

K ODOLNOSTI RÁDIOVÉHO SPOJENÍ

1. K pojmu odolnosti spojení

Spojení je hlavním činitelem zabezpečujícího velení vojskům. Proto odolnost velení je závislá do značné míry na odolnosti spojení.

Zkoumáme-li odolnost spojení a prvky odolnosti, pak zavádíme na organizační soustavu systém. Organizační soustava je v našem případě vševojsková armáda, která má určitý počet lidí a techniky. Spojení přispívá k naplnění cílové funkce organizační soustavy. Úkolem spojení je zabezpečit velitele a štábu armády spojení po všech stránkách — jak uvádí Spoj-1-1.

Odolnost spojení je schopnost spojovací soustavy vzdorovat účinkům vnějších a vnitřních rušivých jevů, bez narušení funkce spojení a plnění cílové funkce organizační soustavy.

Rušivých vlivů je velké množství — jako např. nepřítel, vlastní vojska, terén, morálně politická a psychologická úroveň spojovacího vojska, spojovací technika atd. Odolnost proti rádiovému průzkumu je jednou z důležitých stránek celkové odolnosti spojení.

Odolnost proti rádiovému průzkumu můžeme definovat jako schopnost podsystemu rádiového spojení vzdorovat rádiovému průzkumu nepřítele za jakýchkoliv podmínek, nebo jeho průzkumnou činnost ztížit.

2. K rádiovému průzkumu nepřítele

Rádiový průzkum nepřítele je součástí tzv. elektronické války. Otázkám organizace a vedení elektronické války přikládají armády NATO velký význam. Považují ji za důležitý druh bojového a operačního zabezpečení činnosti vojsk a její úspěšné vedení za jednu z rozhodujících podmínek k dosažení úspěchu nejen v jednotlivých operacích, ale i ve válce vůbec, zejména v jejím počátečním období.

Otázky elektronické války rozpracovává

a zabezpečuje nejvíce americká armáda. Dílčí oblasti řeší anglická, západoněmecká a francouzská armáda. Vojenští odborníci NATO předpokládají, že rozvoj nové moderní elektronické techniky a její využití v armádě podstatně zvýší roli elektronické války.

Obsahem elektronické války je veškerá činnost, která směřuje ke snížení účinnosti elektronických zařízení protivníka a k zabezpečení účinnosti a spolehlivosti vlastních spojovacích zařízení. Elektronická válka zahrnuje:

- průzkum radiotechnických prostředků,
- radiotechnické rušení,
- radiotechnické klamání,
- utajení spojení,
- ochranu vlastních radiotechnických zařízení před průzkumem protivníka a zabezpečení jejich spolehlivé činnosti,
- ničení radiotechnických prostředků protivníka.

Důležitost otázek elektronické války je dána i tím, že vývoj organizačních a operačních koncepcí, taktiky i techniky k vedení elektronické války, za přípravu jednotek zodpovídá např. v armádě USA vždy velitel (počínaje velitelem pozemních sil, přes velitele válečnických, velitele skupiny armád a velitele armád). Na jednotlivých stupních jsou k jejímu zabezpečení určeny skupiny odborníků.

Např. v polní armádě je tzv. sekce elektronické války armádního taktického a operačního střediska. Sekce ovlivňuje, koordinuje a řídí veškeré oblasti elektronické války.

Pro rádiový průzkum má polní armáda USA skupinu radiotechnického průzkumu a kontroly. Organizaci skupiny — viz obr. 1.

Prapory radiotechnického průzkumu se přidělují armádním sborům. Roty radiotechnického průzkumu a kontroly se přidělují divizím.

Tabulka 1

Zařízení rádiového průzkumu	Prapor			Prapor 3X	Roty		Celkem skupina
	odřad	rota	prapor		„A“	„B“	
Průzkumné stanoviště KV	2	8	24	72	60	—	132
Průzkumné stanoviště VKV	3	12	36	108	—	45	153

V pásmu nepřátelské polní armády můžeme kalkulovat s prostředky rádiového průzkumu — viz **tabulka 1**.

