VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

OCHRANA UTAJOVANÝCH INFORMACÍ

Autor práce: Kristýna Richterová
Studijní obor: Bezpečnostně právní činnost ve veřejné správě
Forma studia: Kombinovaná
Vedoucí práce: JUDr. Jozef Bandžak, Ph.D.
Katedra: Katedra právních oborů a bezpečnostních studií

2017

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v této páci.

Souhlasím, aby práce byla uložena v knihovně Vysoké školy evropských a regionálních studií v Českých Budějovicích a zpřístupněna v souladu s § 47b zákona č. 111/1998 Sb. v platném znění.

……

ABSTRAKT

RICHTEROVÁ, K. *Ochrana utajovaných informací: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2017. 61 **s.** Vedoucí bakalářské práce: JUDr. Jozef Bandžak, Ph.D.

Klíčová slova: utajovaná informace, ochrana informací, fyzická bezpečnost, riziko, režimová opatření

Bakalářská práce podává základní informace o ochraně utajovaných informací na základě zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti. Teoretická část je zaměřena na analýzu tohoto zákona a dále zpracovává problematiku fyzické bezpečnosti utajovaných informací. V další části pojednává o analýze rizik v rámci fyzické bezpečnosti utajovaných informací a snaží se blíže představit metodu kontrolního listu. V empirické části jsou na základě získaných poznatků a autorčiných zkušeností navržena režimová opatření pro objekt, ve kterém se nachází zabezpečená oblast.

ABSTRACT

RICHTEROVÁ, K. *Protection of Classified Information: Bachelor thesis.* České Budějovice: The College of European and Regional Studies, 2017. 61 **s.** Supervisor: JUDr. Jozef Bandžak, Ph.D.

Keywords: classified information, protection of information, physical security, risk, special handling measures

This Bachelor's thesis provides basic information on the protection of classified information under Act no. 412/2005 Coll. on the protection of classified information and security eligibility. The theoretical part analyses this act and also deals with physical security of classified information. The next part of the thesis discusses about the risks analysis related to physical security of classified information. It attempts to present the Check List method. Based on the acquired knowledge and author's experience, the empirical part proposes special handling measures for premises where a security area is situated.

Děkuji vedoucímu bakalářské práce JUDr. Jozefovi Bandžakovi, Ph.D. za cenné rady, připomínky a metodické vedení práce. Dále děkuji doc. RNDr. Daně Procházkové, DrSc. za spolupráci a její odborné vyjádření k dané problematice.

OBSAH

ÚVOD

Způsob, kterým v průběhu historie docházelo ve společnosti k výměně informací, značně ovlivňoval sociální rozvoj. Po mnoho staletí existovaly současně navzájem odlišné kultury, které se v důsledku pomalého šíření informace významně neovlivňovaly. Informační přenos byl závislý na lidském faktoru, který byl především při přemisťování na dlouhou vzdálenost velice pomalý. Např. řecký vyslanec, který působil v Persii, chtěl dát na vědomí řeckým městům, že je vhodná doba pro povstání proti tehdejšímu perskému králi. Protože si byl vědom, že by byl jeho posel na cestě zadržen a zpráva zničena, nechal jednomu otroku oholit hlavu, napsal mu na ni nesmazatelně zprávu a počkal do té doby, než otrokovi opět vlasy narostly. Poté teprve poslal otroka a ten zprávu úspěšně doručil. Při přenosu informací za využití poslů často docházelo k jejich zadržování nebo zabíjení nepřátelskou stranou.[1]

Urychlování informačního přenosu bylo přímo úměrné vývoji dopravních prostředků. Jeden z nejzásadnějších okamžiků byl vynález telegrafu, který umožňoval komunikaci za pomoci signálů v reálném čase. Rozvoj komunikačních možností ve dvacátém století ovlivnil neformální procesy na úrovni mezilidské interakce, ale také procesy formální na úrovni politických zájmů. S rostoucí dostupností komunikačních prostředků se zvyšovaly také tendence na ochranu předávaných zpráv. Citlivost některých informací měla za následek jejich utajení. Při tomto procesu dochází ke klasifikaci informací na základě následků, které by mělo jejich případné vyzrazení či zneužití.

„Není pochyb o tom, že se lidé nachází v době převratných technologických a společenských změn. Vývoj digitálních technologií určených k vytváření, zpracování, šíření a užívání informací závažně přispěl ke vzniku nové informační společnosti. Někteří vizionáři vidí novou informační společnost jakožto panaceu (všelék) na vyřešení světových problémů a na vybudování lepšího světa, zatímco jiní vyjadřují obavy z nebezpečí, které s sebou mohou nové technologie přinést, a z jejich negativního vlivu na lidskou společnost. **Je zřejmé, že informační technologie jsou pouze nástrojem, kterého lze použít k dobrým či špatným účelům**.“[2]

[1] VONDRUŠKA, P. *Cesta kryptografie do nového tisíciletí: od Kámasutry k osobním zápiskům K. H. Máchy*. [online]. Praha: Crypto-World, 2000 [cit. 2008-04-24]. Dostupné z WWW: <http://www.math.muni.cz/~bulik/vyuka/aplikace/vondruska-cesta.pdf>.

[2] KNÝ, M. a POŽÁR, J.. Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti. Brno: Tribun EU, 2010, s. 79.

