Generálmajor Ing. Antonín Kutil

ROZVOJ A PERSPEKTIVA UTAJENÍ V ČSLA

Nové politické myšlení má mj. i svůj konkrétní projev v idejích rozumné dostatečnosti výzbroje a společného evropského domu a naprosto logicky se tedy dotýká oblasti kulturní, hospodářské, politické a pochopitelně i vojenské.

Z těchto důvodů jsou zaváděny dříve neznámé normy otevřenosti a vzájemné informovanosti, prověřování a kontroly uzavřených závazků. Inspekční skupina USA navštívila a kontrolovala vícekrát cvičení sovětských vojsk, obdobnou kontrolu uskutečňují ostatní státy NATO i Varšavské smlouvy, jsou zveřejňovány roční plány vojenské činnosti. Sovětský svaz umožnil vojákům a diplomatům ze 45 států světa zúčastnit se výjimečné akce v Šichanech, kde SSSR předvedl vzorky své chemické munice a způsob jejího ničení.

V průběhu vzájemných jednání mezi státy Varšavské smlouvy a NATO byla vyměněna řada vojenských údajů, do té doby utajovaných. Z toho všeho by mohl být vyvozen **nesprávný závěr, že nemáme v rámci členských států Varšavské smlouvy co utajovat**. Naopak se v důsledku nových jevů v mezinárodní vojenskopolitické situaci potvrzuje, že požadavky na utajení neustále rostou. Dochází jen k **určité změně v kvalitě, obsahu utajovaných vojenských skutečností (OUS) a částečně se mění i formy získávání vojenských informací**.

Z pohledu ochrany utajovaných skutečností je zřejmé, že dosavadní normy pro ochranu státního, hospodářského a služebního tajemství **kolidují** s novými politickými přístupy co do rozsahu utajovaných skutečností, důslednosti jejich ochrany i sankcí, které vyplývají z jejich porušení.

Mnohá opatření helsinských závazků i dohod o likvidaci raket středního a kratšího doletu v podstatné míře umožňují rozšířit sběr informací o ČSLA, které doposud byly předmětem utajení.

Současně, s ohledem na technické možnosti dálkového a kosmického průzkumu Země, je žádoucí zaujmout racionálnější postoj k utajování existence objektů na zemském povrchu.

Tyto faktory, spolu se všeobecnou potřebou rozšíření technickoekonomické spolupráce s vyspělými zeměmi západního světa, vedly předsednictvo ÚV KSČ k předložení návrhu Federálnímu ministerstvu vnitra redukovat ve všech resortech skutečnosti tvořící předmět státního, hospodářského a služebního tajemství.

Vývoj a perspektivy oblasti ochrany utajovaných skutečností

Pozitivní změny v mezinárodních vztazích a z nich vyplývající současný trend obecného uvolnění, bezprostředně ovlivní i změny v zákonných normách oblasti utajovaných skutečností v ČSSR s dopadem na oblast utajení v rámci ČSLA. Toto představuje kvalitativně nové, perspektivní zaměření práce ve všech oblastech působnosti 8. oddělení GŠ ČSLA. Změny si již vynutily některé **dílčí úpravy celoarmádních norem**, např. **v oblasti ochrany utajovaných skutečností**. Předně byla novelizována příloha 8 předpisu Všeob-P-70 (práv.) – Cesty do ciziny. Při zpracování bylo využito usnesení PÚV KSČ z 15. ledna 1988, které schválilo výjimky z Pořádku pro stranické schvalování zahraničních cest československých občanů, změny v organizaci a povolování výjezdů do ciziny vydaných Ústřední správou pasů a víz FMV,

kritické připomínky ze stranických jednání i vlastní poznatky 8. oddělení GŠ ČSLA z praktické realizace cest do ciziny. Mezi **hlavní změny**, které byly v rámci novelizace zapracovány, patří rozšíření pravomoci velitelů útvarů a funkcionářů na roveň jim postavených při **povolování soukromých cest do členských států Varšavské smlouvy**, která se nyní vztahuje i na **další vybrané státy, a to MoLR, KLDR, VSR a Kubu**. Dále byla dána pravomoc ředitelům státních podniků v působnosti ČSLA k povolování soukromých cest do ciziny občanským pracovníkům vojenské správy, kteří nejsou nositeli státního tajemství a v neposlední řadě byl snížen rozsah údajů dosud vyžadovaných při hlášení a vyhodnocování soukromých cest.