Kmitočtově je rádiový průzkum veden v pásmu KV od 1,5–18 MHz, v pásmu VKV od 20–230 MHz. Zařízení umožňuje vést průzkum VKV do 40–50 km s využitím pozemních prostředků a do hloubky 400 km při využití leteckých průzkumných prostředků. V pásmu KV povrchovou vlnou 100–200 km ve dne, v noci do 25 km. Odrazenou vlnou do 600 km.

Uvažujeme-li tyto údaje v souvislosti s umísťováním pozemních prostředků rádiového průzkumu nepříteli a vzdálenostmi míst velení naší armády od předního okraje, je dosah prostředků průzkumu — viz **obr. 2**.

Při určitém zjednodušení můžeme říci, že jakýkoliv rádiový provoz v pásmu a hloubce naší armády mohou odposlouchávat nepřátelské průzkumné prostředky. Armáda USA i ostatní státy NATO jsou zabezpečeny velkým množstvím prostředků rádiového průzkumu a překrývají prakticky kmitočtové pásmo, které používají naše rádiové prostředky.

Vedle pozemních jednotek elektronické války jsou v rámci NATO v taktickém a strategickém letectvu speciální letecké jednotky a skupiny elektronické války. Tyto jsou určeny k rádiovému a radiotechnickému rušení a zaměřování. Každá letecká armáda USA má roj elektronické války. Kromě toho je na evropském

válčišti letecké křídlo elektronické války.

V každém armádním sboru armády NSR je předurčen jeden radiotechnický prapor pro průzkum na VKV a KV pásmu.

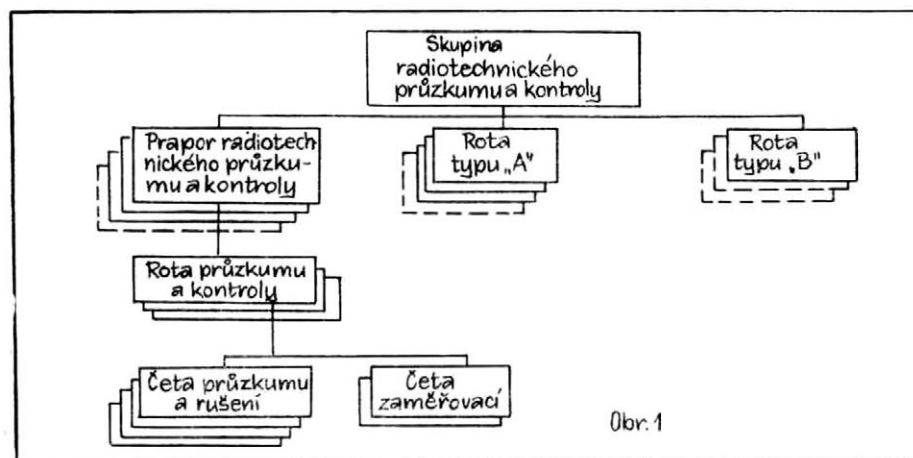
Materiály radiotechnického průzkumu o všech druzích vyzařování se soustřeďují ve středisku radiotechnického průzkumu. K jejich vyhodnocení široce využívají moderní elektronkové počítačové stroje.

Velení USA věnuje též velkou pozornost vývoji kosmických průzkumných prostředků. Průzkumné družice Země umožňují mimo jiné vést rádiový průzkum objektů na území socialistických států. Praktické použití amerických družic pro radiotechnický průzkum započalo v roce 1962 vypuštěním družice FERRER (typu SAMOS). Později to byly typy DISKAVERE a SAMOS. Družice se vypouštějí na oběžnou dráhu do výše 300–500 km.

