1. Darmofon.

Darmofon jest urządzeniem skonstruowanym przeze mnie przypadkowo, podczas próby skonstruowania prostego układu samoczynnie odbierającego przychodzące połączenia telefoniczne. Coś w stylu automatycznej sekretarki.

Odkryłem wówczas, że na centralach elektromechanicznych, zwanych potocznie analogowymi, układ ten powoduje uruchomienie ciekawego mechanizmu pracy centrali telefonicznej.

Otóż układ który skonstruowałem odbiera połączenia, ale połączenia te są dla osoby do mnie dzwoniącej bezpłatne.

Robiłem wiele prób i doskonaliłem urządzenie, choć jego konstrukcja jest bardzo prosta.

Według moich informacji taka praca centrali jaką opisałem nie jest spowodowana błędem w jej konstrukcji, lecz zamierzoną funkcją konstrukcyjną.

Służyła i służy ona do instalowania bezpłatnych zapowiedzi słownych na tych typach central przez operatorów telekomunikacyjnych (tu TPSA) na jednym konkretnym numerze telefonu (np. o zmianie numeru konkretnego abonenta.

Słowo „darmofon” nie zostało wymyślone przeze mnie. Okazało się, że w trakcie eksploatacji tego urządzenia spotkałem osobę, która ma podobne o nieco innej konstrukcji ale spełniające tę samą funkcję. Ta osoba nazywała to urządzenie „darmofonem”. Wiem, że można je spotkać również za granicą ale w krajach położonych na wschód od Polski np. w Rosji, Bułgarii itp. Można to tam kupić na bazarze za 100 dolarów.

Ja, jako że skonstruowałem to sam równolegle do innych, postanowiłem posiadając niejako prawa autorskie do swojej konstrukcji (jest trochę inna niż tamtych urządzeń), opublikować pełny materiał o darmofonie.

W internecie jest już o tym urządzeniu informacja na stronie http://phreak.warsaw.com.pl/poiw grupy phreakerskiej 974, której byłem członkiem jako VIP.

Poniżej zamieszczony jest schemat ideowy darmofonu.

Należy zwrócić uwagę na biegunowość (polaryzację) linii telefonicznej i dołączyć ją zgodnie ze schematem. Polaryzację należy sprawdzać w stanie spoczynkowym linii tzn. wtedy gdy nikt nie rozmawia przez telefon.

Dioda powinna być diodą Schotky’ego i najlepiej o prądzie Imax równym lub większym od 1A.

Kondensator C powinien mieć pojemność 470 nF i być kondensatorem foliowym o napięciu przebicia większym niż 250 V. Rezystor R powinien mieć rezystancję 1 kOhm o dowolnej mocy.

Także biegunowość zasilania darmofonu jest istotna.

Darmofon należy zasilać z zasilacza stabilizowanego (w celu uniknięcia tętnień) o napięciu od 12 do 20 V lub poprzez dwie połączone szeregowo baterie 9V.

Pobór prądu przez darmofon odbywa się tylko w trybie pracy darmowej i jest znikomy (baterie 9V starczają na tydzień pracy przy rozmowach rzędu 10 godzin dziennie !!). Przy rozmowach o normalnej intensywności starczają na pół roku.

Instrukcja obsługi darmofonu:

Należy podłączyć darmofon do linii telefonicznej, do aparatu i do zasilania.

Izostat (przełącznik) bistabilny powinien być wyciśnięty. Po podniesieniu słuchawki powinien być normalny sygnał ciągły.

Gdy wciśniemy izostat w słuchawce zanika sygnał, ale słychać ciche brzęczenie. Tak jest na centralach analogowych Pentaconta i K-66.

Odbieranie połączeń.

Dzwoni telefon. Wciskamy izostat i podnosimy słuchawkę. Po chwili nie dłuższej niż 3 sekundy usłyszymy brzdęknięcie w słuchawce i możemy prowadzić rozmowę z abonentem który do nas zadzwonił. Ten abonent za to połączenie nie płaci. Po skończonej rozmowie najpierw odkładamy słuchawkę a potem wyciskamy izostat.