Na základě usnesení 66. schůze PÚV KSČ je **připravována novelizace** přílohy 5 předpisu Všeob-P-70 (práv.) – **Seznam utajovaných skutečností v oboru působnosti FMNO**. Zde dochází ke značnému snížení stupňů utajení v jednotlivých odborných oblastech utajovaných vojenských informací, a to zejména na stupni útvaru a svazku. Předpokládáme, že **nebudou např. utajovány otevřené názvy vševojskových, leteckých, ale i dalších útvarů a jejich dislokace včetně svazků. Dochází i ke snížení stupně utajení dislokací a otevřených názvů raketových útvarů, útvarů PVO a PVOS.** Na stupni útvaru (mimo útvarů se speciální technikou) nebudou (kromě zvláštních případů) žádné informace tvořit předmět státního tajemství. **Na vyšších stupních velení, zejména svazku**, bude snížen stupeň utajení u řady zpracovávaných informací. Např. proti dosud platnému Seznamu utajovaných skutečností, kdy bylo utajováno téměř 700 druhů vojenských informací stupněm utajení PT-ZD a PT, tedy státním tajemstvím, dojde novelizací k jejich snížení o 1/3. Dosáhneme podstatného snížení okruhu utajovaných informací, čímž následně předpokládáme i zmenšení počtu nositelů státního tajemství, zvláště na stupni útvaru. Jsou tím vytvořeny i lepší podmínky pro ochranu nynějších skutečností charakteru státního tajemství, na druhé straně to umožní v daleko větším rozsahu publikační činnost o životě ČSLA v hromadných sdělovacích prostředcích.

Tyto skutečnosti jsou prozatím výchozím stavem pro další zákonité změny v celé oblasti administrativy a ochrany utajovaných skutečností vůbec. Je jenom otázkou nedaleké budoucnosti, jak se promítnou do dalších norem, které s touto oblastí souvisejí.

Situace si nepochybně vyžádá změnu v postoji k zásadám pro **fotografování a filmování v ČSLA**, a to nejen v zájmu popularizace armády a brannosti v hromadných sdělovacích prostředcích, ale také pro zvyšující se požadavky využít letecké a kosmické snímky pro potřeby národního hospodářství.

Další oblast, která nepochybně dozná změny, má souvislost s pojmem – **zařízení na obranu vlasti**. Jistě bude žádoucí pružněji než doposud vybavovat oprávněné žádosti o povolení vstupu do objektů s tímto statutem, protože při většině vstupů nejsou nepovolané osoby včetně cizinců seznamovány s problematikou, která je předmětem utajení. Často jde o poskytnutí servisních služeb na jejich vlastní výrobky a zařízení. Jsme toho názoru, že velitelé (ředitelé) útvarů a zařízení ČSLA mají dostatek možností, jak ve své pravomoci účinnou ochranu utajovaných skutečností zabezpečit i při oprávněném vstupu nepovolaných osob. Souvisí to i s otázkou posilování nedílné velitelské pravomoci tak, jak odezněla na celoarmádním stranickém aktivu.

Stále citlivým místem ochrany utajovaných skutečností je **problematika zvláštního režimu utajení**, neboť se týká nejmodernější raketové techniky. V souvislosti s tím, co bylo doposud řečeno, je však cítit určitý anachronismus v požadavku nejpřísnějšího utajování objektů, jejichž rozměry jsou několikametrové (vzhledem ke kvalitnímu kosmickému průzkumu). Proto i z této oblasti bude zapotřebí vytypovat informace, které jsou nepodstatné, které lze získat běžně dostupnými formami a legálními zdroji.

V těchto souvislostech se stává aktuální i otázka **novelizace** příloh 6 a 7 předpisu Všeob-P-70 (práv.), které obsahují **zásady ochrany vojenského tajemství v hromadných sdělovacích prostředcích** a vymezují přehled skutečností v oboru působnosti FMNO, jež je možné v tisku uveřejňovat.

Jsou jistě i další oblasti OUS, které budeme muset upravit, jako např. otázky **soukromého styku** rodinných příslušníků vojáků v činné službě a občanských pracovníků s cizinou a otázky **spisové a archívní služby** v souvislosti s adresováním zásilek při používání otevřených názvů útvarů.

Na všechny tyto podněty však v rámci ČSLA můžeme reagovat až poté, kdy budeme znát definitivní podobu nového Zákona o ochraně státního tajemství.

