

Ochrana utajovaných informací

1 Utajované informace

1.1 Právní úprava ochrany utajovaných informací

Ochranu utajovaných informací upravuje **zák. č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti** (dále jen „zákon“) a prováděcí předpisy k tomuto zákonu. Jedná se o **nařízení vlády č. 522/2005 Sb.**, kterým se stanoví seznamy utajovaných informací, **vyhlášku č. 523/2005 Sb.**, o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor **vyhlášku č. 524/2005 Sb.**, o zajištění kryptografické ochrany utajovaných informací, **vyhlášku č. 525/2005 Sb.**, o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, **vyhlášku č. 526/2005 Sb.**, o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti), **vyhlášku č. 527/2005 Sb.**, o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti), **vyhlášku č. 528/2005 Sb.**, o fyzické bezpečnosti a certifikaci technických prostředků a o **vyhlášku č. 529/2005 Sb.**, o administrativní bezpečnosti a o registrech utajovaných informací.

1.2 Klasifikace utajovaných informací

Informace a data, se kterými se setkáváme nejen v rámci Hasičského záchranného sboru ČR, ale v rámci celé státní správy, lze rozdělit do dvou základních skupin, a to neutajované informace a utajované informace. V této souvislosti je nezbytné upozornit na skutečnost, že i neutajované informace jsou ve vymezených případech určitým způsobem chráněny a jejich manipulace podléhá různým režimům ochrany. Do této kategorie patří skutečnosti, na které se váže povinnost mlčenlivosti (v podmínkách Hasičského záchranného sboru je tato povinnost stanovena v § 19 zák. č. 238/2000 Sb.), ochrana osobních údajů ve smyslu zák. č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů a zvláštní skutečnosti ve smyslu zák. č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů. Pro přehlednost se uvádí tabulka tohoto členění:

Utajované informace	Neutajované informace
Přísně tajné	Neklasifikované <i>Nepodléhají žádné ochraně</i>
Tajné	Skutečnosti, na které se vztahuje <u>povinnost mlčenlivosti</u>
Důvěrné	Osobní údaje Chráněné dle zák. č. 101/2000 Sb., o ochraně osobních údajů
Vyhrazené	Zvláštní skutečnosti Chráněné dle zák. č. 240/2000 Sb., krizový zákon

Bylo by tedy základním omylem domnívat se, že je nutné chránit pouze utajované informace a ostatní skutečnosti žádnou ochranu nevyžadují. Toto členění je uvedeno pro základní orientaci v problematice ochrany s tím, že není předmětem tohoto materiálu podrobně rozebírat způsoby a systém ochrany neutajovaných informací, což je oblast značně složitá a zasluhuje si samostatný rozbor.

Předmětem tohoto studijního materiálu jsou utajované informace, a proto se budeme věnovat v dalších částech výhradně utajovaným informacím.

1.3 Utajovaná informace

Utajovanou informací je informace v jakémkoliv podobě zaznamenaná na jakémkoliv nosiči, označená v souladu se zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací. Návrh seznamů utajovaných informací zpracovává Národní bezpečnostní úřad. Seznam utajovaných informací vydá vláda svým nařízením. Zájmem České republiky se rozumí zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob. Újmou zájmu České republiky se ve smyslu zákona rozumí poškození nebo ohrožení zájmu České republiky. Podle závažnosti poškození nebo ohrožení zájmu České republiky se újma člení na mimořádně vážnou újmu, vážnou újmu a prostou újmu.

Utajované informace se na základě možné způsobené újmy či nevýhodnosti zájmům České republiky klasifikují do stupňů utajení:

- **Přísně tajné** - do tohoto stupně utajení se utajovaná informace klasifikuje v případě, jestliže její vyzrazení neoprávněně osobě nebo zneužití může způsobit mimořádně vážnou újmu zájmům České republiky,
- **Tajné** - do tohoto stupně utajení se utajovaná informace klasifikuje v případě, jestliže

její vyjádření neoprávněné osobě nebo zneužití může způsobit vážnou újmu zájmům České republiky,

- **Důvěrné** - do tohoto stupně utajení se utajovaná informace klasifikuje v případě, jestliže její vyjádření neoprávněné osobě nebo zneužití může způsobit prostou újmu zájmům České republiky,
- **Vyhrazené** - do tohoto stupně utajení se utajovaná informace klasifikuje v případě, jestliže její vyjádření neoprávněné osobě nebo zneužití může být nevýhodné pro zájmy České republiky.

Do uvedených stupňů se rovněž klasifikují utajované informace cizí moci poskytnuté České republice cizí mocí nebo utajované informace cizí moci, k jejichž ochraně se Česká republika zavázala.

Mimořádně vážná újma zájmu České republiky vznikne vyjádřením utajované informace neoprávněné osobě nebo zneužitím utajované informace, které může mít za následek

- a) bezprostřední ohrožení svrchovanosti, územní celistvosti nebo demokratických základů České republiky,
- b) rozsáhlé ztráty na lidských životech nebo rozsáhlé ohrožení zdraví obyvatel,
- c) mimořádně vážné nebo dlouhodobé poškození ekonomiky České republiky,
- d) značné narušení vnitřního pořádku a bezpečnosti České republiky,
- e) mimořádně vážné ohrožení významných bezpečnostních operací nebo činnosti zpravodajských služeb,
- f) mimořádně vážné ohrožení činnosti nebo existence Organizace Severoatlantické smlouvy, Evropské unie nebo členského státu,
- g) mimořádně vážné ohrožení bojové schopnosti ozbrojených sil České republiky, Organizace Severoatlantické smlouvy nebo jejího členského státu nebo členského státu Evropské unie, nebo
- h) mimořádně vážné poškození diplomatických nebo jiných vztahů České republiky k Organizací Severoatlantické smlouvy, Evropské unii nebo členskému státu.

Vážná újma zájmu České republiky vznikne vyjádřením utajované informace neoprávněné osobě nebo zneužitím utajované informace, které může mít za následek

- a) ohrožení svrchovanosti, územní celistvosti a demokratických základů České republiky,
- b) značnou škodu České republiky ve finanční, měnové nebo hospodářské oblasti,
- c) ztráty na lidských životech nebo ohrožení zdraví obyvatel,
- d) narušení vnitřního pořádku a bezpečnosti České republiky,
- e) vážné ohrožení bojové schopnosti ozbrojených sil České republiky, Organizace Severoatlantické smlouvy nebo jejího členského státu nebo členského státu Evropské unie,
- f) vážné ohrožení významných bezpečnostních operací nebo činnosti zpravodajských služeb,
- g) vážné ohrožení činnosti Organizace Severoatlantické smlouvy, Evropské unie nebo členského státu,
- h) vážné narušení diplomatických vztahů České republiky k Organizací Severoatlantické smlouvy, Evropské unii nebo členskému státu nebo jinému státu, nebo

- i) vážné zvýšení mezinárodního napětí.