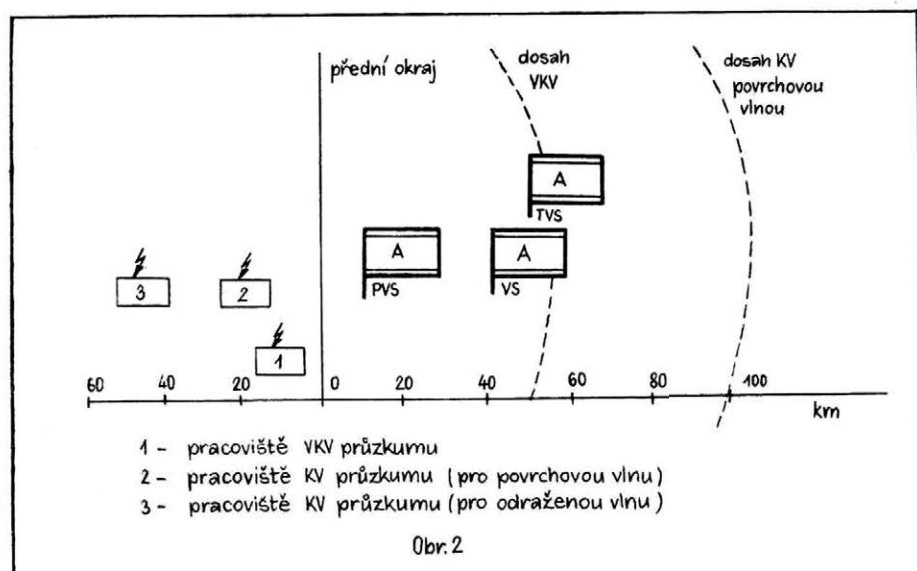
Informace z družice na Zemi se předávají jak pomocí speciálních rádiových kanálů pro předávání zpráv, tak shozem kontejnerů s materiály. Předpokládá se, že bude vytvořen plně automatizovaný systém palubního průzkumného zařízení pro družice.

3. Analýza odolnosti rádiového spojení armády proti rádiovému průzkumu nepříteli

V pásmu vševojskové armády bude při naplnění bojové sestavy a při úplné aktivaci rádiového spojení obsazen počet kmi-



Obr. 1



Obr. 2

točtů podle typů rádiových stanic — viz **tabulka 2**.

Počty sítí a směrů, jakož i typy rádiových stanic odpovídají situaci vševojskové armády v roce 1967. V počtu nejsou zahrnuty prostředky frontu, frontového letectva a teritoriálních orgánů.

Tabulka 2

Typ stanice	Celkem vševojsková armáda
R 102, 118, 830	49
RM 31 Ma	66
RM 31 A (P)	8
R 112	82
RM 33	39
RF 12 M	298
R 113	211
R 109	57
R 108	160
R 105	183
z toho KV	244
VKV	909

Počty kmitočetů nemají nic společného s celkovým počtem kmitočetů, které má armáda a které se přidělují do několika variant rádiových sítí a směrů. Čísla v tabulce 2 určují počet kmitočetů, které budou v dané době obsazeny pojítky. Podle bojové situace nemusí na všech frekvencích probíhat korespondence.

Systém velitelského rádiového spojení se na stupni front - armáda, armáda - vševojsková divize (arb) opírá o rádiové dálkopisné směry. Rádiové dálkopisné směry

jsou svými vnějšími fyzikálními vlastnostmi (výkon, modulace, frekvenční zdvih, stabilita kmitočtu apod.) velmi charakteristické. Navíc provoz probíhá většinou dálkopisem s využitím zařízení pro utajení spojení (ŠD 3, ZAS) a duplexním provozem. Můžeme předpokládat, že zpravodajská služba západních států zná organizaci rádiového dálkopisného spojení na operačním stupni. Bude-li probíhat trvalý provoz na rádiových dálkopisných směrech armády, což bude představovat 12 až 16 duplexních kmitočetů, stanou se jistě tyto spoje cílem rádiového průzkumu nepřítele. Pracovní kmitočty mohou být trvale sledovány, přičemž nepomůže ani eventuální přeladování a změna variant dopravních údajů.