Tyto změny se však **nedotknou zavedených zásad pro ochranu utajovaných informací a pro výběr i výchovu osob určených pro styk s utajovanými skutečnostmi.** Jestliže přistoupíme (a v některých případech jsme již přistoupili) na snížení množství utajovaných skutečností, neznamená to, že omezíme nároky na osvědčené zásady jejich ochrany zejména na výběr a výchovu nositelů, kteří v systému OUS doposud tvoří nejslabší článek.

Naším hlavním cílem je při zužování rozsahu ochrany utajovaných skutečností zabezpečit důslednost v kontrolní činnosti a vyšší kvalitu v dodržování norem ochrany utajovaných skutečností v ČSLA.

Základní problémy ochrany informací v ASVŘ

V souvislosti s řešením otázek kvality OUS bude mít novou polohu i oblast technické ochrany nejdůležitějších míst velení, řízení a zpracovávání informací.

V současné době prudce narůstá nasazení výpočetní techniky, která pracuje v automatizovaném systému velení a řízení (ASVŘ) a v jeho rámci dochází k vysoké koncentraci chráněných informací a dat. Podle stupně velení nabývají informace v nich zpracovávané různých úrovní důležitosti, stupňů utajení a od nich odvozujeme požadavky na ochranu. Pokud hovoříme o ochraně dat, je tím myšleno vytvoření takových zábran, které ve svém komplexním působení znemožňují neoprávněně proniknout k utajované informaci s cílem ji zničit nebo zneužít nepovolanou osobou. Zničení informace nebo její kompromitace může nastat úmyslným jednáním, ale i z nedbalosti.

Jedním z principů bezpečnosti je zajištění důležitých míst velení, řízení a zpracování informací (štáby, velitelská stanoviště, počítače, terminály spojovací sítě apod.) fyzickými prostředky ochrany. Jde o **zabezpečení budov, místností, archívů médií, technických prostředků, napájecích a sdělovacích tras takovým způsobem, aby případný pokus narušitele byl včas zpozorován a signalizován.** Tato opatření spolu s organizací režimu v zabezpečovaném objektu vytvářejí první dvě základní překážky, které musí narušitel překonat. Dalšími bezpečnostními opatřeními jsou technické prostředky identifikace osob a detekce neoprávněného přístupu nebo zásahu. Nedílnou součástí komplexního bezpečnostního systému jsou logické bariéry realizované speciálními programovými prostředky, které umožňují regulovat a kontrolovat přístup k chráněným informacím, tvořit, ověřovat a rozdělovat hesla, vést záznamy o jejich využívání a další speciální funkce.

Jedním, v současné době vysoce aktuálním způsobem získávání utajovaných informací, je **zachycování** (odposlech) **elektromagnetického vyzařování** doprovázejícího činnost elektronických zařízení. Jde zejména o ta zařízení komerčního provedení, která nejsou pro zpracování utajovaných informací již svou konstrukcí uzpůsobena. K ochraně přenášených dat po spojovacích kanálech, kde obdobně dochází k vyzařování, jsou pro dálkový přenos dat používány šifrovací prostředky. Složitější situace nastává při zabezpečování informace při **přenosu dat v lokálních sítích** uvnitř VpS, VS nebo v rámci budovy, kdy zpravidla použití šifrovacích prostředků by bylo vzhledem k nákladům nerealizovatelné. K odvrácení této možnosti kompromitace přenášených dat používáme komplexu speciálních metod a technických prostředků. Tato opatření jsou také poměrně investičně, technicky a provozně náročná a jejich použití je nutné zvažovat v souvislosti s důležitostí chráněného objektu a zpracovávaných informací. **Jde zejména o:**

- elektromagnetické odstínění místností, kde je instalován počítač, terminály a přídavná zařízení,
- použití optoelektronických systémů přenosu dat, mikropočítačů ve funkci terminálů s inteligencí,
- programové zabezpečení přístupu a kódování dat.

Většina počítačových řídících a informačních systémů je velice zranitelná a neexistuje absolutně dokonalá metoda jejich ochrany. K hranici dokonalosti se lze přiblížit vhodnou kombinací různých metod, přitom je však třeba respektovat požadavek, aby systém zabezpečení jen

na nejnutnější míru omezoval práci systému a jeho účinnost (je uváděno snížení účinnosti asi o 20 % při vyšších stupních zabezpečení). To však vyžaduje, aby se touto problematikou zabýval k tomu určený pracovní kolektiv odborníků z oblasti operačních systémů, programování a technických prostředků a v neposlední řadě také z problematiky OUS s aplikací na ASVŘ.