Prostá újma zájmu České republiky vznikne vyzrazením utajované informace neoprávněné osobě nebo zneužitím utajované informace, které může mít za následek

- a) zhoršení vztahů České republiky s cizí mocí,
- b) ohrožení bezpečnosti jednotlivce,
- c) ohrožení bojeschopnosti ozbrojených sil České republiky, Organizace Severoatlantické smlouvy nebo jejího členského státu nebo členského státu Evropské unie,
- d) ohrožení bezpečnostních operací nebo činnosti zpravodajských služeb,
- e) ohrožení činnosti či existence Evropské unie nebo jejího členského státu,
- f) zmaření, ztížení anebo ohrožení prověřování nebo vyšetřování zvláště závažných trestných činů (viz § 41 odst. 2 trestního zákona) nebo usnadnění jejich páčání,
- g) vznik nezanedbatelné škody České republice, nebo
- h) závažné narušení ekonomických zájmů České republiky.

Nevýhodné pro zájmy České republiky je vyzrazení utajované informace neoprávněné osobě nebo zneužití utajované informace, které může mít za následek

- a) narušení činnosti ozbrojených sil České republiky, Organizace Severoatlantické smlouvy nebo jejího členského státu nebo členského státu Evropské unie,
- b) zmaření, ztížení anebo ohrožení prověřování nebo vyšetřování ostatních trestných činů než uvedených v odstavci 4 písm. f) nebo usnadnění jejich páčání,
- c) poškození významných ekonomických zájmů České republiky nebo Evropské unie nebo jejího členského státu,
- d) narušení důležitých obchodních nebo politických jednání České republiky s cizí mocí, nebo
- e) narušení bezpečnostních nebo zpravodajských operací.

Pro obor působnosti Hasičského záchranného sboru ČR je předpoklad zpracovávání utajovaných informací stupně utajení Vyhrazené, popřípadě Důvěrné. Vyšší stupně utajení mohou být poskytnuty pouze ve výjimečných případech a pro vymezené funkce.

Utajované informace **jsou vždy v dokumentové formě, tj. fixované na materiálním nosiči**. Používáme pro ně termín utajované písemnosti, resp. utajované dokumenty, jež zahrnuje všechny listiny, nosná media (zejména média prostředků výpočetní techniky) a jiné materiály, obsahující utajované informace vyjádřené v jakékoli podobě (tzn. nejen materiály v grafické podobě, jako je text na papíru, popřípadě nákres, ale i v podobě audiovizuální, jako jsou audio a video záznamy, popřípadě v podobě fotografické, jako jsou fotografie, mikrofilmy, mikrofiše či diapozitivy).

Příslušný stupeň utajení stanoví nebo mění původce, který zároveň zodpovídá za jeho správnost. Při stanovování stupně utajení se posuzuje každý nově vznikající dokument nebo jeho část samostatně. Skládá-li se utajovaný dokument z více částí, stanoví se stupeň utajení podle části s nejvyšším stupněm utajení.

Na utajovanou informaci je původce povinen vyznačit svůj název (název útvaru), stupeň jejího utajení, její evidenční označení a datum jejího vzniku. Na utajované informaci poskytnuté České

republike cizí mocí vyznačí orgán státu, pokud tuto utajovanou informaci eviduje jako první, stupeň utajení, a to v souladu s mezinárodní smlouvou, kterou je Česká republika vázána a na jejímž základě je utajovaná informace poskytována, včetně případné zkratky podle této smlouvy (například zkratka „EU“, „EURA“ nebo „NATO“), nebo v souladu s požadavkem cizí moci anebo se stupněm utajení cizí moci na poskytnuté utajované informaci vyznačeným. Název původce a datum vzniku utajované informace se v těchto případech nevyznačuje. Na utajované informaci, která vyžaduje zpřísněné podmínky při zajišťování jednotlivých druhů ochrany utajovaných informací v oblastech stanovených zejména mezinárodní smlouvou, kterou je Česká republika vázána, nebo předpisy mezinárodní organizace, jíž je Česká republika členem, se vyznačí též příslušné doplňující označení (například označení „KRYPTO“, jde-li o utajovanou informaci z oblasti kryptografické ochrany, popřípadě označení „ATOMAL“, jde-li o utajovanou informaci z oblasti zbraní hromadného ničení). Nelze-li na uvedené údaje vyznačit přímo na nosič, vyznačí se jiným vhodným způsobem.

Utajovaná informace se eviduje v administrativních pomůckách určených prováděcím právním předpisem (vyhláška č. 529/2005 Sb.). Na nich se zaznamenává též její předávání, přebírání nebo jiný pohyb. Opis, kopie nebo překlad utajované informace stupně utajení Přísně tajné nebo výpis z ní mohou být vyhotoveny pouze na základě písemného souhlasu původce; jde-li o utajovanou informaci stupně utajení Tajné nebo Důvěrné, mohou být vyhotoveny pouze s písemným souhlasem přímo nadřízené osoby. Utajovanou informaci lze přepravovat nebo přenášet pouze v přenosných schránkách nebo v uzavřeném obalu v závislosti na jejím stupni utajení a na jejím nosiči; přepravovat ji lze pouze prostřednictvím kurýrní služby nebo držitele poštovní licence. Převzetí utajované informace příjemce potvrdí. Formu potvrzení při převzetí utajované informace stupně utajení Vyhrazené v rámci orgánu státu stanoví odpovědná osoba. V podmínkách Ministerstva vnitra je stanovena odpovědnou osobou (tj. ministrem vnitra) forma potvrzení při převzetí utajované informace stupně utajení Vyhrazené vždy oproti podpisu (to platí pro generální ředitelství Hasičského záchranného sboru České republiky). Formu potvrzení při převzetí utajované informace stupně utajení Vyhrazené v rámci (tj. uvnitř) jednotlivých hasičských záchranných sborů krajů stanoví odpovědná osoba, kterou je ve smyslu zákona ředitel příslušného hasičského záchranného sboru kraje.

Utajovanou informaci lze v průběhu její skartační lhůty, stanovené podle zvláštního právního předpisu (zák. č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů), zapůjčit pouze fyzickým osobám, které jsou k orgánu státu ve služebním poměru nebo v pracovněprávním či obdobném vztahu. Při vyřazování utajované informace ve skartačním řízení se postupuje podle příslušného skartačního řádu.

Stupeň utajení se na utajované informaci vyznačí při jejím vzniku. Vyznačení stupně utajení na utajované informaci musí být zachováno po celou dobu trvání důvodů utajení. Bez souhlasu původce nebo poskytující cizí moci nesmí být stupeň utajení změněn nebo zrušen. Vyžaduje-li to charakter utajované informace, musí původce vyznačit na utajované informaci dobu, po kterou bude informace utajována; stupeň utajení zaniká uplynutím vyznačené doby. Stupeň utajení původce neprodleně zruší nebo změní po zjištění, že pominul důvod pro utajení informace, důvody pro utajení neodpovídají stanovenému stupni utajení nebo byl-li stupeň utajení stanoven neoprávněně a na utajované informaci toto zrušení nebo změnu jejího stupně utajení vyznačí. Původce je povinen prověřit, zda důvod pro utajení informace trvá, a to nejméně jednou za pět let ode dne jejího vzniku. Provedl-li původce zrušení nebo změnu stupně utajení, oznámí tuto

skutečnost neprodleně písemně adresátům utajované informace. Adresáti utajované informace oznámí neprodleně písemně tuto skutečnost všem dalším adresátům, kterým utajovanou informaci předali. Adresát po obdržení oznámení o zrušení nebo změně stupně utajení na utajované informaci zrušení nebo změnu stupně utajení vyznačí.