Utajování informací mělo a stále má zejména strategické důvody. Držitel takovéto informace má oproti ostatním, kteří k utajovaným informacím (dále jen UI) přístup nemají, výhodu v tom, že může své další kroky učinit již na základě znalosti této informace. Naopak ten, kdo s touto informací seznámen není, musí přijmout méně výhodnou pozici.

„Informační bezpečnost vyžaduje celou řadu organizačních opatření, různých technik, přístupů a nových metod, neboť data a informace je třeba chránit určitým způsobem nejen proti neúmyslnému narušení, jako např. nedbalosti, selhání technických prostředků informačních a komunikačních technologií, živelným pohromám, chybám programů, chybám při přenosu dat, ale také proti úmyslnému, záměrnému narušení a ničení, sabotáži, zvědavosti nebo počítačové kriminalitě.“[3]

„Obecně lze rozdělit informační bezpečnost do několika oblastí. Bezpečnostní politika, řízení aktiv, řízení přístupu, organizační, personální, fyzická bezpečnost, řízení komunikací a provozu, oblast vývoje a údržby informačních systémů, řízení kontinuity činností organizace, zvládání bezpečnostních incidentů a také soulad s požadavky. Přesto platí známé pravidlo informační bezpečnosti, že systém je tak bezpečný, jak je zabezpečen jeho nejslabší článek.“[4]

Bakalářská práce (dále jen „práce“) se zabývá především současnou právní úpravou ochrany UI se zaměřením na problematiku fyzické bezpečnosti v rámci České republiky. Práce je založena na studiu zákonů, vyhlášek, nařízení a v neposlední řadě odborné literatury. Podstatnou roli při zpracování práce mají konzultace s odborníky, kteří působí v oboru fyzické bezpečnosti, personální bezpečnosti a oblasti vyhodnocování rizik.

[3] POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, s. 7.
[4] DRASTICH, M. *Systém managementu bezpečnosti informací*. Praha: Grada, 2011, s. 19.

1 CÍLE A METODIKA BAKALÁŘSKÉ PRÁCE

1.1 Cíle

Práce si klade za úkol splnění dvou hlavních cílů. **Prvním z hlavních cílů** této práce je vytvoření uceleného materiálu, jehož bude dosaženo za pomoci jednotlivých dílčích cílů. Prvním z nich je zpracování historické chronologie právní úpravy utajovaných informací na území České republiky spolu s analýzou zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Dalším z dílčích cílů je analýza působnosti vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. Posledním dílčím cílem je definice základních pojmů v rámci rizik fyzické bezpečnosti.

Druhým hlavním cílem je vytvořit na základě získaných poznatků a vlastních zkušeností autentická režimová opatření pro objekt státní správy, ve kterém se nachází zabezpečená oblast.

Cílem této práce není vytvoření analýzy veškeré platné legislativy vztahující se k oblasti ochrany utajovaných informací. Vzhledem ke stanovenému rozsahu práce by tuto oblast nebylo možné dostatečně obsáhnout. Z tohoto důvodu se práce bude soustředit především na oblast fyzické bezpečnosti utajovaných informací a vzniku možných rizik právě v této konkrétní problematice.

1.2 Metodika

Hlavní metodou, která byla použita k dosažení stanovených cílů, byl především rozbor příslušných zákonů, normativních aktů a vyhlášek. Vzhledem k náročnosti zvoleného tématu autorka své postupy konzultovala s odborníky, kteří mají v oblasti fyzické bezpečnosti UI mnohaleté zkušenosti. V neposlední řadě vývoj práce provázely konzultace s vedoucím práce.

2 HISTORIE UTAJOVANÝCH INFORMACÍ V ČR

Zákon č. 50/1923 Sb., na ochranu republiky

Poprvé se tendence legislativně řešit UI v novodobé historii českého státu objevuje v roce 1923, kdy byl vydán zákon č. 50/1923 Sb., na ochranu republiky. Tento zákon zavádí institut utajovaných informací pod názvem státní tajemství. Zrady státního tajemství se dle §5 dopustí ten, kdo přímo nebo nepřímo cizí moci vyzradí skutečnost, opatření nebo předmět, který vláda před cizí mocí tají. Dále ten, kdo takovou skutečnost, opatření nebo předmět vyzvídá, aby je přímo nebo nepřímo cizí moci vyzradil, kdo hrubou nedbalostí způsobí, že se taková skutečnost, opatření nebo předmět stanou nebo se mohou stát známými cizí moci.[5]

Zákon č. 231/1948 Sb., na ochranu lidově demokratické republiky

Roku 1948 byl vydán zákon č. 231/1948 Sb., na ochranu lidově demokratické republiky. Ten v §5 odst. 3 definuje státní tajemství jako „skutečnost, opatření nebo předmět, jež vláda tají v důležitém zájmu republiky, zejména v zájmu politickém, vojenském nebo hospodářském, nebo jež v takovém zájmu mají zůstati utajeny před cizí mocí nebo před cizími činiteli.“[6]