V souladu s rozvojem automatizovaného systému velení a řízení není oblast obraně technických opatření (OTO) omezována pouze na technická opatření a prostředky, ale sleduje další zkvalitňování systému ochrany informací tak, jak se rozšiřuje i spektrum jejich ohrožení. Především jsou zkoumány a ověřovány systémové ochrany datových bází mírových i polních ASVŘ a obdobně je přistupováno k řešení problematiky terminálových a počítačových sítí.

Požadavky efektivnosti a vysokého stupně ochrany jsou sledovány při naplňování všech možností, které současné naše poznání, technika a technologie dovolují. Stranou nezůstává oblast preventivně výchovné, normotvorné a kontrolní činnosti.

V dalším období **zaměříme pozornost** v oblasti OTO jednak na prohlubování účinnosti již realizovaných opatření a metod ochrany utajovaných skutečností a na ověřování i postupné zavádění systémových a programových prostředků i metod ochrany terminálových, počítačových systémů a datových bází na úrovni nejnovějších vědeckotechnických poznatků. Cílem je postupně vybudovat ucelený, komplexně působící **bezpečnostní systém** ochrany informací a dat v ASVŘ ČSLA. K tomu jsou postupně zadávány požadavky na výzkum, vývoj a výrobu technických prostředků odpovídající kvality pro zpracování utajovaných informací, výzkum a ověřování systémového a programového zabezpečení, k čemuž směřuje i postupná příprava kvalifikovaných kádrů pro správu datových bází a bezpečnostních systémů.

Vývoj a perspektiva šifrové služby

Šifrová služba v ČSLA byla organizována zpočátku jen v rámci zpravodajských orgánů. Začátkem padesátých let byl vytvořen samostatný šifrový orgán (šifrové oddělení) u FMNO/GŠ ČSLA a na ostatních stupních velení včetně svazků (divize, brigáda). (U ZS/GŠ zůstal jen luštitelský orgán, ale v roce 1955 byl ustaven opět šifrový orgán k zabezpečení šifrového spojení v síti ZS/GŠ.)

Začátkem šedesátých let jsou ustaveny šifrové orgány (důstojníci pro speciální spojení) i u útvarů (pluků), které však byly během dvou let (u útvarů v rámci vševojskových divizí) zrušeny.

Šifrové oddělení plnilo tyto **hlavní úkoly**:

– zabezpečení šifrového spojení pro celé štáby, včetně zpravodajských orgánů, u GŠ i se zahraničními zastupitelstvími (používaly se ruční prostředky šifrování vyvinuté na generálním štábu – s omezenou a postupně i nekonečně náhodnou klíčovou dokumentací),

– zajišťování pomůcek kódového spojení (utajené velení) pro štáby a školení s těmito pomůckami,

– kontrolu ochrany utajovaných skutečností včetně manipulace s vojenskými písemnostmi (na vydávání norem na tomto úseku se šifrové oddělení GŠ jen podílelo – garantem byl sekretariát NGŠ); od poloviny padesátých let se na šifrové oddělení přesunuly postupně povinnosti v normotvorné činnosti na úseku OUS a vojenské cenzury,

– u FMNO/GŠ byl rovněž zajišťován vývoj technických prostředků šifrování, který po přechodu technické skupiny k FMV v roce 1955 postupně vyústil v dokončení vývoje a zahájení výroby šifrovacího dálnopisu ŠD-3 (začátkem šedesátých let).

Šifrovací stroj ŠD-3 byl v té době jediným technickým prostředkem zajišťujícím utajení informací přenášených technickými prostředky. Na základě toho se jich u šifrových orgánů začalo využívat nejen k ochraně přenášených informací charakteru státního tajemství, ale i informací nižších stupňů utajení. Šifrová oddělení tak začala plnit prakticky úkoly utajeného spojení.

