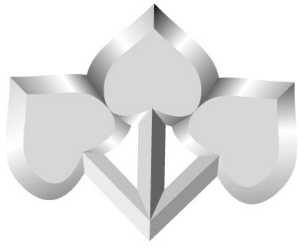
OBSAH

PERSONÁLNÍ BEZPEČNOST



PERSONÁLNÍ BEZPEČNOST

1. Obecně k personální bezpečnosti

Personální bezpečnost je základním druhem zajištění ochrany utajovaných informací a je upravena v hlavě II zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon č. 412/2005 Sb.“).

Vedle ověřování podmínek, které musí fyzická osoba splnit, aby jí byl umožněn přístup k utajované informaci, zahrnuje personální bezpečnost i výchovu těchto osob. Za zajištění proškolení fyzických osob, které mají přístup k utajované informaci, ručí odpovědná osoba. Ta je povinna jednou ročně zajistit u osob, které mají přístup k utajované informaci, proškolení z právních předpisů v oblasti ochrany utajovaných informací. Rovněž je povinna neprodleně písemně oznámit Národnímu bezpečnostnímu úřadu (dále jen „Úřad“), že před vydáním osvědčení fyzické osoby nebo rozhodnutí o nevydání osvědčení pominuly skutečnosti, kterými byla žádost fyzické osoby odůvodněna, stejně tak neprodleně oznámit Úřadu skončení služebního nebo pracovněprávního, členského či obdobného vztahu, ve kterém byl fyzické osobě umožněn přístup k utajované informaci stupně utajení Přísně tajné, Tajné nebo Důvěrné.

Způsob a rozsah ověřování podmínek, které musí fyzická osoba splnit, aby jí byl umožněn přístup k utajované informaci, se liší podle stupňů utajení, k nimž má mít fyzická osoba přístup. V následující tabulce jsou uvedeny podmínky pro jednotlivé stupně utajení, které musí fyzická osoba splňovat:

PODMÍNKY	**VYHRAZENÉ (oznámení)**	**DŮVĚRNÉ, TAJNÉ, PŘÍSNĚ TAJNÉ (osvědčení)**
Svéprávnost	ANO	ANO
Věk minimálně 18 let	ANO	ANO
Bezúhonnost	ANO	ANO
Státní občanství ČR, země EU, NATO	NE	ANO
Osobnostní způsobilost	NE	ANO
Bezpečnostní spolehlivost	NE	ANO

Pro stupeň utajení Vyhrazené ověřuje podmínky ten, kdo je vůči fyzické osobě v rámci služebního nebo pracovněprávního, členského či obdobného vztahu odpovědnou osobou, nebo jí určená osoba. Není-li jí, ověření provede odpovědná osoba nebo jí určená osoba toho, kdo umožní fyzické osobě přístup k utajované informaci stupně utajení Vyhrazené. V ostatních případech ověření provede Úřad na základě odůvodněné písemné žádosti.

Pro stupně utajení Důvěrné, Tajné a Přísně tajné se splnění podmínek ověřuje v bezpečnostním řízení, které je oprávněn provádět Úřad, zpravodajské služby u svých příslušníků, zaměstnanců a uchazečů o přijetí a Ministerstvo vnitra u příslušníků policie vybraných v zájmu plnění závažných úkolů.

Ministerstva a další ústřední správní úřady jsou povinny každoročně do 31. července zpracovat a zaslat Úřadu **personální projekt** (§ 72 zákona č. 412/2005 Sb.). Jeho obsahem je zhodnocení stavu v oblasti personální bezpečnosti za uplynulý kalendářní rok včetně uvedení celkového počtu utajovaných informací, počtu přístupů k těmto utajovaným informacím a počtu držitelů osvědčení. V personálním projektu musí být dále uveden předpokládaný počet osob, které budou mít v následujícím kalendářním roce přístup k utajovaným informacím, a osob, u nichž bude nutné v následujícím kalendářním roce provést bezpečnostní řízení s rozlišením podle stupňů utajení.

Úřad posuzuje zaslané personální projekty po obsahové a formální stránce a uplatňuje k nim připomínky. Náležitosti pro zpracovávání a vyhodnocování personálních projektů, včetně procesu zvláštního připomínkového řízení, řeší usnesení vlády České republiky ze dne 19. června 2012 č. 439. Úřad personální projekty předkládá spolu se svým vyjádřením vládě vždy do 30. listopadu příslušného kalendářního roku.

2. Informace k podání žádosti o vydání oznámení pro přístup k utajovaným informacím stupně utajení Vyhrazené

Kdo standardně provádí ověření podmínek a vydává oznámení pro přístup k utajovaným informacím stupně utajení Vyhrazené (dále jen „oznámení“)

- ověření provádí odpovědná osoba zaměstnavatele nebo jí určená osoba (např. bezpečnostní ředitel), která také vydává oznámení,
- v případě, že ověření neprovádí zaměstnavatel, provádí je a oznámení vydává ten, kdo fyzické osobě umožní přístup k utajované informaci stupně Vyhrazené.

Kdo provádí ověření podmínek a vydává oznámení odpovědné osobě, která je zároveň i bezpečnostním ředitelem

- ověření může provést osoba určená odpovědnou osobou, která jí pak také vydá oznámení, neexistují žádné předpoklady, které tato určená osoba musí splňovat, může jít o podřízenou osobu této odpovědné osoby a třeba i o osobu, která samotná není držitelem oznámení.

Kdy může fyzická osoba požádat Úřad o vydání oznámení

- pouze ve výjimečných případech, pokud neexistuje vůči fyzické osobě subjekt, který by mohl vystupovat jako její odpovědná osoba nebo jí pověřená osoba ve smyslu zákona č. 412/2005 Sb., tzn., že fyzická osoba nemá žádný služební poměr, pracovněprávní či obdobný vztah, v jehož rámci by nezbytně potřebovala mít přístup k utajované informaci stupně Vyhrazené, ani neexistuje ten, kdo jí umožní nezbytně nutný přístup k vlastní utajované informaci, tzn. poskytovatel utajované informace, avšak fyzická osoba z konkrétně definovaného důvodu nezbytně nutně tento přístup potřebuje; žádost musí být písemná a řádně odůvodněná a fyzická osoba ji musí podat, společně s předložením níže uvedených písemností, osobně na podatelně Úřadu.

Co musí fyzická osoba předložit

- odůvodněnou žádost o vydání oznámení - pouze pro případ, že ověření podmínek a následné vydání oznámení by měl provést Úřad,
- prohlášení fyzické osoby o svéprávnosti,
- občanský průkaz nebo cestovní doklad,
- výpis z Rejstříku trestů (nesmí být starší 3 měsíců), cizí státní příslušník předkládá také obdobný doklad státu, jehož je státním občanem, jakož i státu, v němž pobýval nepřetržitě po dobu delší než 6 měsíců (doklady nesmí být starší 3 měsíců).

Veškeré písemnosti jsou předkládány v českém jazyce.

V případě písemnosti vyhotovené v cizím jazyce musí být tato předložena v originálním znění a současně v úředně ověřeném překladu do jazyka českého.

Co musí fyzická osoba splňovat

- svéprávnost,
- věk 18 let,
- bezúhonnost (podmínku bezúhonnosti splňuje fyzická osoba, která nebyla pravomocně odsouzena za spáchání úmyslného trestného činu nebo trestného činu vztahujícího se k ochraně utajovaných informací, anebo se na ni hledí, jako by odsouzena nebyla).

Podmínku svéprávnosti a podmínku bezúhonnosti musí fyzická osoba, která je držitelem oznámení, splňovat po celou dobu přístupu k utajované informaci stupně Vyhrazené.

Kdy může mít fyzická osoba přístup k utajované informaci stupně utajení Vyhrazené

- v případě nezbytné potřeby při výkonu své funkce, pracovní nebo jiné činnosti, je-li držitelem oznámení nebo držitelem osvědčení (DŮVĚRNÉ, TAJNÉ, PŘÍSNĚ TAJNÉ) nebo dokladu o bezpečnostní způsobilosti fyzické osoby (dále jen „doklad“) a zároveň je poučena, není-li stanoveno jinak (§ 58 až § 62 zákona č. 412/2005 Sb.).

Povinnosti držitele oznámení

1. Písemně sdělovat tomu, kdo vydal oznámení
   - změnu týkající se podmínky svéprávnosti a podmínky bezúhonnosti,
   - odcizení, ztrátu, poškození oznámení nebo změnu údaje v něm obsaženém,
   - den doručení osvědčení nebo dokladu,
   - vznik služebního poměru nebo pracovněprávního, členského či obdobného vztahu, ve kterém má být fyzické osobě umožněn přístup k utajované informaci, vydal-li oznámení Úřad nebo tzv. poskytovatel utajované informace.
2. Na žádost toho, kdo vydal oznámení, předložit ve lhůtě, kterou stanovil, výpis z Rejstříku trestů (cizí státní příslušník také obdobný doklad státu, jehož je státním občanem, jakož i státu, v němž pobýval nepřetržitě po dobu delší než 6 měsíců v posledních 5 letech) a prohlášení o svéprávnosti; doklady nesmí být starší 3 měsíců.

Platnost a zánik platnosti oznámení

Doba platnosti oznámení není časově omezena s tím, že ten, kdo toto oznámení vydal, má povinnost **každých 5 let** ověřovat u fyzické osoby znovu podmínky pro jeho vydání (v případě důvodných pochybností toto činí kdykoliv před uplynutím této lhůty).

Ověřování splnění podmínek se provádí po 5 letech ode dne vydání oznámení bez ohledu na to, zda bylo oznámení vydáno před nebo po 1. 1. 2012. Tzn., že pokud bylo oznámení vydáno 1. 4. 2007 a ověření splnění podmínek pro jeho vydání bylo provedeno podle předchozí právní úpravy k 1. 4. 2010, musí být další ověření splnění podmínek provedeno nejpozději k 1. 4. 2015.

Platnost oznámení zaniká

- doručením vyrozumění o nesplnění podmínek (vyrozumění o nesplnění podmínek vydává ten, kdo oznámení vydal),
- skončením služebního poměru nebo pracovněprávního vztahu, ve kterém byl fyzické osobě umožněn přístup k utajované informaci,
- vznikem služebního poměru nebo pracovněprávního, členského či obdobného vztahu, ve kterém má být fyzické osobě umožněn přístup k utajovaným informacím, pokud bylo oznámení vydáno Úřadem nebo tzv. poskytovatelem utajované informace,
- úmrtím fyzické osoby,
- ohlášením jeho odcizení, ztráty,
- poškozením majícím za následek nečitelnost zápisů v něm uvedených nebo porušením jeho celistvosti,
- doručením vyrozumění o nesplnění povinnosti předložit aktuální podklady k ověření podmínek pro jeho vydání (vyrozumění o nesplnění povinnosti vydává ten, kdo oznámení vydal),
- vrácením tomu, kdo jej vydal, a není-li jej, tak Úřadu,
- patnáctým dnem od doručení osvědčení nebo dokladu, nebo
- změnou některého z údajů v něm obsažených.

V případech odcizení, ztráty, poškození nebo změny údajů vydá na základě písemné žádosti fyzické osoby ten, kdo oznámení vydal, oznámení nové, a to do 5 dnů ode dne doručení žádosti. Tato žádost musí být podána do 15 dnů ode dne zániku platnosti oznámení.

Upozornění

Pokud nebude žádost ve stanovené lhůtě podána, přístup k utajovaným informacím zanikne a fyzická osoba si bude muset, v případě nutnosti zachování přístupu k utajované informaci stupně utajení Vyhrazené, znovu požádat o vydání jiného oznámení, tzn. předložit opět všechny potřebné písemnosti – viz výše bod ***Co musí fyzická osoba předložit***. Bude-li toto oznámení vydáno, musí být fyzická osoba před prvním přístupem k utajované informaci opět poučena.

Platnost všech oznámení vydaných Úřadem před 1. 1. 2012 zanikla v souladu s bodem 3 čl. II Přechodných ustanovení zákona č. 255/2011 Sb. k 1. 4. 2012.

3. Informace k podání žádosti o vydání osvědčení (D,T,PT)

Podle zákona č. 412/2005 Sb. je za **podání** žádosti o vydání osvědčení fyzické osoby (dále jen „žádost o vydání osvědčení“) **odpovědný žadatel**, jakožto účastník řízení.

O vydání osvědčení může požádat pouze příslušník členského státu Evropské unie nebo Organizace Severoatlantické smlouvy.

V bezpečnostním řízení se jedná a písemnosti se vyhotovují v českém jazyce, pokud nejde o výkon práv příslušníka národnostní menšiny.

V případě písemnosti vyhotovené v cizím jazyce musí účastník řízení tuto předložit v originále a současně v úředně ověřeném překladu do jazyka českého.

Náležitosti základní žádosti o vydání osvědčení podle zákona č. 412/2005 Sb.:

1. **formulář žádost o vydání osvědčení**, který ve své první části obsahuje
   - identifikační údaje žadatele,
   - zdůvodnění nutnosti přístupu k utajované informaci žadatelem (včetně uvedení funkce nebo činnosti v rámci služebního poměru nebo pracovněprávního, členského či obdobného vztahu, na jehož základě má být osvědčení vydáno),
   - stupeň utajení, pro který žádá o vydání osvědčení,
   - prohlášení, že údaje uvedené v žádosti a jejích přílohách jsou pravdivé, žadatel se seznámil s podmínkami bezpečnostního řízení a souhlasí s jeho provedením,
   - místo a datum vyplnění,
   - podpis žadatele.

   Dále obsahuje
   - potvrzení zdůvodnění nutnosti přístupu k utajované informaci odpovědnou osobou, bezpečnostním ředitelem nebo tím, kdo bude utajovanou informaci žadateli poskytovat, jež tvoří
     - identifikační údaje tohoto subjektu,
     - označení konkrétního místa nebo funkce stanovené podle § 69 odst. 1 písm. b) zákona č. 412/2005 Sb. a zařazení tohoto místa nebo funkce v tomto přehledu,
     - specifikace utajovaných informací, které na daném místě nebo funkci již byly poskytnuty nebo vznikaly, a utajovaných informací, které zde budou poskytnuty nebo zde mohou vznikat,
     - místo a datum vyplnění,
     - podpis a otisk razítka.

Položka *„specifikace utajovaných informací, které na daném místě nebo funkci již byly poskytnuty nebo vznikaly, a utajovaných informací, které zde budou poskytnuty nebo zde mohou vznikat“* musí vždy obsahovat nejprve sdělení, zda na daném místě nebo funkci již byly/nebyly utajované informace v minulosti poskytnuty nebo vznikaly/nevznikaly. Pokud byly poskytnuty nebo vznikaly, musí být uveden minimálně odkaz na nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, jeho konkrétní přílohu, její konkrétní bod a nejvyšší stupeň těchto utajovaných informací.

Dále musí následovat vyjádření, že na tomto místě nebo funkci budou utajované informace vznikat nebo budou poskytnuty, opět minimálně s uvedením odkazu na nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, jeho konkrétní přílohu, její konkrétní bod a nejvyšší možný stupeň těchto utajovaných informací (např. T), kdy tento stupeň musí odpovídat stupni utajení, který uvádí fyzická osoba v horní části žádosti. Nelze uvést rozsah stupňů utajení (např. V-T). Pokud je uváděno více příloh a více bodů nařízení vlády č. 522/2005 Sb., rovněž nelze uvést rozsah stupňů utajení (např. V-T), ale musí být uveden nejvyšší stupeň utajení (např. T) s tím, že tento stupeň musí odpovídat stupni utajení, který uvádí fyzická osoba v horní části žádosti.

Dále je možné doplnit, že fyzické osobě bude povolen vstup do zabezpečené oblasti kategorie (uvést příslušný stupeň), a to z důvodu (rozvést důvody).

2. **prohlášení žadatele o svéprávnosti** (od 1. 1. 2014 je platný nový formulář prohlášení fyzické osoby o svéprávnosti, jehož vzor je uveden v příloze č. 1 vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění vyhlášky č. 415/2013 Sb. (dále jen „vyhláška o personální bezpečnosti a o bezpečnostní způsobilosti“),
3. **prohlášení žadatele k osobnostní způsobilosti,**

4. **prohlášení žadatele o zproštění povinnosti mlčenlivosti věcně a místně příslušného správce daně a jiné osoby zúčastněné na správě daní podle § 52 odst. 2 daňového řádu, a to v plném rozsahu údajů za účelem provedení bezpečnostního řízení,**
5. **je-li žadatel cizincem, doklad obdobný výpisu z evidence Rejstříku trestů státu, jehož je státním příslušníkem, jakož i státu, v němž pobýval nepřetržitě po dobu delší než 6 měsíců** (u stupně Důvěrné 10 let zpětně, u stupně Tajné 15 let zpětně, u stupně Přísně tajné 20 let zpětně), doklad nesmí být starší než 3 měsíce,
6. fotografie žadatele 35 x 45 mm,
7. **vyplněný dotazník fyzické osoby v listinné i elektronické podobě** (soubor výhradně ve formátu .zfo, nebo .xml) – od 1. 1. 2014 je platný nový formulář dotazníku fyzické osoby, jehož vzor je uveden v příloze č. 6 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti,
8. písemnosti dosvědčující správnost údajů uvedených v dotazníku fyzické osoby:

- **rodný nebo křestní list** v prosté kopii,
- **doklad o nejvyšším dosaženém vzdělání** (podle stupně dosaženého vzdělání - výuční list, maturitní vysvědčení, vysokoškolský diplom, postgraduální studium…) v originále nebo úředně ověřené kopii,
- **potvrzení zaměstnavatele o příjmech s uvedením jejich výše po odečtení povinných zákonných odvodů, v případě jiného druhu příjmu daňové přiznání** (musí být ověřeno příslušným finančním úřadem, nepostačuje kopie s podacím razítkem podatelny příslušného finančního úřadu – může být nahrazeno též např. výpisem údajů daně z příjmu fyzických osob příslušného finančního úřadu) **nebo jiný doklad potvrzující tento příjem, za posledních 5 let** (např. v případě podpory v nezaměstnanosti – potvrzení příslušného úřadu práce, dále potvrzení o rodičovském příspěvku, sociálním příspěvku, zaopatřovacím příspěvku, dávkách pěstounské péče, porodném, pohřebném, vdovském důchodu, příspěvku na bydlení, odchodném, příspěvku za službu, rozhodnutí o výši přídavku na dítě, pokud je již žadateli vyplácen, rozhodnutí o sociálních dávkách, které jsou přiznány v případě neposkytnutí podpory v nezaměstnanosti, rozsudek o schválení dohody rodičů o výši výživného na děti, v případě prodeje nemovitosti smlouvu o prodeji …) v originále nebo úředně ověřené kopii,
- **doklad o právu jiné osoby omezující vlastnictví žadatele** (např. smlouva o úvěru, leasingová, hypoteční smlouva, smlouva o ručitelském závazku (pouze v případě, že se ručitel stal dlužníkem a je povinen závazek uhradit), případně výpisy z úvěrových účtů (pokud je v nich uvedena celková původní výše úvěru), v případě zástavního práva k nemovitosti smlouvu o zřízení zástavního práva k nemovitosti nebo výpis z katastru nemovitostí s uvedením zástavního práva k nemovitosti, rozsudek o schválení dohody rodičů o výši výživného na děti…) v prosté kopii,
- **rozhodnutí příslušného orgánu o nařízení výkonu rozhodnutí** (např. exekuce…) v prosté kopii.

Příklady údajů uváděných v dotazníku fyzické osoby, které souvisejí s novým občanským zákoníkem (zákon č. 89/2012 Sb.)

1) Půjčil jsem kamarádovi peníze a kamarád mi ručí na tuto půjčku svojí nemovitostí. Uvádím vzniklé zástavní právo k jeho nemovitosti při podání žádosti o vydání osvědčení fyzické osoby v dotazníku?

Ano, pokud došlo ke vzniku zástavního práva k nemovitosti vlastněné Vaším kamarádem po 1. 1. 2014. Podle nového občanského zákoníku (zákon č. 89/2012 Sb.) je zástavní právo k nemovitosti samostatnou nemovitostí. V dotazníku uvedete zástavní právo do bodu:

9.9 Nemovitý majetek

9.9.1 Vedeno u katastrálního úřadu (v případě nemovitosti mimo Českou republiku uveďte adresu) – **katastrální úřad, kde se nachází nemovitost vlastněná kamarádem, k níž bylo zřízeno zástavní právo**

9.9.2 Popis nemovitosti a způsob jejího využití – **zástavní právo**

9.9.3 Způsob nabytí – **ostatní**

9.9.4 Vlastní odhad ceny – **0**

9.9.5 Nabývací cena – **0**

9.9.6 Měna – **CZK**

2) Tchán mi umožnil postavit chatu na jeho zahradě. Uvádím tuto skutečnost při podání žádosti o vydání osvědčení fyzické osoby v dotazníku?

Ano, pokud k této skutečnosti, bez ohledu na to, zda se jedná o chatu již postavenou nebo dosud nepostavenou, došlo po 1. 1. 2014. Podle nového občanského zákoníku (zákon č. 89/2012 Sb.) se jedná **o právo stavby**, které je samostatnou nemovitostí. V dotazníku uvedete právo stavby do bodu:

9.9 Nemovitý majetek

9.9.1 Vedeno u katastrálního úřadu (v případě nemovitosti mimo Českou republiku uveďte adresu) – **katastrální úřad, kde se nachází pozemek Vašeho tchána**

9.9.2 Popis nemovitosti a způsob jejího využití – **právo stavby**

9.9.3 Způsob nabytí – **např. ostatní**

9.9.4 Vlastní odhad ceny – **0**

9.9.5 Nabývací cena – **např. 0; v případě, že jste za právo stavby zaplatil např. 50000 Kč**

9.9.6 Měna – **CZK**

3) Bydlím v bytě, který není v mém osobním vlastnictví/spoluvlastnictví, ale je majetkem družstva, já vlastním družstevní podíl. Uvádím tento byt při podání žádosti o vydání osvědčení fyzické osoby v dotazníku?

Ano, pokud jste nabyl družstevní podíl po 1. 1. 2014. Podle nového občanského zákoníku (zákon č. 89/2012 Sb.) je družstevní podíl věcí movitou. V dotazníku uvedete družstevní podíl do bodu:

9.8 Movitý majetek
(podle druhů, jejichž hodnota v případě jednoho druhu převyšuje 100 000 Kč, např. sbírka, osobní automobil, starožitnosti, technika, elektronika)

9.8.1 Druh – **družstevní podíl + procentuální podíl**

9.8.2 Počet kusů – **0**

9.8.3 Celková hodnota – **např. 800 000 Kč**

Náležitosti žádosti o vydání osvědčení podle § 94 odst. 4 a 5 zákona

Pokud fyzická osoba, která má mít přístup k utajovaným informacím po uplynutí platnosti stávajícího osvědčení, požádá o vydání nového osvědčení před uplynutím doby platnosti dosavadního osvědčení ve lhůtě nejméně:

- **3 měsíců** u nové žádosti o vydání osvědčení pro stupeň utajení Důvěrné,
- **7 měsíců** u nové žádosti o vydání osvědčení pro stupeň utajení Tajné,
- **10 měsíců** u nové žádosti o vydání osvědčení pro stupeň utajení Přísně tajné,

předkládá žadatel tyto materiály:

1. **formulář žádost o vydání osvědčení**, který ve své první části obsahuje
   - identifikační údaje žadatele,
   - zdůvodnění nutnosti přístupu k utajované informaci žadatelem (včetně uvedení funkce nebo činnosti v rámci služebního poměru nebo pracovněprávního, členského či obdobného vztahu, na jehož základě má být osvědčení vydáno),
   - stupeň utajení, pro který žádá o vydání osvědčení,
   - prohlášení, že údaje uvedené v žádosti a jejích přílohách jsou pravdivé, žadatel se seznámil s podmínkami bezpečnostního řízení a souhlasí s jeho provedením,
   - místo a datum vyplnění,
   - podpis žadatele.

   Dále obsahuje
   - potvrzení zdůvodnění nutnosti přístupu k utajované informaci odpovědnou osobou, bezpečnostním ředitelem nebo tím, kdo bude utajovanou informaci žadateli poskytovat, jež tvoří
     - identifikační údaje tohoto subjektu,
     - označení konkrétního místa nebo funkce stanovené podle § 69 odst. 1 písm. b) zákona č. 412/2005 Sb. a zařazení tohoto místa nebo funkce v tomto přehledu,
     - specifikaci utajovaných informací, které na daném místě nebo funkci již byly poskytnuty nebo

vznikaly, a utajovaných informací, které zde budou poskytnuty nebo zde mohou vznikat, tato položka musí obsahovat tytéž informace, jež jsou podrobně uvedeny v bodu 1 kapitoly **Náležitosti základní žádosti o vydání osvědčení podle zákona č. 412/2005 Sb.,**

- místo a datum vyplnění,
- podpis a otisk razítka.

2. **prohlášení žadatele o svéprávnosti** (od 1. 1. 2014 je platný nový formulář prohlášení fyzické osoby o svéprávnosti, jehož vzor je uveden v příloze č. 1 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti),
3. **prohlášení žadatele k osobnostní způsobilosti,**
4. **prohlášení o zproštění povinnosti mlčenlivosti věcně a místně příslušného správce daně a jiné osoby zúčastněné na správě daní podle § 52 odst. 2 daňového řádu, a to v plném rozsahu údajů za účelem provedení bezpečnostního řízení,**
5. **je-li žadatel cizincem, doklad obdobný výpisu z evidence Rejstříku trestů státu, jehož je státním příslušníkem, jakož i státu, v němž pobýval nepřetržitě po dobu delší než 6 měsíců** (u stupně Důvěrné 10 let zpětně, u stupně Tajné 15 let zpětně, u stupně Přísně tajné 20 let zpětně), doklad nesmí být starší než 3 měsíce,
6. **fotografii žadatele 35 x 45 mm,**
7. **vyplněný dotazník fyzické osoby v listinné i elektronické podobě (soubor výhradně ve formátu .zfo, nebo .xml)** s tím, že v dotazníku fyzické osoby se vyplňují pouze **základní identifikační údaje, v rozsahu jméno, příjmení, rodné číslo, pokud nebylo přiděleno, datum narození, příjmy s uvedením jejich výše po odečtení povinných zákonných odvodů za období od podání předchozí žádosti a údaje, které se změnily v průběhu platnosti osvědčení a nebyly oznámeny podle § 10 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti** – od 1. 1. 2014 je platný nový formulář dotazníku fyzické osoby, jehož vzor je uveden v příloze č. 6 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti,
8. **potvrzení zaměstnavatele o příjmech s uvedením jejich výše po odečtení povinných zákonných odvodů, v případě jiného druhu příjmu daňové přiznání** (musí být ověřeno příslušným finančním úřadem, nepostačuje kopie s podacím razítkem podatelny příslušného finančního úřadu – může být nahrazeno též např. výpisem údajů daně z příjmu fyzických osob příslušného finančního úřadu) **nebo jiný doklad potvrzující tento příjem, za období od podání předchozí žádosti** (např. v případě podpory v nezaměstnanosti – potvrzení příslušného úřadu práce, dále potvrzení o rodičovském příspěvku, sociálním příspěvku, zaopatřovacím příspěvku, dávkách pěstounské péče, porodném, pohřebném, vdovském důchodu, příspěvku na bydlení, odchodném, příspěvku za službu, rozhodnutí o výši přídavku na dítě, pokud je již žadateli vyplácen, rozhodnutí o sociálních dávkách, které jsou přiznány v případě neposkytnutí podpory v nezaměstnanosti, rozsudek o schválení dohody rodičů o výši výživného na děti, v případě prodeje nemovitosti smlouvu o prodeji …) v originále nebo úředně ověřené kopii,
9. **písemnosti dosvědčující správnost údajů uvedených v dotazníku fyzické osoby, stanoví-li tak vyhláška o personální bezpečnosti a o bezpečnostní způsobilosti** – viz výše – bod 8 kapitoly **Náležitosti základní žádosti o vydání osvědčení podle zákona č. 412/2005 Sb.**

Pro příklad uvádíme:

Fyzická osoba při podání základní žádosti o vydání osvědčení podle zákona č. 412/2005 Sb. uvedla v dotazníku fyzické osoby mimo jiné účty, nejvyšší ukončené vzdělání (např. střední škola). Po vydání osvědčení u ní došlo ke změně účtu, vzniku finančního závazku – úvěru ve výši 20 tisíc Kč, a změnilo se její nejvyšší ukončené vzdělání (vysoká škola). Fyzická osoba má v tomto případě podle § 10 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti povinnost oznámit pouze nejvyšší dosažené vzdělání, které je povinna zároveň doložit originálem nebo úředně ověřenou kopií dokladu potvrzujícího správnost tohoto údaje. Změnu účtu a vznik finančního závazku – úvěru ve výši 20 tisíc Kč nemá povinnost oznámit. Fyzická osoba tedy oznámí a požadovanou písemností doloží nejvyšší dosažené vzdělání.

Při podání následné žádosti o vydání osvědčení podle § 94 odst. 4 a 5 zákona č. 412/2005 Sb. je pak povinna v dotazníku fyzické osoby uvést údaje uvedené pod bodem 7. včetně údajů o změněném účtu a uzavření finančního závazku – úvěru ve výši 20 tisíc Kč, který musí i doložit písemností dosvědčující jeho správnost, a to v prosté kopii – viz bod 9.

Upozornění

Pokud fyzická osoba nedodrží výše uvedené minimální lhůty pro podání žádosti o vydání osvědčení podle § 94 odst. 4 a 5 zákona č. 412/2005 Sb., bude její povinností podat novou kompletní základní žádost podle zákona č. 412/2005 Sb. – viz výše – kapitola ***Náležitosti základní žádosti o vydání osvědčení podle zákona č. 412/2005 Sb.***

Za žádost podle § 94 odst. 4 a 5 zákona č. 412/2005 Sb. není považovaná každá následně podaná žádost bez ohledu na skutečnost, jakým způsobem bylo (nebylo) bezpečnostní řízení týkající se předchozí žádosti ukončeno.

Pro příklad uvádíme:

Podala-li fyzická osoba žádost o vydání osvědčení pro stupeň Důvěrné a řízení:

a) bylo zastaveno,

b) bylo ukončeno rozhodnutím o nevydání osvědčení nebo

c) stále probíhá,

následně fyzickou osobou podaná žádost o vydání osvědčení pro kterýkoliv stupeň musí být novou kompletní základní žádostí podle zákona č. 412/2005 Sb. – viz výše – kapitola ***Náležitosti základní žádosti o vydání osvědčení podle zákona č. 412/2005 Sb.***

Na fyzické osoby, které podaly žádost o vydání osvědčení podle zákona č. 412/2005 Sb. před 1. 1. 2012, se vztahují stejná pravidla (práva i povinnosti) jako na osoby, které podají žádost o vydání osvědčení po 1. 1. 2012.

Způsob a forma podání žádosti o vydání osvědčení

Nejběžnějším způsobem podání žádosti je osobní podání (možnost objednat se na tel. č. 257 283 225) v podatelně místa sídla Úřadu (Na Popelce 2/16, Praha 5 – Košíře), v úředních hodinách.

Úřední hodiny podatelny	
Pondělí a středa:	8:00 – 17:00
Úterý a čtvrtek:	8:00 – 15:00
Pátek:	8:00 – 12:00

Osobní podání je pro žadatele výhodné, protože pracovníci Úřadu mu mohou pomoci odstranit formální nedostatky v žádosti na místě. Žadateli je také vydáno potvrzení o převzetí žádosti.

Žádost lze také zaslat prostřednictvím držitele poštovní licence nebo zvláštní poštovní licence na adresu Úřadu (P.O.BOX 49, Praha 56, PSČ 150 06) nebo ji nechat doručit na podatelnu Úřadu prostřednictvím jiné, k tomu účelu pověřené, osoby.

Vyplněný dotazník fyzické osoby je v tomto případě podáván zároveň v elektronické podobě.

V elektronické podobě lze podat žádost dodáním do **datové schránky Úřadu** (ID Úřadu – h93aayw, do pole „Věc“ se uvede „Žádost o vydání osvědčení fyzické osoby“) nebo na **elektronickou podatelnu Úřadu** (posta@nbu.cz, do pole „Předmět“ se uvede „Žádost o vydání osvědčení fyzické osoby“).

V těchto případech podání:

- **formulář žádost o vydání osvědčení fyzické osoby** musí být výstupem z autorizované konverze nebo musí být podepsaný fyzickou osobou a odpovědnou osobou, a to zaručeným elektronickým podpisem,
- **prohlášení o zproštění povinnosti mlčenlivosti** věcně a místně příslušného správce daně a jiné osoby zúčastněné na správě daní musí být výstupem z autorizované konverze nebo musí být podepsané fyzickou osobou, a to zaručeným elektronickým podpisem,

- je-li žadatel cizincem, **doklad obdobný výpisu z evidence Rejstříku trestů státu, jehož je státním příslušníkem, jakož i státu, v němž pobýval nepřetržitě po dobu delší než 6 měsíců** (u stupně Důvěrné 10 let zpětně, u stupně Tajné 15 let zpětně, u stupně Přísně tajné 20 let zpětně), musí být výstupem autorizované konverze a jeho úředně ověřená kopie překladu do českého jazyka musí být také výstupem z autorizované konverze nebo musí být podepsaná osobou, která úřední ověření provedla, a to zaručeným elektronickým podpisem,
- **doklad o nejvyšším dosaženém vzdělání** musí být výstupem z autorizované konverze,
- **potvrzení zaměstnavatele o příjmech s uvedením jejich výše po odečtení povinných zákonných odvodů, v případě jiného druhu příjmu daňové přiznání nebo jiný doklad potvrzující tento příjem** musí být výstupy z autorizované konverze nebo musí být podepsány osobou, která tuto písemnost vydala, a to zaručeným elektronickým podpisem,
- **prohlášení žadatele o svéprávnosti, prohlášení žadatele k osobnostní způsobilosti, dotazník fyzické osoby a další písemnosti dosvědčující správnost údajů uvedených v dotazníku** nemusí splňovat požadavky uvedené v předchozích bodech, u dodání na elektronickou podatelnu musí být jejich podání podepsané fyzickou osobou, a to zaručeným elektronickým podpisem,
- **dotazník fyzické osoby musí být předložen také v listinné podobě.**

4. Informace k podání žádosti o vydání osvědčení fyzické osoby pro cizí moc (dále jen „certifikát“)

Certifikát potvrzuje cizí moci, že u jeho držitele bylo provedeno bezpečnostní řízení v souladu s příslušnými právními předpisy ČR a že je držitelem platného osvědčení daného stupně utajení.

Kdy vydává Úřad certifikát

- má-li mít fyzická osoba přístup k utajované informaci NATO, splňuje-li podmínky podle § 11 zákona č. 412/2005 Sb., a požaduje-li tak NATO,
- je-li to v souladu s bezpečnostními a ekonomickými zájmy České republiky a se závazky vyplývajícími pro Českou republiku z mezinárodní smlouvy,
- neprobíhá-li s danou osobou řízení podle § 101 odst. 1 zákona č. 412/2005 Sb.

Certifikát je možné vydat pouze na základě písemné odůvodněné žádosti fyzické osoby, jejíž vzor je uveden v příloze č. 8 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti.

Lhůta pro vyřízení žádosti o vydání certifikátu Úřadem není zákonem stanovena.

Certifikát se nevydává osobám uvedeným v § 58 odst. 6 zákona č. 412/2005 Sb. (prezident republiky, předseda Senátu Parlamentu, předseda Poslanecké sněmovny Parlamentu, předseda vlády a ministr zahraničních věcí), které mají přístup k utajovaným informacím cizí moci, aniž by byly držiteli platného osvědčení, respektive certifikátu.

Druhy certifikátů, které jsou Úřadem vydávány

NATO CONFIDENTIAL	NATO CONFIDENTIAL ATOMAL
NATO SECRET	NATO SECRET ATOMAL
COSMIC TOP SECRET	COSMIC TOP SECRET ATOMAL

U stupně utajení Vyhrazené se certifikáty nevystavují.

Pro potřeby orgánů Evropské unie se certifikát nevydává, plně jej nahrazuje „národní“ osvědčení vydané podle zákona č. 412/2005 Sb.

5. Informace k platnosti, zániku platnosti a výměně osvědčení a certifikátu

Osvědčení je veřejnou listinou.

Platnost osvědčení je

- pro stupeň Důvěrné 9 let,
- pro stupeň Tajné 7 let,
- pro stupeň Přísně tajné 5 let,

od data vydání.

Platnost osvědčení zaniká

1. uplynutím doby platnosti osvědčení, úmrtím fyzické osoby nebo byla-li prohlášena za mrtvou,
2. zrušením jeho platnosti (dnem vykonatelnosti rozhodnutí Úřadu o zrušení jeho platnosti),
3. ohlášením jeho odcizení nebo jeho ztráty,
4. poškozením (majícím za následek nečitelnost údajů, porušení celistvosti), změnou některého z údajů v něm uvedených,
5. vznikem služebního poměru příslušníka zpravodajské služby nebo pracovního poměru zaměstnance zařazeného do zpravodajské služby, jde-li o osvědčení, vydané Úřadem,
6. skončením služebního poměru příslušníka zpravodajské služby nebo pracovního poměru zaměstnance zařazeného do zpravodajské služby, nebo dnem, kdy přestane být fyzická osoba osobou uvedenou v § 141 odst. 1 zákona č. 412/2005 Sb., jde-li o osvědčení, vydané příslušnou zpravodajskou službou nebo Ministerstvem vnitra,
7. vrácením jeho držitelem tomu, kdo jej vydal,
8. dnem doručení nového osvědčení (pro jakýkoliv stupeň),
9. dnem doručení rozhodnutí o nevydání osvědčení pro stejný stupeň utajení.

Práva a povinnosti fyzické osoby v případě zániku platnosti osvědčení

a) **V případech zániku platnosti osvědčení podle bodu 2, 4 až 6, 8 nebo 9** má fyzická osoba **povinnost vrátit osvědčení do 15 dnů** tomu, kdo jej vydal (§ 66 odst. 1 písm. b) zákona č. 412/2005 Sb.).

b) **V případě odcizení nebo ztráty** osvědčení **(bod 3)** má fyzická osoba **povinnost neprodleně ohlásit tuto skutečnost** tomu, kdo vydal osvědčení (§ 66 odst. 1 písm. c) zákona č. 412/2005 Sb.).

Upozornění

Porušením uvedených povinností se fyzická osoba dopouští přestupku, za který lze ***uložit pokutu do 50 000 Kč*** (§ 150 zákona č. 412/2005 Sb.).

c) **V případech zániku platnosti** osvědčení podle **bodu 3 nebo 4** vydá ten, kdo osvědčení vydal, na **základě písemné žádosti fyzické osoby** podané **do 15 dnů** ode dne zániku platnosti osvědčení **do 5 dnů** od jejího doručení nové osvědčení (§ 56 odst. 4 zákona č. 412/2005 Sb.).

Upozornění

Pokud nebude ve stanovené lhůtě žádost podána, zanikne přístup fyzické osoby k utajovaným informacím a fyzická osoba bude muset v případě nutnosti budoucího přístupu k utajované informaci stupně Důvěrné, Tajné nebo Přísně tajné požádat o vydání nového osvědčení příslušného stupně, tzn. bude její povinností podat novou kompletní základní žádost podle zákona č. 412/2005 Sb. – viz výše – kapitola ***Náležitosti základní žádosti o vydání osvědčení podle zákona č. 412/2005 Sb.***

Bude-li toto osvědčení vydáno, musí být fyzická osoba před prvním přístupem k utajované informaci opět poučena.

d) **V případech zániku platnosti** osvědčení podle **bodu 6** vydá Úřad na **základě písemné žádosti fyzické osoby** do 5 dnů od doručení žádosti nové osvědčení (§ 56a odst. 2 písm. c) zákona č. 412/2005 Sb.). **Tato žádost musí být podána do 30 dnů ode dne zániku platnosti osvědčení.**

Obdobně postupuje zpravodajská služba v případech zániku platnosti osvědčení podle bodu 5.

Platnost osvědčení nezaniká jiným než výše uvedeným způsobem, tzn. nedochází k zániku platnosti, např. ukončením pracovního/služebního poměru (s výjimkou bodu 6) – chce-li fyzická osoba v tomto případě zrušit platnost jí vydaného osvědčení, protože již nepředpokládá další přístup k utajovaným informacím, použije postup uvedený v bodu 7.

Certifikát je veřejnou listinou.

Doba platnosti certifikátu (§ 57 odst. 6 zákona č. 412/2005 Sb.)

- může být nejdéle taková, jaká je platnost osvědčení, certifikát je však v zásadě vydáván na dobu nezbytně nutnou.

Platnost certifikátu **zaniká**

1. uplynutím doby jeho platnosti,
2. ohlášením jeho odcizení nebo jeho ztráty,
3. poškozením (majícím za následek nečitelnost údajů, porušení celistvosti),
4. vrácením jeho držitelem Úřadu,
5. dnem doručení rozhodnutí o nevydání osvědčení pro stejný stupeň utajení.

Platnost certifikátu dále **zaniká** zánikem platnosti osvědčení

6. změnou některého z údajů v něm uvedených,
7. úmrtím fyzické osoby nebo byla-li prohlášena za mrtvou,
8. vznikem služebního poměru příslušníka zpravodajské služby nebo pracovního poměru zaměstnance zařazeného do zpravodajské služby,
9. skončením služebního poměru příslušníka zpravodajské služby nebo pracovního poměru zaměstnance zařazeného do zpravodajské služby, nebo dnem, kdy přestane být fyzická osoba osobou uvedenou v § 141 odst. 1 zákona č. 412/2005 Sb.,
10. zrušením jeho platnosti (dnem vykonatelnosti rozhodnutí Úřadu o zrušení jeho platnosti),
11. dnem doručení nového osvědčení (pro stejný nebo jiný stupeň),
12. vrácením jeho držitelem tomu, kdo jej vydal.

Práva a povinnosti fyzické osoby v případě zániku platnosti certifikátu

a) **V případech zániku platnosti** certifikátu podle bodu **3, 5, 6, 8 až 12** má fyzická osoba povinnost vrátit certifikát Úřadu do 15 dnů (§ 57 odst. 8 zákona č. 412/2005 Sb.).

b) **V případě odcizení nebo ztráty** certifikátu **(bod 2)** má fyzická osoba **povinnost neprodleně ohlásit tuto skutečnost Úřadu** (§ 66 odst. 1 písm. c) zákona č. 412/2005 Sb.).

c) **V případě zániku platnosti certifikátu podle bodu 2, 3 nebo 6 vydá Úřad, na základě písemné žádosti, jejíž vzor je uveden v příloze č. 8 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti, nový certifikát.**

Upozornění

Porušením uvedených povinností se fyzická osoba dopouští přestupku, za který lze ***uložit pokutu do 50 000 Kč*** (§ 150 zákona č. 412/2005 Sb.).

Přístup fyzické osoby k utajované informaci cizí moci také zaniká, zanikla-li platnost osvědčení ohlášením jeho odcizení nebo jeho ztráty nebo poškozením (majícím za následek nečitelnost údajů, porušení celistvosti), neboť fyzická osoba přestala splňovat podmínky podle § 11 zákona č. 412/2005 Sb. Pokud fyzická osoba v tomto případě do 15 ode dne zániku platnosti osvědčení nepožádá písemně toho, kdo osvědčení vydal, o vydání nového osvědčení, zaniká také platnost certifikátu.

Platnost certifikátu nezaniká jiným než výše uvedeným způsobem, tzn. nedochází k zániku platnosti, např. ukončením pracovního/služebního poměru (s výjimkou bodu 9) – chce-li fyzická osoba v tomto případě zrušit platnost jí vydaného certifikátu, protože již nepředpokládá další přístup k utajovaným informacím cizí moci, použije postup uvedený v bodu 4.

6. Informace k oznamování změn

Změny údajů:

- **v žádosti o vydání osvědčení fyzické osoby,**
- **v prohlášení o svéprávnosti,**
- **v prohlášení k osobnostní způsobilosti nebo**

- **v dotazníku fyzické osoby**

má fyzická osoba povinnost Úřadu neprodleně oznámit, je-li účastníkem řízení (§ 103 odst. 2 zákona č. 412/2005 Sb.) nebo držitelem osvědčení (§ 66 odst. 1 písm. d) zákona č. 412/2005 Sb.).

Fyzická osoba má povinnost oznamovat změny údajů písemně, a to neprodleně – jedná se o právně neurčitý pojem, tzn., jakmile jí to okolnosti dovolí a zároveň bez zbytečného odkladu.

Změny údajů uvedených v dotazníku fyzické osoby oznamuje v rozsahu stanoveném v § 10 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti.

Výčet změn údajů, které je fyzická osoba povinna, v rozsahu položek dotazníku fyzické osoby, oznamovat:

1. **základní identifikační údaje,**
2. **adresa místa trvalého pobytu,**
3. **adresa pro účely doručování,**
4. **zaměstnavatel,**
5. **příslušnost ke spolkům, nadacím a obecně prospěšným společnostem,**
6. **zahájení trestního řízení, respektive trestního stíhání, včetně uvedení, kdy a kým bylo zahájeno a z jakého důvodu,**
7. **nařízení výkonu rozhodnutí,**
8. **údaje k osobě manžela (manželky) nebo partnera (partnerky) a osob starších l8 let žijících s fyzickou osobou v domácnosti.**

Změnu údajů uvedenou pod bodem 7 dokládá fyzická osoba písemností dosvědčující její správnost, písemnost Úřadu předkládá v prosté kopii. Změnu lze doložit např. rozhodnutím soudu o nařízení výkonu rozhodnutí.

Dále je fyzická osoba povinna oznamovat:

1. **nabytí či pozbytí movité věci, jejíž hodnota přesahuje 100 000 Kč nebo pětinásobek průměrného měsíčního příjmu fyzické osoby po odečtení povinných zákonných odvodů, podle toho, která částka je vyšší,**
2. **nabytí či pozbytí nemovitého majetku,**
3. **dosažení vyššího stupně vzdělání,**
4. **vznik závazků, jejichž nominální hodnota jednotlivě nebo v souhrnu přesahuje 100 000 Kč nebo pětinásobek průměrného měsíčního příjmu fyzické osoby po odečtení povinných zákonných odvodů, podle toho, která částka je vyšší,**
5. **mimořádnou splátku závazku, přesáhla-li její hodnota 100 000 Kč nebo pětinásobek průměrného měsíčního příjmu fyzické osoby po odečtení povinných zákonných odvodů, podle toho, která částka je vyšší,**
6. **vznik pohledávek, jejichž nominální hodnota jednotlivě nebo v souhrnu přesahuje 100 000 Kč nebo pětinásobek průměrného měsíčního příjmu fyzické osoby po odečtení povinných zákonných odvodů, podle toho, která částka je vyšší.**

Změny údajů uvedené pod body 3 a 4 dokládá fyzická osoba písemnostmi dosvědčujícími jejich správnost s tím, že písemnost dokládající změnu údajů v bodu 3 předkládá v originále nebo úředně ověřené kopii, písemnost dokládající změnu údajů v bodu 4 předkládá v prosté kopii.

Změnu v bodu 3 lze doložit např. diplomem, změnu v bodu 4 např. smlouvou o úvěru, smlouvou o půjčce apod.

Upozornění

Vzhledem ke skutečnosti, že povinností fyzické osoby je oznamovat také změny v žádosti o vydání osvědčení fyzické osoby (formulář), je nutné, pokud dojde ke změně zaměstnání, kdy fyzická osoba bude mít i nadále přístup k utajovaným informacím, nahlásit i novou odpovědnou osobu (fyzická osoba ukončí

služební poměr u Policie ČR a nastoupí k Ministerstvu obrany, kde bude mít přístup k utajovaným informacím – odpovědná osoba Ministerstva obrany je novou odpovědnou osobou).

V případě, že dojde ke změně zaměstnání a v novém zaměstnání již fyzická osoba nebude mít přístup k utajovaným informacím, je nutné Úřadu oznámit, že dosavadní odpovědná osoba již odpovědnou osobou není (např. fyzická osoba ukončí služební poměr u Policie ČR a v novém zaměstnání již nebude mít přístup k utajovaným informacím – odpovědná osoba Ministerstva vnitra již není odpovědnou osobou).

Zákon č. 412/2005 Sb. neupravuje povinnost držitelů osvědčení oznamovat změny, pokud bylo osvědčení vydáno na základě provedené bezpečnostní prověrky podle zákona č. 148/1998 Sb. Případné oznámení změn ze strany takových osob nicméně není v rozporu se zákonem č. 412/2005 Sb.

Na fyzické osoby, které podaly žádost o vydání osvědčení podle zákona č. 412/2005 Sb. před 1. 1. 2012 a bylo jim vydáno osvědčení nebo bezpečnostní řízení po 1. 1. 2012 bude stále probíhat, se vztahují stejná pravidla pro oznamování změn jako na fyzické osoby, které podají žádost o vydání osvědčení podle zákona č. 412/2005 Sb. po 1. 1. 2012.

Pro příklad uvádíme:

Před 1. 1. 2012 fyzická osoba v dotazníku fyzické osoby vyplňovala údaje k občanskému průkazu, pobytům v zahraničí delším než 30 dnů, finančním závazkům. Po 1. 1. 2012 dojde ke změně občanského průkazu, rovněž zahraničního pobytu delšího než 30 dnů a vzniku finančního závazku – úvěru 650 000 Kč („čistý“ měsíční příjem fyzické osoby je 20 000 Kč). Podle právní úpravy platné do 31. 12. 2011 bylo povinností oznamovat tyto změny všechny. Změna povinností týkající se oznamování změn, která je upravena vyhláškou o personální bezpečnosti a o bezpečnostní způsobilosti, již neobsahuje oznamování změn občanského průkazu a nového pobytu v zahraničí. Finanční závazek v uvedené výši při deklarovaném měsíčním příjmu oznámen být musí a současně musí být doložen písemností dokládající správnost údajů (např. smlouvou o úvěru) v prosté kopii.

Způsob a forma oznamování změn

Pro hlášení změn, v jejichž případě stanoví vyhláška o personální bezpečnosti a o bezpečnostní způsobilosti rozsah položek dotazníku fyzické osoby, lze využít změnový dotazník fyzické osoby, který je k dispozici na internetových stránkách Úřadu (www.nbu.cz), případně jej lze učinit volně formulovaným prohlášením v rozsahu položek dotazníku fyzické osoby.

Oznamování jiných změn lze učinit volně formulovaným prohlášením nebo formou uvedení změněných údajů do elektronických šablon vzorů (žádost o vydání osvědčení fyzické osoby, prohlášení o svéprávnosti, prohlášení k osobnostní způsobilosti), které jsou k dispozici na internetových stránkách Úřadu (www.nbu.cz).

Je-li to požadavek vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti, musí být hlášená změna doložena příslušnými písemnostmi, a to ve stanovené formě (viz výše).

Z oznámení změn musí být patrné, kdo jej činí (je třeba uvést jméno a příjmení, datum narození, případně místo trvalého pobytu) a čeho se týká. Dále toto oznámení musí obsahovat označení orgánu, jemuž je určeno (Úřad) a podpis osoby, která změny oznamuje.

Oznámení změn lze podat v listinné nebo elektronické podobě.

V listinné podobě lze podat oznámení změn osobně nebo prostřednictvím jiné, k tomu účelu pověřené, osoby v podatelně místa sídla Úřadu (Na Popelce 2/16, Praha 5 - Košíře), v úředních hodinách.

Úřední hodiny podatelny	
Pondělí a středa:	8:00 – 17:00
Úterý a čtvrtek:	8:00 – 15:00
Pátek:	8:00 – 12:00

Oznámení změn lze také zaslat prostřednictvím držitele poštovní licence nebo zvláštní poštovní licence na adresu Úřadu (P.O.BOX 49, Praha 56, PSČ 150 06).

V elektronické podobě lze podat oznámení změn dodáním do datové schránky Úřadu (ID Úřadu –

h93aayw, do pole „Věc“ se uvede „Bezpečnostní řízení – Hlášení změn“) nebo na elektronickou podatelnu Úřadu (posta@nbu.cz, do pole „Předmět“ se uvede „Bezpečnostní řízení – Hlášení změn“).

V těchto případech podání

- **formulář žádost o vydání osvědčení fyzické osoby** musí být výstupem z autorizované konverze nebo musí být podepsaný fyzickou osobou a odpovědnou osobou, a to zaručeným elektronickým podpisem,
- **doklad o dosažení vyššího stupně vzdělání musí být výstupem z autorizované konverze,**
- **prohlášení žadatele o svéprávnosti, prohlášení žadatele k osobnostní způsobilosti, změny oznámené volnou formou nebo formou změnového dotazníku a další písemnosti dosvědčující správnost oznamovaných změn** nemusí splňovat požadavky uvedené v předchozích bodech, u dodání na elektronickou podatelnu musí být jejich podání podepsané fyzickou osobou, a to zaručeným elektronickým podpisem.

Jakou sankci lze uložit za nesplnění povinnosti hlásit změny

- až 50 000 Kč (§ 148 a § 150 zákona č. 412/2005 Sb.)

Neoznámení změny může být Úřadem rovněž vyhodnoceno jako bezpečnostní riziko ve smyslu § 14 odst. 3 zákona č. 412/2005 Sb., což může mít za následek nevyhovění žádosti o vydání osvědčení fyzické osoby, resp. zrušení platnosti existujícího osvědčení.

7. Informace k přístupu k utajovaným informacím

Přístup k utajovaným informacím může mít:

1. fyzická osoba, která je:
   - v případě utajovaných informací stupně utajení VYHRAZENÉ držitelem oznámení, platného dokladu nebo osvědčení pro stupeň utajení DŮVĚRNÉ, TAJNÉ, PŘÍSNÉ TAJNÉ a zároveň svým podpisem stvrdila poučení,
   - v případě utajované informace stupně utajení DŮVĚRNÉ, TAJNÉ, nebo PŘÍSNÉ TAJNÉ držitelem platného osvědčení odpovídajícího nebo vyššího stupně a zároveň svým podpisem stvrdila poučení,
2. fyzická osoba se zvláštním přístupem k utajované informaci (§ 58 zákona č. 412/2005 Sb.),
3. fyzická osoba, které bylo uznáno bezpečnostní oprávnění vydané úřadem cizí moci, která je zároveň poučena,
4. fyzická osoba, které byl udělen souhlas s jednorázovým přístupem k utajované informaci (§ 59 zákona č. 412/2005 Sb.), která je zároveň poučena,
5. fyzická osoba, která není držitelem osvědčení nebo nemá přístup k utajovaným informacím stupně utajení Vyhrazené, a to v případě účasti ČR v ozbrojeném konfliktu v zahraničí nebo v záchranné nebo humanitární akci v zahraničí, v případě vyhlášení válečného stavu a v případě stavu nebezpečí, nouzového stavu nebo stavu ohrožení státu (§ 60 zákona č. 412/2005 Sb.).

Ad 1)

	Přístup k utajované informaci stupně Vyhrazené	**Přístup k utajované informaci stupně Důvěrné nebo Tajné nebo Přísně tajné**
Typ dokumentu nebo veřejné listiny	Oznámení	
	Osvědčení	Osvědčení
	Doklad o bezpečnostní způsobilosti	

Poučení

Fyzická osoba musí být poučena nejpozději před prvním přístupem k utajované informaci o svých povinnostech při nakládání a manipulaci s utajovanými informacemi a o zákonných normách v dané oblasti.

Poučení podepisuje vždy ten, kdo jej provedl (zpravidla odpovědná osoba nebo osoba jí určená), a fyzická osoba. Pro stupeň VYHRAZENÉ se vyhotovuje ve dvou výtiscích, kdy jeden předá fyzické osobě a jeden uloží ten, kdo poučení provedl, na místě určeném pro ukládání těchto dokumentů ve smyslu ustanovení § 68 odst. 1 zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. Pro stupně DŮVĚRNÉ, TAJNÉ a PŘÍSNĚ TAJNÉ se poučení vyhotovuje ve třech výtiscích. Jeden předá fyzické osobě a jeden uloží ten, kdo poučení provedl, na místě určeném pro ukládání těchto dokumentů a jeden zašle Úřadu.

Platnost poučení je ukončena zánikem platnosti oznámení nebo osvědčení **a rovněž skončením služebního poměru nebo pracovněprávního, členského či obdobného vztahu, ve kterém byl fyzické osobě umožněn přístup k utajované informaci, tzn. že v případech, kdy dojde následně ke vzniku nového služebního poměru nebo pracovněprávního, členského či obdobného vztahu, je povinností odpovědné osoby nebo jí určené osoby fyzickou osobu znovu poučit.**

Pokud je fyzická osoba držitelem platného národního osvědčení a odpovědná osoba ví, že fyzická osoba bude muset být i držitelem certifikátu, může odpovědná osoba poučit fyzickou osobu a v poučení zaškrtnout, že fyzická osoba byla seznámena s předpisy NATO, aniž by byla fyzická osoba již držitelem platného certifikátu, a tím v rámci jednoho poučení splnit povinnost stanovenou jak pro přístup k národní utajované informaci, tak i pro přístup k utajované informaci cizí moci. V poučení se uvádí pouze číslo národního osvědčení. V rámci poučení lze seznámit zároveň se všemi právními předpisy v oblasti utajovaných informací, tzn. s předpisy NATO, EU. V tomto případě se z důvodu následného přístupu fyzické osoby k utajovaným informacím těchto institucí její opětné poučení neprovádí.

Pokud je fyzická osoba držitelem platného národního osvědčení a je poučena, aniž by byla seznámena s předpisy NATO, EU a následně je fyzické osobě vydán certifikát, má mít přístup k utajovaným informacím cizí moci, musí být fyzická osoba opětovně poučena s tím, že v poučení se uvede číslo národního osvědčení, nikoliv číslo certifikátu, a zaškrtne se, že fyzická osoba byla seznámena s příslušnými předpisy.

Ad 2)

Zvláštní přístup (§ 58 zákona č. 412/2005 Sb.)

K utajovaným informacím mají bez platného osvědčení a poučení přístup

- prezident republiky, poslanci a senátoři Parlamentu, členové vlády, Veřejný ochránce práv a jeho zástupce, soudci a členové Nejvyššího kontrolního úřadu včetně prezidenta a viceprezidenta (§ 58 odst. 1 zákona č. 412/2005 Sb.).

Tyto osoby mají přístup ode dne zvolení nebo jmenování do funkce po celou dobu jejího výkonu a v rozsahu nezbytném pro výkon této funkce.

Tyto osoby, s výjimkou prezidenta republiky, předsedy Senátu Parlamentu, předsedy Poslanecké sněmovny Parlamentu, předsedy vlády a ministra zahraničních věcí, **nemají bez platného osvědčení a popř. certifikátu a poučení přístup k utajované informaci cizí moci** (§ 58 odst. 6 zákona č. 412/2005 Sb.).

Přístup k utajovaným informacím bez platného osvědčení lze umožnit:

- fyzické osobě jednající ve prospěch zpravodajské služby, informátorovi nebo fyzické osobě, které je poskytována zvláštní nebo krátkodobá ochrana podle zvláštního předpisu, nebo příslušníku zpravodajské služby, který je zařazen v záloze zvláštní (§ 58 odst. 3 zákona č. 412/2005 Sb.).

Poučení této osoby provede ten, kdo jí přístup k utajované informaci umožní.

Těmto osobám nelze bez platného osvědčení a popř. certifikátu a poučení umožnit přístup k utajované informaci cizí moci.

V rámci trestního řízení, občanského soudního řízení, správního řízení a soudního řízení správního je osobám bez platného osvědčení umožněn přístup k utajované informaci za účelem uplatnění jejich práv a plnění povinností v těchto řízeních. Podmínky a výčet osob, kterých se týká taková možnost, jsou stanoveny Trestním řádem, Občanským soudním řádem, Správním řádem a Soudním řádem správním. Přístup k utajované informaci je i v těchto případech umožněn na základě poučení, které musí obsahovat spisové označení věci, která je předmětem řízení, a poučení o tom, že údaje o osobách se zvláštním přístupem jsou evidovány Úřadem. Poučení provede ten, o kom tak stanoví Trestní řád, Občanský soudní řád, Správní řád nebo Soudní řád správní, a současně s fyzickou osobou je i podepisuje.

Ad 3)

Přístup k utajované informaci na základě uznání bezpečnostního oprávnění vydaného úřadem cizí moci (§ 62 zákona č. 412/2005 Sb.)

Na základě žádosti fyzické osoby provede Úřad uznání cizího bezpečnostního oprávnění. Žádost lze podat i prostřednictvím úřadu cizí moci, který má v působnosti ochranu utajovaných informací. Jedná se o případy, kdy to umožňuje mezinárodní smlouva, kterou je ČR vázána, nebo kdy je uznání v souladu se zahraničně politickými a bezpečnostními zájmy ČR. Na toto uznání není právní nárok.

K žádosti je nutné přiložit úřední překlad bezpečnostního oprávnění nebo jeho úředně ověřenou kopii; tyto doklady se nevyžadují, je-li žádost podána prostřednictvím úřadu cizí moci, který má v působnosti ochranu utajovaných informací, pokud tento na žádosti potvrdí, že žadatel je držitelem příslušného bezpečnostního oprávnění.

Žádost musí obsahovat také důvod, proč má být uznání provedeno, a dobu, na jakou má být provedeno. Pokud je bezpečnostní oprávnění uznáno, odpovědná osoba provede poučení fyzické osoby.

Ad 4)

Jednorázový přístup k utajované informaci (§ 59, § 61 zákona č. 412/2005 Sb.)

Úřad může ve výjimečných a odůvodněných případech vydat souhlas s jednorázovým přístupem k utajované informaci o jeden stupeň vyšším, než na který je vydáno platné osvědčení, nejdéle však na dobu 6 měsíců; jednorázový přístup nelze umožnit k utajované informaci stupně PŘÍSNĚ TAJNÉ. **Jednorázový přístup tedy může být udělen pouze pro přístup k** utajované informaci stupně utajení **Tajné**.

Žádost o jednorázový přístup je vždy písemná, podepisuje ji odpovědná osoba a obsahuje zdůvodnění potřeby jednorázového přístupu, označení oblasti utajovaných informací, ke kterým má být přístup umožněn, a požadovanou dobu jednorázového přístupu. Přílohou žádosti musí být kopie osvědčení. Téže osobě lze souhlas udělit jen jednou a není na něj právní nárok. V kladném případě je souhlas vydán nejpozději do 5 dnů.

Pokud je souhlas udělen, odpovědná osoba provede poučení fyzické osoby.

K utajované informaci cizí moci lze jednorázový přístup umožnit pouze v souladu s požadavky této cizí moci.

Ad 5)

Přístup k utajované informaci v případě účasti ČR v ozbrojeném konfliktu v zahraničí nebo v záchranné nebo humanitární akci v zahraničí, v případě vyhlášení válečného stavu a v případě stavu nebezpečí, nouzového stavu nebo stavu ohrožení státu (§ 60 zákona č. 412/2005 Sb.).

Pokud není fyzická osoba držitelem osvědčení nebo nemá přístup k utajovaným informacím stupně utajení Vyhrazené, lze jí, ve výše uvedených případech, umožnit přístup k utajované informaci v případě, že neexistují pochybnosti o její důvěryhodnosti a schopnosti utajovat informace.

Poučení této osoby provede odpovědná osoba. Hrozí-li nebezpečí z prodlení nebo z důvodu jiné naléhavosti a významu konkrétního úkolu, lze poučení nahradit ústním seznámením osoby s jejími povinnostmi v oblasti ochrany utajovaných informací a následky jejich porušení.

K utajované informaci cizí moci lze přístup umožnit pouze v souladu s požadavky této cizí moci.

8. Dokumenty odesílané a přijímané v rámci bezpečnostního řízení prostřednictvím informačního systému datových schránek v oblasti personální bezpečnosti

1) Náležitosti žádostí o vydání osvědčení podle zákona č. 412/2005 Sb. – viz
   3. Informace k podání žádosti o vydání osvědčení (D,T,PT).

2) Oznamování změn – viz
   6. Informace k oznamování změn.

3) Prostřednictvím datové schránky zřízené pro fyzickou osobu lze činit všechny úkony týkající se řízení o vydání osvědčení fyzické osoby (vyjma osobních úkonů).

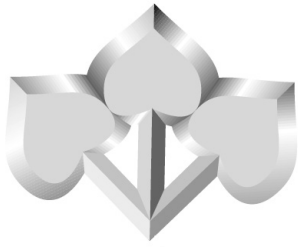
4) Komunikace s orgánem státu, právnickou osobou, podnikající fyzickou osobou, od kterých vyžaduje Úřad informace k účastníkovi řízení nebo držiteli osvědčení.

Upozornění

*Při komunikaci podle bodu 3) a 4) je vhodné uvádět v datové zprávě v poli „**Věc**“ – „**Bezpečnostní řízení**“.*

*V případě, že fyzická osoba nebo subjekt uvedený v bodu 4) reaguje na **písemnost Úřadu (dožádání, sdělení, oznámení, rozhodnutí...)**, je vhodné uvádět také číslo jednací, kterým byla tato písemnost označena (např. 110002/2014-NBÚ/P, 111265/2014-NBÚ/E, ...), a to rovněž do pole „**Věc**“ (např. Bezpečnostní řízení č.j.110002/2014-NBÚ/P...).*

BEZPEČNOSTNÍ ZPŮSOBILOST



BEZPEČNOSTNÍ ZPŮSOBILOST

1. Obecně k bezpečnostní způsobilosti

Bezpečnostní způsobilost je upravena v části třetí zákona č. 412/2005 Sb.

Ověřování podmínek pro vydání dokladu provádí Úřad v bezpečnostním řízení u fyzických osob, které budou vykonávat činnost, jejímž zneužitím by mohlo dojít k ohrožení zájmu České republiky – tzv. „citlivou činnost". Citlivá činnost je, mimo zákona č. 412/2005 Sb., stanovena zvláštními právními předpisy. **Citlivou činnost může vykonávat pouze osoba, která je držitelem platného dokladu nebo platného osvědčení**.