Zákon č. 86/1950 Sb., trestní zákon

Výše uvedený zákon č. 231/1948 Sb. na ochranu lidově demokratické republiky pozbyl platnosti roku 1950, kdy vešel v platnost zákon č. 86/1950 Sb., trestní zákon. Tento zákon definuje trestné činy proti republice, mezi které mj. patří vyzvědačství. V §86 odst. 1 je stanoveno, že trestného činu vyzvědačství se dopustí ten, kdo vyzvídá státní tajemství v úmyslu je vyzradit cizí moci, nebo kdo státní tajemství úmyslně cizí moci vyzradí. Přímo ohrožení státního tajemství řeší §88, který stanoví, že státní tajemství ohrozí ten, kdo vyzvídá státní tajemství v úmyslu vyzradit je nepovolané osobě, nebo kdo státní tajemství úmyslně takové osobě vyzradí. Tento zákon dále řeší vyzrazení

[5] Česko. Zákon č. 50/1923 Sb., na ochranu republiky. In *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.beck-online.cz/bo/chapterview-document.seam >.
[6] Česko. Zákon č. 231/1948 Sb., na ochranu lidově demokratické republiky. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <http://www.zakonyprolidi.cz/cs/1948-231>.

státního tajemství z nedbalosti, kterého se dopustí ten, kdo způsobí, že se státní tajemství může stát známým cizí moci nebo že se stalo známým nepovolané osobě.[7]

Zákon č. 140/1961 Sb., trestní zákon

Od 1. 1. 1962 se dle §105 trestního zákona č. 140/1961 Sb. trestného činu vyzvědačství dopustí ten, kdo vyzvídá státní tajemství za účelem vyzradit je cizí moci, kdo s takovým cílem sbírá údaje, obsahující státní tajemství, nebo kdo státní tajemství cizí moci úmyslně vyzradí. Stejně jako v předešlém trestním zákoně (tj. zákon č. 86/1950 Sb.) je i zde v §106 definován trestný čin ohrožení státního tajemství, kterého se dopustí ten, kdo vyzvídá státní tajemství s cílem vyzradit je nepovolané osobě, kdo s takovým cílem sbírá údaje obsahující státní tajemství, nebo kdo státní tajemství nepovolané osobě úmyslně vyzradí. Mimo vyzrazení státního tajemství nepovolané osobě nově tento zákon v §107 zavádí i ztrátu listiny nebo věci obsahující státní tajemství.[8] Tímto dochází k prvnímu legislativnímu ošetření manipulace s nosiči státního tajemství.

Vyhláška č. 181/1964 Sb., o základních skutečnostech tvořících státní tajemství

Vyhláška ministerstva vnitra o základních skutečnostech tvořících státní tajemství č. 181/1964 Sb. v článku 1 rozděluje potřebu utajovat údaje o skutečnostech podle oblastí, do kterých tyto skutečnosti věcně spadají. Těmito oblastmi jsou obrana bezpečnosti státu, oblast hospodářského zájmu a oblast politického nebo jiného důležitého zájmu.

Zákon č. 102/1971 Sb., o ochraně státního tajemství

V roce 1971 došlo k přijetí federálního zákona č. 102/1971 Sb., o ochraně státního tajemství. §1 tohoto zákona stanoví, že tento zákon upravuje ochranu státního tajemství, vymezuje způsob jeho určení i ochrany před vyzrazením i zneužitím proti společenskému a státnímu zřízení Československé socialistické republiky a jejím zájmům. Základní zásady tohoto zákona platí přiměřeně i pro úpravu ochrany hospodářského a služebního tajemství.[9] Tento zákon poprvé ucelenou legislativní formou

[7] ŠIMÁK, J., CIRKL B. Trestní zákon: komentář k zákonu ze dne 12. července 1950, č. 86 Sb. 1. vyd. Praha: Orbis, 1953, s. 257.
[8] ČESKO. Zákon č. 140/1961 Sb., trestní zákon. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/1961-140>.
[9] ČESKO. Zákon č. 102/1971 Sb., o ochraně státního tajemství. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/1971-102>.

definuje státní tajemství, odpovědnost za ochranu státního tajemství a povinnosti osob, které mají přístup ke státnímu tajemství. Na základě §2 odst. 2 tohoto zákona bylo vydáno nařízení vlády č. 149/1971 Sb., nařízení vlády Československé socialistické republiky o základních skutečnostech tvořících předmět státního tajemství. Hlavními oblastmi, ve kterých docházelo k utajování informací, byly především oblasti politické, oblasti obrany a bezpečnosti Československé socialistické republiky a oblasti hospodářské. Tyto oblasti jsou dále jednotlivě rozděleny na konkrétní základní skutečnosti.

Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností

Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností, jak je již z názvu zákona patrné, poprvé zavádí namísto státního tajemství institut utajovaných skutečností. V §1 vymezuje skutečnosti, které je nutno v zájmu České republiky utajovat (dále jen „utajované skutečnosti“), způsob jejich ochrany, působnost a pravomoc orgánů státu při výkonu státní správy v oblasti ochrany utajovaných skutečností, povinnosti orgánů státu, práva a povinnosti fyzických a právnických osob a odpovědnost za porušení povinností stanovených tímto zákonem a upravuje postavení Národního bezpečnostního úřadu.[10]

Zákon o ochraně utajovaných skutečností z roku 1998 v §5 poprvé stanoví klasifikaci utajovaných skutečností do stupňů utajení:

a) **přísně tajné;**
b) **tajné;**
c) **důvěrné, nebo**
d) **vyhrazené.**

Dále dělí jednotlivé části bezpečnosti utajovaných skutečností dle místa vzniku možného rizika na:

- **personální bezpečnost;**
- **administrativní bezpečnost;**
- **objektovou bezpečnost;**
- **technickou bezpečnost;**

[10] ČESKO. Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/1998-148>.

