z podstawowych funkcji, które musi spełnić każda klawiatura:
- wprowadzanie liter, cyfr i znaków specjalnych,
- obsługa klawiszy funkcyjnych (typowo od F1 do F12), a także funkcji specjalnych, jak tabulacja, kasowanie, wstawianie itd.,
- sterowanie kursorem,
- sygnalizowanie momentu naciśnięcia i puszczenia każdego klawisza,
- automatyczne powtarzanie znaku, gdy klawisz pozostaje przyciskany odpowiednio długo.

Dla zrealizowania tak bogatego zestawu funkcji, bez zabierania cennego czasu procesora centralnego, trzeba wyposażyć klawiaturę w specjalnie do tego celu oprogramowany procesor jednoukładowy. Procesor taki zajmuje się skanowaniem pola klawiszy, rejestruje moment naciśnięcia i puszczenia każdego z nich, a następnie informacje te, w formie specjalnego kodu, poprzez synchroniczny interfejs szeregowy wysyła do jednostki centralnej. Taki sposób obsługi klawiatury pojawił się już w pierwszych komputerach PC skonstruowanych przez firmę IBM, a następnie upowszechnił w milionach ich klonów. Z biegiem czasu także klawiatura nieco się zmieniła, generalnie jednak sposób współpracy między nią a jednostką centralną komputera pozostał taki sam. Największe zmiany, oprócz cech estetycznych (wygląd klawiatury) i mechanicznych (jakość przycisków i odporność na zużycie), polegają na tym, że:
- transmisja z jednokierunkowej (klawiatura przesyła dane do PC-ta) zmieniła się na dwukierunkową (komputer może przesłać do klawiatury nowe parametry jej pracy, np. szybkość repetycji),

Rys. 1a. Rozkład klawiszy typowej klawiatury PC z kodami klawiszy.

Rys. 1b. Rozkład klawiszy specjalnych i numerycznych wraz z kodami.

- zwiększona została liczba oraz rozkład klawiszy.

Dzięki możliwości dwustronnej wymiany danych, komputer może w każdej chwili skontrolować stan klawiatury, np. czy w ogóle jest dołączona, a także zażądać powtórnego wysłania danych w sytuacji, gdy podczas transmisji pojawił się w nich błąd.

Rozkład i oznaczenie klawiszy na typowej współczesnej klawiaturze pokazujemy na **rys. 1a**, **1b**. Drobne różnice w klawiaturach różnych producentów polegają najczęściej na dodaniu specjalnych klawiszy funkcyjnych emulujących naciśnięcie grupy klawiszy (np. klawisz WIN umożliwiający szybkie uruchomienie systemu WINDOWS). Na symbolu każdego z klawiszy, obok oznaczenia jego funkcji, podana została liczba w kodzie szesnastkowym. Są to tzw. *scan codes*, czyli kody oznaczające konkretny klawisz (w zapisie szesnastkowym).

Tak więc, wysłanie przez procesor klawiatury kodu 1Ch oznaczać będzie, że naciśnięty został klawisz „a", a kod 05h oznacza naciśnięcie klawisza funkcyjnego F1 itd. Przy niektórych klawiszach, np. prawego ALT-u, pojawia się dodatkowa liczba E0h. Pełni ona rolę prefiksu poprzedzającego kody klawiszy nie występujących w najstarszych klawiaturach. Dzięki temu zapewniona została kompatybilność ze starszym oprogramowaniem, nie potrafiącym rozróżnić prawego i lewego klawisza ALT.

Natomiast nowe oprogramowanie po odebraniu kodu 11h, poprzedzonego kodem E0h, będzie „wiedziało", że chodzi o prawy ALT.

Typowa akcja w czasie obsługi naciskania jednego klawisza wygląda następująco. Najpierw kablem łączącym klawiaturę z komputerem popłynie kod klawisza. Jeżeli klawisz będzie naciskany odpowiednio długo, uaktywniona zostanie funkcja powtarzania i kod ten będzie wysyłany z częstotliwością równą szybkości powtarzania klawiatury tak długo, aż w tym samym czasie nie zostanie naciśnięty inny klawisz lub klawisz nie zostanie zwolniony. W tym ostatnim przypadku klawiatura wygeneruje najpierw kod F0h, a następnie kod zwolnionego klawisza. Jak z tego widać, każde naciśnięcie i zwolnienie klawisza powoduje wysłanie do jednostki centralnej przynajmniej 3 kodów. Sprawa się nieco komplikuje, jeżeli komputer ma zinterpretować naciskany klawisz np. jako znak „@", a nie cyfrę „2". W tym celu jak wiadomo, niezbędne staje się użycie klawisza SHIFT, np. lewego. Ciąg wysyłanych znaków (bez repetycji) będzie wyglądał następująco: 12h+1Eh+F0h+1Eh+F0h+ +12h. Jak widzimy, prosta z pozoru czynność wymaga przesłania sporej porcji informacji.