Bezpečnostní řízení lze provádět pouze na základě žádosti o vydání dokladu, kterou podává fyzická osoba. Žádost musí obsahovat písemné zdůvodnění výkonu citlivé činnosti potvrzené odpovědnou osobou.

Právnická osoba, podnikající fyzická osoba a orgán státu jsou povinny zajistit výkon citlivé činnosti pouze osobami, které jsou držiteli platného dokladu nebo osvědčení fyzické osoby. Dále jsou povinny vést evidenci fyzických osob, které vykonávají citlivou činnost a jsou vůči nim ve služebním poměru nebo v pracovně právním, členském či obdobném vztahu, rovněž tak jsou pak povinny zajistit neprodlené písemné oznámení Úřadu o tom, že před vydáním dokladu nebo rozhodnutí o nevydání pominuly skutečnosti, kterými byla žádost odůvodněna, že byl zahájen výkon citlivé činnosti, anebo že byl ukončen z důvodu skončení služebního poměru nebo pracovněprávního, členského či obdobného vztahu držitele dokladu.

Problematiku bezpečnostní způsobilosti upravují ustanovení § 80 – § 88 zákona č. 412/2005 Sb.

Pro vydání dokladu musí fyzická osoba splňovat tyto podmínky:

- svéprávnost,
- věk minimálně 18 let,
- bezúhonnost,
- osobnostní způsobilost,
- spolehlivost.

Citlivé činnosti, pro jejichž výkon musí být fyzická osoba držitelem dokladu nebo osvědčení, jsou stanoveny těmito předpisy:

- zákon č. 38/1994 Sb., o zahraničním obchodu s vojenským materiálem a o doplnění zákona č. 455/1991 Sb., (živnostenský zákon), ve znění pozdějších předpisů, a zákona č. 140/1961 Sb. (trestní zákon), ve znění pozdějších předpisů,
- zákon č. 18/1997 Sb., o mírovém využití jaderné energie a ionizujícího záření (atomový zákon) a o změně některých zákonů, ve znění pozdějších předpisů,
- zákon č. 61/1988 Sb., o hornické činnosti, výbušninách a o státní báňské správě,
- zákon č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů,
- zákon č. 312/2006 Sb., o insolvenčních správcích, ve znění pozdějších předpisů, kdy se od 1. 8. 2013 v souvislosti s nabytím účinnosti zákona č. 185/2013 Sb., kterým byl tento zákon novelizován, považuje za citlivou činnost výkon činnosti insolvenčního správce dlužníka,

Dne 19. 11. 2014 nabyl účinnost zákon č. 266/2014 Sb., kterým se mění zákon č. 229/2013 Sb., o nakládání s některými věcmi využitelnými k obranným a bezpečnostním účelům na území České republiky (zákon o nakládání s bezpečnostním materiálem), ve znění zákona č. 64/2014 Sb. (dále jen „zákon č. 266/2014 Sb.")

Zákon č. 266/2014 Sb. zrušil veškeré citlivé činnosti dosud stanovené zákonem č. 229/2013 Sb.
Jedná se o následující citlivé činnosti:

1. nakládání s bezpečnostním materiálem skupiny 5 nebo 6,
2. výkon funkce člena odpovědného zástupce při činnosti nakládání s bezpečnostním materiálem skupiny 5 nebo 6,
3. výkon funkce člena statutárního orgánu, člena dozorčí rady nebo jiného kontrolního orgánu, pro-

kuristy, odpovědného zástupce, je-li ustanoven, právnické osoby, která nakládá s bezpečnostním materiálem skupiny 5 nebo 6.

Vzhledem ke skutečnosti, že byly zrušeny citlivé činnosti uvedené pod bodem 1 až 3, fyzické osoby již nežádají Úřad o vydání dokladu o bezpečnostní způsobilosti fyzické osoby z důvodu výkonu těchto citlivých činností.

2. Informace k podání žádosti o vydání dokladu

Podle zákona č. 412/2005 Sb. je za podání žádosti o vydání dokladu odpovědný žadatel, jakožto účastník řízení.

V bezpečnostním řízení se jedná a písemnosti se vyhotovují v českém jazyce, pokud nejde o výkon práv příslušníka národnostní menšiny.

V případě písemnosti vyhotovené v cizím jazyce musí účastník řízení tuto předložit v originále a současně v úředně ověřeném překladu do jazyka českého.

Náležitosti základní žádosti o vydání dokladu podle zákona č. 412/2005 Sb.:

1. **formulář žádost o vydání dokladu**, který ve své první části obsahuje
   - identifikační údaje žadatele,
   - uvedení citlivé činnosti, kterou má fyzická osoba na základě vydaného dokladu vykonávat,
   - ustanovení právního předpisu, podle kterého bude vykonávána citlivá činnost,
   - prohlášení, že údaje uvedené v žádosti a jejích přílohách jsou pravdivé, žadatel se seznámil s podmínkami bezpečnostního řízení a souhlasí s jeho provedením,
   - místo a datum vyplnění,
   - podpis žadatele.

   Dále obsahuje
   - potvrzení zdůvodnění výkonu citlivé činnosti odpovědnou osobou nebo jí pověřenou osobou, jež tvoří
     - identifikační údaje tohoto subjektu,
     - popis konkrétního místa nebo funkce vztahující se k výkonu citlivé činnosti,
     - místo a datum vyplnění,
     - podpis a otisk razítka.
2. **prohlášení žadatele o svéprávnosti** (od 1. 1. 2014 je platný nový formulář prohlášení fyzické osoby o svéprávnosti, jehož vzor je uveden v příloze č. 1 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti),
3. **prohlášení žadatele k osobnostní způsobilosti,**
4. **prohlášení žadatele o zproštění povinnosti mlčenlivosti věcně a místně příslušného správce daně a jiné osoby zúčastněné na správě daní podle § 52 odst. 2 daňového řádu, a to v plném rozsahu údajů za účelem provedení bezpečnostního řízení,**
5. **je-li žadatel cizincem, doklad obdobný výpisu z evidence Rejstříku trestů státu, jehož je státním příslušníkem, jakož i státu, v němž pobýval nepřetržitě po dobu delší než 6 měsíců v posledních 10 letech, doklad nesmí být starší než 3 měsíce,**
6. **fotografie žadatele 35 x 45 mm,**
7. **vyplněný dotazník v listinné i elektronické podobě** (soubor výhradně ve formátu .zfo, nebo .xml) – od 1. 1. 2014 je platný nový formulář dotazníku, jehož vzor je uveden v příloze č. 6 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti,
8. písemnosti dosvědčující správnost údajů uvedených v dotazníku
   - **rodný nebo křestní list** v prosté kopii,
   - **doklad o nejvyšším dosaženém vzdělání** (podle stupně dosaženého vzdělání - výuční list, maturitní

vysvědčení, vysokoškolský diplom, postgraduální studium…) v originále nebo úředně ověřené kopii,

- **potvrzení zaměstnavatele o příjmech s uvedením jejich výše po odečtení povinných zákonných odvodů, v případě jiného druhu příjmu daňové přiznání** (musí být ověřeno příslušným finančním úřadem, nepostačuje kopie s podacím razítkem podatelny příslušného finančního úřadu - může být nahrazeno též např. výpisem údajů daně z příjmu fyzických osob příslušného finančního úřadu) **nebo jiný doklad potvrzující tento příjem, za posledních 5 let** (např. v případě podpory v nezaměstnanosti – potvrzení příslušného úřadu práce, dále potvrzení o rodičovském příspěvku, sociálním příspěvku, zaopatřovacím příspěvku, dávkách pěstounské péče, porodném, pohřebném, vdovském důchodu, příspěvku na bydlení, odchodném, příspěvku za službu, rozhodnutí o výši přídavku na dítě, pokud je již žadateli vyplácen, rozhodnutí o sociálních dávkách, které jsou přiznány v případě neposkytnutí podpory v nezaměstnanosti, rozsudek o schválení dohody rodičů o výši výživného na děti, v případě prodeje nemovitosti smlouvu o prodeji …) v originále nebo úředně ověřené kopii,
- **doklad o právu jiné osoby omezující vlastnictví žadatele** (např. smlouva o úvěru, leasingová, hypoteční smlouva, smlouva o ručitelském závazku (pouze v případě, že se ručitel stal dlužníkem a je povinen závazek uhradit), případně výpisy z úvěrových účtů (pokud je v nich uvedena celková původní výše úvěru), v případě zástavního práva k nemovitosti smlouvu o zřízení zástavního práva k nemovitosti nebo výpis z katastru nemovitostí s uvedením zástavního práva k nemovitosti, rozsudek o schválení dohody rodičů o výši výživného na děti…) v prosté kopii,
- **rozhodnutí příslušného orgánu o nařízení výkonu rozhodnutí** (např. exekuce…) v prosté kopii.

Příklady údajů uváděných v dotazníku, které souvisejí s novým občanským zákoníkem (zákon č. 89/2012 Sb.)

1) Půjčil jsem kamarádovi peníze a kamarád mi ručí na tuto půjčku svojí nemovitostí. Uvádím vzniklé zástavní právo k jeho nemovitosti při podání žádosti o vydání dokladu o bezpečnostní způsobilosti v dotazníku?

Ano, pokud došlo ke vzniku zástavního práva k nemovitosti vlastněné Vaším kamarádem po 1. 1. 2014. Podle nového občanského zákoníku (zákon č. 89/2012 Sb.) je zástavní právo k nemovitosti samostatnou nemovitostí. V dotazníku uvedete zástavní právo do bodu:

9.9 Nemovitý majetek

9.9.1 Vedeno u katastrálního úřadu (v případě nemovitosti mimo Českou republiku uveďte adresu) – **katastrální úřad, kde se nachází nemovitost vlastněná kamarádem, k níž bylo zřízeno zástavní právo**

9.9.2 Popis nemovitosti a způsob jejího využití – **zástavní právo**

9.9.3 Způsob nabytí – **ostatní**

9.9.4 Vlastní odhad ceny – **0**

9.9.5 Nabývací cena – **0**

9.9.6 Měna – **CZK**

2) Tchán mi umožnil postavit chatu na jeho zahradě. Uvádím tuto skutečnost při podání žádosti o vydání dokladu o bezpečnostní způsobilosti v dotazníku?

Ano, pokud k této skutečnosti, bez ohledu na to, zda se jedná o chatu již postavenou nebo dosud nepostavenou, došlo po 1. 1. 2014. Podle nového občanského zákoníku (zákon č. 89/2012 Sb.) se jedná **o právo stavby**, které je samostatnou nemovitostí. V dotazníku uvedete právo stavby do bodu:

9.9 Nemovitý majetek

9.9.1 Vedeno u katastrálního úřadu (v případě nemovitosti mimo Českou republiku uveďte adresu) - **katastrální úřad, kde se nachází pozemek Vašeho tchána**

9.9.2 Popis nemovitosti a způsob jejího využití – **právo stavby**

9.9.3 Způsob nabytí – **např. ostatní**

9.9.4 Vlastní odhad ceny – **0**

9.9.5 Nabývací cena – **např. 0; v případě, že jste za právo stavby zaplatil např. 50 000 Kč**

9.9.6 Měna – **CZK**

3) Bydlím v bytě, který není v mém osobním vlastnictví/spoluvlastnictví, ale je majetkem družstva, já vlastním družstevní podíl. Uvádím tento byt při podání žádosti o vydání dokladu o bezpečnostní způsobilosti v dotazníku?

Ano, pokud jste nabyl družstevní podíl po 1. 1. 2014. Podle nového občanského zákoníku (zákon č. 89/2012 Sb.) je družstevní podíl věcí movitou. V dotazníku uvedete družstevní podíl do bodu:

9.8 Movitý majetek
(podle druhů, jejichž hodnota v případě jednoho druhu převyšuje 100 000 Kč, např. sbírka, osobní automobil, starožitnosti, technika, elektronika)

9.8.1 Druh – **družstevní podíl + procentuální podíl**

9.8.2 Počet kusů – **0**

9.8.3 Celková hodnota – **např. 800 000 Kč**

Náležitosti žádosti o vydání dokladu podle § 99 odst. 4 a 5 zákona

Pokud fyzická osoba, která má vykonávat citlivou činnost po uplynutí platnosti stávajícího dokladu, požádá o vydání nového dokladu před uplynutím doby platnosti dosavadního dokladu **ve lhůtě nejméně 5 měsíců**, předkládá žadatel tyto materiály:

1. formulář žádost o vydání dokladu, který ve své první části obsahuje
   - identifikační údaje žadatele,
   - uvedení citlivé činnosti, kterou má fyzická osoba na základě vydaného dokladu vykonávat,
   - ustanovení právního předpisu, podle kterého bude vykonávána citlivá činnost,
   - prohlášení, že údaje uvedené v žádosti a jejích přílohách jsou pravdivé, žadatel se seznámil s podmínkami bezpečnostního řízení a souhlasí s jeho provedením,
   - místo a datum vyplnění,
   - podpis žadatele.

   Dále obsahuje
   - potvrzení zdůvodnění výkonu citlivé činnosti odpovědnou osobou nebo jí pověřenou osobou, jež tvoří
     - identifikační údaje tohoto subjektu,
     - popis konkrétního místa nebo funkce vztahující se k výkonu citlivé činnosti,
     - místo a datum vyplnění,
     - podpis a otisk razítka.
2. **prohlášení žadatele o svéprávnosti** (od 1. 1. 2014 je platný nový formulář prohlášení fyzické osoby o svéprávnosti, jehož vzor je uveden v příloze č. 1 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti,
3. **prohlášení žadatele k osobnostní způsobilosti,**
4. **prohlášení žadatele o zproštění povinnosti mlčenlivosti věcně a místně příslušného správce daně a jiné osoby zúčastněné na správě daní podle § 52 odst. 2 daňového řádu, a to v plném rozsahu údajů za účelem provedení bezpečnostního řízení,**
5. **je-li žadatel cizincem, doklad obdobný výpisu z evidence Rejstříku trestů státu, jehož je státním příslušníkem, jakož i státu, v němž pobýval nepřetržitě po dobu delší než 6 měsíců v posledních 10 letech, doklad nesmí být starší než 3 měsíce,**
6. **fotografii žadatele 35 x 45 mm,**
7. **vyplněný dotazník v listinné i elektronické podobě** (soubor výhradně ve formátu .zfo, nebo .xml) s tím, že v dotazníku se vyplňují pouze **základní identifikační údaje, v rozsahu jméno, příjmení, rodné číslo, pokud nebylo přiděleno, datum narození, příjmy s uvedením jejich výše po odečtení povinných zákonných odvodů za období od podání předchozí žádosti a údaje, které se změnily v průběhu platnosti dokladu a nebyly oznámeny podle § 10 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti** – od 1. 1. 2014 je platný nový formulář dotazníku, jehož vzor je uveden v příloze č. 6 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti,
8. **potvrzení zaměstnavatele o příjmech s uvedením jejich výše po odečtení povinných zákonných odvodů, v případě jiného druhu příjmu daňové přiznání** (musí být ověřeno příslušným finančním

úřadem, nepostačuje kopie s podacím razítkem podatelny příslušného finančního úřadu – může být nahrazeno též např. výpisem údajů daně z příjmu fyzických osob příslušného finančního úřadu) **nebo jiný doklad potvrzující tento příjem, za období od podání předchozí žádosti** (např. v případě podpory v nezaměstnanosti – potvrzení příslušného úřadu práce, dále potvrzení o rodičovském příspěvku, sociálním příspěvku, zaopatřovacím příspěvku, dávkách pěstounské péče, porodném, pohřebném, vdovském důchodu, příspěvku na bydlení, odchodném, příspěvku za službu, rozhodnutí o výši přídavku na dítě, pokud je již žadateli vyplácen, rozhodnutí o sociálních dávkách, které jsou přiznány v případě neposkytnutí podpory v nezaměstnanosti, rozsudek o schválení dohody rodičů o výši výživného na děti, v případě prodeje nemovitosti smlouvu o prodeji …) v originále nebo úředně ověřené kopii,

9. **písemnosti dosvědčující správnost údajů uvedených v dotazníku, stanoví-li tak vyhláška o personální bezpečnosti a o bezpečnostní způsobilosti** – viz výše – bod 8 kapitoly **Náležitosti základní žádosti o vydání dokladu podle zákona č. 412/2005 Sb.**

Pro příklad uvádíme:

Fyzická osoba při podání základní žádosti o vydání dokladu podle zákona č. 412/2005 Sb. uvedla v dotazníku mimo jiné účty, nejvyšší ukončené vzdělání (např. střední škola). Po vydání dokladu u ní došlo ke změně účtu, vzniku finančního závazku – úvěru ve výši 20 tisíc Kč, a změnilo se její nejvyšší ukončené vzdělání (vysoká škola). Fyzická osoba má v tomto případě podle § 10 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti povinnost oznámit pouze nejvyšší dosažené vzdělání, které je povinna zároveň doložit originálem nebo úředně ověřenou kopií dokladu potvrzující správnost tohoto údaje. Změnu účtu a vznik finančního závazku – úvěru ve výši 20 tisíc Kč nemá povinnost oznámit. Fyzická osoba tedy oznámí a požadovanou písemností doloží nejvyšší dosažené vzdělání.

Při podání následné žádosti o vydání dokladu podle § 99 odst. 4 a 5 zákona č. 412/2005 Sb. je pak povinna v dotazníku uvést údaje uvedené pod bodem 7. včetně údajů o změněném účtu a uzavření finančního závazku - úvěru ve výši 20 tisíc Kč, který musí i doložit písemností dosvědčující jeho správnost a to v prosté kopii – viz bod 9.

Upozornění

Pokud fyzická osoba nedodrží výše uvedenou minimální lhůtu pro podání žádosti o vydání dokladu podle § 99 odst. 4 a 5 zákona č. 412/2005 Sb., bude její povinností podat novou kompletní základní žádost podle zákona č. 412/2005 Sb. – viz výše – kapitola ***Náležitosti základní žádosti o vydání dokladu podle zákona č. 412/2005 Sb.***

Za žádost podle § 99 odst. 4 a 5 zákona č. 412/2005 Sb. není považovaná každá následně podaná žádost bez ohledu na skutečnost, jakým způsobem bylo (nebylo) bezpečnostní řízení týkající se předchozí žádosti ukončeno.

Pro příklad uvádíme:

Podala-li fyzická osoba žádost o vydání dokladu a řízení:

a) bylo zastaveno nebo

b) bylo ukončeno rozhodnutím o nevydání dokladu,

následně fyzickou osobou podaná žádost o vydání dokladu musí být novou kompletní základní žádostí podle zákona č. 412/2005 Sb. – viz výše – kapitola ***Náležitosti základní žádosti o vydání dokladu podle zákona č. 412/2005 Sb.***

Na fyzické osoby, které podaly žádost o vydání dokladu podle zákona č. 412/2005 Sb. před 1. 1. 2012, se vztahují stejná pravidla (práva a povinnosti) jako na osoby, které podají žádost o vydání dokladu po 1. 1. 2012.

Způsob a forma podání žádosti o vydání dokladu

Žádost o vydání dokladu lze podat v listinné nebo elektronické podobě.

Nejběžnějším způsobem podání žádosti je osobní podání (možnost objednat se na tel. č. 257 283 225) v podatelně místa sídla Úřadu (Na Popelce 2/16, Praha 5 – Košíře), v úředních hodinách.

Úřední hodiny podatelny	
Pondělí a středa:	8:00 – 17:00
Úterý a čtvrtek:	8:00 – 15:00
Pátek:	8:00 – 12:00

Osobní podání je pro žadatele výhodné, protože pracovníci Úřadu mu mohou pomoci odstranit formální nedostatky v žádosti na místě. Žadateli je také vydáno potvrzení o převzetí žádosti.

Žádost lze také zaslat prostřednictvím držitele poštovní licence nebo zvláštní poštovní licence na adresu Úřadu (P.O.BOX 49, Praha 56, PSČ 150 06) nebo ji nechat doručit na podatelnu Úřadu prostřednictvím jiné, k tomu účelu pověřené, osoby.

Vyplněný dotazník je v tomto případě podáván zároveň v elektronické podobě.

V elektronické podobě lze podat žádost dodáním do **datové schránky Úřadu** (ID Úřadu – h93aayw, do pole „Věc“ se uvede „Žádost o vydání dokladu o bezpečnostní způsobilosti“) nebo na **elektronickou podatelnu Úřadu** (posta@nbu.cz, do pole „Předmět“ se uvede „Žádost o vydání dokladu o bezpečnostní způsobilosti“).

V těchto případech podání:

- **formulář žádost o vydání dokladu** musí být výstupem z autorizované konverze nebo musí být podepsaný fyzickou osobou a odpovědnou osobou, a to zaručeným elektronickým podpisem,
- **prohlášení o zproštění povinnosti mlčenlivosti** věcně a místně příslušného správce daně a jiné osoby zúčastněné na správě daní musí být výstupem z autorizované konverze nebo musí být podepsané fyzickou osobou, a to zaručeným elektronickým podpisem,
- je-li žadatel cizincem, **doklad obdobný výpisu z evidence Rejstříku trestů státu, jehož je státním příslušníkem, jakož i státu, v němž pobýval nepřetržitě po dobu delší než 6 měsíců v posledních 10 letech**, musí být výstupem autorizované konverze a jeho úředně ověřená kopie překladu do českého jazyka musí být také výstupem z autorizované konverze nebo musí být podepsaná osobou, která úřední ověření provedla a to zaručeným elektronickým podpisem,
- **doklad o nejvyšším dosaženém vzdělání** musí být výstupem z autorizované konverze,
- **potvrzení zaměstnavatele o příjmech s uvedením jejich výše po odečtení povinných zákonných odvodů, v případě jiného druhu příjmu daňové přiznání nebo jiný doklad potvrzující tento příjem** musí být výstupem z autorizované konverze nebo musí být podepsaný osobou, která tuto písemnost vydala, a to zaručeným elektronickým podpisem,
- **prohlášení žadatele o svéprávnosti, prohlášení žadatele k osobnostní způsobilosti, dotazník a další písemnosti dosvědčující správnost údajů uvedených v dotazníku** nemusí splňovat požadavky uvedené v předchozích bodech, u dodání na elektronickou podatelnu musí být jejich podání podepsané fyzickou osobou, a to zaručeným elektronickým podpisem,
- **dotazník musí být předložen také v listinné podobě.**

3. Informace k platnosti, zániku platnosti a výměně dokladu

Doklad je veřejnou listinou.

Platnost dokladu je 5 let od data vydání.

Platnost dokladu **zaniká**

1. uplynutím doby platnosti dokladu, úmrtím fyzické osoby nebo byla-li prohlášena za mrtvou,
2. zrušením jeho platnosti (dnem vykonatelnosti rozhodnutí Úřadu o zrušení jeho platnosti),
3. ohlášením jeho odcizení nebo jeho ztráty,
4. poškozením (majícím za následek nečitelnost údajů, porušení celistvosti), změnou některého z údajů v něm uvedených,
5. vrácením dokladu jeho držitelem Úřadu,
6. dnem doručení osvědčení nebo nového dokladu.

Práva a povinnosti fyzické osoby v případě zániku platnosti dokladu

a) **V případech zániku platnosti dokladu podle bodu 2, 4 a 6** má fyzická osoba **povinnost vrátit doklad do 15 dnů** Úřadu (§ 87 odst. 1 písm. a) zákona č. 412/2005 Sb.).

b) **V případě odcizení nebo ztráty dokladu (bod 3)** má fyzická osoba **povinnost neprodleně ohlásit tuto skutečnost** Úřadu (§ 87 odst. 1 písm. b) zákona č. 412/2005 Sb.).

Upozornění

Porušením uvedených povinností se fyzická osoba dopouští přestupku, za který lze uložit pokutu do 50 000 Kč (§ 152 zákona č. 412/2005 Sb.).

c) **V případech zániku platnosti** dokladu podle **bodu 3 nebo 4** vydá Úřad, na **základě písemné žádosti fyzické osoby** podané **do 15 dnů** ode dne zániku platnosti dokladu **do 5 dnů** od jejího doručení nový doklad (§ 85 odst. 4 zákona č. 412/2005 Sb.).

Upozornění

Pokud nebude ve stanovené lhůtě žádost podána, zanikne fyzické osobě možnost vykonávat citlivou činnost a fyzická osoba bude muset, v případě nutnosti budoucího výkonu citlivé činnosti, požádat o vydání nového dokladu, tzn. bude její povinností podat novou kompletní základní žádost podle zákona č. 412/2005 Sb. – viz výše – kapitola ***Náležitosti základní žádosti o vydání dokladu podle zákona č. 412/2005 Sb.***

Platnost dokladu nezaniká jiným než výše uvedeným způsobem, tzn., nedochází k zániku platnosti např. ukončením pracovního/služebního poměru ani ukončením výkonu citlivé činnosti – chce-li fyzická osoba v tomto případě zrušit platnost jí vydaného dokladu, protože již nepředpokládá další výkon citlivé činnosti, užije postup uvedený v bodu 5.

4. Informace k oznamování změn

Změny údajů:

- **v žádosti o vydání dokladu,**
- **v prohlášení o svéprávnosti,**
- **v prohlášení k osobnostní způsobilosti nebo**
- **v dotazníku**

má fyzická osoba povinnost Úřadu neprodleně oznámit, je-li účastníkem řízení (§ 103 odst. 2 zákona č. 412/2005 Sb.) nebo držitelem dokladu (§ 87 odst. 1 písm. c) zákona č. 412/2005 Sb.).

Fyzická osoba má povinnost oznamovat změny údajů písemně, a to neprodleně - jedná se o právně neurčitý pojem, tzn., jakmile jí to okolnosti dovolí a zároveň bez zbytečného odkladu.

Změny údajů uvedených v dotazníku oznamuje v rozsahu stanoveném v § 10 vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti.

Výčet změn údajů, které je fyzická osoba povinna, v rozsahu položek dotazníku, oznamovat

1. **základní identifikační údaje,**
2. **adresa místa trvalého pobytu,**
3. **adresa pro účely doručování,**
4. **zaměstnavatel,**
5. **příslušnost k nadacím, spolkům a obecně prospěšným společnostem,**
6. **zahájení trestního řízení, respektive trestního stíhání, včetně uvedení, kdy a kým bylo zahájeno a z jakého důvodu,**
7. **nařízení výkonu rozhodnutí.**

Změnu údajů uvedenou pod bodem 7 dokládá fyzická osoba písemností dosvědčující její správnost, písemnost Úřadu předkládá v prosté kopii. Změnu lze doložit např. rozhodnutím soudu o nařízení výkonu rozhodnutí.

Dále je fyzická osoba povinna oznamovat

1. **nabytí či pozbytí movité věci, jejíž hodnota přesahuje 100 000 Kč nebo pětinásobek průměrného měsíčního příjmu fyzické osoby po odečtení povinných zákonných odvodů, podle toho, která částka je vyšší,**
2. **nabytí či pozbytí nemovitého majetku,**
3. **dosažení vyššího stupně vzdělání,**
4. **vznik závazků, jejichž nominální hodnota jednotlivě nebo v souhrnu přesahuje 100 000 Kč nebo pětinásobek průměrného měsíčního příjmu fyzické osoby po odečtení povinných zákonných odvodů, podle toho, která částka je vyšší,**
5. **mimořádnou splátku závazku, přesáhla-li její hodnota 100 000 Kč nebo pětinásobek průměrného měsíčního příjmu fyzické osoby po odečtení povinných zákonných odvodů, podle toho, která částka je vyšší,**
6. **vznik pohledávek, jejichž nominální hodnota jednotlivě nebo v souhrnu přesahuje 100 000 Kč nebo pětinásobek průměrného měsíčního příjmu fyzické osoby po odečtení povinných zákonných odvodů, podle toho, která částka je vyšší.**

Změny údajů uvedené pod body 3 a 4 dokládá fyzická osoba písemnostmi dosvědčujícími jejich správnost s tím, že písemnost dokládající změnu údajů v bodu 3 předkládá v originále nebo úředně ověřené kopii, písemnost dokládající změnu údajů v bodu 4 předkládá v prosté kopii.

Změnu v bodu 3 lze doložit např. diplomem, změnu v bodu 4 např. smlouvou o úvěru, smlouvou o půjčce apod.

Upozornění

Vzhledem ke skutečnosti, že je povinností fyzické osoby je oznamovat také změny v žádosti o vydání dokladu (formulář), je nutné, pokud dojde ke změně zaměstnání, kde bude fyzická osoba i nadále vykonávat citlivou činnost, nahlásit i novou odpovědnou osobu (např. fyzická osoba ukončí pracovní poměr u ČEZ a.s. a nastoupí do pracovního poměru ke společnosti Česká zbrojovka a.s., kde bude i nadále vykonávat citlivou činnost – odpovědná osoba společnosti Česká zbrojovka a.s. je novou odpovědnou osobou).

V případě, že dojde ke změně zaměstnání a v novém zaměstnání fyzická osoba citlivou činnost vykonávat nebude, je nutné Úřadu oznámit, že dosavadní odpovědná osoba již odpovědnou osobou není (např. fyzická osoba ukončí pracovní poměr u ČEZ a.s. a v novém zaměstnání nebude nadále vykonávat citlivou činnost – odpovědná osoba ČEZ a.s, již není odpovědnou osobou).

Na fyzické osoby, které podaly žádost o vydání dokladu podle zákona č. 412/2005 Sb. před 1. 1. 2012 a byl jim vydán doklad, se vztahují stejná pravidla pro oznamování změn jako na fyzické osoby, které podají žádost o vydání dokladu podle zákona č. 412/2005 Sb. po 1. 1. 2012.

Pro příklad uvádíme:

Před 1. 1. 2012 fyzická osoba v dotazníku vyplňovala údaje k občanskému průkazu, finančním závazkům. Po 1. 1. 2012 dojde ke změně občanského průkazu a vzniku finančního závazku - úvěru 650 000 Kč („čistý“ měsíční příjem fyzické osoby je 20 000 Kč). Podle právní úpravy platné do 31. 12. 2011 bylo povinností oznamovat tyto změny všechny. Změna povinností týkající se oznamování změn, která je upravena novou vyhláškou o personální bezpečnosti a o bezpečnostní způsobilosti, již neobsahuje oznamování změn občanského průkazu. Finanční závazek v uvedené výši při deklarovaném měsíčním příjmu oznámen být musí a současně musí být doložen písemností dokládající správnost údajů (např. smlouvou o úvěru) v prosté kopii.

Způsob a forma oznamování změn

Pro hlášení změn, v jejichž případě stanoví vyhláška o personální bezpečnosti a o bezpečnostní způsobilosti rozsah položek dotazníku, lze využít změnový dotazník, který je k dispozici na internetových stránkách Úřadu (www.nbu.cz), případně jej lze učinit volně formulovaným prohlášením v rozsahu položek dotazníku.

Oznamování jiných změn lze učinit volně formulovaným prohlášením nebo formou uvedení změněných údajů do elektronických šablon vzorů (žádost o vydání dokladu, prohlášení o svéprávnosti, prohlášení k osobnostní způsobilosti), které jsou k dispozici na internetových stránkách Úřadu (www.nbu.cz).

Je-li to požadavek vyhlášky o personální bezpečnosti a o bezpečnostní způsobilosti, musí být hlášená změna doložena příslušnými písemnostmi, a to ve stanovené formě (viz výše).

Z oznámení změn musí být patrné, kdo jej činí (je třeba uvést jméno a příjmení, datum narození, případně místo trvalého pobytu) a čeho se týká. Dále toto oznámení musí obsahovat označení orgánu, jemuž je určeno (Úřad) a podpis osoby, která změny oznamuje.

Oznámení změn lze podat v listinné nebo elektronické podobě.

V listinné podobě lze podat oznámení změn osobně nebo prostřednictvím jiné, k tomu účelu pověřené, osoby v podatelně místa sídla Úřadu (Na Popelce 2/16, Praha 5 - Košíře), v úředních hodinách.

Úřední hodiny podatelny	
Pondělí a středa:	8:00 – 17:00
Úterý a čtvrtek:	8:00 – 15:00
Pátek:	8:00 – 12:00

Oznámení změn lze také zaslat prostřednictvím držitele poštovní licence nebo zvláštní poštovní licence na adresu Úřadu (P.O.BOX 49, Praha 56, PSČ 150 06).

V elektronické podobě lze podat oznámení změn dodáním do **datové schránky Úřadu** (ID Úřadu – h93aayw, do pole „Věc“ se uvede „Bezpečnostní řízení – Hlášení změn“) nebo na **elektronickou podatelnu Úřadu** (posta@nbu.cz, do pole „Předmět“ se uvede „Bezpečnostní řízení – Hlášení změn“).

V těchto případech podání

- **formulář žádost o vydání dokladu** musí být výstupem z autorizované konverze nebo musí být podepsaný fyzickou osobou a odpovědnou osobou, a to zaručeným elektronickým podpisem,
- **doklad o dosažení vyššího stupně vzdělání** musí být výstupem z autorizované konverze,
- **prohlášení žadatele o svéprávnosti, prohlášení žadatele k osobnostní způsobilosti, změny oznámené volnou formou nebo formou změnového dotazníku a další písemnosti dosvědčující správnost oznamovaných** nemusí splňovat požadavky uvedené v předchozích bodech, u dodání na elektronickou podatelnu musí být jejich podání podepsané fyzickou osobou, a to zaručeným elektronickým podpisem.

Jakou sankci lze uložit za nesplnění povinnosti hlásit změny

- až 50 000 Kč (§ 148 a § 152 zákona č. 412/2005 Sb.)

Neoznámení změny může být Úřadem rovněž vyhodnoceno jako negativní okolnost ve smyslu § 84 odst. 3 zákona č. 412/2005 Sb., což má za následek nevyhovění žádosti o vydání dokladu, resp. zrušení platnosti existujícího dokladu.

5. Dokumenty odesílané a přijímané v rámci bezpečnostního řízení prostřednictvím informačního systému datových schránek v oblasti bezpečnostní způsobilosti

1) Náležitosti žádostí o vydání dokladu podle zákona č. 412/2005 Sb. – viz kapitola

   2. Informace k podání žádosti o vydání dokladu.

2) Oznamování změn – viz kapitola

   4. Informace k oznamování změn.

3) Prostřednictvím datové schránky zřízené pro fyzickou osobu lze činit všechny úkony týkající se řízení o vydání dokladu (vyjma osobních úkonů).

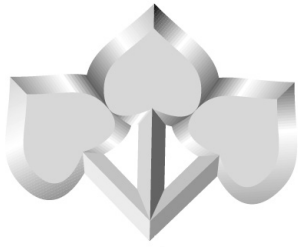
4) Komunikace s orgánem státu, právnickou osobou, podnikající fyzickou osobou, od kterých vyžaduje Úřad informace k účastníkovi řízení nebo držiteli dokladu.

Upozornění

*Při komunikaci podle bodu 3) a 4) je vhodné uvádět v datové zprávě v poli „**Věc**“ – „**Bezpečnostní řízení**“.*

*V případě, že fyzická osoba nebo subjekt uvedený v bodu 4) reaguje na **písemnost Úřadu (dožádání, sdělení, oznámení, rozhodnutí...)**, je vhodné uvádět také číslo jednací, kterým byla tato písemnost označena (např. 110002/2014-NBÚ/P, 111265/2014-NBÚ/E, ...), a to rovněž do pole „**Věc**“ (např. Bezpečnostní řízení č.j.110002/2014-NBÚ/P...).*

PRŮMYSLOVÁ BEZPEČNOST



1. Obecně k průmyslové bezpečnosti

Průmyslová bezpečnost je jedním z druhů zajištění ochrany utajovaných informací a je upravena v hlavě III zákona č. 412/2005 Sb. Dnem 1. 1. 2014 vstoupily v platnost nové právní předpisy soukromého práva, zejména pak nový občanský zákoník, se kterým souvisí i změny v právních předpisech upravujících oblast ochrany utajovaných informací. Změny jsou provedeny zákonem č. 303/2013 Sb., část 60, článek LXX a v oblasti průmyslové bezpečnosti vyhláškou č. 416/2013 Sb., kterou se mění vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti. Úpravy spojené s touto rekodifikací jsou již v následujícím textu zapracovány.

2. Informace k přístupu podnikatele k utajovaným informacím stupně utajení Vyhrazené

Pro přístup k utajované informaci POUZE stupně utajení Vyhrazené již není podmínkou provedení bezpečnostního řízení a následného vydání osvědčení podnikatele Úřadem, podnikatel bude mít přístup k této utajované informaci na základě svého písemného prohlášení, kterým doloží svou schopnost zabezpečit ochranu utajovaných informací (dále jen „prohlášení podnikatele“).

Jaké jsou formy přístupu podnikatele k utajované informaci stupně utajení Vyhrazené (§ 20 zákona č. 412/2005 Sb.)

Podle způsobu, jakým bude podnikatel k utajované informaci přistupovat, mohou nastat dvě varianty přístupu označované jako formy přístupu podnikatele k utajované informaci. Podnikatel má podle tohoto ustanovení přístup k utajované informaci:

a. která u něho vzniká, nebo je mu poskytnuta, nebo
b. která u něho nevzniká, ani mu není poskytována, ale ke které mají přístup zaměstnanci podnikatele nebo osoby jednající jménem podnikatele nebo za podnikatele, a to v souvislosti s výkonem pracovní nebo jiné činnosti pro podnikatele na základě smlouvy.

Forma přístupu podle bodu a. znamená, že podnikatel utajovanou informaci vytváří ve svých prostorách nebo že je mu poskytována k dalšímu nakládání ve vlastních prostorách, a to na jakémkoliv nosiči. V případě přístupu podnikatele podle bodu b. se jedná o seznamování se s utajovanou informací, tzn. že utajovaná informace není podnikateli předávána a podnikatel se s ní pouze seznámí např. u zadavatele zakázky.

Podmínky, které musí podnikatel nezbytně splňovat, aby byl oprávněn učinit prohlášení podnikatele s formou přístupu podle § 20 odst. 1 písm. a) zákona č. 412/2005 Sb., zahrnují též podmínky stanovené pro formu přístupu podle § 20 odst. 1 písm. b) zákona č. 412/2005 Sb. To znamená, že pokud podnikatel učiní prohlášení podnikatele s formou přístupu podle písm. a), má v tomto případě přístup k utajované informaci i ve formě podle písm. b).

Kdy může mít podnikatel přístup k utajované informaci stupně utajení Vyhrazené

- v případě nezbytné potřeby k výkonu své činnosti, doloží-li prohlášením podnikatele svou schopnost zabezpečit ochranu utajovaných informací nebo je-li držitelem osvědčení podnikatele (DŮVĚRNÉ, TAJNÉ, PŘISNĚ TAJNÉ), není-li stanoveno jinak (§ 58 až § 62 zákona č. 412/2005 Sb.).

Splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené na základě vydaného prohlášení podnikatele prokazuje podnikatel **poskytovateli této informace předáním prohlášení podnikatele před prvním přístupem k této informaci.** Poskytovatel utajované informace je oprávněn od podnikatele požadovat předložení bezpečnostní dokumentace podnikatele. Poskytovatel vyhrazené informace zašle kopii prohlášení podnikatele neprodleně Úřadu.

Pokud bude u podnikatele utajovaná informace stupně utajení Vyhrazené pouze vznikat, aniž by existoval poskytovatel utajované informace, podnikatel zašle originál prohlášení podnikatele neprodleně poté, co ho učiní, Úřadu.

Kdy je podnikatel oprávněn učinit prohlášení podnikatele

- pokud má vytvořeny podmínky pro ochranu utajované informace stupně utajení Vyhrazené, které

odpovídají formě přístupu k ní (§ 20 zákona č. 412/2005 Sb.) a příslušnému druhu zajištění její ochrany (§ 5 zákona č. 412/2005 Sb.),

- odpovědná osoba podnikatele je držitelem oznámení o splnění podmínek pro přístup k utajované informaci stupně utajení Vyhrazené, osvědčení nebo dokladu.

Platnost a zánik platnosti prohlášení podnikatele

Doba platnosti prohlášení podnikatele je 5 let ode dne, kdy bylo učiněno. Má-li mít podnikatel přístup k utajované informaci stupně utajení Vyhrazené i po uplynutí této platnosti, učiní nové prohlášení podnikatele a dále s ním nakládá stejně jako s původním prohlášením.

Platnost prohlášení podnikatele podle § 15a odst. 5 zákona č. 412/2005 Sb. zaniká:

1. uplynutím 5 let ode dne, kdy bylo učiněno,
2. dnem doručení písemného oznámení podnikatele, že ukončuje svůj přístup k utajované informaci, tomu, komu předal nebo zaslal prohlášení podnikatele (tj. poskytovateli vyhrazené informace nebo Úřadu),
3. dnem doručení osvědčení podnikatele,
4. zrušením nebo zánikem podnikatele,
5. přestal-li podnikatel splňovat některou z podmínek, které jej oprávnily učinit prohlášení podnikatele (viz výše: **Kdy je podnikatel oprávněn učinit prohlášení podnikatele**),
6. změnou některého z údajů uvedených v prohlášení podnikatele.

Podnikatel neprodleně písemně oznámí zánik platnosti prohlášení podnikatele podle bodu 3. až 6. tomu, komu předal nebo zaslal prohlášení podnikatele.

Povinnosti podnikatele, který učinil prohlášení podnikatele (§ 68a zákona č. 412/2005 Sb.)

- vést bezpečnostní dokumentaci podnikatele v rozsahu:
  - způsoby realizace jednotlivých druhů zajištění ochrany utajovaných informací,
  - seznam funkcí a osob, u nichž se předpokládá přístup k utajovaným informacím,
- na vyžádání poskytovatele vyhrazené informace mu poskytnout bezpečnostní dokumentaci,
- zabezpečit ochranu utajovaných informací při zániku přístupu k utajované informaci,
- zaslat prohlášení podnikatele Úřadu, pokud bude u něho utajovaná informace stupně utajení Vyhrazené pouze vznikat,
- oznámit písemně Úřadu nebo poskytovateli vyhrazené informace ukončení přístupu k ní nebo zánik platnosti prohlášení podnikatele,
- při zániku platnosti prohlášení podnikatele je podnikatel povinen odevzdat poskytnuté **utajované informace** poskytovateli nebo tomu, do jehož působnosti náleží, vlastní utajované informace odevzdá orgánu státu, do jehož působnosti utajované informace náleží; nelze-li tak učinit, je povinen odevzdat je Úřadu,
- učinit a neprodleně předat poskytovateli vyhrazené informace nebo Úřadu nové prohlášení podnikatele, pokud i po zániku platnosti původního prohlášení podnikatele z důvodu uplynutí 5 let ode dne, kdy bylo učiněno, nebo z důvodu změny některého z údajů uvedených v prohlášení podnikatele i nadále nezbytně potřebuje přístup k utajované informaci stupně utajení Vyhrazené.

3. Informace k podání žádosti o vydání osvědčení podnikatele (D, T, PT)

Podnikateli, který nezbytně k výkonu své činnosti potřebuje přístup k utajované informaci stupně utajení Důvěrné a vyšší, lze umožnit tento přístup, pokud je držitelem platného osvědčení podnikatele příslušného stupně utajení nebo vyššího, pokud zákon č. 412/2005 Sb. nestanoví jinak (§ 58 až 62).

Osvědčení podnikatele vydává Úřad podnikateli, který splňuje podmínky pro jeho vydání stanovené zákonem č. 412/2005 Sb. (§ 16), po provedeném bezpečnostním řízení.

Kdo je účastníkem bezpečnostního řízení

Účastníkem bezpečnostního řízení je podle § 92 písm. b) zákona č. 412/2005 Sb. podnikatel, který podal žádost o vydání osvědčení podnikatele. Okruh osob, které jsou považovány za podnikatele, vymezují ustanovení § 420 a 421 občanského zákoníku.

V bezpečnostním řízení se jedná a písemnosti se vyhotovují v českém jazyce, pokud nejde o výkon práv příslušníka národnostní menšiny.

V případě písemnosti vyhotovené v cizím jazyce musí účastník bezpečnostního řízení tuto předložit v originále a současně v úředně ověřeném překladu do jazyka českého.

Rozhodnutí podat žádost o vydání osvědčení podnikatele je plně v kompetenci statutárního orgánu. V praxi tento případ nastane obvykle na základě obchodního kontaktu, například jednání s cílem uzavřít kupní smlouvu nebo smlouvu o dílo s institucí nebo obchodním partnerem, který požaduje, aby podnikatel byl držitelem platného osvědčení podnikatele, protože při plnění podmínek smlouvy se bude seznamovat s utajovanými informacemi, utajované informace mu budou poskytovány nebo u něho budou utajované informace vznikat.

Jaké jsou formy přístupu podnikatele k utajované informaci (§ 20 zákona č. 412/2005 Sb.)

Podle způsobu, jakým bude podnikatel k utajované informaci přistupovat, mohou nastat dvě varianty přístupu označované jako formy přístupu podnikatele k utajované informaci. Podnikatel má podle tohoto ustanovení přístup k utajované informaci:

a. která u něho vzniká, nebo je mu poskytnuta, nebo
b. která u něho nevzniká, ani mu není poskytována, ale ke které mají přístup zaměstnanci podnikatele nebo osoby jednající jménem podnikatele nebo za podnikatele, a to v souvislosti s výkonem pracovní nebo jiné činnosti pro podnikatele na základě smlouvy.

Forma přístupu podle bodu a. znamená, že podnikatel utajovanou informaci vytváří ve svých prostorách nebo že je mu poskytována k dalšímu nakládání ve vlastních prostorách, a to na jakémkoliv nosiči. V případě přístupu podnikatele podle bodu b. se jedná o seznamování se s utajovanou informací, tzn. že utajovaná informace není podnikateli předávána a podnikatel se s ní pouze seznámí např. u zadavatele zakázky.

Podmínky, které musí podnikatel nezbytně splňovat pro vydání osvědčení podnikatele s formou přístupu podle § 20 odst. 1 písm. a) zákona č. 412/2005 Sb., zahrnují též podmínky stanovené pro formu přístupu podle § 20 odst. 1 písm. b) zákona č. 412/2005 Sb. To znamená, že pokud podnikatel požádá o vydání osvědčení podnikatele s formou přístupu podle písm. a), má v případě vydání požadovaného osvědčení podnikatele přístup k utajované informaci i ve formě podle písm. b). **Na základě uvedeného je v takovém případě u žádostí o vydání osvědčení podnikatele podaných po 1. 1. 2012 na vydaných osvědčeních vyznačována pouze forma přístupu podnikatele k utajované informaci podle § 20 odst. 1 písm. a) zákona č. 412/2005 Sb.**

Forma přístupu podle § 20 odst. 1 písm. b) zákona č. 412/2005 Sb. je na osvědčeních podnikatele vydaných na základě žádostí podaných po 1. 1. 2012 vyznačována, pokud podnikatel požádá pouze o formu přístupu podle písm. b).

Od 1. 1. 2012 se tedy nepodává žádost podnikatele o vydání jednoho osvědčení podnikatele pro obě formy přístupu podnikatele k utajované informaci.

Poznámka:

*U osvědčení vydaného na základě **žádosti podnikatele podané před 1. 1. 2012** a dále u **osvědčení podnikatele vydaného před tímto datem**, na němž jsou vyznačeny obě formy přístupu k utajované informaci (§ 20 odst. 1 písm. a) a b) zákona č. 412/2005 Sb.), **zůstávají v případě vydání osvědčení a v případě vydání nového osvědčení podle § 56 odst. 4 zákona č. 412/2005 Sb.**, jež ze specifických důvodů (odcizení, ztráta, poškození, nečitelnost, změna údajů) nahrazuje osvědčení původní, **vyznačeny obě formy přístupu k utajované informaci, tj. § 20 odst. 1 písm. a) a b) zákona č. 412/2005 Sb.***

Náležitosti základní žádosti o vydání osvědčení podnikatele podle zákona č. 412/2005 Sb.:

1. **formulář žádost podnikatele,** který obsahuje
   - identifikační údaje podnikatele,

- stupeň utajení a formu přístupu k utajované informaci, pro který žádá o vydání osvědčení,
- zdůvodnění nutnosti přístupu k utajované informaci podnikatelem (včetně uvedení veřejné zakázky, koncesní smlouvy, smlouvy nebo jiné skutečnosti, zadavatele nebo veřejného zadavatele, okolností odůvodňujících požadovanou formu přístupu)
  - předmět podnikání, v jehož rámci podnikatel požaduje přístup k utajované informaci,
  - veřejná zakázka, v rámci které je požadován přístup k utajované informaci, její zadavatel a předpokládaná doba trvání zadávacího řízení,
  - koncesní smlouva, v rámci které je požadován přístup k utajované informaci, její veřejný zadavatel a předpokládaná doba trvání koncesního řízení,
  - veřejná zakázka nebo koncesní smlouva před zahájením zadávacího nebo koncesního řízení, o kterou se podnikatel hodlá ucházet a v rámci které se předpokládá přístup k utajované informaci, její zadavatel nebo veřejný zadavatel a předpokládaný termín zahájení zadávacího nebo koncesního řízení,
  - smlouva, případně jiné právní skutečnosti, na základě které je požadován přístup k utajované informaci, předmět této smlouvy a poskytovatel utajované informace,
  - skutečnost, na základě které bude u podnikatele vznikat utajovaná informace,
  - okolnosti, které odůvodňují požadovanou formu přístupu podle § 20 zákona č. 412/2005 Sb.,
- prohlášení, že údaje uvedené v žádosti a jejích přílohách jsou pravdivé a úplné,
- datum vyplnění,
- podpis odpovědné osoby podnikatele,

2. **prohlášení podnikatele o zproštění povinnosti mlčenlivosti věcně a místně příslušného správce daně a jiné osoby zúčastněné na správě daní podle § 52 odst. 2 daňového řádu, a to v plném rozsahu údajů za účelem provedení bezpečnostního řízení,**
3. **vyplněný dotazník podnikatele v listinné i elektronické podobě** (soubor výhradně ve formátu .zfo nebo .xml),

Pro příklad uvádíme:

Při vyplňování údajů v písmenu h) dotazníku podnikatele (§ 97 písm. h) zákona č. 412/2005 Sb.) – **zahraniční obchodní partneři, s výjimkou obchodních partnerů z členských států Evropské unie, s celkovým finančním objemem uskutečněných obchodů nad 2.000.000 Kč v posledních pěti letech**, podnikatel v **žádosti podle § 96 odst. 1 zákona** zjišťuje, zda v posledních pěti letech uzavřel obchody se zahraničním partnerem, jejichž celkový **roční** objem alespoň v jednom z pěti sledovaných let přesáhl částku 2 mil. korun. Pokud ano, je údajem vyplňovaným v dotazníku podnikatele; do položky „objem obchodů“ uvede výši všech obchodů s tímto partnerem za celé období pěti let.

Příklady:

1) r. 2008 – 500 tis., r. 2009 – 2 mil., r. 2010 – 200 tis., r. 2011 – 300 tis., r. 2012 – 1 mil. = **nehlásí**, protože v žádném z posledních pěti let nepřesáhl celkový roční objem výši 2 mil. Kč;
2) r. 2008 – 600 tis., r. 2009 – **2,1** mil., r. 2010 – 300 tis., r. 2011 – 1,7 mil., r. 2012 – 500 tis. = **hlásí**, protože v roce 2009 přesáhl celkový roční objem výši 2 mil. Kč a v položce objem obchodů uvede částku **5,2** mil., tedy součet všech obchodů za 5 let

4. **písemnosti nutné k ověření podmínek podle § 16 zákona č. 412/2005 Sb.:**

- **podnikatel, který je právnickou osobou, přikládá**

(a) *doklady o rozhodnutích jeho orgánů o skutečnostech, které se zapisují do obchodního rejstříku a nejsou v něm dosud zapsány*, v originále, úředně ověřené kopii nebo prosté kopii, na které odpovědná osoba svým podpisem potvrdí úplnost uvedených údajů a shodu kopie s originálem,

(b) *smlouvu o tichém společenství u podnikatele* v originále, úředně ověřené kopii nebo prosté kopii, na které odpovědná osoba svým podpisem potvrdí úplnost uvedených údajů a shodu kopie s originálem,

(c) *doklad o vydání dluhopisů s uvedením důvodu vydání a celkové výše vydaných dluhopisů* v originále, úředně ověřené kopii nebo prosté kopii, na které odpovědná osoba svým podpisem potvrdí úplnost uvedených údajů a shodu kopie s originálem,

(d) *smlouvy o nájmu prostor, budov a pozemků uvedených v § 97 písm. d) zákona č. 412/2005 Sb.*

v originále, úředně ověřené kopii nebo prosté kopii, na které odpovědná osoba svým podpisem potvrdí úplnost uvedených údajů a shodu kopie s originálem,

(e) *řádné účetní závěrky za posledních 5 let* v originále, úředně ověřené kopii nebo prosté kopii, na které odpovědná osoba svým podpisem potvrdí úplnost uvedených údajů a shodu kopie s originálem,

(f) *ovládací smlouvu nebo písemnou zprávu o vztazích*[1]*), pokud je podnikatel ovládanou osobou, za posledních 5 let* v originále, úředně ověřené kopii nebo prosté kopii, na které odpovědná osoba svým podpisem potvrdí úplnost uvedených údajů a shodu kopie s originálem,

(g) *písemné zprávy auditora o ověření řádných účetních závěrek za posledních 5 let v rozsahu výroku auditora, pokud tak stanoví jiný právní předpis*[2]*)*, v originále, úředně ověřené kopii nebo prosté kopii, na které odpovědná osoba svým podpisem potvrdí úplnost uvedených údajů a shodu kopie s originálem,

(h) *přehled závazků z podnikatelské činnosti, které jsou po lhůtě splatnosti více než 180 dnů, s uvedením jednotlivých věřitelů a důvodu nezaplacení* datovaný a podepsaný odpovědnou osobou ne starší než 60 dnů od data vystavení v originále nebo úředně ověřené kopii,

(i) *výpis z účtu vlastníka v centrální evidenci investičních nástrojů* ne starší 60 dnů od data vystavení v originále nebo úředně ověřené kopii,

(j) *přehled všech účastí na akciových společnostech a majetkového podílu v procentech* datovaný podepsaný odpovědnou osobou ne starší než 60 dnů od data vystavení v originále nebo úředně ověřené kopii,

(k) *přehled ostatních investičních cenných papírů*[3]*) za předpokladu, že nejsou v centrální evidenci, podílů a vkladů do základního kapitálu veřejné obchodní společnosti, komanditní společnosti a společností s ručením omezeným a členských vkladů v družstvech* datovaný a podepsaný odpovědnou osobou ne starší než 60 dnů od data vystavení v originále nebo úředně ověřené kopii,

■ **podnikající fyzická osoba k žádosti podnikatele přikládá**

(a) *smlouvy o nájmu prostor, budov a pozemků uvedených v § 97 písm. d) zákona č. 412/2005 Sb.* v originále, úředně ověřené kopii nebo prosté kopii, na které odpovědná osoba svým podpisem potvrdí úplnost uvedených údajů a shodu kopie s originálem,

(b) *řádné účetní závěrky, vede-li účetnictví, nebo daňová přiznání, pokud vede daňovou evidenci podle zákona o daních z příjmů, a to za posledních 5 let*, v originále, úředně ověřené kopii nebo prosté kopii, na které odpovědná osoba svým podpisem potvrdí úplnost uvedených údajů a shodu kopie s originálem,

(c) *písemné zprávy auditora o ověření řádných účetních závěrek za posledních 5 let v rozsahu výroku auditora, pokud tak stanoví jiný právní předpis*[2]*)*, v originále, úředně ověřené kopii nebo prosté kopii, na které odpovědná osoba svým podpisem potvrdí úplnost uvedených údajů a shodu kopie s originálem,

(d) *přehled závazků z podnikatelské činnosti, které jsou po lhůtě splatnosti více než 180 dnů, s uvedením jednotlivých věřitelů a důvodu nezaplacení* datovaný a podepsaný odpovědnou osobou ne starší než 60 dnů od data vystavení v originále nebo úředně ověřené kopii,

(e) *výpis z účtu vlastníka v centrální evidenci investičních nástrojů* ne starší 60 dnů od data vystavení v originále nebo úředně ověřené kopii,

(f) *přehled všech účastí na akciových společnostech a majetkového podílu v procentech* datovaný podepsaný odpovědnou osobou ne starší než 60 dnů od data vystavení v originále nebo úředně ověřené kopii,

(g) *přehled ostatních investičních cenných papírů*[3]*) za předpokladu, že nejsou v centrální evidenci, podílů a vkladů do základního kapitálu veřejné obchodní společnosti, komanditní společnosti a společností s ručením omezeným a členských vkladů v družstvech* datovaný a podepsaný odpovědnou osobou ne starší než 60 dnů od data vystavení v originále nebo úředně ověřené kopii,

[1]) § 66a obchodního zákoníku, § 82 a násl. zákona o obchodních korporacích.
[2]) Zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů.
[3]) Zákon č. 89/2012 Sb., občanský zákoník.

5. **bezpečnostní dokumentaci podnikatele**, která obsahuje systém ochrany utajovaných informací u podnikatele, jeden výtisk je uložen u podnikatele, který je povinen ji průběžně aktualizovat, tvoří ji:

- výčet utajovaných informací uložených u podnikatele s uvedením jejich původce a stupně utajení a v případě, že utajovaná informace mu byla poskytnuta nebo u něj vznikla na základě zakázky, též s uvedením specifikace této zakázky, a dále specifikaci utajovaných informací, k nimž by měl mít podnikatel přístup, s uvedením jejich původce a stupně utajení a v případě, že utajovaná informace by mu měla být poskytnuta nebo by u něj měla vzniknout na základě zakázky, též s uvedením předpokládané specifikace této zakázky,
- analýza možného ohrožení utajovaných informací, vhodná a účinná ochranná opatření ke snížení rizik,
- popis způsobů realizace jednotlivých druhů zajištění ochrany utajovaných informací,
- seznam funkcí a osob, u kterých se předpokládá přístup k utajovaným informacím, s uvedením jejich rodného čísla a stupně utajení, na který tyto osoby o vydání osvědčení žádají, a u již vydaného osvědčení jeho číslo a datum vydání a stupeň utajení, na který bylo vydáno, u oznámení datum jeho vydání a u dokladu jeho číslo a datum vydání.

Upozornění:

Podnikatel nemůže v rámci jedné žádosti požádat o tzv. kombinaci stupňů, tedy žádat o rozdílný stupeň utajení pro tzv. „seznamování se“ s utajovanou informací (viz § 20 odst. 1 písm. b) zákona č. 412/2005 Sb.) a jiný stupeň utajení pro tzv. „poskytování, vznik a uchovávání“ utajované informace (viz § 20 odst. 1 písm. a) zákona č. 412/2005 Sb.)!

Jednou z podmínek pro vydání osvědčení podnikatele je uhrazení správního poplatku podle zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů, při podání žádosti o vydání osvědčení podnikatele.

Bez uhrazení poplatku nebude žádost o vydání osvědčení podnikatele Úřadem přijata k provedení bezpečnostního řízení!

Poplatková povinnost pro přijetí žádosti o vydání osvědčení podnikatele je podle zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů, v závislosti na formě přístupu stanovena následujícím způsobem:

- **5.000 Kč**, žádá-li podnikatel o vydání osvědčení podnikatele **ve formě přístupu podle § 20 odst. 1 písm. b) zákona č. 412/2005 Sb.**, tj. pro případ, že u něho utajovaná informace nevzniká, ani mu není poskytována, ale ke které mají přístup zaměstnanci podnikatele nebo osoby jednající jménem podnikatele nebo za podnikatele, a to v souvislosti s výkonem pracovní nebo jiné činnosti pro podnikatele na základě smlouvy,
- **10.000 Kč**, žádá-li podnikatel o vydání osvědčení podnikatele **ve formě přístupu podle § 20 odst. 1 písm. a) zákona č. 412/2005 Sb.**, tj. pro případ, že u něho utajovaná informace vzniká, nebo je mu poskytnuta.

Vzhledem k tomu, že forma přístupu podnikatele podle § 20 odst. 1 písm. a) zákona č. 412/2005 Sb. zahrnuje rovněž formu přístupu podle § 20 odst. 1 písm. b) zákona č. 412/2005 Sb., **se správní poplatky za jednotlivé formy přístupu, pokud podnikatel požádá o vydání osvědčení podnikatele pro přístup podle § 20 odst. 1 písm. a) zákona č. 412/2005 Sb., nesčítají**. Podnikatel tedy za přijetí žádosti uhradí buď 5.000 Kč pro formu přístupu podle § 20 odst. 1 písm. b) zákona č. 412/2005 Sb. nebo 10.000 Kč pro formu přístupu podle § 20 odst. 1 písm. a) zákona č. 412/2005 Sb.

Poplatkové povinnosti nepodléhá žádost o vydání osvědčení podnikatele podle § 96 odst. 4 a 5 zákona č. 412/2005 Sb., pokud podnikatel, který má mít přístup k utajované informaci i po uplynutí doby platnosti stávajícího osvědčení podnikatele, požádá o vydání nového osvědčení podnikatele **před uplynutím doby platnosti dosavadního osvědčení podnikatele ve lhůtě nejméně**

a) 7 měsíců u osvědčení podnikatele pro stupeň utajení Důvěrné,

b) 9 měsíců u osvědčení podnikatele pro stupeň utajení Tajné a

c) 11 měsíců u osvědčení podnikatele pro stupeň utajení Přísně tajné.

Jestliže **je podnikatel držitelem osvědčení** podnikatele pro přístup k utajované informaci **podle § 20 odst. 1 písm. b) zákona č. 412/2005 Sb.** a **podá žádost o vydání osvědčení** podnikatele **pro formu**

přístupu podle § 20 odst. 1 písm. a) zákona č. 412/2005 Sb., a to i v případě, že se jedná o žádost podanou ve lhůtě stanovené podle § 96 odst. 4 zákona č. 412/2005 Sb., správní poplatek 10.000 Kč hradí, neboť vzhledem k rozšíření formy přístupu jde **vždy o novou žádost podle § 96 odst. 1 zákona č. 412/2005 Sb.**

Podá-li podnikatel, jenž je **držitelem osvědčení pro formu přístupu podle § 20 odst. 1 písm. a) zákona č. 412/2005 Sb., žádost o vydání osvědčení podnikatele pro formu podle § 20 odst. 1 písm. b) zákona č. 412/2005 Sb.** (tj. „zužuje-li" podnikatel formu přístupu), **poplatková povinnost mu v případě, jedná-li se o žádost podanou ve lhůtě stanovené podle § 96 odst. 4 zákona č. 412/2005 Sb., nevzniká.**

Způsoby a formy úhrady správního poplatku:

- v hotovosti na podatelně Úřadu před osobním podáním žádosti o vydání osvědčení podnikatele,
- vylepením kolků v hodnotě požadovaného poplatku na formulář žádost podnikatele (pouze do 5.000 Kč),
- bezhotovostním převodem na účet Úřadu: 19-105881/0710 vedený u České národní banky, jako variabilní symbol musí být uvedeno IČ podnikatele, ve zprávě pro příjemce podnikatel uvede, že se jedná o správní poplatek a ID své datové schránky: „správní poplatek, ISD: xxxxxx", přičemž úhradou se rozumí připsání platby na účet Úřadu. (Vzhledem k tomu, že může nastat prodleva několika dnů mezi podáním příkazu k úhradě a jejím připsáním na účet Úřadu, je třeba vyčkat s podáním žádosti o vydání osvědčení podnikatele až po obdržení datové zprávy od Úřadu, která obsahuje potvrzení o uhrazení poplatku a je zasílána neprodleně po připsání úhrady na účet Úřadu.)

Zahraniční osoba, která je podnikatelem podle zvláštního právního předpisu, doloží písemnosti uvedené v bodě 4 formou obdobných dokladů z příslušných evidencí podle země původu.

Část bezpečnostní dokumentace podnikatele – *„seznam funkcí a osob…"* – je přiřazena k příslušné sekci dotazníku podnikatele, tento seznam není nutno přikládat k bezpečnostní dokumentaci podnikatele, ale při zpracování bezpečnostní dokumentace podnikatele se uvede pouze odkaz na tento seznam.

Část bezpečnostní dokumentace podnikatele – *„popis způsobů realizace jednotlivých druhů zajištění ochrany utajovaných informací"* – je nutné strukturovat podle těchto druhů specifikovaných v § 5 zákona č. 412/2005 Sb.:

- personální bezpečnost (Hlava II. zákona č. 412/2005 Sb.),
- administrativní bezpečnost (Hlava IV. zákona č. 412/2005 Sb.),
- fyzická bezpečnost (Hlava V. zákona č. 412/2005 Sb.),
- bezpečnost informačních systémů nebo komunikačních systémů (Hlava VI. zákona č. 412/2005 Sb.),
- kryptografická ochrana (Hlava VIII. zákona č. 412/2005 Sb.).

Při zpracování bezpečnostní dokumentace podnikatele v oblasti použití prostředků zajištění ochrany utajovaných informací je nutné vždy vycházet z prováděcích právních předpisů k zákonu č. 412/2005 Sb. (vyhlášek). Pokud podnikatel zamýšlí nakládat s utajovanými informacemi v informačním a komunikačním systému nebo využívat kryptografické prostředky ochrany, musí v podobě samostatné žádosti požádat Odbor informačních technologií Úřadu o certifikaci informačního a komunikačního systému nebo certifikaci kryptografického prostředku (postup doporučujeme předem konzultovat s uvedeným odborem).

Pokud podnikatel v žádosti o vydání osvědčení podnikatele žádá o formu přístupu k utajované informaci, která spočívá pouze v tzv. „seznamování se" s utajovanými informacemi, obsahuje bezpečnostní dokumentace podnikatele v části – *„popis způsobů realizace jednotlivých druhů zajištění ochrany utajovaných informací"* – jen popis realizace opatření personální bezpečnosti.