Tento trend přetrvává do dnešní doby i přes zavádění nových prostředků přenosu informací s utajovacími zařízeními se zaručenou odolností utajeného spojení (dovážená zařízení ZAS, Interier a zařízení z tuzemské výroby – Páska, Modast, MOMI). Příčiny jsou v návycích štábů

a jejich zkušenostech, že odesílání informací při velení a řízení vojsk prostřednictvím šifrových orgánů zajišťuje jak jejich utajení, tak nejspolehlivější pronikání. Tyto nové prostředky utajeného spojení však přes některé své přednosti (zejména rychlost přenosu při použití prostředků typu Páska) dosud takovéto potřeby štábů plně nezabezpečují. Je to způsobeno jednak omezeným rozsahem jejich zavedení v ČSLA, nižší provozní spolehlivostí a rovněž nedořešeností přípravy informací k přenosu (kromě informací připravovaných pomocí převozných minipočítačů MOMI, které zabezpečují i jejich automatický přenos).

Přesto je nutné předpokládat, že rozšiřování použití technických prostředků utajeného spojení přinese zvýšení jejich provozní spolehlivosti, vyžádá si řešení přípravy informací v systémech velení a řízení, čímž budou zlepšeny i podmínky pro plnění požadavků štábů zajišťovat na vyšší úrovni, než v současné době šifrové spojení uskutečňované příslušnými orgány. Je však zapotřebí vidět, že přechod na takovéto uspokojování požadavků štábů je možné zajistit jen postupně. Nadále je proto nutné zkvalitňovat práci šifrových orgánů zdokonalováním šifrovacích prostředků. Tento úkol je zdůrazněn i skutečností, že šifrovému spojení je přikládán velký význam i v rámci součinnostního spojení mezi štáby armád členských států Varšavské smlouvy.

Současně je nezbytné sledovat rozvoj utajeného spojení, ovlivňovat jeho správnou funkci dodávkami klíčové dokumentace a dohledem (kontrolou) nad dodržováním stanovených zásad pro ochranu v utajeném spojení, včetně ochrany přenášených informací. Tato funkce šifrových orgánů bude narůstat v souladu s rozvojem utajeného spojení na úkor vlastních šifrových prací a bude nutné zajišťovat jejich potřebnou přípravu v tomto směru.

I v rámci **rozvoje šifrovacích prostředků** je potřebné zvažovat předpokládaný a realizovaný růst prostředků utajeného spojení. Je nutné počítat i s předpokladem, že na základě rozšíření prostředků a organizace utajeného spojení budou sníženy požadavky na šifrování informací (jen zvlášť stanovený jejich okruh charakteru státního tajemství nebo informace jednotlivě stanovené velitelem, náčelníkem). Na základě toho je pak možné vyvodit závěr, že je nevyhnutelné zabezpečit pro šifrové orgány speciální **šifrovací zařízení nového typu**. Mělo by zajistit zašifrování a předání informace na přenosový prostředek (utajeného nebo neutajeného spojení) a naopak na médiu, které bude využíváno přenosovými prostředky.

Vývoj a perspektivy kódového spojení

Úkolem kódového spojení je společně s ostatními druhy utajeného spojení (šifrovým, ZAS aj.) zabezpečit ochranu utajovaných informací při jejich předávání pojítky.

Zatím co šifrové spojení, které je základním druhem utajeného spojení v ČSLA, je určeno především k ochraně přísně tajných informací, **kódové spojení** je používáno převážně k ochraně informací, které tvoří **předmět služebního tajemství** (tajných) **a informací určených výhradně pro služební potřebu**. Požadavky na zabezpečení ochrany kódového spojení odpovídající charakteru kódovaných informací jsou méně náročné, než požadavky na ochranu šifrového spojení.

Pro kódové spojení používáme kódovací stroje sovětské výroby, tabulky kódového spojení (kódové, hovorové a signální) a systémy kódování map.

Prostředky kódového spojení mají z uživatelského hlediska tyto **přednosti**:

- umožňují rychlé předávání krátkých zpráv (stručných nařízení a hlášení),
- operativním způsobem je možné kódovat údaje z formalizované dokumentace, zvláště číselné údaje,
- lze jimi organizovat směrové, oběžníkové, ale i vzájemné kódové spojení,
- uživateli prostředků kódového spojení mohou být vojáci z povolání, zpracovatelé zpráv, vojáci základní služby i občanští pracovníci (nároky z hlediska výběru a přípravy kádrů jsou menší než na obsluhy šifrovací techniky),
- pořizovací náklady na prostředky kódového spojení jsou většinou nízké,
- některé tabulky tohoto spojení a údaje pro kódování map je možné podle potřeby poměrně snadno a rychle zhotovovat vlastními silami, prostředky štábů svazků a útvarů i v polních podmínkách.