1.4 Utajované informace v rámci Evropské unie a Severoatlantické aliance

V souvislosti s členstvím České republiky v Evropské unii a v Severoatlantické alianci dochází k vzájemné výměně utajovaných informací v rámci uvedených společenství. Vzhledem k tomu, že naše národní zásady a principy ochrany utajovaných informací jsou plně kompatibilní se zásadami a principy ostatních mezinárodních subjektů, jsou požadavky na ochranu těchto utajovaných informací obdobné a pomocí stanovených jazykových ekvivalentů jsou jim při jejich doručení do České republiky přidělovány odpovídající stupně utajení. Na tyto utajované informace, s výjimkou utajovaných informací stupně utajení Vyhrazené, jsou uplatňovány pouze odlišné požadavky na jejich evidenci a ukládání s tím, že se utajované informace vzniklé v rámci Evropské unie a Severoatlantické aliance evidují odděleně do samostatných evidenčních pomůcek a ukládají se odděleně od ostatních utajovaných informací. V této souvislosti se dá do budoucna předpokládat stále se zvyšující počet vzájemně poskytovaných utajovaných informací.

1.5 Povinnosti při ochraně utajovaných informací

1.5.1 Výkon státní správy

Národní bezpečnostní úřad (dále jen „Úřad“) je ústřední správní úřad pro oblast ochrany utajovaných informací a bezpečnostní způsobilosti a vykonává státní správu v oblasti utajovaných informací. Ve své činnosti se Úřad řídí zákonem. Úřad zejména zajišťuje jednotné provádění ochrany utajovaných informací v České republice, vykonává státní dozor a metodickou činnost, vede ústřední registry utajovaných informací poskytovaných v rámci mezinárodních styků a plní úkoly v souladu se závazky vyplývajícími z členství České republiky v Evropské unii, NATO a z mezinárodních smluv, jimiž je Česká republika vázána v oblasti ochrany utajovaných informací. Provádí bezpečnostní řízení a vykonává státní dozor. V rozsahu stanoveném platnou právní úpravou rozhoduje o vydání osvědčení fyzické osoby a vydání dokladu o zrušení platnosti osvědčení fyzické osoby. Současně rozhoduje v dalších věcech a plní další úkoly na úseku ochrany utajovaných informací a bezpečnostní způsobilosti stanovené zákonem.

1.5.2 Odpovědnost za ochranu utajovaných informací

Za ochranu utajovaných informací u Ministerstva vnitra (včetně generálního ředitelství Hasičského záchranného sboru České republiky a Policie České republiky) odpovídá **odpovědná osoba**, tj. ministr vnitra. Ministr vnitra ve smyslu zákona pověřil plněním svých povinností bezpečnostního ředitele Ministerstva vnitra (tím je v rámci organizace Ministerstva vnitra ředitel bezpečnostního odboru). **Bezpečnostní odbor** v této souvislosti plní funkci odborného útvaru ochrany utajovaných informací pro rozsah působnosti Ministerstvo vnitra, tzn. i pro generální

ředitelství Hasičského záchranného sboru České republiky. Z hlediska své působnosti zajišťuje jednotné provádění ochrany utajovaných informací, analyzuje stav ochrany utajovaných informací, navrhuje ministru vnitra příslušná opatření, koordinuje aplikaci druhů ochrany utajovaných informací, zpracovává zprávu o stavu ochrany utajovaných informací za kalendářní rok za rozsah působnosti Ministerstva vnitra a předkládá ji ministru vnitra ke schválení. V oblasti ochrany utajovaných informací spolupracuje s Úřadem, podílí se na šetření příčin porušení ochrany utajovaných informací, organizuje a ve vymezeném rozsahu provádí preventivní opatření a kontrolní činnost na úseku ochrany utajovaných informací.

Jiná situace je u hasičských záchranných sborů krajů. U těchto útvarů **je odpovědnou osobou** ve smyslu zákona ředitel hasičského záchranného sboru kraje, kterému zákon dává možnost buď zřídit a obsadit funkci bezpečnostního ředitele, který zajišťuje a plní povinnosti stanovené mu písemně odpovědnou osobou v rozsahu zákona, nebo mohou funkci bezpečnostního ředitele vykonávat ředitelé hasičského záchranného sboru krajů sami (viz § 71 zákona). Funkci bezpečnostního ředitele nelze vykonávat u více orgánů státu souběžně.

Ředitelé hasičských záchranných sborů krajů v rámci dané působnosti odpovídají za ochranu utajovaných informací na řízeném úseku a k tomu jsou zejména povinni vytvářet podmínky pro zabezpečení ochrany utajovaných informací, kontrolovat dodržování ochrany utajovaných informací, přijímat opatření při zjištění porušení povinností k ochraně utajovaných informací, zabezpečit, aby všichni podřízení zaměstnanci a příslušníci hasičského záchranného sboru byli seznámeni nejméně jednou ročně s předpisy upravujícími ochranu utajovaných informací a s povinnostmi a omezeními v rozsahu jejich služebního nebo pracovního zařazení, projednat nejméně jednou ročně stav a úroveň ochrany utajovaných informací a zpracovat přehled funkcí a pracovních míst, u kterých je nezbytné seznamovat se s utajovanými informacemi a tento přehled zpracovat do systemizace pracovních míst.

U generálního ředitelství Hasičského záchranného sboru České republiky, které je součástí Ministerstva vnitra, se zřizuje odborné pracoviště ochrany utajovaných informací. Toto pracoviště zajišťuje a plní opatření na úseku ochrany utajovaných informací u útvaru a zabezpečuje praktický výkon ochrany utajovaných informací v daném rozsahu.

1.5.3 Povinnosti fyzických osob

S utajovanými informacemi se mohou seznamovat osoby, které podle zákona mají přístup k utajované informaci. Podmínky, které musí tyto osoby splňovat, jsou podrobně rozebrány v části týkající se personální bezpečnosti. Pro **fyzické osoby**, které mají přístup k utajované informaci, stanoví platná právní úprava základní povinnosti, kterými jsou:

- dodržovat povinnosti při ochraně utajovaných informací,
- odevzdat tomu, kdo osvědčení fyzické osoby vydal, do 5 dnů své osvědčení fyzické osoby, jehož platnost zanikla jinak než uplynutím doby platnosti
- neprodleně písemně oznámit tomu, kdo osvědčení fyzické osoby nebo osvědčení fyzické osoby pro cizí moc vydal, ztrátu nebo odcizení svého osvědčení fyzické osoby nebo osvědčení fyzické osoby pro cizí moc a neprodleně odevzdat neplatné osvědčení pro cizí moc,
- neprodleně oznámit Úřadu změny údajů, které byly uvedeny v její žádosti fyzické

- osoby v podkladových materiálech pro bezpečnostní řízení,
- neprodleně oznamovat tomu, kdo provedl její poučení, porušení povinností stanovených zákonem,
- účastnit se pravidelného ročního proškolení.