Co musí podnikatel v rámci bezpečnostního řízení zajistit ve vztahu k osobám (zaměstnancům) u podnikatele, u kterých se předpokládá přístup k utajovaným informacím

Odpovědná osoba podnikatele, který podal žádost o vydání osvědčení podnikatele, musí zajistit, aby fyzické osoby u podnikatele, u nichž se předpokládá přístup k utajovaným informacím na základě platného osvědčení podnikatele příslušného stupně utajení, podaly u Úřadu žádost o vydání tohoto osvědčení. Podrobné informace k tomuto postupu jsou uvedeny v sekci PERSONÁLNÍ BEZPEČNOST.

Náležitosti žádosti o vydání osvědčení podnikatele podle § 96 odst. 4 a 5 zákona

Pokud podnikatel, který má mít přístup k utajovaným informacím po uplynutí platnosti stávajícího osvědčení podnikatele, požádá o vydání nového osvědčení podnikatele před uplynutím doby platnosti dosavadního osvědčení podnikatele **ve lhůtě nejméně**:

- **7 měsíců** u nové žádosti o vydání osvědčení podnikatele pro stupeň utajení Důvěrné,
- **9 měsíců** u nové žádosti o vydání osvědčení podnikatele pro stupeň utajení Tajné,
- **11 měsíců** u nové žádosti o vydání osvědčení podnikatele pro stupeň utajení Přísně tajné,

předkládá podnikatel tyto materiály:

1. **formulář žádost podnikatele**, který obsahuje
   - identifikační údaje podnikatele,
   - stupeň utajení a formu přístupu k utajované informaci, pro který žádá o vydání osvědčení,
   - zdůvodnění nutnosti přístupu k utajované informaci podnikatelem (včetně uvedení veřejné zakázky, koncesní smlouvy, smlouvy nebo jiné skutečnosti, zadavatele nebo veřejného zadavatele, okolností odůvodňujících požadovanou formu přístupu),
     - předmět podnikání, v jehož rámci podnikatel požaduje přístup k utajované informaci,
     - veřejná zakázka, v rámci které je požadován přístup k utajované informaci, její zadavatel a předpokládaná doba trvání zadávacího řízení,
     - koncesní smlouva, v rámci které je požadován přístup k utajované informaci, její veřejný zadavatel a předpokládaná doba trvání koncesního řízení,
     - veřejná zakázka nebo koncesní smlouva před zahájením zadávacího nebo koncesního řízení, o kterou se podnikatel hodlá ucházet a v rámci které se předpokládá přístup k utajované informaci, její zadavatel nebo veřejný zadavatel a předpokládaný termín zahájení zadávacího nebo koncesního řízení,
     - smlouva, případně jiné právní skutečnosti, na základě které je požadován přístup k utajované informaci, předmět této smlouvy a poskytovatel utajované informace,
     - skutečnost, na základě které bude u podnikatele vznikat utajovaná informace,
     - okolnosti, které odůvodňují požadovanou formu přístupu podle § 20 zákona č. 412/2005 Sb.,
   - prohlášení, že údaje uvedené v žádosti a jejích přílohách jsou pravdivé a úplné,
   - datum vyplnění,
   - podpis odpovědné osoby podnikatele,
2. **prohlášení podnikatele o zproštění povinnosti mlčenlivosti věcně a místně příslušného správce daně a jiné osoby zúčastněné na správě daní podle § 52 odst. 2 daňového řádu, a to v plném rozsahu údajů za účelem provedení bezpečnostního řízení,**
3. **vyplněný dotazník podnikatele v listinné i elektronické podobě** (soubor výhradně ve formátu .zfo nebo .xml) s tím, že v dotazníku podnikatele se vyplňují pouze **základní identifikační údaje, v rozsahu název nebo obchodní firma a identifikační číslo osoby a údaje**, které se změnily v průběhu platnosti osvědčení podnikatele a nebyly oznámeny podle § 6 odst. 2 a 3 vyhlášky o průmyslové bezpečnosti,
4. **písemnosti nutné k ověření podmínek podle § 16 zákona č. 412/2005 Sb.,** stanoví-li tak vyhláška o průmyslové bezpečnosti – viz výše – bod 4 kapitoly **Náležitosti základní žádosti o vydání osvědčení podnikatele podle zákona č. 412/2005 Sb.,**
5. **bezpečnostní dokumentaci podnikatele** v rozsahu změn, které nebyly Úřadu oznámeny podle § 6 vyhlášky o průmyslové bezpečnosti.

Pro příklad uvádíme:

Podnikatel při podání základní žádosti o vydání osvědčení podnikatele podle zákona č. 412/2005 Sb. uvedl v dotazníku podnikatele mimo jiné údaje o jednateli podnikatele – **položka a)** – a údaje o platných účtech – **položka c)**.

Neuvedl žádné zahraniční obchodní partnery – **položka h)**, protože neuzavřel žádné smlouvy, jejichž celkový finanční objem uskutečněného obchodu by činil více než 2.000.000 Kč, a neuvedl žádné údaje **v položce g)** – smlouvy, jejichž předmět plnění obsahuje utajované informace.

Po vydání osvědčení podnikatele u něho **došlo ke změnám spočívajícím ve jmenování druhého jednatele, v přistoupení tichého společníka, založení nových účtů, uzavření smlouvy s obchodním partnerem z USA s celkovým objemem uskutečněného obchodu 2.500.000 Kč a s obchodním partnerem z Egypta, přičemž celkový objem tohoto obchodu činil 1.500.000 Kč. Podnikatel také zřídil dvě nové zabezpečené oblasti a na základě smluvního vztahu došlo k přijetí utajovaných informací, které jsou uloženy u podnikatele**.

Podnikatel má v tomto případě podle § 6 odst. 2 a 3 vyhlášky o průmyslové bezpečnosti povinnost oznámit pouze změny:

- **v položce a) a b)** formou vyplnění těchto údajů v dotazníku podnikatele a doložením rozhodnutí orgánu podnikatele o jmenování druhého jednatele (např. rozhodnutí valné hromady) a smlouvou o tichém společenství u podnikatele, **a to neprodleně**,
- **v bezpečnostní dokumentaci** v části „popis způsobů realizace jednotlivých druhů zajištění ochrany utajovaných informací" formou aktualizovaného popisu druhu fyzická bezpečnost, **a to neprodleně**,
- **v položce h)** formou vyplnění těchto údajů v dotazníku podnikatele (pouze obchodního partnera z USA, protože celkový objem obchodu s ním přesahuje výši 2.000.000 Kč), **a to v rámci ročního oznamování změn, které je povinen učinit ke dni, který se shoduje se dnem vydání osvědčení podnikatele,**
- **v položce g)** formou vyplnění těchto údajů v dotazníku podnikatele a formou aktualizované části **bezpečnostní dokumentace** „výčet utajovaných informací uložených u podnikatele…", **a to v rámci ročního oznamování změn, které je povinen učinit ke dni, který se shoduje se dnem vydání osvědčení podnikatele**.

Při podání následné žádosti o vydání osvědčení podnikatele podle § 96 odst. 4 a 5 zákona č. 412/2005 Sb. je pak povinen **v dotazníku podnikatele uvést údaje způsobem popsaným pro tuto žádost pod bodem 3. včetně údajů o nových účtech vyplněním položky c) dotazníku podnikatele**.

Protože od posledního ročního oznamování změn (§ 6 odst. 3 vyhlášky o průmyslové bezpečnosti) došlo i k obměně utajovaných informací uložených u podnikatele, je povinen také vyplnit údaje **v položce g) dotazníku podnikatele a předložit aktualizovanou část bezpečnostní dokumentace – „výčet utajovaných informací uložených u podnikatele…"**.

Upozornění:

Pokud podnikatel nedodrží výše uvedené minimální lhůty pro podání žádosti o vydání osvědčení podnikatele podle § 96 odst. 4 a 5 zákona č. 412/2005 Sb., bude jeho povinností podat novou kompletní základní žádost podle zákona č. 412/2005 Sb. – viz výše – kapitola ***Náležitosti základní žádosti o vydání osvědčení podnikatele podle zákona č. 412/2005 Sb. – včetně uhrazení správního poplatku podle zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů, při podání žádosti o vydání osvědčení podnikatele.***

Bez uhrazení správního poplatku nebude žádost o vydání osvědčení podnikatele Úřadem přijata k provedení bezpečnostního řízení!

Za žádost podle § 96 odst. 4 a 5 zákona č. 412/2005 Sb. není považovaná každá následně podaná žádost bez ohledu na skutečnost, jakým způsobem bylo (nebylo) bezpečnostní řízení týkající se předchozí žádosti ukončeno.

Pro příklad uvádíme:

Podal-li podnikatel žádost o vydání osvědčení podnikatele a řízení:

a) bylo zastaveno,

b) bylo ukončeno rozhodnutím o nevydání osvědčení podnikatele nebo

c) stále probíhá,

následně podnikatelem podaná žádost o vydání dalšího osvědčení podnikatele musí být novou kompletní základní žádostí podle zákona č. 412/2005 Sb. – viz výše – kapitola ***Náležitosti základní žádosti o vydání osvědčení podnikatele podle zákona č. 412/2005 Sb. – včetně uhrazení správního poplatku podle zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů, při podání žádosti o vydání osvědčení podnikatele.***

Bez uhrazení správního poplatku nebude žádost o vydání osvědčení podnikatele Úřadem přijata k provedení bezpečnostního řízení!

Způsob a forma podání žádosti o vydání osvědčení podnikatele

Podání je možno učinit osobním podáním na podatelnu Úřadu, zasláním ve formě poštovní zásilky, prostřednictvím informačního systému datových schránek nebo elektronické podatelny Úřadu.

Nejběžnějším způsobem podání žádosti je osobní podání (možnost objednat se na tel. č. 257 283 153, 258) v podatelně místa sídla Úřadu (Na Popelce 2/16, Praha 5 – Košíře), v úředních hodinách.

Úřední hodiny podatelny	
Pondělí a středa:	8:00 – 17:00
Úterý a čtvrtek:	8:00 – 15:00
Pátek:	8:00 – 12:00

Osobní podání je pro podnikatele výhodné, protože pracovníci Úřadu mu mohou pomoci odstranit formální nedostatky žádosti na místě. Podnikateli je také vydáno potvrzení o převzetí žádosti.

Žádost lze také zaslat prostřednictvím držitele poštovní licence nebo zvláštní poštovní licence na adresu Úřadu (P. O. BOX 49, Praha 56, PSČ 150 06) nebo ji nechat doručit na podatelnu Úřadu prostřednictvím jiné, k tomu účelu pověřené, osoby.

Vyplněný dotazník podnikatele je v tomto případě podáván zároveň v elektronické podobě na technickém nosiči dat.

V elektronické podobě lze podat žádost dodáním do **datové schránky Úřadu** (ID Úřadu – h93aayw, do pole „Věc“ se uvede „Žádost o vydání osvědčení podnikatele“) nebo na **elektronickou podatelnu Úřadu** (posta@nbu.cz, do pole „Předmět“ se uvede „Žádost o vydání osvědčení podnikatele“).

V těchto případech podání:

- **formulář žádost podnikatele** musí být výstupem z autorizované konverze nebo musí být podepsaný odpovědnou osobou, a to uznávaným elektronickým podpisem,
- **prohlášení o zproštění povinnosti mlčenlivosti** věcně a místně příslušného správce daně a jiné osoby zúčastněné na správě daní musí být výstupem z autorizované konverze nebo musí být podepsané statutárním orgánem právnické osoby nebo podnikající fyzickou osobou, a to uznávaným elektronickým podpisem,
- **výpis z účtu vlastníka v centrální evidenci investičních nástrojů** musí být výstupem z autorizované konverze nebo musí být podepsaný osobou, která písemnost vydala, a to uznávaným elektronickým podpisem,
- **ostatní písemnosti nutné k ověření podmínek podle § 16 zákona č. 412/2005 Sb.** při podání na **elektronickou podatelnu** musí být výstupem z autorizované konverze nebo musí být podepsané odpovědnou osobou, a to uznávaným elektronickým podpisem; při dodání do **datové schránky** nemusí výše uvedené požadavky splňovat,
- **dotazník podnikatele a bezpečnostní dokumentace podnikatele** nemusí splňovat požadavky uvedené v předchozích bodech, u dodání na elektronickou podatelnu musí být podání podepsané odpovědnou osobou, a to uznávaným elektronickým podpisem,
- **dotazník podnikatele** musí být předložen také v listinné podobě.

4. Informace k podání žádosti o vydání certifikátu NATO

Certifikát (osvědčení podnikatele pro cizí moc) potvrzuje cizí moci, že u jeho držitele bylo provedeno bezpečnostní řízení v souladu s příslušnými právními předpisy ČR a že je držitelem platného osvědčení podnikatele daného stupně utajení.

Kdy vydává Úřad certifikát NATO

- má-li mít podnikatel přístup k utajované informaci NATO, splňuje-li podmínky podle § 15 písm. b) zákona č. 412/2005 Sb., a požaduje-li tak NATO,

- je-li to v souladu s bezpečnostními a ekonomickými zájmy České republiky a se závazky vyplývajícími pro Českou republiku z mezinárodní smlouvy,
- neprobíhá-li s daným podnikatelem řízení podle § 101 odst. 1 zákona č. 412/2005 Sb.

Certifikát je možné vydat pouze na základě písemné odůvodněné žádosti podnikatele.

Lhůta pro vyřízení žádosti o vydání certifikátu Úřadem není zákonem stanovena.

Druhy certifikátů, které jsou Úřadem vydávány

NATO CONFIDENTIAL
NATO SECRET
COSMIC TOP SECRET

Na stupeň utajení Vyhrazené se certifikáty nevystavují.

Pro potřeby orgánů Evropské unie se certifikát nevydává, plně jej nahrazuje „národní“ osvědčení vydané podle zákona č. 412/2005 Sb.

5. Informace k platnosti, zániku platnosti a výměně osvědčení podnikatele a certifikátu

Osvědčení podnikatele je veřejnou listinou.

Platnost osvědčení podnikatele je
- pro stupeň Důvěrné 9 let,
- pro stupeň Tajné 7 let,
- pro stupeň Přísně tajné 5 let,

od data vydání.

Platnost osvědčení podnikatele zaniká

1. uplynutím doby platnosti osvědčení, zrušením nebo zánikem podnikatele,
2. zrušením jeho platnosti (dnem vykonatelnosti rozhodnutí Úřadu o zrušení jeho platnosti),
3. ohlášením jeho odcizení nebo jeho ztráty,
4. poškozením (majícím za následek nečitelnost údajů, porušení celistvosti), změnou některého z údajů v něm uvedených,
5. vrácením jeho držitelem tomu, kdo jej vydal,
6. dnem doručení nového osvědčení podnikatele pro stejnou formu přístupu podnikatele k utajované informaci (pro jakýkoliv stupeň),
7. dnem doručení rozhodnutí o nevydání osvědčení podnikatele pro stejnou formu přístupu podnikatele k utajované informaci (pro jakýkoliv stupeň).

Práva a povinnosti podnikatele v případě zániku platnosti osvědčení podnikatele

a) **V případech zániku platnosti osvědčení podnikatele** podle **bodu 2, 4, 6 nebo 7** má podnikatel **povinnost vrátit osvědčení podnikatele do 15 dnů** tomu, kdo jej vydal (§ 68 písm. a) zákona č. 412/2005 Sb.).

b) **V případě odcizení nebo ztráty osvědčení podnikatele (bod 3)** má podnikatel **povinnost neprodleně ohlásit tuto skutečnost** Úřadu (§ 68 písm. b) zákona č. 412/2005 Sb.).

Upozornění:

Porušením uvedených povinností se podnikatel dopouští správního deliktu, za který lze ***uložit pokutu do 50.000 Kč*** *(§ 155 zákona č. 412/2005 Sb.).*

c) **V případech zániku platnosti** osvědčení podnikatele podle **bodu 3 nebo 4** vydá Úřad na **základě**

písemné žádosti podnikatele podané **do 15 dnů** ode dne zániku platnosti osvědčení podnikatele **do 5 dnů** od jejího doručení nové osvědčení podnikatele (§ 56 odst. 4 zákona č. 412/2005 Sb.).

Upozornění:

Pokud nebude ve stanovené lhůtě žádost podána, zanikne přístup podnikatele k utajovaným informacím a podnikatel bude muset v případě nutnosti budoucího přístupu k utajované informaci stupně utajení Důvěrné, Tajné nebo Přísně tajné požádat o vydání nového osvědčení podnikatele příslušného stupně a příslušné formy přístupu, tzn. bude jeho povinností podat novou kompletní základní žádost o vydání osvědčení podnikatele podle zákona č. 412/2005 Sb. – viz výše – kapitola ***Náležitosti základní žádosti o vydání osvědčení podnikatele podle zákona č. 412/2005 Sb. – včetně uhrazení správního poplatku podle zákona č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů, při podání žádosti o vydání osvědčení podnikatele.***

Bez uhrazení správního poplatku nebude žádost o vydání osvědčení podnikatelem Úřadem přijata pro provedení bezpečnostního řízení!

Platnost osvědčení podnikatele nezaniká jiným než výše uvedeným způsobem – chce-li podnikatel zrušit platnost jemu vydaného osvědčení podnikatele, protože již nepředpokládá další přístup k utajovaným informacím, užije postup uvedený v bodě 5.

Certifikát NATO je veřejnou listinou.

Doba platnosti certifikátu (§ 57 odst. 6 zákona č. 412/2005 Sb.)

- může být nejdéle taková, jaká je platnost osvědčení podnikatele, certifikát je však v zásadě vydáván na dobu nezbytně nutnou.

Platnost certifikátu **zaniká**

1. uplynutím doby jeho platnosti,
2. ohlášením jeho odcizení nebo jeho ztráty,
3. poškozením (majícím za následek nečitelnost údajů, porušení celistvosti),
4. vrácením jeho držitelem Úřadu,
5. dnem doručení rozhodnutí o nevydání osvědčení podnikatele pro stejnou formu přístupu podnikatele k utajované informaci (pro jakýkoliv stupeň),

Platnost certifikátu dále **zaniká** zánikem platnosti osvědčení podnikatele

6. změnou některého z údajů v něm uvedených,
7. zrušením nebo zánikem podnikatele,
8. zrušením jeho platnosti (dnem vykonatelnosti rozhodnutí Úřadu o zrušení jeho platnosti),
9. dnem doručení nového osvědčení podnikatele pro stejnou formu přístupu podnikatele k utajované informaci (pro jakýkoliv stupeň),
10. vrácením jeho držitelem Úřadu.

Práva a povinnosti podnikatele v případě zániku platnosti certifikátu

a) **V případech zániku platnosti** certifikátu podle bodu **3, 5 až 10** má podnikatel povinnost vrátit certifikát Úřadu do 15 dnů (§ 57 odst. 8 zákona č. 412/2005 Sb.).

b) **V případě odcizení nebo ztráty certifikátu (bod 2)** má podnikatel **povinnost neprodleně ohlásit tuto skutečnost Úřadu** (§ 68 písm. b) zákona č. 412/2005 Sb.).

Upozornění:

Porušením uvedených povinností se podnikatel dopouští správního deliktu, za který lze ***uložit pokutu do 50.000 Kč*** *(§ 155 zákona č. 412/2005 Sb.).*

Přístup podnikatele k utajované informaci cizí moci také zaniká, zanikla-li platnost osvědčení podnikatele ohlášením jeho odcizení nebo jeho ztráty nebo poškozením (majícím za následek nečitelnost údajů, porušení celistvosti), neboť podnikatel přestal splňovat podmínky podle § 15 písm. b) zákona č. 412/2005 Sb. Pokud podnikatel v tomto případě do 15 dnů ode dne zániku platnosti osvědčení

podnikatele nepožádá písemně Úřad o vydání nového osvědčení podnikatele, zaniká také platnost certifikátu.

Platnost certifikátu nezaniká jiným než výše uvedeným způsobem – chce-li podnikatel zrušit platnost jemu vydaného certifikátu, protože již nepředpokládá další přístup k utajovaným informacím cizí moci, užije postup uvedený v bodě 4.

6. Informace k oznamování změn

Podnikatel má povinnost oznámit Úřadu:

- změny všech údajů v **žádosti podnikatele, v dotazníku podnikatele, v bezpečnostní dokumentaci podnikatele**, je-li účastníkem řízení, **a to neprodleně** (§ 103 odst. 2 zákona č. 412/2005 Sb.),
- změny údajů **v položce a), b) a p) dotazníku podnikatele** a v části ***„popis způsobů realizace jednotlivých druhů zajištění ochrany utajovaných informací“* bezpečnostní dokumentace v rozsahu aktualizace toho druhu zajištění ochrany utajovaných informací, u kterého nastala změna**, je-li držitelem osvědčení podnikatele, **a to neprodleně** (§ 68 písm. c) zákona č. 412/2005 Sb.)

pozn.: „neprodleně“ – jedná se o právně neurčitý pojem, tzn., jakmile to okolnosti podnikateli dovolí a zároveň bez zbytečného odkladu,

- změny údajů v **žádosti podnikatele, v dotazníku podnikatele** (s výjimkou položek c), j) až l))**, v bezpečnostní dokumentaci podnikatele** (v rozsahu aktualizace té části, která se změnila), je-li držitelem osvědčení podnikatele, **a to jedenkrát za kalendářní rok, vždy ke dni, který se datem shoduje se dnem vydání osvědčení podnikatele** (§ 68 písm. d) zákona č. 412/2005 Sb.).

Změny údajů v dotazníku podnikatele podnikatel dokládá písemnostmi k ověření podmínek podle § 16 zákona č. 412/2005 Sb. v rozsahu a formě stanovenými v § 3 vyhlášky o průmyslové bezpečnosti.

Upozornění:

Pokud je podnikatel držitelem více osvědčení podnikatele, oznamuje změny údajů pouze v jednom vyhotovení. Ve „změnovém dotazníku podnikatele“ uvede všechny stupně utajení a formy přístupu, která tato osvědčení obsahují.

Oznamování změn údajů jedenkrát za kalendářní rok (§ 68 písm. d) zákona č. 412/2005 Sb.) v tomto případě předkládá podnikatel Úřadu k tomu dni, na který připadá datum vydání osvědčení podnikatele, které bylo podnikateli vydáno dříve.

Je-li podnikateli vydáno „náhradní“ osvědčení podnikatele, neboť ohlásil Úřadu odcizení nebo ztrátu „původně vydaného“ osvědčení podnikatele nebo došlo k jeho poškození nebo změně některého z údajů v něm uvedených, je za den vydání osvědčení podnikatele nadále pokládán den vydání „původně vydaného“ osvědčení podnikatele.

Podnikatel, který má přístup k utajované informaci, má také povinnost neprodleně písemně oznamovat Úřadu skutečnost, která může mít vliv na vydání nebo na platnost osvědčení (fyzické osoby) nebo osvědčení podnikatele (§ 69 zákona č. 412/2005 Sb.).

Způsob a forma oznamování změn

Pro oznamování změn údajů v dotazníku podnikatele v průběhu bezpečnostního řízení použije podnikatel dotazník podnikatele a pro oznamování změn údajů v dotazníku podnikatele po vydání osvědčení podnikatele příslušný „změnový dotazník podnikatele“, které jsou k dispozici na internetových stránkách Úřadu (www.nbu.cz).

Pro oznamování změn údajů ve formuláři žádost podnikatele může použít podnikatel šablonu vzoru žádost podnikatele, která je k dispozici na internetových stránkách Úřadu (www.nbu.cz).

Je-li to požadavek vyhlášky o průmyslové bezpečnosti, musí být oznamovaná změna doložena příslušnými písemnostmi, a to ve stanovené formě (viz výše).

Z oznámení změn musí být patrné, kdo jej činí (je třeba uvést identifikační údaje podnikatele a jméno

a příjmení odpovědné osoby podnikatele) a čeho se týká. Dále toto oznámení musí obsahovat označení orgánu, jemuž je určeno (Úřad) a podpis odpovědné osoby podnikatele.

Oznámení změn lze podat v listinné nebo elektronické podobě.

V listinné podobě lze podat oznámení změn osobně nebo prostřednictvím jiné, k tomu účelu pověřené, osoby v podatelně místa sídla Úřadu (Na Popelce 2/16, Praha 5 – Košíře), v úředních hodinách.

Úřední hodiny podatelny	
Pondělí a středa:	8:00 – 17:00
Úterý a čtvrtek:	8:00 – 15:00
Pátek:	8:00 – 12:00

Oznámení změn lze také zaslat prostřednictvím držitele poštovní licence nebo zvláštní poštovní licence na adresu Úřadu (P.O.BOX 49, Praha 56, PSČ 150 06).

V elektronické podobě lze podat oznámení změn dodáním do **datové schránky Úřadu** (ID Úřadu – h93aayw, do pole „Věc“ se uvede „Bezpečnostní řízení – Hlášení změn“) nebo na **elektronickou podatelnu Úřadu** (posta@nbu.cz, do pole „Předmět“ se uvede „Bezpečnostní řízení – Hlášení změn“).

V těchto případech podání:

- **formulář žádost podnikatele** musí být výstupem z autorizované konverze nebo musí být podepsaný odpovědnou osobou, a to uznávaným elektronickým podpisem,
- **výpis z účtu vlastníka v centrální evidenci investičních nástrojů** musí být výstupem z autorizované konverze nebo musí být podepsaný osobou, která písemnost vydala, a to uznávaným elektronickým podpisem,
- **ostatní písemnosti nutné k ověření podmínek podle § 16 zákona č. 412/2005 Sb.** při podání na **elektronickou podatelnu** musí být výstupem z autorizované konverze nebo musí být podepsané odpovědnou osobou, a to uznávaným elektronickým podpisem; při podání do **datové schránky** nemusí výše uvedené požadavky splňovat,
- **změnový dotazník podnikatele a bezpečnostní dokumentace podnikatele** nemusí splňovat požadavky uvedené v předchozích bodech, u dodání na elektronickou podatelnu musí být podání podepsané odpovědnou osobou, a to uznávaným elektronickým podpisem.

Jakou sankci lze uložit za nesplnění povinnosti hlásit změny

- až 50.000 Kč nesplní-li povinnost stanovenou v § 68 písm. c) nebo d) zákona č. 412/2005 Sb. (§ 155 č. 412/2005 Sb.)

Neoznámení změny může být Úřadem rovněž vyhodnoceno jako bezpečnostní riziko podle § 18 odst. 3 zákona č. 412/2005 Sb., což může mít za následek nevyhovění žádosti o vydání osvědčení podnikatele, resp. zrušení platnosti existujícího osvědčení podnikatele.

7. Odpovědná osoba

Za účastníka bezpečnostního řízení jedná pouze odpovědná osoba, nejde-li o zastupování účastníka řízení advokátem nebo jiným zástupcem (§ 89 odst. 6 zákona č. 412/2005 Sb.). Úřad tedy může akceptovat pouze podání učiněná odpovědnou osobou podnikatele nebo advokátem nebo jiným zástupcem. Tento postup platí jak pro bezpečnostní řízení, tak i pro oznamování změn.

Odpovědnou osobou u podnikatele je:

1. u podnikající fyzické osoba tato osoba,
2. u právnické osoby
   a) statutární orgán – jednotlivec nebo
   b) osoba, která je členem vícečlenného statutárního orgánu, nebo
   c) osoba mimo statutární orgán.

V případě bodu 2. písmena b) prokazuje podnikatel pověření osoby ze statutárního orgánu výkonem

funkce odpovědné osoby **písemným pověřením** konkrétního člena statutárního orgánu učiněným podle způsobu jednání za podnikatele.

V případě bodu 2. písmena c) prokazuje podnikatel pověření osoby výkonem funkce odpovědné osoby **písemným pověřením** této osoby a **zmocněním jednat jménem či za právnickou osobu podle zvláštního právního předpisu** (např. § 15 obchodního zákoníku, § 441 občanského zákoníku) učiněným podle způsobu jednání za podnikatele.

Písemné pověření a zmocnění podle bodu 2. předkládá podnikatel Úřadu na základě jeho výzvy.

8. Bezpečnostní ředitel (§ 71 zákona č. 412/2005 Sb.)

Podnikatel, který má přístup k utajované informaci, je povinen zřídit a obsadit funkci bezpečnostního ředitele. Do 15 dnů ode dne obsazení funkce bezpečnostního ředitele je povinen oznámit písemně Úřadu jméno, příjmení a rodné číslo osoby vykonávající tuto funkci.

Bezpečnostní ředitel schvaluje přehled míst nebo funkcí podle § 69 odst. 1 písm. b) zákona č. 412/2005 Sb., u nichž je vyžadován přístup k utajované informaci, a plní další povinnosti stanovené mu písemně odpovědnou osobou v rozsahu zákona č. 412/2005 Sb.

Funkci bezpečnostního ředitele nemůže fyzická osoba vykonávat u více subjektů souběžně. Pro výkon této funkce u podnikatele musí být fyzická osoba držitelem osvědčení pro přístup k utajované informaci nejméně takového stupně utajení, pro který má podnikatel vydané osvědčení podnikatele, a dále musí být poučena (§ 11 zákona č. 412/2005 Sb.).

9. Informace k přístupu k utajovaným informacím

Přístup k utajovaným informacím může mít:

1. podnikatel, který:
   - v případě utajovaných informací stupně utajení VYHRAZENÉ doloží prohlášením podnikatele svou schopnost zabezpečit ochranu utajovaných informací nebo je držitelem osvědčení podnikatele (DŮVĚRNÉ, TAJNÉ, PŘISNĚ TAJNÉ),
   - v případě utajované informace stupně utajení DŮVĚRNÉ, TAJNÉ nebo PŘÍSNÉ TAJNÉ je držitelem platného osvědčení podnikatele odpovídajícího nebo vyššího stupně,
2. podnikatel, kterému bylo uznáno bezpečnostní oprávnění vydané úřadem cizí moci (§ 62 zákona č. 412/2005 Sb.),
3. podnikatel, kterému byl udělen souhlas s jednorázovým přístupem k utajované informaci (§ 59 zákona č. 412/2005 Sb.),
4. podnikatel, který není držitelem osvědčení podnikatele nebo nemá přístup k utajovaným informacím stupně utajení Vyhrazené, a to v případě účasti ČR v ozbrojeném konfliktu v zahraničí nebo v záchranné nebo humanitární akci v zahraničí, v případě vyhlášení válečného stavu a v případě stavu nebezpečí, nouzového stavu nebo stavu ohrožení státu (§ 60 zákona č. 412/2005 Sb.).

Ad 1)

	Přístup k utajované informaci stupně Vyhrazené	**Přístup k utajované informaci stupně Důvěrné nebo Tajné nebo Přísně tajné**
Typ dokumentu nebo veřejné listiny	Prohlášení podnikatele	Osvědčení
	Osvědčení	

Ad 2)

Přístup k utajované informaci na základě uznání bezpečnostního oprávnění vydaného úřadem cizí moci (§ 62 zákona č. 412/2005 Sb.)

Na základě žádosti podnikatele provede Úřad uznání cizího bezpečnostního oprávnění. Žádost lze

podat i prostřednictvím úřadu cizí moci, který má v působnosti ochranu utajovaných informací. Jedná se o případy, kdy to umožňuje mezinárodní smlouva, kterou je ČR vázána, nebo kdy je uznání v souladu se zahraničně politickými a bezpečnostními zájmy ČR. Na toto uznání není právní nárok.

K žádosti je nutné přiložit úřední překlad bezpečnostního oprávnění nebo jeho ověřenou kopii; tyto doklady se nevyžadují, je-li žádost podána prostřednictvím úřadu cizí moci, který má v působnosti ochranu utajovaných informací, pokud tento na žádosti potvrdí, že podnikatel je držitelem příslušného bezpečnostního oprávnění.

Žádost musí obsahovat také důvod, proč má být uznání provedeno, a dobu, na jakou má být provedeno.

Ad 3)

Jednorázový přístup k utajované informaci (§ 59, § 61 zákona č. 412/2005 Sb.)

Úřad může ve výjimečných a odůvodněných případech vydat souhlas s jednorázovým přístupem k utajované informaci o jeden stupeň vyšším, než na který je vydáno platné osvědčení podnikatele, nejdéle však na dobu 6 měsíců a pouze pro formu přístupu podnikatele, která spočívá pouze v tzv. seznamování se s utajovanou informací, tzn. že utajovaná informace není podnikateli předávána a podnikatel se s ní pouze seznámí např. u zadavatele zakázky; jednorázový přístup nelze umožnit k utajované informaci stupně utajení PŘÍSNĚ TAJNÉ. **Jednorázový přístup tedy může být udělen pouze pro přístup k utajované informaci stupně utajení Tajné.**

Žádost o jednorázový přístup je vždy písemná, podepisuje ji odpovědná osoba podnikatele a obsahuje zdůvodnění potřeby jednorázového přístupu, označení oblasti utajovaných informací, ke kterým má být přístup umožněn a požadovanou dobu jednorázového přístupu. Přílohou žádosti musí být kopie osvědčení podnikatele a písemný souhlas poskytovatele utajované informace s vydáním souhlasu s jednorázovým přístupem. Témuž podnikateli lze souhlas udělit jen jednou a není na něj právní nárok. V kladném případě je souhlas vydán nejpozději do 5 dnů.

K utajované informaci cizí moci lze jednorázový přístup umožnit pouze v souladu s požadavky této cizí moci.

Ad 4)

Přístup k utajované informaci v případě účasti ČR v ozbrojeném konfliktu v zahraničí nebo v záchranné nebo humanitární akci v zahraničí, v případě vyhlášení válečného stavu a v případě stavu nebezpečí, nouzového stavu nebo stavu ohrožení státu (§ 60 zákona č. 412/2005 Sb.).

Pokud není podnikatel držitelem osvědčení podnikatele nebo nemá přístup k utajovaným informacím stupně utajení Vyhrazené, lze mu, ve výše uvedených případech, umožnit přístup k utajované informaci.

Odpovědná osoba podnikatele je povinna o přístupu zpracovat písemný záznam a neprodleně jej zaslat Úřadu.

K utajované informaci cizí moci lze přístup umožnit pouze v souladu s požadavky této cizí moci.

10. Dokumenty odesílané a přijímané v rámci bezpečnostního řízení prostřednictvím informačního systému datových schránek v oblasti průmyslové bezpečnosti

1) Náležitosti žádostí o vydání osvědčení podnikatele podle zákona č. 412/2005 Sb. – viz kapitola **3. Informace k podání žádosti o vydání osvědčení podnikatele (D, T, PT).**
2) Oznamování změn – viz kapitola **6. Informace k oznamování změn.**
3) Prostřednictvím datové schránky zřízené pro podnikatele lze činit všechny úkony týkající se řízení o vydání osvědčení podnikatele (vyjma osobních úkonů).
4) Komunikace s orgánem státu, právnickou osobou, podnikající fyzickou osobou, od kterých vyžaduje Úřad informace k účastníkovi řízení nebo držiteli osvědčení podnikatele.

Upozornění:

Při komunikaci podle bodu 3) a 4) je vhodné uvádět v datové zprávě v poli ***„Věc“ – „Bezpečnostní řízení“****.*

V případě, že podnikatel nebo subjekt uvedený v bodě 4) reaguje na ***písemnost Úřadu (dožádání, sdělení, oznámení, rozhodnutí...)****, je vhodné uvádět také číslo jednací, kterým byla tato písemnost označena (např. 110002/2012-NBÚ/21 ...), a to rovněž do pole „****Věc****“ (např. Bezpečnostní řízení č.j. 110002/2012-NBÚ/21).*

ABECEDNÍ SEZNAM PODNIKATELŮ,
kterým bylo vydáno osvědčení podnikatele podle § 121 odst. 1 zákona č. 412/2005 Sb.
(stav k 22. 2. 2015):

obchodní firma	*IČ*	*číslo osvědčení*	*platnost do*	*stupeň utajení pro seznamování se s UI*	*stupeň utajení pro poskytování nebo vznik UI*
"SCHWARZ s.r.o."	61677744	001285	16.2.2019	Důvěrné	-
100MEGA Distribution s.r.o.	60707968	000648	8.11.2016	Důvěrné	-
A L K O M - I P C spol. s r.o.	41694538	000209	7.6.2015	Důvěrné	-
AB Facility a.s.	24172413	001831	19.11.2021	Důvěrné	-
ABAS IPS Management s.r.o.	25842811	000431	15.2.2016	Důvěrné	Důvěrné
ABEL C & C s.r.o.	25233157	001885	4.4.2022	Důvěrné	-
AboutNet s.r.o.	26721996	001997	9.6.2021	Tajné	-
Actinet Informační systémy s.r.o.	25552635	001436	17.8.2017	Tajné	-
ADASTRA, s.r.o.	26202981	000511	27.6.2015	Důvěrné	Důvěrné
ADC CZ spol. s r.o.	15038459	000145	12.4.2015	Důvěrné	-
AEC, spol. s r.o.	26236176	001906	22.8.2016	Důvěrné	-
AED project, a.s.	61508594	001772	2.5.2021	Důvěrné	Důvěrné
AERO TRADE a.s.	49240161	001343	18.4.2019	Důvěrné	Důvěrné
AERO Vodochody a.s.	00010545	000794	28.5.2017	Důvěrné	Důvěrné
AERO Vodochody a.s.	00010545	001497	25.10.2017	Tajné	-
AERO Vodochody AEROSPACE a.s.	24194204	001824	25.10.2021	Důvěrné	-
AERO Vodochody AEROSPACE a.s.	24194204	002057	1.2.2022	-	Tajné
Aerokoraab s.r.o.	28234464	001888	9.4.2022	Důvěrné	-
AG COM, a.s.	47452081	000691	10.1.2017	Důvěrné	Důvěrné
ALARM CZ s.r.o.	60913223	001873	7.3.2020	Tajné	-
ALEF NULA,a.s.	61858579	001761	3.4.2021	Důvěrné	-
ALES, s.r.o.	48208388	000316	7.9.2015	Důvěrné	Důvěrné
ALES, s.r.o.	48208388	001892	12.5.2020	Tajné	-
ALIMEX s.r.o.	49613529	001418	21.7.2019	Důvěrné	Důvěrné
ALKOM Security, a.s.	26184672	000197	29.5.2015	Důvěrné	Důvěrné
ALLSAT s.r.o.	48109720	000408	11.1.2016	Důvěrné	Důvěrné
ALTRON, a.s.	64948251	001944	16.12.2020	Tajné	-
ALTRON, a.s.	64948251	002050	14.12.2023	-	Důvěrné
ALZAKOM, spol. s r.o.	26819104	001504	1.11.2019	Důvěrné	Důvěrné
ANAKAN s.r.o.	27443795	001957	29.1.2021	Tajné	-
ANECT a.s.	25313029	001859	7.9.2015	Tajné	Tajné
ANTA spol. s r.o.	45793891	000889	1.9.2017	Důvěrné	-
Apex Bohemia s.r.o.	64788440	001975	9.7.2015	Důvěrné	-
AQUASOFT spol. s r.o.	64946274	001272	27.1.2017	Tajné	-
ARAMY s.r.o.	29026121	001629	16.5.2020	Důvěrné	-
AREA G.K. spol. s r.o.	25094459	001899	2.6.2022	Důvěrné	-
ARGUS, spol. s r.o.	00203459	001993	3.3.2018	Důvěrné	Důvěrné
ARGUS, spol. s r.o.	00203459	001994	25.1.2018	Tajné	-
ARSEL, spol. s r.o.	25339052	000512	5.6.2016	Důvěrné	-
ARYKA IN-WEST a.s.	26722411	001810	29.8.2021	Důvěrné	Důvěrné
ASD Software, s.r.o.	62363930	000730	9.3.2017	Důvěrné	Důvěrné
ASD Software, s.r.o.	62363930	002027	5.10.2021	Tajné	-
ASEC - elektrosystémy s.r.o.	26277930	001791	26.6.2021	Důvěrné	-
Asseco Central Europe, a.s.	27074358	001856	18.6.2017	Důvěrné	-

Asseco Central Europe, a.s.	27074358	001857	16.12.2015	Tajné	Tajné
ASTOR-KOMPLEX s.r.o.	47469781	001626	31.3.2019	Důvěrné	Důvěrné
ATALIAN CZ s.r.o.	25059394	001688	7.4.2019	Důvěrné	-
ATELIER PENTA v.o.s.	47916621	001188	11.10.2018	Důvěrné	Důvěrné
ATICO s r.o.	49712624	001787	20.6.2021	Důvěrné	Důvěrné
ATICO s r.o.	49712624	001816	19.9.2019	Tajné	-
Atos IT Solutions and Services, s.r.o.	44851391	001966	4.3.2021	-	Tajné
ATS-TELCOM PRAHA a.s.	61860409	001349	28.4.2017	Tajné	Tajné
AURA, s.r.o.	46991573	001448	30.8.2019	Důvěrné	-
AUROTON COMPUTER, spol.s r.o.	43871437	000260	9.7.2015	Důvěrné	-
AutoCont CZ a.s.	47676795	002007	16.7.2023	-	Důvěrné
AVERS, spol. s r.o.	41190840	001930	19.9.2016	Důvěrné	Důvěrné
AXENTA a.s.	28349822	001970	20.6.2021	Důvěrné	-
AŽD Praha s.r.o.	48029483	000868	12.8.2017	Důvěrné	Důvěrné
B.O.I.S. - FILTRY, spol. s r.o.	44962592	001741	27.5.2017	Důvěrné	Důvěrné
BARA HK spol. s r.o.	49815211	000908	21.9.2017	Důvěrné	Důvěrné
Bartoň a Partner s.r.o.	26810093	001829	7.11.2021	Důvěrné	-
BDO IT a.s.	25056646	001336	13.4.2019	Důvěrné	Důvěrné
BDO IT a.s.	25056646	001337	13.4.2017	Tajné	-
BEDEA spol. s r.o.	48907065	001382	9.6.2019	Důvěrné	-
BERGER BOHEMIA a. s.	45357269	000198	29.5.2015	Důvěrné	Důvěrné
BEScom Security s.r.o.	26817403	000535	26.6.2016	Důvěrné	Důvěrné
BLESK Servis s.r.o.	27607429	002049	27.4.2020	Důvěrné	-
BLOCK a.s.	18055168	000421	25.1.2016	Důvěrné	Důvěrné
Blue Partners s.r.o.	27373622	001683	12.9.2020	Důvěrné	Důvěrné
Blue Partners s.r.o.	27373622	001809	28.8.2019	Tajné	-
BMT Medical Technology s.r.o.	46346996	002055	19.1.2024	-	Důvěrné
BOHEMIA MARTEN SECURITY s.r.o.	24288152	001972	31.3.2023	Důvěrné	-
BULL s.r.o.	49242954	001901	20.3.2016	Důvěrné	-
BULL s.r.o.	49242954	001902	14.12.2016	Tajné	-
CASUA, spol.s r.o.	44846908	002039	10.11.2023	Důvěrné	-
CATEGORY a.s.	25571192	001363	16.5.2019	Důvěrné	Důvěrné
CB SERVIS CENTRUM s.r.o.	48201464	000954	24.11.2017	Důvěrné	Důvěrné
CENTR GROUP, a.s.	26865301	002021	27.6.2019	Tajné	-
CENTR GROUP, a.s.	26865301	002022	29.5.2021	Důvěrné	Důvěrné
Centrum výzkumu Řež s.r.o.	26722445	001838	16.12.2017	Tajné	-
CESA a.s.	13585096	001728	3.5.2015	Důvěrné	Důvěrné
CESA a.s.	13585096	001979	24.4.2021	Tajné	-
CGI IT Czech Republic s.r.o.	62412388	001934	24.10.2017	Tajné	-
CGI IT Czech Republic s.r.o.	62412388	001967	4.3.2023	-	Důvěrné
COBAP s.r.o.	28953673	001904	27.6.2021	Důvěrné	-
COFI s.r.o.	27187616	001874	7.3.2022	Důvěrné	-
COLAS CZ, a.s.	26177005	000857	4.8.2017	Důvěrné	Důvěrné
COLAS CZ, a.s.	26177005	000867	11.8.2015	Tajné	-
Colsys s.r.o.	14799634	000981	17.12.2017	Důvěrné	Důvěrné
Colsys s.r.o.	14799634	000982	17.12.2015	Tajné	-
ComArr, spol. s r.o.	15050084	000829	30.6.2015	Tajné	-
ComArr, spol. s r.o.	15050084	000866	11.8.2017	Důvěrné	Důvěrné
COMIMPEX spol. s r.o.	46972439	001134	28.6.2018	Důvěrné	Důvěrné

COMINFO, a.s.	63482576	001122	9.6.2018	Důvěrné	Důvěrné
COMPANY GLANC s.r.o.	28878663	001259	20.1.2019	Důvěrné	-
Comproject s.r.o.	28494652	001926	9.10.2022	-	Důvěrné
Computer System cz s.r.o.	26834979	001650	26.6.2020	Důvěrné	-
Computer System Praha spol. s r.o.	26154471	000045	1.3.2015	Důvěrné	-
Com-Sys TRADE spol. s r.o.	16188781	001066	2.4.2018	Důvěrné	-
CONMEDITECH s.r.o.	24165841	001917	11.9.2022	Důvěrné	-
CSC Computer Sciences s.r.o.	64938140	001853	7.1.2022	-	Důvěrné
CZ team s.r.o.	27134601	001945	15.11.2015	Důvěrné	-
Czasch spol. s r.o.	47972947	001550	20.12.2017	Tajné	-
Czasch spol. s r.o.	47972947	001596	20.3.2020	Důvěrné	Důvěrné
Czech Airlines Handling, a.s.	25674285	001798	1.10.2017	Důvěrné	-
ČD - Informační Systémy, a.s.	24829871	001907	18.7.2022	-	Důvěrné
ČD - Telematika a.s.	61459445	001846	18.12.2019	Tajné	Tajné
ČD Cargo, a.s.	28196678	001018	2.2.2018	Důvěrné	Důvěrné
ČEPRO, a.s.	60193531	002045	8.12.2023	Důvěrné	-
Česká pošta, s.p.	47114983	001026	11.2.2018	Důvěrné	Důvěrné
Česká zbrojovka a.s.	46345965	001076	19.4.2016	Tajné	-
Česká zbrojovka a.s.	46345965	001182	24.9.2018	Důvěrné	Důvěrné
České aerolinie a.s.	45795908	001799	12.8.2019	Důvěrné	Důvěrné
České dráhy, a.s.	70994226	001514	10.11.2019	Důvěrné	Důvěrné
České Radiokomunikace a.s.	24738875	001812	27.6.2019	Tajné	Tajné
ČEZ Distribuce, a. s.	24729035	001962	10.2.2023	-	Důvěrné
ČEZ ICT Services, a. s.	26470411	001651	15.8.2015	Důvěrné	Důvěrné
ČEZ ICT Services, a. s.	26470411	001652	13.12.2017	Tajné	Tajné
ČEZ, a. s.	45274649	001925	8.10.2020	-	Tajné
ČOS - Česká ochranná společnost a.s.	25853317	000774	6.5.2017	Důvěrné	-
D.I.S., spol. s r.o.	46975616	001731	23.4.2018	Důvěrné	-
Dalibor Mikeš	72143037	002041	19.11.2021	Tajné	-
Dálniční stavby Praha, a.s.	40614948	000231	20.6.2015	Důvěrné	Důvěrné
DATASYS s.r.o.	61249157	001815	11.9.2021	Důvěrné	-
DAVELO spol. s r.o.	44684347	001886	9.4.2022	Důvěrné	-
DBD CONTROL SYSTEMS spol. s r.o.	42407982	000823	26.6.2017	Důvěrné	Důvěrné
DCIT, a.s.	26143097	001842	12.12.2021	Důvěrné	-
Deepview s.r.o.	24734462	001880	27.3.2022	Důvěrné	-
DEFCON s.r.o.	28877446	001291	24.2.2019	Důvěrné	Důvěrné
DELINFO, spol. s r.o.	49448218	002032	12.8.2017	Důvěrné	Důvěrné
DELINFO, spol. s r.o.	49448218	002033	12.8.2015	Tajné	-
Deloitte Security s.r.o.	27899152	000672	5.12.2016	Důvěrné	Důvěrné
Deloitte Security s.r.o.	27899152	002015	24.8.2021	Tajné	-
DICOM, spol. s r.o.	47912502	000635	24.10.2016	Důvěrné	Důvěrné
DICOM, spol. s r.o.	47912502	001989	14.5.2021	Tajné	-
Dimension Data Communications Czech s.r.o.	26175738	001983	2.5.2020	Tajné	Tajné
DKNV stavební, s.r.o.	27375021	001991	6.12.2019	Důvěrné	Důvěrné
DMS s.r.o.	49436392	001137	30.6.2016	Tajné	Tajné
DRAKAS s.r.o.	26301342	000973	10.12.2017	Důvěrné	-
Družstvo HLS, výrobní družstvo Plzeň	40526801	001396	28.6.2019	Důvěrné	-
DUSIL a spol., v.o.s.	45806730	001256	13.1.2019	Důvěrné	-
E + M plus spol. s r.o.	61944769	000710	3.2.2017	Důvěrné	Důvěrné

EBIS, spol. s r.o.	45477388	001453	31.8.2017	Tajné	Tajné
EDIKT a.s.	25172328	000484	26.4.2016	Důvěrné	Důvěrné
EDIKT a.s.	25172328	002003	26.6.2021	Tajné	-
EGEM s.r.o.	63886464	001007	24.6.2016	Důvěrné	Důvěrné
EGEM s.r.o.	63886464	001941	18.1.2016	Tajné	-
EKOKLIMA akciová společnost	00474835	001747	8.1.2018	Důvěrné	Důvěrné
EKOSA s.r.o.	62583565	001807	31.10.2019	Důvěrné	Důvěrné
EKOSYSTEM spol. s r.o.	44851804	000223	18.6.2015	Důvěrné	-
ELBES PRAHA, spol. s r.o.	26751232	000166	25.4.2015	Důvěrné	-
ELDIS Pardubice, s.r.o.	15050742	001070	8.4.2016	Tajné	Tajné
ELMES PRAHA,s.r.o.	65411587	001782	4.6.2021	Důvěrné	-
ELSO PHILIPS SERVICE, spol. s r.o.	48113336	000413	17.1.2016	Důvěrné	Důvěrné
ELTES, s.r.o.	61504513	001022	9.2.2018	Důvěrné	Důvěrné
ELTODO, a.s.	45274517	001943	16.12.2017	Důvěrné	Důvěrné
EMV s.r.o.	48038792	001470	9.11.2018	Důvěrné	Důvěrné
ENNIT, s.r.o.	25054538	002046	8.12.2023	Důvěrné	-
eNovation s.r.o.	27909751	001746	21.9.2020	Důvěrné	-
EPLcond a.s.	26346575	002040	12.11.2023	Důvěrné	-
Equica, a.s.	26490951	001455	1.9.2017	Tajné	-
ERA a.s.	60916427	001327	31.3.2017	Tajné	Tajné
ERICSSON spol. s r.o.	48583456	001422	4.8.2017	Tajné	Tajné
Ernst & Young Audit, s.r.o.	26704153	001955	25.6.2015	Důvěrné	Důvěrné
ESET Praha, s.r.o.	27108481	001954	19.1.2021	Tajné	-
ETV security, s.r.o.	27631176	002018	24.3.2017	Důvěrné	-
EUGEO s.r.o.	01446860	001990	12.5.2022	Důvěrné	-
Europatron s.r.o.	48290394	001691	21.9.2020	Důvěrné	Důvěrné
EUROPROTECT s.r.o.	27403521	001868	11.2.2022	Důvěrné	-
Excello s.r.o.	27444899	000808	10.6.2017	Důvěrné	-
Explosia a.s.	25291581	000961	1.12.2017	Důvěrné	Důvěrné
EZH,a.s.	26901005	001884	3.4.2020	Tajné	-
F.S.C. BEZPEČNOSTNÍ PORADENSTVÍ, a.s.	25884646	001869	19.8.2015	Tajné	Tajné
FASS, s.r.o.	45808163	000136	6.4.2015	Důvěrné	Důvěrné
FATO a.s., člen holdingu FATO	27473295	001150	12.7.2018	Důvěrné	Důvěrné
FITCOM s.r.o.	60320117	002006	7.7.2023	Důvěrné	-
FM solutions, a.s.	25692445	000150	13.4.2015	Důvěrné	-
FMIB, s.r.o.	25908898	001821	10.10.2019	Důvěrné	-
FORTE a.s.	25322303	000240	26.6.2015	Důvěrné	Důvěrné
FSC Elektro s.r.o.	26249316	001844	14.6.2020	Důvěrné	-
Fujitsu Technology Solutions s.r.o.	26115310	001083	20.5.2017	Důvěrné	-
G4S Secure Solutions (CZ), a.s.	00175439	001813	4.6.2015	Důvěrné	Důvěrné
G4S Secure Solutions (CZ), a.s.	00175439	001863	24.1.2020	Tajné	-
GC System a.s.	64509826	001491	17.10.2017	Tajné	-
GEFOS a.s.	25684213	001971	27.3.2023	-	Důvěrné
GEOREAL spol. s r.o.	40527514	001735	18.10.2019	Důvěrné	-
GEOtest, a.s.	46344942	001981	29.4.2021	-	Tajné
GESPOL s.r.o.	25216767	002048	9.12.2023	Důvěrné	-
GiTy, a.s.	25302400	001489	13.10.2017	Tajné	Tajné
GLANZIS s.r.o.	27623891	001309	14.3.2019	Důvěrné	-
Glomex MS, s.r.o.	28426525	001699	6.10.2018	Tajné	-

GOPE Systems a.s.	24831271	001767	19.4.2019	Tajné	-
GORDIC spol. s r.o.	47903783	000833	1.7.2017	Důvěrné	Důvěrné
GORDIC spol. s r.o.	47903783	000907	18.9.2015	Tajné	-
Griffin, a.s.	25649345	001912	13.8.2020	Tajné	Tajné
GUNNEBO CZ s.r.o.	61249114	000945	11.11.2015	Tajné	-
Hana Skálová	48019712	001773	3.5.2019	Tajné	-
HaSaM, s.r.o.	49968319	000642	5.4.2015	Důvěrné	-
ha-vel internet s.r.o.	25354973	001937	13.11.2022	-	Důvěrné
Heberger CZ s.r.o.	61508926	001895	17.8.2019	Důvěrné	Důvěrné
HELIKA, a.s.	60194294	000952	24.11.2017	Důvěrné	Důvěrné
HES, s.r.o.	46974954	000169	2.5.2015	Důvěrné	Důvěrné
HEWLETT-PACKARD s.r.o.	17048851	001875	10.3.2020	-	Tajné
HI Software Development s.r.o.	26829819	001575	4.12.2017	Důvěrné	-
HOCHTIEF CZ a. s.	46678468	001881	28.3.2020	-	Tajné
CHEMCOMEX Praha, a.s.	25076451	001752	8.12.2018	Důvěrné	Důvěrné
I P P S, s.r.o.	45315973	002009	2.8.2016	Důvěrné	-
I.B.S.A. - czech, s.r.o.	28195469	001159	22.7.2016	Tajné	-
I.B.S.A. - czech, s.r.o.	28195469	001475	3.10.2019	Důvěrné	Důvěrné
I3 Consultants s.r.o.	27921344	001584	23.6.2018	Důvěrné	-
IBM Česká republika, spol. s r.o.	14890992	001867	10.2.2020	-	Tajné
ICZ a.s.	25145444	001985	2.7.2016	Důvěrné	Důvěrné
IMOS Brno, a.s.	25322257	001949	11.8.2019	Důvěrné	Důvěrné
Indra Czech Republic s.r.o.	65409981	002005	27.11.2019	Tajné	Tajné
INEL - Technik, s.r.o.	25249649	001898	23.5.2022	Důvěrné	-
INEX Česká republika s.r.o.	61328987	001284	16.2.2019	Důvěrné	-
Ing. arch. Vlastislav RUBEK	10141642	000960	1.12.2017	Důvěrné	-
Ing. František Reitoral	12184691	001744	11.1.2021	Důvěrné	-
Ing. Zdeněk Jäger	11253274	001819	15.10.2021	Důvěrné	-
Ing. Zdeněk Jiříček	88597750	001894	13.5.2022	Důvěrné	-
Ing.arch. Jaroslav Kačer	13785958	001832	26.11.2021	Důvěrné	-
INGBAU CZ s.r.o.	25941127	000846	20.7.2017	Důvěrné	Důvěrné
INKOS-OSTRAVA, a.s.	48394637	001786	17.6.2019	Tajné	Tajné
INNA s.r.o.	45275131	000631	16.10.2016	Důvěrné	Důvěrné
INNA s.r.o.	45275131	001897	23.5.2020	Tajné	-
INSTALACE Praha, spol. s r.o.	45804371	001932	13.12.2021	-	Důvěrné
Institut mikroelektronických aplikací s.r.o.	45277397	000317	10.9.2015	Důvěrné	Důvěrné
INTAR a.s.	25594443	001987	12.12.2015	Důvěrné	Důvěrné
INTAR a.s.	25594443	001988	14.7.2020	Tajné	-
Integoo s.r.o.	26912571	002023	13.5.2017	Důvěrné	Důvěrné
Integraf, s.r.o.	47451980	002020	3.9.2023	-	Důvěrné
Intermont, Opatrný, s.r.o.	49900854	001156	20.7.2018	Důvěrné	-
INTRIPLE, a.s.	27448827	001344	19.4.2019	Důvěrné	Důvěrné
INTV, spol. s r.o.	40766063	000423	1.2.2016	Důvěrné	Důvěrné
INVEA-TECH a.s.	27730450	001939	26.11.2020	Tajné	-
Inženýrsko-realizační s.r.o.	27809986	001800	23.7.2019	Tajné	-
Iron Mountain Česká republika s.r.o.	25064631	000811	15.6.2017	Důvěrné	Důvěrné
ISS Facility Services s.r.o.	60470291	001801	23.7.2021	Důvěrné	-
it&t s.r.o.	25422731	001742	5.1.2021	Důvěrné	Důvěrné
ITS akciová společnost	14889811	001754	6.3.2021	Důvěrné	Důvěrné

Ivo Menšík	18138225	001197	28.10.2018	Důvěrné	Důvěrné
IXTENT s.r.o.	27071162	001850	11.3.2019	Důvěrné	-
Jaroslav Havel	12159956	001270	27.1.2019	Důvěrné	-
Jaroslav Prukner	12159948	001297	4.3.2019	Důvěrné	-
JIMI CZ, a.s.	25313436	001219	9.4.2016	Tajné	Tajné
JIMI CZ, a.s.	25313436	001823	21.10.2017	Přísně tajné	-
Jiří Novák	67176739	001329	5.4.2017	Tajné	-
Jiří Vrba	10084673	001021	5.2.2018	Důvěrné	Důvěrné
JOHNSON CONTROLS INTERNATIONAL, spol. s r.o.	43871143	001726	31.3.2019	Důvěrné	Důvěrné
JOSYMA MB, s.r.o.	27174557	001931	23.10.2022	Důvěrné	-
JUDr. Jiří Kameník	13127373	001600	28.3.2020	Důvěrné	-
JVM Computers spol. s r.o.	45311684	001258	18.1.2019	Důvěrné	-
K.T.S. - MONTÁŽE, s.r.o.	26287579	001399	29.6.2019	Důvěrné	-
K+H bezpečnostní systémy s.r.o.	27440028	001961	9.2.2023	Důvěrné	-
KALÁB-stavební firma, spol. s r. o.	49436589	001047	8.3.2018	Důvěrné	Důvěrné
Kancelářské stroje s.r.o.	26467658	001611	14.4.2020	Důvěrné	-
KAPPENBERGER + BRAUN, Elektro-Technik spol. s r.o.	16736907	001836	22.7.2016	Důvěrné	Důvěrné
KAPPENBERGER + BRAUN, Elektro-Technik spol. s r.o.	16736907	001837	26.8.2015	Tajné	-
KD Pragma, a.s.	25676644	000850	21.7.2017	Důvěrné	Důvěrné
KELCOM International Liberec, společnost s ručením omezeným	60277301	001909	18.5.2018	Důvěrné	Důvěrné
KLIMAX TEPLICE, s.r.o.	25409174	001765	12.4.2021	Důvěrné	-
KLIRO spol. s.r.o.	27117405	001444	25.8.2019	Důvěrné	-
K-net Technical International Group, s.r.o.	47916745	000955	26.11.2017	Důvěrné	-
KOMFORT, a.s.	25524241	000728	29.10.2015	Důvěrné	Důvěrné
KOMIX s.r.o.	47117087	000404	27.12.2015	Důvěrné	Důvěrné
Komwag, podnik čistoty a údržby města, a.s.	61057606	001947	18.12.2022	Důvěrné	-
KonekTel, a.s.	15051145	000681	17.12.2016	Důvěrné	Důvěrné
KONEX, spol. s r.o.	14799812	001933	2.12.2021	Důvěrné	-
KONSIT a.s.	18630197	001890	9.11.2015	Důvěrné	Důvěrné
Konstruktis Novostav a.s.	26416247	000164	25.4.2015	Důvěrné	Důvěrné
KPMG Advisory, s.r.o.	27570193	001965	27.2.2021	Tajné	-
LABOX spol. s r.o.	49707833	000965	4.12.2017	Důvěrné	Důvěrné
Lamtech CZ s.r.o.	27905161	001958	30.1.2021	Tajné	-
LEC s.r.o.	25132768	001165	3.8.2018	Důvěrné	Důvěrné
Lesní stavby, s.r.o.	64834042	001661	25.7.2020	Důvěrné	-
Lesní stavby, s.r.o.	64834042	001739	20.12.2020	Důvěrné	Důvěrné
Letecké přístroje Praha, s.r.o.	48112062	001410	19.7.2019	Důvěrné	-
LETIŠTĚ BRNO a.s.	26237920	001968	11.11.2019	Důvěrné	Důvěrné
Letiště Praha, a. s.	28244532	000880	20.8.2017	Důvěrné	Důvěrné
Liberecká IS, a.s.	25450131	001820	15.10.2021	Důvěrné	-
LOM PRAHA s.p.	00000515	002008	25.3.2016	Tajné	Tajné
Luděk Šmejkal	63873982	001567	26.1.2020	Důvěrné	-
LUKAM s.r.o.	25246453	001520	23.11.2019	Důvěrné	Důvěrné
LUMEN a.s.	25197452	001364	19.5.2019	Důvěrné	Důvěrné
M - SILNICE a.s.	42196868	001028	12.2.2018	Důvěrné	Důvěrné
M + M servis, s.r.o.	25100734	001860	26.9.2021	Důvěrné	-
MACON a.s.	25062425	001805	6.8.2021	Důvěrné	-
MARCO-CZECH s.r.o.	26706954	001625	8.5.2020	Důvěrné	Důvěrné

MARHOLD a.s.	15050050	000826	27.8.2016	Důvěrné	Důvěrné
MAX MERLIN spol. s r.o.	41188390	001130	19.6.2015	Důvěrné	-
MAXPROGRES, s.r.o.	25307126	001304	9.3.2017	Tajné	Tajné
MC Systems & Services s.r.o.	28252063	001852	7.1.2022	Důvěrné	-
MCnet, s.r.o.	25394720	001849	9.10.2020	Důvěrné	-
MEDTEC-VOP, spol. s r.o.	64791319	000645	5.11.2016	Důvěrné	Důvěrné
MENIER s.r.o.	28957211	001783	11.6.2021	Důvěrné	-
MERCATOR, s.r.o.	47053135	000948	19.11.2017	Důvěrné	-
MERCATOR, s.r.o.	47053135	001046	3.3.2018	Důvěrné	Důvěrné
Mercedes-Benz Česká republika s.r.o.	48024562	001673	23.8.2018	Tajné	-
MERIT GROUP a.s.	64609995	001445	26.8.2019	Důvěrné	Důvěrné
MERO ČR, a.s.	60193468	001952	9.1.2023	-	Důvěrné
MESIT přístroje spol. s r.o.	60709235	002030	8.10.2021	-	Tajné
Mgr. Radek Zapletal	71285610	001633	22.5.2018	Tajné	-
MHM computer a.s.	00539422	000683	13.2.2016	Důvěrné	Důvěrné
MHM computer a.s.	00539422	001940	1.12.2020	Tajné	-
MICROSOFT s.r.o.	47123737	000313	30.8.2015	Důvěrné	Důvěrné
MONET+,a.s.	26217783	000820	25.6.2017	Důvěrné	Důvěrné
MONTSERVIS PRAHA, a.s.	00551899	002047	8.12.2023	-	Důvěrné
MOS CZ, s.r.o.	25347691	001992	18.6.2015	Důvěrné	-
MPI CZ s.r.o.	27562468	000708	3.2.2017	Důvěrné	Důvěrné
MSM Informační systémy,s.r.o.	25115103	001347	22.4.2017	Tajné	-
MÚZO Praha s.r.o.	49622897	001774	8.5.2021	Důvěrné	-
NAM system, a.s.	25862731	001936	13.11.2022	-	Důvěrné
NEFELE, s.r.o.	28969006	001822	11.7.2020	Důvěrné	-
NESS Czech s.r.o.	45786259	001789	20.6.2021	Důvěrné	Důvěrné
NET-SYSTEM s.r.o.	47784164	001808	21.8.2019	Tajné	-
NeXA, s.r.o.	26779234	001148	6.3.2015	Důvěrné	-
NHK s.r.o.	25095005	001757	7.7.2018	Důvěrné	-
NOEL, s.r.o.	48908991	000861	6.8.2017	Důvěrné	-
NSN CS, s.r.o.	63474522	001017	28.1.2016	Tajné	Tajné
O2 Czech Republic a.s.	60193336	002001	20.10.2020	-	Tajné
oaza - net spol. s r.o.	47282711	001911	2.9.2019	Důvěrné	Důvěrné
OHL ŽS, a.s.	46342796	001946	17.12.2022	-	Důvěrné
OKIN GROUP, a.s.	27449734	001653	30.6.2020	Důvěrné	-
OKsystem a.s.	27373665	002054	1.3.2020	Důvěrné	Důvěrné
OM-KOMPLEX spol. s r.o.	49813781	001597	14.7.2017	Důvěrné	Důvěrné
OMNICON s.r.o.	45277133	002035	21.10.2023	-	Důvěrné
OPTOKON, a.s.	13692283	001756	27.1.2017	Důvěrné	Důvěrné
OPTYS, spol. s r.o.	42869048	001920	16.9.2022	-	Důvěrné
Oracle Czech s.r.o.	61498483	002059	8.2.2024	-	Důvěrné
ORITEST spol. s r.o.	45808121	001976	9.4.2023	Důvěrné	-
ORZO SECURITY, spol. s r.o.	60321601	000913	23.9.2017	Důvěrné	Důvěrné
OT Energy Services a.s.	49433431	001982	15.1.2017	Důvěrné	Důvěrné
OVA!!!CLOUD.net a.s.	25857568	001762	27.1.2019	Důvěrné	Důvěrné
oXy Online s.r.o.	27404129	001922	10.11.2017	Důvěrné	-
P.D. ELEKTRO-TEAM s.r.o.	26341573	001105	26.5.2018	Důvěrné	-
P.DUSSMANN spol. s r.o.	45806276	001784	11.9.2020	Důvěrné	-
PAMÁTKY TÁBOR, s.r.o.	44797958	001370	30.5.2019	Důvěrné	Důvěrné