Průzkum bude identifikovat jednotlivé stanice nejen podle rádiových volacích znaků a charakteristických zvyklostí rádiových dálkopisů, ale zejména podle fyzikálních vlastností každé stanice. Tyto spoje budou v průběhu operace zdrojem informací za předpokladu, že se protivníkovi podaří rozšifrovat a rozkódovat vysílaný text, že nebude mít technické problémy odposlechu rádiového dálkopisného provozu a že v místě příjmu bude dostatečně kvalitní signál.

Zbývající KV spoje představují většinou sítě a směry s telegrafním provozem, obsah textu je utajen předšifrováním, kódováním. Je to přibližně 30 kmitočetů stanic R 102, R 118, R 830, provoz F1 (minimální počet s provozem A1) 74 kmitočetů s provozem A1 na typech RM 31 Ma, 82 kmitočetů na R 112 a 39 kmitočetů obsazených stanicemi RM 33.

Na obsazených 244 kmítočtů KV má nepřítel 132 průzkumných pracovišť. Teoreticky by měl možnost odposlouchávat 50 % rádiových sítí a směrů, podaří-li se mu získat dostačující signál na vstupech přijímačů. Z praxe víme, že v polních podmínkách dělá rádiové spojení v některých případech problémy našim spojářům, zejména při provozu v noci, za pohybu, za atmosférických poruch apod.

Zdrojem informace může být doprava fónů na stanicích VKV. Na nižších stupních četa - rota - prapor, i v jiných případech se velí otevřeně. Je to celkem 900 kmítočtů, na které má nepřítel 153 pracovišť průzkumu VKV. Z toho můžeme usuzovat, že teoreticky může sledovat až 17 % VKV spojů. Výhodnější podmínky mu poskytují stanice typu ASTRA, R 113, méně již stanice RF 12, hlavně z důvodů dosahu.

Prosté porovnávání obsazených kmítočtů s pracovišti průzkumu skrývá nebezpečí nereálného přístupu. U nepřítelů uvažujeme, že má v činnosti všechna pracoviště průzkumu. Víme však, že zejména v pohybové fázi operace část prostředků plní úkol, část se přemísťuje, dále vznikají ztráty vlivem činnosti našich vojsk, letectva, ZHN a vlivem poruchovosti techniky a likvidace části sil.

Specifika provozu podle druhu vojsk, podle používání pomůcek utajení a zvláštností provozu je velkým identifikujícím znakem. Jsou to zejména sítě letectva, PVO, dělostřelecké sítě k řízení palby, armádní radiační výstrahy apod.

Pozitivní výsledky rádiového průzkumu jsou základním předpokladem pro

- získání informací o utajovaných skutečnostech,
- zaměření vysílacích míst a z toho odhalení systému rádiového spojení,
- vyhodnocení míst velení,
- rušení provozu a rádiovou diverzi,
- fyzické ničení spojovacích prvků.

Z praktického hlediska nás zajímá dopad činnosti nepřítelů na rádiové spojení na základě výsledků rádiového průzkumu. Z hlediska času pak doba, potřebná od zjištění objektu odposlechu do zahájení přímého vlivu na tento objekt. Tato může být různá. Záleží na výsledcích a zkušenostech průzkumu, na pohotovosti analytiků - operátorů, na stupni využití automatických systémů a samočinných počítaců. Tato doba má náhodný charakter.