V souvislosti s ochranou utajovaných informací stanoví platná právní úprava obecné povinnosti všem fyzickým osobám, to znamená, že:

- každý je povinen neprodleně odevzdat nalezenou utajovanou informaci nebo utajovanou informaci získanou v rozporu se zákonem anebo osvědčení fyzické osoby, osvědčení podnikatele, osvědčení fyzické osoby pro cizí moc nebo osvědčení podnikatele pro cizí moc Úřadu, policii nebo zastupitelskému úřadu České republiky,
- každý, kdo měl nebo má přístup k utajované informaci, je povinen zachovávat o ní mlčenlivost a nesmí k ní umožnit přístup neoprávněné osobě,
- každý, kdo podal žádost podle § 94 zákona, je povinen neprodleně oznámit Úřadu změny údajů, které jsou v ní uvedeny,
- každý je povinen při výkonu státní kontroly Úřadem plnit pokyny kontrolního pracovníka při provádění neodkladných opatření podle § 144 odst. 1 zákona.

1.6 Druhy ochrany utajovaných informací

Ochrana utajovaných informací je zajišťována

- personální bezpečností, kterou tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana,
- průmyslovou bezpečností, kterou tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu se zákonem (v podmínkách Ministerstva vnitra a Hasičského záchranného sboru ČR se neaplikuje),
- administrativní bezpečností, kterou tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi,
- fyzickou bezpečností, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat,
- bezpečností informačních nebo komunikačních systémů, kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému a
- kryptografickou ochranou, kterou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací.

1.6.1 Personální bezpečnost

Personální bezpečnost je jedním z druhů ochrany utajovaných informací. Vychází se ze zásady, že možnost seznamovat se s utajovanou informací nemůže být pojímána jako nárokový faktor.

Vzhledem k tomu, že se jedná o informace, jejichž ochrana je pojmána ve vztahu k zájmům České republiky, je samozřejmé, že je v zájmu České republiky, aby byly stanoveny takové podmínky, které dávají garance, že utajované informace budou zpřístupňovány osobám, které splňují zákonem stanovené podmínky a současně splňují podmínky osobnostní a bezpečnostní spolehlivosti. Skutečnost, že zákon stanoví podmínky pro seznamování osob s utajovanými informacemi, znamená provedení volby a výběru mezi možnými kandidáty. Zákon proto stanoví kritéria, podle nichž se tento výběr vhodných osob provádí, resp. podle nichž se provádí vyloučení osob nevhodných. Stanovení těchto kritérií je možné samozřejmě pouze právním předpisem. Je v souladu s principem svobodné volby povolání, aby každý jedinec sám rozhodl, zda je ochoten umožnit orgánu státu, aby o jeho vhodnosti či naopak nevhodnosti ve vztahu k přístupu k utajovaným informacím rozhodl. Osoby, které požadují od orgánu státu vydání osvědčení, se dobrovolně rozhodly vykonávat takové povolání nebo zastávat takovou funkci, u níž je nutný přístup k utajované informaci. Proto musí splňovat podmínky, které zákon pro přístup k utajovaným informacím stanoví.

V tomto smyslu se s utajovanými informacemi může seznamovat pouze fyzická osoba, která je nezbytně nutně potřebuje k výkonu své funkce (zásada „need to know“), pracovní nebo jiné činnosti, je držitelem platného oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené (dále jen „oznámení“) nebo platného osvědčení fyzické osoby vydané Úřadem a je poučena. Tato osoba je oprávněna seznamovat se s utajovanými informacemi do příslušného stupně utajení.

1.6.2 Podmínky pro vydání oznámení o splnění podmínek přístupu k utajované informaci stupně utajení Vyhrazené

Pro stupeň utajení Vyhrazené splňuje podmínky pro vydání oznámení osoba, která je způsobilá k právním úkonům v plném rozsahu, dosáhla alespoň 18 let věku a je bezúhonná (bezúhonnost se posuzuje podle výpisu z Rejstříku trestů a znamená, že osoba nebyla pravomocně odsouzena za spáchání úmyslného trestného činu nebo trestného činu vztahujícího se k ochraně utajovaných informací).

Ten, kdo je vůči fyzické osobě v rámci služebního poměru nebo pracovněprávního, členského či obdobného vztahu osobou odpovědnou, zajistí její poučení před jejím prvním přístupem k utajované informaci stupně utajení Vyhrazené. Jde-li o fyzickou osobu, vůči níž není odpovědná osoba podle věty první, zajistí poučení odpovědná osoba toho, kdo přístup k utajované informaci umožní. Poučení podepisuje fyzická osoba a ten, kdo poučení provedl, jeden výtisk poučení jí předá a jeden výtisk uloží.

Ten, kdo vydal oznámení, je povinen každé 3 roky ode dne jeho vydání ověřovat splnění uvedených podmínek.

Platnost oznámení zaniká

- doručením písemného vyrozumění toho, kdo oznámení vydal, že fyzická osoba přestala splňovat podmínky pro vydání osvědčení,
- skončením služebního poměru nebo pracovněprávního, členského či obdobného vztahu, ve kterém byl fyzické osobě umožněn přístup k utajovaným informacím,
- vznikem služebního poměru nebo pracovněprávního, členského či obdobného vztahu,

- ve kterém má být fyzické osobě umožněn přístup k utajovaným informacím, pokud oznámení vydal Úřad,
- úmrtím nebo prohlášením osoby za mrtvou,
 - odcizením nebo ztrátou,
 - takovým poškozením, že zápisy v něm uvedené jsou nečitelné nebo je porušena jeho celistvost, nebo
 - doručením písemného vyrozumění toho, kdo oznámení vydal, že fyzická osoba nespĺnila ve stanovené lhůtě povinnost doručit ve stanovené tříleté lhůtě výpis z evidence Rejstříku trestů a prohlášení fyzické osoby o způsobilosti k právním úkonům.

Při zániku platnosti oznámení je fyzická osoba povinna odevzdat oznámení do 5 dnů tomu, kdo oznámení vydal.

Podmínky pro přístup musí fyzická osoba, která je držitelem oznámení, splňovat po celou dobu přístupu k utajované informaci stupně utajení Vyhrazené. Fyzická osoba je v této souvislosti povinna písemně sdělovat tomu, kdo vydal oznámení, změnu týkající se těchto podmínek a dále změnu údajů, které se v oznámení uvádějí, a to ve lhůtě 5 dnů ode dne, kdy tato změna nastala. V případech ověřování splnění podmínek každé 3 roky, je osoba povinna předložit ve stanovené lhůtě na žádost toho, kdo vydal oznámení, výpis z evidence Rejstříku trestů a prohlášení fyzické osoby o způsobilosti k právním úkonům; tyto doklady nesmějí být starší než 3 měsíce.