- **bezpečnost informačních systémů;**
- **kryptografickou ochranu;**
- **průmyslovou bezpečnost.**

Zákonem č. 148/1998 Sb. se v rámci výkonu státního dozoru nově zřizuje Národní bezpečnostní úřad (dále jen „Úřad“). Ten má za úkol působit jako ústřední správní úřad pro oblast ochrany utajovaných informací. Mimo jiné do jeho povinností spadá i výkon metodické činnosti v oblasti ochrany utajovaných skutečností.

„Zákon č. 148/1998 Sb. tak představuje nárůst ochrany utajovaných skutečností spojený se zintenzivněním zásahů do základních práv a svobod. Od počátku projednávání návrhu zákona se proto vyskytovaly pochyby odborné veřejnosti, zda jsou tyto zásahy a jejich rozsah ústavně konformní (a samozřejmě konformní s mezinárodními smlouvami o lidských právech, které Česká republika podepsala). Pozdější rozhodnutí Ústavního soudu jim dala v mnohém za pravdu. Zákon prošel několika novelizacemi, přičemž zásadní význam má novela přijatá jako zákon č. 310/2002 Sb. I jejím účelem bylo odstranění neústavností či ustanovení větší právní jistoty pro prověřované osoby a zavedení alespoň minimálního přezkumu rozhodnutí Národního bezpečnostního úřadu.“[11]

„V období let 1998-2002 ukončil NBÚ celkem 15 352 bezpečnostních prověrek osob; z toho 14 866 skončilo vydáním osvědčení a 486 nevydáním osvědčení. Je jen těžko představitelné, aby v minulosti ale i současnosti byla provedena podrobná kontrola tak velkého množství bezpečnostních prověrek. Předmětem interního auditu bylo cca 1700 bezpečnostních prověrek na stupeň utajení Přísně tajné a v cca 20 případech lze hovořit o možných nestandardních postupech. Informace získané interním auditem byly využity při vytváření současného systému provádění bezpečnostních prověrek.“[12]

[11] SVATOŠOVÁ, H. *Utajování versus základní práva a demokratické standardy včetně problematiky zbraní* [online]. Iuridicum remedium, 2005 [cit. 2016-12-29]. Dostupné z WWW: <http://www.iure.org/534579>.
[12] Národní bezpečnostní úřad. *Národní bezpečnostní úřad*. [online]. 2016 [cit. 2016-12-27]. Dostupné z WWW: <https://www.nbu.cz/cs/o-nas/o-nas/#otazka12>.

3 LEGISLATIVNÍ ÚPRAVA OCHRANY UTAJOVANÝCH INFORMACÍ V ČR

Následující kapitola pojednává o platné legislativní úpravě ochrany utajovaných informací na území České republiky. Jsou zde uvedeny tři základní právní předpisy, jejichž působnost koresponduje se zaměřením empirické části práce.

Trestnost ohrožení UI je stanovena trestním zákoníkem v platném znění, které je možné najít ve Sbírce zákonů.

Utajovanou informací se rozumí informace v jakékoliv podobě (elektronické, písemné i ústní), jejichž vyzrazení nebo zneužití může způsobit újmu zájmům České republiky, členských zemí EU nebo NATO, nebo mohou být pro tento zájem nevýhodné. Utajované informace jsou uvedeny v seznamu utajovaných informací, který je vydán jako vládní nařízení ve Sbírce zákonů.[13]

3.1 Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

„Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.“[14] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění (dále jen „zákon“) je rozdělen do devíti částí. Tyto části se systematicky dále dělí na hlavy označené římskými číslicemi. Výše uvedené části zákona se nazývají:

1) ČÁST PRVNÍ – Základní ustanovení;
2) ČÁST DRUHÁ – Ochrana utajovaných informací;
3) ČÁST TŘETÍ – Bezpečnostní způsobilost;
4) ČÁST ČTVRTÁ – Bezpečnostní řízení;
5) ČÁST PÁTÁ – Výkon státní správy;
6) ČÁST ŠESTÁ – Státní dozor;
7) ČÁST SEDMÁ – Kontrola činnosti Úřadu;

[13]DRAKAS. *DRAKAS* [online]. 2016 [cit. 2017-02-09]. Dostupné z WWW: <http://www.drakas.cz/dotazy.html#utajovana>.
[14] PROCHÁZKOVÁ, D. *Ochrana osob a majetku*. V Praze: České vysoké učení technické, 2011, s. 256.

8) ČÁST OSMÁ – Správní delikty;
9) ČÁST DEVÁTÁ – Přechodná a závěrečná ustanovení.

3.1.1 Základní ustanovení

V této části (§1 – §2) je vymezen předmět úpravy zákona spolu s definicí klíčových pojmů, které se vztahují k oblasti ochrany utajovaných informací. Těmito pojmy se rozumí:

a) utajovaná informace;
b) zájem České republiky;
c) porušení povinnosti při ochraně UI;
d) orgán státu;
e) odpovědná osoba;
f) původce UI;
g) cizí moc;
h) neoprávněná osoba;
i) poučení;
j) bezpečnostní standard;
k) bezpečnostní provozní mód.

