

Mieczysław Hucal

TAJNE ŁAMANE PRZEZ POUFNE, CZYLI SPRZET ŁĄCZNOŚCI SPECJALNEJ PO 1945 ROKU

Łączność wojskowa zawsze miała dwa oblicza: jawne i utajnione. O ile o obecnej łączności specjalnej „niewskazane” jest pisanie artykułów do publikacji jawnych, o tyle o łączności utajnionej z poprzedniej epoki możemy nieco napisać.

Po zakończeniu drugiej Wojny Światowej w Wojsku Polskim w procesie utajniania i szyfrowania informacji, zaczęły dominować maszyny szyfrujące produkcji radzieckiej- **Fiałka – M-125** - był to początek lat pięćdziesiątych. W połowie 1965 roku na wyposażenie WP wprowadzono ulepszone odmiany Fiałki o oznaczeniu kodowym M-125-3, które były eksploatowane do chwili wycofania ich z użytkowania w roku 2000.

Każdy członek Układu Warszawskiego posiadał własne odmiany Fiałki, wyposażone we własną klawiaturę oraz głowicę drukującą. Większość maszyn posiadało klawiaturę zawierającą znaki alfabetu łacińskiego i cyrylicę. Zastosowanie znaków cyrylicy czyniło maszynę zdolną do wymiany informacji z każdym członkiem Układu Warszawskiego (kiedy zastosowano takie same zestawy kół szyfrujących).

Urządzenie M-125-3 oferowało trzy tryby pracy: „Kodowanie, Odkodowanie, Zwykły tekst”.



Fialka M-125-3 (zasoby CBSLiI CSLiI)



Zasilacz do M-125-3 /zasoby CBSLiI/

Następnym urządzeniem szyfrującym produkcji radzieckiej opracowanym w latach 60-tych, a wykorzystywanym w Wojsku Polskim była **maszyna M-105**, nazwa

kodowa AGAT. Podobnie jak Fiałka, urządzenie AGAT było na wyposażeniu wszystkich członków Układu Warszawskiego.



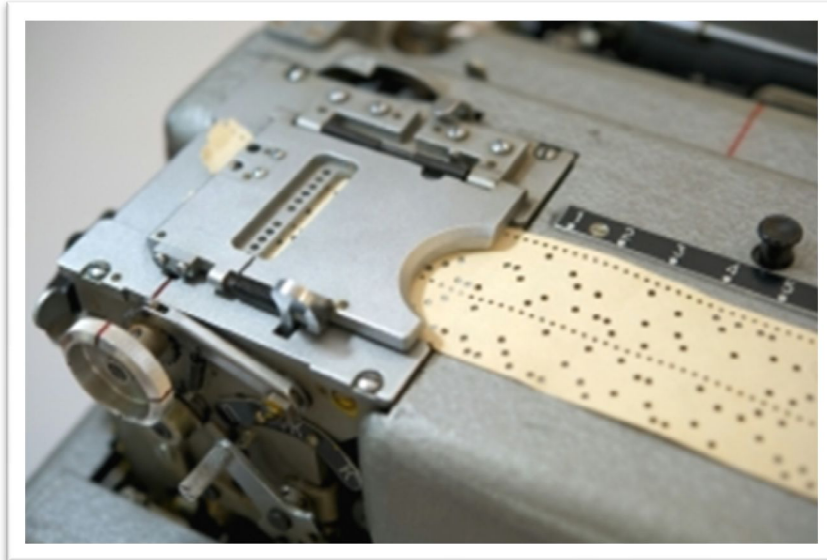
M-105 AGAT (zasoby CBSŁiI CSŁiI)

Klawiatura M-105 AGAT zawierała dwie litery, jedna w kolorze czarnym – cyrylica i w kolorze czerwonym – łacińska. Podczas szyfrowania przycisk spacji jest odblokowywany a przycisk Ъ2 jest zablokowany. W trybie pracy na rozszyfrowanie sytuacja się odwraca. Natomiast podczas pracy w trybie pisania zwykłej informacji (przełącznik trybu pracy ustawionej jest na „O”) do użycia pozostają przycisk spacji oraz przycisk Ъ2 (na zdjęciu zasłonięty metalową płytką). Dwa czarne przyciski nie były wykorzystywane w procesie szyfrowania.