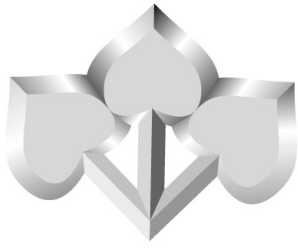
Pavel Perlík - STARGLANS	44292287	000266	16.7.2015	Důvěrné	-
PBR KOMTECH spol.s r.o.	46349758	002052	8.1.2024	-	Důvěrné
PERFECTED s.r.o.	27683028	000856	3.8.2017	Důvěrné	Důvěrné
Peritas servis, s.r.o.	24688738	001745	11.1.2021	Důvěrné	-
Petr Lukschanderl	66538009	001253	12.1.2019	Důvěrné	-
Petr MERREL	71277455	001560	19.1.2020	Důvěrné	-
PHAR SERVICE, a.s.	44851057	000806	10.6.2017	Důvěrné	-
Phonexia s.r.o.	27680258	001918	12.9.2022	Důvěrné	-
PIK s.r.o.	47152150	001394	22.6.2019	Důvěrné	Důvěrné
PilsCom, s.r.o.	25219103	001719	2.11.2020	Důvěrné	-
PKE ČR s.r.o.	63278782	001214	26.11.2016	Tajné	Tajné
Plotové centrum spol. s r.o.	26051851	001766	18.4.2021	Důvěrné	-
PMP Com s.r.o.	25941861	001995	16.12.2019	Důvěrné	-
Poličské strojírny a.s.	46504851	001840	16.8.2016	Důvěrné	Důvěrné
Pontech s.r.o.	27977315	001717	8.2.2020	Důvěrné	-
Pontech s.r.o.	27977315	001718	8.2.2018	Tajné	-
Pontech s.r.o.	27977315	001790	25.6.2019	Tajné	Tajné
Porr a.s.	43005560	002019	10.2.2017	Důvěrné	Důvěrné
Power Tech spol. s r.o.	26196930	000346	12.10.2015	Důvěrné	-
Pramacom Prague spol. s r.o.	18630782	001938	21.11.2020	Tajné	-
PRAMACOM-HT, spol. s r.o.	26514753	001883	3.4.2020	Tajné	-
PrimaTech s.r.o.	48244694	001266	27.1.2017	Tajné	-
Princip a.s.	41690311	001000	12.1.2018	Důvěrné	Důvěrné
PRISIMA, spol. s r.o.	19014597	002000	9.6.2021	Tajné	-
PROBEST COMPANY s.r.o.	27641244	001921	24.9.2022	Důvěrné	-
PROBIN s.r.o.	25143000	001679	18.4.2017	Tajné	Tajné
Prototypa-ZM, s.r.o.	49453653	000885	31.8.2017	Důvěrné	Důvěrné
PRŮMSTAV, a.s.	25105825	001963	1.9.2017	Důvěrné	Důvěrné
První brněnská strojírna Velká Bíteš, a.s.	00176109	000828	30.6.2017	Důvěrné	Důvěrné
První KEY - STAV, a.s.	25385127	002034	7.10.2019	Důvěrné	Důvěrné
PSG-International a.s.	13694341	001401	7.7.2019	Důvěrné	Důvěrné
PSG-International a.s.	13694341	001737	19.12.2018	Tajné	Tajné
PSP PLUS, s.r.o.	25063707	001053	19.3.2018	Důvěrné	-
Puntera s.r.o.	28330501	001555	5.1.2018	Tajné	-
R.D.Engineering s.r.o.	60109581	001282	15.2.2019	Důvěrné	-
RAPOS, spol. s r.o.	25504487	000890	3.9.2017	Důvěrné	Důvěrné
RCD Radiokomunikace spol. s r. o.	48173703	002013	4.6.2018	Důvěrné	Důvěrné
RCD Radiokomunikace spol. s r. o.	48173703	002014	7.1.2020	Tajné	-
REI s.r.o.	48593681	000477	18.4.2016	Důvěrné	-
REISSWOLF likvidace dokumentů a dat, s.r.o.	25097008	001751	2.2.2019	Tajné	-
REKMA, spol. s r.o.	25551337	001109	6.4.2015	Důvěrné	-
REKO a.s.	13690299	001084	28.4.2018	Důvěrné	-
Rekomont, a.s.	00499838	000212	8.6.2015	Důvěrné	-
RELSIE spol. s r.o.	62417339	001146	29.5.2015	Důvěrné	-
RETIA, a.s.	25251929	001893	12.5.2020	-	Tajné
Risk Analysis Consultants, s.r.o.	63672774	000807	10.6.2017	Důvěrné	Důvěrné
ROGER - security, a.s.	25473476	001539	9.12.2019	Důvěrné	-
ROHDE & SCHWARZ - Praha, s.r.o.	62906127	001577	14.2.2020	Důvěrné	-
RTZ Holding, a.s.	25585380	000491	2.5.2016	Důvěrné	-

Řízení letového provozu České republiky, státní podnik (ŘLP ČR, s.p.)	49710371	001059	29.3.2018	Důvěrné	Důvěrné
S com s.r.o.	25668901	001179	5.10.2015	Důvěrné	Důvěrné
S group FACILITY MANAGEMENT, a.s.	25025449	001913	27.8.2017	Důvěrné	Důvěrné
S u b t e r r a a.s.	45309612	001969	23.1.2016	Důvěrné	Důvěrné
S&T CZ s.r.o.	44846029	000848	21.7.2017	Důvěrné	Důvěrné
S&T CZ s.r.o.	44846029	002056	26.1.2022	Tajné	-
S.ICZ a.s.	26482444	001986	14.10.2018	Přísně tajné	-
S.ICZ a.s.	26482444	002028	7.10.2021	-	Tajné
Saab Czech s.r.o.	27184561	002010	3.8.2021	-	Tajné
SAP ČR, spol. s r.o.	49713361	001872	1.11.2019	Důvěrné	Důvěrné
SAPROS, spol. s r.o.	00246557	002024	22.9.2023	Důvěrné	-
SATRA, spol. s r.o.	18584209	001254	9.11.2015	Důvěrné	Důvěrné
SATTURN HOLEŠOV spol. s r.o.	46900250	000722	20.2.2017	Důvěrné	-
SCSA Security s.r.o.	26170400	001604	4.4.2020	Důvěrné	-
Sec-Communication, a.s.	24309443	001935	13.11.2022	-	Důvěrné
SECURITAS ČR s.r.o.	43872026	001827	31.10.2019	Tajné	-
SECURITY TECHNOLOGIES s.r.o.	44015542	000910	21.9.2015	Tajné	-
SECURITY TECHNOLOGIES s.r.o.	44015542	000923	13.10.2017	Důvěrné	Důvěrné
SEFIRA spol. s r.o.	62907760	001711	17.10.2018	Tajné	-
Sellier & Bellot a.s.	28982347	001916	15.9.2019	Důvěrné	Důvěrné
SEOS CZ s.r.o.	49704478	001595	9.4.2016	Důvěrné	Důvěrné
SETERM CB a.s.	26031949	001638	31.10.2016	Důvěrné	-
SEVENOAKS, s.r.o.	27138925	001942	25.7.2020	Tajné	-
SCHLIKE - DOMI, spol. s r.o.	44569564	001521	23.11.2017	Tajné	-
Schrack Technik spol. s r.o.	15039137	001730	1.12.2020	Důvěrné	-
Siemens, s.r.o.	00268577	001300	16.12.2016	Tajné	Tajné
SIEZA, s.r.o.	44795131	002004	1.7.2021	-	Tajné
SILBA-Elstav s.r.o.	64358844	001903	26.1.2019	Důvěrné	Důvěrné
SILICON GRAPHICS, s.r.o.	60723530	000236	20.6.2015	Důvěrné	-
Simac Technik ČR, a.s.	63079496	000682	17.12.2016	Důvěrné	Důvěrné
SIMACEK FACILITY CZ, spol. s r.o.	15549470	001710	17.10.2020	Důvěrné	-
SINIT, a.s.	25397401	001078	20.4.2018	Důvěrné	Důvěrné
SITEL, spol. s r.o.	44797320	001439	22.8.2019	Důvěrné	Důvěrné
SITEL, spol. s r.o.	44797320	001440	22.8.2017	Tajné	-
Skanska a.s.	26271303	001262	23.4.2017	Důvěrné	Důvěrné
Skanska a.s.	26271303	001561	20.1.2018	Tajné	-
Skanska Facility s.r.o.	25661531	001797	6.11.2018	Tajné	-
SKILL s.r.o.	48039039	000784	5.2.2016	Důvěrné	Důvěrné
SKILL s.r.o.	48039039	002017	26.8.2021	Tajné	-
SKR stav, s.r.o.	26961474	002029	7.10.2023	-	Důvěrné
SKS s.r.o.	43420117	001864	17.3.2017	Tajné	Tajné
SODATSW spol. s r.o.	25323989	002012	13.7.2017	Důvěrné	-
SOITRON s.r.o.	27270599	001870	27.2.2022	Důvěrné	-
solit project, s.r.o.	25146131	001252	7.1.2019	Důvěrné	-
Special Service International, spol. s r.o.	26116570	001948	18.12.2022	Důvěrné	-
SPEL, a.s.	00473057	002025	23.9.2023	-	Důvěrné
SPL servis.cz s.r.o.	28894430	001331	6.4.2019	Důvěrné	-
Sprinx Systems, a.s.	26770211	001276	28.1.2019	Důvěrné	-

STAEG Facility, spol. s r.o.	24141623	001960	9.2.2023	-	Důvěrné
STAEG Stavby, spol. s r.o.	24140520	002044	15.5.2022	-	Důvěrné
STAEG, spol. s r.o.	25520059	001703	3.12.2016	Důvěrné	Důvěrné
STAFI FINALIZACE STAVEB s.r.o.	25968203	001562	23.1.2020	Důvěrné	Důvěrné
STÁTNÍ TISKÁRNA CENIN, státní podnik	00001279	001023	9.2.2016	Tajné	Tajné
STAVEBNÍ OBNOVA ŽELEZNIC a.s.	63078953	000295	10.8.2015	Důvěrné	-
STAVITELSTVÍ ŘEHOŘ, s.r.o.	25075543	000842	14.7.2017	Důvěrné	Důvěrné
STAVOS Brno, a.s.	65277911	001460	14.9.2019	Důvěrné	Důvěrné
STIS stavební a inženýrská společnost, s.r.o.	62582933	001384	10.6.2019	Důvěrné	-
STRABAG Property and Facility Services a.s.	26157799	001828	31.10.2019	Tajné	-
STREICHER, spol. s r.o. Plzeň	14706768	001743	13.5.2018	Důvěrné	Důvěrné
SUDOP PRAHA a.s.	25793349	001529	9.5.2016	Důvěrné	Důvěrné
SUDOP Project Plzeň a.s.	45359148	001887	9.4.2022	Důvěrné	Důvěrné
SUPTel a.s.	25229397	001627	2.8.2016	Důvěrné	Důvěrné
Svoboda a syn, s.r.o.	25548531	001928	17.10.2020	-	Tajné
SVOS, spol. s r.o.	48152056	001953	6.6.2020	Důvěrné	-
SWIETELSKY stavební s.r.o.	48035599	001010	29.3.2016	Důvěrné	Důvěrné
SYNER Morava, a.s.	63493675	002060	18.2.2024	-	Důvěrné
SYSCOM SOFTWARE spol. s r.o.	61498084	002036	28.10.2023	-	Důvěrné
ŠUMAVAPLAN, spol. s r. o.	49787454	000288	1.8.2015	Důvěrné	-
Technický a zkušební ústav stavební Praha, s.p.	00015679	002037	6.11.2023	-	Důvěrné
TECHNICOM, s.r.o.	49101358	001153	14.7.2018	Důvěrné	Důvěrné
TECHNICOM, s.r.o.	49101358	001154	14.7.2016	Tajné	-
TECHNISERV IT, spol. s r.o.	26298953	001330	6.4.2019	Důvěrné	Důvěrné
TECHNISERV, spol. s r.o.	44264020	002011	6.8.2021	-	Tajné
TELE DATA CONTROL, spol. s r.o.	44264682	001405	18.7.2019	Důvěrné	-
TELE DATA SYSTEM, spol. s r.o.	18051286	000050	6.3.2015	Důvěrné	-
TELECOM 21 CB s.r.o.	25160681	001649	23.6.2020	Důvěrné	Důvěrné
TELECOM ALARM, spol. s r.o.	44268351	001380	9.6.2019	Důvěrné	Důvěrné
TELECOM ALARM, spol. s r.o.	44268351	001381	9.6.2017	Tajné	-
TELEPROG s.r.o.	60721197	001086	29.4.2018	Důvěrné	-
TELESPOJ, s.r.o.	48202983	001923	11.10.2016	Důvěrné	Důvěrné
TELMO a.s.	47307781	002031	2.7.2016	Důvěrné	Důvěrné
TERMOMONT s.r.o.	45538875	001704	14.10.2017	Důvěrné	Důvěrné
TESCO SW a.s.	25892533	001915	7.3.2019	Důvěrné	Důvěrné
TESLA, akciová společnost	00009709	000416	22.1.2016	Důvěrné	Důvěrné
TESLA, akciová společnost	00009709	002058	3.2.2022	Tajné	-
TEZAO s.r.o.	45313067	000533	24.6.2016	Důvěrné	Důvěrné
TIPA Telekom plus a.s.	27746631	000835	2.7.2017	Důvěrné	Důvěrné
T-Mobile Czech Republic a.s.	64949681	001978	31.8.2019	Důvěrné	Důvěrné
TOVEK, spol. s r.o.	49687981	000422	25.1.2016	Důvěrné	-
Tractebel Engineering a.s.	15049451	001128	20.1.2017	Důvěrné	Důvěrné
Trade FIDES, a.s.	61974731	001348	27.4.2017	Tajné	Tajné
TransTech Electronic, s.r.o.	61065391	001034	14.5.2016	Důvěrné	-
TRIGON PLUS spol. s r.o.	46350110	000946	11.11.2017	Důvěrné	Důvěrné
TRIMR s.r.o.	14616238	001871	26.5.2020	Důvěrné	Důvěrné
Triocom s.r.o.	27577996	000771	29.4.2017	Důvěrné	Důvěrné
Trusted Network Solutions,a.s.	26239701	001771	2.5.2021	Důvěrné	-
T-SOFT a.s.	40766314	001117	20.2.2016	Důvěrné	Důvěrné

TTC TELEKOMUNIKACE, s.r.o.	41194403	001877	12.3.2020	-	Tajné
UJP Praha a.s.	60193247	000674	6.12.2016	Důvěrné	Důvěrné
ÚJV Řež, a. s.	46356088	001924	29.9.2020	-	Tajné
UNIS, a.s.	00532304	001973	18.1.2020	Důvěrné	Důvěrné
UNIS, a.s.	00532304	001974	14.11.2017	Tajné	-
UNISMINI - služby, spol.s r.o.	62418742	001803	31.7.2019	Tajné	-
URC Systems, spol. s r.o.	25547526	001825	28.11.2015	Důvěrné	Důvěrné
URC Systems, spol. s r.o.	25547526	001826	27.6.2019	Tajné	-
ÚVT, s.r.o.	25701118	002038	26.10.2019	Důvěrné	-
VAE CONTROLS, s.r.o.	48390470	000788	20.5.2017	Důvěrné	Důvěrné
VARIEL, a. s.	45148287	001278	18.3.2016	Důvěrné	Důvěrné
VATACK s.r.o.	25996851	001613	18.4.2020	Důvěrné	-
VCES a.s.	26746573	001043	1.3.2016	Tajné	Tajné
Vegacom a.s.	25788680	001216	12.10.2017	Důvěrné	Důvěrné
Vegacom a.s.	25788680	001217	12.10.2015	Tajné	-
Versa Systems s.r.o.	25891863	001879	14.3.2020	Tajné	-
VIAVIS a.s.	25848402	001721	3.11.2019	Důvěrné	-
VÍTKOVICE IT SOLUTIONS a.s.	28606582	001648	23.6.2020	Důvěrné	Důvěrné
VKUS-BUSTAN s.r.o.	26841410	000248	28.6.2015	Důvěrné	Důvěrné
Vodafone Czech Republic a.s.	25788001	002051	3.3.2020	Důvěrné	Důvěrné
Vodohospodářské stavby, společnost s ručením omezeným	40233308	000888	1.9.2017	Důvěrné	Důvěrné
Vojenské lesy a statky ČR, s.p.	00000205	002026	4.4.2016	Důvěrné	Důvěrné
Vojenský technický ústav, s.p.	24272523	001848	18.12.2019	-	Tajné
Vojenský výzkumný ústav, s. p.	29372259	001847	18.12.2019	-	Tajné
VOP CZ, s.p.	00000493	001769	29.10.2015	Důvěrné	Důvěrné
VOP CZ, s.p.	00000493	001770	5.1.2017	Tajné	Tajné
VPÚ DECO PRAHA a.s.	60193280	001980	27.4.2021	-	Tajné
VR Group, a.s.	25699091	001778	1.11.2016	Důvěrné	-
VR Group, a.s.	25699091	001779	4.8.2018	Tajné	-
VUMS LEGEND, spol. s r.o.	61855057	002042	19.11.2023	Důvěrné	-
VYDIS a.s.	24660345	001738	10.11.2020	Důvěrné	Důvěrné
VYDOS BOHEMIA ,s.r.o.	64581381	001379	9.6.2019	Důvěrné	-
WAK System, spol. s r.o.	25720384	000874	18.8.2015	Tajné	-
WAKKENHAT ZETTA s.r.o., koncern	27123197	001804	11.2.2017	Důvěrné	-
WEBER v.o.s.	25030540	001622	4.5.2020	Důvěrné	-
Weinhold Legal, v.o.s. advokátní kancelář	25628470	001977	26.2.2015	Důvěrné	-
XEROX CZECH REPUBLIC s.r.o.	48109193	000507	31.5.2016	Důvěrné	-
YOUR SYSTEM, spol.s r.o.	00174939	001664	27.7.2018	Tajné	-
Z.L.D. s.r.o.	25631365	001861	21.1.2020	Tajné	-
Z.L.D. s.r.o.	25631365	002053	11.1.2024	-	Důvěrné
Zdeněk Novák	11618248	001163	28.7.2018	Důvěrné	-
Zdeněk Pešička	67176712	001320	28.3.2017	Tajné	-
ZENOVA services s.r.o.	25051865	001312	16.3.2019	Důvěrné	-
Zeppelin CZ s.r.o.	18627226	002002	11.12.2021	Důvěrné	Důvěrné
ZEVA cz s.r.o.	26796678	001763	9.4.2021	Důvěrné	-
ZEVETA AMMUNITION a.s.	26950065	002043	29.1.2023	Důvěrné	-
ZVI a.s.	47673621	000851	23.7.2015	Tajné	-
ZVI a.s.	47673621	001135	29.6.2018	Důvěrné	Důvěrné
ZVVZ-Enven Engineering, a.s.	25696882	001862	21.1.2020	-	Tajné

OPRAVNÉ PROSTŘEDKY



1. Rozklad

Proti rozhodnutí Úřadu vydanému v bezpečnostním řízení má účastník řízení právo podat **rozklad**, pokud se tohoto práva po doručení rozhodnutí písemně nevzdal nebo pokud zákon č. 412/2005 Sb. nestanoví jinak (§ 125 zákona č. 412/2005 Sb.).

Rozklad lze podat proti těmto rozhodnutím Úřadu:

1. rozhodnutí Úřadu o **nevydání** osvědčení fyzické osoby, osvědčení podnikatele, dokladu o bezpečnostní způsobilosti (§ 121 odst. 2 zákona č. 412/2005 Sb.),
2. rozhodnutí Úřadu o **zrušení platnosti** osvědčení fyzické osoby, osvědčení podnikatele, dokladu o bezpečnostní způsobilosti (§ 121 odst. 3 zákona č. 412/2005 Sb.) – podání rozkladu nemá v tomto případě odkladný účinek,
3. rozhodnutí Úřadu o **zastavení řízení** (§ 113 odst. 1 písm. c), d) a h) zákona č. 412/2005 Sb.),
4. rozhodnutí Úřadu o **rozkladu** (§ 128 a 129 zákona č. 412/2005 Sb.),
5. **opravné rozhodnutí** Úřadu (§ 122 odst. 6 zákona č. 412/2005 Sb.).

Způsob a forma podání rozkladu

Rozklad se podává u Úřadu **do 15 dnů** ode dne doručení rozhodnutí (§ 126 odst. 1 zákona č. 412/2005 Sb.).

V listinné podobě lze podat rozklad osobně nebo prostřednictvím jiné, k tomu účelu pověřené, osoby v podatelně místa sídla Úřadu (Na Popelce 2/16, Praha 5 - Košíře), v úředních hodinách.

Úřední hodiny podatelny	
Pondělí a středa:	8:00 – 17:00
Úterý a čtvrtek:	8:00 – 15:00
Pátek:	8:00 – 12:00

Rozklad lze také zaslat prostřednictvím držitele poštovní licence nebo zvláštní poštovní licence na adresu Úřadu (P.O.BOX 49, Praha 56, PSČ 150 06).

V elektronické podobě lze podat rozklad dodáním do **datové schránky Úřadu** (ID Úřadu – h93aayw, do pole „Věc“ se uvede „Bezpečnostní řízení – Rozklad“) nebo na **elektronickou podatelnu Úřadu** (posta@nbu.cz, do pole „Předmět“ se uvede „Bezpečnostní řízení – Rozklad“).

Pokud účastník řízení lhůtu k podání rozkladu zmešká ze závažných důvodů, může požádat Úřad o její prominutí, a to do 15 dnů ode dne, kdy příčina zmeškání pominula. Podmínkou však je, aby spolu s žádostí o prominutí lhůty byl podán i samotný rozklad.

Náležitosti rozkladu (§ 127 zákona č. 412/2005 Sb.):

1. **identifikace** účastníka řízení – jméno, příjmení a rodné číslo u fyzických osob; název a identifikační číslo u právnických osob,
2. **adresa** trvalého pobytu u fyzických osob, adresa sídla u právnických osob; případně adresa pro doručování,
3. **datum a podpis** fyzické osoby; u podnikatele podpis osoby či osob oprávněných jednat jménem právnické osoby,
4. **označení rozhodnutí,** proti němuž je rozklad podáván (tj. číslo jednací a datum jeho vydání),
5. **čeho se účastník řízení domáhá** (tj. např. zrušení rozhodnutí Úřadu o zrušení platnosti osvědčení fyzické osoby nebo osvědčení podnikatele nebo dokladu o bezpečnostní způsobilosti, zrušení rozhodnutí Úřadu o nevydání osvědčení fyzické osoby nebo podnikatele nebo dokladu o bezpečnostní způsobilosti, zrušení rozhodnutí o zastavení bezpečnostního řízení, apod.),
6. **důvody**, pro něž je napadené rozhodnutí nesprávné, případně v čem účastník řízení spatřuje rozpor

s právními předpisy (tj. účastník řízení konkrétně popíše, z jakých důvodů s napadeným rozhodnutím nesouhlasí). Rozklad lze podat proti výroku rozhodnutí, nikoliv proti jeho odůvodnění.

Upozornění:

Pokud rozklad nemá předepsané náležitosti, je účastník řízení písemně vyzván k odstranění nedostatků a řízení je přerušeno (§ 112 odst. 1 písm. b) zákona č. 412/2005 Sb.).

Jestliže účastník řízení nedostatky ve stanovené lhůtě neodstraní, řízení o rozkladu se rozhodnutím zastaví (§ 113 odst. 1 písm. c) zákona č. 412/2005 Sb. – proti tomuto rozhodnutí může účastník řízení podat rozklad).

Kdykoliv v průběhu řízení o rozkladu může účastník řízení vzít podaný rozklad zpět. Tento úkon lze provést pouze písemně. V tomto případě se řízení o rozkladu rozhodnutím zastaví (§ 113 odst. 1 písm. a) zákona č. 412/2005 Sb.), proti tomuto rozhodnutí nelze podat rozklad.

Postup při rozhodování o rozkladu

Podaným rozkladem se nejprve zabývá Úřad, tj. ten organizační celek Úřadu, který napadené rozhodnutí vydal. Úřad postupuje následujícím způsobem:

1. pokud je rozklad podle zákona č. 412/2005 Sb. nepřípustný nebo byl podán po uplynutí lhůty, nebylo-li její zmeškání Úřadem prominuto (viz výše), Úřad jej **zamítne** rozhodnutím, proti němuž lze dále podat rozklad (§ 128 zákona č. 412/2005 Sb.),
2. shledá-li pro to důvody, **vyhoví** Úřad rozkladu v plném rozsahu a **napadené rozhodnutí zruší** (tzv. autoremedura); proti takovému rozhodnutí lze opět podat rozklad (§ 129 odst. 1 a 2 zákona č. 412/2005 Sb.),
3. pokud Úřad nerozhodne ani jedním z výše uvedených způsobů, **předloží** rozklad spolu se svým stanoviskem a veškerým spisovým materiálem do 15 dnů od doručení řediteli Úřadu (§ 129 odst. 3 zákona č. 412/2005 Sb.),
4. pokud jsou dány důvody podle § 113 zákona č. 412/2005 Sb. (účastník řízení vzal žádost o rozklad zpět, účastník řízení neodstranil nedostatky v rozkladu), Úřad řízení o rozkladu **zastaví**.

Ředitel Úřadu rozhoduje o rozkladu na základě návrhu rozkladové komise (§ 130 zákona č. 412/2005 Sb.) a to ve lhůtě **3 měsíců** ode dne jeho doručení (§ 131 odst. 6 zákona č. 412/2005 Sb.). Ředitel Úřadu rozhodne jedním z následujících způsobů:

1. jsou-li dány důvody podle § 113 zákona č. 412/2005 Sb. (např. účastník řízení vzal rozklad zpět), **řízení o rozkladu zastaví a napadené rozhodnutí potvrdí** (§ 131 odst. 1 zákona č. 412/2005 Sb.); v případě, že účastník řízení zemře, byl prohlášen za mrtvého, byl zrušen nebo zanikl (§ 113 odst. 1 písm. i) zákona č. 412/2005 Sb.), **řízení o rozkladu zastaví a napadené rozhodnutí zruší, neboť se stalo zastavením řízení bezpředmětným** (§ 131 odst. 1 zákona č. 412/2005 Sb.),
2. shledá-li pro to důvody, rozkladu proti rozhodnutí o zrušení platnosti osvědčení fyzické osoby, osvědčení podnikatele, dokladu o bezpečnostní způsobilosti **vyhoví a napadené rozhodnutí zruší** (§ 131 odst. 2 zákona č. 412/2005 Sb.); spolu s rozhodnutím o rozkladu se účastníku řízení zasílá zpět osvědčení fyzické osoby, osvědčení podnikatele, doklad o bezpečnostní způsobilosti, jehož platnost se obnovuje dnem právní moci rozhodnutí o rozkladu (tj. dnem doručení) - § 132 zákona č. 412/2005 Sb.; řízení o zrušení platnosti osvědčení fyzické osoby, osvědčení podnikatele, dokladu o bezpečnostní způsobilosti podle § 101 zákona č. 412/2005 Sb. pokračuje,
3. shledá-li pro to důvody, rozkladu proti rozhodnutí o nevydání osvědčení fyzické osoby, osvědčení podnikatele, dokladu o bezpečnostní způsobilosti **vyhoví a napadené rozhodnutí zruší;** dnem doručení rozhodnutí o rozkladu účastníku řízení je Úřadem zahájeno bezpečnostní řízení (§ 93 odst. 1 písm. d) zákona č. 412/2005 Sb.), toto bezpečnostní řízení Úřad ukončí ve lhůtě stanovené pro daný typ bezpečnostního řízení v § 117 zákona č. 412/2005 Sb.,
4. shledá-li pro to důvody, rozkladu proti rozhodnutí o zastavení bezpečnostního řízení **vyhoví a napadené rozhodnutí zruší;** dnem doručení rozhodnutí o rozkladu účastníku řízení Úřad pokračuje

v bezpečnostním řízení, které ukončí ve lhůtě stanovené pro daný typ bezpečnostního řízení v § 117 zákona č. 412/2005 Sb.,

5. v případě, že neshledá důvody k zastavení řízení o rozkladu či zrušení napadeného rozhodnutí, **rozklad zamítne a napadené rozhodnutí potvrdí** (§ 131 odst. 4 zákona č. 412/2005 Sb.).

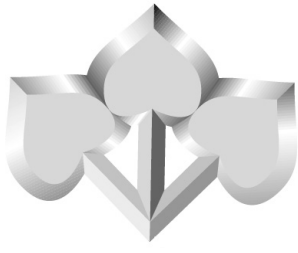
Důvody pro **vyhovění rozkladu, zrušení napadeného rozhodnutí a vrácení věci Úřadu k novému projednání a rozhodnutí** tak, jak je uvedeno v bodech 2 až 4, je shledání, že výrok napadeného rozhodnutí byl vydán v rozporu s právními předpisy, nebo je jinak nesprávný, nebo zjištění, že po vydání napadeného rozhodnutí nastaly skutečnosti, které mají vliv na rozhodnutí (§ 131 odst. 3 zákona č. 412/2005 Sb.).

2. Žaloba

Proti rozhodnutí ředitele Úřadu o rozkladu lze podat **žalobu** podle zákona **č. 150/2002 Sb.**, soudního řádu správního. Proti rozhodnutí ředitele Úřadu o zastavení řízení lze podat žalobu pouze v případě, kdy je podle § 113 odst. 5 zákona č. 412/2005 Sb. proti důvodu zastavení řízení přípustný rozklad (tj. § 113 odst. 1 písm. c), d) a h) zákona č. 412/2005 Sb.).

Žaloba se podává ve lhůtě **30 dnů** ode dne doručení napadeného rozhodnutí, a to příslušnému krajskému soudu rozhodujícího ve správním soudnictví – tj. **Městskému soudu v Praze** (§ 133 odst. 1 zákona č. 412/2005 Sb.).

BEZPEČNOST INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ



Úvod do problematiky informačních a komunikačních technologií v zákoně č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

verze 2.1.1, únor 2014

Obsah

Část I
Bezpečnost informačních systémů

1.1 Vývoj legislativy

Od roku prvého vydání byl zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti několikrát novelizován, avšak až do roku 2011 se novelizace nedotkla paragrafů zabývajících se bezpečností informačních a komunikačních technologií.

Poslední novela, realizovaná zákonem č. 255/2011 Sb., kterým se mění zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, a zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů (dále jen „zákon č. 255/2011 Sb.), se již bezpečnosti informačních a komunikačních systémů a kryptografické ochrany dotýká. Zákon č. 255/2011 Sb. je v platnosti od 1. ledna 2012.

V dalším textu budeme z praktických důvodů pracovat s úplným zněním zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, platným od 1. 1. 2012 (dále jen „zákon č. 412/2005 Sb.“), přičemž budou zvýrazněny nejdůležitější změny zavedené zákonem č. 255/2011 Sb.

Od 1. ledna 2012 je v platnosti také novela vyhlášky č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. Tato novela je realizována vyhláškou č. 453/2011 Sb., ze dne 21. prosince 2011, kterou se mění vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor. Aktuálně platné znění vyhlášky č. 523/2005 Sb. je tedy označováno jako vyhláška č. 523/2005 Sb. ve znění vyhlášky č. 453/2011 Sb. (dále jen „vyhláška č. 523/2005 Sb.“).

Dnem 1. ledna 2012 vstoupila v platnost nová vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, která nahrazuje vyhlášku č. 524/2005 Sb., a vyhláška č. 434/2011 Sb., kterou se mění vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany. V roce 2013 byla vyhláška č. 432/2011 Sb. novelizována vyhláškou č. 417/2013 Sb., s účinností od 1. ledna 2014.

Problematika kryptografické ochrany je pojednána v samostatné části Věstníku.

1.2 Zákon č. 412/2005 Sb. a oblast informačních a komunikačních technologií

Zákon č. 412/2005 Sb. (2012) obsahuje nyní 22 paragrafů upravujících oblast informačních a komunikačních technologií (ICT), když se zabývá

- bezpečností informačních systémů (§ 34, § 35a)
- bezpečností komunikačních systémů (§ 35),
- bezpečností některých elektronických zařízení provozovaných mimo informační nebo komunikační systémy (§ 36),
- kompromitujícím vyzařováním (§ 45),
- kryptografickou ochranou utajovaných informací (§ 37, § 37a, § 38 až 43, § 43a, § 44)
- certifikací informačních systémů, kryptografických prostředků, kryptografických pracovišť a stínicích komor (§ 46, § 48, § 49, § 50, § 51, § 53)
- možností spolupráce Úřadu s orgánem státu nebo podnikatelem při zajišťování některých činností ve výše uvedených oblastech (§ 52)

V zákoně č. 412/2005 Sb. je dále několik paragrafů, které upravují oblast informačních a komunikačních technologií v některých svých odstavcích nebo písmenech a kterým je třeba věnovat náležitou pozornost.

Jedná se

- v § 67 o povinnosti odpovědné osoby stanovené v odst. 1 písm. d), e),
- v § 69 o povinnosti právnické nebo podnikající fyzické osoby, které mají přístup k utajované informaci, a orgánu státu, stanovené v odst.1 písm. e), f), g), h), i), j),

- v § 148 o přestupky fyzické osoby týkající se kryptografické ochrany, specifikované v odst. 1 písm. f) a g), případně i v písm. h), i) a j), a pokuty, které mohou být za ně uloženy,
- v § 149 o přestupky fyzické osoby týkající se informačních a komunikačních systémů a dalších elektronických zařízení, specifikované v odst. 1 písm. g), h) a i), případně i v písm. j) a k), a pokuty, které mohou být za ně uloženy,
- v § 153 o správní delikty, kterých by se dopustila právnická nebo podnikající fyzické osoba mající přístup k utajované informaci, obsažené v odst. 1 písm. b), s), t), u) a v), případně i v písm. w) až z), a pokuty, které mohou být za ně uloženy.

Nadále se nebudeme zabývat problematikou kryptografické ochrany a soustředíme se na

- bezpečnost informačních systémů a jejich certifikaci,
- bezpečnost komunikačních systémů a schvalování jejich projektů bezpečnosti,
- zabezpečení některých elektronických zařízení a jejich bezpečnostní směrnice,
- kompromitující vyzařování, certifikaci stínících komor.

Pokusíme se pro každou z uvedených oblastí shrnout, co je pro ni závazné podle zákona č. 412/2005 Sb. a podle vyhlášky č. 523/2005 Sb. Tučně budou vyznačeny změny platné v zákoně č. 412/2005 Sb. a ve vyhlášce č. 523/2005 Sb. od 1. 1. 2012.

1.3 Bezpečnost informačních systémů

1.3.1 Zákon č. 412/2005 Sb. a bezpečnost informačních systémů

V zákoně č. 412/2005 Sb. se nejprve v § 5 specifikuje bezpečnost informačního systému jako systém opatření a současně jsou uvedeny nejdůležitější cíle bezpečnosti informačního systému, kterými jsou zajištění důvěrnosti, integrity a dostupnosti utajovaných informací, s nimiž informační systém nakládá, a odpovědnosti správy a uživatele systému za jejich činnost v informačním systému.

V § 34 je pak uvedena definice informačního systému pro účely zákona č. 412/2005 Sb. Definice byla navržena podle definice reálného otevřeného systému v OSI referenčním modelu (EN ISO/IEC 7498), v legislativním procesu byla poněkud změněna, nicméně k posunu ve významu tím nedošlo.

Podle této definice se informačním systémem nakládajícím s utajovanými informacemi 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.

V § 34 se také stanovuje povinnost používat pro nakládání s utajovanými informacemi pouze informační systémy certifikované Úřadem, a to pro všechny stupně utajení utajovaných informací. Kromě toho musí být certifikovaný informační systém před uvedením do provozu schválen do provozu odpovědnou osobou, nebo osobou jí pověřenou.

Schválení informačního systému do provozu musí pak být písemně oznámeno do 30 dnů Úřadu.

Veškeré další požadavky na informační systém nakládající s utajovanými informacemi a obsah bezpečnostní dokumentace informačního systému jsou specifikovány ve vyhlášce č. 523/2005 Sb.

1.3.2 Vyhláška č. 523/2005 Sb. a bezpečnost informačních systémů (požadavky)

Přeneseme se nyní do vyhlášky č. 523/2005 Sb. V § 2 lze nalézt definice odborných pojmů, používaných v této vyhlášce. Z důvodu dosažení kompatibility s novými pravidly Rady (ROZHODNUTÍ RADY o bezpečnostních pravidlech na ochranu utajovaných informací EU, ze dne 31. 3. 2011, 6952/2/11, dále jen „Bezpečnostní pravidla Rady“) **jsou zavedeny dva nové pojmy, a to „pravost“ a „nepopiratelnost“.** Definice jsou přejaty z oficiálního překladu Bezpečnostních pravidel Rady. Pravostí informací se rozumí záruka, že informace jsou autentické a z důvěryhodných zdrojů. Nepopiratelností se rozumí schopnost prokázat zpětně jednání či událost tak, aby dané jednání či událost nemohly být následně popřeny.

Vzhledem k důležitosti prvého odstavce § 3 si připomeňme znění tohoto odstavce, který specifikuje soubor opatření k dosažení bezpečnosti informačního systému.

Bezpečnosti informačního systému se dosahuje uplatněním souboru opatření z oblasti:

- počítačové a komunikační bezpečnosti,

- kryptografické ochrany,
- ochrany proti úniku kompromitujícího vyzařování,
- administrativní bezpečnosti a organizačních opatření,
- personální bezpečnosti a
- fyzické bezpečnosti informačního systému.

Důležitý je také § 4, specifikující požadovanou bezpečnostní dokumentaci informačního systému. Vyžadována je projektová bezpečnostní dokumentace a provozní bezpečnostní dokumentace.

Projektová bezpečnostní dokumentace informačního systému obsahuje
- bezpečnostní politiku informačního systému a výsledky analýzy rizik,
- návrh bezpečnosti informačního systému zajišťující splnění bezpečnostní politiky informačního systému, přičemž podrobnost jeho popisu musí umožnit přímou realizaci navrhovaných opatření a
- dokumentaci k testům bezpečnosti informačního systému,

Provozní bezpečnostní dokumentace informačního systému obsahuje
- bezpečnostní směrnice informačního systému pro činnost bezpečnostních správců informačního systému v jednotlivých rolích zavedených v informačním systému pro zajištění bezpečnostní správy informačního systému,
- bezpečnostní směrnice informačního systému pro činnost správců informačního systému v jednotlivých rolích zavedených v informačním systému pro správu informačního systému, pokud se týká zajištění bezpečnosti informačního systému
- bezpečnostní směrnice informačního systému pro činnost uživatelů informačního systému, pokud se týká zajištění bezpečnosti informačního systému.

V § 5 je stanovena povinnost zpracovat jako první dokument bezpečnostní dokumentace bezpečnostní politiku informačního systému, v níž jsou stanoveny zásady a postupy pro zajištění důvěrnosti, integrity a dostupnosti utajovaných informací v informačním systému, odpovědnosti uživatelů, správců a bezpečnostních správců za jejich činnost v informačním systému, a **dále pravosti informací a nepopiratelnosti, pokud to charakter informačního systému vyžaduje**. Zásady uvedené v bezpečnostní politice musí být rozpracovány v návrhu bezpečnosti informačního systému a v jeho provozní bezpečnostní dokumentaci.

V § 6 jsou uvedeny tři základní oblasti, z nichž se dá čerpat při formulaci bezpečnostní politiky. Jedná se o
- minimální bezpečnostní požadavky v oblasti počítačové bezpečnosti, které jsou obecného charakteru (blíže v § 7),
- požadavky specifické pro konkrétní informační systém, vyplývající ze zvoleného bezpečnostního provozního módu, uživatelských požadavků na funkci systému a z analýzy rizik (§ 8 až 11),
- požadavky vyplývající z nadřízené bezpečnostní politiky.

V § 7 jsou stanoveny minimální bezpečnostní požadavky v oblasti počítačové bezpečnosti k zajištění základní úrovně důvěrnosti, integrity a dostupnosti utajovaných informací a odpovědnosti osob působících v informačním systému a to pomocí jednoznačné identifikace a autentizace každé z těchto osob (odst. 1 písm. a), řízení jejich přístupu k informacím na základě jejich přístupových práv (odst. 1 písm. b), zaznamenávání a uchovávání údajů o jejich činnosti v informačním systému (odst. 1 písm. c, písm. d), ochrany důvěrnosti informací při jejich ukládání i přenosu komunikačním prostředím (odst. 1 písm. e, písm. f).

Důležitý § 8 obsahuje popis přípustných bezpečnostních provozních módů. Podle odst. 1 mohou být informační systémy nakládající s utajovanými informacemi provozovány v jednom z následujících bezpečnostních provozních módů (základní definice bezpečnostního provozního módu je definována v pojmech jak v zákoně tak ve vyhlášce). Výčet bezpečnostních provozních módů je následující:
- bezpečnostní provozní mód vyhrazený,
- bezpečnostní provozní mód s nejvyšší úrovní,
- **bezpečnostní provozní mód s formálním řízením přístupu k informacím,**
- bezpečnostní provozní mód víceúrovňový.

Přidání čtvrtého bezpečnostního provozního módu se odvozuje z textu Bezpečnostních pravidel Rady.

Pro každý z uvedených bezpečnostních provozních módů je v § 8 uvedena jeho definice a požadavky, které musí být při jeho realizaci splněny.

Uvedeme pouze specifikaci pro bezpečnostní provozní mód s nejvyšší úrovní s formálním řízením přístupu. Jeho název, v anglickém originálu „compartmented“, byl přejat z oficiálního překladu Bezpečnostních pravidel Rady.

Bezpečnostní provozní mód s nejvyšší úrovní s formálním řízením přístupu k informacím je takové prostředí, které odpovídá bezpečnostnímu provoznímu módu s nejvyšší úrovní, kde však formální řízení přístupu navíc předpokládá formální centrální správu kontroly přístupu.

Bezpečnostní provozní mód vyhrazený a bezpečnostní provozní mód s nejvyšší úrovní (a tedy i s formálním řízení přístupu k informacím) představují takové prostředí, které umožňuje současné zpracování utajovaných informací různého stupně utajení, přičemž všichni uživatelé musí splňovat podmínky pro přístup k utajovaným informacím nejvyššího stupně utajení, které jsou v informačním systému obsaženy. 0patření z oblasti administrativní a personální bezpečnosti a fyzické bezpečnosti informačních systémů a opatření k zajištění důvěrnosti dat během přenosu musí odpovídat úrovni požadované pro nejvyšší stupeň utajení utajovaných informací, se kterými informační systém nakládá. Všechny informace jsou v těchto bezpečnostních provozních módech chráněny jako by měly nejvyšší stupeň utajení, se kterým systém nakládá. Uvedené bezpečnostní provozní módy nevyžadují spojení informace s údajem o jejím skutečném stupni utajení. Pokud informace vystupuje z informačního systému a není spolehlivě označena stupněm utajení nebo její stupeň utajení není před výstupem posouzen uživatelem, je rovněž považována za klasifikovanou tímto nejvyšším stupněm utajení.

V současných systémech se zejména pro distribuci souborů s utajovanými informacemi jako přílohy k elektronické poště zavádějí obálky, v nichž je stupeň utajení uveden. Tím se však informační systém nedostává na úroveň systému víceúrovňového, protože stále platí, že všichni uživatelé musí být prověřeni pro přístup k utajovaným informacím nejvyššího stupně utajení, se kterými se v informačním systému nakládá.

Odlišnost bezpečnostního provozního módu vyhrazeného od bezpečnostního provozního módu s nejvyšší úrovní nebo s formálním řízením přístupu k informacím spočívá ve způsobu uplatnění zásady „need-to- know“.

Bezpečnostní provozní mód vyhrazený je určen pro informační systém, v němž jsou všichni uživatelé oprávněni pracovat se všemi utajovanými informacemi, které jsou v informačním systému obsaženy.

Bezpečnostní provozní mód s nejvyšší úrovní nebo **s formálním řízením přístupu k informacím** je určen pro informační systém, v němž všichni uživatelé nejsou oprávněni pracovat se všemi utajovanými informacemi, je tedy nutno zavést v oblasti počítačové bezpečnosti také opatření, která omezí přístup určitého uživatele anebo skupiny uživatelů jen na informace, pro které mají „need-to-know“.

V informačních systémech pracujících v bezpečnostním provozním módu vyhrazeném, s nejvyšší úrovní nebo s formálním řízením přístupu k informacím se používají operační systémy zajišťující splnění minimálních požadavků počítačové bezpečnosti uvedených v § 7. Pro informační systémy nakládající s utajovanými informacemi stupně utajení Důvěrné nebo vyššího se zpravidla vyžaduje použití operačního systému, jehož bezpečnostní funkce byly ověřeny hodnocením podle Common Criteria na úrovni záruk nejméně EAL4 (případně na ekvivalentní úrovni podle ITSEC). Tento přístup se doporučuje i pro informační systémy na úrovni Vyhrazené. Z aktuálně dostupných (nebo stále provozovaných) operačních systémů se jedná o Windows NT 4.0, Windows 2000 Workstation, Windows 2000 Server (Advanced Server), Windows XP Professional, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, z Unixových systémů např. AIX 6.1, HP UX 11i, Solaris 10 Release 11, z otevřených zdrojů některé distribuce Linuxu (Red Hat Enterprise Linux ver. 5.1 a ver. 5.3, SUSE Linux Enterprise Server 10). Podrobnosti lze nalézt např. na portálu www.commoncriteriaportal.org.

Čtvrtým z možných bezpečnostních provozních módů je bezpečnostní provozní mód víceúrovňový. Jedná se o takové prostředí, které umožňuje v jednom informačním systému současné zpracování utajovaných informací klasifikovaných různými stupni utajení, ve kterém mohou pracovat uživatelé s různými úrovněmi bezpečnostní prověrky a s různým „need-to-know“ i v rámci své bezpečnostní úrovně.

Kromě minimálních požadavků počítačové bezpečnosti musí proto být v informačním systému zavedeno povinné řízení přístupu uživatele k informacím a dalším prostředkům informačního systému. K tomu je nutno zajistit trvalé spojení každého subjektu informačního systému (uživatel, proces) a objektu informačního systému (informace, soubor, adresář a další zdroje systému) s bezpečnostním atributem, který pro subjekt informačního systému vyjadřuje úroveň oprávnění subjektu informačního systému a pro

objekt informačního systému jeho stupeň utajení. Tento atribut (label) musí být chráněn, aby nemohlo dojít k jeho neautorizované změně. Systém před umožněním přístupu uživatele k objektu informačního systému porovnává úroveň jeho bezpečnostní prověrky a stupeň utajení objektu a podle stanovených pravidel přístup umožní nebo zamítne. V dalším kroku je pak aplikováno standardní volitelné řízení přístupu podle need-to-know. Úroveň použitých opatření z oblasti administrativní a personální bezpečnosti, fyzické bezpečnosti informačních systémů a opatření k zajištění důvěrnosti dat během přenosu se stanoví na základě principu povinného řízení přístupu, což znamená, že odpovídá skutečné úrovni klasifikace, která je v dané části informačního systému zpracovávána.

Užitná hodnota informačního systému realizovaného v bezpečnostním provozním módu víceúrovňovém by byla vysoká, avšak jeho realizace vyžaduje vysoké záruky za správnost implementace, a je cenově a provozně náročná.

Z víceúrovňových operačních systémů certifikovaných podle uznávaných kritérií hodnocení (Common Criteria, případně ITSEC), které mohou být základním prostředkem pro realizaci víceúrovňového informačního systému, lze uvést v současné době AIX 6 6100-00-02 for POWER V6.1 Technology level, HP UX 11i v3 on HP 9000/HP Integrity Servers, Solaris 10 release 11/06 Trusted Extensions na několika HW konfiguracích specifikovaných v certifikační zprávě, IBM z/0S ver.1. Release 10 pro IBM System z mainframe computer. Ve všech případech je víceúrovňový režim pojat jako režim provozu volitelný, vedle základního režimu jednoúrovňového. Podrobnosti lze opět nalézt např. na portálu www.commoncriteriaportal.org.

Pro řešení založená na aplikační úrovni je velmi obtížné prokázat jejich správnost. V současné době nám není v rámci NATO a EU v oblasti zpracování utajovaných informací známa žádná realizace víceúrovňového informačního systému pro zpracování utajovaných informací.

§ 9 Bezpečnost v prostředí počítačových sítí se v obecné rovině zabývá ochranou utajovaných informací během jejich přenosu komunikačními kanály. Základním požadavkem je zajištění důvěrnosti a integrity utajované informace při jejím přenosu komunikačním kanálem (odst. 1), přičemž základním prostředkem pro zajištění důvěrnosti utajované informace je kryptografická ochrana (odst. 2), pro zajištění integrity pak spolehlivá detekce záměrné i náhodné změny utajované informace (odst. 3).

V odstavcích 4, 6 a 7, jsou stanoveny požadavky na zabezpečení komunikačního kanálu vedeného v různých prostředích.

Pokud je komunikační kanál veden mimo objekt (ve smyslu zákona č. 412/2005 Sb.), musí být utajovaná informace chráněna šifrováním, prováděným kryptografickým prostředkem certifikovaným Úřadem minimálně pro stejný stupeň utajení jako je stupeň utajení informace, pro který je komunikační kanál používán (odst. 6).

Pokud je komunikační kanál veden v rámci zabezpečené oblasti nebo objektu může být, na základě analýzy rizik, zabezpečen pouze s využitím opatření fyzické bezpečnosti všech komponentů komunikačního kanálu, aniž je přenášená utajovaná informace chráněna kryptografickou ochranou nebo je chráněna kryptografickou ochranou na nižší úrovni, nežli je vyžadována pro stupeň utajení informace, pro jejíž přenos je komunikační kanál používán (odst. 4). Takový způsob ochrany musí být schválen Úřadem v rámci certifikace informačního systému.

Během certifikace informačního systému může Úřad schválit pro určitý komunikační kanál, na základě posouzení výsledků příslušné analýzy rizik a možnosti aplikovat specifická opatření pro detekci narušení kanálu a následnou rychlou reakci vedoucí ke snížení důsledku útoku, nešifrovaný přenos utajované informace i mimo zabezpečenou oblast nebo objekt (odst. 7). Takový způsob ochrany je třeba chápat jako výjimečný a musí být provozovatelem systému zdůvodněn. Reálně lze o něm uvažovat např. pokud je nezbytné vést část rozvodů LAN v rámci budovy provozovatele systému mimo objekty (ve smyslu zákona č. 412/2005 Sb.) jím zřízené v dané budově, nikoliv však pokud komunikační kanál vychází z oblasti, která je pod přímou kontrolou provozovatele informačního systému.

Dalším okruhem aktuálních problémů je propojování informačních systémů. Ve vyhlášce č. 523/2005 Sb. je od 1. 1. 2012 obsažen nový **§ 9a v následujícím znění:**

- **Odst. 1 – Propojením informačních systémů se pro účely této vyhlášky rozumí přímé spojení dvou nebo více informačních systémů nebo informačního systému a informačního systému pro nakládání s neutajovanými informacemi za účelem jednosměrného či vícesměrného sdílení údajů a dalších informačních zdrojů. Propojení informačního systému s jiným informačním**

systémem nebo s informačním systémem pro nakládání s neutajovanými informacemi lze realizovat pouze v případě nezbytné provozní potřeby.

- **Odst. 2 – Certifikovaný informační systém lze propojit s jiným certifikovaným informačním systémem, pokud to bylo na základě analýzy rizik schváleno v rámci certifikace těchto informačních systémů, je mezi nimi realizováno bezpečnostní rozhraní a jsou certifikovány pro nakládání s utajovanými informacemi**

a) téhož stupně utajení, nebo

b) odlišného stupně utajení kdy se uplatňují opatření podle odstavce 3.

- **Odst. 3 – Propojení informačních systémů certifikovaných pro nakládání s utajovanou informací odlišného stupně utajení musí být realizováno tak, aby mezi nimi bylo zabráněno přenosu utajované informace vyššího stupně utajení, nežli je stupeň utajení, pro které je informační systém certifikován.**
- **Odst. 4 – Certifikovaný informační systém nesmí být propojen s veřejnou komunikační sítí, s výjimkou případů, kdy má instalované pro tento účel mezi sebou a veřejnou komunikační sítí vhodné bezpečnostní rozhraní, schválené na základě analýzy rizik v rámci jeho certifikace tak, aby bylo zamezeno průniku do certifikovaného informačního systému a byl umožněn pouze kontrolovaný přenos dat, který nenarušuje důvěrnost, integritu a dostupnost certifikovaného informačního systému.**
- **Odst. 5 - Certifikovaný informační systém, který nakládá s utajovanou informací stupně utajení Přísně tajné, nebo s utajovanou informací vyžadující zvláštní režim nakládání označenou ATOMAL, nesmí být přímo ani postupně propojen s veřejnou sítí.**
- **Odst. 6 – Pokud je veřejná komunikační síť využívána výhradně k přenosu dat mezi informačními systémy nebo lokalitami informačního systému a přenášené informace jsou chráněny certifikovaným kryptografickým prostředkem, nepovažuje se takové spojení za propojení. Mezi informačním systémem a veřejnou komunikační sítí musí být realizováno vhodné bezpečnostní rozhraní tak, aby bylo zamezeno průniku do informačního systému. Připojení je předmětem analýzy rizik a musí být schváleno v rámci certifikace informačního systému.**

Návrh vychází do značné míry z Bezpečnostních pravidel Rady a bezpečnostních politik a směrnic EU, jakož i z bezpečnostních politik a směrnic NATO a je veden snahou reflektovat rozvoj informačních a komunikačních technologií a potřeby uživatelské komunity sdílet informace a to i informace utajované.

POZN. V současné době jsou povolována plnohodnotná propojení pouze informačních systémů certifikovaných pro nakládání s utajovanými informacemi stejného stupně utajení, dále použití rozhraní pro jednosměrný přenos informací ze systému s nižší klasifikací do systému s vyšší klasifikací (datová dioda), případně použití rozhraní realizujícího v podstatě funkci vzduchové mezery. Rozhraní mezi informačními systémy, z nichž alespoň jeden je certifikován pro nakládání s utajovanými informacemi, musí být ohodnoceno a schváleno Úřadem v rámci jeho certifikace. Silně se doporučuje uvažovat o použití komponent hodnocených podle Common Criteria nejméně na úrovni EAL4.

§ 10 Požadavky na dostupnost utajované informace a služeb informačního systému se zabývá problematikou dostupnosti utajované informace a služeb informačního systému. Jde o oblast, která často není chápána jako bezpečnostní problém, avšak ve skutečnosti zajištění dostupnosti informací, která je podmíněna i dostupností služeb informačního systému, patří k hlavním cílům při ochraně utajovaných informací v informačních systémech. Požadavky uvedené v § 10 jsou převzaty z všeobecně uznávané „nejlepší praxe“ a bezpečnostních standardů.

§ 11 ukládá v obecné rovině provedení analýzy rizik, z níž mají vyplynout další potřebná bezpečnostní opatření nad rámec minimálních požadavků uvedených ve vyhlášce. Na základě provedené analýzy rizik se provádí výběr vhodných protiopatření a určují se zbytková rizika a jejich úroveň. Nově je doplněn požadavek dbát principu minimality, tedy implementovat pouze funkce, zařízení a služby, které jsou nezbytné **pro splnění účelu, pro který je informační systém zřizován.**

§ 12 umožňuje navrhnout v odůvodněných případech náhradu prostředků počítačové bezpečnosti zavedením vhodných opatření z oblasti personální, fyzické a administrativní bezpečnosti. Tento postup nesmí vést k degradaci bezpečnostních funkcí a musí být schválen během certifikace informačního systému. Je používán ve velmi omezené míře.

§ 13 Požadavky na ochranu mobilních a přenosných informačních systémů se týká mobilních a přenosných systémů. Cílem je upozornit na specifika těchto systémů.

§ 14 se zabývá požadavkem ochrany informačního systému proti úniku utajovaných informací prostřednictvím kompromitujícího vyzařování. Jeho současné znění je následující:

- **Odst. 1 – Komponenty informačního systému, které nakládají s utajovanými informacemi stupně utajení Důvěrné nebo vyššího a zabezpečená oblast nebo objekt, ve kterém se v informačním systému zpracovávají utajované informace stupně utajení Důvěrné nebo vyššího, musí být zabezpečeny takovým způsobem, aby kompromitující vyzařování nezpůsobilo únik utajované informace.**
- **Odst. 2 – Požadavky na zabezpečení proti kompromitujícímu vyzařování jsou závislé na stupni utajení utajované informace, se kterou informační systém nakládá a jsou stanoveny v bezpečnostním standardu.**
- **Odst. 3 – Instalace informačního systému, který nakládá s utajovanou informací stupně utajení Důvěrné nebo vyššího, z hlediska jeho zabezpečení proti kompromitujícímu vyzařování musí být provedena v souladu s požadavky bezpečnostního standardu. Záznam o instalaci komponent informačního systému se vkládá do bezpečnostní dokumentace informačního systému. Obsah a forma záznamu jsou stanoveny v bezpečnostním standardu.**

Připomeňme si, že podle zákona č. 412/2005 Sb. je bezpečnostní standard využíván v případě, že úprava určité oblasti ochrany zahrnuje utajované informace. V současné době jsou v platnosti 2 standardy NBÚ pro tuto oblast – Bezpečnostní standard NBÚ-1/2007, Klasifikace prostorů z hlediska kompromitujícího elektromagnetického vyzařování, verze 1.0 z roku 2007 a Bezpečnostní standard NBÚ-2/2007, verze 2 z roku 2011, Instalace zařízení z hlediska kompromitujícího elektromagnetického vyzařování. Oba tyto standardy jsou klasifikovány stupněm utajení Důvěrné a jsou šířeny přísně podle zásady „need-to-know“. Dále jsou využívány i utajované standardy NATO a EU. Problematikou se zabývají také § 30 až § 36 vyhlášky č. 523/2005 Sb.

§ 15 Požadavky na bezpečnost. nosičů utajovaných informací je zařazen proto, že vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů neupravuje některé problémy týkající se počítačových médií používaných pouze v provozu informačního systému pro ukládání utajovaných informací.

V § 15 odst. 1 vyhlášky č. 523/2005 Sb. se stanovuje, že takové nosiče dat musí být evidovány. Evidence má být vedena ve vhodné administrativní pomůcce, i s údaji o typu nosiče dat (disketa, CD, DVD, pevný disk, magnetická páska, optický disk, flash memory aj.), o jeho výrobním čísle (je-li na něm uvedeno), o jeho uvedení do provozu, vyřazení z provozu apod.

Stupeň utajení nosiče utajovaných informací musí odpovídat bezpečnostnímu provoznímu módu informačního systému, v němž je nosič používán a nejvyššímu stupni utajení na nosiči uložených.

Nosiče utajovaných informací používané rutinně v bezpečnostním provozním módu vyhrazeném nebo s nejvyšší úrovní budou klasifikovány nejvyšším stupněm utajení, s nímž daný informační systém nakládá. Tím není vyloučen export informací nižšího stupně utajení nebo neutajovaných, pokud uživatel kvalifikovaně posoudí stupeň utajení určité dílčí informace nebo je nižší stupeň utajení určitého typu informace stanoven v bezpečnostní dokumentaci, a poté takovou informaci uloží na nosič příslušného stupně utajení nebo neutajovaný.

V bezpečnostním provozním módu víceúrovňovém se používají nosiče informací všech stupňů utajení – zde musí být zajištěno, že každý výstupní kanál je označen stupněm utajení a systém sám zajistí, že na něj pošle jen informace příslušného stupně utajení.

V § 15 odst. 2 se stanovuje, že na popisném štítku nosiče utajovaných informací používaného výhradně v provozu určitého informačního systému, je vyznačen spolu se stupněm utajení také evidenční číslo nosiče informací a název informačního systému, v němž je daný nosič provozním datovým nosičem.

Odlišný je režim pro nosiče informací používané pro vydání informací mimo informační systém – ty pak nesou stupeň utajení a číslo jednací a řídí se striktně administrativní vyhláškou.

§ 15 odst. 3 pojednává o nosičích informací a jiných komponentách umožňujících uchování utajovaných informací, zabudovaných pevně do zařízení. Nosiče utajovaných informací zabudované do zařízení a jiné komponenty umožňující uchování utajovaných informací musí být evidovány a označeny stupněm utajení nejpozději po jejich vyjmutí z daného zařízení. V každém případě musí být ale v rámci provozní bezpečnostní dokumentace informačního systému evidováno každé takové zařízení, s informací o tom, jaké nosiče a jakého stupně utajení obsahuje.

§ 15 odst. 4 pojednává o zachování stupně utajení nosiče utajovaných informací stupně utajení Přísně

tajné po celou dobu jeho životního cyklu, s jedinou výjimkou pro případ, kdy bylo možno prokázat, že na něm během jeho dosavadního životního cyklu byly uloženy pouze utajované informace nižšího stupně utajení.

V § 15 odst. 5, ve kterém se stanovují podmínky pro snížení stupně utajení nosičů utajovaných informací stupně utajení Tajné, Důvěrné nebo Vyhrazené, jsou nyní **uvedeny případy, ve kterých je možno stupeň utajení snížit nebo zrušit. Jde o případ, kdy je provedeno vymazání utajovaných informací z nosiče informací v souladu s odst. 6, nebo o případ, kdy je prokázáno, že na nosiči informací byly během jeho dosavadního životního cyklu uloženy pouze informace nižšího stupně utajení či neutajované nebo je prokázáno, že stupeň utajení utajovaných informací uložených na něm během jeho dosavadního životního cyklu byl zrušen nebo snížen.**

V § 15 odst. 6 se specifikuje, co je míněno „bezpečným vymazáním utajované informace". **Jde o vymazání utajované informace z nosiče utajovaných informací stupně utajení, které umožňuje snížení nebo zrušení jeho stupně utajení. Takové vymazání musí být provedeno tak, aby utajované informace uložené na nosiči během jeho dosavadního životního cyklu byly obtížně zjistitelné i při použití laboratorních metod. Podmínky a postupy bezpečného vymazání stanoví Úřad v bezpečnostním standardu. Postup vymazání utajované informace musí být uveden v provozní bezpečnostní dokumentaci certifikovaného informačního systému a být schválen v rámci jeho certifikace.**

V § 15 odst. 7 je stanoveno, že ničení nosiče utajovaných informací informačního systému musí být provedeno tak, aby se znemožnilo utajovanou informaci z něho opětovně získat.

V odst. 8 je zdůrazněna potřeba zajistit informační systémy proti neoprávněnému importu/exportu utajovaných informací, zejména při použití velkokapacitních vyměnitelných počítačových médií, tím, že již v bezpečnostní politice informačního systému (a tím i v návrhu bezpečnosti a bezpečnostních směrnicích informačního systému) je specifikováno řízení přístupu uživatele ke vstupním a výstupním zařízením.

§ 16 a § 17 se zabývají požadavky na přístup k utajované informaci v informačním systému a odpovědností uživatelů za činnost v informačním systému. Jsou v nich shrnuty nejdůležitější zásady týkající se osob působících v informačních systémech:

- autorizace uživatele, jeho bezpečnostní prověrka,
- jedinečný identifikátor subjektu v informačním systému,
- podmínky pro sdílení ID (stálá služba),
- princip minimálních privilegií,
- zajištění odpovědnosti uživatele,
- vyžaduje-li to činnost, pro kterou je informační systém zřízen, zajištění nepopiratelnosti.

V tomto výčtu chybí zásada „need-to-know", avšak pouze proto, že platí ze zákona všeobecně.

V § 16 je upravena úroveň bezpečnostní prověrky uživatelů, správců a bezpečnostních správců informačního systému.