3.1.2 Ochrana utajovaných informací

Ústředním správním úřadem pro oblast ochrany utajovaných informací a zároveň orgánem výkonné moci, jehož oblastí je ochrana utajovaných informací a bezpečnostní způsobilost, je Úřad, který má od samého počátku působení (jak podle zákona č. 148/1998 Sb., tak i podle nového zákona č. 412/2005 Sb.) stále stejné postavení. Kontrolním orgánem dohlížejícím na činnost Úřadu se od 1. 1. 2006 stala Stálá komise pro kontrolu činnosti NBÚ, která je zřízena Poslaneckou sněmovnou Parlamentu ČR.[15]

Samotnou ochranou utajovaných informací se rozumí soubor postupů a prostředků, které jsou aplikovány v rámci jednotlivých druhů zabezpečení ochrany utajovaných informací za účelem zajištění svrchovanosti, územní celistvosti, vnitřního pořádku a bezpečnosti, ekonomické stability, demokratických základů a ochrany životů a zdraví občanů České republiky.

[15] Národní bezpečnostní úřad. *Národní bezpečnostní úřad.* [online]. 2016 [cit. 2016-12-29]. Dostupné z WWW: <https://www.nbu.cz/cs/o-nas/o-nas/#otazka01>.

Druh a míra ochrany UI jsou aplikovány v závislosti na předpokladu, jakou újmu by zájmům České republiky mohlo způsobit vyzrazení UI neoprávněné osobě nebo její zneužití. Na základě závažnosti poškození nebo ohrožení zájmu rozlišujme **čtyři stupně utajení**:

a) **VYHRAZENÉ –** vyzrazení neoprávněné osobě nebo zneužití UI tohoto stupně může být pro zájmy ČR **nevýhodné**. Oznámení při splnění podmínek pro tento stupeň utajení se v praxi uděluje např. příslušníkům bezpečnostních sborů, kteří se v rámci výkonu služby potřebují seznamovat s UI. Tito příslušníci mohou být běžnými referenty či příslušníky v pozici vyšetřovatele;

b) DŮVĚRNÉ – vyzrazení neoprávněné osobě nebo zneužití UI tohoto stupně může zájmům ČR způsobit **prostou újmu**. Osvědčení při splnění podmínek pro tento stupeň utajení se v praxi uděluje např. příslušníkům bezpečnostních sborů, u kterých si to žádá povaha jejich služebního zařazení. Mohou to být vyšetřovatelé závažnějších trestných činů, pracovníci bezpečnostních oddělení či referenti, kteří zpracovávají UI;

c) **TAJNÉ –** vyzrazení neoprávněné osobě nebo zneužití UI tohoto stupně může zájmům ČR způsobit **vážnou újmu**. Osvědčení při splnění podmínek pro tento stupeň utajení se v praxi uděluje např. příslušníkům zpravodajských služeb, bezpečnostním ředitelům či jiným pracovníkům bezpečnostních oddělení;

d) **PŘÍSNĚ TAJNÉ –** vyzrazení neoprávněné osobě nebo zneužití UI tohoto stupně může zájmům ČR způsobit **mimořádně vážnou újmu**. Osvědčení při splnění podmínek pro tento stupeň utajení se v praxi uděluje např. příslušníkům zpravodajských služeb, armádním příslušníkům, zaměstnancům kanceláře prezidenta republiky atp.

Konkrétní činnosti, které vedou k újmě na zájmu České republiky, jsou uvedeny v §3 zákona.

Zajištění bezpečnosti UI dochází pomocí šesti druhů ochrany UI. Zákon tyto druhy klasifikuje a dále definuje, čím jsou tyto druhy ochrany UI tvořeny.

Dle §5 zákona je ochrana UI zajišťována:

a) **personální bezpečností**, kterou tvoří výběr fyzických osob, které mají mít přístup k utajovaným informacím, ověřování podmínek pro jejich přístup k utajovaným informacím, jejich výchova a ochrana;

b) **průmyslovou bezpečností**, kterou tvoří systém opatření k zjišťování a ověřování podmínek pro přístup podnikatele k utajovaným informacím a k zajištění nakládání s utajovanou informací u podnikatele v souladu s tímto zákonem;
c) **administrativní bezpečností**, kterou tvoří systém opatření při tvorbě, příjmu, evidenci, zpracování, odesílání, přepravě, přenášení, ukládání, skartačním řízení, archivaci, případně jiném nakládání s utajovanými informacemi;
d) **fyzickou bezpečností**, kterou tvoří systém opatření, která mají neoprávněné osobě zabránit nebo ztížit přístup k utajovaným informacím, popřípadě přístup nebo pokus o něj zaznamenat;
e) **bezpečností informačních nebo komunikačních systémů**, kterou tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost utajovaných informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním nebo komunikačním systému a;
f) **kryptografickou ochranou**, kterou tvoří systém opatření na ochranu utajovaných informací použitím kryptografických metod a kryptografických materiálů při zpracování, přenosu nebo ukládání utajovaných informací.[16]

Personální bezpečnost

Oblast personální bezpečnosti je ošetřena prováděcím předpisem, kterým je vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, v platném znění.