Gdy zrobimy to w odwrotnej kolejności, czyli wyciśniemy izostat przed położeniem słuchawki lub przed rozłączeniem się rozmówcy to zapłaci on 1 impuls bo nasz aparat przejdzie w tryb pracy normalnej czyli płatnej.

Trzeba pamiętać o wyciśnięciu izostatu po rozmowie, bowiem w przeciwnym wypadku nikt się do nas nie dodzwoni.

Jest pewna trudność w rozmowach. Otóż praca darmofonu polega na tym, iż centrale myślą, że my nie podnieśliśmy słuchawki więc nie zaliczają impulsów naszemu rozmówcy. To jest tak jakby nas nie było w domu i nasz rozmówca gadał z sygnałem wołania.

Niestety centrale telefoniczne mają układy tzw. temporyzacji, czyli funkcje rozłączania połączeń niedoszłych do skutku po upłynięciu paru minut po to aby niepotrzebnie nie zajmować łącz międzycentralowych. I tak czas jednej sesji na darmofonie waha się od 1,5 do 6 minut.

Nie jest to straszne bo po upłynięciu tych 6 minut co prawda centrala nas rozłączy, ale nasz rozmówca powinien połączyć się jeszcze raz urzywając na przykład funkcji redial w swoim telefonie. My po upłynięciu czasu temporyzacji nie musimy odkładać słuchawki ani wyciskać izostatu. Po prostu po zerwaniu połączenia i usłyszeniu brzęczenia spoczynkowego centrali, czekamy ze słuchawką przy uchu na połączenie ponowne. Darmofon sam odbierze za nas połączenie w trybie darmowym i możemy dalej rozmawiać. I tak w nieskończoność aż nam się znudzi rozmowa albo się zmęczymy.

Nasz rozmówca po upłynięciu czasu temporyzacji usłyszy w swoim telefonie sygnał zajętości jeśli jest abonentem sieci stacjonarnej, albo trójtonowy sygnał nieosiągalności jeśli jest abonenetem komórkowym (zobaczy też na wyświetlaczu komunikat : „nie odbiera”).

Pamiętajmy o tym, że nie powinniśmy mieć w domu podłączonych dwóch lub więcej aparatów bowiem jeśli ktoś z rodziny podniesie słuchawkę gdy my rozmawiamy przez darmofon, to naszemu rozmówcy zostanie zaliczony impuls.

A teraz pewien problem. Z darmofonu nie można kożystać gdy dzwoni ktoś do nas z budki telefoicznej, z zagranicy (ale nie z każdego kraju) lub z pewnych aparatów komórkowych w systemie abonamentowym.

Co prawda rozmowa będzie i tak za darmo, ale my nie będziemy słyszeć naszego rozmówcy.

Automaty telefoniczne włączają mikrofon gdy dostaną impuls taryfikacyjny albo gdy dzonimy na numer darmowy znajdujący się na liście numerów bezpłatnych zapisanej w pamięci automatu.

To samo dzieje się gdy dzwonimy z nietórych sieci komórkowych a mamy aparat niektórych firm w systemie abonamentowym. Np. Ericssona w IDEA w abonamencie. Na szczęście taki problem trafia się rzadko. Podobna sytuacja jest w rozmowach przychodzących z innych krajów (najczęściej zachodnich) choć i tu są wyjątki np. nie słychać mojego rozmówcy gdy dzwonił do mnie z Londynu z sieci stacjonarnej i jednej z komórkowych, ale z sieci CELLNET już było go słychać.

Pamiętajmy że nas słychać zawsze i w sytuacji gdy ktoś dzwoni z budki telefonicznej to on może naciskając klawiaturę wysyłać do nas DTMF czyli wybieranie tonowe. Ja zawsze pytałem, gdy miałem taki głuchy telefon na darmofonie : „Jeśli dzwonisz z budki i chcesz rozmawiać to wciśnij dwa razy dwójkę, wtedy rozmowa będzie płatna ale będę cię słyszał”. I gdy dostałem dwa razy ton DTMF lub pstrykanie (jeśli budka chodziła pulsowo) to wysiskałem izostat i rozmawiałem płatnie.

Informacja odnośnie bezpieczeństwa.