- **Podle odst. 3 – Správce informačního systému, který vykonává funkci administrátora s právy úplného řízení systému, a bezpečnostní správce celého informačního systému, musí splňovat podmínky pro přístup fyzické osoby k utajované informaci stupně utajení o jeden stupeň vyššího, nežli je nejvyšší stupeň utajení informací, se kterými může informační systém nakládat. U správce informačního systému, který vykonává funkci administrátora s právy úplného řízení systému, a u bezpečnostního správce celého informačního systému malého rozsahu nebo s nízkým podílem zpracování utajovaných informací nejvyššího stupně utajení, pro jejichž zpracování je informační systém určen, nebo v nichž nedochází ke kumulaci utajovaných informací nebo v nichž se zpracovává pouze taktická utajovaná informace, může Úřad, se zvážením identifikovaných rizik, uznat jako dostačující splnění podmínek pro přístup fyzické osoby k utajované informaci na úrovni shodné s nejvyšším stupněm utajení informací, se kterými může informační systém nakládat.**
- **Podle odst. 4 – Správce informačního systému, který vykonává funkci administrátora s omezenými právy řízení systému, zejména správu serverů, správu aplikace nebo lokální správu a bezpečnostní správce informačního systému zajišťující dílčí oblast bezpečnosti, zejména určitou bezpečnostní technologii,nebo lokální správu, musí splňovat podmínky pro přístup fyzické osoby k utajované informaci stupně utajení shodného s nejvyšším stupněm utajení informací, se kterými může informační systém nakládat.**

- **Podle odst. 5 – V případě, že odpovědná osoba nebo jí pověřená osoba schválí informační systém do provozu pro nakládání s utajovanou informací do stupně utajení nižšího, nežli je stupeň utajení, se kterými může informační systém nakládat, je pro stanovení nutné úrovně podmínek pro přístup fyzické osoby k utajované informaci, určující stupeň utajení utajovaných informací, pro který je informační systém schválen do provozu.**

Příkladem informačního systému malého rozsahu je informační systém sestávající z jednoho či dvou samostatných osobních počítačů s periferními zařízeními nebo LAN obsahující server, několik pracovních stanic a tiskáren.

V § 17 v odst. 3 se v souvislosti s požadavkem odpovědnosti uživatele za činnost v informačním systému uvádí i zajištění nepopiratelnosti (pokud to vyžaduje činnost, pro kterou byl systém zřízen). Je-li v informačním systému požadována funkcionalita spisové služby v elektronické podobě, musí být její SW hodnocen během certifikace informačního systému. Elektronická spisová služba totiž může být aplikačním programem kritickým z hlediska bezpečnosti utajovaných informací, pokud přebírá od operačního systému zajištění některých bezpečnostních funkcí (řízení přístupu k utajovaným informacím, audit).

§ 18 Bezpečnostní správa informačního systému obsahuje důležitá ustanovení, rozvádějící povinnost zavést v informačním systému vhodný systém bezpečnostní správy a personálně oddělit roli bezpečnostního správce informačního systému od dalších rolí ve správě informačního systému. Ve velkých nebo složitých informačních systémech se zavádí podle potřeby více bezpečnostních správců, ať již na principu hierarchickém, územním, podle technologií apod. Naopak v informačním systému malého rozsahu může Úřad v rámci jeho certifikace umožnit spojení role bezpečnostního správce a některých dalších rolí ve správě informačního systému.

Stanovena je i povinnost správce informačního systému, plnit, mimo činnosti pro zajištění funkčnosti informačního systému a řízení jeho provozu, také stanovené činnosti pro zajištění počítačové a komunikační bezpečnosti informačního systému.

§ 19 Požadavky personální bezpečnosti při provozu informačního systému stanovuje základní postupy pro provoz informačního systému – formální autorizaci uživatele a osob pro bezpečnostní správu a správu informačního systému, vedení seznamu uživatelů, školení ve znalosti bezpečnostních provozních směrnic – úvodní a nejméně jednou ročně.

§ 20 popisuje rámcově požadavky fyzické bezpečnosti informačních systémů. Stanovuje se povinnost ochran zařízení informačních systémů před neoprávněným přístupem, poškozením a ovlivněním, dále před negativními vlivy prostředí (přírodní katastrofy, nevhodné podmínky pro provoz IT zařízení - teplota, vlhkost, prach, infrastruktura budov apod.). Stanovuje se umístění komponent informačního systému zamezující kompromitaci utajovaných informací jejich odezíráním. Dále se uvádí povinnost ochrany komunikační infrastruktury i prostředky fyzické bezpečnosti.

Během certifikace informačního systému se stanovuje, které komponenty musí být umístěny v zabezpečené oblasti, které v zabezpečeném objektu a jejich kategorie.

V oblasti fyzické bezpečnosti je závazná rovněž vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.

V odst. 5 se proto uvádí, že minimální míra zabezpečení zabezpečené oblasti pro umístění části informačního systému, v níž mohou být ukládány utajované informace, se určuje v souladu s tabulkami bodových hodnot nejnižší míry zabezpečení fyzické bezpečnosti uvedenými v příloze č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti, ve znění pozdějších předpisů.

A dále, že bodové ohodnocení fyzické bezpečnosti informačního systému je uvedeno v příloze č. 3 k vyhlášce č.523/2005 Sb. Tímto se problematika bodového ohodnocení zabezpečené oblasti ve vztahu ke komponentám informačního systému, v ní umístěným, částečně přesouvá do vyhlášky č. 523/2005 Sb.

§ 21 Požadavky testování bezpečnosti informačního systému, ačkoliv velmi krátký, je při certifikaci informačního systému velmi důležitý a vždy je jeho aplikace vyžadována.

§ 22 upravuje požadavky na bezpečnost při instalaci informačního systému. Je zde stanoveno, na jaké úrovni musí být prověřeny osoby provádějící instalaci komponent informačního systému. Bezpečnostně kritické komponenty musí instalovat osoby prověřené pro nejvyšší stupeň utajení informací, s nimiž bude informační systém nakládat; ostatní komponenty mohou instalovat i osoby s bezpečnostní prověrkou nižší úrovně nebo dokonce neprověřené, pokud to ovšem schválí bezpečnostní ředitel a za stálého do-

hledu prověřených a kompetentních osob ze správy informačního systému. Bude tedy i úkolem pro bezpečnostní ředitele dohlédnout na správnou aplikaci § 22.

§ 23 shrnuje nejdůležitější požadavky na bezpečnost provozovaného informačního systému. Jednotlivé odstavce je třeba rozpracovat do bezpečnostní dokumentace informačního systému. Zjednodušeně řečeno:

- bezpečnost provozovaného informačního systému musí být průběžně sledována,
- jakoukoliv změnu v informačním systému je třeba projednat s Úřadem, který způsob její realizace posoudí z bezpečnostního hlediska,
- musí být instalován vhodný antivirový SW,
- může být používáno pouze softwarové a hardwarové vybavení odpovídající bezpečnostní dokumentaci informačního systému schválené Úřadem a podmínkám certifikační zprávy k certifikátu informačního systému,
- musí být prováděno zálohování programového vybavení a utajovaných informací, záloha programového vybavení a utajovaných informací musí být uložena tak, aby nemohlo dojít k jejímu poškození nebo ke zničení při ohrožení informačního systému anebo zneužití pro narušení důvěrnosti utajovaných informací,
- servisní činnost v provozovaném informačním systému se musí organizovat tak, aby nebyla ohrožena jeho bezpečnost, z nosičů utajovaných informací informačního systému přístupných při servisní činnosti musí být vymazány utajované informace a dálková diagnostika musí být zabezpečena před zneužitím (většinou není povolena),
- údržbu komponent informačního systému zajišťujících bezpečnostní funkce informačního systému nebo přímo ovlivňujících bezpečnost informačního systému musí zajišťovat osoby prověřené pro přístup k utajovaným informacím nejvyššího stupně utajení, pro jehož nakládání je informační systém určen; údržbu ostatních komponentů informačního systému mohou provádět osoby splňující podmínky zákona pro nižší stupeň utajení nebo osoby schválené bezpečnostním ředitelem provozovatele informačního systému, avšak pod neustálým dohledem pracovníka správy informačního systému
- v termínech stanovených v bezpečnostní dokumentaci informačního systému a při vzniku krizové situace neprodleně musí být prováděno vyhodnocení auditních záznamů; auditní záznamy musí být archivovány po dobu stanovenou v bezpečnostní dokumentaci informačního systému a chráněny před modifikací nebo zničením (zpravidla 3-5 roků),
- pro řešení krizové situace provozovaného informačního systému a pro případ havárie SW nebo HW vybavení musí být v bezpečnostní dokumentaci informačního systému stanovena opatření zaměřená na jeho uvedení do známého bezpečného stavu v souladu s bezpečnostní dokumentací informačního systému a příslušné postupy a odpovědnosti
- před trvalým ukončením provozu informačního systému musí být provedeno vyjmutí nebo zničení nosičů utajovaných informací, se kterými informační systém nakládal; postupy doporučujeme konzultovat s Úřadem.
- **je ověřována pravost informací, které vstupují do informačního systému,** *pravost (autentičnost) znamená, že informace nejsou podvržené, že známe jejich zdroj a považujeme ho za důvěryhodný, že informace do informačního systému mohou vkládat jen oprávnění uživatelé; za ověření pravosti v některých případech lze pokládat i znalost, že některé informace nejsou autentické, potom musí být v systému jako takové nějakým způsobem identifikovány.*
- **v zabezpečené oblasti, v níž jsou umístěny komponenty informačního systému pro nakládání s utajovanými informacemi stupně utajení Tajné nebo Přísně tajné se na žádost orgánu státu nebo podnikatele provádí kontrola ke zjištění nedovoleného použití technických prostředků určených k získávání informací. Tato kontrola se provede před prvním zpracováním utajované informace a dále opakovaně zpravidla v intervalu dvou let. Tuto kontrolu provádí Úřad nebo koordinuje její provedení se zpravodajskými službami, pro provozovatele informačního systému nevznikají tím žádné finanční náklady. Časově se váže na období prvé nebo opakované certifikace informačního systému.**

1. 4 Certifikace informačních systémů

1.4.1 Zákon č. 412/2005 Sb. a certifikace informačních systémů

Nyní přejdeme k tématu certifikace informačního systému a vrátíme se proto opět do zákona č. 412/2005 Sb. a to k § 46. Tento velmi důležitý paragraf obsahuje společná ustanovení o certifikacích prováděných Úřadem.

Certifikace informačního systému je definována jako postup, jímž Úřad ověřuje způsobilost informačního systému k nakládání s utajovanými informacemi. Pokud Úřad zjistí tuto způsobilost určitého informačního systému, vydá pro něj certifikát.

Certifikát je charakterizován jako veřejná listina, je uveden jeho povinný obsah a je stanoveno, že přílohou certifikátu je certifikační zpráva.

Certifikace nemusí vždy dopadnout úspěšně – pak Úřad rozhodne o nevydání certifikátu. Odvolání proti rozhodnutí o nevydání certifikátu v případě informačního systému nebo kryptografického prostředku není možné.

Může také nastat případ, kdy se během provozu informačního systému buď objeví nová rizika nebo bezpečnost informačního systému během jeho provozu není udržena na požadované úrovni. Pak může Úřad rozhodnout o předčasném zániku platnosti certifikátu. Proti rozhodnutí Úřadu o zániku platnosti certifikátu informačního systému a certifikátu kryptografického prostředku není odvolání přípustné.

Specifická ustanovení týkající se certifikace informačních systémů obsahuje § 48. V něm se stanovuje, že žadatelem o certifikaci informačního systému je orgán státu nebo podnikatel, který bude informační systém provozovat, že žadatel předkládá v průběhu certifikace na žádost Úřadu dokumentaci nezbytnou pro provedení certifikace (tedy nikoliv povinně současně s podáním žádosti) a že dobu platnosti certifikátu stanoví Úřad.

Maximální doba platnosti certifikátu informačního systému je zákonem omezena pro stupeň utajení Přísně tajné a Tajné nejdéle na 2 roky, pro stupeň utajení Důvěrné nejdéle na 3 roky a pro stupeň utajení Vyhrazené nejdéle na 5 let.

V § 48 odst. 4 je také stanoveno, že platnost certifikátu informačního systému zaniká uplynutím doby jeho platnosti, v případě informačního systému pro nakládání s utajovanými informacemi stupně utajení Důvěrné nebo vyššího zánikem platnosti osvědčení podnikatele, zrušením orgánu státu, oznámením držitele certifikátu o zrušení informačního systému nebo rozhodnutím Úřadu o zániku platnosti certifikátu, přestal-li být informační systém způsobilý k nakládání s utajovanými informacemi.

V § 48 odst. 5 je upravena opakovaná certifikace informačního systému po řádném vypršení platnosti certifikátu a lhůta pro podání nové žádosti. Má-li být informační systém používán i bezprostředně po uplynutí doby platnosti jeho certifikátu, je žadatel povinen opětovně požádat Úřad o certifikaci informačního systému. Opakovaná žádost musí být Úřadu doručena nejméně 6 měsíců před uplynutím doby platnosti původního certifikátu informačního systému.

V § 48 odst. 6 jsou pak stanoveny lhůty pro provedení certifikace, kterými jsou modifikovány lhůty ze správního řádu (zákon č. 500/2004 Sb.), který vstoupil v platnost společně se zákonem č. 412/2005 Sb.

Úřad je povinen rozhodnout o certifikaci informačního systému do 1 roku od zahájení řízení o certifikaci, ve zvlášť složitých případech do 2 let; nelze-li vzhledem k povaze věci rozhodnout v této lhůtě, může ji přiměřeně prodloužit ředitel Úřadu, nejvýše však o 6 měsíců. Lhůta neběží, pokud odbor informačních technologií čeká na dodání jednotlivých podkladů pro provedení certifikace anebo na dokončení implementace informačního systému a jeho uvedení do souladu s bezpečnostní dokumentací.

1.4.2 Vyhláška č. 523/2005 Sb. a certifikace informačních systémů

Nyní opět přejdeme do vyhlášky č. 523/2005 Sb., neboť obsahuje i několik paragrafů blíže specifikujících problematiku certifikace informačních systémů. Jedná se o § 24, § 25 a §26.

§ 24 upravuje žádost o certifikaci informačního systému a způsob a podmínky jejího provedení. Žádost o certifikaci se podává jako běžný dopis s obsahem stanoveným v tomto paragrafu. **V souvislosti s novým postupem pro bezpečnostní prověření podnikatele pro přístup k utajované informace stupně utajení Vyhrazené se doplňuje povinnost doložit v jeho případě kopii platného prohlášení podnikatele.** Specifikovány jsou i podklady vyžadované pro certifikaci, přičemž se nevyžaduje, aby byly přiloženy k žádosti již v době jejího podání. Pro žadatele je naopak výhodné po podání žádosti a zahájení správního řízení k certifikaci konzultovat otázky bezpečnosti informačního systému a obsah

dokumentace s Úřadem (odbor informačních technologií). Již v počáteční fázi je např. výhodné dosáhnout shody v oblasti fyzické bezpečnosti a ověřit podmínky pro instalaci komponent informačního systému v zamýšleném prostředí z hlediska kompromitujícího vyzařování.

Podle odstavce 4 existuje také možnost předložit jako podklad pro certifikaci výsledek dílčího hodnocení některých komponent informačního systému, které si nechá žadatel o certifikaci provést na pracovišti, s nímž bude mít Úřad uzavřenou smlouvu o zajištění činnosti podle § 52 zákona č. 412/2005 Sb. (2012). Do současné doby však žádný subjekt z oblasti IT neprojevil zájem o uzavření takové smlouvy.

§ 25 upravuje certifikační zprávu informačního systému. Je nutno zdůraznit, že obsah certifikační zprávy je pro provoz informačního systému závazný. V certifikační zprávě lze uvést i případná zbytková přijatelná rizika spjatá s provozem informačního systému.

V § 26 je upraven postup při opakované certifikaci informačního systému, který má být provozován i po ukončení doby platnosti stávajícího certifikátu. Je umožněno několik způsobů provedení opakované certifikace informačního systému.

Pokud žadatel doloží, že ke dni ukončení platnosti dosavadního certifikátu bude informační systém provozován v rámci podmínek stanovených v certifikační zprávě a žadatel ani Úřad neidentifikovali nová rizika pro informační systém, vydá Úřad certifikát na základě existující bezpečnostní dokumentace a provedené kontroly bezpečnosti informačního systému.

Pokud ke dni ukončení platnosti dosavadního certifikátu provozovatel navrhuje změnu bezpečnostní politiky informačního systému, případně byla identifikována nová rizika pro informačního systému, vyžádá si Úřad doplnění nebo úpravu odpovídajících částí dokumentace a provede doplňující hodnocení informačního systému v rozsahu stanoveném Úřadem. Pokud informační systém vyhoví stanoveným bezpečnostním podmínkám, Úřad vydá certifikát.
V ostatních případech, kdy navrhované změny bezpečnostní politiky informačního systému jsou podstatné pro celkovou bezpečnost informačního systému, se certifikace provede v plném rozsahu, tedy jako by se jednalo o novou certifikaci.

Část II

Bezpečnost komunikačních systémů a některých samostatných elektronických zařízení

2.1 Bezpečnost komunikačních systémů

2.1.1 Zákon č. 412/2005 Sb. a bezpečnost komunikačních systémů

Oblast bezpečnosti komunikačních systémů používaných pro sdělování utajovaných informací je v zákoně č. 412/2005 Sb. upravena v § 35. Především je uvedena definice komunikačního systému pro účely tohoto zákona jako systému, který zajišťuje přenos utajovaných informací mezi koncovými uživateli a zahrnuje koncové komunikační zařízení, přenosové prostředí, kryptografické prostředky, obsluhu a provozní podmínky a postupy. Příkladem komunikačního systému může být telefonní spojení (současné vládní utajené spojení) nebo faxové spojení.

Na rozdíl od systému informačního komunikační systém neobsahuje počítače, neumožňuje zpracování utajovaných informací; nicméně v § 5 zákona č. 412/2005 Sb. je bezpečnost komunikačního systému vymezena podobně jako bezpečnost informačního systému, tedy bezpečnosti komunikačního systému se dosahuje uplatněním souboru opatření z oblasti komunikační bezpečnosti, kryptografické ochrany, ochrany proti úniku kompromitujícího vyzařování, administrativní bezpečnosti a organizačních opatření, personální bezpečnosti a fyzické bezpečnosti.

Komunikační systém Úřad necertifikuje, jeho jádrem je totiž certifikovaný kryptografický prostředek. Úřad pouze schvaluje projekt bezpečnosti komunikačního systému. To však je nutná podmínka pro jeho provoz s utajovanými informacemi.

Projekt bezpečnosti komunikačního systému je nástrojem pro správné nasazení kryptografického prostředku do konkrétního komunikačního systému. Řeší se v něm také otázka dostupnosti služeb, fyzická, personální a administrativní bezpečnost i zajištění bezpečnosti utajovaných informací mimo komunikační zařízení.

V § 35 se stanovuje, že o schválení projektu bezpečnosti komunikačního systému písemně žádá u Úřadu orgán státu, právnická osoba nebo podnikající fyzická osoba, která jej bude provozovat. Zákon č. 412/2005 Sb. neupravuje obsah projektu bezpečnosti komunikačního systému, úprava je přesunuta do novely vyhlášky č. 523/2005 Sb.

Komunikační systém, podobně jako informační systém, musí být písemně schválen do provozu odpovědnou osobou nebo jí pověřenou osobou. Komunikační systém podnikatele, který má přístup k utajovaným informacím stupně utajení Vyhrazené, může být schválen do provozu jen v době platnosti prohlášení podnikatele; zánikem platnosti prohlášení podnikatele zaniká též schválení komunikačního systému do provozu.

2.1.2 Vyhláška č. 523/2005 Sb. a bezpečnost komunikačních systémů

Další požadavky týkající se obsahu projektu bezpečnosti komunikačního systému, žádosti o jeho schválení Úřadem a způsobu jeho schvalování jsou uvedeny ve vyhlášce č. 523/2005 Sb., v části třetí nazvané Komunikační systém (§ 27, § 28 a § 29).

V § 27 jsou v odst. 1 specifikovány náležitosti projektu bezpečnosti komunikačního systému. Projekt bezpečnosti komunikačního systému obsahuje tyto náležitosti

a) bezpečnostní politiku komunikačního systému,

b) organizační a provozní postupy provozování komunikačního systému,

c) provozní směrnice pro bezpečnostní správu komunikačního systému a

d) provozní směrnice uživatele komunikačního systému.

V odstavcích 2, 3, 4 a 5 je specifikován obsah jednotlivých částí projektu bezpečnosti.

V bezpečnostní politice je třeba shrnout zásady a požadavky z oblasti personální, administrativní, fyzické a komunikační bezpečnosti, stanovené s cílem zajistit důvěrnost, integritu a dostupnost utajované informace a odpovědnost uživatele za jeho činnost v komunikačním systému. V úvodu bezpečnostní politiky je vhodné popsat stručně daný komunikační systém. Bezpečnostní politika komunikačního systému vychází z charakteru komunikačního systému, ze stupně utajení utajovaných informací, které

v něm budou přenášeny, z analýzy rizik komunikačního systému a do značné míry ze zásad a podmínek provozování kryptografického prostředku, uvedených v certifikační zprávě kryptografického prostředku. Opomenout nelze, v závislosti na stupni utajení přenášených utajovaných informací, požadavky ochrany před únikem utajovaných informací kompromitujícím vyzařováním a dále otázky požadované dostupnosti služeb komunikačního systému.

V odst. 4 § 27 je blíže specifikován obsah části projektu bezpečnosti komunikačního systému označené jako „organizační opatření a provozní postupy provozování komunikačního systému". Jedná se o zjednodušenou obdobu návrhu bezpečnosti informačního systému, o konkrétní provádění požadavků bezpečnostní politiky komunikačního systému. Je nutno se zaměřit na plnění podmínek certifikační zprávy kryptografického prostředku při jeho nasazení v daném komunikačním systému, v závislosti na specifické struktuře tohoto systému, jeho rozsahu a charakteru, na provozních potřebách apod. Vyžaduje se specifikace struktury správy komunikačního systému a stanovení veškerých dalších potřebných organizačních opatření a zásad pro ochranu utajovaných informací i před jejich vstupem do koncového komunikačního zařízení a po jejich výstupu z něho a pro bezpečný provoz komunikačního systému.

Na základě prvých dvou částí projektu bezpečnosti komunikačního systému je pak možno zpracovat provozní směrnice komunikačního systému, popisující zejména povinnosti zúčastněných osob a příslušné provozní postupy. Poslední odstavec § 27 obsahuje požadavek, aby byly provozní směrnice pro bezpečnostní správu komunikačního systému zpracovány odděleně od provozních směrnic pro uživatele komunikačního systému. Bezpečnostní správa komunikačního systému zahrnuje činnosti v oblasti personální, fyzické a administrativní bezpečnosti, činnosti v organizaci bezpečného provozu i činnosti pracovníků kryptografické ochrany.

V § 28 je specifikován obsah žádosti o schválení projektu bezpečnosti komunikačního systému. Žadatelem o schválení projektu bezpečnosti komunikačního systému je budoucí provozovatel komunikačního systému. Žádost má obsahovat standardně vyžadované údaje o žadateli, kontaktním spojení, komunikačním systému samotném a o stupni utajení informací, s nimiž bude nakládat.

V průběhu schvalování předkládá pak žadatel jednotlivé části projektu bezpečnosti komunikačního systému.

V § 29 je stanoveno, jak probíhá proces schvalování projektu bezpečnosti komunikačního systému. V prvé fázi se posuzuje vhodnost souboru zásad a požadavků v oblasti personální, administrativní, fyzické a komunikační bezpečnosti (bezpečnostní politika komunikačního systému) pro daný komunikační systém, s navrženým kryptografickým prostředkem. Následuje hodnocení navržených organizačních opatření a provozních postupů pro realizaci bezpečnostní politiky. Zjištěné nedostatky nebo nejasnosti jsou sděleny žadateli a projednány s ním, se snahou nalézt vhodné řešení. Po dosažení vyhovující verze uvedených částí projektu bezpečnosti se posuzují provozní směrnice komunikačního systému. Poté, co Úřad shledá, že projekt bezpečnosti komunikačního systému je vyhovující, provede kontrolu skutečného stavu bezpečnosti v provozním prostředí komunikačního systému. V té době tedy musí být již komunikační systém odzkoušen z funkčního hlediska, musí být instalován v dohodnutém rozsahu a musí být aplikována všechna deklarovaná bezpečnostní opatření. Rozšiřování systému po schválení jeho projektu bezpečnosti je zpravidla v kompetenci provozovatele.

Pokud je reálný stav zabezpečení komunikačního systému v souladu s projektem jeho bezpečnosti, Úřad schválí uvedený projekt a oznámí tuto skutečnost písemně žadateli. Pokud Úřad zjistí, že daný komunikační systém není způsobilý pro nakládání s utajovanými informacemi, sdělí tuto skutečnost žadateli rovněž písemně. K takové situaci by však mělo docházet jen výjimečně, neboť žadatel se může předem seznámit v certifikační zprávě kryptografického prostředku s příslušnými podmínkami pro jeho nasazení, Úřad se během procesu schvalování vyjadřuje k předkládaným materiálům a poskytuje potřebné konzultace a prakticky vždy lze nalézt vhodné řešení.

2.2 Bezpečnost některých elektronických zařízení provozovaných mimo informační nebo komunikační systémy

2.2.1 Zákon č. 412/2005 Sb. a bezpečnost elektronických zařízení provozovaných mimo informační nebo komunikační systémy

Ochrana utajovaných informací při zpracování v elektronické podobě v zařízení, které není součástí informačního nebo komunikačního systému je upravena § 36. Tento paragraf byl pro znění platné od 1. 1. 2012 v zákoně č. 412/2005 Sb. přeformulován, má čtyři odstavce, namísto původních pěti, přičemž věcná podstata se nemění.

Aktuální znění je následující:

- **Odst. 1 – Při zpracování utajované informace v elektronické podobě v zařízení, které není součástí informačního nebo komunikačního systému, zejména v psacím stroji s pamětí a v zařízení umožňujícím kopírování, záznam nebo zobrazení utajované informace anebo její převod do jiného datového formátu, musí být zajištěna ochrana této utajované informace.**
- **Odst. 2 – Orgán státu, právnická osoba a podnikající fyzická osoba jsou povinni pro jimi provozované zařízení uvedené v odstavci 1 vydat bezpečnostní provozní směrnici; pouze v souladu s ní lze zpracovávat utajovanou informaci.**
- **Odst. 3 – V bezpečnostní provozní směrnici podle odstavce 2 se uvedou pro zařízení podle odstavce 1**

a) způsob jeho bezpečného provozování,

b) provozní směrnice pro jeho uživatele.

- **Odst. 4 – Podmínky bezpečného provozování zařízení uvedeného v odstavci 1 v závislosti na stupni utajení v něm zpracovávaných utajovaných informací stanoví prováděcí právní předpis.**

Bezpečnostní provozní směrnice daného zařízení nepodléhá schvalování Úřadem. Nicméně v § 153 je mezi správními delikty, kterých se může dopustit právnická nebo podnikající fyzická osoba nebo orgán státu uvedeno nezpracování bezpečnostní provozní směrnice pro kopírovací zařízení, zobrazovací zařízení nebo psací stroje s pamětí, používané k nakládání s utajovanými informacemi.

Cílem ustanovení § 36 je zamezit možným únikům utajovaných informací (jinak pečlivě chráněných) např. tím, že budou kopírovány na kopírovacím stroji umístěném na chodbě s přístupem neoprávněných osob nebo tím, že zůstanou uloženy v paměti volně přístupného elektrického psacího stroje nebo na pevném disku či jiné nevolatilní paměti kopírky, přístupné např. při servisním zásahu. Důsledkem úvah může být i přehodnocení počtu např. kopírek a scannerů, na kterých je povoleno reprodukovat utajované informace, i s ohledem na pravidla stanovená v oblasti administrativní bezpečnosti pro možnost kopírování utajovaných informací vyšších stupňů utajení, a redukce počtu osob, které mohou kopie pořizovat.

Je také třeba upozornit, že fyzická osoba, která by použila pro nakládání s utajovanými informacemi kopírovacího nebo zobrazovacího zařízení nebo psacího stroje s pamětí v rozporu s jejich bezpečnostní provozní směrnicí, dopouští se podle § 149 přestupku, spjatého s vysokou pokutou.

2.2.2 Vyhláška č. 523/2005 Sb. a bezpečnost elektronických zařízení provozovaných mimo informační nebo komunikační systémy

Ve vyhlášce č. 523/2005 Sb. pojednává o této problematice předposlední paragraf s číslem 38, v němž se blíže vymezují podmínky bezpečného provozování uvedených zařízení. Podstatné je, že bezpečného provozování např. kopírovacího zařízení, zobrazovacího zařízení nebo psacího stroje s pamětí, které nejsou součástí informačního nebo komunikačního systému, se dosahuje opět celým systémem opatření. Uvažovat je nutno o opatřeních z oblasti

- personální bezpečnosti,
- fyzické bezpečnosti,
- administrativní bezpečnosti a organizačních opatření a
- ochrany utajované informace před jejím únikem kompromitujícím vyzařováním.

Úroveň bezpečnostních opatření závisí na stupni utajení utajovaných informací, k jejichž zpracování má dané zařízení sloužit. Zabezpečení proti úniku utajovaných informací kompromitujícím vyzařováním se týká zařízení, která jsou určena pro nakládání s utajovanými informacemi stupně utajení Důvěrné nebo vyššího. Úřad na žádost provozovatele zařízení provede potřebná měření a hodnocení daných zařízení a prostor, v nichž mají být umístěna a výsledek sdělí žadateli.

Požadovaná fyzická bezpečnost elektronických zařízení provozovaných mimo informační nebo komunikační systémy závisí na stupni utajení utajovaných informací a rovněž na analýze rizik, kterou se pro konkrétní typ zařízení odhalí jeho zranitelná místa, pravděpodobnost realizace možných hrozeb a jejich dopad.

Cílem je zamezit neoprávněnému přístupu k uvedeným zařízením (a tím potenciálně i k utajovaným informacím), poškození nebo ovlivnění těchto zařízení. Uvedená zařízení je nutno rozmístit tak, aby se tím nepovolaným osobám zamezilo i odezírání utajovaných informací.

V úvahu je nutno vzít i vliv prostředí, jak v bezprostředním okolí (teplota, vlhkost, prašnost), tak v širším měřítku (např. možnost záplav).

Na elektronických zařízeních provozovaných mimo informační nebo komunikační systémy, které obsahující zabudované nosiče utajovaných informací nebo jiné komponenty umožňující uchování utajovaných informací musí být připevněn štítek s vyznačením nejvyššího stupně utajení utajovaných informací, které v nich mohou být zpracovávány. Pokud to není možné, je alternativou stanovení stupně utajení v bezpečnostní provozní směrnici nebo jiný vhodný způsob. Samotné nosiče utajovaných informací (např. i paměti psacích strojů) nebo jakékoliv komponenty umožňující uchování utajovaných informací musí být evidovány a označeny stupněm utajení. Pokud je jejich vyjímání ze zařízení technicky problematické, lze vyčkat do jejich prvého vyjmutí. Tyto nosiče nebo komponenty musí být v případě vyřazení zařízení z provozu nebo při své poruše ničeny jako utajované informace odpovídajícího stupně utajení.

Poslední podmínkou bezpečného provozování elektronických zařízení provozovaných mimo informační nebo komunikační systémy je zajištění bezpečnosti utajovaných informací v souvislosti se servisní činností. Jedná se jednak o možnost ovlivnění zařízení, které by vedlo k následné kompromitaci utajovaných informací, jednak o přístup (na servisní úrovni) k informacím, uloženým na nosičích informací (disky apod.) a dalších nevolatilních pamětech zabudovaných v zařízení.

Souhrnně lze doporučit, aby pro nakládání s utajovanými informacemi byl používán jen omezený počet takových zařízení, ještě postačující pro plnění provozních potřeb. Použití jednoduchých zařízení (bez zabudovaných nevolatilních paměťových prvků) nebo zařízení s vyjímatelnými paměťmi značně snižuje potřebnou úroveň bezpečnostních opatření.

Zákon č. 412/2005 Sb. ani vyhláška č. 523/2005 Sb. nestanovují blíže formu bezpečnostní provozní směrnice pro předmětná zařízení. Ve velkých resortech může být vhodné zpracovat pro jednotlivé typy zařízení generické směrnice, které jsou pak lokalizovány na jednotlivých pracovištích.

Část III

Kompromitující vyzařování, smlouvy o zajišťování činnosti

3.1 Kompromitující vyzařování

3.1.1 Zákon č. 412/2005 Sb. a problematika kompromitujícího vyzařování

Problematika kompromitujícího elektromagnetického vyzařování ve spojitosti s ochranou utajovaných informací se v legislativě České republiky objevuje poprvé v zákoně č. 412/2005 Sb., nicméně ochrana utajovaných informací před jejich únikem elektromagnetickým vyzařováním z elektrických a elektronických zařízení, byla uplatňována již v době platnosti zákona č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, díky vyhlášce č. 56/1999 Sb., o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi. Namísto pojmu kompromitující elektromagnetického vyzařování se používalo pojmu parazitní elektromagnetické vyzařování, který je dnes již považován za zastaralý. V současné době se v zákoně č. 412/2005 Sb. objevuje **širší pojem kompromitující vyzařování.**

POZNÁMKA. V zákoně č. 412/2005 Sb. byla původně v § 45 nejprve uvedena definice kompromitujícího elektromagnetického vyzařování. Definice je přesunuta do vyhlášky č. 523/2005 Sb., stejně jako definice stínicí komory.

V zákoně č. 412/2005 Sb. je prvém odstavci § 45 odst. 1 uvedeno, co je míněno ochranou utajovaných informací stupně utajení Důvěrné a vyššího před jejich únikem kompromitujícím vyzařováním. Tato ochrana je chápána jako zabezpečení elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu a v podstatě se realizuje použitím IT zařízení s omezeným elektromagnetickým vyzařováním, zejména na frekvencích nesoucích užitečnou informaci, umístěním uvedených zařízení do prostorů ve všech směrech dostatečně vzdálených od míst, z nichž by bylo možno kompromitující vyzařování zachycovat, umístěním uvedených zařízení do prostorů vykazujících silný útlum kompromitujícího vyzařování z nich vycházejícího nebo kombinací těchto postupů.

Vzhledem k požadavkům fyzické bezpečnosti se v zákoně č. 412/2005 Sb. jako prostory pro umístění elektrických a elektronických zařízení nakládajících s utajovanými informacemi uvažují zabezpečené

oblasti a objekty. Ověřování způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím vyzařováním zajišťuje Úřad zpravidla při certifikaci informačního systému nebo kryptografického prostředku, **při schvalování projektu bezpečnosti komunikačního systému nebo na základě odůvodněné písemné žádosti orgánu státu nebo podnikatele v souvislosti s ochranou utajovaných informací.**

Jednou z možností ochrany je vytvoření uzavřeného prostoru, z něhož kompromitující vyzařování nemůže z fyzikálních důvodů uniknout (z hlediska elektromagnetického vyzařování se jedná o tzv. Faradayovu klec). Takový prostor se označuje jako stínicí komora. Stínicí komora používaná k ochraně utajované informace před únikem kompromitujícím vyzařováním musí být certifikována Úřadem (§ 45 odst. 2).

3.1.2 Vyhláška č. 523/2005 Sb. a problematika kompromitujícího vyzařování

Problematika kompromitujícího vyzařování je ve vyhlášce č. 523/2005 Sb. řešena § 30 až 36, a dvěma paragrafy, označenými jako § 29a, 31a.

V § 29a je uvedena definice pojmu kompromitující vyzařování, jako vyzařování elektrických a elektronických zařízení, které by mohlo způsobit únik utajované informace stupně utajení Přísně tajné, Tajné nebo Důvěrné.

V celém tomto bloku paragrafů se nyní používá pojmu „kompromitující vyzařování“ místo „kompromitujících elektromagnetické vyzařování“. Do § 32 byl přidán odst. 1 s definicí stínicí komory, jako uzavřeného elektromagneticky stíněného prostoru zabraňujícího šíření elektromagnetického, optického a akustického vyzařování mimo tento prostor.

V § 30 je uveden obsah žádosti o ověření způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu, která se podává u Úřadu. Žádost (§ 30 odst. 1) obsahuje údaje o žadateli, o předmětu žádosti a stupni utajení utajovaných informací, které mají být chráněny.

V § 31 se specifikuje, jakým způsobem Úřad hodnotí vlastnosti elektrických a elektronických zařízení, jakož i prostorů v nichž jsou umístěna (v případě zařízení pro nakládání s utajovanými informacemi zpravidla zabezpečená oblast, zabezpečený objekt), z hlediska možného úniku informací kompromitujícím vyzařováním. V případě elektrického nebo elektronického zařízení se provede laboratorní měření elektromagnetického vyzařování z daného zařízení a naměřené hodnoty se porovnají s bezpečnostními standardy Úřadu (odst. 1), v případě prostorů se provede měření jeho útlumových vlastností a porovná se s bezpečnostními standardy Úřadu (odst. 2).

Podle § 30 odstavce 2 navíc může být k žádosti přiložena zpráva o výsledku hodnocení způsobilosti elektrického nebo elektronického zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím elektromagnetickým vyzařováním, provedeného orgánem státu nebo podnikatelem na základě smlouvy o zajištění činnosti uzavřené s Úřadem. V tom případě Úřad pouze porovná takto zjištěné výsledky se svými standardy.

Zmíněné bezpečnostní standardy jsou utajovanými dokumenty a jsou uvolňovány přísně na základě „potřeby znát“. Obsahují i podmínky hodnocení a podmínky pro používání elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně utajovaných informací před únikem utajované informace kompromitujícím vyzařováním. Úřad během certifikace informačního systému nebo kryptografického prostředku nebo schvalování projektu bezpečnosti komunikačního systému poskytuje žadateli adekvátní pomoc a potřebné informace.

Pokud jsou v průběhu hodnocení zjištěny odstranitelné nedostatky, vyzve Úřad žadatele k jejich odstranění (§ 31 odst. 3), poté provede hodnocení znovu. Úřad vždy vypracuje o průběhu a výsledcích hodnocení způsobilosti elektrických a elektronických zařízení, zabezpečené oblasti nebo objektu k ochraně před únikem utajované informace kompromitujícím vyzařováním zprávu, dokumentující provedená měření a jejich následné vyhodnocení a výsledek písemně oznámí žadateli (§ 31 odst. 4) .

3.1.3 Problematika certifikace stínících komor

V této kapitole budou uvedena specifika certifikace stínicí komory. V zákoně č. 412/2005 Sb. se v § 51 uvádí, že o certifikaci stínicí komory písemně žádá u Úřadu orgán státu nebo podnikatel, u kterého je stínicí komora používána a že ten, kdo o certifikaci stínicí komory požádal, předkládá v průběhu certifikace na žádost Úřadu dokumentaci nezbytnou pro provedení certifikace. Dobu platnosti certifikátu stínicí komory stanoví Úřad na dobu nejdéle 5 let.

Podmínky pro zánik certifikátu stínicí komory jsou obdobné jako např. u certifikátu informačního systému. Platnost certifikátu stínicí komory zaniká uplynutím doby jeho platnosti, zánikem platnosti osvědčení podnikatele, zrušením orgánu státu, nebo rozhodnutím Úřadu o zániku platnosti certifikátu, přestala-li být komora způsobilá k ochraně utajovaných informací.

Rozhodnutí o zániku certifikátu nemá odkladný účinek, avšak odvolání proti rozhodnutí je v tomto případě možné.

V § 51 odst. 5 se pak uvádí, že pokud má být komora používána i bezprostředně po uplynutí doby platnosti jejího certifikátu, je žadatel povinen požádat Úřad o její opakovanou certifikaci. Opakovaná žádost musí být Úřadu doručena nejméně 12 měsíců před uplynutím doby platnosti původního certifikátu komory. Důvodem je, že komory jsou často umístěny ve vzdálených lokalitách a Úřad si musí činnost naplánovat.

Úřad je povinen rozhodnout o certifikaci komory do 6 měsíců od zahájení řízení o certifikaci, ve zvlášť složitých případech do 1 roku; nelze-li vzhledem k povaze věci rozhodnout v této lhůtě, může ji přiměřeně prodloužit ředitel Úřadu, nejvýše však o 3 měsíce.

Ve vyhlášce č. 523/2005 Sb. se certifikace stínicích komor týkají § 32 až § 36. V § 32 se uvádí definice pojmu stínicí komora a opakuje ustanovení zákona č. 412/2005 Sb. že k ochraně utajovaných informací před jejich únikem kompromitujícím vyzařováním se může používat pouze komora certifikovaná Úřadem. Podmínky hodnocení komory k ochraně utajovaných informací stanoví Úřad v bezpečnostních standardech.

V § 33 je rozveden obsah žádosti o certifikaci komory. Jedná se o standardní údaje o žadateli o certifikaci, o označení a umístění komory a identifikaci výrobce komory. U podnikatele se navíc vyžaduje údaj o stupni a čísle osvědčení podnikatele pro seznamování se s utajovanými informacemi nebo kopie prohlášení podnikatele. K žádosti může být přiložena zpráva o výsledku hodnocení komory, provedeného orgánem státu nebo podnikatelem na základě smlouvy o zajištění činnosti uzavřené s Úřadem; výsledek hodnocení nesmí být starší 6 měsíců.

V § 34 je uveden způsob provádění certifikace stínicí komory, když se konstatuje, že certifikace stínicí komory se provádí měřením útlumových vlastností komory a jejich porovnáním s bezpečnostními standardy. Měření komory se provádí za spoluúčasti žadatele a v případě potřeby i dodavatele komory. O průběhu a dílčích výsledcích certifikace komory vypracuje Úřad zprávu.

Certifikát komory je doprovázen certifikační zprávou, která podle § 35 obsahuje zejména orientační popis komory, jejího umístění a účelu jejího používání, podmínky provozu komory a typy změn, které vyžadují provedení opakované certifikace komory.

Žádost o opakovanou certifikaci komory a způsob jejího provedení je obsahem § 36. Žádost o opakovanou certifikaci stínicí komory obsahuje obdobné údaje jako žádost o prvou certifikaci, dále také její identifikaci a další údaje z existujícího platného certifikátu.

Pro vyřízení žádosti existují podle okolností dva scénáře.

Pokud žadatel doloží, že ke dni ukončení platnosti dosavadního certifikátu nedochází ke změnám podmínek podmiňujících platnost stávajícího certifikátu, vydá Úřad certifikát i na další období.

Doložením trvajícího plnění podmínek certifikace může být zpráva o výsledku hodnocení komory osvědčující soulad s bezpečnostním standardem NBÚ, provedeného orgánem státu nebo podnikatelem na základě smlouvy o zajištění činnosti uzavřené s Úřadem, ne starší 6 měsíců, doplněné o informace o trvalém umístění stínicí komory, o řádném provádění údržby stínicí komory a o skutečnost, že nebyla žadatelem ani Úřadem identifikována nová rizika pro tuto komoru. Hodnocení komory dle smlouvy o zajištění činnosti uzavřené s Úřadem lze provést pouze jedenkrát po certifikačním měření provedeném Úřadem. V takovém případě Úřad neprovádí vlastní nová měření útlumu stínicí komory, vydá certifikát na další období s maximální platností 4 roky a poté provede opět certifikační měření.

V případě, že ke dni ukončení platnosti dosavadního certifikátu provozovatel nemůže doložit trvalost podmínek podmiňujících platnost dosavadního certifikátu, provede Úřad doplňující hodnocení stínicí komory k ověření její způsobilosti k ochraně utajovaných informací. V případě podstatných změn se postupuje jako při nové certifikaci.

3.2 Možnosti uplatnění orgánů státu nebo podnikatelů v procesu certifikace podle zákona č. 412/2005 Sb.

3.2.1 Zákon č. 412/2005 Sb. a smlouva o zajištění činnosti

Zákon č. 412/2005 Sb. nadále umožňuje ustanovením uvedeným v § 46, odst. 15 orgánu státu nebo podnikateli účast na ověřování způsobilosti informačního systému k nakládání s utajovanými informacemi, kryptografického prostředku k ochraně utajovaných informací, kryptografického pracoviště k zajišťování jeho činnosti, komory k ochraně utajovaných informací. Podle § 45 odstavce 6 může se orgán státu nebo podnikatel rovněž účastnit na zjišťování způsobilosti elektrických a elektronických zařízení, zabezpečených oblastí a objektů k ochraně před únikem utajovaných informací kompromitujícím elektromagnetickým vyzařováním. Zde uvedené činnosti jsou pouze dílčího charakteru a jejich výsledek se využívá v procesu certifikace. Prováděny mohou být pouze za předpokladu, že orgán státu nebo podnikatel uzavře s Úřadem smlouvu o zajištění činnosti podle § 52.

Podle § 39 odstavce 7 může orgán státu provádět odbornou zkoušku a vydávat osvědčení o zvláštní odborné způsobilosti pracovníka kryptografické ochrany. Zde se jedná o plné zajištění školení pracovníků kryptografické ochrany. Předpokladem je opět uzavření smlouvy o zajištění této činnosti podle § 52, tedy mezi daným orgánem státu a Úřadem.

Smlouva o zajištění činnosti se podle § 52 uzavírá na základě písemné žádosti orgánu státu nebo podnikatele a musí mít písemnou formu. Žadatel musí zajistit, aby činnosti, které jsou předmětem smlouvy, byly prováděny jeho odborně způsobilými zaměstnanci a vytvořit pro ně potřebné organizační, materiální a technické podmínky.

Smlouvu s podnikatelem může Úřad uzavřít pouze tehdy, je-li jeho sídlo nebo místo podnikání na území ČR a je-li držitelem osvědčení podnikatele příslušného stupně utajení. Náležitosti smlouvy jsou uvedeny v § 52 odst. 4.

Během účinnosti smlouvy Úřad kontroluje, zda druhý účastník smlouvy dodržuje ustanovení tohoto zákona, prováděcích právních předpisů a uzavřené smlouvy. Mezi podmínkami smlouvy musí být uvedeno, že Úřad při zjištění nedostatků v těchto oblastech od smlouvy odstoupí. Změnit obsah smlouvy lze pouze písemnou dohodou účastníků smlouvy. Smlouvu lze vypovědět pouze písemnou formou. Nestanoví- li zákon jinak,použijí se v ostatním přiměřeně ustanovení obchodního zákoníku.

3.2.2 Vyhláška č. 523/2005 Sb. a smlouva o zajištění činnosti

Ve vyhlášce č. 523/2005 Sb. je v § 37 uveden obsah žádosti, kterou podává orgán státu nebo podnikatel, pokud chce uzavřít s Úřadem smlouvu o zajištění určité činnosti. Kromě obvyklých identifikačních údajů se vyžaduje

- identifikace příslušného odborného pracoviště žadatele (předmět činnosti a podrobná specifikace
- umístění pověřovaného pracoviště, jméno a příjmení kontaktního pracovníka a kontaktní spojení),
- specifikace činností, které mají být prováděny podle smlouvy,
- personální předpoklady pracoviště k provádění požadovaných činností (identifikace a kvalifikace vedoucího pracovníka odborného pracoviště a ostatních odborných pracovníků),
- prohlášení odpovědné osoby o úrovni fyzické, personální a administrativní bezpečnosti, která je zajištěna pro odborné pracoviště,
- stupeň a evidenční číslo certifikátu informačního systému, pokud je použití certifikovaného informačního systému potřebné pro provádění činností podle smlouvy a
- vybavenost odborného pracoviště technickým zařízením, potřebným pro provádění činností podle smlouvy.

Je-li žadatelem podnikatel, musí uvést také stupeň a číslo osvědčení podnikatele pro seznamování se s utajovanými informacemi nebo kopii platného prohlášení podnikatele.

Seznam orgánů státu a podnikatelů s nimiž NBÚ uzavřel smlouvu o zajištění činnosti podle § 52 zákona č. 412/2005 Sb.

Stav k 1. lednu 2015

Techniserv, s. r. o.
Baarova 231/36, Praha 4
IČ: 44264020

Podle ustanovení § 45 odst. 4 zákona č. 412/2005 Sb. může podnikatel Techniserv, s.r.o. zajišťovat činnosti spočívající v provádění dílčích úloh při ověřování způsobilosti podle § 46 odst. 1 písm. e) uvedeného zákona.

S.ICZ a. s.
Na hřebenech II 1718/10, Praha 4
IČ: 26482444

Podle § 39 odst. 3 písm. a) zákona č. 412/2005 Sb. může podnikatel S.ICZ a. s. provádět části odborné zkoušky (zkouška zvláštní odborné způsobilosti pracovníka kryptografické ochrany) a vydávat potvrzení o jejím absolvování.

ATS – TELCOM PRAHA a. s.
Trojská 195/88, Praha 7
IČ: 61860409

Podle § 39 odst. 3 písm. a) zákona č. 412/2005 Sb. může podnikatel ATS TELCOM a. s. provádět části odborné zkoušky (zkouška zvláštní odborné způsobilosti pracovníka kryptografické ochrany) a vydávat potvrzení o jejich absolvování.

Česká republika Ministerstvo zahraničních věcí
Loretánské náměstí 5, Praha 1
IČ: 45769851

Podle ustanovení § 45 odst. 4 zákona č. 412/2005 Sb. může Ministerstvo zahraničních věcí zajišťovat činnosti spočívající v provádění dílčích úloh při ověřování způsobilosti podle § 46 odst. 1 písm. e) uvedeného zákona.

Podle § 39 odst. 3 písm. a) zákona č. 412/2005 Sb. může Ministerstvo zahraničních věcí provádět odborné zkoušky (zkouška zvláštní odborné způsobilosti pracovníka kryptografické ochrany) a vydávat osvědčení o zvláštní odborné způsobilosti.

Česká republika Ministerstvo obrany
Tychonova 1, Praha 6
IČ: 60162694

Podle ustanovení § 45 odst. 4 zákona č. 412/2005 Sb. může Ministerstvo obrany zajišťovat činnosti spočívající v provádění dílčích úloh při ověřování způsobilosti podle § 46 odst. 1 písm. b) uvedeného zákona.

Podle § 39 odst. 3 písm. a) zákona č. 412/2005 Sb. může Ministerstvo obrany provádět odborné zkoušky (zkouška zvláštní odborné způsobilosti pracovníka kryptografické ochrany) a vydávat osvědčení o zvláštní odborné způsobilosti.

Česká republika Ministerstvo vnitra
Nad štolou 3, Praha 7
IČ: 00007064

Podle ustanovení § 45 odst. 4 zákona č. 412/2005 Sb. může Ministerstvo vnitra zajišťovat činnosti spočívající v provádění dílčích úloh při ověřování způsobilosti podle § 46 odst. 1 písm. b) uvedeného zákona.

Podle § 39 odst. 3 písm. a) zákona č. 412/2005 Sb. může Ministerstvo vnitra provádět odborné zkoušky (zkouška zvláštní odborné způsobilosti pracovníka kryptografické ochrany) a vydávat osvědčení o zvláštní odborné způsobilosti.

Intriple, a. s.
Podnikatelská 550, Praha 9, PSČ 190 11
IČ: 27448827

Podle ustanovení § 45 odst. 4 zákona č. 412/2005 Sb. může podnikatel Intriple, a.s. zajišťovat činnosti spočívající v provádění dílčích úloh při ověřování způsobilosti podle § 46 odst. 1 písm. b) a písm. e) uvedeného zákona.

Skybergtech, s. r. o
Tichonická 1329/52, 104 00 Praha 10
IČ: 25092235

Podle ustanovení § 45 odst. 4 zákona č. 412/2005 Sb. může podnikatel Skybergtech, s.r.o. zajišťovat činnosti spočívající v provádění dílčích úloh při ověřování způsobilosti podle § 46 odst. 1 písm. b) uvedeného zákona.

Vojenský technický ústav, s. p., odštěpný závod VTÚPV
V. Nejedlého 691, Dědice, Vyškov
IČ: 24272523

Podle ustanovení § 45 odst. 4 zákona č. 412/2005 Sb. může podnikatel Vojenský technický ústav, s. p., odštěpný závod VTÚPV zajišťovat činnosti spočívající v provádění dílčích úloh při ověřování způsobilosti podle § 46 odst. 1 písm. e) uvedeného zákona.

Minimální obsah bezpečnostní dokumentace pro malé informační systémy pro zpracování utajovaných informací

(verze 3.00)

Následující návod je určen pro informační systém pro nakládání s utajovanými informacemi, realizovaný na jednom nebo několika samostatných osobních počítačích nebo v lokální počítačové síti (LAN) malého rozsahu, v bezpečnostním provozním módu vyhrazeném nebo s nejvyšší úrovní, případně s nejvyšší úrovní s formálním řízením přístupu k informacím. Cílem je zejména usnadnit vytvoření koncepce zabezpečení a bezpečnostní provozní dokumentace pro účely certifikace informačního systému vlastními silami žadatele.

POZNÁMKA 1
Pro informační systém založený na použití jednoho nebo více samostatných osobních počítačů se vynechají části týkající se komunikací a jejich zabezpečení.

POZNÁMKA 2
Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění zákona č. 255/2011 Sb. je v dalším textu uváděn jako zákon č. 412/2005 Sb.

POZNÁMKA 3
Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb. je v dalším textu uváděna jako VYHLÁŠKA.

POZNÁMKA 4
Během certifikačního procesu poskytuje odbor informačních technologií žadatelům o certifikaci informačního systému potřebné konzultace, nastavení bezpečnostních charakteristik operačních systémů Windows, bezplatné měření kompromitujícího vyzařování, informace k bezpečnému používání USB zařízení, k možnostem bezpečného vymazávání informací, k možnostem kryptografické ochrany, k zabezpečení kabeláže LAN a pomoc při řešení dalších bezpečnostních problémů.

BEZPEČNOSTNÍ POLITIKA INFORMAČNÍHO SYSTÉMU

1. Úvod

Stručný popis informačního systému

Uvést

- počet samostatných osobních počítačů a zahrnutá periferní zařízení nebo stručně popsat LAN (předpokládaný rozsah, pracovní stanice, servery a jejich role, periferní zařízení, síťové tiskárny a skenery, logická topologie sítě, model komunikace aj.),
- nejvyšší stupeň utajení zpracovávaných informací,
- zvolený bezpečnostní provozní mód,
- základní účel zpracování utajovaných informací a aplikační SW,
- předpokládaný počet uživatelů,
- předpokládaný rozsah zpracování utajovaných informací,
- použitý operační systém (systémy),
- vztah k jiným počítačovým sítím (u samostatných osobních počítačů např. vyjmutí síťové karty, zákaz použití modemu, u LAN zpravidla izolace od jiných počítačových sítí),
- rámcově zásady pro umístění informačního systému z hlediska fyzické bezpečnosti, včetně aktivních prvků LAN a vedení datových rozvodů,
- u samostatných osobních počítačů, zda je pevný disk vyměnitelný nebo zabudovaný, u LAN případné použití vyměnitelných pevných disků v serverech a pracovních stanicích, využití bezdiskových pracovních stanic, terminálů apod.
- v případě záměru použití kryptografických prostředků uvést účel.

2. Bezpečnostní cíle

Uvést následující teze:

- Bezpečnostní cílem spojeným s využíváním informačního systému je zajištění důvěrnosti a integrity utajované informace všude, kde se vyskytuje, dostupnosti informace a služeb informačního systému a odpovědnosti uživatele informačního systému za jeho činnost v něm, dále nepopiratelnosti a pravosti informací, kde je to aplikovatelné.
- Zpracování utajovaných informací musí probíhat v souladu s požadavky zákona č. 412/2005 Sb. a s příslušnými vyhláškami NBÚ v platném znění.
- Uvedou se i další právní předpisy, normy, mezinárodní smlouvy a s nimi spjaté bezpečnostní požadavky, nadřízené bezpečnostní politiky, interní předpisy apod., které musí informační systém splňovat.

3. Personální bezpečnost (zákon č. 412/2005 Sb. a § 16, § 17, § 18 a § 19 VYHLÁŠKY)

- Deklarovat požadavky na uživatele:
  - splnění podmínek přístupu fyzické osoby k utajované informaci[1]) stupně utajení odpovídajícího nejvyššímu stupni utajení informace, která může být v informačním systému zpracovávána (§ 6 nebo § 11 zákona č. 412/2005 Sb.),
  - získání autorizace pro přístup k informacím prostřednictvím daného informačního systému,
  - další podle potřeb organizace.
- Deklarovat zavedení formálních postupů pro udělení oprávnění pro přístup do informačního systému, zavedení uživatele do informačního systému, pro včasné vyřazení uživatele při zániku jeho Osvědčení nebo Oznámení, změně jeho pracovního zařazení, odchodu z organizace apod. K tomu vedení seznamu oprávněných uživatelů informačního systému.
- Deklarovat, že povinnosti uživatelů budou stanoveny v bezpečnostní provozní dokumentaci informačního systému. Uživatelé budou pro svou činnost v informačním systému proškoleni, znalost dokumentace v příslušném rozsahu potvrdí před zavedením do informačního systému svým podpisem.
- Deklarovat zásadu, že přístup do informačního systému je založen na jedinečném identifikátoru uživatele v rámci informačního systému. V případě potřeby používání společného účtu pro více uživatelů uvést její zdůvodnění a deklarovat, že bude zaveden postup umožňující určit, který uživatel/bezpečnostní správce/správce informačního systému v dané době daný identifikátor používal (předpokládá se zejména ve stálém provozu na operačních střediscích).
- Uvést požadované funkce pro správu informačního systému:
  - Funkce (role) bezpečnostního správce, předpokladem je splnění podmínek pro přístup fyzické osoby k utajované informaci minimálně pro nejvyšší stupeň utajení informace, zpracovávané v informačním systému. Povinnosti bezpečnostního správce informačního systému budou uvedeny v příslušné bezpečnostní směrnici. Uvést, zda je požadováno splnění požadavků pro přístup fyzické osoby k utajované informaci vyššího stupně utajení (§ 16 odst. 3 VYHLÁŠKY), pokud ne, odůvodnit.
  - Funkce (role) správce informačního systému (administrátor spravující operační systémy a aplikační programové vybavení, síťové prostředí, případně provádějící jednoduchou HW údržbu), předpokladem je splnění podmínek pro přístup fyzické osoby k utajované informaci minimálně pro nejvyšší stupeň utajení informace, zahrnuté v informačním systému. Povinnosti správce informačního systému budou uvedeny v příslušné bezpečnostní směrnici. Uvést, zda je požadováno splnění požadavků pro přístup fyzické osoby k utajované informaci vyššího stupně utajení (§ 16 odst. 4 VYHLÁŠKY), pokud ne, odůvodnit.
  - Deklarovat případné sloučení obou funkcí a odůvodnit je.
  - V případě informačního systému sestávajícího ze samostatných pracovních stanic rozmístěných v různých lokalitách, zajištění centrální a lokální správy informačního systému.
  - V případě potřeby, např. při využívání kryptografické ochrany utajovaných informací nebo správě komunikační části LAN zavedení dalších funkcí (rolí).
  - Zajištění zástupnosti v bezpečnostní správě a správě informačního systému.

[1]) Zahrnuje držení oznámení nebo osvědčení, poučení a dodržení zásady „need-to-know“.

4. Splnění minimálních požadavků počítačové bezpečnosti

Uvést minimální bezpečnostní požadavky počítačové bezpečnosti podle § 7 a § 8 VYHLÁŠKY, podle zvoleného bezpečnostního provozního módu a nejvyššího stupně utajení:

- Jednoznačná identifikace a autentizace uživatele
  - prostředky operačního systému s vhodným nastavením bezpečnostních parametrů – minimální délka hesla 8 znaků, doba platnosti hesla zpravidla maximálně 6 měsíců, uzamčení stanice nejdéle po 30-ti minutové nečinnosti, povolení nejvýše tří neplatných pokusů o přihlášení během 60 minut, nepovolit opakování posledních nejméně 3 hesel uživatele, vynucení změny hesla přiděleného administrátorem při prvém přihlášení uživatele do systému, atd.
  - případně dále i na aplikační úrovni (vstup do kritické aplikace),
  - se zajištěním re-autentizace uživatele po stanovené době nečinnosti nebo krátkodobém opuštění zapnutého samostatného osobního počítače nebo pracovní stanice,
  - se zajištěním ochrany důvěrnosti a integrity autentizační informace během přenosu sítí.
- Volitelné řízení přístupu k objektům informačního systému
  - prostředky operačního systému,
  - případně dále na aplikační úrovni,
  - v bezpečnostním provozním módu vyhrazeném uplatnit pouze požadavek oddělení uživatelů od systémových souborů a prostředků a správců systému (pokud nejsou zároveň uživateli informačního systému) od uživatelských dat,
  - v bezpečnostním provozním módu s nejvyšší úrovní pravidla pro řízení přístupu k objektům informačního systému (např. vytvoření domovských, adresářů pro jednotlivé uživatele v jejich vlastnictví, skupiny uživatelů a vytvoření sdílených adresářů pro skupiny uživatelů, přistup k aplikačnímu SW …), vhodné oddělení uživatelů od systémových souborů a prostředků a správců systému (pokud nejsou zároveň uživateli informačního systému) od uživatelských dat,
  - v bezpečnostním provozním módu s nejvyšší úrovní s formálním řízením přístupu k informacím způsob realizace centrální správy řízení přístupu.
- Vytváření auditních záznamů, jejich ochrana a zkoumání
  - prostředky operačního systému s vhodným nastavením bezpečnostních parametrů – zpravidla zaznamenávat úspěšné i neúspěšné pokusy o přihlášení do systému, správu uživatelů a skupin, změnu v metodě zabezpečení a neúspěšné pokusy o přístup k souborům a objektům, o použití přístupových práv, selhání restartu a vypnutí nebo sledování procesu,
  - pokud operační systém neumožňuje automatické vytváření auditních záznamů, mohou být ve výjimečných případech nahrazeny manuální evidencí, umožňující jednoznačně určit, který uživatel a kdy v systému pracoval – např. uživatel se zapíše (nebo je zapsán a potvrdí svou přítomnost podpisem) do provozního deníku s datem a dobou práce v informačním systému; politika určí rámcově i způsob vedení takových evidencí, jejich ochranu před modifikací nebo zničením, dobu archivace apod.; může jít o evidenci fyzického vstupu do místnosti, převzetí výměnného HDD apod.; použitelné výlučně pro samostatná PC,
  - případné vytváření auditních záznamů i na aplikační úrovni,
  - zásada omezení přístupu uživatelů k auditním záznamům, spravovány jsou bezpečnostním správcem; politika také určuje, jak často se mají kontrolovat auditní záznamy, v jaké formě, kde a jak dlouho mají být uchovávány pro zpětné zkoumání, kdo má přístup k auditním záznamům; zpravidla se vyžaduje kontrola nejméně jednou měsíčně a pořizování záložních kopií auditních záznamů a jejich uchovávání takovým způsobem, aby byly přístupné pro zpětné zkoumání po dobu nejméně 3 let, přičemž po celou dobu musí být chráněny před modifikací a zničením.
- Opakované použití objektů – je řešeno operačním systémem (*řeší systémy Microsoft Windows od W NT 4.0 výše, UNIXové systémy*), pro počítačová média stanovením pravidel pro deklasifikaci a ničení médií.

5. Komunikační bezpečnost (pouze pro LAN, § 9 VYHLÁŠKY)

Zabývat se zejména následujícími oblastmi:

- způsob ochrany důvěrnosti a integrity informací během přenosu v LAN
  – prostředky fyzické bezpečnosti podle odst. 4 § 9 VYHLÁŠKY nebo

– nasazením kryptografického prostředku certifikovaného pro ochranu utajovaných informací[2]) stupně utajení odpovídajícího stupni utajení chráněné informace nebo vyššího podle odst. 6 § 9 VYHLÁŠKY nebo
– záměr využití odst. 7 § 9 VYHLÁŠKY a jeho odůvodnění,

- zásady pro I&A v síťovém prostředí a ochranu přístupových hesel (*fyzická ochrana linek a jejich pravidelná kontrola, kryptografický prostředek, pokročilá autentizační technika zajišťující šifrování hesel nebo využívající heslo na jedno použití apod.*),
- zásady pro ochranu síťových prvků, jako jsou rozbočovače, mosty, přepínače, směrovače (fyzická ochrana, manuální plnění tabulek a statický režim),
- zásady pro připojení LAN k externím sítím (ve většině případů úplná izolace LAN, vyloučení propojení na Internet, zákaz modemových připojení, zákaz WiFi apod.),
- požadavky na používání utilit pro správu LAN, kontrolu integrity SW vybavení apod.,
- pro síťové protokoly a služby uplatňovat zásadu „co není explicitně povoleno, je zakázáno“.

Zásadou je, že datové rozvody pro přenos utajovaných informací v otevřeném (nezašifrovaném) tvaru je nutno vést tak, aby vycházely mimo zabezpečené oblasti kategorie odpovídající stupni utajení chráněné informace jen v dobře odůvodněných situacích (např. nepřiměřené náklady, technické důvody). Nešifrované sekce mimo odpovídající zabezpečenou oblast mají být co nejkratší a být vedeny objektem odpovídající kategorie, zabezpečenou oblastí jiné kategorie nebo objektem jiné kategorie. K této problematice je zpracováván jiný metodický materiál.

6. Kryptografická ochrana

Tato část se zařazuje pouze v případě, že bude v informačním systému provozován kryptografický prostředek certifikovaný podle zákona č. 412/2005 Sb. Je třeba uvést, zda kryptografický prostředek bude použit pro ochranu utajované informace uložené na počítačovém médiu nebo pro ochranu komunikací a deklarovat zajištění souladu se zákonem č. 412/2005 Sb. a vyhláškou č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb.

7. Požadavky na dostupnost (§ 10 VYHLÁŠKY).

Rozvést požadavky na dostupnost informace a služeb informačního systému – v čase a místě, jak dlouho smí být služby nedostupné, jaká minimální funkčnost musí být zajištěna i v krizových situacích, redundance HW a SW, plánování kapacit, plán obnovení činnosti informačního systému po havárii …

8. Analýza rizik a další bezpečnostní opatření (§ 11 VYHLÁŠKY)

Na základě analýzy rizik stanovit další bezpečnostní opatření, pro vnější hrozby nepokryté již identifikovanými požadavky a případně sílu mechanismů, kterými mají být (vzhledem ke zvýšenému riziku) bezpečnostní funkce realizovány (např. identifikace a autentizace nikoliv jen na základě uživatelského jména a hesla, ale pomocí tokenu).