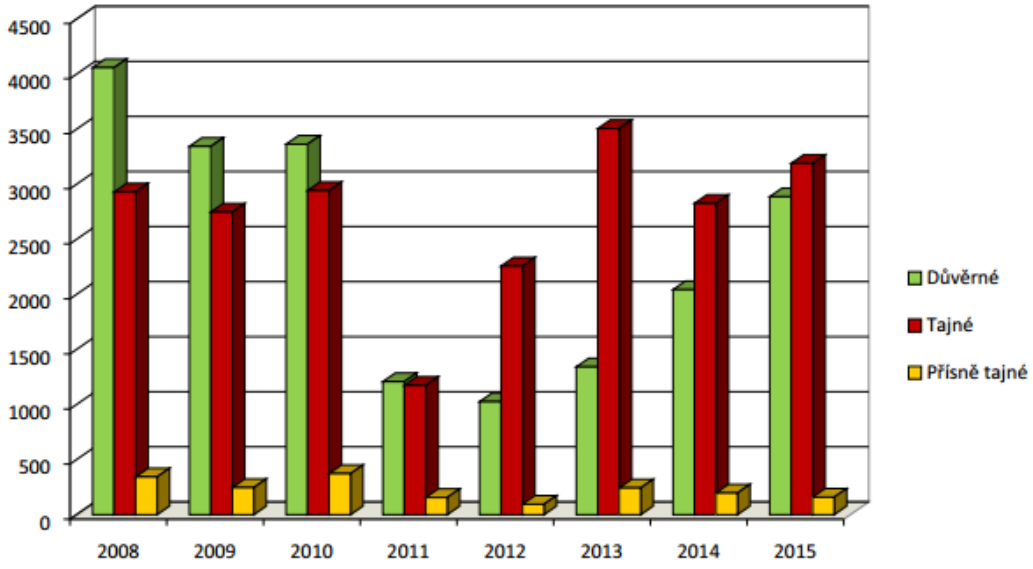
Cílem personální bezpečnosti je, aby k UI měla přístup a mohla se s ní seznámit pouze ta osoba, která tuto informaci nutně potřebuje znát k výkonu své pracovní činnosti.

Do styku s utajovanými informacemi nepřichází pouze státní zaměstnanci, ale také zaměstnanci firem, které se státními složkami navazují vztahy např. v podobě státních zakázek. Takovými firmami jsou např. firma Forsolution, která je prodejcem speciální techniky; firma Jablotron, která je prodejcem komunikačních a zabezpečovacích systémů; firma Sellier & Bellot, která je výrobcem a prodejcem střeliva atd.

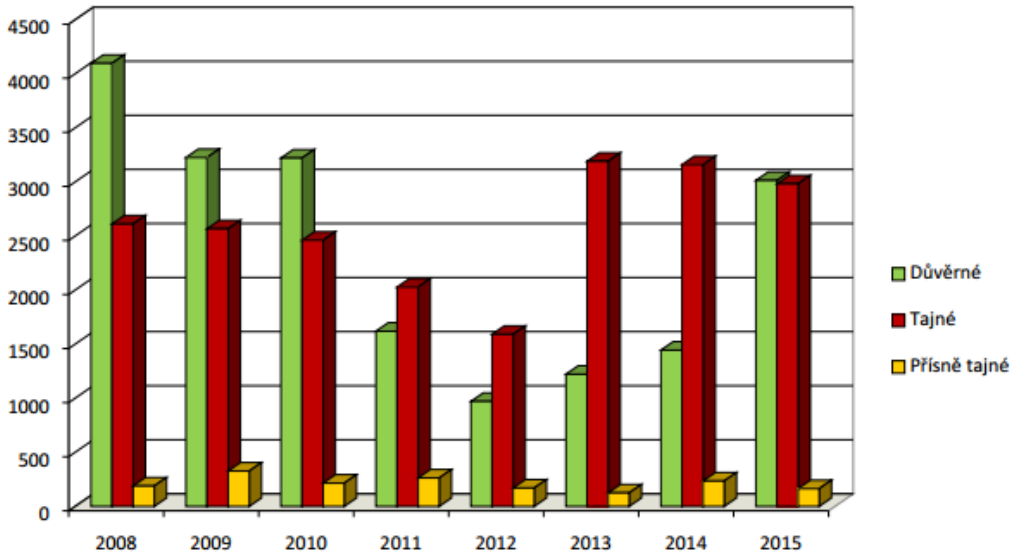
[16] ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-412>.

V rámci personální bezpečnosti Úřad provádí zejména bezpečnostní řízení o žádostech fyzických osob, vydává osvědčení fyzické osoby a rozhodnutí o nevydání osvědčení fyzické osoby.

Graf 1: Přijaté žádosti o vydání osvědčení fyzické osoby v letech 2008 až 2015[17]



Graf 2: Vydaná osvědčení fyzické osoby v letech 2008 až 2016[18]



[17] Národní bezpečnostní úřad. *Národní bezpečnostní úřad* [online]. 2017 [cit. 2017-02-10]. Dostupné z WWW: <https://www.nbu.cz/cs/informacni-centrum/povinne-zverejnovane-informace/906-vyrocni-zpravy-o-cinnosti-nbu>.

[18] Národní bezpečnostní úřad. *Národní bezpečnostní úřad* [online]. 2017 [cit. 2017-02-10]. Dostupné z WWW: <https://www.nbu.cz/cs/informacni-centrum/povinne-zverejnovane-informace/906-vyrocni-zpravy-o-cinnosti-nbu>.

V oblasti personální bezpečnosti Úřad spolupracuje s orgány státu jako je Policie ČR, zpravodajské služby a další subjekty, které disponují informacemi podstatnými pro bezpečnostní řízení.[19]

Průmyslová bezpečnost

Oblast průmyslové bezpečnosti je ošetřena prováděcím předpisem, kterým je vyhláška č. 405/2011 Sb., o průmyslové bezpečnosti, v platném znění.

