|  |  |
| --- | --- |
|  | **TSP91 CZYLI NIEBIESKI URMET**  Widok niebieskiego urmeta, powszechnie znanego aparatu na karty magnetyczne, na dobre wkomponowal sie w krajobraz szarych, polskich miast. Niestety, nasz monopolista dokonal eksterminacji tych, jakze przez nas kochanych, aparatow.  Niebieskie do najnowszych zdobyczy techniki juz od dawna nie naleza i czestokroc znajdowaly sie w oplakanym stanie. Poysl na pomalowanie blachy farba sie nie sprawdzil, kilka lat wystawienia automatu na warunki atmosferyczne fatalnie wplywalo na jego powierzchnie i niebieskie przestawaly byc niebieskie. To i znaczna podatnosc na phreaking sprawily, ze w wielu czesciach kraju zaczely byc one masowo zastepowane jajkami i srebrnymi. Ostatnimi miejscami, gdzie niebieskich pozostalo do konca relatywnie najwiecej zostaly m.in. Poznan i Bydgoszcz. |

**ZAMEK**

|  |  |  |
| --- | --- | --- |
|  |  | Na zdjeciu obok widzimy spod niebieskiego z zamkiem produkcji Abloya. Moze byc to AY1 lub AY3. Po przekreceniu zamka, nie da sie juz klucza wyciagnac. Trzeba z powrotem zamknac zamek i dopiero wtedy odzyskamy klucz. Tak wiec, niestety, nie ma szans, zeby monter zostawil przez pomylke otwarty zamek. Zamek jest przymocowany do pretu (widac go na zdjeciu ponizej), umozliwia poruszanie takze mechanizmu zamykajacego na gorze aparatu. Dzieki temu aparat jest solidnie zamykany zarowno od gory jak i od dolu. |

**BUDOWA WEWNETRZNA**

|  |  |
| --- | --- |
| Zobacz [**wieksze zdjecie**](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\open.jpg) [34KB] | Niebieski sklada sie glownie z plyty glownej, czytnika, klawiatury i wysietlacza 1x16, polaczonych "tasmami" nieco podobnymi do tych w komputerze PC. Co do wartosci tego aparatu mozna bylo slyszec rozne rzeczy. W pewnej gazecie mozna bylo przeczytac, ze sam czytnik wart jest 2000 zl, zas w innej, ze tysiac. Myse, ze mozna spokojnie stwierdzic, ze pojedynczy egzemplarz kosztowal tepse na pewno nie mniej niz 2 tys zl. Duzy wplyw na wartosc ma czas - kiedys niebieskie byly szczytem techniki (nie potrzebowaly zewnetrznego zasilania), potem ich cena musiala zaczac spadac, w koncu zostaly nawet wycofane ze sprzedazy. Dzis dla operatorow telekomunikacyjnych jest to zlom. Tak wiec trudno podac jakas konkretna cene, szczegolnie jesli potrzeba sporzadzic bilnans strat spowodowanych przez phreakerow. No ale znajac tepse, to chetnie podaje najwyzsza cene (pewnie jeszcze z 1991 roku). |

**PLYTA GLOWNA**

Podstawowym skladnikiem kazdego niebieskiego jest **plyta glowna**. Na niej znajduje sie EPROM, procesor, RAM i masa innych czesci elektronicznych. W przeciwienstwie do srebrnego, czesci nie sa montowane powierzchniowo i latwo jest je wylutowac, a potem uzyc do wlasnych celow. Plyte (i wyswietlacz) mozna zobaczyc [**tutaj**](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\mainboard.jpg) **[uwaga: 257KB].** Z plyty na zdjeciu EPROM zostal wyjety, wiec latwo zauwazyc, gdzie on sie normalnie znajduje. Procesor jest zazwyczaj firmy Motorola, chcoc ja widywalem i Toshiby. Ukladem obok EPROMu jest RAM.

W instrukcji do niebieskiego, na stronie 12, sa niescislosci (jak nie bledy) jesli chodzi o rozmieszczenie blokow funkcjonalnych. Kalendarz i aktualna godzina znajduje sie on nad RAMem; DTMF transreceiver o dziwo tez znajduje sie w nieco innym miejscu niz ma niby byc uklad wybierania.

**CZYTNIK**

Czytnik od niebieskiego Urmeta jest dosc ciekawym urzadzeniem. Jego "dziobek" wystaje przez otwor w obudowie. Czytnik wewnatrz posiada beben i karta moze poruszac sie tylko w jedna strone. Dzieki temu istnieja 2 otwory - wejscie i wyjscie, co umozliwia latwe blokowanie kart. W srodku mamy 2 glowice: czytajaca i zapisujaca. Czytnik posiada swoj wlasny EPROM. Warto wspomniec, ze ostatnio tepsa wprowadzac zaczyna nowe czytniki, majace na celu wyeliminowanie (przynajmniej czesci) lewych kart, co najprawdopodobniej oznacza, ze calkowita eksterminacja niebieskich jednak zbyt szybko nie nastapi (czytnik jest najdrozsza czescia aparatu). Nie mniej jednak, ja u siebie z nowymi czytnikami sie nie spotkalem, wiec nie mam co tu o nich pisac. Z tego czytnika mozna "latwo" zrobic nagrywarke. Mozna tez uzyc hybrydki do zczytywania zawartosci karty i sprawdzania, czy jest ladnie nagrana, czy tez moze cos nie gra. [**Tutaj**](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\czytajka.jpg) [109KB] mozna zobaczyc jak wyglada taka odczytywarka. Calosc podlaczamy oczywiscie do karty dzwiekowej PC'ta, gdzie uzywamy np. GoldWave'a do zczytania przebiegu karty. Warto tez troche pogrzebac w opcjach i ustawic sobie glosnosc na odpowiednia wartosc, tak zeby amplituda byla optymalna i wszystko bylo widac jak na dloni.