Jednou z hrozeb specifických pro osobní počítač je, že k němu neoprávněná osoba získá fyzický přístup i přes použitá opatření fyzické bezpečnosti a poté buďto odcizí, poškodí nebo zničí počítačové médium s utajovanými informacemi nebo HW vybavení, získá logický přístup do systému (např. nabootování z externího média) umožňující narušení systémového a aplikačního programového vybavení a manipulaci s utajovanými informacemi, získá informaci uloženou na zcizeném pevném disku přímo nebo speciálními prostředky v případě zbytkových informací.

V souvislosti s tím je nutno pro samostatný osobní počítač nebo pracovní stanici vyřešit (adekvátně skutečné úrovni rizik)

- ochranu utajované informace, která by zůstala uložena v počítači, je-li ponechán buďto po určitou dobu zapnutý bez obsluhy autorizovaného uživatele nebo vypnutý po ukončení práce v informačním systému (neoprávněné odkrytí, modifikace, zničení utajované informace, tedy ohrožení důvěrnosti, integrity a dostupnosti utajované informace),
- ochranu integrity HW (neoprávněná modifikace, např. vložení škodlivé komponenty, zničení, tedy ohrožení důvěrnosti, integrity a dostupnosti utajované informace a dostupnosti služeb systému),
- ochranu integrity operačního systému (neoprávněné vložení škodlivého kódu, modifikace systémo-

[2]) Zákon č. 412/2005 ve znění pozdějších předpisů, § 37.

vých souborů apod., tedy ohrožení důvěrnosti, integrity a dostupnosti utajované informace a dostupnosti služeb systému),

- ochranu integrity aplikačního SW – podobně jako operačního systému,
- ochranu utajovaných informací uložených na výměnných počítačových médiích,
- ochranu USB portů.

Pro LAN je nutno zabývat se dále riziky spjatými se serverem, dalšími aktivními prvky sítě a samotnou kabeláží, zejména vyřešit adekvátní

- ochranu LAN před fyzickým poškozením nebo neoprávněnou modifikací kabeláže a odposlechem na linkách (přenášené informace, autentizační informace),
- ochranu rozbočovačů, mostů, přepínačů, směrovačů před fyzickým poškozením a neoprávněnou modifikací jejich konfigurace,
- ochranu integrity HW serveru, integrity operačního systému i aplikačního SW na serveru, podobně jako pro samostatný osobní počítač,
- ochranu autentizační informace přenášené v LAN,
- ochranu utajovaných informací přenášených v LAN,
- ochranu utajovaných informací uložených na pevných discích (diskovém poli) serveru.

Během analýzy rizik je třeba zvažovat, pro jaké možné útočníky mají zpracovávané utajované informace hodnotu a jaký typ útoku by pravděpodobně byli schopni a ochotni podniknout, případně **určit zbytkové riziko a jeho přijatelnost z hlediska jeho možného dopadu a nápravy vzniklých škod**.

Na základě analýzy rizik musí být stanoveny bezpečnostní požadavky jako je zahrnutí nadstandardních prvků fyzické bezpečnosti, použití bezdiskových pracovních stanic, pracovních stanic a samostatných PC s výměnnými HDD, serverů s výměnnými HDD, pokročilých technik identifikace a autentizace, **kryptografické ochrany utajovaných informací uložených na pevných discích nebo přenášených komunikačními kanály (certifikovanými kryptografickými prostředky zajišťujícími deklasifikaci utajovaných informací nebo necertifikovanými prostředky jako doplňkové opatření)**, statický režim (statické adresní tabulky) pro huby, switche, routery apod.

Analýza rizik ovlivňuje také míru požadavků na ochranu v oblasti kompromitujícího elektromagnetického vyzařování, zejména v případě zpracování informací stupně utajení Důvěrné.

9. Fyzická bezpečnost

Uvést zásady fyzického zabezpečení informačního systému v závislosti na tom, zda na daném zařízení se informace pouze zpracovávají a zobrazují nebo i ukládají (VYHLÁŠKA a vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb.) a na výsledcích analýzy rizik.

- Použití bezdiskových pracovních stanic, pracovních stanic a osobních počítačů s výměnnými HDD, kryptografické ochrany apod. snižuje nutnou úroveň fyzického zabezpečení.
- Jsou-li používány pracovní stanice nebo servery se zabudovaným pevným diskem, na který jsou ukládány utajované informace (nebo nelze jejich uložení v pracovních oblastech disku vzhledem k používanému SW vyloučit) pak musí být tyto počítače umístěny v zabezpečené oblasti kategorie odpovídající stupni utajení jejího pevného disku, přičemž tato zabezpečená oblast musí splňovat standardy NBÚ pro fyzickou bezpečnost pro případ, že v ní jsou utajované informace ukládány v informačním systému (viz Příloha č. 1 k vyhlášce č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků ve znění vyhlášky č. 454/2011 Sb., kapitoly 12 a 13, Příloha č. 3 k VYHLÁŠCE). Tento požadavek platí i pro k nim připojená disková pole.
- Neopomenout stanovit zásady fyzické ochrany pro datové rozvody LAN a aktivní prvky sítě a pro kontrolu jejich neporušenosti.
- Na základě analýzy rizik stanovit opatření jako je pečetění HW, použití ochranných skříní pro HW, zvýšené požadavky fyzické bezpečnosti pro serverovnu (nadstandardní prvky vzhledem ke stupni utajení informací) apod.
- Uvést požadavek ochrany zařízení před riziky prostředí (prach, voda, oheň, živelní katastrofa atd., podle analýzy rizik).
- Fyzickou bezpečnost pro informační systém je nutno popsat, nebo uvést odkaz na jinou dokumentaci (např. schválený projekt fyzické bezpečnosti objektu), která ovšem musí být přístupná NBÚ i uživatelům podle potřeby.
- Uvést požadavek, že výpočetní technika musí být umístěna tak, aby bylo znemožněno odezírání utajovaných informací z obrazovek, klávesnic a periferních zařízení nepovolanými osobami.

- Je třeba zahrnout také požadavek označit zařízení náležející do určitého informačního systému štítkem s identifikací tohoto informačního systému a nejvyšším stupněm utajení informací, které mohou být v daném informačním systému zpracovávány.

Komentář

Soubor bezpečnostních požadavků pro určitý informační systém se vytváří z minimálních bezpečnostních požadavků, z požadavků vyplývajících z použitého bezpečnostního provozního módu a z nejvyššího stupně utajení utajovaných informací, který může být v informačním systému zpracováván, a z požadavků odvozených z analýzy rizik provedené pro tento informační systém (nebo typ informačního systému).

Fyzickou bezpečností pro informační systémy se rámcově zabývá § 20 VYHLÁŠKY. Podle něho se během certifikace informačního systému stanovuje, které komponenty informačního systému musí být umístěny v zabezpečené oblasti nebo objektu a jejich kategorie.

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. a vyhlášky č. 454/2011 Sb., stanoví bodové ohodnocení jednotlivých opatření fyzické bezpečnosti a **nejnižší** míru zabezpečení zabezpečené oblasti. Bodové ohodnocení parametrů SS1 a SS2 pro komponenty informačního systému je uvedeno v příloze č. 3 VYHLÁŠKY.

O konkrétní realizaci zvýšení úrovně fyzické bezpečnosti se potom rozhoduje v rámci certifikace informačního systému, vhodné řešení se hledá s uvážením charakteru zpracovávaných utajovaných informací a se snahou o co nejnižší dodatečné náklady, s přihlédnutím k možnostem žadatele o certifikaci.

Zabezpečené oblasti všech kategorií jsou v rámci bezpečnostní prověrky podnikatele často hodnoceny ještě bez zahrnutí možnosti, že v nich bude umístěn informační systém, který vyžaduje certifikaci.

10. Kompromitující vyzařování

Komentář

Požadavkem ochrany informačního systému proti úniku utajovaných informací prostřednictvím kompromitujícího vyzařování se zabývá § 14 zákona č. 412/2005 Sb. Jeho současné znění je následující:

Odst. 1: Komponenty informačního systému, které nakládají s utajovanými informacemi stupně utajení Důvěrné nebo vyššího a zabezpečená oblast nebo objekt, ve kterém se v informačním systému zpracovávají utajované informace stupně utajení Důvěrné nebo vyššího, musí být zabezpečeny takovým způsobem, aby kompromitující vyzařování nezpůsobilo únik utajované informace.

Odst. 2: Požadavky na zabezpečení proti kompromitujícímu vyzařování jsou závislé na stupni utajení utajované informace, se kterou informační systém nakládá a jsou stanoveny v bezpečnostním standardu.

Odst. 3: Instalace informačního systému, který nakládá s utajovanou informací stupně utajení Důvěrné nebo vyššího, z hlediska jeho zabezpečení proti kompromitujícímu vyzařování musí být provedena v souladu s požadavky bezpečnostního standardu. Záznam o instalaci komponent informačního systému se vkládá do bezpečnostní dokumentace informačního systému. Obsah a forma záznamu jsou stanoveny v bezpečnostním standardu.

V současné době jsou v platnosti 2 standardy NBÚ pro tuto oblast – Bezpečnostní standard NBÚ-1/2007, Klasifikace prostorů z hlediska kompromitujícího elektromagnetického vyzařování, verze 1.0 z roku 2007 a Bezpečnostní standard NBÚ-2/2007, verze 2 z roku 2011, Instalace zařízení z hlediska kompromitujícího elektromagnetického vyzařování. Oba tyto standardy jsou klasifikovány stupněm utajení Důvěrné a jsou šířeny přísně podle zásady „need-to-know“. Dále jsou využívány utajované standardy NATO a EU.

Problematikou se zabývají také § 30 až § 36 VYHLÁŠKY.

Kompromitující vyzařování je elektromagnetické, akustické nebo optické vyzařování elektrických a elektronických zařízení, které by mohlo způsobit únik utajované informace. S definicí kompromitujícího vyzařování úzce souvisí termín TEMPEST, což je odborný termín vztahující se ke zjišťování a zkoumání kompromitujícího elektromagnetického vyzařování, což jsou vlastně neúmyslně vyzářené elektromagnetické signály, které, pokud jsou zachyceny a analyzovány, mohou odhalit (prozradit) obsah zpracovávané informace (např. zobrazované na monitoru nebo tištěné na tiskárně).

Elektronická zařízení vzhledem ke své konstrukci a použité technologii jsou citlivá na vnější rušení a sama také elektromagnetickou energii (rušení) vyzařují. Pokud elektronická zařízení (která jsou vždy součástí informačních systémů) zpracovávají informace, může jimi vyzařovaná energie v sobě nést zpracovávanou informaci.

Proto u informačních systémů, které zpracovávají utajované informace, je třeba při jejich návrhu, instalaci a provozu dodržet jistá pravidla, která snižují riziko úniku utajované informace formou tohoto kompromitujícího elektromagnetického vyzařování.

V ČR je aplikován tzv. „zónový princip“, při němž se hodnotí jednak jednotlivé komponenty nebo celý

informační systém (tzv. třída zařízení – 0, 1 nebo 2) a dále prostory, ve kterých je informační systém umístěn (tzv. zóna – 0, 1 nebo 2). Bezpečnostní standardy stanoví pro zpracování utajované informace v závislosti na jejím stupni utajení možné kombinace třídy zařízení a zóny prostoru, v němž je umístěno.

Již v etapě záměru vybudovat informační systém pro zpracování utajovaných informací stupně utajení Důvěrné nebo vyššího je doporučováno vybrat vhodně prostory pro jeho umístění. Je nutné zohlednit nejen požadavky na fyzickou bezpečnost, ale také požadavky na TEMPEST. Vhodně zvolené umístění informačního systému například i v rámci jedné budovy, může znamenat lepší zónu daného prostoru a snižuje tak požadavky na třídu použitých prostředků a tím **výrazně** i finanční náklady.

Kromě toho existují i požadavky na rozmístění komponent informačního systému v rámci vybraného prostoru. Tyto požadavky jsou uvedeny v bezpečnostních standardech NATO, EU a NBÚ a udávají především požadované vzdálenosti informačního systému od ostatních metalických vedení (např. telefonní linky, silová a signálová vedení, vytápění, klimatizace aj.) a jiných elektronických zařízení, které je nutné dodržovat.

Hodnocení zařízení a prostorů provádí v NBÚ pracoviště TEMPEST na základě vlastních měření nebo měření provedených na odborném pracovišti, se kterým má/bude mít NBÚ uzavřenou smlouvu o provádění takových činností (podle zákona č. 412/2005 Sb.). Na pracovišti TEMPEST je k dispozici seznam dodavatelů zařízení třídy 0 a stínicích komor. Tato zařízení však vždy musí být podrobena kontrolnímu měření a odsouhlasena NBÚ.

Jako podklad pro hodnocení zóny, v níž má být umístěn informační systém pro nakládání s utajovanými informacemi stupně utajení Důvěrné nebo vyššího, je třeba dodat popis (včetně plánku) umístění informačního systému vzhledem k místům, kde by mohlo být nepozorovaně umístěno nepřátelské zařízení pro detekci elektromagnetického vyzařování (většinou se jedná o veřejná parkoviště a prostory které nepatří provozovateli informačního systému). Tento popis by měly zahrnovat všechny prostory sousedící s místností, kde je informační systém instalován, jak v horizontální tak i vertikální linii a pokud je informační systém v místnosti s okny, popsat prostor ve směru oken a to do vzdálenosti minimálně 100 metrů od informačního systému. Rovněž je třeba popsat předpokládaný rozsah zpracovávání utajovaných informací a jejich časové rozložení. Pro posouzení rizika není rozhodující množství utajovaných informací uložených v informačním systému, ale množství a charakter zpracovávaných utajovaných informací a rozsah, charakter a časové rozložení zpracovávání těchto informací. Riziko z hlediska TEMPEST je spjato především se zobrazováním utajovaných informací na monitoru, jejich vkládáním pomocí klávesnice, tiskem a vypalováním na CD či DVD. Z hlediska časového rozložení je vyšší riziko spjato s pravidelným zpracováváním utajovaných informací nebo zpracováním, jehož zahájení může útočník odvodit z určitých příznaků.

Pracoviště TEMPEST provádí i poradenskou činnost v oblasti kompromitujícího vyzařování.

10.1 Základní požadavky na informační systém podle standardů NBÚ

Při zpracovávání utajovaných informací stupně utajení Vyhrazené nejsou požadována (kromě Prohlášení o shodě, kterým se dokládá splnění požadavků na elektrickou bezpečnost a elektromagnetickou kompatibilitu (EMC) podle zákona č. 22/1997 Sb. o technických požadavcích na výrobky a o změně a doplnění některých zákonů.) žádná opatření v oblasti kompromitujícího vyzařování (KV).

V případě zpracovávání utajovaných informací stupně utajení Důvěrné se rovněž přihlíží k charakteru organizace provozující daný informační systém a charakteru zpracovávaných informací, rozsahu zpracovávání utajovaných informací stupně utajení Důvěrné, časovému rozložení a způsobu jejich zpracovávání. Pokud dochází ke zpracovávání utajovaných informací týkajících se krizového plánování, činnosti zpravodajských služeb, činnosti a zabezpečení zastupitelských úřadů a jiných důležitých objektů, kryptografické ochrany utajovaných skutečností, operativní techniky, vojenského a jaderného materiálu a dalších kritických oblastí, je třeba bez ohledu na jejich množství aplikovat přísnější požadavky.

U informací stupně utajení Důvěrné posoudí pracovník OIT NBÚ z dokumentace předložené k certifikaci informačního systému nebo přímo na místě, zda se bude provádět zónové měření.

Předpokládá-li se zpracovávání utajovaných informací stupně utajení Tajné nebo Přísně tajné, provede se zónové měření zpravidla vždy.

Pokud jsou zpracovávány utajované informace stupně utajení Důvěrné, Tajné nebo Přísně tajné, vyžaduje se u některých instalací, určených v bezpečnostních standardech, napájení ze síťového přívodu vybaveného vysokofrekvenčním filtrem. Pro zpracování utajovaných informací stupně utajení Důvěrné je nutné použít vhodný typ s útlumem minimálně 30dB v kmitočtovém pásmu 100 kHz – 1 GHz. Pro zpracování utajovaných informací stupně utajení Tajné nebo Přísně tajné je nutná konzultace s odborným pracovištěm OIT NBÚ. K využití útlumových vlastností zapojených filtrů je nutná jejich odpovídající instalace (patřičné oddělení vodičů vstupní a výstupní části).

V případě, že informační systém obsahuje vysílač (radiostanice, radiomodem, Wi-Fi, infračervený přenos aj.), je třeba vždy konzultace s pracovištěm OIT NBÚ.

Požadovaná opatření se pak u požadavků na zařízení pohybují od doložení splnění elektromagnetické kompatibility pro jednotlivé komponenty informačního systému případně použití komponent s nižší úrovní kompromitujícího elektromagnetického vyzařování až po použití "tempestovaných" zařízení. U požadavků na zlepšení zóny se jedná o přemístění informačního systému nebo použití stínicích komor případně stíněných místností.

Pro LAN je nutno zahrnout do úvah i kabeláž a aktivní prvky sítě. V této oblasti je opět nutné posouzení NBÚ. U nově budovaných sítí pro stupeň utajení Důvěrné a vyšší doporučujeme konzultovat v NBÚ již ve fázi záměru, jaká bezpečnostní opatření jsou vyžadována.

10.2 Požadovaná specifikace způsobu ochrany v bezpečnostní politice

V bezpečnostní politice je třeba minimálně stanovit, že elektronická zařízení informačního systému budou splňovat požadavky bezpečnostních standardů NBÚ v oblasti kompromitujícího vyzařování.

Podle úrovně aktuálně známých informací (v době tvorby prvé verze bezpečnostní politiky informačního systému) se dále uvádí:

- zóna pro prostor, v němž bude informační systém umístěn,
- pro stupeň utajení Důvěrné předpokládaný rozsah zpracovávání utajovaných informací a jejich časové rozložení a z hlediska provozovatele posoudit riziko spjaté s hrozbou útoku využívajícího k získání utajovaných informací kompromitujícího elektromagnetického vyzařování,
- navržený způsob ochrany v oblasti kompromitujícího vyzařování, s uvážením požadavků uvedených v odstavci 10.1 a Komentáři (např. „pro zpracování utajovaných informací do stupně utajení Tajné, v počítačové místnosti nacházející se v zóně 1, bude použito zařízení třídy y“, nebo „ v zóně 0 bude použito tempestované zařízení“, „bude použita stínicí komora“ apod.),
- v případě LAN požadavky pro kabeláž (např. optické kabely) a pro prvky síťové infrastruktury.

11. Administrativní bezpečnost, bezpečnost počítačových médií

- Deklarovat splnění požadavků vyhlášky č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění pozdějších předpisů.
- Deklarovat požadavky na bezpečnost počítačových médií podle § 15 VYHLÁŠKY (tzv. provozní nosiče informací), uvést stupeň utajení těchto médií vzhledem k bezpečnostnímu provoznímu módu vyhrazenému nebo s nejvyšší úrovní/nejvyšší úrovní s formálním řízením přístupu k informacím.
- Uvést, jaká počítačová média pro ukládání utajovaných informací budou používána, zásady pro jejich evidenci, označování stupněm utajení, ukládání, ničení (viz aktuální standardy NBÚ v příloze vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů).
- Uvést, jaká počítačová média budou používána pro vstup/výstup informací do/z informačního systému a požadavky na řízení přístupu uživatelů k příslušným mechanikám/portům; zejména v případě USB paměťových zařízení.
- V případě používání vyměnitelných pevných disků v multiuživatelském prostředí uvést způsob zajištění nepřetržité odpovědnosti.
- Uvést zásady pro vyřazování počítačových médií z provozu informačního systému (porouchané nebo poškozené pevné disky, poškozené diskety, CD, ZIP, pásky aj.) nebo v případě likvidace informačního systému, zajišťující, že médiu je poskytována ochrana podle jeho stupně utajení až do doby komisionelního zničení.

POZNÁMKA 5

Počítačová média, která jsou používána výhradně pro potřeby provozu informačního systému, např. vyměnitelné pevné disky, CD/DVD, ZIP, pásky a další média používaná pro zálohování v informačním systému mají být evidována v administrativní pomůcce vytvořené pro tento účel. Jednotlivému počítačovému médiu pak musí být přiděleno jedinečné evidenční číslo a stupeň utajení a musí pro ně být uveden typ média, jeho výrobní číslo (pokud je médiem neseno), datum uvedení do provozu informačního systému, datum vyřazení z provozu. Na popisném štítku se pak vyznačí stupeň utajení média, jeho evidenční číslo, název organizace/orgánu státu provozujícího informační systém a název informačního systému. Je vhodné, aby tuto evidenci vedla osoba pověřená vedením jednacího protokolu nebo bezpečnostní správce informačního systému.

Nosiče utajovaných informací používané rutinně v bezpečnostním provozním módu vyhrazeném nebo

s nejvyšší úrovní budou klasifikovány nejvyšším stupněm utajení, s nímž daný informační systém nakládá. Tím není vyloučen export informací nižšího stupně utajení nebo neutajovaných, pokud uživatel kvalifikovaně posoudí stupeň utajení určité dílčí informace nebo je nižší stupeň utajení určitého typu informace stanoven v bezpečnostní dokumentaci, a poté takovou informaci uloží na nosič příslušného stupně utajení nebo neutajovaný.

V § 15 VYHLÁŠKY je v odst. 8 zdůrazněna potřeba zajistit informační systémy proti neoprávněnému importu/ exportu utajovaných informací, zejména při použití velkokapacitních vyměnitelných počítačových médií, tím, že již v bezpečnostní politice informačního systému (a tím i v návrhu bezpečnosti a bezpečnostních směrnicích informačního systému) je specifikováno řízení přístupu uživatele ke vstupním a výstupním zařízením.

POZNÁMKA 6

Evidenci a označení jako utajovaná informace podléhají i zabudované pevné disky. V případě obtížné realizace tohoto opatření je možno omezit se v odůvodněných případech na neprodlené zaevidování a označení pevného disku odpovídajícím stupněm utajení po vyjmutí z počítače (porucha, výměna), což mu zajistí adekvátní ochranu v další fázi jeho života.

- Deklarovat, že počítače/jiná zařízení obsahující zabudované pevné disky/jiné nevolatilní paměti budou evidovány v provozní bezpečnostní dokumentaci informačního systému (je-li to relevantní).
- Deklarovat, že utajovaná informace, která vystupuje z informačního systému, musí být označena odpovídajícím stupněm utajení, způsobem zaručujícím adekvátní nakládání s touto informací. Uvést, že tiskové výstupy musí být bez odkladu evidovány jako utajovaná písemnost. Uvést zásady pro import a export utajovaných informací do/z informačního systému na počítačových médiích, v souladu s principy bezpečnostního provozního módu. Výstupem z informačního systému se neníní uložení na tzv. provozní počítačová média, používaná výhradně v provozu informačního systému.

12. Další bezpečnostní dokumentace

Deklarovat, že bude vypracován návrh bezpečnosti informačního systému a zpracovány bezpečnostní směrnice informačního systému, jak budou členěny (např. pro bezpečnostního správce informačního systému, pro správce informačního systému, pro uživatele, pro oblast kryptografické ochrany apod.).

13. Požadavky bezpečného provozu

Uvést zejména následující bezpečnostní požadavky (převážně uvedeny v § 23 VYHLÁŠKY):

- zajištění antivirové ochrany,
- dodržování schválené konfigurace HW a SW (správa konfigurace),
- bezpečné uložení hlavních kopií SW vybavení (znemožnění modifikace nebo zničení),
- systém zálohování souborů s utajovanými informacemi, případně programového vybavení, záložní média, odpovědnost za vytváření záloh (server, pracovní stanice apod.),
- povinnost evidovat záložní počítačová média, jejich stupeň utajení (daný nejvyšším stupněm utajení, s nímž informační systém nakládá), jejich ukládání,
- zajištění požadavků § 22 VYHLÁŠKY pro fázi instalace informačního systému,
- zajištění instalačních záznamů a dodržování v nich schválené konfigurace a rozmístění komponent informačního systému během jeho provozu (§ 14 odst. 3 VYHLÁŠKY),
- pro informační systémy nakládající s utajovanou informací stupně utajení Tajné nebo vyššího zajištění obranně technické prohlídky (§ 23 odst. 9 VYHLÁŠKY),
- zajištění požadavků § 23 odst. 5 a 6 VYHLÁŠKY v oblasti servisní činnosti; deklarovat, že bude prováděna tak, aby nemohlo dojít k neoprávněnému přístupu k utajovaným informacím nebo narušení integrity HW nebo SW vybavení vedoucímu ke kompromitaci utajovaných informací, že o každé opravě bude pořízen zápis, záznamy budou uchovávány nejméně po dobu …… let, uvést zda opravy budou zajišťovány pracovníky organizace nebo pracovníky externími (volba servisní organizace); u komponent informačního systému, které obsahují paměti typu RAM (např. tiskárny apod.), je nutné počítat s tím, že informace v těchto pamětech mohou zůstávat i po odpojení napájecího napětí. Tomu je třeba přizpůsobit režim zacházení s těmito komponentami. V případě odeslání do servisu nebo jiné manipulace, kdy nebude zařízení pod dohledem odpovědné osoby, je třeba obsah paměti přepsat neutajovanými informacemi,

- zajištění postupu pro autorizaci uživatele a pracovníků bezpečnostní správy a správy informačního systému pro činnost v informačním systému,
- zajišťování úvodního a periodického školení uživatelů,
- zásady administrace pracovní stanice a síťového serveru (lokální, vzdálená) a odpovídající bezpečnostní opatření,
- opatření pro přijímání návštěv – např. že návštěvy mají přístup do místnosti s informačním systémem pouze za doprovodu oprávněného uživatele po schválení bezpečnostním správcem informačního systému a zápisu do knihy návštěv, že nesmí dojít k odezírání utajovaných informací, že jiným prověřeným osobám s need-to-know lze umožnit přístup za přítomnosti oprávněného uživatele…..,
- základní krizové (havarijní) situace - vyjmenovat, které situace je třeba ošetřit (oheň-kouř-výbuch, voda - záplavy či prosakování tekutin, výpadek proudu, porucha HW (včetně narušení kabeláže), selhání SW, problémy s konstrukcí budov, přírodní katastrofa, sabotáž - terorismus a další). O výskytu každé mimořádné situace a jejím vyřešení se pořídí zápis a uloží se po dobu …, kde ..,
- povinnost bezpečnostního správce zkoumat auditní záznamy jedenkrát týdně (měsíčně, denně) a vždy po bezpečnostním incidentu či podezření na něj, vytváření kopií auditních záznamů a jejich uložení tak, aby byly přístupné pro zpětné zkoumání po dobu nejméně ... roků, se zajištěním jejich integrity; pokud je v auditních záznamech nalezen příznak bezpečnostního incidentu, vypracuje bezpečnostní správce záznam a tento bude uchováván po dobu nejméně …, udat také kde,
- základní seznam bezpečnostních incidentů - projev počítačového viru nebo jiného zlomyslného SW, kompromitace hesla/PINu čipové karty k autentizaci uživatele nebo podezření na ni, ztráta počítačového média, čipové karty k autentizaci uživatele nebo listinné utajované písemnosti nebo podezření na ni, proniknutí nepovolané osoby do místnosti s informačním systémem nebo pokusy o ně, hlášení auditu operačního systému (nebo aplikačního SW), neobvyklé chování některého uživatele informačního systému nebo neobvyklý postup uplatněný v informačním systému, neoprávněná změna HW nebo SW konfigurace informačního systému, pro LAN narušení kabeláže, neúmyslné nebo úmyslné vyzrazení utajovaných informací neoprávněné osobě, nedodržení předpisu o ukládání výměnného pevného disku nebo přenosného počítače do úschovného objektu aj.,
- že incidenty budou uživateli hlášeny bezpečnostnímu správci, který je vyhodnotí, komu je ohlásí dále, že o jejich výskytu a vyřešení bude pořízen zápis, že bude archivován pod dobu nejméně ….., kde bude uložen,
- zajištění školení uživatelů o jejich povinnostech v oblasti bezpečnosti,
- další bezpečnostní požadavky podle potřeb uživatelů, vnitřních předpisů organizace, nadřízených bezpečnostních politik, mezinárodních smluv aj., vše co je nad rámec VYHLÁŠKY.

NÁVRH BEZPEČNOSTI INFORMAČNÍHO SYSTÉMU

Návrh bezpečnosti informačního systému musí být konsistentní s bezpečnostní politikou a spolu s bezpečnostními provozními směrnicemi naplnit všechny bezpečnostní požadavky a deklarace v ní uvedené.

1. Popis HW a SW vybavení

➢ Uvést konkrétní konfiguraci HW

Samostatný osobní počítač

- samostatný osobní počítač – typ s bližšími údaji o jeho komponentách (včetně síťové karty, grafické karty atd.), zabudovaném HDD nebo vyměnitelných HDD a jejich počtu, odstranění pevných disků apod., výrobní číslo počítače a HDD,
- HW kryptografické prostředky,
- periferní zařízení,
- disková pole,
- zálohovací zařízení,
- UPS,
- použité speciální HW prostředky, např. pro identifikaci a autentizaci uživatelů,
- typy a výrobní čísla komponent (s podrobností specifikovanou NBÚ během certifikačního procesu),
- aj.

Lokální počítačová síť

- servery – typ a bližší údaje o jeho komponentách,
- pracovní stanice – typy a bližší údaje o komponentách (včetně síťové karty, grafické karty atd.), zabudovaném HDD nebo vyměnitelných HDD a jejich počtu, odstranění pevných disků apod.)
- HW kryptografické prostředky,
- periferní zařízení, síťové tiskárny, kopírky, multifunkční zařízení,
- disková pole,
- zálohovací zařízení,
- UPS,
- použité speciální HW prostředky, např. pro identifikaci a autentizaci uživatelů,
- u jednotlivých zařízení typy a výrobní čísla komponent (s podrobností specifikovanou NBÚ během certifikačního procesu),
- datové rozvody a prvky síťové infrastruktury,
- aj.

➢ Uvést konkrétní SW konfiguraci jednotlivých zařízení

- operační systémy,
- aplikační SW,
- antivirové programy,
- SW kryptografické prostředky,
- zálohovací utility,
- utility pro kontrolu integrity SW vybavení,
- použité speciální SW prostředky, např. pro I&A uživatelů nebo bezpečné vymazávání informací,
- aj.

➢ Uvést prostředky pro řízení přístupu k zařízením pro vstup/výstup informací do/z informačního systému, zejména pro případ USB paměťových zařízení.

➢ Uvést způsob zajištění správy konfigurace – vedení seznamu HW a SW bezpečnostním správcem informačního systému v přehledné formě, včetně údaje o zabudovaných nosičích utajovaných informací, případně používaný SW nástroj.

➢ Uvést způsob zajištění údržby SW – aplikace opravných programových balíčků (service pack) vydávaných výrobci SW.

2. Počítačová bezpečnost

➢ Jednoznačná identifikace a autentizace uživatele je zajišťována např.

- prostředky operačního systému s vhodným nastavením bezpečnostních parametrů, podrobně uvést nastavení v příloze Nastavení bezpečnostních charakteristik OS;
- specielními prostředky pro identifikaci a autentizaci – konkrétní údaje (smart card, biometrické zařízení) a specifikace potřebného nastavení, instalační předpis apod.,
- na aplikační úrovni – popsat, pokud je používána a specifikovat potřebné nastavení,
- uzamčením pracovní stanice nebo samostatného osobního počítače při krátkodobém opuštění zapnutého počítače a umožněním opětovné práce v systému až po úspěšné identifikaci a autentizaci uživatele,
- zajištěním důvěrnosti a integrity autentizační informace během přenosu sítí.

➢ Volitelné řízení přístupu k objektům informačního systému

- prostředky operačního systému (podrobnosti v příloze Nastavení bezpečnostních charakteristik OS),
- případně na aplikační úrovni, popsat, pokud je používáno a specifikovat potřebné nastavení,
- popsat řízení přístupu zejména k USB (zablokování přístupu všech uživatelů, umožnění přístupu pro konkrétní média konkrétním uživatelům apod.), uvést použité prostředky a příslušná nastavení,
- logická struktura pevných disků, pravidla pro řízení přístupu uživatelů k datové části pevného disku,
- matice přístupových práv pro uživatele.

- Vytváření auditních záznamů, jejich ochrana a jejich zkoumání
  - Základem je vytváření auditních záznamů prostředky operačního systému s vhodným nastavením bezpečnostních parametrů – zpravidla zaznamenávat úspěšné i neúspěšné pokusy o přihlášení do systému, správu uživatelů a skupin, změnu v metodě zabezpečení a neúspěšné pokusy o přístup k souborům a objektům, o použití přístupových práv, selhání restartu a vypnutí nebo sledování procesu. Podrobně nastavení popsat v příloze Nastavení bezpečnostních charakteristik OS. V případě LAN uvést zda se vede audit na serverech i jednotlivých pracovních stanicích.
  - Případně vytváření auditních záznamů i na aplikační úrovni, popsat, pokud je používáno a specifikovat potřebné nastavení.
  - Případně využití speciálních prostředků a specifikace potřebného nastavení, instalační předpis apod.
  - Omezit přístup uživatelů k auditním záznamům, aby je spravovat mohl pouze bezpečnostní správce. Uvést, jak často kontroluje auditní záznamy (na serveru, pracovní stanici), v jaké formě, kde a jak dlouho musí být uchovávány pro zpětné zkoumání, kdo má přístup k zálohám auditních záznamů,
  - Uvést nástroje pro analýzu auditních záznamů.
- Opakované použití objektů
  - řešeno operačním systémem (W XP, VISTA, W 7, W server 2003, W server 2008 atd., UNIXové systémy,
  - případně řešeno speciálními prostředky, např. utility pro bezpečné vymazávání informací z pevných disků, popsat, pokud je používáno a specifikovat potřebné nastavení,
  - řešeno také zákazem deklasifikace médií a správnou metodou jejich ničení.
  - u komponent informačního systému, které obsahují paměti typu RAM (např. tiskárny), je nutné počítat s tím, že informace v těchto pamětech zůstávají i po odpojení napájecího napětí; tomu je třeba přizpůsobit režim zacházení s těmito komponentami; v případě servisu či jiné manipulace neprověřenými osobami se např. doporučuje obsah paměti přepsat neutajovanými informacemi.

3. Komunikační bezpečnost

- Uvést kompletní údaje o LAN:
  - typ kabeláže a použité standardy,
  - síťové protokoly a pro ně potřebná konfigurace (např. MAC adresy, IP adresy a masky podsítí pro IP protokol),
  - topografie LAN (fyzické umístění jednotlivých zařízení - servery, pracovní stanice, aktivní prvky sítě, kryptografické prostředky, kabely),
  - topologie LAN (např. sběrnicová, hvězdicová, kruhová, fyzická segmentace na jednotlivých vrstvách OSI modelu a skutečná konfigurace síťových komponent, případně logická segmentace na bázi VLAN a konfigurační soubory), aj.

Pouze pro LAN, pro samostatné PC se neuvádí.

4. Personální bezpečnost

Uvést
- povinnost vedení seznamu uživatelů bezpečnostním správcem informačního systému (s číslem Osvědčení a pro jaký stupeň utajení platí, mezní doba platnosti Osvědčení, případně s údaji o Oznámení), vzor seznamu uživatelů,
- postup pro zařazení/vyřazení uživatele do/z informačního systému (kdo o tom rozhodne, kdo informuje bezpečnostního správce o zrušení oprávnění pro přístup do informačního systému před odchodem dané osoby z organizace, zánikem jejího Osvědčení nebo Oznámení, způsob sdělování této informace bezpečnostnímu správci, vzor formuláře se schválením zařazení/vyřazení uživatele do informačního systému),
- způsob jmenování osob vyžadovaných bezpečnostní politikou pro správu informačního systému bezpečnostní politikou (bezpečnostního správce, případně jeho zástupce, administrátora systému, kryptografické obsluhy aj.); odkaz na přílohu, v níž jsou uvedeny osoby, aktuálně jmenované do těchto funkcí, s čísly jejich Osvědčení od NBÚ pro přístup k odpovídajícímu stupni utajení, případně s údaji o Oznámení; doložení požadované kvalifikace pro kryptografickou obsluhu; vzory formulářů pro jmenování uvedených osob; zajištění zástupnosti,
- kde jsou uloženy identifikátor a aktuální heslo bezpečnostního správce, administrátora atd. (v zapečetěné obálce v určeném trezoru pro uchovávání utajovaných informací),

- systém bezpečnostního školení – kdo školí, jak často, že znalost a pochopení bezpečnostních směrnic musí uživatel stvrdit podpisem, dříve nežli je reálně zaveden do informačního systému a vždy po pravidelném ročním školení,
- požadavek na úroveň bezpečnostní prověrky pracovníků bezpečnostní správy a správy informačního systému a pracovníků kryptografické ochrany (je-li využívána).

5. Požadavky na dostupnost

Uvést systém zálohování, jaké konkrétní prostředky pro zálohování budou používány, kdo odpovídá za vytváření záloh systémového a aplikačního programového vybavení a datových uživatelských souborů, jaká záložní média budou používána, jejich stupeň utajení, způsob nakládání s nimi apod.

6. Administrativní bezpečnost

Uvést odkaz na dokument, podle nějž je administrativní bezpečnost v dané organizaci zajišťována, nebo ji popsat. Pokryty musí být rovněž požadavky § 15 VYHLÁŠKY a požadavky bezpečnostní politiky informačního systému.

- Shrnout všechny typy používaných počítačových médií, účel používání, jejich stupeň utajení, způsob evidence, označování.
- Uvést zásady pro ukládání počítačových médií.
- Uvést zásady pro ničení počítačových médií – komisionelní ničení s učiněním záznamu o zničení, soulad se skartačním řádem organizace, prostředky fyzického ničení a soulad s aktuálními standardy NBÚ, postup pro pevné disky.
- Uvést příslušné administrativní pomůcky realizující požadavek nepřetržité a prokazatelné odpovědnosti za jednotlivá počítačová média (např. evidence výdeje/uložení vyměnitelného pevného disku).
- Připravit procedury a manuální evidence spojené s identifikací a autentizací uživatelů, vytvářením auditních záznamů apod., pokud jsou potřebné k naplnění bezpečnostní politiky informačního systému
- Shrnout všechny manuální evidence a formuláře vedené v informačním systému, kdo je vede, kde jsou ukládány během používání, kde a jak dlouho jsou uchovávány, jejich vzory, jejich stupeň utajení.

Obvykle:

- seznam uživatelů,
- souhrnný seznam osob spravujících informační systém nebo jednotlivá jmenování,
- evidence provozních počítačových médií (viz. Poznámka 5),
- u vyměnitelných HDD evidence výdeje/příjmu HDD z úschovného objektu, charakteru administrativní pomůcky,
- umístění komponent informačního systému a jejich rozmístění v stanovených místnostech,
- seznam konfigurace HW a příslušného SW,
- provozní deník informačního systému – záznamy o opravách a údržbě, o provedení zálohy systémového programového vybavení či updatu antivirového programu, o kontrole auditních záznamů a jejich zálohování, o krizových situacích a bezpečnostních incidentech (s odkazem na příslušnou zpráva o řešení), o dalších bezpečnostně relevantních událostech, charakteru administrativní pomůcky, s uvedením data, času, zúčastněných osob a jejich podpisů,
- evidence bezpečnostních školení (prohlášení s podpisy uživatelů).

Podle potřeby:

- formuláře pro zavedení/vyřazení uživatele, s datem zavedení a vyřazení,
- evidence nahrazující identifikaci a autentizaci uživatele a/nebo auditní záznamy, charakteru administrativní pomůcky,
- evidence vstupu do prostor informačního systému, charakteru administrativní pomůcky,
- evidence vstupu návštěv, charakteru administrativní pomůcky.

- Shrnout položky bezpečnostní provozní dokumentace informačního systému – uvést seznam směrnic – např. pro bezpečnostního správce, pro uživatele, pro kryptografickou obsluhu. Jak se distribuuje bezpečnostní dokumentace informačního systému a jak je klasifikována.

7. Fyzické zabezpečení informačního systému

- Popsat zabezpečení všech prostor, v nichž budou umístěny komponenty informačního systému:
  - identifikace místnosti, které komponenty v ní jsou a aplikovaná opatření fyzické bezpečnosti včetně režimových opatření, pro podrobnější popis je možno provést odkaz na příslušný bezpečnostní projekt nebo směrnici,
  - zvlášť opatření pro servery a pro pracovní stanice,
  - rozmístění jednotlivých zařízení v místnosti, se zohledněním instalačních požadavků (možnost odezírání utajovaných informací, požadavky v oblasti kompromitujícího vyzařování podle čl. 8).
- Uvést, kdo a v jaké formě povede přehled umístění všech zařízení a jejich rozmístění v stanovených místnostech (obvykle bezpečnostní správce).
- Uvést, jak bude vedena evidence spjatá se vstupem uživatelů do počítačové místnosti, pokud je vyžadována bezpečnostní politikou informačního systému, evidenční pomůcky, procedury.
- Uvést, jak bude vedena evidence spjatá se vstupem návštěv do počítačové místnosti, pokud jsou povoleny v bezpečnostní politice.
- Uvést konkrétně, do jakých úschovných objektů budou ukládána výměnná média pro uchovávání utajovaných informací, kde jsou úschovné objekty umístěny a jak je řešeno řízení fyzického přístupu k těmto médiím. Např. pokud jde o vyměnitelné pevné disky, může být zvoleno řešení, kdy přístup do trezoru má pouze bezpečnostní správce, disky jsou tedy vydávány bezpečnostním správcem a jejich použití evidováno. Média mohou vydávat a ukládat také osoby pověřené vedením evidencí utajovaných informací (splňující podmínky pro přístup k utajovaným informacím).
- Uvést způsob pečetění krytů počítačů a dalších zařízení, umístění serveru v racku (ochranné skříni apod.).
- Uvést umístění informativních štítků na zařízení náležející do informačního systému (identifikace informačního systému a nejvyššího stupně utajení informací, které mohou být v něm zpracovávány).
- Zvláštní pozornost věnovat fyzické ochraně kryptografických zařízení, aby odpovídala požadavkům certifikační zprávy a Pravidel pro používání kryptografického prostředku a schválené dokumentaci kryptografické ochrany.
- Fyzická ochrana kabeláže LAN a aktivních síťových zařízení

8. Kompromitující vyzařování

Pro informační systém nakládající jen s informací stupně utajení Vyhrazené se tato část neuvádí.

Od stupně utajení Důvěrné výše je třeba v dokumentaci popsat a na výkresech znázornit umístění informačního systému vzhledem k místům, kde by mohlo být nepozorovaně umístěno nepřátelské zařízení pro detekci elektromagnetického vyzařování (většinou se jedná o veřejná parkoviště a prostory které nepatří uživateli informačního systému). Tento popis by měl zahrnovat všechny prostory sousedící s místností, kde je informační systém instalován, jak v horizontální tak i vertikální linii a pokud je informační systém v místnosti s okny, popsat prostor ve směru oken a to do vzdálenosti minimálně 100 metrů od informační systém. Rovněž je třeba popsat předpokládaný rozsah zpracovávání utajovaných informací a jejich časové rozložení. Pro posouzení rizika není rozhodující množství utajovaných informací uložených v informačním systému, ale množství a charakter zpracovávaných utajovaných informací a rozsah, charakter a časové rozložení zpracovávání těchto informací. Riziko z hlediska TEMPEST je spjato především se zobrazováním utajovaných informací na monitoru, jejich vkládáním pomocí klávesnice, tiskem a vypalováním na CD či DVD. Z hlediska časového rozložení je vyšší riziko spjato s pravidelným zpracováváním utajovaných informací nebo zpracováním, jehož zahájení může útočník odvodit z určitých příznaků.

Musí být zohledněny instalační požadavky – většinou dodržení určité vzdálenosti komponent informačního systému (počítač, monitor, klávesnice, myš, tiskárna atp.) od metalických vedení a jiných zařízeních (např. běžných telefonů), orientace monitorů vzhledem k oknům a stěnám místností.

9. Kryptografická ochrana

- Uvést jaký kryptografický prostředek bude v informačním systému používán, přesný typ a počty prostředků, jak bude zajišťován klíčový materiál, kde bude umístěn a jak bude zajištěna jeho fyzická bezpečnost, vyškolený personál požadovaný pro jeho provoz, jaké dokumenty pro jeho provoz budou vytvořeny apod.

Komentář

Tato specifická oblast se řídí podle ustanovení § 37 až § 43a a vyhlášky č. 432/2011 Sb., o zajištění

kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb. Nasazení kryptografického prostředku je vhodné konzultovat v OIT NBÚ již ve fázi výběru vhodného zařízení. Pro každý certifikovaný kryptografický prostředek je k certifikátu pro určitý stupeň utajení chráněné informace vydána certifikační zpráva a tzv. Pravidla pro používání kryptografického prostředku, kde se stanovují podmínky pro jeho nasazení. Uvedená „Pravidla“ poskytuje NBÚ v souladu s principem „need-to-know“. Na základě těchto dokumentů je třeba zpracovat provozní dokumentaci pro konkrétní informační systém. Tuto dokumentaci rovněž schvaluje NBU v rámci certifikace informačního systému a je součástí jeho dokumentace k certifikaci.

POZNÁMKA 7
Během zpracování návrhu bezpečnosti je nutno mít na zřeteli kromě minimálních požadavků vyplývajících z legislativní úpravy také požadavky vyplývající z analýzy rizik.

POZNÁMKA 8
V rámci kontroly před vydáním certifikátu informačního systému k nakládání s utajovanými informacemi stupně utajení Důvěrné nebo vyššího provede NBÚ odbornou prohlídku z hlediska splnění požadavků na instalaci zařízení a vyhotoví tzv. **instalační záznam**. Touto činností může být na základě smlouvy o zajištění činnosti podle § 51 zákona č. 412/2005 Sb. pověřeno odborné pracoviště provozovatele informačního systému. Pro informační systém k nakládání s utajovanou informací stupně utajení Tajné nebo vyššího je dále vyžadována tzv. obranná prohlídka, kterou provede NBÚ nebo jím pověřené odborné pracoviště.

BEZPEČNOSTNÍ SMĚRNICE INFORMAČNÍHO SYSTÉMU

Pro zajištění bezpečnosti během provozu informačního systému je VYHLÁŠKOU vyžadováno oddělené zpracování bezpečnostních směrnic pro bezpečnostního správce informačního systému, správce informačního systému a pro jednotlivé typy uživatelů informačního systému. Obecně se i v malém informačním systému specifikuje role správce informačního systému, v odůvodněných případech je slučována s rolí bezpečnostního správce informačního systému. Provozní bezpečnostní směrnice musí konkretizovat povinnosti osob při manipulaci s informacemi a informačním systémem v ochraně utajovaných informací.

V dalším textu jsou uvedeny obvyklé povinnosti uživatelů a bezpečnostních správců/správců informačního systému malých informačních systémů. Tyto seznamy nepředstavují univerzální a úplný seznam povinností uživatelů a bezpečnostních správců/správců informačních systémů a je třeba k nim přistupovat z hlediska požadavků konkrétního informačního systému. Jednotlivé body vyžadují konkretizaci a rozvedení do potřebných podrobností. Rozdělení povinností mezi správce informačního systému a bezpečnostního správce informačního systému je možno modifikovat, s ohledem na úroveň bezpečnostního prověření správce informačního systému a předpokládané technické znalosti bezpečnostního správce informačního systému.

Pokud je v informačním systému zavedena další role související se zabezpečením informačního systému, je nutno navíc specifikovat povinnosti a procedury s ní spjaté (např. „odpovědný uživatel“, který má ve svém osobním trezoru uložen výměnný pevný disk a vydává ho stanoveným způsobem malému okruhu uživatelů z jeho oddělení).

Pojetím bezpečnostních provozních směrnic se v obecnější rovině zabývá také další metodický materiál NBÚ – Bezpečnostní provozní směrnice informačního systému.

1. Typické povinnosti bezpečnostního správce

- Udržuje aktuální seznam oprávněných uživatelů na základě schématu vymezujícího způsob, jakým uživatel získá od odpovědného funkcionáře oprávnění pro přístup do informačního systému, jak je získání tohoto oprávnění sděleno bezpečnostnímu správci, zápis do seznamu uživatelů, způsob a důvody zrušení autorizace uživatele.
- Zajišťuje, aby fyzický přístup do prostor s komponentami informačního systému, k vyměnitelným pevným diskům apod. mohli získat jen oprávnění uživatelé informačního systému (jde i o přidělení klíčů či kódů zámků dveří do místností s komponentami informačního systému, předmětů vyžadovaných pro identifikaci a autentizaci, zavedení uživatele do databáze EZS a audit přístupů do místností a podobné činnosti podle konkrétní situace)
- Přiděluje uživateli uživatelské jméno a prvotní heslo do informačního systému, vytváří uživatelské

účty a spravuje je ve shodě s bezpečnostní politikou, v případě potřeby mu v této činnosti poskytuje technickou podporu správce informačního systému.

- Ručí za trvalé dodržování schválené konfigurace HW i SW informačního systému, včetně nastavení bezpečnostních charakteristik operačního systému a aplikačního SW.
- Ručí za dodržování umístění informačního systému a instalačních požadavků.
- Ve shodě s bezpečnostní politikou zkoumá pravidelně auditní záznamy a předepsané manuální evidence, vytváří záložní kopie auditních záznamů takovým způsobem, aby bylo umožněno jejich zpětné zkoumání, obvykle 3 roky nazpět.
- Zajišťuje ochranu záložních kopií auditních záznamů před modifikací nebo zničením.
- Zkoumá auditní záznamy a manuální evidence po bezpečnostním incidentu.
- Zkoumá a řeší bezpečnostní incidenty, hlásí je řediteli organizace (nebo jinému příslušnému funkcionáři).
- Zajišťuje školení uživatelů v oblasti bezpečnosti informačního systému.
- Kontroluje dodržování bezpečnostních směrnic.
- Zajišťuje v předepsaném rozsahu bezpečnost počítačových médií, zejména vyřazování a ničení médií. Popsat proceduru pro ničení médií a jak se zničení eviduje a další potřené procedury.
- Vede potřebné evidence (podle bezpečnostní politiky a návrhu systému, uvést seznam evidencí).
- Zajišťuje kontrolu vstupu návštěv (popsat jakým způsobem).
- Provádí zálohování systémového programového vybavení, zajišťuje ochranu záložních dat (konkretizovat systém zálohování, kde jsou zálohy ukládány apod.).
- Provádí správu dokumentace bezpečnosti informačního systému (kde je uložena apod.).
- Vydává uživatelům výměnné pevné disky, přenosný počítač (popsat jak, pokud je ovšem tento postup použit).
- Zajišťuje bezpečnost utajovaných informací v případě oprav počítače, kdy hlavní zásadou je, že
  - je stanoveno, kým mohou být opravy prováděny (stanovení pracovníci organizace, stanovená externí firma, případně pouze určití její pracovníci),
  - před započetím oprav HW v místě musí být odstraněny z dosahu klasifikované tiskové výstupy a odstranitelná paměťová média a odpojeno napájení všech zařízení, aby byly vymazány vyrovnávací paměti,
  - opravy HW musí být prováděny pod dohledem bezpečnostního správce a případně dalšího uživatele informačního systému s dostatečným technickým vzděláním, aby byla vyloučena možnost modifikovat HW nepovoleným způsobem (vložení neschválené komponenty) a/nebo možnost neoprávněného přístupu k utajovaným informacím,
  - porouchané pevné disky použité v informačním systému nesmí být opravovány nebo připojovány k jinému systému, mohou být pouze nahrazeny novými a uloženy jako utajovaná písemnost a posléze zničeny podle platných standardů,
  - v případě nutnosti provedení opravy mimo organizaci (bez neustálé přímé kontroly odpovědného uživatele a/nebo správce informačního systému) musí být z počítače odstraněny veškeré nevolatilní paměti, používané pro ukládání utajovaných informací.
- Dojde-li k havárii operačního systému nebo aplikačního SW, zajistí ve spolupráci se správcem informačního systému uvedení informačního systému do zabezpečeného stavu odpovídajícího schválené bezpečnostní dokumentaci informačního systému.
- Hraje klíčovou úlohu při řešení základních krizových situací - uvést povinnosti bezpečnostního správce.
- Je-li oblastí působnosti bezpečnostního správce LAN, musí být veškeré povinnosti rozšířeny do síťového prostředí, musí být zahrnuta kontrola neporušenosti kabeláže, aktivních prvků sítě, konfigurace VLAN apod.
- Je-li aplikována kryptografická ochrana, přejímá v některých případech i roli pracovníka kryptografické ochrany utajovaných informací podle vyhlášky č. 432/2011Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417 Sb. Pro tuto činnost je závazná provozní dokumentace konkrétního kryptografického prostředku.

POZNÁMKA 9

V některých obdobích jsou vydávány aktualizace virových databází tak často, že stanovená minimální perioda provedení aktualizace je příliš dlouhá. Pro správce samostatných osobních počítačů je obtížné

provádět lokálně aktualizaci vždy po vydání nové verze antivirového SW a při malém provozu na PC to může být i zbytečné. V tom případě je nutné zavést postup, kdy v případě, že na PC má být použito pro vstup informací jakékoliv externí počítačové médium, oznámí uživatel tuto skutečnost bezpečnostnímu správci, tento zajistí aktualizaci antivirového SW (a zapíše do provozního deníku) a teprve poté je médium použito na PC.

2. Správce informačního systému (oblastí činnosti je počítač a připojená zařízení, LAN)

- provádí činnost administrátora operačního systému (správce sítě LAN), stanoveným způsobem zabezpečuje denní provoz informační systém po technické stránce,
- instaluje operační systém, aplikační SW, zajišťuje aktualizaci antivirového SW,
- spolupracuje s bezpečnostním správcem informačního systému při nastavení bezpečnostních charakteristik operačního systému a aplikačního SW podle schválené bezpečnostní dokumentace informačního systému,
- spravuje uživatelské účty ve spolupráci s bezpečnostním správcem informačního systému,
- spolupracuje s bezpečnostním správcem informačního systému při vyčištění a zotavení systému po napadení viry,
- spolupracuje s bezpečnostním správcem při uvedení informačního systému do stavu odpovídajícího schválené bezpečnostní dokumentaci informačního systému po ostatních bezpečnostních incidentech nebo mimořádných událostech,
- nemá možnost modifikovat auditní záznamy operačního systému ani aplikačního SW,
- je-li aplikována kryptografická ochrana, přejímá v některých případech i roli pracovníka kryptografické ochrany utajovaných informací podle vyhlášky č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, ve znění vyhlášky č. 417/2013 Sb. Pro tuto činnost je závazná schválená provozní dokumentace konkrétního kryptografického prostředku.

3. Typické povinnosti uživatele informačního systému

Bezpečnostní směrnice pro uživatele vyžaduje přehledné a srozumitelné zpracování. Nesmí obsahovat údaje, které uživatel nepotřebuje znát a které by mu umožnily zneužití informačního systému. Zejména je třeba, aby byl uživatel informován

- o účelu informačního systému,
- kde smí pracovat s utajovanými informacemi, případně v jakém časovém rozpětí během dne,
- jaké je standardní zahájení práce v informačním systému (přístup k¨ počítači, přihlašovací procedura a postup identifikace a autentizace uživatele, jaká jsou omezení v počtu chybných přihlášení, délce hesla a době jeho platnosti, délce PINu čipové karty apod.),
- jakou kontrolu HW (případně kabeláže), prostředí nebo podle okolností i jiných prvků informačního systému má provést před započetím práce,
- jak má zacházet s vyměnitelnými pevnými disky a dalšími počítačovými médii používanými výhradně v daném informačním systému, že je nesmí použít mimo daný informační systém a musí s nimi nakládat jako s utajovanými informacemi,
- do jakého úschovného objektu má ukládat klasifikovaná počítačová média nebo od koho je před započetím práce v informačním systému získá a komu je po skončení práce vrací k uložení,
- jakým způsobem získá vyměnitelný pevný disk nebo přenosný počítač nebo jiný HW systému před započetím práce, jakým způsobem ho opět vrací, s tím spjaté povinnosti a evidence,
- v jaké oblasti pevného disku může/má ukládat uživatelské soubory, případně že je na pevný disk ukládat nesmí/nemůže apod.,
- jak musí/může zálohovat uživatelská data a na jaká média, jak musí chránit záložní média,
- jak se chovat k návštěvě, jak k pracovníkům úklidu (aby to vyhovovalo bezpečnostní politice a návrhu bezpečnosti),
- o své povinnosti dodržovat schválenou konfiguraci HW a SW,
- o své povinnosti hlásit poruchy HW i SW, výskyt bezpečnostního incidentu nebo podezření na možnost kompromitace utajovaných informací bezpečnostnímu správci,
- o tom, jaké základní bezpečnostní incidenty se mohou vyskytnout a jak má bezprostředně reagovat, pokud to typ události vyžaduje, před kontaktem s bezpečnostním správcem,

- o zavedené ochraně USB portů, zejména v souvislosti s používáním USB paměťových zařízení („klíčenky“, disky),
- o postupu pro export informací z informačního systému na počítačovém médiu, pokud je uživateli povolen, např.:
  - médium musí být označeno nejvyšším stupněm utajení obsažené informace, do příslušné mechaniky se vkládá bezprostředně před aplikací uvedeného příkazu a vyjme se z ní ihned po jeho provedení, předání média se řídí pravidly administrativní bezpečnosti pro utajované informace,
  - při výstupu utajovaných informací nižších stupňů utajení (resp. neutajovaných) na počítačové médium odpovídajícího stupně utajení (resp. neutajované) je povinností uživatele posoudit osobně obsah souboru a ujistit se o nižším stupni utajení (resp. neutajovanosti) obsažených informací, médium musí být označeno stupněm utajení obsažené informace, předání se řídí pravidly administrativní bezpečnosti pro utajované informace,
  - podle potřeby je možno předepsat, že export informací na počítačových médiích povoluje v určených případech bezpečnostní správce nebo vedoucí pracovník, apod.

POZNÁMKA 10. Windows 2000, Windows XP, Windows 2003, VISTA, Windows 2008 a vyšší verze Windows již nepřenášejí celé bloky dat, soubory je možno kopírovat běžným způsobem; pokud starší operační systém přenáší celé bloky, pak pro předání určitých informací z informačního systému na počítačovém médiu jinému subjektu je třeba použít nové čisté médium (nebo poskytnuté tímto subjektem) a ukládat soubory příkazem typu Uložit (Save) z aplikací.

- o postupu pro import informací do informačního systému prostřednictvím počítačového média, např.:
  - import informace stupně utajení vyššího, nežli je nejvyšší stupeň utajení, pro který je informační systém určen, je zakázán,
  - je-li importována informace stupně utajení nižšího (resp. neutajovaná) na médiu odpovídajícího stupně utajení, je nutno ochránit toto médium před zápisem a vložit je do mechaniky jen na dobu nezbytně nutnou pro načtení informace, pokud ochrana před zápisem není možná nebo nebyla správně aplikována, musí být dané médium překlasifikováno na nejvyšší stupeň utajení, se kterým se v daném informačním systému nakládá,
- o povinnosti označit tiskové výstupy stupněm utajení a dalšími náležitostmi podle požadavků administrativní bezpečnosti a zajistit neprodleně jejich zaevidování v knize utajovaných písemností,
- o postupech při ničení a skartaci médií a příslušných pravidlech administrativní bezpečnosti,
- o předepsaném postupu při nutnosti opustit počítač v běhu, povolená lhůta,
- o proceduře pro standardní bezpečné ukončení práce v informačním systému - veškeré povinnosti týkající se počítače, periférií, místnosti, klíčů, EZS atd.
- o správném používání hesla, jak ho tvořit, že ho nesmí sdílet, prozradit atd.,
- o ochraně, kterou musí poskytovat magnetické nebo čipové kartě (případně jiným pomůckám) využívané pro identifikaci a autentizaci uživatele v informačním systému,
- o způsobu používání klíčů od místnosti, systému elektrické zabezpečovací signalizace, systému elektronické kontroly vstupu, podle konkrétní situace, je možno řešit i odkazem na příslušný bezpečnostní projekt objektové a technické bezpečnosti,
- o tom, jaké základní mimořádné (krizové) situace mohou nastat a jaké jsou jeho povinnosti při jejich řešení,
- o všech svých dalších povinnostech vyplývajících z bezpečnostní politiky informačního systému a návrhu její realizace (např. povinnost provádět bezpečné vymazávání utajovaných informací z pevného disku a způsob, jakým tuto povinnost splnit, povinnost upozornit bezpečnostního správce na záměr použít externí médium ve smyslu Poznámky 7),
- v potřebné míře o okolnostech umožňujících mu pochopení jeho povinností.

Povinnosti uživatele v oblasti obsluhy kryptografického prostředku využívaného v informačním systému jsou obvykle popsány ve zvláštní bezpečnostní směrnici, v jednoduchých případech mohou být součástí bezpečnostní směrnice uživatele. Uživatel musí být informován o rozsahu ochrany, kterou poskytuje kryptografický prostředek jeho datům (např., že je šifrován automaticky obsah celého pevného disku a/nebo veškerá informace vystupující na CD/DVD/disketu, že je zašifrován určitý soubor po stisknutí příslušné klávesy nebo provedení jiné definované akce uživatele).

POZNÁMKA 11

Uživateli informačního systému je nutno poskytnout potřebné školení, aby byl schopen provádět

činnost vyžadovanou bezpečnostními směrnicemi a efektivně využívat informační systém. Důraz je třeba klást na to, aby uživatelé pochopili jednotlivá bezpečnostní opatření a důvody jejich zavedení.

Možné řešení krizových situací a bezpečnostních incidentů

Jde-li o situaci, která přímo nesouvisí s funkcí HW a SW, je základním opatřením ukončit činnost systému, vyjmout veškerá počítačová média z počítače, vypnout počítač a připojená zařízení (vyprázdnění volatilních pamětí) a uložit počítačová média, dokumenty s utajovanými informacemi i dokumentaci informačního systému do příslušného úschovného objektu. Není-li to v době výskytu mimořádné události možné, je třeba uchovat veškeré nosiče utajovaných informací v osobní péči oprávněného uživatele informačního systému, oprávněné osoby nebo bezpečnostního správce informačního systému, do doby, kdy je možno je uložit podle zásad ochrany utajovaných informací.
Pokud situace vyžaduje zásah nepovolaných osob, musí být zamezeno neoprávněnému přístupu k utajovaným informacím a zařízením informačního systému, zásahu (hasičů, instalatérů, příslušníků bezpečnostní služby zajišťujících fyzickou ostrahu apod.) musí být přítomen bezpečnostní správce nebo oprávněný uživatel informačního systému nebo statutární zástupce, bezpečnostní tajemník apod.

Pokud jde o poruchu HW, SW nebo výskyt počítačového viru, přeruší uživatel práci s informačním systémem a přivolá bezpečnostního správce, který situaci vyřeší.

Opravy HW se musí provádět pod dohledem bezpečnostního správce informačního systému a tak, aby se technik provádějící opravu nemohl seznámit s utajovanými informacemi a zároveň, aby nemohlo dojít k narušení schválené konfigurace informačního systému. Bez svolení bezpečnostního správce nesmí technik přinést ani odnést žádnou komponentu informačního systému ani počítačové médium.

Údržba SW, řešení selhání operačního systému nebo aplikačního SW a řešení virového incidentu musí být prováděno buďto správcem informačního systému (administrátorem) prověřeným pro nejvyšší stupeň utajení informací zpracovávaných v informačním systému nebo bezpečnostním správcem informačního systému. Výsledkem činnosti musí být uvedení informačního systému do zabezpečeného stavu podle bezpečnostní dokumentace informačního systému.

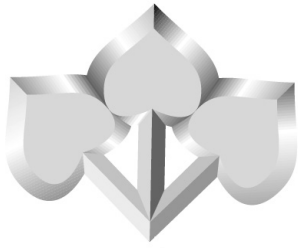
Výjimečně může tuto správu provádět osoba prověřená pouze pro nižší stupeň utajení, avšak pod stálým dohledem bezpečnostního správce. V tom případě obnovení systému a aplikačního SW provede z instalačních médií uložených u bezpečnostního správce a neodnáší žádné médium.

O každé z mimořádných situací nebo z bezpečnostních incidentů musí být bezpečnostním správcem pořízen zápis, s uvedením dne a doby výskytu, způsobem řešení, jmen zúčastněných osob, podepsaný zúčastněnými osobami. Zápis je dán na vědomí i statutárnímu orgánu, který z něj vyvodí i akce, vyžadované případně zákonem.

Základní pokyny pro práci s hesly

- Heslo je kombinací velkých a malých písmen a nejméně jedné číslice a oddělovacích symbolů (včetně mezery), nesmí být použito slovo některého běžného jazyka, musí začínat písmenem,
- heslem nebo jeho součástí nesmí být jméno jeho nebo jeho blízkých, číslo jeho průkazu apod.,
- své heslo musí uživatel chránit obdobně jako utajovanou informaci nejvyššího stupně utajení, jaký je v informačním systému zpracováván,
- dočasné opuštění pracovní stanice během pracovní doby je možné pouze po uzamčení stanice (např. CTRL-ALT-DEL a volba ”Uzamknout stanici”),
- své heslo nesmí uživatel sdílet s jiným uživatelem,
- v systému pro zpracování utajovaných informací nesmí být používáno stejné heslo, jako v jiných systémech,
- pro Systémy MS Windows heslo administrátora pro účet Administrator (přejmenovaný) je uloženo v zalepené obálce v úschovném objektu,
- pro UNIX-ové systémy heslo superuživatele je uloženo v zalepené obálce v úschovném objektu,
- administrátor používá účet Administrator nebo účet s právy superuživatele jen pro správu operačního systému, pro své uživatelské aktivity užívá jiného účtu, podle principu nejmenších privilegií.

KRYPTOGRAFICKÁ OCHRANA
UTAJOVANÝCH INFORMACÍ



Informace o změnách v legislativě upravující zajištění kryptografické ochrany utajovaných informací

NBÚ, 20. ledna 2015

Kryptografickou ochranu utajovaných informací upravuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Poslední novela, realizovaná zákonem č. 255/2011 Sb., kterým se mění zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, a zákon č. 634/2004 Sb., o správních poplatcích, ve znění pozdějších předpisů (dále jen „zákon“), se významně dotkla také oblasti kryptografické ochrany utajovaných informací.