K **nedostatkům** prostředků kódového spojení je možné zařadit:
- nevhodnost pro kódování obsažnějších zpráv,
- operativnost jen při možnosti přenosu informací z děrné pásky,
- složitost (v některých případech) sítí kódového spojení,
- omezení počtu uživatelů tabulek v sítích kódového spojení s ohledem na zabezpečení kryptologické odolnosti kódogramů,
- ohraničenost délky a počtu zpráv, které lze kódovat podle jednoho nastavení směnných prvků, tj. potřeba časté výměny směnných prvků tabulek,
- nutnost zabezpečení ochrany kódového spojení a velká spotřeba směnných prvků (způsobují problémy s vytvářením, skladováním a vyvážením zásob prostředků),
- složitost (poměrná) evidence prostředků kódového spojení (mnoho položek).

Kódové spojení je v ČSLA používáno v širokém měřítku zejména na taktických stupních velení a jako doplňkový druh utajeného spojení i na operačních stupních. Jsou organizovány sítě a směry vnitřního i součinnostního kódového spojení.

Rozvoj kódového spojení je orientován na zdokonalování prostředků kódového spojení a na jeho organizaci.

V roce 1988 byl **ukončen vývoj přídavného zařízení** ke kódovacímu stroji, které umožňuje operativní předávání kódogramů linkovými i rádiovými pojítky a vytváří z technického hlediska optimální podmínky pro používání zavedené kódovací techniky k zabezpečení činnosti vojsk v poli.

Osmé oddělení GŠ se bude přímo podílet na řešení otázek umístění i obsluhy kódovacích strojů s přídavným zařízením při práci štábů vševojskových svazků a útvarů v poli.

Směnné prvky k tabulkám kódového spojení jsou připravovány na počítačích. V předchozích letech bylo úspěšně vyřešeno využití automatizované tiskárenské sazby. V roce 1988 byl používaný projekt rozšířen o další úlohy a je zpracován ideový projekt pro **automatizovanou tvorbu tabulek** kódového spojení na počítači EC-1045.

Kódové spojení je organizováno se zřetelem na požadavek zamezení případnému úniku utajovaných informací na neutajených spojovacích kanálech. Nové sítě a směry kódového spojení organizují (podle potřeby) štáby v rámci své působnosti.

Možnosti, které skýtá kódové spojení pro zabezpečení utajeného velení vojskům, nejsou ještě vyčerpány.

V současné době jsou vytvářeny základní předpoklady pro uskutečnění rozhodující **kvalitativní změny v kódovém spojení** – nahrazení většiny používaných tabulek malým kódovacím zařízením Katka, které odstraní většinu nedostatků prostředků kódového spojení a bude výrazným přínosem pro práci štábů.

Jednou z hlavních metod dodržování zásad bdělosti a ostražitosti, zachování vojenského tajemství je zvyšování politického uvědomění, vedení příslušníků ČSLA k náročnému plnění ustanovení vojenských řádů a požadavek uvědomělé vojenské kázně. Přitom neméně důležitým prvkem je propracovaný systém ochrany utajovaných skutečností, který odpovídá kvalitativně novým podmínkám, včetně optimálního využívání moderní utajovací techniky.

Zvláštní pozornost je zapotřebí věnovat úsilí západních rozvědek a špionážních center o získání informací o utajovaných skutečnostech, jež souvisejí s upevňováním obranyschopnosti země. **Všichni bychom měli znát formy a metody činnosti nepřátelských rozvědek.** Nemalý význam mají **znalosti základních právních norem a předpisů upravujících systém ochrany utajovaných skutečností**, zejména přílohy 7 a 6 předpisu Všeob-P-70 (práv.).

Ve výchovné práci má nezastupitelné místo velitel, náčelník, nejbližší vychovatel vojáků. Svoji úlohu musí mít v preventivně výchovné činnosti nejen při školeních, ale i v osobním příkladě a přijímání opatření pro zamezení úniku utajovaných skutečností. Zpravidla bývá rozhodujícím činitelem, který ovlivňuje úroveň právní výchovy a tím znalost vojáků. Je nutné, aby byl na to sám všestranně připraven. Musí osobně dbát na dodržování stanovených norem utajení. Je zodpovědný za správné pochopení úlohy a místa každého vojáka podle funkčního zařazení v systému ochrany utajovaných skutečností. Téze V. I. Lenin O nutnosti nepřetržité bdělosti jako hlavní vlastnosti, kterou si musí osvojit všichni pracující, je pro nás nevyčerpatelným zdrojem trvalého poučení.