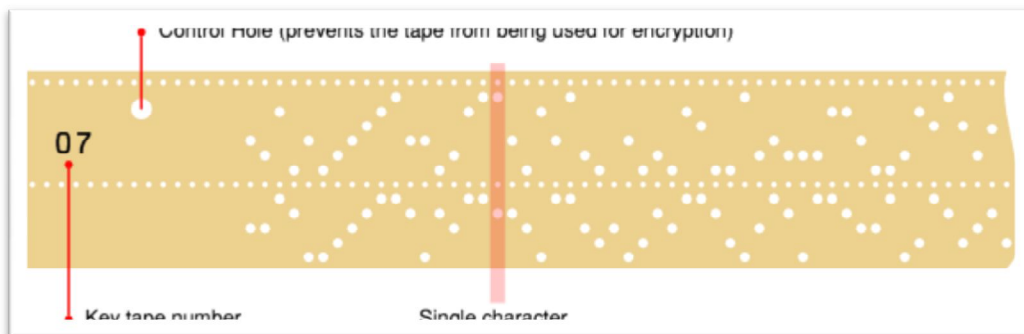
Klawiatura M-105 (zasoby CBSŁiI CSŁiI)

W przeciwieństwie do M-125-3, która wykorzystuje do zaszyfrowania wiadomości 10 kół konfigurowanych elektrycznie (klucz pseudolosowy), M-105 posiadał wbudowany generator klucza mechanicznego.



Czytnik taśmy klucza M-105

Ciekawostką jest to, że taśmę „klucz” można było wykorzystać tylko raz do szyfrowania jednej wiadomości. W tym celu na taśmie wykrawane były otwory kontrolne.



Taśma klucz dla M-105

W użyciu istniały taśmy z kluczem TI indywidualnym, przeznaczone do komunikacji jeden na jeden. Taki zestaw składał się z dwóch taśm: jedna taśma służyła do zaszyfrowania wiadomości a druga do rozszyfrowania. Dokumenty szyfrowe zawierały tabelę składającą się z 20 grup identyfikujących oraz 20 taśm kluczowych. Grupa identyfikująca informowała szyfranta, jaki dokument kryptograficzny został użyty do zaszyfrowania informacji, a jaką otrzymał do rozszyfrowania.

Wysyłano również wiadomości na tzw. „na okólnik”, do tego wykorzystywano trzy taśmy kluczowe lub więcej, w zależności od potrzeb. Oczywiście nie było to bezpieczne (tak jak w kluczu TI), ale pozwalało wysłać jedną ważną informację do wszystkich adresatów jednocześnie. Klucz nosił oznaczenia TIŁ: Grupa. Materiał kryptograficzny dostarczony był w postaci książki kodowej zawierającej tabelę ze wskaźnikami i 25 kluczowych taśm, lub kasety z tabelą wskaźnika i 75 kluczowych taśm.

Tak jak w każdym urządzeniu szyfrującym produkcji rosyjskiej, również i M-105 AGAT posiadał możliwość wyboru trybu pracy. AGAT posiadał trzy możliwości ustawienia trybów pracy:

- „O” - zwykły tekst,
- „3” - szyfrowanie,
- „P” - rozszyfrowanie.

Kolejnym ciekawym urządzeniem szyfrującym skonstruowanym przez inżynierów radzieckich, a wykorzystywanym w wojskach Układu Warszawskiego była meteorologiczna **maszyna szyfrująca M-130 Koral**. Wykorzystywana była do przekazywania zaszyfrowanych informacji pogodowych.