Gdy darmofon jest wyłączony (izostat wyciśnięty) wówczas żaden próbnik, miernik czy system nie jest w stanie go wykryć bo faktycznie jest on odłączony i ominięty przez przełącznik.

Natomiast gdy rozmawiamy za darmo, to również wykrycie jest małoprawdopodobne z zewnątrz a prawie niemożliwe na naszej centrali.

W zasadzie obsługa naszej centrali musiała by wiedzieć, że coś takiego mamy, bo żaden układ na centrali automatycznie obsługi o działającym darmofonie nie poinformuje. Musieli by podczas pracy darmofonu włączyć się np. woltomierzem i słuchawką z kondensatorem w szeregu w naszą linię i stwierdzić że jest rozmowa a napięcie jest takie jakby nikt nie rozmaiał. Natomiast na centrali abonenta który do nas dzwoni jest możliwość stwierdzenia nadużycia, ale tylko wówczas gdy robimy wiele sesji darmofonowych na raz (gdy rozmówca dzwoni wiele razy pod rząd)

Wprowadzają teraz taki system zwany fault detection który będzie sygnalizował dziwne zachowanie abonentów. A dziwne jest gdy ktoś do nas dzwoni 50 razy pod rząd a my nie odbieramy telefonu a on za każdym razem czeka na odebranie do końca czyli do temporyzacji.

W zasadzie TPSA nic nie robi w takich przypadkach. Moja obsługa cntrali dzwoniła do mnie w związku z darmofonem ale rozmawialiśmy po przyjacielsku. Dzonił też ktoś z PLUS GSM, bo mój rozmówca rozmawiał ze mną po 10 godzin dziennie w ten sposób, ale dali sobie spokój.

Żadnych sankcji prawnych nie było. Tylko pani z centrali mówiła że to nieładnie i że jej ambicja została poruszona i postara się zbadać jak to działa i uniemożliwić. Niestety nie udało jej się to nigdy. Jest co prawda sposób na to aby to ukrócić 9rozmow będzie zawsze darmowa ale nie będziemy słyszeć rozmówcy), ale operatorzy uważają, że to za duże koszty na tak małe straty. Trzeba by wymienić oprogramowanie na centralach tranzytowych a to kosztuje miliony.

Co to za straty możemy wygenerować w porównaniu z kosztami. Zresztą problem sam się rozwiąże gdy wymienią wszystkie centrale na cyfrowe.

Wracając do prawa. Włączenie darmofonu do sieci jest tylko wykroczeniem. Nie jest przestępstwem tak jak podpinanie się do sąsiada w myśl art. 287 kodeksu karnego.

Za darmofon odpowiadalibyśmy tylko z artykułu zabraniającego włączania do sieci urządzeń bez homologacji.

Jak zatem rozpoznać czy nasza centrala „obsługuje” darmofon ?

W zasadzie w Polsce są trzy typy (a dwa na pewno które obsługują darmofon)

Najbardziej rozpowszechnioną i najpewniejszą bo przetestowaną wielokrotnie jest Pentaconta.

Po czym ją poznać ?

Sygnał po wybraniu zera w telefonie jest taki sam jak po podniesieniu słuchawki (brzmienie).

Co prawda jest też inna centrala co robi to samo a nie jest pentacontą i darmofon by na niej nie działał, ale jest już na wymarciu.

Jest to centrala E10A i w zasadzie działa tylko pod Warszawą (numery zaczynają się od 726 i 727).

Poza tym jeśli mamy numery zaczynające się w Warszawie na 641, 643, 678, 679, 837, 857, 6245, 6246, 6247 to mamy pentacontę i darmofon zadziała. Jest to stan na 1 stycznia 2003 roku i może się zmieniać na minus.

W innych częściach Polski też występują jeszcze pentaconty.

Inną centralą która nas interesuje to K-66.

K-66 ma 60V napięcia przy położonej słuchawce na linii. Poza tym ma dwie marszruty (sygnał marszrutowania) przed sygnałem wołania gdy dzwonimy na jej numer z komórki.

K-66 jest już na wymarciu.

Wiem że jest jakaś w Zgorzelcu.