1.6.3 Podmínky pro vydání osvědčení fyzické osoby pro stupně utajení Důvěrné, Tajné nebo Přísně tajné

Pro stupeň utajení Důvěrné, Tajné nebo Přísně tajné splňuje podmínky pro vydání osvědčení osoba, která je státním občanem České republiky nebo státním občanem členského státu Evropské unie nebo NATO, splňuje podmínky stanovené pro stupeň utajení Vyhrazené, je osobnostně způsobilá a je bezpečnostně spolehlivá. Tyto podmínky musí fyzická osoba splňovat po celou dobu platnosti osvědčení fyzické osoby.

Podmínku **osobnostní způsobilosti** splňuje fyzická osoba, která netrpí poruchou či obtížemi, které mohou mít vliv na její spolehlivost nebo schopnost utajovat informace. Osobnostní způsobilost se ověřuje na základě prohlášení k osobnostní způsobilosti a v případech stanovených zákonem (tj. pro stupeň utajení Přísně tajné a v případech, kdy se zjistí skutečnost vyvolávající pochybnost o osobnostní způsobilosti) i na základě znaleckého posudku o osobnostní způsobilosti.

Podmínku **bezpečnostní spolehlivosti** splňuje fyzická osoba, u níž není zjištěno bezpečnostní riziko. Bezpečnostním rizikem je závažná nebo opakovaná činnost proti zájmům České republiky, nebo činnost, spočívající v potlačování základních práv a svobod, anebo podpora takové činnosti. Za bezpečnostní riziko lze též považovat:

- zařazení do složky bývalé Státní bezpečnosti s rozvědným nebo kontrarozvědným zaměřením, zpravodajské správy Generálního štábu Československé lidové armády nebo odboru vnitřní ochrany Sboru nápravné výchovy anebo prokazatelnou spoluprací s bývalou Státní bezpečností nebo zpravodajskou správou Generálního

- štábu Československé lidové armády nebo odborem vnitřní ochrany Sboru nápravné výchovy,
- užívání jiné identity,
 - úmyslné porušení právních předpisů, na jehož základě může nastat újma zájmu České republiky,
 - chování, které má vliv na důvěryhodnost nebo ovlivnitelnost osoby a může ovlivnit její schopnost utajovat informace,
 - styky s osobou, která vyvíjí nebo vyvíjela činnost proti zájmu České republiky,
 - pravomocné odsouzení pro trestný čin,
 - uvedení nepravdivé informace nebo zamlčení informace rozhodné pro objektivní zjištění skutečného stavu věci v řízení podle části čtvrté nebo nenahlášení změny údajů uvedených v příloze k této žádosti o vydání osvědčení fyzické osoby (§ 94) nebo v jiném materiálu poskytnutém Úřadu v příloze k této žádosti,
 - porušení povinnosti při ochraně utajovaných informací, nebo
 - zřejmě nepřiměřené finanční nebo majetkové poměry vzhledem k řádně přiznaným příjmům fyzické osoby.

Bezpečnostní rizika se zjišťují za období od 15 let věku, případně 10 – 20 let zpětně od podání žádosti podle stupně bezpečnostního řízení. Při posuzování bezpečnostních rizik se přihlíží k tomu, do jaké míry může ovlivnit schopnost utajovat informace, k době jejího výskytu, k jejímu rozsahu, charakteru a k chování fyzické osoby v posuzovaném období.

V souvislosti s bezpečnostním řízením se provádí bezpečnostní pohovor, a to v případě, kdy se v průběhu bezpečnostního řízení vyskytnou skutečnosti, které je třeba objasnit pro zjištění skutečného stavu věci.

1.7 Administrativní bezpečnost

Administrativní bezpečnost je pojímána jako systém opatření, jehož cílem je ochrana utajovaných informací při jejich tvorbě, příjmu, evidenci, zpracovávání, přepravě, ukládání, vyřazování, skartaci a archivaci, případně i jiné manipulaci. Tuto oblast upravuje vyhl. č. 529/2005 Sb., o podrobnostech stanovení a označení stupně utajení a o zajištění administrativní bezpečnosti. Smyslem administrativní bezpečnosti je zabezpečení utajované informace vyjádřené v materiální formě, stanovení základních evidenčních a manipulačních režimů s takovou utajovanou informací. Pro potřeby administrativní bezpečnosti se pro utajovanou informaci používá pojem „utajovaný dokument“.

Za základní **administrativní pomůcky** pro evidenci a zaznamenávání pohybu utajovaných písemností se považují:

- jednacích protokolů, kterým je kniha nebo sešit pro evidování utajovaného dokumentu,
- pomocných jednacích protokolů, kterým je kniha nebo sešit pro zaznamenávání pohybu utajovaného dokumentu v rámci orgánu státu, právnické osoby nebo podnikající fyzické osoby,
- manipulačních knih, kterou je kniha nebo sešit pro zaznamenávání utajovaného dokumentu při jeho vytváření, převzetí a předávání,

- doručovací kniha, kterou je kniha nebo sešit pro zaznamenávání předání utajovaného dokumentu,
- zápůjční kniha, kterou je kniha nebo sešit pro zaznamenávání zápůjček uloženého utajovaného dokumentu,
- kontrolní list utajovaného dokumentu stupně utajení Důvěrné, Tajné nebo Přísně tajné (dále jen „kontrolní list“) pro vedení přehledu osob, které se s obsahem utajovaného dokumentu u orgánu státu, právnické osoby nebo podnikající fyzické osoby seznámily,
- sběrný arch pro rozšíření evidenčního záznamu v jednacím protokolu v případě evidování většího počtu utajovaných dokumentů k jedné věci.

Kromě uvedených administrativních pomůcek je možné v odůvodněných případech použít další administrativní pomůcky. Další administrativní pomůcky sloužící k evidenci utajovaných dokumentů musí obsahovat podle účelu, pro který jsou používány, položky jako jednacím protokol.

1.7.1 Náležitosti utajovaných dokumentů jsou nezbytné údaje, které musí utajovaný dokument obsahovat. Na utajovaný dokument v listinné podobě se uvede název orgánu státu (útvary), u které utajovaný dokument vznikl, číslo jednacím utajovaného dokumentu nebo jiné evidenční označení, stupeň utajení, datum vyhotovení, číslo výtisku, počet listů, počet utajovaných a neutajovaných příloh v listinné podobě a počet jejich listů, případně počet a druh utajovaných a neutajovaných příloh v nelistinné podobě. Na utajovaném dokumentu se mohou vyznačit další údaje. Jsou-li k dokumentu připojeny přílohy, z nichž některé jsou utajované, vyznačí se stupeň utajení a další údaje podle věty první i v případě, kdy sám dokument neobsahuje utajované informace. Na utajovaný dokument v nelistinné podobě se uvede název orgánu státu (útvary), u které utajovaný dokument vznikl, stupeň utajení, číslo jednacím utajovaného dokumentu nebo, je-li utajovaný dokument evidován v administrativních pomůckách mimo jednacím protokol, jiné evidenční označení nebo, je-li přílohou, označení „Příloha k č. j....“ nebo „Příloha k evid. ozn...“. Nelze-li tyto údaje vyznačit přímo na utajovaný dokument v nelistinné podobě, vyznačí se na popisném štítku nebo jiným vhodným způsobem. Na doručený utajovaný dokument se vyznačí název příjemce, datum zaevidování, evidenční označení příjemce (zpravidla číslo jednacím), počet listů, počet příloh a počet jejich listů; u příloh v nelistinné podobě jejich počet a druh, případně další údaje.