Maszyna szyfrująca M-130 Koral

M-130 Koral podobnie jak poprzednie urządzenia dawał możliwość pracy w trzech różnych trybach:

- Kodowanie „3”,
- Dekodowanie „O”,
- Tekst jawny „P”.

Zaszyfrowany lub rozszyfrowany tekst drukowany był na rolce papieru za pomocą 12 młoteczków, podobnie jak w maszynie do pisania. Młoteczki są sterowane przez zestaw elektromagnesów umiejscowionych z tyłu urządzenia. Ciekawostką jest klawiatura M-130 Koral, która posiada tylko numeryczną klawiaturę bez alfabetu łacińskiego i cyrylicy.

Ustawianie klucza kryptograficznego odbywało się w kilku etapach, w oparciu o dokumenty kluczowe, które zawierały ustawienia kół szyfrujących na kilka tygodni oraz klucze:

- Klucz łątki (plaster),
- Klucz tygodniowy,
- Klucz codzienny.

Można było również wysłać niezaszyfrowane informacje albo zaszyfrowaną wiadomość poprzez kilka M-130 Koral bez jednostki kryptograficznej do adresata właściwego.

Na początku lat sześćdziesiątych w Wielkopolskich Zakładach TELETRA T-7 w Poznaniu oraz Biurze A (Biuro Szyfrów, JW 1919) Ministerstwa Spraw Wewnętrznych PRL została opracowana maszyna szyfrująca TgS-1 DUDEK (dalekopisowe urządzenie do elektronicznego kodowania). Otrzymał on akredytację Ministerstwa Spraw Wewnętrznych do szyfrowania wiadomości o klauzuli Ściśle Tajne. Przystosowany był do pracy z dalekopisami firmy Simens/Ceska T-100.

Urządzenie TgS-1 DUDEK, wykorzystywało funkcję różnicy symetrycznej (XOR) do tworzenia tekstu zaszyfrowanego. Znaki klucza były podawane za pośrednictwem czytników taśm perforowanych. Prędkość urządzenia to około 50-75 bodów na sekundę.

Urządzenie TgS-1 DUDEK wykorzystywane było w czasach PRL w MSW, MO, SB, MON, NBP i MSZ. Również inne armie Układu Warszawskiego używały TgS-1, w tym Ministerstwo Bezpieczeństwa Państwowego NRD (powszechnie zwanego Stasi) jako urządzenia o oznaczeniach T-352 (TgS-1) oraz T-353 (TgS-1M). Urządzenia DUDEK pracowały do upadku NRD. Wschodnie Niemcy posiadały w swoich zasobach aż 1431

urządzeń DUDEK (T-352 i T-353).

W roku 1980 wprowadzono na wyposażenie stacji szyfrowych unowocześnioną konstrukcję DUDKA, był to TgS-3, który różnił się od swojego poprzednika zastosowaniem cyfrowych układów scalonych TTL.

Konstrukcja urządzenia była na tyle dobra, że np. w Polskiej Policji jedno z nich było wykorzystywane aż do stycznia 2011 rok. W Siłach Zbrojnych RP używanie TgS zakończono na początku 2001 roku.



Polskie urządzenie szyfrujące TGS-1 DUDEK

„**ELBRUS-M**” to telefoniczne urządzenie utajniające **T-217M**. Przeznaczone było do automatycznego utajniania rozmów telefonicznych, prowadzonych w łączach dwu- i jednotorowych. Podłączane było do wyjść telefonii wielokrotnej po ich stronie stacyjnej. Urządzenie przewidziane było do pracy również na łączach radioliniowych oraz radiowych krótko- i ultrakrótkofalowych. Czas przygotowania urządzenia do pracy w łączu, włącznie ze zmianą klucza wynosił nie więcej niż 10 minut. Czas wejścia w synchronizm ze współpracującym urządzeniem, po podłączeniu urządzenia do łącza i przy nastawionym kluczu wynosił nie więcej niż 5 sekund.