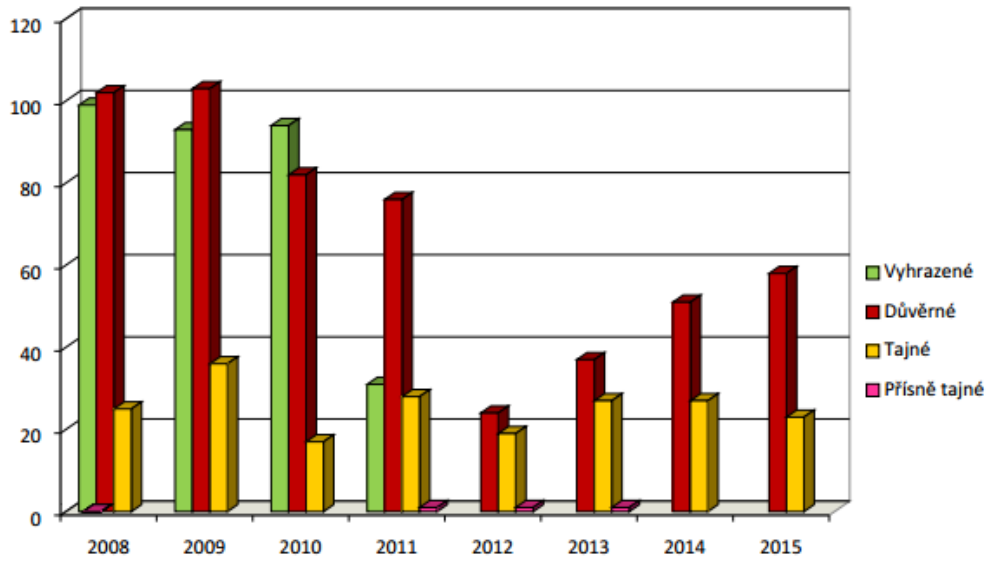
Průmyslovou bezpečností se rozumí souhrn podmínek a opatření, které jsou aplikovány za účelem ochrany UI při přístupu podnikatele k utajované informaci, dále při jejím vytváření a uchovávání podnikatelem.

Hlavní činností, která je Úřadem v oblasti průmyslové bezpečnosti realizována, je zejména provádění bezpečnostních řízení o žádostech podnikatelů o vydání osvědčení podnikatele. Úřad dále přijímá žádosti podnikatelů o osvědčení podnikatele pro cizí moc a při splnění zákonem stanovených podmínek tato osvědčení vydává. Ve vztahu k podnikatelům, kteří již jsou držiteli osvědčení podnikatele, se činnost Úřadu zaměřuje na provádění úkonů, které slouží k prověření, zda podnikatel nadále splňuje zákonné podmínky pro vydání osvědčení podnikatele. [20]

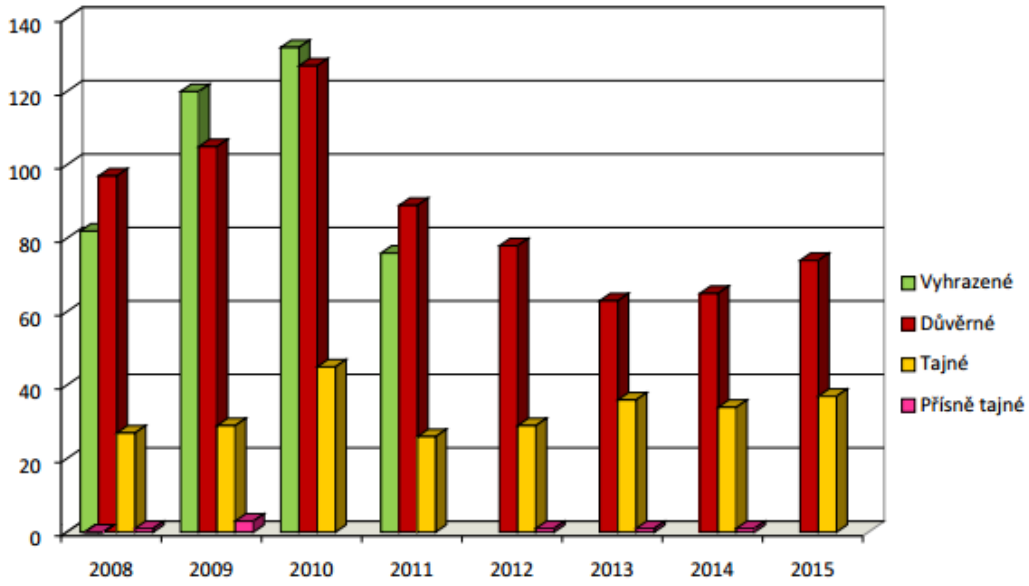
[19] Národní bezpečnostní úřad. *Národní bezpečnostní úřad* [online]. 2017 [cit. 2017-02-10]. Dostupné z WWW: <https://www.nbu.cz/cs/informacni-centrum/povinne-zverejnovane-informace/906-vyrocni-zpravy-o-cinnosti-nbu>.

[20] Národní bezpečnostní úřad. *Národní bezpečnostní úřad* [online]. 2017 [cit. 2017-02-10]. Dostupné z WWW: <https://www.nbu.cz/cs/informacni-centrum/povinne-zverejnovane-informace/906-vyrocni-zpravy-o-cinnosti-nbu>.