Celková doba T_c od zahájení rádiového průzkumu do zahájení přímého působení závisí v obecné rovině na:

$$T_c = T_p + T_{pi} + T_v + T_{vi} + T_{ii}$$

kde T_c je celková doba od zahájení průzkumu do zahájení přímého vlivu,

T_p doba potřebná k zjištění pracovního kmítočtu a doba nutná k sledování provozu postačující k identifikaci důležitosti sítě či směru,

T_{pi} doba potřebná k doručení informace od pracoviště průzkumu na řídící (operační) pracoviště,

T_v doba potřebná k analýze odposlouchaného provozu (rozšifrování, rozkódování) do rozhodnutí o závažnosti rádiové sítě nebo směru až k rozhodnutí o zahájení přímého vlivu,

T_{vi} doba k proniknutí rozkazu o zahájení přímého vlivu k výkonným jednotkám,

T_{ii} doba přípravy k zahájení přímého vlivu, až k dopadu na prvek odolnosti.

V našem příkladu uvažujeme pouze jednu frekvenci. To postačí k zahájení aktivního rušení. K vyhodnocení rádiového vysílače střediska je třeba zaměřeni více vysílačů, vymezit prostor pomocí mapy a vést doplňkový průzkum.

Doplňkový průzkum bude nutný zejména k odhalení míst velení a při jejich ničení klasickými zbraněmi nebo ZHN.

Doba T_c může nabývat různých náhodných hodnot, odhadem řádově desítek minut až hodin. V obecném vzorečku bude největší položku činit čas T_p a T_v . Nepřítel bude mít zájem důležité rádiové sítě a směry raději odposlouchávat než rušit nebo ničit.

Úloha analyzovat odolnost spojení proti rádiovému průzkumu má pravděpodobnostní charakter. S využitím teorie matematické statistiky můžeme řešit některé pravděpodobnostní úlohy:

a) Jaká bude pravděpodobnost, že určitý kmítočet bude zarušen jednotkou elektronické války nepřítel?

$$P(A_1 A_2 A_3) = P_{A_1} \cdot P_{A_2/A_1} \cdot P_{A_3/A_1 A_2}$$

$P(A_1 A_2 A_3)$ pravděpodobnost, že dojde k zarušení kmítočtu,

A_1 jev, že dojde k zjištění pracovního kmítočtu rádiovým průzkumem,

A_2 jev, že budou potvrzeny všechny předpoklady zdůvodňující zarušení frekvence,

A_3 jev, že budou splněny všechny fyzikální podmínky zarušení kmítočtu,

A_2/A_1 závislost jevu A_2 na A_1 ,

$A_3/A_1 A_2$ závislost jevu A_3 na A_1 a A_2 .

b) Tři průzkumná pracoviště mají za úkol zjistit určitou rádiovou síť, pracující na jednom

kmitočtu. Jaká bude pravděpodobnost, že alespoň jeden průzkumný přijímač tuto frekvenci zjistí?

$$P(A) = 1 - (\bar{A}_1 \bar{A}_2 \bar{A}_3)$$

$P(A)$	pravděpodobnost, že alespoň jeden přijímač zjistí hledaný kmitočet,
A_1	jev, že kmitočet zjistí pracoviště č. 1,
A_2	jev, že kmitočet zjistí pracoviště č. 2,
A_3	jev, že kmitočet zjistí pracoviště č. 3.
$\bar{A}_1 \bar{A}_2 \bar{A}_3$	opačný jev k jevům A_1 , A_2 a A_3 .

4. Některé závěry

Odolnost rádiového spojení armády proti rádiovému průzkumu nepřítele má charakter prvku odolnosti proti vnějšímu vlivu. Působení na podsystém rádiového spojení je nepřímé. Až následná činnost nepřítele, která se opírá o výsledky průzkumu, může přímo působit až již rušením, rádiovou diverzí či fyzickým ničením.

Vliv průzkumné činnosti nepřítele je trvalý v míru i ve válce. Prostředky elektronické války nepřítele umožňují trvalý průzkum všech kmitočtových pásem, která používají rádiová pojítka v rámci vševojsové armády. Hlavní rádiové sítě KV a rádiové dálkopisné směry budou sledovány trvale. U VKV spojují do 10—15 % všech rádiových sítí. Limitující je dosah pojítek a počet průzkumných pracovišť, kterými disponuje protivník.