Transmisja klawiatura-komputer i odwrotnie

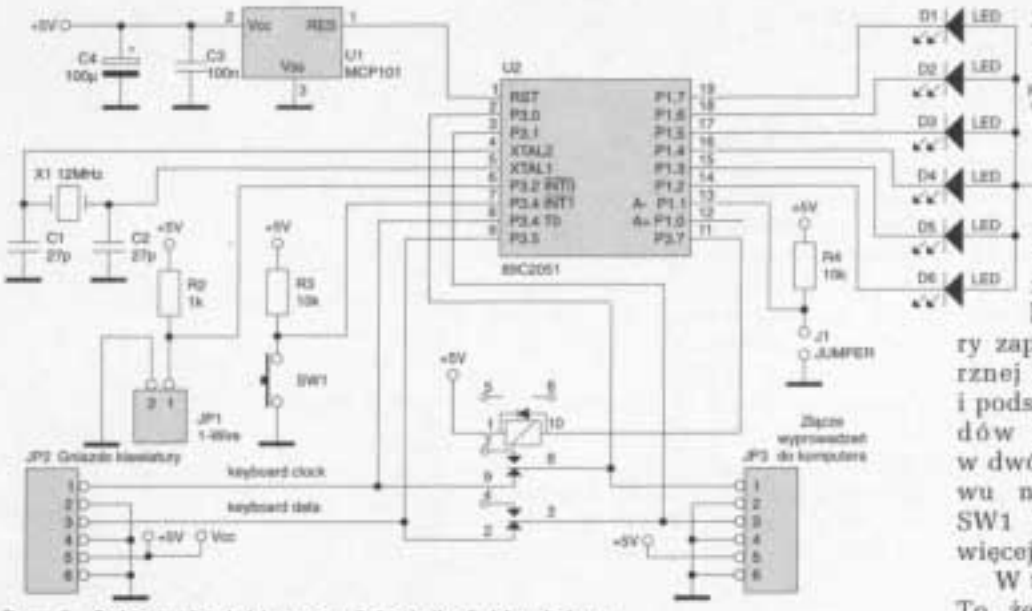
Jak wspomnieliśmy, pomiędzy klawiaturą a komputerem wymieniane są nie tylko informacje o naciskanych klawiszach, ale płyną także kody rozkazów sterujących. Ten dialog jest najżywszy po włączeniu komputera lub po jego zerowaniu. Widocznym efektem w przypadku klawiatur wyposażonych w diody sygnalizacyjne jest ich zapalanie się i gaśnięcie. W tym czasie komputer sprawdza, czy klawiatura jest dołączona oraz ustawia jej parametry. Kodów rozkazów sterujących jest wiele.

W przypadku transmisji od komputera do klawiatury może to być żądanie zerowania klawiatury, sterowanie wspomnianymi diodami sygnalizacyjnymi, żądanie powtórzenia ostatniej transmisji, ustawienie szybkości powtarzania, itp. Klawiatura może wysyłać do komputera kod potwierdzenia, żądanie powtórzenia rozkazu czy komunikat o przepełnieniu wewnętrznego bufora, gdy ilość informacji o naciskanych klawiszach jest większa od szybkości, z jaką mogą być przesłane do jednostki centralnej.

W starszych, wychodzących z użycia modelach jest to 5-stykowy wtyk DIN, w nowych to 6-stykowy MINI DIN. Opis obydwu wtyków podano na **rys. 2**. Na złącze wtyku wyprowadzona jest linia danych (KBD Data), linia sygnału zegarowego (KBD Clock), doprowadzenie napięcia zasilającego klawiaturę +5V (VCC) oraz linia masy (GND). Transmisja jest szeregowa synchroniczna, z bitem startu, 8 bitami danych, bitem parzystości i bitem stopu. Informacja na linii danych jest ważna w momencie opadającego zbocza impulsu zegarowego.