K zákonu jsou vydány dvě vyhlášky NBÚ:

- vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací, která byla novelizována vyhláškou č. 417/2013 Sb.,
- vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, která byla novelizována vyhláškou č. 434/2011 Sb.

V roce 2014 nebyly ve vztahu ke kryptografické ochraně provedeny žádné změny v zákoně ani v uvedených vyhláškách.

V roce 2014 byly vydány dva bezpečnostní standardy NBÚ z oblasti kryptografické ochrany utajovaných informací:

- bezpečnostní standard NBÚ – 1/2014,verze 1.0, ze dne 22. 9. 2014, upravující podmínky, způsob a postupy vyřazování a ničení kryptografického prostředku a materiálu k zajištění jeho funkce,
- bezpečnostní standard NBÚ – 1/2013, verze 1.1, ze dne 22. 9. 2014, upravující podmínky provozu kryptografických prostředků třídy TCE 621 a center řízení TCE 671 (nahrazuje bezpečnostní standard NBÚ – 1/2013, verze 1.0).

Standard NBÚ – 1/2014 se aplikuje zejména na případy ukončení platnosti certifikátu kryptografického prostředku nebo schválení materiálu k zabezpečení funkce kryptografického prostředku a případy jejich neopravitelnosti. Standard se neaplikuje na případy nouzového ničení, které jsou upraveny v pravidlech pro používání kryptografického prostředku a materiálu k zabezpečení jeho funkce.

Pro upřesnění lze uvést, že

- pro konkrétní kryptografický prostředek Úřad stanovuje doplňující podmínky pro ničení prostředku, konkretizuje postupy, podmínky a způsob ničení prostředku a písemně o nich informuje příslušný subjekt,
- v příloze č. 1 jsou stanoveny požadavky pro vytvoření muzejního exponátu, umožňujícího jeho veřejnou prezentaci, z vyřazeného kryptografického prostředku a materiálu k zajištění jeho funkce.

Kryptografické prostředky certifikované ke dni 1. ledna 2015 podle zákona č. 412/2005 Sb., k ochraně utajovaných informací v národních informačních nebo komunikačních systémech

(v tabulce nejsou uvedeny kryptografické prostředky vyvinuté a hodnocené pro speciální účely)

Kryptografický prostředek	Stupeň utajení, kategorie UI	Platnost certifikátu	Výrobce/dovozce	Bližší informace
CSP II	D, NC, EU/C	22. 7. 2018	S.ICZ a.s.	www.i.cz
DST SPIDER_K	D, NC, EU/C	31. 12. 2018	LEC s. r. o.	www.lec.cz
ELCRODAT 4-2	T, NS	21. 9. 2018	Rohde & Schwarz SIT GmbH (SRN) DICOM, spol. s r.o.	www.sit.rohde-schwarz.com www.dicom.cz
ELCRODAT 6-2S	PT, CTS	22. 7. 2018	Rohde & Schwarz SIT GmbH (SRN) Rohde & Schwarz – Praha, s.r.o.	www.sit.rohde-schwarz.com www.rohde-schwarz.cz
HCryptC	V, NR, EU/R	26. 10. 2018	NBÚ	podá NBÚ
HCryptW		28. 8. 2019		
KRYDEC XP	T, NC, EU/C	19. 8. 2017	S.ICZ a.s.	www.i.cz
LANPCS-AES	V, NR, EU/R	22. 1. 2019	S.ICZ a.s.	www.i.cz
LANPCSe-AES		22. 1. 2019		
LANPCS-Rack		13. 10. 2019		
PCS1	T, NC, EU/C	20. 12. 2018		
PCS1e		22. 1. 2019		
RF1302S*)	D, NC, EU/R	1. 12. 2016	DICOM, spol. s r.o.	www.dicom.cz
RF13250S*)		1. 12. 2016		
SECTRA Panthon 2	V, EU/R	29. 7. 2017	SECTRA COMMUNICATIONS AB (Švédsko) ATS – TELCOM PRAHA a.s.	www.communications.sectra.com www.atstelcom.cz
SECTRA Panthon 3		29. 4. 2019		
SECTRA Tiger XS, XS Office	T, EU/S	19. 11. 2018		
SILENTEL v. 5.2	V	19. 10. 2019	ARDACO a. s. (SR) F.S.C. BEZPEČNOSTNÍ PORADENSTVÍ, a. s.	www.ardaco.com www.fsc-ov.cz
SINA-BOX H	T, NS	25. 4. 2015	Secunet Security Networks AG (Německo)	www.secunet.com
SINA-BOX P	T, EU/S	26. 6. 2017		
SINA-CLIENT H	T, NS	25. 4. 2015		
SINA-CLIENT P	T, EU/S	25. 4. 2015		
TCE 621 B/CZ	D, NC, EU/C	14. 7. 2018	ATS – TELCOM PRAHA a.s. (komponenty dodává THALES Norway AS)	www.atstelcom.cz www.thales.no
TCE 621 C/CZ		14. 7. 2018		
TCE 621 B/CZ Dual mode		3. 4. 2019		
TCE 621 C/CZ Dual mode		3. 4. 2019		

TCE 621 IP	PT, CTS	25. 7. 2017	THALES Norway AS (Norsko) ATS – TELCOM PRAHA a.s.	www.thales.no www.atstelcom.cz
TCE 621/B		17. 3. 2016		
TCE 621/C		17. 3. 2016		
TCE 621/B Dual mode		21. 9. 2019		
TCE 621/C Dual mode		21. 9. 2019		
TCE 624/M	T, NS	17. 9. 2019		
TCE 627/M-AES		17.9. 2019		
*) Kryptografický prostředek je určen pro ochranu taktické informace.				

Probíhají certifikace nových kryptografických prostředků:

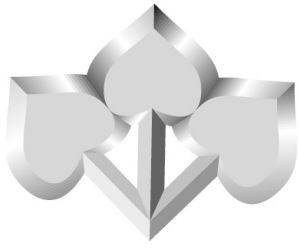
Kryptografický prostředek	Stupeň utajení, kategorie UI	Ukončení certifikace	Výrobce/dovozce	Bližší informace
PCA	předpokládané určení D, NC, EU/C	2015 (červen)	KNZ s. r. o. (vývoj) ATS – TELCOM PRAHA a. s. (výroba)	Kryptografická ochrana dat na PC (externí/off-line)

Národní UI
V = Vyhrazené
D = Důvěrné
T = Tajné
PT = Přísně Tajné

Utajované informace NATO
NR = NATO RESTRICTED
NC = NATO CONFIDENTIAL
NS = NATO SECRET
CTS = COSMIC TOP SECRET

Utajované informace EU
EU/R = RESTREINT UE/EU RESTRICTED
EU/C = CONFIDENTIEL UE/EU CONFIDENTIAL
EU/S = SECRET UE/EU SECRET

FYZICKÁ BEZPEČNOST



Fyzická bezpečnost

Fyzická bezpečnost je druhem zajištění ochrany utajovaných informací a je upravena v Hlavě V zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (dále jen „zákon č. 412/2005 Sb.“). 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 je budova nebo jiný ohraničený prostor, ve kterém se zpravidla nachází zabezpečená oblast nebo jednací oblast. Objekt slouží ke zpracovávání a manipulaci s utajovanou informací.

Zabezpečená oblast slouží k ukládání utajované informace, která se ukládá v zabezpečené oblasti v trezoru nebo jiné uzamykatelné schránce. Zabezpečené oblasti se podle nejvyššího stupně utajení utajované informace, která se v nich ukládá, zařazují do kategorií:

a) Přísně tajné,

b) Tajné,

c) Důvěrné, nebo

d) Vyhrazené.

Utajovanou informaci stupně utajení Přísně tajné nebo Tajné lze pravidelně projednávat pouze v jednací oblasti.

Zabezpečení zabezpečené oblasti, objektu a jednací oblasti je zajišťováno kombinací opatření fyzické bezpečnosti, které jsou ostraha, režimová opatření a technické prostředky. Výkon ostrahy a rozsah použití opatření fyzické bezpečnosti zabezpečené oblasti, jednací oblasti a objektu se stanoví v závislosti na stupni utajovaných informací a na vyhodnocení rizik.

Rozsah použití technických prostředků k zabezpečení zabezpečené oblasti, jednací oblasti a objektu se stanoví v závislosti na kategorii, třídě a vyhodnocení rizik. Pro ochranu zabezpečených oblastí kategorie Vyhrazené se používají certifikované nebo necertifikované technické prostředky. Pro ochranu zabezpečených oblastí kategorie Důvěrné a vyšší se používají certifikované technické prostředky. Necertifikované technické prostředky lze použít pouze za předpokladu, že nesníží úroveň ochrany požadované pro daný stupeň utajení.

Rozsah použití technických prostředků je následující:

- pro kategorii Vyhrazené – mechanické zábranné prostředky,
- pro kategorii Důvěrné – mechanické zábranné prostředky a zařízení elektrické zabezpečovací signalizace,
- pro kategorii Tajné a Přísně tajné – mechanické zábranné prostředky, systémy pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace, speciální televizní systémy, zařízení elektrické požární signalizace.

Bodové hodnoty nejnižší míry zabezpečení technických prostředků jsou stanoveny v příloze č. 1 vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů. Technické prostředky jsou rozděleny do 9 druhů (viz § 30 zákona č. 412/2005 Sb.), znichž Úřad certifikuje následující výrobky:

a) mechanické zábranné prostředky,

b) elektrická zámková zařízení a systémy pro kontrolu vstupu

c) zařízení elektrické zabezpečovací signalizace,

e) tísňové systémy,

h) zařízení fyzického ničení nosičů informací a dat.

Přehled platných certifikovaných technických prostředků je veden a aktualizován na následujícím odkazu:

http://www.nbu.cz/cs/informacni-centrum/seznamy/seznam-certifikovanych-technickych-prostredku/.

CERTIFIKOVANÉ TECHNICKÉ PROSTŘEDKY JSOU UVEDENÉ K DATU 26. 1. 2015.

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. a) zákona č. 412/2005 Sb.
MECHANICKÉ ZÁBRANNÉ PROSTŘEDKY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T0012/2012	Sádrokartonová příčka	Knauf W 118-1	KNAUF Praha, spol. s r.o.	KNAUF Praha, spol. s r.o.	Mladoboleslavská 949	Praha 9 - Kbely 190 00	3	SS3=3	9.2.2015
T0024/2012	Nábytkový trezor JUNIOR	typ NTJ 4, NTJ 5, NTJ 7, NTJ 8	PROFIKON INTERNATIONAL s.r.o.	PROFIKON INTERNATIONAL s.r.o.	Střelniční 1812	Frenštát pod Radhoštěm 744 01	3	SS1=3, SS2=2	22.3.2015
T0025/2012	Stěnový trezor JUNIOR	typ STJ 4, STJ 5, STJ 7, STJ 8	PROFIKON INTERNATIONAL s.r.o.	PROFIKON INTERNATIONAL s.r.o.	Střelniční 1812	Frenštát pod Radhoštěm 744 01	3	SS1=3, SS2=2	22.3.2015
T0026/2012	Bezpečnostní dvoukřídlové dveře NEXT	typ SD 102D	NEXT, spol. s r.o.	NEXT, spol. s r.o.	Potoční 404	Budyně nad Ohří 411 18	3	SS3=3, SS4=2	8.3.2015
T0027/2012	Bezpečnostní dvoukřídlové dveře NEXT	typ SD 102DF s protipožární úpravou EI30/EW30	NEXT, spol. s r.o.	NEXT, spol. s r.o.	Potoční 404	Budyně nad Ohří 411 18	3	SS3=3, SS4=2	8.3.2015
T0030/2012	Bezpečnostní dveře	ZVI 43 db BD 2	SAPELI, a.s.	SAPELI, a.s.	Na Podhoře 185	Polná 588 13	2	SS3=2, SS4=1	22.3.2015
T0031/2012	Bezpečnostní dveře BEDEX VARIO EL VD3	Bezpečnostní dveře BEDEX VARIO EL VD3 s protipožární odolností EI 30 D1	MRB Sazovice, spol. s r.o.	MRB Sazovice, spol. s r.o.	Sazovice 191	Mysločovice 763 01	3	SS3=3, SS4=2	19.4.2015
T0032/2012	Bezpečnostní dveře BEDEX VARIO EL VD4	Bezpečnostní dveře BEDEX VARIO EL VD4 s protipožární odolností EI 30 D1	MRB Sazovice, spol. s r.o.	MRB Sazovice, spol. s r.o.	Sazovice 191	Mysločovice 763 01	4	SS3=4, SS4=3	19.4.2015
T0035/2012	Skříň na zbraně, Skříň na spisy, Skříň kombinovaná (na zbraně i spisy)	typ MAXI	SAFETRONICS a.s.	SAFEtronics PRAHA a.s.	Českomoravská 7/808	Praha 9 190 00	1B	S1=2	4.4.2015
T0036/2012	Mobilní skříňový trezor typ nábytkový trezor	NHD/II 90, NHD/II 115, NHD/II 145, NHD/II 180, NHD/II 210, NHD/II 240	T - SAFE s.r.o.	T - SAFE s.r.o.	Bezručova 537	Frenštát pod Radhoštěm 744 01	4	SS1=4, SS2=2	29.5.2015
T0041/2012	Nábytkový trezor	typ ANT 33, ANT 65, ANT 81, ANT 90, ANT 111, ANT 140	AXI MONT, spol. s r. o.	AXI MONT, spol. s r. o.	Neurazy č.p. 152	Neurazy 335 55	3	SS1=3, SS2=2	21.7.2015
T0042/2012	Bezpečnostní dveře BEDEX	STANDARD 3 s protipožární odolností	MRB Sazovice, spol. s r.o.	MRB Sazovice, spol. s r.o.	Sazovice 191	Mysločovice 763 01	3	SS3=3, SS4=2	9.8.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. a) zákona č. 412/2005 Sb.
MECHANICKÉ ZÁBRANNÉ PROSTŘEDKY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T0043/2012	Bezpečnostní dveře BEDEX	STANDARD 2 s protipožární odolností	MRB Sazovice, spol. s r.o.	MRB Sazovice, spol. s r.o.	Sazovice 191	Mysločovice 763 01	2	SS3=2, SS4=1	9.8.2015
T0044/2012	Mobilní skříňový trezor	typ CST 1, CST 2, CST 3, CST 4, CST 5, CST 6 a CST 7	AXI MONT, spol. s r. o.	AXI MONT, spol. s r. o.	Neurazy č.p. 152	Neurazy 335 55	3	SS1=3, SS2=2	4.9.2015
T0045/2012	Sádrokartonová bezpečnostní předstěna	Knauf W523 RC3 a W626/629 RC3	KNAUF Praha, spol. s r.o.	KNAUF Praha, spol. s r.o.	Mladoboleslavská 949	Praha 9 - Kbely 90 00	3	SS3=3	10.5.2015
T0046/2012	Sádrokartonový bezpečnostní strop	Knauf D131 A RC3 a D131 B RC3	KNAUF Praha, spol. s r.o.	KNAUF Praha, spol. s r.o.	Mladoboleslavská 949	Praha 9 - Kbely 190 00	3	SS3=3	10.5.2015
T0047/2012	Mobilní skříňový trezor	typ NEUTRON STAR viz příloha	Charvát spol. s.r.o.	Charvát spol. s.r.o.	Údolní 259	Smržovka 468 51	3	SS1=3, SS2=2	20.9.2015
T0051/2012	Cylindrická vložka	TOKOZ PRO 300	TOKOZ a.s.	TOKOZ a.s.	Santiniho 20/26	Žďár nad Sázavou 591 02	2	SS4=2	19.4.2015
T0052/2012	Cylindrická vložka	TOKOZ PRO 400+	TOKOZ a.s.	TOKOZ a.s.	Santiniho 20/26	Žďár nad Sázavou 591 02	3	SS4=3	6.9.2015
T0055/2012	Bezpečnostní zámková vložka CONSTRUCT	typ C012	CONSTRUCT A 3.40.05 R3; 3.40.06 R3	Saint-Gobain Construction Products CZ a.s.	Saint-Gobain Construction Products CZ a.s.	Počernická 272/96 Praha 10 108 03	3	SS3=3	27.2.2017
T0031/2014	Bezpečnostní předstěna spřažená	3.21.08 R3	Saint-Gobain Construction Products CZ a.s.	Saint-Gobain Construction Products CZ a.s.	Počernická 272/96	Praha 10 108 03	3	SS3=3	27.2.2017
T0032/2014	Bezpečnostní předstěna volně stojící	3.22.08 R3	Saint-Gobain Construction Products CZ a.s.	Saint-Gobain Construction Products CZ a.s.	Počernická 272/96	Praha 10 108 03	3	SS3=3	27.2.2017
T0033/2014	Bezpečnostní mezistrop	4.10.92 R3	Saint-Gobain Construction Products CZ a.s.	Saint-Gobain Construction Products CZ a.s.	Počernická 272/96	Praha 10 108 03	3	SS3=3	27.2.2017
T0034/2014	Bezpečnostní mezibytová stěna	3.41.19 R3	Saint-Gobain Construction Products CZ a.s.	Saint-Gobain Construction Products CZ a.s.	Počernická 272/96	Praha 10 108 03	3	SS3=3	27.2.2017
T0035/2014	Mobilní skříňový trezor	typ TLA-1 až TLA-13	P-KOVO Brno, spol. s r.o.	TRESORAG - FIRESAFE s.r.o.	Březová 43/1711	Praha 8 - Kobylisy 182 00	3	SS1=3, SS2=2	22.3.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. a) zákona č. 412/2005 Sb.
MECHANICKÉ ZÁBRANNÉ PROSTŘEDKY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T0036/2014	Bezpečnostní cylindrická vložka GUARD	typ CPS, G330, G550 a G570 SGHK vše v systému ABS Plus	Guard - Mudroch, spol. s r. o.	Guard - Mudroch, spol. s r. o.	Koráb 132	Tišnov 666 01	2	SS4=2	27.2.2017
T0037/2014	Bezpečnostní cylindrická vložka GUARD	typ CPS, G330, G550 a G570 SGHK vše v systému ABS +, ABS ++	Guard - Mudroch, spol. s r. o.	Guard - Mudroch, spol. s r. o.	Koráb 132	Tišnov 666 01	2	SS4=2	27.3.2017
T0038/2014	Mobilní skříňový trezor typ TM-I-001 až TM-I-007 a typ TN-I-001 až TN-I-007	Vestavěný skříňový trezor typ TV-I-001 až TV-I-006	Stanislav Kulhavý	Stanislav Kulhavý	Žampach 4	Kamenný Přívoz 254 01	3	SS1=3, SS2=2	13.1.2017
T0039/2014	Mobilní skříňový trezor typ TM-0-001 až TM-0-007 a typ TN-0-001 až TN-0-007	Vestavěný skříňový trezor typ TV-0-001 až TV-0-006	Stanislav Kulhavý	Stanislav Kulhavý	Žampach 4	Kamenný Přívoz 254 01	2	SS1=2, SS2=2	13.1.2017
T0040/2014	Bezpečnostní dveře protipožární MASONITE B3	v ocelové zárubni tloušťky 2 mm	Masonite CZ spol. s r.o.	Masonite CZ spol. s r.o.	Hruškové Dvory 82	Jihlava 586 02	3	SS3=3, SS4=2	27.6.2016
T0041/2014	Cylindrická vložka FAB 300HdB	varianty v příloze	ASSA ABLOY Czech & Slovakia s. r.o.	ASSA ABLOY Czech & Slovakia s. r.o.	Strojnická 633	Rychnov nad Kněžnou 516 01	2	SS4=2	16.1.2017
T0047/2014	Visací zámek	ABLOY PL 230 v provedení PL 330	ABLOY Oy	ASSA ABLOY Czech & Slovakia s. r.o.	Strojnická 633	Rychnov nad Kněžnou 516 01	2	SS4=2	28.6.2015
T0051/2014	Bezpečnostní protipožární dveře	typ PYROSAFE SF B2	CAG s.r.o.	CAG s.r.o.	Kytín 19	Mníšek pod Brdy 252 10	2	SS3=2, SS4=1	24.4.2017
T0052/2014	Bezpečnostní kování typ RC101	provedení v příloze	Richter Czech s. r.o.	Richter Czech s. r.o.	Křesomyslova 543/13	Praha 4 - Nusle 140 00	1	SS4=1	12.6.2017
T0053/2014	Bezpečnostní cylindrická vložka EVVA typ EPS/DPI SG	včetně bezpečnostního kování s krytem cylindrické vložky	EVVA Sicherheitstechnologie GmbH	EVVA spol. s r.o.	V Bokách II 1048	Praha 5 - Hlubočepy 152 00	3	SS4=3	18.4.2016
T0054/2014	Mobilní skříňový trezor typ NTR	typy včetně variant v příloze	SAFETRONICS a.s.	SAFEtronics PRAHA a.s.	Českomoravská 7/808	Praha 9 190 00	3	SS1=3, SS2=2	20.9.2015
T0055/2014	Mobilní skříňový trezor typ MAXI	varianty v příloze	SAFETRONICS a.s.	SAFEtronics PRAHA a.s.	Českomoravská 7/808	Praha 9 190 00	1B	S1=2	13.3.2017

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. a) zákona č. 412/2005 Sb.
MECHANICKÉ ZÁBRANNÉ PROSTŘEDKY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T0056/2014	Bezpečnostní uzamykací vložka Kaba penta	varianty: KABA quattro S, KABA quattro pluS, KABA experT	Kaba GmbH	Kaba GmbH, organizační složka	Naskové 3	Praha 5 150 00	3	SS4=3	30.3.2017
T0057/2014	Nábytkový trezor	typ SL I/0, SL I/1, SL I/2, SL I/3, SL I/4, SL I/5, SL I/6	PROFIKON INTERNATIONAL s.r.o.	PROFIKON INTERNATIONAL s.r.o.	Střelniční 1812	Frenštát pod Radhoštěm 744 01	3	SS1=3, SS2=2	18.7.2015
T0058/2014	Nábytkový trezor	typ SL II/0, SL II/1, SL II/2, SL II/3, SL II/4, SL II/5, SL II/6	PROFIKON INTERNATIONAL s.r.o.	PROFIKON INTERNATIONAL s.r.o.	Střelniční 1812	Frenštát pod Radhoštěm 744 01	4	SS1=4, SS2=2	18.7.2015
T0059/2014	Cylindrická vložka EURO Secure	chráněná bezpečnostním kováním s krytem cylindrické vložky	Richter Czech s. r.o.	Richter Czech s. r.o.	Křesomyslova 543/13	Praha 4 - Nusle 140 00	2	SS4=2	2.5.2016
T0060/2014	Visací zámek	RV 2601	Richter Czech s. r.o.	Richter Czech s. r.o.	Křesomyslova 543/13	Praha 4 - Nusle 140 00	2	SS4=2	31.7.2017
T0062/2014	Visací zámek	HERMES a HERMES plus	Richter Czech s.r.o.	Richter Czech s.r.o.	Křesomyslova 543/13	Praha 4 - Nusle 140 00	1	SS4=1	11.9.2017
T0063/2014	Bezpečnostní příčka Knauf W118	v provedení W115 - RC3 s elektrokrabicí	KNAUF Praha, spol. s r.o.	KNAUF Praha, spol. s r.o.	Mladoboleslavská 949	Praha 9 - Kbely 197 00	3	SS3=3	13.2.2017
T0064/2014	Bezpečnostní příčka Knauf W118	v provedení W112 - RC3 s deskami TOPAS a elektrokrabicí	KNAUF Praha, spol. s r.o.	KNAUF Praha, spol. s r.o.	Mladoboleslavská 949	Praha 9 - Kbely 197 00	3	SS3=3	12.6.2017
T0065/2014	Bezpečnostní příčka Knauf W118	v provedení W353 - RC3 s volným koncem příčky	KNAUF Praha, spol. s r.o.	KNAUF Praha, spol. s r.o.	Mladoboleslavská 949	Praha 9 - Kbely 197 00	3	SS3=3	12.6.2017
T0066/2014	Bezpečnostní příčka Knauf W118	v provedení W112 - RC3	KNAUF Praha, spol. s r.o.	KNAUF Praha, spol. s r.o.	Mladoboleslavská 949	Praha 9 - Kbely 197 00	3	SS3=3	12.6.2017
T0067/2014	Bezpečnostní příčka Knauf W118	v provedení W112 - RC2 s plechem	KNAUF Praha, spol. s r.o.	KNAUF Praha, spol. s r.o.	Mladoboleslavská 949	Praha 9 - Kbely 197 00	2	SS3=2	18.12.2016
T0068/2014	Bezpečnostní příčka Knauf W118	v provedení W112 - RC2 se skelnou výztužnou tkaninou	KNAUF Praha, spol. s r.o.	KNAUF Praha, spol. s r.o.	Mladoboleslavská 949	Praha 9 - Kbely 197 00	2	SS3=2	18.12.2016
T0069/2014	Bezpečnostní cylindrická vložka EVVA typ EPS/EPS-M/DPI SG	včetně bezpečnostního kování s krytem cylindrické vložky	EVVA Sicherheitstechnologie GmbH	EVVA spol. s r. o. Praha	V Bokách II 1048	Praha 5 - Hlubočepy 152 00	3	SS4=3	18.4.2016

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. a) zákona č. 412/2005 Sb.
MECHANICKÉ ZÁBRANNÉ PROSTŘEDKY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T0070/2014	Bezpečnostní dveře BEDEX STANDARD 2 R	s požární odolností EI 30 D2 do stávající zárubně	MRB Sazovice, spol. s r.o.	MRB Sazovice, spol. s r.o.	Sazovice 191	Mysločovice 763 01	2	SS3=2, SS4=1	10.4.2017
T0071/2014	Bezpečnostní dveře BEDEX STANDARD 2 R	do stávající zárubně	MRB Sazovice, spol. s r.o.	MRB Sazovice, spol. s r.o.	Sazovice 191	Mysločovice 763 01	2	SS3=2, SS4=1	10.4.2017
T0072/2014	Bezpečnostní dveře BEDEX STANDARD 3 R	s požární odolností EI 30 D2 do stávající zárubně	MRB Sazovice, spol. s r.o.	MRB Sazovice, spol. s r.o.	Sazovice 191	Mysločovice 763 01	3	SS3=3, SS4=2	10.4.2017
T0073/2014	Bezpečnostní dveře BEDEX STANDARD 3 R	do stávající zárubně	MRB Sazovice, spol. s r.o.	MRB Sazovice, spol. s r.o.	Sazovice 191	Mysločovice 763 01	3	SS3=3, SS4=2	10.4.2017
T0074/2014	Mobilní skříňový trezor typ HS 0 a MST 00	varianty jsou uvedeny v příloze	Metalsafe s.r.o.	Metalsafe s.r.o.	Jana Švermy 1339	Smržovka 468 51	2	SS1=2, SS2=2	9.10.2017
T0075/2014	Mobilní skříňový trezor typ HS I a MST 10	varianty jsou uvedeny v příloze	Metalsafe s.r.o.	Metalsafe s.r.o.	Jana Švermy 1339	Smržovka 468 51	3	SS1=3, SS2=2	9.10.2017
T0076/2014	Mobilní skříňový trezor typ HS II a MST 20	varianty jsou uvedeny v příloze	Metalsafe s.r.o.	Metalsafe s.r.o.	Jana Švermy 1339	Smržovka 468 51	4	SS1=4, SS2=2	9.10.2017
T0077/2014	Mobilní skříňový trezor typová řada TSS	odvozené varianty jsou uvedeny v příloze	SAFETRONICS a.s.	SAFEtronics PRAHA a.s.	Českomoravská 7/808	Praha 9 190 00	3	SS1=3, SS2=2	20.1.2015
T0078/2014	Bezpečnostní dveře BEDEX FRD IV RC3 jednokřídlové a dvoukřídlové	s požární odolností EW 15 - EW 90 DP1 a panikovou funkcí	MRB Sazovice, spol. s r.o.	MRB Sazovice, spol. s r.o.	Sazovice 191	Mysločovice 763 01	3	SS3=3, SS4=2	16.5.2016
T0079/2014	Bezpečnostní dveře FRD IV RC3 jednokřídlové a dvoukřídlové	s požární odolností EW 15 - EW 90 DP1 a panikovou funkcí	VIPAX, a.s.	VIPAX, a.s.	Tečovská 1052	Zlín - Malenovice 763 02	3	SS3=3, SS4=2	16.5.2016
T0080/2014	Nůžková mříž dvoukřídlová typ NMK3RC	Nůžková mříž jednokřídlová typ NMK3RC	KOPEČEK company s.r.o.	KOPEČEK company s.r.o.	Viničné Šumice 393	Viničné Šumice 664 06	3	SS3=3, SS4=2	20.11.2017

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. a) zákona č. 412/2005 Sb.
MECHANICKÉ ZÁBRANNÉ PROSTŘEDKY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T0081/2014	Trezorové dveře TDV	varianty jsou uvedeny v příloze	T-SAFE s.r.o.	T-SAFE s.r.o.	Lomná 537	Frenštát pod Radhoštěm 744 01	3	SS1=3, SS2=2	16.9.2017
T0082/2014	Mobilní skříňový trezor typ nábytkový trezor NT/Z3	varianty jsou uvedeny v příloze	T-SAFE s.r.o.	T-SAFE s.r.o.	Lomná 537	Frenštát pod Radhoštěm 744 01	1C	S1=3	20.11.2017
T0083/2014	Trezorové dveře typ TDD	varianty jsou uvedeny v příloze	T-SAFE s.r.o.	T-SAFE s.r.o.	Lomná 537	Frenštát pod Radhoštěm 744 01	3	SS1=3, SS2=2	15.4.2017
T0084/2014	Archivační skříň typ AS 6, AS 10	Skříň na zbraně typ SZ 6, SZ 10	T-SAFE s.r.o.	T-SAFE s.r.o.	Lomná 537	Frenštát pod Radhoštěm 744 01	1B	S1=2	22.7.2017
T0085/2014	Stěnový sejf	typ SS	T-SAFE s.r.o.	T-SAFE s.r.o.	Lomná 537	Frenštát pod Radhoštěm 744 01	1B	S1=2	14.6.2017
T0086/2014	Nábytkový sejf	typ NS	T-SAFE s.r.o.	T-SAFE s.r.o.	Lomná 537	Frenštát pod Radhoštěm 744 01	1B	S1=2	14.6.2017
T0001/2015	Bezpečnostní protipožární dveře typ DPB2	instalované v ocelové protipožární zárubni z plechu tloušťky 1,5 mm	SOLODOOR a.s.	SOLODOOR a.s.	Nádražní 166	Sušice 342 01	2	SS3=2, SS4=1	11.9.2017
T0002/2015	Stěnový trezor	typ ST, varianty jsou uvedeny v příloze	SAFETRONICS a.s.	SAFEtronics PRAHA a.s.	Českomoravská 7/808	Praha 9 190 00	3	SS1=3, SS2=2	4.12.2017
T0003/2015	Datová komora	typ GranITE-Room. cert	RZ-Products GmbH	SYPROS RBW s.r.o.	Revoluční 1082/8	Praha 1 - Nové Město 110 00	2	SS3=2, SS4=1	20.11.2017
T0004/2015	Pevná otevírací mříž typ MKO3RC	jednokřídlová a dvoukřídlová	KOPEČEK company s.r.o.	KOPEČEK company s.r.o.	Viničné Šumice 393	Viničné Šumice 664 06	3	SS3=3, SS4=2	1.1.2018
T0005/2015	Pevná mříž	typ MPK3RC	KOPEČEK company s.r.o.	KOPEČEK company s.r.o.	Viničné Šumice 393	Viničné Šumice 664 06	3	SS3=3	1.1.2018
T0006/2015	Bezpečnostní protipožární dveře ADORY DP II - RC 3/1	jednokřídlové dveře otevírané směrem do a z chráněného prostoru	ADOR CZ s.r.o.	ADOR CZ s.r.o.	Dobrovského 981	Lanškroun - Žichlínské Předměstí 563 01	3	SS3=3, SS4=2	28.8.2017

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. b) zákona č. 412/2005 Sb.
ELEKTRICKÁ ZÁMKOVÁ ZAŘÍZENÍ A SYSTÉMY PRO KONTROLU VSTUPŮ

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T3006/2012	Systém kontroly vstupů	IDSIMA 4-PRO	IMA s.r.o.	IMA s.r.o.	Na Valentince 1003/1	150 00 Praha 5	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	04.04.2015
T3007/2012	Systém kontroly vstupů	NORTHERN PRO-2200	Honeywell Access Systems	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	22.05.2015
T3009/2012	Systém kontroly vstupů s biometrickou čtečkou	FACEglobe	EPLcond s.r.o.	EPLcond s.r.o.	Purkyňova 2873/19a	301 00 Plzeň	3 - 4	V závislosti na realizaci systému SS6=3 až 4 body.	04.09.2015
T3010/2012	Systém kontroly vstupů	Bewator Cotag řady 4000 a 5000	Siemens AG - Security Products	Sieza, s.r.o.	Štúrova 1282	142 00 Praha 4	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	14.08.2015
T3011/2012	Systém kontroly vstupu	N-1000-III/IV (SW-WIN-PAK SE/PE)	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	09.10.2015
T3012/2012	Systém kontroly vstupu	NetAXS (SW-WIN-PAK SE/PE), NetAXS-123 (SW-WIN-PAK SE/PE)	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	09.10.2015
T3013/2012	Systém kontroly vstupu	MAXM2000	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	09.10.2015
T3014/2012	Systém kontroly vstupu	C080	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	09.10.2015
T3015/2012	Systém kontroly vstupu	PW-6000 (SW-ProWatch)	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	09.10.2015
T3001/2013	Systém kontroly vstupu	ASSET 812 X	Trade FIDES, a.s.	Trade FIDES, a.s.	Dornych 57	617 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	26.11.2015
T3002/2013	Systém kontroly vstupu	ASSET 801 Z	Trade FIDES, a.s.	Trade FIDES, a.s.	Dornych 57	617 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	26.11.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. b) zákona č. 412/2005 Sb.
ELEKTRICKÁ ZÁMKOVÁ ZAŘÍZENÍ A SYSTÉMY PRO KONTROLU VSTUPŮ

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T3003/2013	Systém kontroly vstupů	IDENT-KEY 3 - N023312.10	Honeywell Security Group Novar GmbH	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	12.12.2015
T3004/2013	Systém kontroly vstupu	REA::MP	Cominfo, a.s	Cominfo, a.s	Nábřeží 695	760 01 Zlín	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	18.01.2016
T3005/2013	Systém kontroly vstupu - identifikační snímač	ISP PRIME	Jan Nižník - ELVIS	Jan Nižník - ELVIS	Brněnská 40	591 01 Žďár nad Sázavou	2		07.02.2016
T3006/2013	Systém kontroly vstupu	ACS-8	Honeywell Security Group, Novar GmbH	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 3	V závislosti na realizaci systému SS6=2 až 3 body.	25.03.2016
T3007/2013	Systém kontroly vstupu	AKTION	EFG CZ spol. s r.o.	EFG CZ spol. s r.o.	Na Jarově 4	130 00 Praha 3	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	02.05.2016
T3008/2013	Systém kontroly vstupu	ZaSU	ORZO SECURITY, spol. s r.o.	NOVON SECURITY, s.r.o.	Poděbradova 3264/73	702 00 Ostrava	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	20.11.2015
T3009/2013	Systém kontroly vstupu	SiPass Integrated	Siemens, s.r.o.	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	26.09.2016
T3010/2013	Systém kontroly vstupů	Bewator Cotag řady 4000 a 5000	Siemens A G Security Products	Sieza, s.r.o.	Štúrova 1282	142 00 Praha 4	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	26.09.2016
T3011/2013	Systém kontroly vstupů	ALTEX	ALIMEX s.r.o.	ALIMEX s.r.o.	Ke Zvoli 339	252 41 Dolní Břežany	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	10.10.2016
T3012/2013	Systém kontroly vstupů	ID-WARE	ID-KARTA s.r.o.	ID-KARTA s.r.o.	Hlavní 3	747 70 Opava 9	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	10.10.2016
T3013/2013	Systém kontroly vstupů	CND 5.0	Colsys s.r.o.	Colsys s.r.o.	Buštěhradská 109	272 03 Kladno-Dubí	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	24.10.2016
T3014/2013	Čtečka bezkontaktních karet	RSW.04	IMA s.r.o.	IMA s.r.o.	Na Valentince 1003/1	150 00 Praha 5	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	24.10.2016

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. b) zákona č. 412/2005 Sb.
ELEKTRICKÁ ZÁMKOVÁ ZAŘÍZENÍ A SYSTÉMY PRO KONTROLU VSTUPŮ

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T3015/2013	Systém kontroly vstupů	ANeT-UNI-II	ANeT - Advanced Network Technology, s.r.o.	ANeT - Advanced Network Technology, s.r.o.	Šumavská 35	602 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	21.11.2016
T3001/2014	Systém kontroly vstupů	NetAXS-123 (SW-WIN-PAK XE/SE/PE) s řídící jednotkou NX2P (NX1P)	Honeywell Access Systems	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	05.12.2016
T3002/2014	Systém kontroly vstupů	NetAXS-123 (SW-WIN-PAK XE/SE/PE) s řídící jednotkou NX3MPS (NX2MPS, NX1MPS)	Honeywell Access Systems	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	05.12.2016
T3003/2014	Systém kontroly vstupů	ANeT-LAN-APAS	ANeT - Advanced Network Technology, s.r.o.	ANeT - Advanced Network Technology, s.r.o.	Šumavská 35	602 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	13.3.2017
T3004/2014	Systém kontroly vstupů	HUB Pro (SW SBI/ SW SKYLA Pro II)	Honeywell, spol. s r. o. - Security Products o.z.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	29.5.2017
T3005/2014	Systém kontroly vstupů	ASSET 804Z	Trade FIDES, a.s.	Trade FIDES, a.s.	Dornych 57	617 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	9.10.2017
T3006/2014	Systém kontroly vstupů	PRO-3200 (SW: WIN-PAK XE/SE/PE)	Honeywell Access Systems	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	25.9.2017
T3007/2014	Systém kontroly vstupů	ATS	UTC Fire & Security	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	23.10.2017
T3008/2014	Systém kontroly vstupů	IDENT-KEY 3	Honeywell Security Deutschland	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2 - 4	V závislosti na realizaci systému SS6=2 až 4 body.	6.11.201

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1018/2012	Detektor pohybu kombinovaný (PIR +MW)	KX15DTAM	Pyronix Ltd.	ABBAS, a.s.	Edisonova 5	612 00 Brno	3	SS91=3	4.4.2015
T1019/2012	Otřesový detektor	VV600/602 Plus	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	4	SS91=4	4.4.2015
T1020/2012	Otřesový detektor	FENCE GUARD	N - ETS, s.r.o.	N - ETS, s.r.o.	Mladoboleslavská 76/35	Praha 9, PSČ 197 00	3	SS91=3	24.5.2015
T1021/2012	Ústředna EZS	MC 1500	ABI Sicherheitssysteme GmbH	CM security system, s.r.o.	B. Němcové 29	388 01 Blatná	4	SS91=4	15.6.2015
T1022/2012	Detektor pohybu PIR	OML-AM	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	3	SS91=3	23.05.2015
T1023/2012	Detektor pohybu kombinovaný (PIR +MW)	MX50QZ-G2	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	2	SS91=2	23.05.2015
T1024/2012	Detektor pohybu kombinovaný (PIR +MW)	MX40QZ-G2	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	2	SS91=2	23.05.2015
T1025/2012	Detektor pohybu kombinovaný (PIR +MW)	MX40PT-G2	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	2	SS91=2	23.05.2015
T1026/2012	Detektor pohybu PIR	LX802N	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	2	SS91=2	04.06.2015
T1027/2012	Detektor pohybu PIR	LX402	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	2	SS91=2	04.06.2015
T1028/2012	Detektor pohybu PIR	VX402	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	2	SS91=2	04.06.2015
T1029/2012	Detektor pohybu PIR	CX702	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	2	SS91=2	04.06.2015
T1030/2012	Detektor pohybu PIR	RX40QZD	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	2	SS91=2	04.06.2015
T1031/2012	Detektor pohybu PIR	FX50SQD	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	2	SS91=2	04.06.2015
T1032/2012	Detektor směrový (infrazávora)	AX-350DH MkIII, AX-650DH MkIII	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	4	SS91=4	19.06.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1033/2012	Detektor směrový (infrazávora)	AX-100TF (BE), AX-200TF (BE)	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	4	SS91=4	19.06.2015
T1034/2012	Detektor směrový (infrazávora)	AX-70TN (BE), AX-130TN (BE), AX-200TN (BE)	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	4	SS91=4	19.06.2015
T1035/2012	Detektor směrový (infrazávora)	AX-350TF, AX-650TF	Optex Co., Ltd.	Optex Co., Ltd.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	4	SS91=4	19.06.2015
T1036/2012	Detektor pohybu kombinovaný (PIR +MW)	Viewguard N033440	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	23.05.2015
T1037/2012	Detektor pohybu PIR	Viewguard N033430	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	23.05.2015
T1038/2012	Detektor pohybu kombinovaný (PIR +MW)	DT7435EU	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	23.05.2015
T1039/2012	Detektor pohybu PIR	IS215T, IS215TCE	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	23.05.2015
T1040/2012	Detektor otevření	EMPS50	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015
T1041/2012	Detektor otevření	N030260.16, N030261.16	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	4	SS91=4	19.06.2015
T1042/2012	Detektor otevření	N030295	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	19.06.2015
T1043/2012	Detektor otevření	N030210.16, N030247.16	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015
T1044/2012	Detektor otevření	N030201.16, N030243.16	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1045/2012	Detektor otevření	N030270.16, N030271.16	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	4	SS91=4	19.06.2015
T1046/2012	Detektor otevření	N030100.16	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015
T1047/2012	Otřesový detektor	SC100	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	4	SS91=4	19.06.2015
T1048/2012	Otřesový detektor	SC105	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	4	SS91=4	19.06.2015
T1049/2012	Detektor rozbití skla	FG730	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015
T1050/2012	Detektor rozbití skla	FG1625TAS-G3	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	19.06.2015
T1062/2012	Detektor otevření	DC101	UTC Fire & Security B.V.	UTC Fire & Security ČR s.r.o.	Uzbecká 572/32	625 00 Brno	2	SS91=2	20.03.2015
T1063/2012	Detektor otevření	DC103, DC111	UTC Fire & Security B.V.	UTC Fire & Security ČR s.r.o.	Uzbecká 572/32	625 00 Brno	3	SS91=3	20.03.2015
T1064/2012	Otřesový detektor	VV700RA	UTC Fire & Security B.V.	UTC Fire & Security ČR s.r.o.	Uzbecká 572/32	625 00 Brno	4	SS91=4	20.03.2015
T1065/2012	Detektor pohybu PIR	EV1012AM, EV1116AM, VE735AM, VE736AM	UTC Fire & Security B.V.	UTC Fire & Security ČR s.r.o.	Uzbecká 572/32	625 00 Brno	3	SS91=3	20.03.2015
T1066/2012	Tísňové tlačítko	HB304/1	UTC Fire & Security B.V.	UTC Fire & Security ČR s.r.o.	Uzbecká 572/32	625 00 Brno	2	SS91=2	20.03.2015
T1067/2012	Detektor pohybu kombinovaný (PIR +MW)	DD669AM, DD477AM	UTC Fire & Security B.V.	UTC Fire & Security ČR s.r.o.	Uzbecká 572/32	625 00 Brno	3	SS91=3	20.03.2015
T1068/2012	Detektor pohybu kombinovaný (PIR +MW)	DD669	UTC Fire & Security B.V.	UTC Fire & Security ČR s.r.o.	Uzbecká 572/32	625 00 Brno	2	SS91=2	20.03.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1069/2012	Detektor pohybu PIR	EV1012, EV1116, VE735, VE736	UTC Fire & Security B.V.	UTC Fire & Security ČR s.r.o.	Uzbecká 572/32	625 00 Brno	2	SS91=2	20.03.2015
T1070/2012	Duální (PIR + MW) detektor s antimaskingem	TOWER12AM (0-101612)	Visonic, Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	23.05.2015
T1071/2012	Stropní duální (PIR + MW) detektor	DUO240E (0-1826-0)	Visonic, Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	23.05.2015
T1072/2012	Stropní PIR detektor	DISC (0-1110-0)	Visonic, Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	23.05.2015
T1073/2012	Duální (PIR + MW) detektor s antimaskingem	DT7550UK2	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	23.05.2015
T1074/2012	Jiskrově bezpečný duální detektor Viewguard v sestavě	VW33440Ex, relé typ MM5016DC12, zdroj typ MM2012-4/1	MM Group, s.r.o.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	23.05.2015
T1075/2012	PIR detektor	PRESTIGE COMPACT IR	Texecom, Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	23.05.2015
T1076/2012	Duální (PIR + MW) detektor s antimaskingem	NEXT PLUS DUO AM	Visonic, Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	23.05.2015
T1077/2012	PIR detektor	SPY1, SPY2, SPY3, SPY4	Visonic, Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	23.05.2015
T1078/2012	Magnetický kontakt	MC2108	Knight Fire & Security Products Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015
T1079/2012	Magnetický kontakt	MC2304	Knight Fire & Security Products Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015
T1080/2012	Magnetický kontakt	QST-GN	Elmdene International Limited	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1081/2012	Magnetický kontakt	EN3-QSC-GN	Elmdene International Limited	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	19.06.2015
T1082/2012	Magnetický kontakt	6RSL-GN	Elmdene International Limited	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015
T1083/2012	Magnetický kontakt	SC517/WH/MULTI/G2	CQR Security	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015
T1084/2012	Magnetický kontakt	SC517/WH/MULTI/G3	CQR Security	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	19.06.2015
T1085/2012	Otřesový detektor	AEB-0001	Texecom Limited	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015
T1086/2012	Detektor tříštění skla	N032420 (DETEKT 1000, BUS1)	Honeywell Security Deutschland	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	19.06.2015
T1087/2012	Infrapasivní detektor	3D ANTI-MASK	MAXIMUM ELECTRONICS LTD.	VARIANT plus, spol. s r.o.	U Obůrky 5	674 01 Třebíč	3	SS91=3	09.08.2015
T1088/2012	Kombinovaný detektor PIR+MW, AM	DOUBLE-TEC	MAXIMUM ELECTRONICS LTD.	VARIANT plus, spol. s r.o.	U Obůrky 5	674 01 Třebíč	3	SS91=3	09.08.2015
T1089/2012	Kombinovaný detektor PIR+MW, AM	OUT-LOOK	MAXIMUM ELECTRONICS LTD.	VARIANT plus, spol. s r.o.	U Obůrky 5	674 01 Třebíč	3	SS91=3	09.08.2015
T1090/2012	Kombinovaný detektor PIR+MW, AM	GUARD	MAXIMUM ELECTRONICS LTD.	VARIANT plus, spol. s r.o.	U Obůrky 5	674 01 Třebíč	3	SS91=3	09.08.2015
T1091/2012	Ústředna PZTS	SPC5320.320-L1, SPC4320.320-L1	SIEMENS	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2	SS91=2	28.06.2015
T1092/2012	Ústředna PZTS	SPC6330.320-L1, SPC5330.320-L1	SIEMENS	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	3	SS91=3	28.06.2015
T1093/2012	Ústředna PZTS	SPC6330.420-L1	SIEMENS	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	4	SS91=4	28.06.2015
T1094/2012	Detektor tříštění skla	AD700, AD700AM	SIEMENS	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2	SS91=2	28.06.2015
T1095/2012	Seismický detektor	GM730, GM760, GM775	SIEMENS	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	4	SS91=4	28.06.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1102/2012	Ústředna PZTS	561-MB256	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	4	SS91=4	09.10.2015
T1103/2012	Ústředna PZTS	561-MB24	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1104/2012	Sběrnicový PIR detektor	"NO 33332.20, NO 33332.20 + NO 33434 typ záclona, NO 33332.20 + NO 33435 typ dlouhý dosah"	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1105/2012	Sběrnicový PIR detektor	"NO 33432.20, NO 33432.20 + NO 33434 stěna, NO 33432.20 + NO 33435 chodba"	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	09.10.2015
T1106/2012	Venkovní PIR detektor	GJD300 (D-Tect2)	GJD Manufacturing Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1107/2012	Venkovní duální PIR + MW detektor	GJD310 (D-Tect3)	GJD Manufacturing Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1108/2012	Venkovní PIR detektor	GJD350 (D-Tect50)	GJD Manufacturing Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1109/2012	Ústředna PZTS	"GALAXYGD-520 TPKIT (C520-C E4-TCKP1), GALAXYGD-520, GALAXYGD-264, (264TPKIT), GALAXYGD-96, (96TPKIT), GALAXYGD-48"	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	09.10.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1110/2012	Ústředna PZTS	GALAXY FLEX 100 (C001-M-E2-100), GALAXY FLEX 50, GALAXY FLEX 20	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1111/2012	Bezdrátové tísňové tlačítko	MCT201-868, MCT201 WP-868	Visonic	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1112/2012	Tísňové tlačítko	ART476	Cooper Csa Srl.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1113/2012	Tísňové tlačítko	ELM-PA-G3-W	Elmdene International Limited	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	4	SS91=4	09.10.2015
T1114/2012	Tísňové tlačítko	S3040/SR	Sentrol INC.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	09.10.2015
T1115/2012	Napájecí zdroj zálohovaný v krytu	AXSP K40/10A, AXSP K40/5A	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	09.10.2015
T1116/2012	Napájecí zdroj zálohovaný v krytu	SMPSW K15/1,7A	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1117/2012	Napájecí zdroj zálohovaný v krytu	UNIPOWER MINI/ K15T	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	09.10.2015
T1118/2012	Stropní PIR detektor s AM	PRESTIGE AM360QD	Texecom Limited	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	09.10.2015
T1119/2012	PIR detektor	PRESTIGE IR	Texecom Limited	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1120/2012	PIR detektor	PRESTIGE MR	Texecom Limited	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1121/2012	Duální detektor PIR + MW	PRESTIGE DT	Texecom Limited	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1122/2012	PIR detektor s AM	PRESTIGE AMQD PLUS	Texecom Limited	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	09.10.2015
T1123/2012	Duální detektor PIR + MW s AM	PRESTIGE AMDT PLUS	Texecom Limited	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	09.10.2015
T1124/2012	Poplachový zabezpečovací a tísňový systém	JA-80 OASIS	JABLOTRON ALARMS	JABLOTRON ALARMS	Pod Skalkou 4567/33	466 01 Jablonec nad Nisou	2	SS91=2	21.12.2015
T1125/2012	Detektor pohybu PIR	JS-20	JABLOTRON ALARMS	JABLOTRON ALARMS	Pod Skalkou 4567/33	466 01 Jablonec nad Nisou	2	SS91=2	21.12.2015
T1127/2012	Kombinovaný detektor pohybu a rozbití skla	JS-25	JABLOTRON ALARMS	JABLOTRON ALARMS	Pod Skalkou 4567/33	466 01 Jablonec nad Nisou	2	SS91=2	21.12.2015
T1128/2012	Detektor rozbití skla	GBS-210	JABLOTRON ALARMS	JABLOTRON ALARMS	Pod Skalkou 4567/33	466 01 Jablonec nad Nisou	2	SS91=2	15.12.2016
T1129/2012	Duální detektor s AM - standardní zrcadlo	"NO33442.20, NO33442.20 + NO33434 stěna, NO33442.20 + NO33435 chodba"	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	09.10.2015
T1130/2012	Duální detektor - standardní zrcadlo	"NO33443.20, NO33443.20 + NO33434 stěna, NO33443.20 + NO33435 chodba"	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	09.10.2015
T1131/2012	Ústředna PZTS	561-MB100, 561-MB100 v krytu ZG4	Honeywell	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	4	SS91=4	09.10.2015
T1132/2012	Detektor otevření	DC115	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	3	SS91=3	21.11.2015
T1133/2012	Detektor otevření	DC128	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	3	SS91=3	21.11.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1134/2012	Detektor otevření	DC138	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	3	SS91=3	21.11.2015
T1135/2012	Detektor otevření	DC148	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	3	SS91=3	21.11.2015
T1136/2012	Detektor otevření	DC408	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	3	SS91=3	21.11.2015
T1137/2012	Detektor pohybu kombinovaný (PIR +MW)	DD1012	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	2	SS91=2	21.11.2015
T1138/2012	Detektor pohybu kombinovaný (PIR +MW)	DD1012RAM	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	2	SS91=2	21.11.2015
T1139/2012	Detektor pohybu kombinovaný (PIR +MW)	DD1012AM	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	3	SS91=3	21.11.2015
T1140/2012	Detektor pohybu kombinovaný (PIR +MW)	DDV1016	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	2	SS91=2	21.11.2015
T1141/2012	Detektor pohybu kombinovaný (PIR +MW)	DDV1016AM	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	3	SS91=3	21.11.2015
T1142/2012	Ústředna EZS s bezdrátovou nástavbou	DIGIPLEX EVO 192	PARADOX SECURITY SYSTEMS	VARIANT plus, spol. s r.o.	U Obůrky 5	674 01 Třebíč	2 - 3	SS91=3, SS91=2 (při použití radiového systému)	09.08.2015
T1143/2012	Detektor otevření	3G-RM-20	SENTEK	VARIANT plus, spol. s r.o.	U Obůrky 5	674 01 Třebíč	3	SS91=3	15.11.2015
T1144/2012	Detektor otevření	3G-SM-60	SENTEK	VARIANT plus, spol. s r.o.	U Obůrky 5	674 01 Třebíč	3	SS91=3	15.11.2015
T1145/2012	Detektor otevření	3G-SM-70MET	SENTEK	VARIANT plus, spol. s r.o.	U Obůrky 5	674 01 Třebíč	3	SS91=3	15.11.2015
T1146/2012	Detektor otevření	3G-SM-85MET	SENTEK	VARIANT plus, spol. s r.o.	U Obůrky 5	674 01 Třebíč	3	SS91=3	15.11.2015
T1001/2013	Ústředna PZTS	ASSET 812 X	Trade FIDES, a.s.	Trade FIDES, a.s.	Dornych 57	617 00 Brno	4	SS91=4	26.11.2015
T1002/2013	Ústředna PZTS	ASSET 801 Z	Trade FIDES, a.s.	Trade FIDES, a.s.	Dornych 57	617 00 Brno	3	SS91=3	26.11.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1003/2013	Perimetrický systém	PERIDECT	SIEZA, s.r.o.	SIEZA, s.r.o.	Štúrova 1282	142 00 Praha 4	4	SS91=4	18.12.2015
T1004/2013	Systém pro kontrolu a ochranu strážních/nástrahový radiový systém	"RGS/RSS RSS-SMD, RGS/RSS-CVP, RGS-M"	SIEZA, s.r.o.	SIEZA, s.r.o.	Štúrova 1282	142 00 Praha 4	3	SS91=3	18.12.2015
T1005/2013	Detektor pohybu PIR	RK312PR	RISCO Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	12.12.2015
T1006/2013	Detektor pohybu kombinovaný (PIR +MW)	RK315DT	RISCO Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	12.12.2015
T1007/2013	Detektor pohybu PIR	RK800Q-G3	RISCO Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	12.12.2015
T1008/2013	Detektor pohybu kombinovaný (PIR +MW)	RK825DT-G3, RK815DT-G3	RISCO Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	12.12.2015
T1009/2013	Detektor pohybu PIR	RXC-ST (CORE)	OPTEX Co., Ltd.	OPTEX SECURITY Sp. z o.o.	Bitwy Warszawskiej 1920r 7B	02-366 Warszawa, Poland	2	SS91=2	12.12.2015
T1010/2013	Detektor pohybu PIR	SIP-100 (Redwall-V)	OPTEX Co., Ltd.	OPTEX SECURITY Sp. z o.o.	Bitwy Warszawskiej 1920r 7B	02-366 Warszawa, Poland	2	SS91=2	12.12.2015
T1011/2013	Detektor pohybu PIR	SIP-404/5 (Redwall-V), SIP-404 (Redwall-V)	OPTEX Co., Ltd.	OPTEX SECURITY Sp. z o.o.	Bitwy Warszawskiej 1920r 7B	02-366 Warszawa, Poland	2	SS91=2	12.12.2015
T1012/2013	Detektor pohybu PIR	SIP-3020/5 (Redwall-V), SIP-3020 (Redwall-V)	OPTEX Co., Ltd.	OPTEX SECURITY Sp. z o.o.	Bitwy Warszawskiej 1920r 7B	02-366 Warszawa, Poland	2	SS91=2	12.12.2015
T1013/2013	Detektor pohybu PIR	SIP-4010/5 (Redwall-V), SIP-4010 (Redwall-V)	OPTEX Co., Ltd.	OPTEX SECURITY Sp. z o.o.	Bitwy Warszawskiej 1920r 7B	02-366 Warszawa, Poland	2	SS91=2	12.12.2015
T1014/2013	Detektor pohybu PIR	SIP-5030 (Redwall-V)	OPTEX Co., Ltd.	OPTEX SECURITY Sp. z o.o.	Bitwy Warszawskiej 1920r 7B	02-366 Warszawa, Poland	2	SS91=2	12.12.2015
T1015/2013	Detektor pohybu PIR	SX360Z	OPTEX Co., Ltd.	OPTEX SECURITY Sp. z o.o.	Bitwy Warszawskiej 1920r 7B	02-366 Warszawa, Poland	2	SS91=2	12.12.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1016/2013	Detektor rozbití skla	FG1625, FG1625F, FG1625RT, FG1625TAS	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	12.12.2015
T1017/2013	Detektor směrový (infrazávora)	RN4 75-150 (REDNET 75-150), RN4 25-75, RN4 10-25	OPTEX Co., Ltd.	OPTEX SECURITY Sp. z o.o.	Bitwy Warszawskiej 1920r 7B	02-366 Warszawa, Poland	4	SS91=4	12.12.2015
T1018/2013	Otřesový detektor	VIBRO	OPTEX Co., Ltd.	OPTEX SECURITY Sp. z o.o.	Bitwy Warszawskiej 1920r 7B	02-366 Warszawa, Poland	2	SS91=2	12.12.2015
T1019/2013	Detektor pohybu kombinovaný (PIR +MW)	RK150DT-G3	RISCO Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	12.12.2015
T1020/2013	Detektor pohybu kombinovaný (PIR +MW)	RK150T	RISCO Ltd.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	12.12.2015
T1021/2013	Perimetrický systém (otřesový detektor)	FP 300	VARIANT plus, spol. s r.o.	VARIANT plus, spol. s r.o.	U Obůrky 5	674 01 Třebíč	3	SS91=3	05.11.2015
T1022/2013	Perimetrický systém (otřesový detektor)	FP 600	VARIANT plus, spol. s r.o.	VARIANT plus, spol. s r.o.	U Obůrky 5	674 01 Třebíč	3	SS91=3	05.11.2015
T1023/2013	Detektor otevření	DC108	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	2	SS91=2	07.02.2016
T1024/2013	Detektor otevření	DC120	UTC Fire & Security B.V.	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	2	SS91=2	07.02.2016
T1025/2013	Detektor pohybu PIR	IS2535T, IS2535TC	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	21.02.2016
T1026/2013	Detektor pohybu PIR	IS2560T, IS2560TC	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	21.02.2016
T1027/2013	Detektor pohybu PIR	IS25100TC	Honeywell International Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	21.02.2016
T1028/2013	Detektor pohybu PIR	HX-40AM, HX-40	OPTEX Co., Ltd.	OPTEX SECURITY Sp. z o.o.	Bitwy Warszawskiej 1920r 7B	02-366 Warszawa, Poland	2	SS91=2	21.02.2016
T1029/2013	Detektor pohybu PIR	HX-80NAM, HX-80N	OPTEX Co., Ltd.	OPTEX SECURITY Sp. z o.o.	Bitwy Warszawskiej 1920r 7B	02-366 Warszawa, Poland	2	SS91=2	21.02.2016

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1030/2013	Detektor otevření	GP001/AB/G2	CQR Fire & Security	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	21.02.2016
T1031/2013	Detektor otevření	GP001/AB/G3	CQR Fire & Security	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	21.02.2016
T1032/2013	Ústředna PZTS	ZaSU	ORZO SECURITY, spol. s r.o.	NOVON SECURITY, s.r.o.	Poděbradova 3264/73	702 00 Ostrava	3	SS91=3	20.11.2015
T1033/2013	Detektor pohybu PIR	ADM-Q12	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1034/2013	Detektor pohybu PIR	IR100B	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1035/2013	Detektor pohybu PIR	IR120C	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1036/2013	Detektor pohybu PIR	IR200C-II	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1037/2013	Detektor pohybu PIR	IR261	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1038/2013	Detektor pohybu PIR	ADM-Q12T	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	3	SS91=3	14.03.2016
T1039/2013	Detektor pohybu PIR	IR270T	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	3	SS91=3	14.03.2016
T1040/2013	Detektor pohybu kombinovaný (PIR +MW)	ADM-QXB12	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1041/2013	Detektor pohybu kombinovaný (PIR +MW)	IRM120C	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1042/2013	Detektor pohybu kombinovaný (PIR +MW)	IRM270MD	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1043/2013	Detektor pohybu kombinovaný (PIR +MW)	ADM-QXB12T	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	3	SS91=3	14.03.2016

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1044/2013	Detektor pohybu kombinovaný (PIR +MW)	IRM270T	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	3	SS91=3	14.03.2016
T1045/2013	Detektor pohybu kombinovaný (PIR +MW)	UP370T	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	3	SS91=3	14.03.2016
T1046/2013	Detektor pohybu PIR	IR120C Ex	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1047/2013	Detektor pohybu PIR	IR200C-II Ex	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1048/2013	Detektor pohybu PIR	IS390	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1049/2013	Detektor pohybu PIR	IS392	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1050/2013	Detektor pohybu PIR	IS404	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1051/2013	Detektor otevření	MK240	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1052/2013	Detektor otevření	MK250	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1053/2013	Detektor otevření	MK446	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1054/2013	Detektor otevření	MK270	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	3	SS91=3	14.03.2016
T1055/2013	Detektor otevření	MK272	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	3	SS91=3	14.03.2016
T1056/2013	Detektor otevření	MK470	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	3	SS91=3	14.03.2016
T1057/2013	Detektor otevření	MK472	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	3	SS91=3	14.03.2016
T1058/2013	Detektor směrový (infrazávora)	IS433, IS434, IS435	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	4	SS91=4	14.03.2016
T1059/2013	Detektor směrový (infrazávora)	IS443, IS444, IS445	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	4	SS91=4	14.03.2016

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1060/2013	Detektor rozbití skla	AGB600	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1061/2013	Tísňové tlačítko	HB 105	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1062/2013	Tísňové tlačítko	FK 32	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	2	SS91=2	14.03.2016
T1063/2013	Ústředna PZTS	SI 410/411, SAK41	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 PRAHA 13	3	SS91=3	14.03.2016
T1064/2013	Ústředna PZTS	SATEL INTEGRA 32 (INTEGRA 64, INTE-GRA 128)	SATEL Sp. z o.o.	EUROALARM, spol. s r.o.	Dražovice 275	683 01 Dražovice	2	SS91=2	07.06.2015
T1065/2013	Poplachový zabez-pečovací systém	JA-100	JABLOTRON ALARMS a.s.	JABLOTRON ALARMS a.s.	Pod Skalkou 4567/33	466 01 Jablonec nad Nisou	2	SS91=2	19.07.2017
T1001/2014	Detektor pohybu PIR	PDM-I12	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2	SS91=2	10.11.2016
T1002/2014	Detektor pohybu PIR	PDM-I12T	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	3	SS91=3	10.11.2018
T1003/2014	Detektor pohybu PIR	PDM-I18	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2	SS91=2	10.11.2016
T1004/2014	Detektor pohybu PIR	PDM-I18T	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	3	SS91=3	10.11.2016
T1005/2014	Ústředna PZTS	NX-8E (AC 948 Plus)	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	3	SS91=3	19.11.2016
T1006/2014	Ústředna PZTS	NX-8 (AC 948)	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	3	SS91=3	19.11.2016
T1007/2014	Bezdrátový přijímač	SPCW130.100	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2	SS91=2	8.1.2017
T1008/2014	Bezdrátová nad-stavba	SPCW110.000 (SPCW101.000)	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2	SS91=2	8.1.2017
T1009/2014	Detektor pohybu PIR	PDM-I12T	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	3	SS91=3	10.11.2016
T1010/2014	Bezdrátový detektor pohybu PIR	ADM-I12W1	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2	SS91=2	8.1.2017