Te dwie centrale które opisałem zostały przetestowane z darmofonem.

Teoretycznie jeszcze jedna powinna działać, a mianowicie Strowger.

Nie wiem czy jest jeszcze gdzieś w Polsce w sieci TPSA ale na pewno są Strowgery zakładowe np. w Świnoujsciu i są do nich podłączeni prywatni abonenci.

Powodzenia w próbach i wielu godzin miłych darmowych rozmów życzy

VARI

2. Pulse Dialer (metoda na srebrne urmety)

Pulse Dialer jest urządzeniem zaprojektowanym przeze mnie, lecz jeszcze nie sprawdzonym w praktyce. Wszyscy wiemy co to jest Tone Dialer . Otóż pulse dialer spełnia tę samą funkcję co tone dialer w naszych phreakerskich zastosowaniach.

Służy do wybierania numerów w automacie telefonicznym w ... pulsie ! Niektóre linie automatów telefonicznych pracują obecnie tylko z wybieraniem pulsowym. Jak działa taki pulse dialer i czy w ogóle jest to do wykonania ? O tym za chwilę.

Na wstępie teoria wybierania dekadowego czyli pulsowego.

Wybieranie dekadowe to okresowe rozwieranie linii telefonicznej. Czas takiego krótkotrwałego rozwarcia (przerwy), oraz odstęp między przerwami linii są ściśle określone normami telekomunikacyjnymi. Ilość takich następujących po sobie przerw określa wybieraną cyfrę.

Abonent wybierając na przykład cyfrę 8 powoduje pojawienie się na linii ośmiu krótkich rozwarć tej linii. Cyfrze 1 odpowiada jedno rozwarcie, cyfrze 2 , dwa rozwarcia, a cyfrze 0 – dziesięć rozwarć.

W zasadzie między takimi rozwarciami linia telefoniczna powinna być zwarta ale nie jest to koniecznością. Wybieranie pulsowe na obecnie stosowanych centralach działa poprawnie bez całkowitego zwierania linii przed, podczas i krótko po wybieraniu cyfry.

Można założyć (zupełnie poza oficjalnymi normami), że rozwarciu linii odpowiada jej rezystancja większa niż 50 kOhm, jej zwarciu – mniejsza niż 10 Ohm, a stan zamknięcia linii normalną rezystancją aparatu to załóżmy od 100 do 500 Ohm (proszę nie mylić rezystancji z impedancją).

Szczególnie stare aparaty telefoniczne (te z tarczą, choć tarcza nie ma na to wpływu) posiadające mikrofony węglowe odznaczają się dużymi wahaniami rezystancji aparatu. Jest to zależne od rezystancji samego mikrofonu węglowego. Węgiel w tym mikrofonie lubi się „starzeć” oraz „ubijać” podczas wieloletniej eksploatacji aparatu. Objawia się to zniekształceniem odbieranych dzwięków. Gdy mikrotelefonem huknąć w biurko, węgiel się „zamiesza” i jakość audio poprawi się, a i rezystancja się zmieni. Niestety stary węgiel trzeba często „mieszać”.

Ta dygresja miała w zasadzie wyjaśnić odbiegające od normy, ale nie wpływające na poprawność pracy telefonu różnice w rezystancji różnych egzemplarzy telefonów.

A więc do rzeczy.

Jak zbudować pulse dialer i jak z tego zadzwonić, a najlepiej za darmo?

Otóż potrzebne będzie tak zwany kontaktron. Jest to mała szklana rurka ze stykami wśrodku.

Styki te są wrażliwe na pole magnetyczne (np. zwykłego magnesu) i pod jego wpływem stykają się.

Kontaktron można kupić w sklepach z częściami elektronicznymi lub na giełdzie.

Taki kontaktron musimy włączyć w szereg w jedną z żył linii telefonicznej biegnącej do automatu.

Najlepie przykleić kontaktron z tyłu automatu (na ściance wiaty) ale powyżej aparatu np. parę centymetrów, tak aby zbliżenie magnesu położonego na przykład na aparacie (wygoda) zwierało styki (czyli kontaktron musi być tuż z drugiej strony ścianki). Musimy go tak umieścić aby zbliżenie magnesu do np. plastikowej ścianki wiaty na której wisi automat powodowało zwarcie styków.