W przypadku transmisji od lub do PC transmisję inicjuje klawiatura wymuszając na linii danych stan niski i generując w chwilę potem opadające zbocze impulsu zegarowego. Jest to bit START. Następnie wysyłanych jest 8 bitów danych transmitowanego kodu, począwszy od bitu najmłodszego. W przypadku kodu klawisza „a", czyli 1Ch, transmisja bitów danych będzie następująca: 0-0-1-1-1-0-0-0. Następnie wysyłany jest bit parzystości służący do kontroli poprawności transmisji. Wartość tego bitu zależy od liczby jedynek w przesyłanym bajcie danych. Gdy liczba jedynek jest parzysta, bit jest 1, zaś dla wartości nieparzys-

Rys. 2. Funkcje poszczególnych styków w gniazdach DIN i PS2.



Rys. 3. Schemat elektryczny "strażnika" klawiatury.

tej bit zostaje ustawiony na 0. W podanym przykładzie bit parzystości będzie wyzerowany.

W przypadku transmisji kodów sterujących do klawiatury akcję rozpoczyna komputer ustawiając linię sygnału zegarowego w stan niski na czas dłuższy niż 60 ms. Następnie linia danych także ustawiana jest na poziom niski, a linia zegara zostaje zwolniona. Od tego momentu generowanie taktujących impulsów zegarowych przejmuje klawiatura. Jeżeli po odebraniu przez klawiaturę bitu parzystości linia danych pozostaje na poziomie wysokim, klawiatura wysyła impuls potwierdzenia ACK i transmisja rozkazu z komputera zostaje zakończona.

Klucz do PC-ta

W tym miejscu Czytelnik może pomyśleć, jak praktycznie wykorzystać wiedzę o sposobie działania klawiatury. Pomysłem autora jest zbudowanie układu pełniącego rolę uniwersalnego klucza przechowującego używane przez nas kody haseł. Czasami może być ich całkiem sporo, począwszy od hasła do naszej skrzynki e-mail, poprzez rozmaite kody dostępu, do niektórych adresów internetowych czy zabezpieczonych programów.

Projekt składa się z miniaturowej stacji-zamka, której schemat pokazano na **rys. 3** oraz klucza z zapisanymi kodami. Kluczem będzie układ i-Buton (pastylka) DALLAS-a, jednego z trzech rodzajów DS1992, DS1993 lub DS1994. Układy te są pamięciami RAM z wewnętrznym podtrzymaniem bateryjnym, komunikujące się z otoczeniem za pomocą magistrali 1-przewodowej MicroLAN i właśnie one będą przechowywały nasze hasła. Stacja-zamek wpięta jest pomiędzy kabel klawiatury a gniazdo klawiatury komputera. Normalnie układ nie ingeruje w działanie klawiatury, której linie danych i zegara, poprzez przekaźnik PK1, doprowadzone są do gniazda klawiatury komputera. Działanie układu składa się z dwóch faz: zapamiętania hasła i jego odtwarzania.

Podsłuchiwanie klawiatury...

Zapamiętanie i wpisanie hasła do pamięci klucza jest możliwe, gdy zwora J1 zostanie rozwarta. Naciskanie przycisku SW1 spowoduje zapalanie się kolejnych diod LED, począwszy od D1 do D6. Świecenie diody oznacza wybranie odpowiadającego jej banku w pamięci klucza. W każdym banku może być zapisane i przechowywane 1 hasło. Maksymalnie układ może zapamiętać 6 haseł o długości 63 bajtów. Jednak w przypadku zastosowania układu DS1992, można skorzystać jedynie z obsługi 2 haseł, co wynika z maksymalnej pojemności pamięci, która w przypadku tego układu wynosi 128 bajtów. Po wybraniu odpowiedniego banku w pamięci klucza i przytrzymaniu naciśniętego przycisku SW1 przez czas dłuższy niż 2s, odpowiednia dioda zaczyna migotać. Po puszczeniu przycisku migotanie diody ustanie i od tej chwili układ znajduje się w fazie rejestracji. Procesor U2 poprzez swoje porty P3.4 i P3.5 kontroluje stan sygnałów na liniach zegarowej i danych. Jeżeli teraz zaczniemy naciskać klawisze klawiatury, procesor po odebraniu transmisji kompletnego kodu wysyłanego z klawiatury zapamięta go w swojej wewnętrznej pamięci. Faza rejestracji i podsłuchiwania przesyłanych kodów może być zakończona w dwóch przypadkach: jeżeli znowu naciśnięty zostanie przycisk SW1 lub gdy procesor odczyta więcej niż 63 kody.