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1011/2014	Bezdrátový detektor otevření	IMKW6-10	Siemens Aktienges-selschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2	SS91=2	8.1.2017
T1012/2014	Tísňové tlačítko	MAS-TH	ASITA spol. s r.o.	ASITA spol. s r.o.	V Mlejnku 611	500 11 Hradec Králové	4	SS91=4	7.4.2017
T1013/2014	Detektor otevření	MAS 203	ASITA spol. s r.o.	ASITA spol. s r.o.	V Mlejnku 611	500 11 Hradec Králové	2	SS91=2	13.4.2017
T1014/2014	Detektor otevření	MAS 273	ASITA spol. s r.o.	ASITA spol. s r.o.	V Mlejnku 611	500 11 Hradec Králové	2	SS91=2	13.4.2017
T1015/2014	Detektor otevření	MAS 283	ASITA spol. s r.o.	ASITA spol. s r.o.	V Mlejnku 611	500 11 Hradec Králové	2	SS91=2	13.4.2017
T1016/2014	Detektor otevření	MAS 333	ASITA spol. s r.o.	ASITA spol. s r.o.	V Mlejnku 611	500 11 Hradec Králové	2	SS91=2	13.4.2017
T1017/2014	Detektor otevření	MAS 303	ASITA spol. s r.o.	ASITA spol. s r.o.	V Mlejnku 611	500 11 Hradec Králové	3	SS91=3	13.4.2017
T1018/2014	Detektor otevření	MAS 353	ASITA spol. s r.o.	ASITA spol. s r.o.	V Mlejnku 611	500 11 Hradec Králové	3	SS91=3	13.4.2017
T1019/2014	Detektor otevření (magnetický kontakt)	"MK-3400-xx, MK-2400-S1, MK-2500-xx, MK-2470-xx, MK-2400-xx, MK-2400-S2"	Siemens Schweiz AG	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2	SS91=2	12.6.2017
T1020/2014	Detektor otevření (magnetický kontakt)	MK-2700-xx, MK-2720-xx	Siemens Schweiz AG	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	3	SS91=3	12.6.2017
T1021/2014	Detektor otevření (magnetický kontakt)	MK-4700, MK-4720	Siemens Schweiz AG	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	3	SS91=3	12.6.2017
T1022/2014	Detektor otevření (magnetický kontakt)	MK-4400, MK-4460	Siemens Schweiz AG	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2	SS91=2	12.6.2017
T1023/2014	Detektor směrový (infrazávora)	AX-70/130/200TN (BE)	OPTEX CO., Ltd.	OPTEX Security Sp. z o.o.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	4	SS91=4	18.12.2016
T1024/2014	Detektor směrový (infrazávora)	AX-100/200TF(BE)	OPTEX CO., Ltd.	OPTEX Security Sp. z o.o.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	4	SS91=4	18.12.2016

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1025/2014	Detektor směrový (infrazávora)	AX-350/650DH MkIII	OPTEX CO., Ltd.	OPTEX Security Sp. z o.o.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	4	SS91=4	26.6.2017
T1026/2014	Detektor směrový (infrazávora)	SL-200/350/650QN/ QDP/QDM	OPTEX CO., Ltd.	OPTEX Security Sp. z o.o.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	4	SS91=4	26.6.2017
T1027/2014	Detektor směrový (infrazávora)	SL-350QFR/QNR	OPTEX CO., Ltd.	OPTEX Security Sp. z o.o.	Bitwy Warszawskiej 1920 r. 7B	02-366 Warszawa, Poland	4	SS91=4	26.6.2017
T1028/2014	Perimetrický detekční systém	INTREPID Micro-Point II	Southwest Microwave, Inc.	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	4	SS91=4	13.3.2017
T1029/2014	Poplachový zabezpečovací a tísňový systém	ALTEX PZTS	ALIMEX s.r.o.	ALIMEX s.r.o.	Ke Zvoli 339	252 41 Dolní Břežany	3	SS91=3	28.8.2017
T1030/2014	Zálohovaný napájecí zdroj	PWR 533, PWR 533 v krytu K70	Trade FIDES, a.s.	Trade FIDES, a.s.	Dornych 57	617 00 Brno	3	SS91=3	16.7.2017
T1031/2014	Detektor pohybu kombinovaný (PIR +MW)	PDM-IXD12, PDM-IXD18	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	2	SS91=2	25.9.2017
T1032/2014	Detektor pohybu kombinovaný (PIR +MW)	PDM-IXD12T, PDM-IXD18T	Siemens Aktiengesselschaft	Siemens, s.r.o.	Siemensova 1	155 00 Praha 13	3	SS91=3	25.9.2017
T1033/2014	Ústředna PZTS	ASSET 804Z	Trade FIDES, a.s.	Trade FIDES, a.s.	Dornych 57	617 00 Brno	3	SS91=3	9.10.2017
T1034/2014	Detektor otevření	UMS001	SIEGENIA-AUBI KG	Trade FIDES, a.s.	Dornych 57	617 00 Brno	2	SS91=2	21.10.2017
T1035/2014	Ústředna PZTS	ATS 4099 (ATS 1099, ATS 2099, ATS 3099, ATS 4599)	UTC Fire & Security	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	3	SS91=3	23.10.2017
T1036/2014	Ústředna PZTS	ATS 4099/1 (ATS 2099/1, ATS 3099/1, ATS 4599/1)	UTC Fire & Security	Techfors CZ s.r.o.	Rozárčina 1480/7	140 00 Praha 4 - Krč	4	SS91=4	23.10.2017
T1037/2014	Detektor pohybu PIR	Viewguard PIR BUS-2/BUS-1 (N033332.21)	Honeywell Security Deutschland	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	6.11.2017
T1038/2014	Detektor pohybu PIR	Viewguard PIR AM BUS-2/BUS-1 (N033432.21)	Honeywell Security Deutschland	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	6.11.2017

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. c) a e) zákona č. 412/2005 Sb.
ZAŘÍZENÍ ELEKTRICKÉ ZABEZPEČOVACÍ SIGNALIZACE A TÍSŇOVÉ SYSTÉMY

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T1039/2014	Detektor pohybu kombinovaný (PIR +MW)	Viewguard DUAL BUS-2/BUS-1 (N033443.21)	Honeywell Security Deutschland	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	2	SS91=2	6.11.2017
T1040/2014	Detektor pohybu kombinovaný (PIR +MW)	Viewguard DUAL AM BUS-2/BUS-1 (N033442.21)	Honeywell Security Deutschland	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	6.11.2017
T1041/2014	Ústředna PZTS	MB Secure 6000 (N013870) vč.odvoz. variant 1000 (N013820), 2000 (N013830), 3000 (N013840), 4000 (N013850), 5000 (N013860)	Honeywell Security Deutschland	Honeywell, spol. s r. o. - Security Products o.z.	Havránkova 33	619 00 Brno	3	SS91=3	6.11.2017

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. h) zákona č. 412/2005 Sb.
ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T5016/2012	Skartovací stroj	KOBRA +1 SS4 (řez 3,8 mm)	ELCOMAN SRL	UNIVOX spol. s r.o.	Kolonie 392	Český Těšín	1	papír	09.02.2015
T5017/2012	Skartovací stroj	KOBRA +1 CC4 (řez 3,5x40 mm)	ELCOMAN SRL	UNIVOX spol. s r.o.	Kolonie 392	Český Těšín	2	papír	09.02.2015
T5018/2012	Skartovací stroj	KOBRA +2 SS4 (řez 3,8 mm)	ELCOMAN SRL	UNIVOX spol. s r.o.	Kolonie 392	Český Těšín	1	papír	09.02.2015
T5019/2012	Skartovací stroj	REXEL Auto+ 80X (řez 4x45 mm)	ACCO Brands Hungaria Kft.	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír, plast.karta	23.02.2015
T5020/2012	Skartovací stroj	REXEL Auto+ 250X (řez 4x40 mm)	ACCO Brands Hungaria Kft.	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír	23.02.2015
T5021/2012	Skartovací stroj	REXEL Auto+ 500X (řez 4x40 mm)	ACCO Brands Hungaria Kft.	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír	23.02.2015
T5022/2012	Velkokapacitní skartovací stroj	EBA 7050-3 C (řez 6x50 mm)	Krug & Priester GmbH & Co. KG	PALA, s.r.o.	Popůvky 199	Popůvky	2	papír	23.02.2015
T5023/2012	Skartovací stroj	HSM 225.2 (řez 0,78x11 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	4	papír	04.04.2015
T5024/2012	Skartovací stroj	HSM 125.2 (řez 1,9 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	2	papír, plast.karta	04.04.2015
T5025/2012	Skartovací stroj	HSM 105.3 (řez 3,9x30 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	2	papír, plast.karta	04.04.2015
T5026/2012	Skartovací stroj	HSM 105.3 (řez 3,9 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	1, 2	papír, plast.karta	04.04.2015
T5027/2012	Skartovací stroj	HSM 104.3 (řez 1,9x15 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	3	papír, plast.karta	04.04.2015
T5028/2012	Skartovací stroj	HSM 104.3 (řez 3,9x30 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	2	papír, plast.karta	04.04.2015
T5029/2012	Skartovací stroj	HSM 104.3 (řez 3,9 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	1, 2	papír, plast.karta	04.04.2015
T5030/2012	Skartovací stroj	REXEL RLWX19 (řez 4x40 mm)	ACCO Brands Hungaria Kft.	XERTEC a.s.	Kloknerova 2278/24	Praha 10	2	papír, plast.karta	10.05.2015
T5031/2012	Skartovací stroj	HSM 105.3 (řez 0,78x11 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	4	papír	07.06.2015
T5032/2012	Skartovací stroj	HSM 125.2 (řez 3,9 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	1, 2	papír, CD, plast. karta	07.06.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. h) zákona č. 412/2005 Sb.
ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T5033/2012	Skartovací stroj	IDEAL 2404 (řez 4 mm)	IDEAL-Werk Krug & Priester GmbH & Co. KG	Reinauer Handelsgmbh., organizační složka	Poděbradská 186/56	Praha 9	1	papír	25.06.2015
T5034/2012	Skartovací stroj	IDEAL 2404 CC (řez 2x15 mm)	IDEAL-Werk Krug & Priester GmbH & Co. KG	Reinauer Handelsgmbh., organizační složka	Poděbradská 186/56	Praha 9	3	papír	25.06.2015
T5035/2012	Skartovací stroj	IDEAL 2404 CC (řez 4x40 mm)	IDEAL-Werk Krug & Priester GmbH & Co. KG	Reinauer Handelsgmbh., organizační složka	Poděbradská 186/56	Praha 9	2	papír	25.06.2015
T5036/2012	Skartovací stroj	IDEAL 2503 (řez 4 mm)	IDEAL-Werk Krug & Priester GmbH & Co. KG	Reinauer Handelsgmbh., organizační složka	Poděbradská 186/56	Praha 9	1	papír	25.06.2015
T5037/2012	Skartovací stroj	IDEAL 2503 CC (řez 2x15 mm)	IDEAL-Werk Krug & Priester GmbH & Co. KG	Reinauer Handelsgmbh., organizační složka	Poděbradská 186/56	Praha 9	3	papír	25.06.2015
T5038/2012	Skartovací stroj	IDEAL 2503 CC (řez 4x40 mm)	IDEAL-Werk Krug & Priester GmbH & Co. KG	Reinauer Handelsgmbh., organizační složka	Poděbradská 186/56	Praha 9	2	papír	25.06.2015
T5039/2012	Skartovací stroj	IDEAL 2604 (řez 4 mm)	IDEAL-Werk Krug & Priester GmbH & Co. KG	Reinauer Handelsgmbh., organizační složka	Poděbradská 186/56	Praha 9	1	papír	25.06.2015
T5040/2012	Skartovací stroj	IDEAL 2604 CC (řez 4x40 mm)	IDEAL-Werk Krug & Priester GmbH & Co. KG	Reinauer Handelsgmbh., organizační složka	Poděbradská 186/56	Praha 9	2	papír	25.06.2015
T5041/2012	Skartovací stroj	IDEAL 2604 MC (řez 0,8x12 mm)	IDEAL-Werk Krug & Priester GmbH & Co. KG	Reinauer Handelsgmbh., organizační složka	Poděbradská 186/56	Praha 9	4	papír	25.06.2015
T5042/2012	Skartovací stroj	HSM 225.2 (řez 5,8 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	1	papír, CD/DVD	20.09.2015
T5043/2012	Skartovací stroj	HSM 225.2 (řez 3,9x40 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	2	papír, CD/DVD, plast.karta	20.09.2015
T5044/2012	Skartovací stroj	HSM Securio B24 (řez 3,9 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	1, 2	papír, CD/DVD, plast.karta	03.12.2015
T5046/2012	Skartovací stroj	HSM Securio B32 (řez 3,9 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	1, 2	papír, CD/DVD, plast.karta	03.12.2015

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. h) zákona č. 412/2005 Sb.
ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T5048/2012	Skartovací stroj	HSM 125.2 (řez 3,9x30 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	2	papír, plast.karta	03.12.2015
T5049/2012	Skartovací stroj	HSM 390.3 (řez 3,9x40 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	2	papír, CD/DVD, plast.karta	03.12.2015
T5050/2012	Skartovací stroj	HSM Securio P36 (řez 3,9 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	1, 2	papír, CD/DVD, plast.karta	03.12.2015
T5051/2012	Skartovací stroj	JAWS C7 (řez 2x10 mm)	Shanghai Sunwood Industrial Co. Ltd	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	3	papír, CD/DVD, plast.karta	03.12.2015
T5052/2012	Skartovací stroj	JAWS C9 (řez 2x8 mm)	Shanghai Sunwood Industrial Co. Ltd	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	3	papír	03.12.2015
T5001/2013	Skartovací stroj	HSM Securio B24 (řez 1,9x15 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	3	papír, plast.karta	17.01.2016
T5002/2013	Skartovací stroj	HSM Securio B32 (řez 1,9x15 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	3	papír, plast.karta	17.01.2016
T5003/2013	Skartovací stroj	AT 12C (řez 3,8x50 mm)	Changzhou Jinpex Electronics Co., Ltd.	AVE TECH, spol. s r. o.	Ve Žlíbku 1800/77	Praha 9	2	papír	18.12.2015
T5004/2013	Skartovací stroj	AT 20S (řez 4 mm)	Changzhou Jinpex Electronics Co., Ltd.	AVE TECH, spol. s r. o.	Ve Žlíbku 1800/77	Praha 9	1	papír	18.12.2015
T5006/2013	Skartovací stroj	REXEL V120 (řez 5,8 mm)	ACCO Europe PLC	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	1	papír	24.01.2016
T5007/2013	Skartovací stroj	REXEL V125 (řez 4x34 mm)	ACCO Europe PLC	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	2	papír	24.01.2016
T5008/2013	Skartovací stroj	REXEL V60WS (řez 5,8 mm)	ACCO Europe PLC	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	1	papír	24.01.2016
T5009/2013	Skartovací stroj	REXEL MERCURY RSX1630 (řez 4x45 mm)	ACCO Europe PLC	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	2	papír, CD/DVD, plast.karta	24.01.2016
T5010/2013	Skartovací stroj	REXEL MERCURY RSM1130 (řez 1,9x15 mm)	ACCO Europe PLC	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	3	papír	24.01.2016
T5011/2013	Skartovací stroj	REXEL MERCURY RDS2250 (řez 5,8 mm)	ACCO Europe PLC	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	1	papír, CD/DVD	24.01.2016

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. h) zákona č. 412/2005 Sb.
ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T5012/2013	Skartovací stroj	REXEL V65WS (řez 4x45 mm)	ACCO UK Limited	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír, plast.karta	21.02.2016
T5013/2013	Skartovací stroj	REXEL MERCURY RDX1850 (řez 4x45 mm)	ACCO Europe PLC	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír, disketa, plast.karta, CD	07.02.2016
T5014/2013	Skartovací stroj	REXEL MERCURY RDX2070 (řez 4x45 mm)	ACCO Europe PLC	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír, disketa, plast.karta, CD	07.02.2016
T5015/2013	Skartovací stroj	Intimus 120SC2 (řez 3,8 mm)	Martin Yale International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	1	papír	07.02.2016
T5016/2013	Skartovací stroj	Intimus 20 SC2 (řez 4 mm)	Martin Yale International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	1, 2	papír, plast.karta	07.02.2016
T5017/2013	Skartovací stroj	Intimus 20 CC3 (řez 4x28 mm)	Martin Yale International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír, plast.karta	07.02.2016
T5018/2013	Skartovací stroj	Intimus 120CC3 (řez 3,8x36 mm)	Martin Yale International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír	07.03.2016
T5019/2013	Skartovací stroj	Intimus 120CC4 (řez 1,9x15 mm)	Martin Yale International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	3	papír	07.03.2016
T5020/2013	Skartovací stroj	KOBRA 300 SS4 E/S (řez 3,8 mm)	ELCOMAN SRL	UNIVOX spol. s r.o.	Kolonie 392	Český Těšín	1, 2	papír, CD/DVD, disketa, plast. karta	07.02.2016
T5021/2013	Skartovací stroj	KOBRA 300 SS5 E/S (řez 5,8 mm)	ELCOMAN SRL	UNIVOX spol. s r.o.	Kolonie 392	Český Těšín	1	papír, CD/DVD, disketa	07.02.2016
T5022/2013	Skartovací stroj	KOBRA 300 CC2 E/S (řez 1,9x15 mm)	ELCOMAN SRL	UNIVOX spol. s r.o.	Kolonie 392	Český Těšín	3	papír, plast.karta	07.02.2016
T5023/2013	Skartovací stroj	KOBRA 300 CC4 E/S (řez 3,5x30 mm)	ELCOMAN SRL	UNIVOX spol. s r.o.	Kolonie 392	Český Těšín	2	papír, CD/DVD, plast.karta	07.02.2016
T5024/2013	Skartovací stroj	KOBRA 390 C4 E/S (řez 3,9x40 mm)	ELCOMAN SRL	UNIVOX spol. s r.o.	Kolonie 392	Český Těšín	2	papír, CD/DVD, disketa, plast. karta	21.02.2016
T5025/2013	Skartovací stroj	KOBRA 390 S5 E/S (řez 5,8 mm)	ELCOMAN SRL	UNIVOX spol. s r.o.	Kolonie 392	Český Těšín	1	papír, CD/DVD, disketa	21.02.2016
T5026/2013	Velkokapacitní skartovací stroj	Intimus VZ 17.00 (řez částice 320 mm2)	Martin Yale International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír	21.03.2018

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. h) zákona č. 412/2005 Sb.
ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T5027/2013	Skartovací stroj	Intimus S 14.95 (řez 5,8 mm)	Martin Yale International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	1	papír, CD/DVD, disketa	11.04.2016
T5028/2013	Skartovací stroj	Fellowes M-8C (řez 4x50 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, plast.karta	21.03.2016
T5029/2013	Skartovací stroj	Fellowes W11C (řez 3,9x35 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, plast.karta	21.03.2016
T5030/2013	Skartovací stroj	Fellowes 60Cs (řez 4x50 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, plast.karta	21.03.2016
T5031/2013	Skartovací stroj	Fellowes 73Ci (řez 4x38 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, CD/DVD, plast.karta	21.03.2016
T5032/2013	Skartovací stroj	Fellowes 79Ci (řez 3,9x38 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, CD/DVD, plast.karta	04.04.2016
T5033/2013	Skartovací stroj	Fellowes 90S (řez 5,8 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	1	papír, CD/DVD	21.03.2016
T5034/2013	Skartovací stroj	Fellowes 99Ci (řez 3,9x38 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, CD/DVD, plast.karta	04.04.2016
T5035/2013	Skartovací stroj	Fellowes MS-460Cs (řez 2x8 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	3	papír	21.03.2016
T5036/2013	Skartovací stroj	Fellowes 225i (řez 5,8 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	1	papír	04.04.2016
T5037/2013	Skartovací stroj	Fellowes 225Ci (řez 3,9x38 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír	04.04.2016
T5038/2013	Skartovací stroj	DAHLE 21112 (řez 4x48 mm)	Dahle Bürotechnik GmbH	NOVUS Česko s.r.o.	Raspenava 191	Raspenava	2	papír	17.12.2015
T5039/2013	Skartovací stroj	DAHLE 21082 (řez 4x45 mm)	Dahle Bürotechnik GmbH	NOVUS Česko s.r.o.	Raspenava 191	Raspenava	2	papír	17.12.2015
T5040/2013	Skartovací stroj	HSM Securio P36 (řez 1,9x15 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	3	papír, plast.karta	26.09.2016
T5041/2013	Skartovací stroj	Intimus 852 CC (řez 3,8x40 mm)	Martin Yale International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír	26.09.2016
T5042/2013	Skartovací stroj	HSM 450.2 (řez 3,9x40 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	2	papír, CD/DVD, disketa, plast. karta	24.10.2016

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. h) zákona č. 412/2005 Sb.
ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T5043/2013	Skartovací stroj	EBA 1524 C (řez 4x40 mm)	Krug & Priester GmbH & Co. KG	PALA, s.r.o.	Popůvky 199	Popůvky	2	papír	25.11.2016
T5044/2013	Skartovací stroj	EBA 1524 C (řez 2x15 mm)	Krug & Priester GmbH & Co. KG	PALA, s.r.o.	Popůvky 199	Popůvky	3	papír	25.11.2016
T5045/2013	Skartovací stroj	IDEAL 3104 CC (řez 4x40 mm)	Krug & Priester GmbH & Co. KG	Reinauer HandelsgmbH., organizační složka	Poděbradská 186/56	Praha 9	2	papír, CD/DVD	21.11.2016
T5001/2014	Skartovací stroj	Intimus 26 CC3 (řez 4x28 mm)	Martin Yale International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír	30.1.2017
T5002/2014	Skartovací stroj	Intimus 32 CC3 (řez 4x28 mm)	Martin Yale International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír	30.1.2017
T5003/2014	Skartovací stroj	Intimus Confidential (řez 2x8 mm)	Martin Yale International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	3	papír	30.1.2017
T5004/2014	Skartovací stroj	REXEL Auto+ 300X (řez 4x40 mm)	ACCO UK Limited	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír, plast.karta	30.1.2017
T5005/2014	Skartovací stroj	IDEAL 3104 CC (řez 2x15 mm)	Krug & Priester GmbH & Co. KG	OPUS Praha s.r.o.	Podolská 557/102	Praha 4	3	papír, CD/DVD, plast.karta	13.2.2017
T5006/2014	Skartovací stroj	AT 15C (řez 4x50 mm)	Changzhou Jinpex Electronics Co., Ltd.	AVE TECH, spol. s r. o.	Ve Žlíbku 1800/77	Praha 9	2	papír	5.12.2016
T5007/2014	Skartovací stroj	AT 15S (řez 4 mm)	Changzhou Jinpex Electronics Co., Ltd.	AVE TECH, spol. s r. o.	Ve Žlíbku 1800/77	Praha 9	1	papír	5.12.2016
T5008/2014	Skartovací stroj	AT 70C (řez 4x40 mm)	Changzhou Jinpex Electronics Co., Ltd.	AVE TECH, spol. s r. o.	Ve Žlíbku 1800/77	Praha 9	2	papír, CD/DVD, plast.karta	5.12.2016
T5009/2014	Skartovací stroj	IDEAL 2604 CC (řez 2x15 mm)	Krug & Priester GmbH & Co. KG	Reinauer HandelsgmbH., organizační složka	Poděbradská 186/56	Praha 9	3	papír, plast.karta	5.12.2016
T5010/2014	Skartovací stroj	IDEAL 3104 (řez 4 mm)	Krug & Priester GmbH & Co. KG	Reinauer HandelsgmbH., organizační složka	Poděbradská 186/56	Praha 9	1, 2	papír, CD/DVD	5.12.2016
T5011/2014	Skartovací stroj	IDEAL 3104 CC (řez 2x15 mm)	Krug & Priester GmbH & Co. KG	Reinauer HandelsgmbH., organizační složka	Poděbradská 186/56	Praha 9	3	papír	5.12.2016
T5012/2014	Velkokapacitní skartovací stroj	intimus S 16.50, intimus S 16.86 s lisem (řez 6x50 mm)	intimus International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír	13.3.2017

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. h) zákona č. 412/2005 Sb.
ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T5013/2014	Skartovací stroj	HSM 125.2 (řez 1,9x15 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	3	papír, plast.karta	27.3.2017
T5014/2014	Skartovací stroj	intimus 45 CC4, intimus 60 CC4 (řez 1,9x15 mm)	intimus International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	3	papír	6.5.2017
T5015/2014	Skartovací stroj	intimus 45 SC2, intimus 60 SC2 (řez 3,8 mm)	intimus International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	1	papír	6.5.2017
T5016/2014	Skartovací stroj	intimus 45 CC3, intimus 60 CC3 (řez 3,8x30 mm)	intimus International GmbH	XERTEC a.s.	Kloknerova 2278/24	Praha 4	2	papír	6.5.2017
T5017/2014	Skartovací stroj	Fellowes W-1C (řez 4x35 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, plast.karta	16.7.2017
T5018/2014	Skartovací stroj	Fellowes W-61Cb (řez 4x50 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, plast.karta	16.7.2017
T5019/2014	Skartovací stroj	Fellowes W-71Ci (řez 4x38 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, CD/DVD, plast.karta	16.7.2017
T5020/2014	Skartovací stroj	Fellowes W-81Ci (řez 4x38 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, CD/DVD, plast.karta	16.7.2017
T5021/2014	Skartovací stroj	Fellowes 99Ms (řez 2x14 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	3	papír, plast.karta	16.7.2017
T5022/2014	Skartovací stroj	Fellowes 225Mi (řez 2x12 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	3	papír	16.7.2017
T5023/2014	Skartovací stroj	Fellowes 450Ms (řez 2x8 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	3	papír, plast.karta	16.7.2017
T5024/2014	Skartovací stroj	Fellowes 460Ms (řez 2x8 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	3	papír, plast.karta	16.7.2017
T5025/2014	Skartovací stroj	Fellowes 425Ci (řez 3,9x30 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, CD/DVD, plast.karta	16.7.2017
T5026/2014	Skartovací stroj	Fellowes AUTOMAX 300C (řez 4x38 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, CD/DVD, plast.karta	16.7.2017
T5027/2014	Skartovací stroj	Fellowes AUTOMAX 500C (řez 4x38 mm)	Fellowes Mfg. Co.	Fellowes Polska SA	ul. Górczewska 69/73	Warszawa, Poland	2	papír, CD/DVD, plast.karta	16.7.2017

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. h) zákona č. 412/2005 Sb.
ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T5028/2014	Skartovací stroj	HSM MultiShred one-4-all (řez 4x35 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	2	papír, CD/DVD, disketa, plast. karta	16.7.2017
T5029/2014	Skartovací stroj	HSM 80.2 (řez 3,9 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	1	papír	31.7.2017
T5030/2014	Skartovací stroj	HSM 102.2 (řez 3,9 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	1, 2	papír, plast.karta	31.7.2017
T5031/2014	Skartovací stroj	HSM 90.2 (řez 3,9 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	1, 2	papír, plast.karta	31.7.2017
T5032/2014	Skartovací stroj	HSM 90.2 (řez 4x25 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	2	papír	31.7.2017
T5033/2014	Skartovací stroj	HSM 225.2 (řez 1,9x15 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	2, 3	papír, CD/DVD, plast.karta	31.7.2017
T5034/2014	Skartovací stroj	JAWS S4 (řez 2x12 mm)	Shanghai Sunwood Industrial Co. Ltd	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	3	papír, CD/DVD, plast.karta	14.8.2017
T5035/2014	Skartovací stroj	KOBRA 240 HS (řez 0,8x9,5 mm)	ELCOMAN SRL	UNIVOX spol. s r.o.	Kolonie 392	Český Těšín	4	papír	28.8.2017
T5036/2014	Skartovací stroj	AT 90C (řez 3x25 mm)	Changzhou Jinpex Electronics Co., Ltd.	AVE TECH, spol. s r. o.	Ve Žlíbku 1800/77	Praha 9	2	papír, CD/DVD, disketa, plast. karta	31.7.2017
T5037/2014	Skartovací stroj	AT 66C (řez 4x25 mm)	Jiangsu Magitech Science Technology Co., Ltd.	AVE TECH, spol. s r. o.	Ve Žlíbku 1800/77	Praha 9	2	papír, plast.karta	31.7.2017
T5038/2014	Skartovací stroj	AT 36C (řez 2x10 mm)	Changzhou Jinpex Electronics Co., Ltd.	AVE TECH, spol. s r. o.	Ve Žlíbku 1800/77	Praha 9	3	papír	31.7.2017
T5039/2014	Skartovací stroj	intimus 802 CC (řez 1,9x15 mm)	intimus International GmbH	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	3	papír	25.9.2017
T5040/2014	Velkokapacitní skar-tovací stroj	intimus 14.95 (řez 6x50 mm)	intimus International GmbH	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	2	papír	25.9.2017
T5041/2014	Velkokapacitní skar-tovací stroj	intimus 14.87 s lisem (řez 6x50 mm)	intimus International GmbH	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	2	papír	25.9.2017
T5042/2014	Skartovací stroj	HSM 102.2 (řez 4x25 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	2	papír	9.10.2017

Certifikované technické prostředky uvedené v § 30 odst. 1, písm. h) zákona č. 412/2005 Sb.
ZAŘÍZENÍ FYZICKÉHO NIČENÍ NOSIČŮ INFORMACÍ NEBO DAT

Identifikační č. TP	Název TP	Označení TP	Výrobce	Držitel jméno	Držitel adresa	Držitel město	Kategorie /typ	Bodové ohodnocení	Platnost do
T5043/2014	Skartovací stroj	HSM 125.2 (řez 0,78x11 mm)	HSM GmbH & Co. KG	KAST, spol. s r.o.	Nad Vršovskou horou 10/1423	Praha 10	4	papír	9.10.2017
T5044/2014	Skartovací stroj	REXEL Auto+ 100M (řez 2x15 mm)	ACCO UK Limited	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	3	papír, plast.karta	9.10.2017
T5045/2014	Skartovací stroj	REXEL Auto+ 300M (řez 2x15 mm)	ACCO UK Limited	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	3	papír	9.10.2017
T5046/2014	Skartovací stroj	KOBRA 260 HS (řez 0,8x9,5 mm)	ELCOMAN SRL	UNIVOX spol. s r.o.	Kolonie 392	Český Těšín	4	papír	6.11.2017
T5047/2014	Skartovací stroj	REXEL Auto+ 100X (řez 4x50 mm)	ACCO UK Limited	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	2	papír, plast.karta	20.11.2017
T5048/2014	Skartovací stroj	EBA 3140 C (řez 2x15 mm)	Krug & Priester GmbH & Co. KG	PALA, s.r.o.	Popůvky 199	Popůvky	3	papír, CD/DVD, plast.karta	28.8.2017
T5049/2014	Skartovací stroj	EBA 3140 C (řez 4x40 mm)	Krug & Priester GmbH & Co. KG	PALA, s.r.o.	Popůvky 199	Popůvky	2	papír, CD/DVD, plast.karta	28.8.2017
T5050/2014	Skartovací stroj	intimus 130CP5 (řez 1,9x15 mm)	intimus International GmbH	XERTEC a.s.	Kloknerova 2278/ 24	Praha 4	3	papír, plast.karta	4.12.2017

Seznam orgánů státu a podnikatelů s nimiž Úřad uzavřel smlouvu podle § 52 zákona č. 412/2005 Sb.

podle ustanovení § 52 a § 46 odst. 15 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

- **IKATES, s.r.o.**

  Technické prostředky dle zákona č. 412/2005 Sb., § 30 odst. 1, **písmeno a)**

  Tolstého 186,
  415 03 Teplice
  Ing. Lubomír Hnilička, ředitel společnosti
  Tel./Fax: 417 502 825
  E-mail: **ikates@volny.cz**

- **Strojírenský zkušební ústav, s. p.**

  Technické prostředky dle zákona č. 412/2005 Sb., § 30 odst. 1, **písmeno a)**

  Hudcova 56b,
  621 00 Brno-město
  Tel.: 541 120 111
  Fax: 541 120 225
  E-mail: **szu@szutest.cz**
  WWW: **www.szutest.cz**

- **TESTALARM Praha spol. s r.o.**

  Technické prostředky dle zákona č. 412/2005 Sb., § 30 odst. 1, **písmeno b), c), e)**

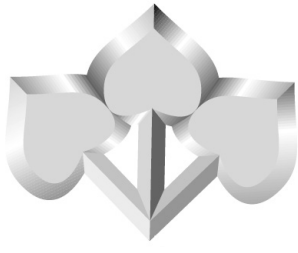
  Božanovská 2098,
  193 00 Praha 9
  Zbyněk Görner
  Tel./Fax: 281 925 639
  E-mail: **info@testalarm.cz**
  WWW: **www.testalarm.cz**

- **TREZOR TEST, s.r.o.**

  Technické prostředky dle zákona č. 412/2005 Sb., § 30 odst. 1, **písmeno a), b), c), e), h)**

  Na Vršku 67,
  250 67 Klecany
  Ing. Petr Koktan, jednatel společnosti
  Tel.: 284 892 997
  Fax: 284 890 139
  E-mail: **trezortest@trezortest.cz**
  WWW:**www.trezortest.cz**

KYBERNETICKÁ BEZPEČNOST



KYBERNETICKÁ BEZPEČNOST

Česká republika v roce 2014 pokračovala v započatém budování kybernetické bezpečnosti. Výsledkem bylo zejména otevření Národního centra kybernetické bezpečnosti (dále „NCKB“) a přijetí zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně související zákonů (dále „ZKB“), a prováděcích právních předpisů k ZKB. Byla posílena mezinárodní spolupráce v oblasti kybernetické bezpečnosti, k účasti na mezinárodních cvičeních zaměřených na technické i netechnické aspekty zajišťování kybernetické bezpečnosti, pořádání národního cvičení a zvyšování potřebného povědomí a osvěty v této oblasti.

Plnění cílů v oblasti kybernetické bezpečnosti za rok 2014 je možné vyjádřit následovně:

- Budování NCKB / GovCERT.CZ[1]):
- Vývoj legislativy v oblasti kybernetické bezpečnosti
- Tvorba dokumentů tvořících kybernetickou bezpečnostní politiku ČR
- Informační systémy důležité pro stát a komunikace se subjekty provozující kritickou informační infrastrukturu a významné informační systémy
- Mezinárodní spolupráce
- Národní spolupráce
- Zvyšování povědomí a osvěta
- Sledování současných trendů kybernetické bezpečnosti

1. BUDOVÁNÍ NCKB / GovCERT.CZ

Počátek činnosti NCKB lze datovat ke konci roku 2011, kdy byl Národní bezpečnostní úřad (dále „NBÚ“) usnesením vlády ze dne 19. října 2011 č. 781 pověřen jeho vybudováním. Od té doby byla provedena celá řada úkonů směřujících k vytvoření jeho operační kapacity. To zahrnovalo značné množství aktivit, od úkonů administrativního charakteru, přes převzetí gesce pro oblast kybernetické bezpečnosti od Ministerstva vnitra (dále „MV“) včetně převzetí či navazování nových vztahů s partnerskými úřady v zahraničí, vybudování prostor a zajištění technického zázemí nutného pro fungování NCKB, až po provádění výběrových řízení a náboru nových pracovníků.

Organizačně je NCKB součástí Sekce kybernetické bezpečnosti NBÚ a dělí se na dvě oddělení – GovCERT.CZ a Oddělení teoretické podpory, vzdělávání a výzkumu (dále „OTPVV“). GovCERT.CZ je tým zejména IT specialistů zabývající se technickou stránkou kybernetické bezpečnosti zahrnující řešení kybernetických bezpečnostních incidentů subjektů spravujících důležité komunikační a informační systémy pro stát, analýzu malware, sběr a vyhodnocování informací o kybernetických útocích a hrozbách apod. OTPVV je odpovědné za přípravu národních strategií, kybernetických bezpečnostních politik, koordinaci s ostatními gestory bezpečnosti České republiky, zajištění plnění mezinárodních závazků a spolupráce v oblasti kybernetické bezpečnosti. Zároveň je odpovědné za určování kritické informační infrastruktury státu (dále „KII“) a komunikaci mezi NBÚ a subjekty KII a správci významných informačních systémů (dále „VIS“). OTPVV také poskytuje nezbytnou právní a administrativní podporu GovCERT.CZ, zabývá se tvorbou vzdělávacích politik a vzděláváním v oblasti kybernetické bezpečnosti a do budoucna i koordinací výzkumu v oblasti kybernetické bezpečnosti na národní úrovni.

Slavnostní otevření rekonstruované budovy NCKB, ve které jsou umístěna pracoviště GovCERT.CZ a OTPVV, proběhlo dne 13. května 2014 za účasti předsedy vlády České republiky Bohuslava Sobotky, ředitele NBÚ Dušana Navrátila, náměstka generálního tajemníka NATO pro nové bezpečnostní výzvy Sorina Ducaru, ředitele Evropské agentury pro bezpečnost sítí a informací (ENISA) Udo Helmbrechta, představitelů české bezpečnostní komunity a dalších významných hostů nejen z oblasti kybernetické bezpečnosti.

[1]) GovCERT.CZ představuje vládní koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty (vládní CERT – Computer Emergency Response Team), které je organizační složkou.
Národního bezpečnostního úřadu, respektive jeho specializovaného pracoviště, Národního centra kybernetické bezpečnosti.

2. VÝVOJ LEGISLATIVY V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

V roce 2014 došlo k několika podstatným událostem na poli kybernetické legislativy. Nejzásadnější bylo přijetí zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Vytvoření tohoto zákona bylo uloženo NBÚ usnesením vlády ze dne 19. října 2011 č. 781. Absence podobných předpisů v právním řádu České republiky nebo u zahraničních partnerů vedla k vytvoření v současné době ojedinělé koncepce zaměřující se na nastavení systému koordinace a kooperace mezi nejdůležitějšími subjekty působícími v oblasti kybernetické bezpečnosti a na zavedení bezpečnostních opatření k ochraně informačních a komunikačních systémů důležitých pro stát.

2.1. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Návrh zákona, vypracovaný ve spolupráci s akademickou sférou, soukromým sektorem a dalšími státními institucemi, byl schválen vládou dne 2. ledna 2014, do konce června 2014 prošel všemi čteními v Poslanecké sněmovně Parlamentu České republiky. Při projednávání zákona došlo na základě připomínek poslanců k několika změnám, nicméně původní koncept byl zachován. Následně byl zákon dne 23. července 2014 schválen Senátem Parlamentu České republiky a dne 13. srpna 2014 jej podepsal Prezident České republiky. ZKB vešel v účinnost k 1. lednu 2015.

Vedle zákona o kybernetické bezpečnosti byly v roce 2014 vypracovány a schváleny také jeho prováděcí právní předpisy, tj. vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, která byla vypracována společně NBÚ a MV, a novela nařízení vlády ze dne 22. prosince 2010 č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

2.2. Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti

Návrh vyhlášky o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti byl podroben dvoukolovému připomínkovému řízení s cílem dosáhnout co možná nejširší diskuse o navržené právní úpravě a její optimalizace v dopadech na veřejnoprávní a soukromoprávní subjekty v České republice.

21. února 2014 byl návrh vyhlášky zveřejněn k připomínkování odbornou veřejností. Připomínky byly jednotlivě vypořádány na veřejném jednání dne 11. dubna 2014.

Po zapracování vypořádaných připomínek byl návrh vyhlášky 31. července 2014 postoupen do meziresortního připomínkového řízení, které bylo ukončeno dne 21. srpna 2014. Připomínky byly jednotlivě vypořádány na jednání dne 18. září 2014. Po zapracování vypořádaných připomínek byl návrh vyhlášky zaslán do Legislativní rady vlády.

Dne 24. listopadu 2014 byl návrh vyhlášky projednán v Pracovní komisi Legislativní rady vlády pro správní právo. Připomínky nebyly zásadního charakteru, přičemž převážná část byla legislativně technická.

2.3. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, byla připravována společně MV a NBÚ. Návrh vyhlášky byl vypracován v první polovině roku 2014 a po vypořádání vzájemných připomínek obou resortů byl v září 2014 návrh odeslán do meziresortního připomínkového řízení. V tomto řízení obdržely předkládající resorty připomínky z 26 připomínkových míst. Řešeny byly zejména připomínky k uvedení některých systémů do přílohy č. 1 vyhlášky, ve které jsou stanoveny VIS, popřípadě se zaměřovaly na rozsah stanovení určujících kritérií a jiné legislativně-technické aspekty vyhlášky. Připomínky byly jednotlivě vypořádány na jednáních ve dnech 6. a 7. listopadu 2014. Dne 20. listopadu 2014 byla vyhláška postoupena Pracovní komisi Legislativní rady vlády pro správní právo k projednání. Obě vyhlášky byly dne 15. prosince 2014 schváleny a nabyly účinnosti dnem 1. ledna 2015.

NBÚ se podílel také na tvorbě novely nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, konkrétně na stanovení odvětvových kritérií pro určení prvku kritické infrastruk-

tury v oblasti kybernetické bezpečnosti. Návrh této novely byl v gesci MV. Novela nařízení také nabyla účinnosti dnem 1. ledna 2015.

3. TVORBA KYBERNETICKÉ BEZPEČNOSTNÍ POLITIKY ČESKÉ REPUBLIKY

Zásadními počiny při utváření politiky kybernetické bezpečnosti České republiky bylo zejména vytváření nové národní strategie kybernetické bezpečnosti České republiky a navazujícího akčního plánu, který dotčenou strategii dále rozpracovává a konkretizuje jednotlivé úkoly pro odpovědné subjekty. Na základě podnětu NBÚ došlo k aktualizaci Bezpečnostní strategie České republiky tak, aby reflektovala změny bezpečnostního paradigmatu v blízkém pohraničí a posilování role nestátních aktérů a hrozeb včetně těch kybernetických. V neposlední řadě NBÚ plnil roli gestora kybernetické bezpečnosti poskytováním stanovisek a komentářů k dalším návrhům materiálů, které se kybernetické bezpečnosti dotýkají, popřípadě připomínkováním legislativy, která by mohla na otázku kybernetické bezpečnosti mít dopady.

3.1. Národní strategie kybernetické bezpečnosti České republiky a Akční plán

V roce 2011 navázal NBÚ na svého předchůdce, MV, a drobnými úpravami aktualizoval tehdejší strategii kybernetické bezpečnosti. Výsledkem těchto úprav byla Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015.

Od té doby se podařilo dosáhnout mimo jiné i dvou důležitých milníků, které byly v této strategii stanoveny, a to:

- přijetí Zákona o kybernetické bezpečnosti
- otevření Národního centra kybernetické bezpečnosti, jehož součástí je funkční GovCERT.CZ pro zvládání kybernetických bezpečnostních incidentů.

Ostatní cíle stanovené v dané strategii bylo také možné považovat za splněné či průběžně naplňované.

S blížícím se ukončením platnosti této strategie a splněním v ní stanovených zásadních cílů a úkolů začal v roce 2013 NBÚ v souladu se svou úlohou národní autority v oblasti kybernetické bezpečnosti vytvářet, ve spolupráci se svými partnery, zcela novou Národní strategii kybernetické bezpečnosti na období let 2015 až 2020 (dále „Strategie“). Nová Strategie představuje pro Českou republiku zásadní předěl ve vnímání kybernetické bezpečnosti. Oproti minulé strategii se kvalitativně přesouvá od budování základních kapacit nezbytných pro zajištění základní míry kybernetické bezpečnosti směrem k jejímu dalšímu hlubšímu a pokročilému zajišťování.

Z cílů Strategie vychází i Akční plán kybernetické bezpečnosti České republiky na období let 2015 až 2020 (dále „Akční plán“), který bude definovat konkrétní úkoly, stanoví u nich zodpovědnost, termíny jejich plnění a kontrolu.

4. INFORMAČNÍ SYSTÉMY DŮLEŽITÉ PRO STÁT A KOMUNIKACE SE SUBJEKTY PROVOZUJÍCÍMI KII A VIS

V roce 2014 bylo dokončeno mapování informačních a komunikačních systémů důležitých pro stát, a to jak u veřejnoprávních, tak soukromoprávních subjektů.

Mapování sloužilo zejména jako podklad pro tvorbu legislativy kybernetické bezpečnosti, přičemž jeho výsledky v posledních fázích posloužily k řádnému vymezení určujících kritérií KII a VIS. V rámci celého mapování bylo osloveno více než 90 subjektů a identifikováno více než 800 informačních systémů, které byly dále hodnoceny z hlediska důležitosti pro chod státu.

V rámci mapování byly započaty také bezpečnostní projekty s některými subjekty, které měly za cíl zlepšit úroveň zabezpečení daných informačních systémů. Tyto projekty probíhaly i v průběhu roku 2014.

Na základě provedeného mapování započala komunikace se subjekty, které by se měly stát správci KII nebo VIS dle ZKB. Cílem této komunikace je zejména příprava na plnění povinností dle ZKB a vymezení jednotlivých informačních systémů a činností daných subjektů k případnému jejich určení za KII, popřípadě za VIS.

Značné úsilí bylo také věnováno poskytování informací o dopadech přijaté právní úpravy včetně

důsledků, které bude standardizovaná spolupráce v oblasti kybernetické bezpečnosti přinášet. Za tím účelem se členové NCKB aktivně účastnili konferencí k ZKB a prováděcím právním předpisům, konferencí ke kybernetické bezpečnosti, odborných seminářů apod. V neposlední řadě byla tato osvěta prováděna i vzájemnými jednáními s mnoha jednotlivými subjekty, které spravují informační nebo komunikační technologie důležité pro stát.

5. MEZINÁRODNÍ SPOLUPRÁCE

Stejně jako tomu bylo v předchozích letech, i v roce 2014 pokračoval NBÚ v navazování a budování bilaterální a multilaterální mezinárodní spolupráce.

Hlavním tématem pro NBÚ na evropské úrovni byla i v roce 2014 bezpečnost sítí a informací. Směrnice o bezpečnosti sítí a informací (dále „Směrnice NIS“) byla Evropskou komisí představena dne 7. února 2013 v souvislosti se společným sdělením Evropské komise a vysoké představitelky Evropské unie (dále „EU“) pro zahraniční věci a bezpečnostní politiku o evropské strategii pro kybernetickou bezpečnost.

NBÚ od počátku aktivně vysílá své experty na jednání na půdě Rady EU, která probíhají v rámci Pracovní skupiny pro telekomunikace a informační společnost. Tato směrnice byla intenzivně projednávána během řeckého i italského předsednictví, přičemž cílem italského předsednictví bylo dokončení jejího projednávání. Za tímto účelem byla od poloviny října 2014 zahájena neformální jednání s Evropským parlamentem, jejichž cílem je sjednotit stanovisko Evropského parlamentu a Rady EU. Cílem NBÚ je prosazení pozice České republiky, která se soustředí zejména na ochranu KII a zabránění významnému rozšiřování oblasti působnosti Směrnice NIS na soukromoprávní subjekty.

Česká republika má své zastoupení formou účasti na pořádaných formálních a neformálních jednáních v Evropské agentuře pro bezpečnost sítí a informací (dále „ENISA“). Dva zástupci NBÚ jsou členy představenstva ENISA[2]), kde jsou zodpovědní za schvalování programu a plánu prací a rozpočtu ENISA. Na podzim roku 2014 byl pracovník NCKB osloven, aby se stal členem užší pracovní skupiny ENISA vytvořené na podporu tvorby a implementace národních strategií kybernetické bezpečnosti. Přizvaný zástupce se tak bude od příštího roku ve spolupráci s dalšími odborníky podílet na konzultacích a přípravě metodických a podpůrných materiálů pro tvorbu strategických dokumentů tak, aby co nejvíce reflektovaly aktuální hrozby a rizika v oblasti kybernetické bezpečnosti.

Otázky kybernetické bezpečnosti jsou diskutovány také na půdě Organizace pro bezpečnost a spolupráci v Evropě (dále „OBSE“). V listopadu 2014 švýcarské předsednictví OBSE uspořádalo konferenci ICT CBMs: Promoting implementation, supporting negotiations, kde zástupce NBÚ spolu se zástupkyní slovenského CSIRT.SK společně prezentovali v panelu týkajícím se regionální spolupráce společnou platformu států Visegrádské čtyřky a Rakouska v oblasti kybernetické bezpečnosti, tzv. CECSP.

Česká republika dosáhla významného úspěchu v oblasti na zvyšování zabezpečení a odolnosti KII skrze regionální spolupráci mezi pracovišti CERT, když byla z její a rakouské iniciativy založena v květnu 2013 Středoevropská platforma kybernetické bezpečnosti (Central European Cyber Security Platform, dále „CECSP“). Za rakouského předsednictví v dubnu 2014 se uskutečnilo již třetí zasedání na strategické úrovni, kde se hodnotil pokrok v dosavadní spolupráci na poli kybernetické bezpečnosti. Prioritou tohoto jednání bylo i přijetí pracovního programu CECSP pro období nadcházejících tří let a dohody o pravidlech a principech spolupráce v rámci této platformy.

V červnu navázal NBÚ spolupráci s příslušným italským úřadem Dipartimento delle Informazioni per la Sicurezza, v říjnu s EC3 Unit Europolu a dále v listopadu s rumunským národním dohledovým pracovištěm CERT-RO. V roce 2014 byla rovněž prohlubována spolupráce se stávajícími partnerskými úřady, zejména ze Slovenska, Rakouska, Maďarska, Polska, Německa, Francie, Jižní Koreje, Spojených států a Izraele. Například se zmíněným slovenským CSIRT.SK došlo k vzájemné výměně bezpečnostních nástrojů vyvíjených jednotlivými týmy.

V případě Spojených států se posílila spolupráce s Department of Homeland Security, jenž NBÚ nabídnul přístup do svého neveřejného portálu a dále možnost účastnit se školení v oblasti průmyslových řídicích systémů. Posílila se i spolupráce s americkým Federálním úřadem pro vyšetřování (Federal Bureau of Investigation), který připravil pro pracovníky NBÚ školení.

Kybernetická bezpečnost se stala jedním z bodů mezivládních konzultací vlády České republiky

[2]) Jedná se o pozice Management Board Member a Alternate Management Board Member.

a Izraele, které se uskutečnily v listopadu v Jeruzalémě. Během těchto konzultací byla podepsána společná deklarace o spolupráci v oblasti kybernetické bezpečnosti, kterou za vládu České republiky podepsal náměstek ředitele NBÚ Jaroslav Šmíd.

Spolupráce v oblasti kybernetické bezpečnosti byla také předmětem jednání ředitele NBÚ Dušana Navrátila s komisařkou EU pro digitální agendu Neelie Kroes, ministrem britské vlády Francisem Maudem a koordinátorem amerického Department of State Christopherem Painterem.

V rámci spolupráce mezi Českou republikou a NATO Cooperative Cyber Defence Centre of Excellence (dále „CCDCOE"), jehož posláním je přispívat ke zvyšování kybernetické obrany a zlepšovat spolupráci a sdílení informací mezi účastnickými státy a NATO, vyslal NBÚ v lednu 2014 jednoho pracovníka do právní a politické divize CCDCOE jako tzv. voluntary national contribution.

Příkladem za všechny může být bezplatné školení expertů, kterých se v roce 2014 zúčastnilo celkem 6 pracovníků GovCERT.CZ. Školení bylo zaměřeno na analýzu malware, bezpečnostní monitoring, forenzní činnost a analýzu pokročilých síťových hrozeb. Vedle toho se dva pracovníci OTPVV účastnili týdenního kurzu zabývajícího se aplikací mezinárodního práva v oblasti kybernetické bezpečnosti.

V srpnu 2014 se GovCERT.CZ stal akreditovaným členem evropského sdružení Trusted Introducer[3]) (dále „TI"). Toto sdružení působí v rámci evropské organizace TERENA a sdružuje evropské bezpečnostní týmy vládní, národní, komerční sféry (např. bank, provozovatelů internetového připojení, výrobců hardware atd.) nebo univerzit. Vstup GovCERT.CZ mezi akreditované týmy TI znamená další krok k užší spolupráci se světovou infrastrukturou bezpečnostních týmů CERT nebo CSIRT a zvýšení prestiže na mezinárodní scéně.

NBÚ se během roku 2014 zúčastnil celkem šesti cvičení – Cyber Europe, Locked Shields, CECSP 2014 Exercise, Cyber Czech, EU-Multi Layer a Cyber Coalition. Měl se zúčastnit i cvičení Crisis Management Exercise 2014, které však bylo na základě rozhodnutí Severoatlantické rady NATO přesunuto na rok 2015.

6. NÁRODNÍ SPOLUPRÁCE

Pro zajišťování kybernetické bezpečnosti je důležitá i široká spolupráce na národní úrovni, přičemž slovo národní zde zahrnuje aktivní kooperaci mezi veřejnou a soukromou sférou a s občanskou společností.

V roce 2014 pokračovala spolupráce mezi bezpečnostním týmem CSIRT.CZ a GovCERT.CZ, která z původní konzultační roviny přešla do roviny praktického řešení kybernetických incidentů. CSIRT.CZ nejenže spolupracoval na řešení útoků na informační infrastrukturu, ale současně se podílel na konzultacích k zákonu o kybernetické bezpečnosti a prováděcím právním předpisům. GovCERT.CZ se rovněž v součinnosti s laboratořemi CZ.NIC zapojil do skenování českých webů na zranitelnost HeartBleed. Spolupráce se osvědčila i v rámci letošního cvičení Cyber Europe, kde oba týmy společně řešily množství technických úkolů. Nelze nezmínit také první národní kybernetické cvičení, pořádané NBÚ, na jehož scénářích se významnou měrou podíleli právě pracovníci CSIRT.CZ.

Mezi další CSIRT týmy, se kterými GovCERT.CZ udržuje úzké vztahy, patří CSIRT Masarykovy univerzity (dále „CSIRT-MU"). Ten se řadí ke špičkovým pracovištím evropského formátu. Spolupráce s CSIRT-MU probíhá převážně v technické oblasti. Teoretická podpora je stejně jako v loňském roce doplněna stážemi v CSIRT-MU. Neméně zajímavé je i zapojení členů GovCERT.CZ do projektu Kybernetický polygon (KYPO), jež se zabývá výzkumem, vývojem a sestavením unikátního prostředí pro provádění a analýzu hrozeb ohrožujících bezpečnost KII či projektu Czech Cyber Crime Centre of Excellence, jehož cílem je vytvořit kvalitní centrum pro školení a vzdělávání v oblasti prevence a represe kybernetické kriminality.

Relevantními partnery v oblasti řešení kybernetických bezpečnostních incidentů jsou také zpravodajské služby a PČR. Meritem takovéto spolupráce je především výměna informací o aktuálních a řešených kybernetických bezpečnostních incidentech, zkušeností s jejich zvládáním a vzájemného know-how.

GovCERT.CZ nadále úzce kooperuje s Centrem CIRC neboli hlavní složkou kybernetické bezpečnosti Armády České republiky. Kromě výměny informací a sdílení zkušeností a informací o kybernetických

[3]) Viz http://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/govcertcz-se-stal-akreditovanym-clenem-evropskeho-sdruzeni-trusted-introducer/.

incidentech se společně účastní také kybernetických cvičení, především Cyber Coalition, kde v rámci společné reprezentace České republiky v NATO představují významné partnery při řešení scénářů.

NBÚ/NCKB již dříve navázal a nadále udržuje vztahy s akademickou sférou v České republice formou smluv o spolupráci. Ke konci roku 2014 byly podepsány smlouvy s následujícími akademickými institucemi: Masarykova univerzita, Vysoké učení technické v Brně, Univerzita obrany, České vysoké učení technické v Praze, Univerzita Palackého v Olomouci a Vysoká škola CEVRO Institut. Jednání probíhají s Policejní akademií České republiky, Vysokou školou báňskou – Technickou univerzitou Ostrava a Karlovou univerzitou v Praze.

Klíčovým partnerem pro NCKB, a to zejména v oblasti analýzy botnetů a poskytování informací o IP adresách a napadených počítačích malware, je společnost Microsoft. NCKB od společnosti získává unikátní data, se kterými dále pracuje. Díky jejich analýze a vyhodnocování dochází ke zvyšování kybernetické bezpečnosti České republiky.

Skrze Českou bankovní asociaci spolupracuje NCKB také s bankami, které mají zájem na zvyšování ochrany jejich počítačové infrastruktury. Právě banky se stávají častým terčem kybernetických útoků.

GovCERT.CZ také úzce kooperuje s členy tzv. Bezpečné VLAN, nyní FENIX. Tento projekt by měl v budoucnu výrazně mírnit následky masivních DDoS útoků obdobných těm, jaké Česká republika zaznamenala v březnu 2013.

Mimo zmíněných partnerů na národní úrovni NCKB aktivně spolupracuje s Asociací krajů České republiky, Krajem Vysočina, AFCEA a Národním centrem pro bezpečnější internet.

V měsíci říjnu uspořádalo NCKB první národní cvičení v oblasti kybernetické bezpečnosti CYBER CZECH 2014. Jednalo se o netechnické, tzv. table-top cvičení, jehož záměrem bylo formou skupinové diskuze procvičit schopnost spolupráce při zvládání kybernetických bezpečnostních incidentů a ověřit komunikační kanály, které se při řešení používají. Celodenního cvičení se zúčastnili zástupci ministerstev dopravy, financí, obrany, průmyslu a obchodu, vnitra, zahraničních věcí, práce a sociálních věcí, spravedlnosti, životního prostředí, školství, mládeže a tělovýchovy, dále Úřadu na ochranu osobních údajů, Českého telekomunikačního úřadu, České národní banky, Úřadu vlády a Správy základního registru. V rámci dvou simulovaných scénářů byli všichni sezvaní cvičící coby bezpečnostní ředitelé a manažeři bezpečnosti informačních technologií fiktivního ministerstva vystaveni otázkám, jak by postupovali v případě rozsáhlých DDoS útoků namířených na webové stránky tohoto ministerstva a cílených phishingových zpráv zaslaných jeho zaměstnancům.

Skupinu šestnácti cvičících doplňovala dvanáctičlenná odborná porota, v níž usedli zástupci bezpečnostního týmu CSIRT.CZ, CSIRT-MU, poskytovatele internetových služeb ACTIVE 24, Nejvyššího státního zastupitelství, PČR, zpravodajských služeb, dále odborníci na právo IT z Masarykovy univerzity a zástupci NBÚ. Jejich úkolem bylo hodnotit a doplňovat návrhy a odpovědi cvičících.

7. ZVYŠOVÁNÍ POVĚDOMÍ A OSVĚTA

NCKB v souladu se svým posláním informuje veřejnost o svém zaměření a činnostech. Mezi tyto aktivity spadá zejména přednášková a osvětová činnost, poskytování rozhovorů do médií či správa internetových stránek www.govcert.cz, na kterých je mimo jiné možné nalézt aktuální informace o kybernetických bezpečnostních incidentech a zranitelnostech, včetně doporučení k jejich řešení a preventivních opatřeních, dále informace o legislativě včetně ZKB a s ním souvisejících prováděcích právních předpisů, podpůrné materiály k procesu určování prvků KII a VIS aj. Pracovníci NCKB se rovněž aktivně účastní odborných konferencí, a to jak konaných v České republice, tak v zahraničí.

Při příležitosti otevření NCKB v Brně uspořádal NBÚ ve dnech 13. a 14. května 2014 mezinárodní konferenci Kybernetická bezpečnost – výsledky a výzvy, kde jako hlavní řečníci vystoupili mimo jiné Sorin Ducaru (náměstek generálního tajemníka NATO pro nové bezpečnosti hrozby), Freddy Dezeure (ředitel CERT-EU), Udo Helmbrecht (generální ředitel ENISA), Melissa Hathaway (bývalá poradkyně amerického prezidenta George W. Bushe pro otázky kybernetické bezpečnosti) či Paul Schneider (bývalý náměstek ředitele amerického Department of Homeland Security).

7.1. Vzdělávací a osvětové kampaně a konference

Úlohou NCKB je kromě koordinace spolupráce na národní a mezinárodní úrovni za účelem předcházení a řešení kybernetických bezpečnostních incidentů také osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti.

Významným partnerem NBÚ pro oblast vzdělávání se v roce 2014 stal Kraj Vysočina. Ten se zapojil

do projektu Kraje pro bezpečný internet[4]) a v rámci osvěty v oblasti kybernetické bezpečnosti pořádá přednášky, školí studenty, rodiče, pedagogy i příslušníky PČR. Pracovníci NCKB se zúčastnili několika ze zmíněných přednášek.

Další osvětové aktivity zaměřuje NCKB na zaměstnance státní správy. Příkladem je přednáška na MV (Problematika kybernetické bezpečnosti z hlediska mezinárodní spolupráce), MO a NATO Allied Command Transformation Cyber Syndicate, kde pracovníci NCKB prezentovali Národní strategii kybernetické bezpečnosti na období let 2015 až 2020 a profil NCKB coby gestora kybernetické bezpečnosti v České republice. V neposlední řadě proběhl v listopadu seminář na téma nové strategie kybernetické bezpečnosti České republiky a ochrany KII i na půdě Poslanecké sněmovny České republiky.

Jak již bylo zmíněno, zaměstnanci NCKB se také často v pozici prezentujících účastní zahraničních konferencí, školení, workshopů a přednášek. Namátkou může být uvedena konference Meridian Process 2014, jež se konala v listopadu v Japonsku, kam byl pozván pracovník NCKB, aby představil proces mapování KII v České republice a seznámil mezinárodní publikum s českým konceptem zabezpečení kybernetického prostředí včetně způsobu určování KII.

Důvodem, proč právě v zahraničí jsou zástupci NCKB žádáni o přednášky s tematikou tvorby národní strategie a procesu mapování KII, je, že Česká republika patří k malé skupině států, které mají pokročilé zkušenosti s těmito procesy.

V rámci tuzemských konferencí lze zmínit přednášku na mezinárodním policejním kongresu Současné trendy v kyberkriminalitě v Ostravě nebo říjnovou IDG Konferenci, kde proběhla prezentace zkušeností s projektem Botnet Feeds. V měsíci říjnu se konala také třídenní mezinárodní konference Future Crisis, jedno z největších setkání národních i mezinárodních bezpečnostních složek se zástupci obranného průmyslu, kde opět vystoupili pracovníci NCKB s cílem seznámit posluchače s procesem určování KII. Soustavná spolupráce pokračovala s organizací AFCEA a s Policejní akademií České republiky.

7.2. Další přednášky a konference

V roce 2014 navázalo NCKB kontakty s několika institucemi zabývajícími se kybernetickou bezpečností. Jednou z aktivních neziskových organizací dlouhodobě se zabývající problematikou kybernetické bezpečnosti je Národní centrum pro bezpečnější internet (dále „NCBI“), jehož nejdůležitějším projektem je Saferinternet.cz, který usiluje o zvyšování povědomí o bezpečnějším užívání internetu. Právě s NCBI byla navázána spolupráce, v jejímž rámci se několik pracovníků NBÚ v čele s ředitelem NCKB jako hosté i jako účinkující zúčastnilo přednášek a workshopů pořádaných právě NCBI. V říjnu 2014 na žádost NCBI převzalo NCKB záštitu nad Evropským měsícem kybernetické bezpečnosti.

Další informace z oblasti kybernetické bezpečnosti najdete na stránkách NCKB – www.govcert.cz.

Seznam použitých zkratek a pojmů

AFCEA – Armed Forces Communications and Electronics Association

CCDCOE – Cooperative Cyber Defence Centre of Excellence

CECSP – Central European Cyber Security Platform

CERT – Computer Emergency Response Team

CESNET – sdružení založené v roce 1996 českými veřejnými vysokými školami a Akademií věd ČR.

CMX – cvičení Crisis Management Exercise

CSIRT – Computer Security Incident Response Team

CSIRT-MU – bezpečnostní tým pro dohled nad sítí Masarykovy univerzity v Brně

CZ.NIC – zájmové sdružení právnických osob založené předními poskytovateli internetových služeb v roce 1998, hlavní činností je provozování registru domén

ČR – Česká republika

DDoS/DoS útok – Distributed Denial of Service / Denial of Service

DoS útok – Denial of Service

EU – Evropská unie

FENIX – nové označení projektu Bezpečná VLAN

[4]) Projekt je pořádán Národním centrem pro bezpečnější internet.

GovCERT.CZ – představuje vládní koordinační místo pro okamžitou reakci na kybernetické bezpečnostní incidenty (vládní CERT – Computer Emergency Response Team), které je organizační složkou Národního bezpečnostního úřadu, respektive jeho specializovaného pracoviště Národního centra kybernetické bezpečnosti.

IDG konference – International Data Group konference

KII – Kritická informační infrastruktura

KYBERKRIMINALITA – specifický druh kriminality páchané prostřednictvím výpočetních a komunikačních technologií

MALWARE – počítačový program určený ke vniknutí nebo poškození počítačového systému.

MBA – Master of Business Administration

MO – Ministerstvo obrany

MV – Ministerstvo vnitra

NATO – Severoatlantická aliance (North Atlantic Treaty Organization)

NBÚ – Národní bezpečnostní úřad

NCKB – Národní centrum kybernetické bezpečnosti

OBSE – Organizace pro bezpečnost a spolupráci v Evropě

OTPVV – Oddělení teoretické podpory, vzdělávání a výzkumu

PČR – Policie České republiky

PHISHING – podvodná technika k získávání citlivých údajů od uživatelů na internetu

TABLE-TOP – je cvičení navrženo k testování teoretických schopností cvičících reagovat ve skupině na určitou krizovou situaci. Velkou výhodu tohoto druhu cvičení představuje možnost vyzkoušet si jakoukoliv hypotetickou situaci bez rizika způsobení škody či jiných důsledků.

TF-CSIRT - Task Force Computer Security Incident Response Team

VIS – Významný informační systém

VLAN – virtual LAN

ZKB – zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně související zákonů

Poznámky:

VĚSTNÍK

NÁRODNÍHO BEZPEČNOSTNÍHO ÚŘADU

1/2015

DUBEN
PRAHA 2015

Věstník Národního bezpečnostního úřadu
Vydavatel: Národní bezpečnostní úřad
Adresa redakce: Národní bezpečnostní úřad, Na Popelce 2/16, 150 06 Praha 5
šéfredaktor Mgr. Dušan Zouhar, tel.: 257 283 307,
e-mail: d.zouhar@nbu.cz
Redakční rada: RNDr. Anna Mašková, CSc., Ing. Petr Nedoma, Ing. Jiří Procházka,
Ing. Iva Pačesová, Mgr. Hana Rešlová, Radek Holý
Vydává a tiskne: Tiskárna MV, s. p. o., Bartůňkova 4, 149 01 Praha 415
Administraci a objednávky přijímá: Obchodní odbor Tiskárny MV, Bartůňkova 1159/4, 149 01 Praha 4
tel.: 974 887 334, 974 887 341, fax: 974 887 333
Vychází nejméně 2x ročně, doporučená cena jednotlivého vydání je 114,– Kč
Podávání novinových zásilek povolila Česká pošta, státní podnik, odštěpný závod Praha,
č. j. nov 6520/99 ze dne 7. 10. 1999
Povoleno MK ČR – 8209
ISSN 1212-7086