Telefoniczne urządzenie utajniające **T-219 „JACHTA”** przeznaczone było do automatycznego utajniania simpleksowych i dupleksowych rozmów telefonicznych, prowadzonych poprzez krótkofalowe, ultrakrótkofalowe, radioliniowe i przewodowe kanały

łączności. Urządzenie zmniejszało zrozumiałość wyrazową nie więcej niż 15% w porównaniu ze zrozumiałością wyrazową w traktach rozmównych łączności jawnej. Czas przejścia z łączności jawnej na utajnioną nie przekraczał 3 sekund. Czas niezbędny do zmiany kaset kluczowych w urządzeniu nie przekraczał 3 minut. T-219 wykorzystywane były między innymi na radiostacjach średniej mocy typu R-140 i R-140M.

Urządzenie T207-2M przeznaczone było do przesyłania danych alfanumerycznych przez dwupleksowe kanały telegraficzne z szybkością do 200 bodów. Urządzenie wyposażone było w blok utajniaszący umożliwiający pracę z szyfrowaniem przekazywanych informacji.



Urządzenie T207-2M

Urządzenie UTD-3CT przeznaczone było do przesyłania danych alfanumerycznych przez dwupleksowe kanały telegraficzne z szybkością do 200 bodów oraz półduplexowe kanały telefoniczne z prędkością do 1200 bodów. Urządzenie wyposażone było w blok utajniaszący umożliwiający pracę z szyfrowaniem przekazywanych informacji.



Urządzenie UTD-3CT (bez bloku utajniającego)

Łącznica KTF-15/20M była przeznaczona do ręcznej komutacji dalekosiężnych, telefonicznych łączy przewodowych oraz łączy abonenckich i międzycentralowych.

Pojemność łącznicy stanowiło 40 zespołów liniowych, które były przeznaczone do:

- 15 zespołów KAN do podłączenia dwutorowych łączy dalekosiężnych pracujących w układach zdalnego wybierania lub komutacji ręcznej;
- 5 zespołów CB do podłączenia dwuprzewodowych linii abonenckich;
- 10 zespołów CB 2/4 do podłączenia dwu- lub czteroprzewodowych linii abonenckich CB;
- 8 zespołów CB/MB do podłączenia dwuprzewodowych linii abonenckich CB lub MB;
- 2 zespoły SL do podłączenia linii połączeniowych od innych central telefonicznych systemu CB lub CA, albo linii abonenckich zakończonych telefonicznymi aparatami polowymi.

Łącznica była wyposażona w 13 par sznurowych, z których 9 par służyło do dokonywania połączeń jednotorowych, 2 pary do dokonywania połączeń dwutorowych i 2 pary do włączania w nie strony liniowej urządzenia końcowego lub dokonywania długotrwałych połączeń tranzytowych.

Poniżej charakterystyka aparatowni zapewniających utrzymanie utajnionej łączności telefonicznej.

Aparatownia P-233TM była przeznaczona do organizacji łączności telefonicznej dalekosiężnej w kanałach przewodowych i radioliniowych z wykorzystaniem urządzeń typu T-217M.

Aparatownia zapewniała:

- podłączenie i wyprowadzenie ośmiu dwutorowych łączy dalekosiężnych;
- podłączenie i wyprowadzenie 15 dwuprzewodowych łączy abonenckich CB;
- podłączenie i wyprowadzenie dwóch dwuprzewodowych linii pracujących w systemie MB lub ATS;
- podłączenie i wyprowadzenie na koncentrator telefoniczny pięciu dwuprzewodowych linii służbowych.

Aparatownia zapewniała połączenie abonentów między sobą, dowolnego abonenta z dowolną linią połączeniową (MB, ATS) oraz dowolnego abonenta z łączem dalekosiężnym poprzez urządzenie T-217M.

Aparatownia P-233TM zamontowana była na pojeździe GAZ-63E.