W tym momencie mała uwaga. To, że procesor potrafi zapamiętać 63 bajty nie oznacza, że z tylu znaków może składać się nasze hasło. Przyczyną jest generowanie przez każdy naciskany i puszczany klawisz przynajmniej 3 bajtów (lub więcej). Z tych powodów hasło może się składać z około 20 znaków, wliczając w to naciskanie klawiszy typu CTRL, ALT itp. W przypadku przepełnienia banku pamięci ponad feralne 63 bajty, procesor przerywa rejestrację, ponownie wchodząc w stan nieaktywny.

Jeżeli nie nastąpiło przepełnienie i naciśnięty został przycisk SW1, dioda ponownie zaczyna migotać. Od tej chwili procesor zaprzestaje rejestracji naciśnięć klawiatury, natomiast poprzez złącze JP1 zaczyna badać, czy do magistrali MicroLAN dołączony jest jeden z układów DS199x. Dołączenie do magistrali pastylki innego rodzaju zostanie zignorowane. W przypadku wybrania do zapisu banku o numerze 3 lub większym, dołączenie do magistrali układu DS1992 także zostanie zignorowane. Dopiero w przypadku powodzenia zapisu magistralą MicroLAN dioda gaśnie, a procesor wraca do trybu nieaktywnego. Istnieje także drugi sposób przejścia do trybu nieaktywnego bez zapisu do pamięci klucza, gdy np. pomyliliśmy się przy wpisywaniu hasła. Po prostu wystarczy jeszcze raz nacisnąć przycisk SW1.

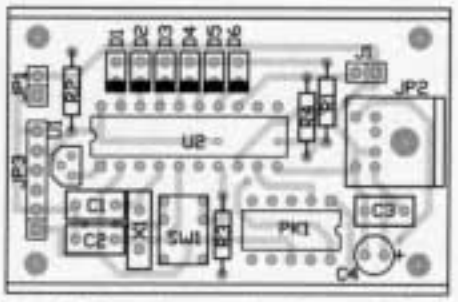
...i oszukiwanie komputera

Odtwarzanie zapisanego w banku pamięci klucza hasła następuje, gdy zwora J1 jest zwarta. Tak jak

w przypadku zapisu, świecenie odpowiedniej diody oznacza wybranie konkretnego banku z zapisanym hasłem. Gdy dioda się świeci, wystarczy złącze JP1 połączyć z odpowiednim układem DS199x. Jeżeli wszystko jest w porządku, procesor przeczyta zawartość pamięci klucza. Następnie przekaźnik PK1 zostaje załączony i od tego momentu układ stacji-zamka „gra" przed komputerem rolę klawiatury. Wygenerowany zostaje odczytany z pamięci kod hasła, po czym przekaźnik ponownie łączy klawiaturę z komputerem, dioda zostaje zgaszona, a procesor układu przechodzi do stanu nieaktywnego. Jeżeli w czasie 60s nie zostanie przeprowadzony pomyślny odczyt banku klucza, dioda zgaśnie, a układ przejdzie samoczynnie do stanu nieaktywnego.

Montaż układu

Cały układ mieści się na niewielkiej płytce dwustronnej o wymiarach 58x38mm (**rys. 4**). Złącze JP2 to gniazdo Mini DIN wlutowane w płytkę. Jeżeli układ będzie współpracował z klawiaturą wyposażoną w duże, 5-stykowe złącze DIN, należy zastosować kabel przejściowy lub zamiast gniazda do odpowiednich wyprowadzeń złącza JP2 dolutować przewody połączone z zewnętrznym dużym gniazdem DIN. Złącze JP3 służy do wlutowania przewodu połączeniowego z komputerem. Można do tego użyć gotowego kabla zakończonego wtyczką pasującą do gniazda klawiatury komputera. Można także wykonać taki kabel samemu, kupując osobno wtyczkę i łącząc ją z odcinkiem przewodu wielożyłowego zgodnie z rozmieszczeniem wyprowadzeń pokazanych na rys. 2. Następnie kabel należy przylutować do płytki. Rozmieszczenie wyprowadzeń sygnałów w złączu JP3 jest następujące:



Rys. 4. Rozmieszczenie elementów na płytce drukowanej.