Rádiový průzkum má v porovnání s ostatními druhy průzkumu své zvláštní místo. Na rozdíl od ostatních forem je veden velmi intenzívně a do celé hloubky našeho území již v hlubokém míru. Z informací, které získává nepřátelská zpravodajská služba, tvoří velkou část informace z rádiového průzkumu. Po této stránce má nepřítel již mnoho výsledků, zkušeností a znalostí. Má přehled o typech bezdrátových pojítek a organizačně provozních otázkách rádiového systému armády. Zná fyzikální vlastnosti kanálů pracujících otevřeně i utajeně. Měl možnost v různé míře poznat všechny otázky rádiového i radioreléového spojení armády. To vše dává nepříteli představu o spojení v polních a bojových podmínkách. Zvyšuje se jen nasycenost pojítek a intenzita provozu. Doprava bude zahájena na dopravních údajích, na kterých dosud nebyl nikdy veden provoz.

Všech takto získaných poznatků a zkušeností má možnost nepřítel využít v průběhu operace. Jistě se bude o ně opírat analýza a vyhodnocení nových pracovních kmitočtů a bude na nich závislá i doba od zachycení korespondence — jako nepřímého vlivu, do přímého ovlivnění.

Výhodou rádiového průzkumu je, že lze organizovat z vlastního území. To zvyšuje jeho bezpečnost a spolehlivost.

Zjištění a zaměření zdrojů elektromagnetického záření je spojeno s nebezpečím, že dojde k realizaci dalších druhů průzkumu a po komplexnějším vyhodnocení výsledků i k odhalení míst velení.

Základním druhem spojení u vševojsové armády je rádiové a radioreléové spojení. Využití určitého spojení je závislé na celé řadě činitelů jako je druh bojové činnosti, rozmach operace, použití ZHN, terén apod. Tím budou ovlivněny i výsledky rádiového průzkumu. Mnoho záleží na rozpracování i na dodržování zásad utajeného velení, maskování a zásad provozu.

Možnosti rádiového průzkumu nemůžeme přeceňovat, ale ani podceňovat. Činnost jednotek elektronické války západních států bude probíhat za aktivní činnosti našich i spojeneckých vojsk. Zejména letectva, ZHN, raketových a dělostřeleckých jednotek, za mobilizace všech složek protirádiového a průzkumného vojska.

Prostředky elektronické války budou západní státy dále vyvíjet. Stále více se bude celá činnost automatizovat, od zjišťování zdrojů vysílání, zaznamenání a přenos výsledků průzkumu, uložení do paměti, porovnání a analýza nových výsledků průzkumu. To bude dále rozšiřovat a prohlubovat jeho možnosti. Zvyšovat jeho pohotovost.

Další specifickou stránkou elektronické války je skutečnost, že organizace, počty, technika, metody a výsledky práce jednotek elektronické války jsou předmětem nejvyššího stupně utajení. V dostupných předpisech a publikacích jsou minimální údaje. To co uvádějí je velmi obecné, takticko-technická data prostředků průzkumu, rušení a zaměření neaktuální. Za těchto podmínek je jakákoliv snaha po analýze, porovnání sil v éteru, úvaha o možné variantě působení nepřítele na spojovací soustavu postavena „na písku“, odtržena od pravděpodobné praxe a proto i méně použitelná pro další práci.

Nedostatek informací o našem protivníkovi by mohl vést k podceňování možného dopadu elektronické války na systém našeho velení. Neznalost nepřítele nelze omlouvat. Západní státy (zejména armáda USA) kladou organizační, technické i metodické stránce elektronické války značnou pozornost a vynakládají mnoho sil a prostředků na zefektivnění činnosti jednotek elektronické války. Nevíme-li mnoho o této stránce budoucího protivníka, nijak to nesnižuje nebezpečí, které pro naše velení z toho může plynout.