Zdjecia czytnika: [widok ogolny](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\reader_main-1.jpg) [111KB], [elektronika](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\reader_electro-1.jpg) [236KB], [przod](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\reader_front-1.jpg) [73KB], [tyl](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\reader_back-1.jpg) [107KB], [gora](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\reader_up-1.jpg) [46KB], [spod](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\reader_down-1.jpg) [102KB].

**KLAWIATURA**

Zastosowanie solidnej metody wytapiania cisnieniowego, ktora zostala tez z powodzeniem zastosowana przy obudowie srebrnych oraz chromowania powierzchni, sprawilo, ze klawiaturka jest dosc odporna na to co moze ja spotkac na ulicy. Wystawiona na warunki zewnetrzne na wiele lat, zazwyczaj nie odnosi uszkodzen ani korozji. Wygladem idealnie pasuje do wszelkich domowych projektow jak np. zamki szyfrowe. Zdjecie klawiatury mozna zobaczyc [**tutaj**](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\keyb.jpg) [68KB].

**WYSWIETLACZ**

Zamontowany wyswietlacz cieklokrystaliczny w jednej lini posiada 16 alfanumerycznych znakow. Jego zdjecie z 2 stron zobaczc mozna [**tutaj**](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\LCD.jpg) [38KB].

**OPROGRAMOWANIE EPROM**

W niebieskim latwo dokonac jest wymiany oprogramowania na wlasne lub starsze wersja i tym samym bardziej dziurawe (tzw. downgrade). Mozna tez ponizsze pliki uzyc do bardziej szlachetnych celow zarzucajac je sobie na IDA;) - patrz [narzedzia](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\strona.php-nr=20.htm).

**> plyta glowna <**

Bazuje na procesorze Motorola 68HC11. Piny wychodzace zostaly pozamieniane, wiec aby przestapic do analizy softu trzeba go rozkodowac - jest do tego gotowy program - [urmet.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\urmet.zip) [5,62 KB]. Wiecej o tym mozna poczytac w [ep\_kod.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\ep_kod.zip) [874 B].

Oryginalne pliki:

> [18.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\18.zip) [19,4 KB] - plyta glowna w wersji 1.8  
> [20.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\20.zip) [19,9 KB] - plyta glowna w wersji 2.0  
> [26.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\26.zip) [20,7 KB] - plyta glowna w wersji 2.6  
> [27.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\27.zip) [20,7 KB] - plyta glowna w wersji 2.7  
> [28.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\28.zip) [20,7 KB] - plyta glowna w wersji 2.8  
> [29.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\29.zip) [20,8 KB] - plyta glowna w wersji 2.9  
> [58.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\58.zip) [20,7 KB] - plyta glowna w wersji 5.8  
> [30.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\30.zip) [21,1 KB] - plyta glowna w wersji 3.0

Przerobki:

> [p20\_nol.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\p20_nol.zip) - przerobiony soft 2.0 (darmowe rozmowy na numery 0..., zniesiona blokada niektorych numerow) autorstwa Nola - [40,4 KB]  
> [p29\_nol.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\p29_nol.zip) - przerobiony soft 2.9 - darmowe rozmowy i pelne menu diagnostyczne po otwarciu drzwiczek - autorstwa Nola [42 KB]  
> [m\_28pl.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\m_28pl.zip) - 2.8 z polskim menu serwisowym [20,6 KB]

**> czytnik <**

Bazuje na procesorze Motorola 6805.

> [rd\_25.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\rd_25.zip) [6,4 KB] - czytnik w wersji 2.5  
> [rd\_28.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\rd_28.zip) [6,5 KB] - czytnik w wersji 2.8  
> [rd\_29.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\rd_29.zip) [2,1 KB] - czytnik w wersji 2.9

**C90**

TSP91 jest jednym z aparatow oblugiwanych przez centrum nadzoru c90. Komunikacja z centrum nadzoru bazuje na sygnalach DTMFu, a predkosc transmisji jest niewielka. Z poziomu c90 mozna zmieniac rozmaite ustawienia, numery darmowe i zablokowane, sprawdzac wersja softu, etc.

Aby moglo dojsc do komunikacji z centrum nadzoru, aparat musi miec wpisany numer tego centrum za pomoca karty serwisowej. NIE jest mozliwe, aby centrum nadzoru ot tak zadzwonilo sobie do jakiegos odleglego aparatu i przeprogramowalo go. Tak wiec Hrabia, piszac w swoim tekscie o c90 'lazimy z przenosnym C90 gotowi w kazdej chwili na kazde wezwanie przeprogramowac budke z drugiego konca Polski a nawet z drugiego konca swiata', jak mozna eufemistycznie stwierdzic "wprowadza nas w blad".

NIE DA RADY przeprogramowac jakiegokolwiek aparatu dopoki sie tam fizycznie nie udamy nie nie ustawimy numeru do centrum nadzoru na numer pod ktorym bedzie czekac nasze c90. Hrabia raczej o tym wie, ale przytoczony przeze mnie fragment tekstu zapewne niejednego wywiodl w pole...

- Jednostka panelowa C90 RACK do niej podlaczonych jest 8 linii - [rack.jpg](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\rack.jpg)  
[142 KB]  
- Zrzuty z ekranu: [1](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\1.gif) | [2](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\2.gif) | [3](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\3.gif) | [4](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\4.gif)  
**-** Jednostka obslugowa dla telefonicznych aparatow publicznych - instrukcja  
hardware'owego dodatku do C90 - [instr\_c90.zip](file:///D:\it\IT\PHRACK\phreak\phreaking%20(phreak.it)\instr_c90.zip) [3,12 MB]