JP3-1	KBD	Clock
JP3-3	KBD	Data
JP3-5	VCC	
JP3-2,4,6	GND	

W modelu diody sygnalizacyjne i przycisk wlutowane zostały bezpośrednio do płytki. Przy stosowaniu obudowy **(wskazanej ze względu na niebezpieczeństwo przypadkowego zwarcia napięcia +5V podawanego przecież bezpośrednio z komputera)** trzeba przewidzieć, aby elementy te były widoczne, a dostęp do przycisku i zwory J1 był zapewniony. Jako gniazdo dołączane do wyprowadzeń JP1 najlepiej zastosować specjalne gniazdo-port do współpracy z układami DALLAS-a. Montowana tam zwykle dioda sygnalizacyjna nie będzie wykorzystywana.

Uruchomienie i użytkowanie

Po zmontowaniu układu, jego sprawdzenie radzę przeprowadzić bez podłączania do gniazda klawiatury PC-ta. Jeśli w czasie montażu na płytce doszło do zwarć, mogłoby to mieć przykre konsekwencje dla naszego komputera. Dlatego na czas testów do styków 5 i 6 gniazda JP3 należy podać stabilizowane napięcie +5V, a do gniazda JP2 dołączyć klawiaturę. Po włączeniu zasilania klawiatura przeprowadzi własne wewnętrzne zerowanie. Po sprawdzeniu, czy na 20. nóżce procesora jest prawidłowe zasilanie (5V, ±0,25V), można rozłączyć zworę J1 i postępując zgodnie z wcześniejszym opisem zasymulować programowanie klucza. Jeżeli po naciskaniu przycisku SW1 diody zapalają się zgodnie z oczekiwaniem, a po dołączeniu do gniazda JP1 układu klucza gasną, prawdopodobnie układ działa poprawnie. Teraz należy założyć zworę J1, wybrać odpowiedni bank pamięci i dotknąć klucz do portu JP1. Ponieważ zaprogramowane kody wysyłane są do komputera z szybkością ok. 10 na sekundę, przekaźnik powinien się załączyć tylko na chwilę, potem rozłączyć, a dioda zgasnąć. Po takich próbach mamy duże prawdopodobieństwo, że wszystko będzie działać prawidłowo i naszemu komputerowi nic nie grozi. **Wszelkie manipulacje polegające na dołączeniu bądź odłączeniu naszego układu od klawiatury i komputera można dokonywać tylko wtedy, gdy ten ostatni jest wyłączony!** W przeciwnym wypadku komputer może się zawiesić i przestać reagować na naciskanie klawiatury, co zmusi nas do jego wyzerowania poprzez wyłączenie, a w przypadku otwartych okienek nie jest to dopuszczalny sposób zakończenia pracy.

Próbę z programowaniem i odczytem zawartości klucza najlepiej przeprowadzić posługując się jakimś prostym edytorem tekstowym. Zarówno zapisu, jak i odczytu klucza nie należy przeprowadzać w momencie, gdy komputer po włączeniu przeprowadza procedury inicjujące. W takim przypadku dojdzie do zaprogramowania przypadkowych kodów, które będą wprowadzały komputer w błąd albo nasz zdezorientowany układ zakłóci procedurę inicjacji i klawiatura przestanie działać. Znowu trzeba będzie komputer wyłączyć itd. Jeżeli w czasie odczytu zaprogramowanego hasła komputer zaczyna dziwnie się zachowywać, wydaje nieoczekiwane dźwięki, należy cały proces programowania powtórzyć bez pośpiechu naciskając przycisk SW1 i wystukując na klawiaturze odpowiednią sekwencję hasła.

Ryszard Szymaniak, AVT
ryszard.szymaniak@ep.com.pl

WYKAZ ELEMENTÓW

Rezystory
R1, R2: 1kΩ
R3, R4: 10kΩ
Kondensatory
C2, C1: 27pF
C3: 100nF
C4: 100µF/10V
Półprzewodniki
D1..D6: diody LED najlepiej różnokolorowe
U1: MCP101(opis parametrów w tekście) układ resetu firmy MICROCHIP lub podobny
U2: 89C2051(zaprogramowany) układ DS1992
Różne
JP1: gniazdo dla układów DALLAS typu i-Button
JP2: gniazdo Mini DIN do druku
J1: zwora
PK1: przekaźnik typu OMRON +5V z wewnętrzną diodą zabezpieczającą
SW1: przełącznik miniaturowy
X1: kwarc 12MHz

Wzory płytek drukowanych w formacie PDF są dostępne w Internecie pod adresem: ***http://www.ep.com.pl/pcb.html*** *oraz na płycie CD-EP05/2000 w katalogu* ***PCB****.*