1.7.2 Příjem utajovaných dokumentů - zásilku přijímá osoba určená k přebírání zásilek, popřípadě osoba pověřená vedením jednacím protokolu. Převzetí zásilky se doručiteli potvrdí podpisem s uvedením data a otiskem razítka orgánu státu, právnické osoby nebo podnikající fyzické osoby. Přijme-li zásilku osoba určená k přebírání zásilek, předá ji neprodleně k zaevidování. Utajovaný dokument musí být prokazatelným způsobem zaevidován. K evidenci lze použít jednacím protokol nebo další administrativní pomůcka. Evidenci provádí osoba pověřená vedením jednacím protokolu. Utajovaný dokument stupně utajení Přísně tajné se eviduje v samostatném jednacím protokolu. Utajované dokumenty stupně utajení Tajné a Důvěrné se mohou evidovat v jednom jednacím protokolu společně s utajovanými dokumenty stupně utajení Vyhrazené. Oprava zápisu v evidenci se provede tak, že se původní zápis přeškrtně tak, aby zůstal čitelný, a provede se zápis nový s uvedením data, příjmení a podpisu osoby, která opravu zápisu provedla.

1.7.3 Číslo jednací je číselná identifikace utajovaného dokumentu a vyjadřuje stupeň utajení dokumentu, jeho evidenční číslo, rok vzniku, původce, respektive držitele utajovaného dokumentu a případně další bližší identifikační údaje. Je nezbytné upozornit, že jeho struktura je odlišná od čísla jednacího neutajované písemnosti a jako vzor lze uvést např. číslo jednací: V99/2006-HZS/01, které vyjadřuje, že stupeň utajení dokumentu je Vyhrazené, pořadové číslo podle jednacího protokolu je 99, rokem vzniku je rok 2006, původcem utajovaného dokumentu je útvar používající spisovou značku HZS s bližším označením organizačního celku 01.

1.7.4 Opis, kopie, překlad a výpis utajované informace lze provádět pouze za stanovených podmínek. Opis, kopie nebo překlad utajované informace stupně utajení Přísně tajné nebo výpis z ní mohou být vyhotoveny pouze na základě písemného souhlasu původce; jde-li o utajovanou informaci stupně utajení Tajné nebo Důvěrné, mohou být vyhotoveny pouze s písemným souhlasem přímo nadřízené osoby. U informace stupně utajení Vyhrazené není třeba souhlasu nadřízeného a je věcí držitele této písemnosti, zda je nezbytné a nutné provádět opis, kopii, překlad nebo výpis, musí však být splněny ostatní evidenční náležitosti. Písemnost, ze které se vyhotovuje opis, kopie, překlad nebo výpis, se opatří záznamem s datem pořízení, počtem výtisků (kopií), důvodem, jménem schvalovatele, jménem a podpisem toho, kdo zhotovuje. Písemnost, která se vytváří (vlastní opis, kopie, překlad nebo výpis), musí obsahovat zřizovací položku např. "Kopie souhlasí s originálem", kopie č. 1 z výtisku č. 5, počet listů a podpis.

1.7.5 Předávání utajovaných dokumentů lze uskutečnit proti potvrzení podpisem, mezi útvary prostřednictvím jednacích protokolů, uvnitř útvaru prostřednictvím pomocného jednacího protokolu, jednacího protokolu nebo prostřednictvím manipulační knihy.

1.7.6 Odesílání utajovaného dokumentu se provádí v rámci rezortu Ministerstva vnitra prostřednictvím rezortní kurýrní služby. Utajovanou písemnost do stupně utajení Důvěrné lze také zaslat prostřednictvím držitele poštovní licence, ve dvou obálkách a za dodržení náležitostí stanovených právní a interní úpravou. Odesílání utajovaných dokumentů stupňů utajení Tajné a Přísně tajné zabezpečuje odesílající útvar. Zásilka stupně utajení Tajné může být dopravována pouze kurýrem, který musí být osobou, která má přístup k utajované informaci příslušného stupně utajení, v doprovodu další osoby. Tato zásilka je vyloučena z přepravy veřejnými dopravními prostředky, s výjimkou přepravy letecké, námořní a vnitrozemské vodní. Zásilka stupně utajení Přísně tajné je dopravována v součinnosti se speciálním ochranným útvarem.

1.7.7 Přeprava utajovaných dokumentů je pojímána vždy jako dopravení dokumentu mimo objekt útvaru za účelem jeho doručení příslušnému adresátu k jinému jednacímu protokolu, tj. kurýrem nebo poštou. Kurýr je každý, kdo přepravuje utajovaný dokument a musí být osobou, která má přístup k utajované informaci na příslušný stupeň utajení. Přeprava utajovaného dokumentu se provádí vždy ve dvou obálkách, přenosná schránka se považuje za vnější obálku za použití přenosné schránky (ta se pečeti, je uzamčená a označená příslušnými náležitostmi).

1.7.8 Přenášením utajovaného dokumentu se rozumí jeho dopravení mimo objekt se

zabezpečenými oblastmi nebo jednacími oblastmi s tím, že se nedoručuje jinému adresátu a nemění se jeho evidenční místo. Uskutečňuje se v rámci objektu volně a mimo objekt v přepravní schránce. Za přenášení se považuje i přeprava utajovaného dokumentu vně objektu v případě, že se dokument vrací zpět k evidenčnímu místu (jednání, porady).

1.7.9 Ukládání utajovaných dokumentů se provádí do certifikovaných nebo necertifikovaných úschovných objektů nebo v zabezpečených oblastech mimo úschovný objekt (Vyhrazené).

1.7.10 Zapůjčovat utajovaný dokument lze na dobu nezbytně nutnou, pouze oprávněné osobě s příslušným souhlasem a v rámci útvaru, kde je evidován.

1. 7. 11 Ničení utajovaných dokumentů v rámci skartačního řízení se provádí na zařízeních pro ničení nosičů, certifikovaných pro daný nebo vyšší stupeň utajení.

Vyřazování utajovaných dokumentů se provádí v souladu s platným skartačním řádem Ministerstva vnitra. Ustanovuje se tříčlenná skartační komise, kdy vedoucí komise nesmí být pracovník pověřený vedením jednacích protokolů. Všichni členové komise musí mít osobami, které mají přístup k utajovaným informacím odpovídající nejvyššímu stupni utajení dokumentů, které mají být vyřazeny.

Utajovaný dokument (doručený i vlastní) se eviduje v jednacím protokolu u útvaru. Přes jedací protokol (zápisem v jednacím protokolu), popřípadě prostřednictvím doručovací knihy se přiděluje zpracovateli a ten jej zapisuje do své manipulační knihy (u stupně utajení Vyhrazené i jiná forma zápisu). V průběhu zpracování může být utajovaná písemnost přenášena (na jednání, porady ap.), popřípadě může být zhotovována její kopie, opis, výpis či překlad. Po zpracování se přes manipulační knihu zpracovatele vrací k jednacímu protokolu k vyřízení. Od jedacího protokolu se přes doručovací knihu zasílá adresátu a průpis se ukládá u útvaru u jedacího protokolu. Uloženou utajovanou písemnost lze v případě potřeby zapůjčit přes zápůjční knihu a písemnost se zaznamenává v manipulační knize toho, kdo si ji zapůjčil. Po uplynutí skartační doby se utajovaná písemnost vyřazuje, to znamená, že se ukládá do archivu nebo se ničí.