Bezpośrednio do kontaktronu przyklejamy słaby magnes np. z lodówki (z drzwi) tak aby kontaktron cały czas był zwarty, a rozwierał się pod wpływem zewnętrznego pola magnetycznego.

Tak podrasowany kontaktron przyklejamy w całości do ścianki wiaty z tyłu jak opisałem.

Do kontaktronu przylutowujemy dwa odcinki krótkich przwodów. Zostawiamy je na razie same sobie.

Musimy kontaktron podłączać tak do linii, aby podczas montażu nie spowodować zaniku napięcia linii co automat zinterpretuje jako (całkiem słusznie) odłaczenie od linii. Dobrze było by ściągnąć z jedej z żył izolację na dość dużej powierzchni i zamontowany - przyklejony do ścianki kontaktron z kabelkami podłączyć tuż na skrajach ogołoconej żyły. Przed podłączeniem upewnijmy się omomierzem, że kontaktron jest zwarty. Gdy przylutujemy wiszące kabelki do przygotowanej żyły, możemy tę żyłę rozpiąć. Obecnie obwód jest poprowadzony przez kontaktron,a automat niczego nie zauważył.

Teraz najważniejsze. Sprawdzamy instalację (zamknąwszy blache maskującą tył wiaty budki).

Dzwonimy z komórki na numer budki. Po pierwszym dzwonku rozłączamy się i podnosimy słuchawkę. Mamy dial-tone a po chwili automat wbija swoją literkę i (gdy linia pracuje w DTMF czyli w tonie) dostajemy albo zajęte, albo „Nie ma takiego numeru”.

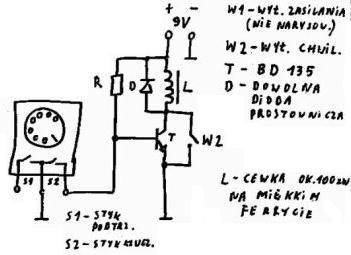
Teraz zbliżamy w znane sobie miejsce nad automatem przyniesiony wcześniej magnes np. z głosnika. Gdy kontaktron się rozłączy, w słuchawce pojawi się cisza. Po odczekaniu ok. sekundy (nie dłużej bo automat zgłosi alarm do STG) odsuwamy magnes. Dostajemy dial-tone. Jeśli linia chodzi w tonie, to możemy za pomocą np. komórki wybrać tonowo numer i rozmawiać za darmo.

Ale to nie jest istota pulse-dialerka.

Ten układ ma zastosowanie tam, gdzie linie chodzą tylko w pulsie !!

I tu dochodzimy do samego pulse-dialera.

Oto jego schemat.



Jak widać jest to bardzo prosty układ. Wykorzystujemy starą tarczę z aparatu telefonicznego, jeden tranzystor i parę innych elementów. Istotna jest też cewka-elektromagnes.

Jak z tego zadzwonić?

Tak jak w przypadku aparatów z linią w tonie, ale nieco inaczej.

Po odebraniu połączenia zainicjowanego z komórki, zbliżamy cewkę do miejsca za którym ukryty jest kontaktronik. Wciskamy na chwilę przycisk W2 po czym odpuszczamy. Spowodowaliśmy tym „położenie i podniesienie słuchawki” dla centrali. Teraz normalnie wybieramy numer tarczą.

Pamiętajmy aby robić co najmniej kilka sekund (do 10) przerwy między cyframi, aby automat nie zinterpretowa wybierania cyfr jako zanik napięcia linii.

Po wybraniu numeru możemy rozmawiać za free.

Gdy nie korzystamy z dialera wyłączajmy zasilanie wyłącznikiem W1 aby nie rozładowywać baterii.

Jak to działa? Tarcza impulsuje swoimi stykami bazę tranzystora, a ten okresowo załącza elektromagnes i rozpina kontaktron w takt impulsów z tarczy. Rozpinający się kontaktronik wybiera cyfry w dekadzie,a rezystancja aparatu jest traktowana jako zamknięcie linii.

Taki sobie pomysł a może pomoże.

vari