Samochód GAZ-63

Kolejna aparatownia jest mi bliska z osobistych powodów. Moje pierwsze stanowisko służbowe po skończeniu studiów to dowódca plutonu aparatowni ATf-TI w 25 pułku łączności. Oczywiście, że teraz zaprezentowana będzie **aparatownia ATf-TI**. Przeznaczona była do zapewnienia dalekosiężnej łączności telefonicznej i telegraficznej między polowymi stanowiskami dowodzenia związków taktycznych, a także realizacji połączeń abonentów telefonicznych w utajnionym lub nieutajnionym systemie łączności.

W zakresie łączności telefonicznej aparatownia umożliwia:

- realizację czterech łączy dalekosiężnych;
- przyjęcie i zapewnienie komutacji w utajnionym systemie łączności od 1 do 10 telefonicznych łączy dwutorowych oraz od 1 do 20 obwodów abonentów bezpośrednich;
- przyjęcie i zapewnienie komutacji od 1 do 100 telefonicznych łączy jednotorowych lub obwodów abonentów bezpośrednich;
- automatyczne utajnianie przekazywanych informacji telefonicznych jednocześnie w od 1 do 4 określonych łączach telefonicznych;
- przekazywanie 4 łączy telefonicznych do innych aparatowni.

W skład ukończenia zasadniczego w zakresie łączności telefonicznej wchodziły następujące urządzenia:

- cztery telefoniczne urządzenia specjalne,
- łącznica telefoniczna KTF-15/20,
- dwie łącznice telefoniczne ŁP-40MR,
- sześć aparatów telefonicznych MB.

Aparatownia zamontowana była na samochodzie STAR-660.

Ostatnią z prezentowanych aparatowni utajnających będzie **aparatownia P-243**. Aparatownia P-243 była przeznaczona do obsługi sieci telefonicznej.

Zapewniała:

- podłączenie i przekazanie na łącznice wyjść 45 kompletów urządzeń;
- podłączenie i przekazanie na łącznice liniowych wyjść 12 kompletów urządzeń przeznaczonych do podłączenia w parze sznurowej;
- wprowadzenie, zabezpieczenie i przełączenie:

- 30 jednotorowych lub dwutorowych linii abonenckich CB,
- 24 jednotorowych linii abonenckich CB/MB,
- 6 połączeń linii CB/ATS,
- 15 jednotorowych linii abonenckich CB.

Wyposażenie zasadnicze w zakresie łączności telefonicznej:

- 3 łącznice KTF-15/20M,
- aparat telefoniczny TA-57,
- 5 aparatów telefonicznych ATS.

Wyposażenie przewożone oddzielnie:

- 60 aparatów telefonicznych ATS lub CB,
- 12 aparatów telefonicznych TA-57,
- 35 bębnow z kablami różnego typu /PTRK, KRPT, P-274/.

Aparatownia była zamontowana na podwoziu samochodu GAZ-66.



Samochód GAZ-66

Także w zakresie utajniania łączności telegraficznej funkcjonowało szereg aparatowni. Niestety nie udało mi się dotrzeć do materiałów opisujących ich możliwości.

Dla porządku „historycznego” chciałbym chociaż je wymienić:

- Aparatownia telegraficzna utajniana P-227 (P-227M),
- Aparatownia transmisji danych A-1 (A-1M),
- Aparatownia telegraficznych urządzeń utajnianych ATgUU,
- Aparatownia telegraficzna utajniana ATG-S,
- Aparatownia telegraficzna współpracująca ze stacją łączności satelitarnej R-440 (TIC).

W tym miejscu chciałbym podziękować ppłk. Andrzejowi Stefańskiemu, byłemu kierownikowi CBSŁiI CSŁiI za pomoc w opracowaniu tego artykułu.

Więcej informacji o sprzęcie służącym do utajniania informacji i innym można znaleźć na stronie internetowej: <http://www.cryptomuseum.com/>