1.8 Registry utajovaných informací

Registry utajovaných informací se používají k evidování utajovaných dokumentů ze zahraničí a poskytovaných z České republiky do zahraničí pro stupně utajení Důvěrné, Tajné a Přísně tajné. Tímto systémem je zaručena oddělená evidence utajovaných dokumentů poskytovaných v rámci mezinárodní spolupráce. V rámci České republiky je veden „ústřední registr“ u Úřadu a orgány státu si zřizují vlastní „registry utajovaných informací“. Registr utajovaných informací pro rozsah působnosti Ministerstva vnitra, tedy i pro generální ředitelství Hasičského záchranného sboru České republiky, vede bezpečnostní odbor.

Pokud to vyžaduje praxe a je nezbytné poskytovat utajované dokumenty Evropské unie a NATO hasičským záchranným sborům krajů, musí být u těchto sborů zřízeny registry utajovaných informací. V praxi to pak znamená, že utajovaný dokument, který má být doručen do zahraničí, musí být doručen přes registr utajovaných informací ústřednímu registru a jeho prostřednictvím je tento utajovaný dokument doručen příslušnému zahraničnímu bezpečnostnímu úřadu a ten

zabezpečí jeho doručení adresátu. Tato cesta platí i naopak při doručování do České republiky. Je nutné upozornit na případy, kdy fyzická osoba přiveze utajované dokumenty ze zahraničí osobně (např. z pracovního jednání) a i v těchto případech povinnost evidence tohoto utajovaného dokumentu poskytnutého v rámci mezinárodní spolupráce v příslušných registrech trvá.

1.9 Fyzická bezpečnost

Fyzickou bezpečnost tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat. Pro zabezpečení ochrany utajovaných informací v rámci fyzické bezpečnosti se určují objekty, zabezpečené oblasti a jednací oblasti. Objektem se zabezpečenými oblastmi je budova nebo jiný ohraničený prostor, ve kterém se nachází zabezpečená oblast nebo jednací oblast. Zabezpečenou oblastí je stavebně nebo jinak viditelně ohraničený prostor v objektu. Jednací oblastí je ohraničený prostor v objektu. Utajovanou informaci stupně utajení Přísně tajné nebo Tajné lze pravidelně projednávat pouze v jednací oblasti.

Utajovanou informaci lze zpracovávat

- v zabezpečených oblastech,
- v objektu mimo zabezpečenou oblast, pokud je zajištěno, že k utajované informaci nemá přístup neoprávněná osoba, nebo
- v odůvodněných případech s písemným souhlasem odpovědné osoby nebo bezpečnostního ředitele mimo objekt, pokud je zajištěno, že k utajované informaci nemá přístup neoprávněná osoba.

Opatřeními fyzické bezpečnosti jsou ostraha, režimová opatření a technické prostředky. Utajovaná informace se ukládá v zabezpečené oblasti a v ní popřípadě v trezoru, uzamykatelné skříni nebo jiné schránce za podmínek stanovených prováděcím právním předpisem. Způsob zabezpečení ochrany objektů upravuje vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a o certifikaci technických prostředků. Certifikací se rozumí proces, jímž Úřad ověřuje způsobilost technických prostředků, informačních systémů, kryptografických prostředků, kryptografických pracovišť a stínících komor k ochraně utajovaných informací

1.10 Bezpečnost informačních a komunikačních systémů

Informačním systémem nakládajícím s utajovanými informacemi se rozumí jeden nebo více počítačů, jejich programové vybavení, k tomu patřící periferní zařízení, správa tohoto informačního systému a k tomuto systému se vztahující procesy nebo prostředky schopné provádět sběr, tvorbu, zpracování, ukládání, zobrazení nebo přenos utajovaných informací. Informační systém musí být certifikován Úřadem a písemně schválen do provozu odpovědnou osobou. Prováděcí právní předpis (vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor) stanoví požadavky na informační systém, podmínky jeho bezpečného provozování v závislosti na stupni utajení utajovaných informací, s nimiž nakládá, a na bezpečnostním provozním módu, a obsah bezpečnostní dokumentace informačního systému.

Komunikačním systémem nakládajícím s utajovanými informacemi se rozumí systém zajišťující přenos těchto informací mezi koncovými uživateli a zahrnující koncové komunikační zařízení, přenosové prostředí, kryptografické prostředky, obsluhu a provozní podmínky a postupy. Komunikační systém nelze provozovat bez projektové bezpečnostní dokumentace informačního systému a provozní bezpečnostní dokumentace informačního systému. Informační systém musí být certifikován Úřadem. O certifikaci informačního systému písemně žádá u Úřadu jeho provozovatel.

V podmínkách Ministerstva vnitra a Hasičského záchranného sboru ČR lze utajované informace zpracovávat na certifikovaných prostředcích výpočetní techniky, které jsou označeny jako systém „Vydra“ (pro zpracovávání utajovaných informací stupně utajení Vyhrazené) a systém „Dudek“ (pro zpracovávání utajovaných informací stupně utajení Důvěrné). Bezpečnostní dokumentace uvedených systémů pak stanoví režimová a organizační opatření, která je nutno dodržovat při zpracovávání utajovaných informací daných stupňů utajení.

Při zpracování utajované informace v elektronické podobě v kopírovacím zařízení, zobrazovacím zařízení nebo psacím stroji s pamětí, které nejsou součástí informačního nebo komunikačního systému, musí být zajištěna ochrana této utajované informace. V podmínkách Ministerstva vnitra se při zpracovávání utajované informace v uvedených zařízeních postupuje podle bezpečnostní provozní směrnice kopírovacího zařízení, zobrazovacího zařízení nebo psacího stroje s pamětí. U hasičských záchranných sborů krajů se postupuje podle bezpečnostních provozních směrnic vydaných řediteli krajů.

1.11 Kryptografická ochrana

Kryptografickou ochranou se rozumí systém prostředků a metod ochrany utajovaných informací pomocí kryptografických metod a kryptografického materiálu, tj. kryptografických prostředků a klíčového materiálu. Jejím výkonem se rozumí bezpečnostní správa, speciální obsluha kryptografického prostředku a výroba klíčového materiálu

1.12 Průmyslová bezpečnost

Pro přehlednost je nezbytné zmínit se o tzv. průmyslové bezpečnosti, která ve svém souhrnu upravuje systém opatření na ochranu utajovaných informací k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu se zákonem. V podmínkách Ministerstva vnitra a Hasičského záchranného sboru ČR se neuplatňuje.

1.13 Následky porušení povinností při ochraně utajovaných informací

Porušení povinností při ochraně utajovaných informací je platnou právní úpravou pojímáno jako porušení povinností uložené zákonem nebo na základě zákona. Neoprávněné nakládání s utajovanou informací by se dalo charakterizovat jako vyzrazení, zneužití, poškození, znehodnocení nebo zničení utajované informace, porušení její ochrany nebo její ztráta. Současně lze za porušení povinností při ochraně utajovaných informací považovat neoznačení nebo nesprávné stanovení stupně utajení utajované informace, její manipulace v rozporu se zákonem

a prováděcími předpisy a nedodržení ostatních povinností zákonem stanovených.

Vyzrazením utajované informace se rozumí její vyzrazení nepovolané osobě. Zneužití utajované informace je jakékoliv užití utajované informace bez souhlasu subjektu oprávněného k nakládání s předmětnými informacemi. Za poškození, znehodnocení nebo zničení utajované informace je třeba považovat zlikvidování nebo poškození formy informací, např. fyzickým zničením nosiče, nezvratným vymazáním informací, zrušením záznamu a poškozením záznamu způsobem měnícím jeho původní obsah. Za poškození utajované informace se považuje rovněž ohrožení účelu, ke kterému mají utajované informace sloužit, snížení jejich informační hodnoty buď trvale (např. takovým zásahem do obsahu a struktury informací, který způsobí, že je nelze trvale použít k určenému účelu) nebo jen pro určitý čas (lze-li např. program s utajovanými informacemi použít k určenému účelu až po složitých a nákladných úpravách). Podstatnou kategorií je porušení ochrany utajované informace, za které se považuje jakákoliv nesprávná manipulace, evidence, včetně zpracovávání utajované písemnosti způsobem odporujícím stanoveným režimům a omezením.

Porušení povinností při ochraně utajovaných informací může zakládat skutkovou podstatu **trestného činu**, popřípadě, nejde-li o trestný čin, může být klasifikováno jako **přestupek**.

Z hlediska trestněprávní odpovědnosti může porušení povinností při ochraně utajovaných informací zakládat skutkovou podstatu trestného činu

- vyzvědačství podle § 105 trestního zákona. V tomto případě ten, kdo vyzvídá utajovanou informaci, jejíž zneužití může vážným způsobem ohrozit nebo poškodit ústavnost, svrchovanost, územní celistvost, obranu a bezpečnost České republiky nebo jiného státu anebo obranu a bezpečnost mezinárodní organizace, k ochraně jejichž zájmů v uvedených oblastech se Česká republika zavázala, s cílem vyzradit ji cizí moci, kdo s takovým cílem sbírá údaje obsahující utajovanou informaci, nebo kdo takovou utajovanou informaci cizí moci úmyslně vyzradí, bude potrestán odnětím svobody na dvě léta až osm let. Stejně bude potrestán, kdo umožní nebo usnadní činnost pachateli tohoto trestného činu nebo organizaci, jejímž cílem je vyzvídat utajované informace. Odnětím svobody na osm až patnáct let bude pachatel potrestán, spáchá-li trestný čin vyzvědačství jako člen organizace, jejímž cílem je vyzvídat utajované informace, spáchá-li takový čin, ačkoli mu ochrana utajovaných informací byla zvlášť uložena, získá-li takovým činem značný prospěch nebo spáchá-li takový čin ve značném rozsahu, nebo týká-li se takový čin utajované informace klasifikované stupněm utajení Přísně tajné. Odnětím svobody na dvanáct až patnáct let nebo výjimečným trestem bude pachatel potrestán, spáchá-li trestný čin vyzvědačství za stavu ohrožení státu nebo za válečného stavu.
- ohrožení utajované informace podle § 106 trestního zákona, tzn. úmyslné ohrožení utajované informace. V tomto případě ten, kdo vyzvídá utajovanou informaci s cílem vyzradit ji nepovolané osobě, kdo s takovým cílem sbírá údaje obsahující utajovanou informaci, nebo kdo takovou utajovanou informaci nepovolané osobě úmyslně vyzradí, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem. Odnětím svobody na dvě léta až osm let bude pachatel potrestán, vyzradí-li úmyslně nepovolané osobě utajovanou informaci klasifikovanou stupněm utajení

Přísně tajné nebo Tajné, spáchá-li tento trestný čin, ačkoli mu ochrana utajovaných informací byla zvlášť uložena, nebo získá-li takovým činem značný prospěch nebo způsobí-li značnou škodu nebo jiný zvlášť závažný následek. Odnětím svobody na pět až dvanáct let bude pachatel potrestán, týká-li se tento trestný čin utajované informace z oblasti zabezpečení obranyschopnosti republiky klasifikované ve zvláštním zákoně stupněm utajení Přísně tajné, nebo spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu.

- ohrožení utajované informace podle § 107 trestního zákona, tzn. nedbalostní ohrožení utajované informace. V tomto případě ten, kdo z nedbalosti způsobí vyzrazení utajované informace klasifikované stupněm utajení Přísně tajné, Tajné nebo Důvěrné, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti nebo peněžitým trestem.

Dalšími trestnými činy, které se váží k uvedeným skutkovým podstatám, jsou trestné činy nepřekážení trestného činu podle § 167 trestního zákona a neoznámení trestného činu podle § 168 trestního zákona, podle kterých je trestný ten, kdo se hodnověrným způsobem doví, že jiný připravuje nebo páchá trestné činy, mimo jiné, vyzvědačství podle § 105 trestního zákona nebo ohrožení utajované informace podle § 106 trestního zákona a spáchání nebo dokončení takového trestného činu nepřekazí, popřípadě se hodnověrným způsobem doví, že jiný spáchal trestné činy, mimo jiné, vyzvědačství podle § 105 trestního zákona nebo ohrožení utajované informace podle § 106 a § 107 trestního zákona a takový trestný čin stanoveným způsobem neoznámí.

Porušení povinností při ochraně utajovaných informací, nejde-li o trestný čin, může být klasifikováno jako přestupek. Při porušení povinností při ochraně utajovaných informací se může fyzická osoba dopustit přestupku, definovaného v části osmé zákona (§ 148 až 152 zákona) a za tyto přestupky lze uložit pokutu, která se podle druhu přestupku pohybuje ve výši 30 000 Kč až 5 000 000 Kč. Orgán státu se může v této souvislosti dopustit správního deliktu vymezeného § 153 zákona a pokuta se v těchto případech pohybuje v rozmezí 300 000 Kč až 1 000 000 Kč. Pokud se přestupku uvedeného v části osmé zákona dopustila fyzická osoba, která není ve služebním poměru k Hasičskému záchrannému sboru České republiky, projednává tento přestupek Úřad. Pokud se přestupku uvedeného v části osmé zákona dopustila fyzická osoba, která je ve služebním poměru k Hasičskému záchrannému sboru České republiky, přísluší jeho projednání příslušnému služebnímu funkcionáři, v tomto případě generálnímu řediteli.

1.14 Závěr

Toto je pouze obecný úvod do problematiky ochrany utajovaných informací. Každý, kdo se bude seznamovat s utajovanými informacemi v rámci svého pracovního nebo služebního zařazení je povinen absolvovat úvodní poučení a pravidelná roční proškolení, kde se podrobně seznámí s režimy a omezeními a s podrobnostmi vyplývající ze specifík útvaru (zařazení) a ve vztahu ke stupni utajení.