Graf 3: Přijaté žádosti o vydání osvědčení podnikatele v letech 2008 až 2015[21]



Graf 4: Vydaná osvědčení podnikatele v letech 2008 až 2015[22]



Administrativní bezpečnost

Oblast administrativní bezpečnosti je ošetřena prováděcím předpisem, kterým je vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, v platném znění (dále jen vyhláška o administrativní bezpečnosti).

[21] Národní bezpečnostní úřad. *Národní bezpečnostní úřad* [online]. 2017 [cit. 2017-02-10]. Dostupné z WWW: <https://www.nbu.cz/cs/informacni-centrum/povinne-zverejnovane-informace/906-vyrocni-zpravy-o-cinnosti-nbu>.
[22] Národní bezpečnostní úřad. *Národní bezpečnostní úřad* [online]. 2017 [cit. 2017-02-10]. Dostupné z WWW: <https://www.nbu.cz/cs/informacni-centrum/povinne-zverejnovane-informace/906-vyrocni-zpravy-o-cinnosti-nbu>.

Administrativní bezpečnost vytváří soubor postupů a opatření, které mají za cíl zajistit dostatečnou ochranu UI při jejím vytváření, přenosu, převzetí, tvorbě jejích opisů a kopií, ukládání, nálezu a při dalších způsobech nakládání s ní.

Pracoviště koncepce administrativní bezpečnosti působí především osvětu a metodický výklad v souvislosti s vyhláškou o administrativní bezpečnosti. Další činnosti uvedeného pracoviště spočívají v popisu procesů, které řeší manipulaci a archivaci dokumentů v elektronické formě.[23]

Fyzická bezpečnost

Oblast fyzické bezpečnosti je ošetřena prováděcím předpisem, kterým je vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, v platném znění. Působnost této vyhlášky je blíže popsána v kapitole 3.3. této práce.

Bezpečnost informačních a komunikačních systémů

Oblast bezpečnosti informačních a komunikačních systémů je ošetřena prováděcím předpisem, kterým je vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, v platném znění.

Bezpečností informačních a komunikačních systémů se rozumí soubor opatření, která mají zajistit, aby při manipulaci s utajovanými informacemi v rámci informačních a komunikačních systémů nedocházelo k jejich poškozování, úniku, kompromitujícímu vyzařování či jiné manipulaci, která by mohla představovat ohrožení chráněného zájmu.

Kryptografická ochrana

Oblast kryptografické ochrany je ošetřena prováděcím předpisem, kterým je vyhláška č. 432/2011 Sb. o zajištění kryptografické ochrany utajovaných informací, v platném znění.

Kryptografickou ochranou se rozumí soubor opatření, která slouží k ochraně utajovaných informací za pomoci kryptografických prostředků. K výrobě nebo testování materiálu k zajištění funkce kryptografického prostředku, ukládání kryptografického

[23] Národní bezpečnostní úřad. *Národní bezpečnostní úřad* [online]. 2017 [cit. 2017-02-10]. Dostupné z WWW: <https://www.nbu.cz/cs/informacni-centrum/povinne-zverejnovane-informace/906-vyrocni-zpravy-o-cinnosti-nbu>.

materiálu nebo k výrobě a testování kryptografických prostředků slouží tzv. kryptografické pracoviště.[24]

Obecně lze říci, že kryptografie je věda o tvorbě šifer, kdy informace mají abecedně číslicový charakter. Kryptografie studuje šifrovací algoritmy, kryptografické nástroje, hardwarové implementace šifrovacích algoritmů, kryptografické protokoly atd. Šifrovacím algoritmem se rozumí takový algoritmus, který se snaží utajit data jejich zašifrováním. Kryptografie se tedy především zabývá problematikou převádění otevřených informací, které lze běžně přečíst, na informace nesrozumitelné, které případný úročník či narušitel nebude schopen bez šifrovacího algoritmu přečíst a dále zneužít.[25]

3.1.3 Bezpečnostní způsobilost

Zákon v § 80 definuje činnost, jejímž zneužitím by mohlo dojít k ohrožení zájmu České republiky. Tuto činnost, může vykonávat pouze ta fyzická osoba, která je bezpečnostně způsobilá (příloha I – vzor dokladu o bezpečnostní způsobilosti[26]) nebo která je držitelem platného osvědčení fyzické osoby (příloha II – vzor osvědčení fyzické osoby[27]). Zákon pro výše uvedené zavádí pojem „citlivá činnost“ a dále stanoví, jaké podmínky musí fyzická osoba splnit, aby tuto činnost mohla provádět.

3.1.4 Bezpečnostní řízení

V § 89 – § 135 jsou stanoveny hlavní zásady, postupy a činnosti, které musí být Úřadem prováděny při bezpečnostním řízení, které je obligatorním krokem k získání osvědčení fyzické osoby a osvědčení osoby podnikatele, na základě kterého se tato osoba může dále seznamovat s utajovanými informacemi toho stupně, pro který jí bude výše uvedené osvědčení vydáno.

Žádost fyzické osoby i žádost podnikatele o vydání osvědčení musí obsahovat požadované náležitosti a přílohy, které zákon stanoví. V případě, že fyzická osoba

[24] ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-412>.
[25] POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, s. 191.
[26] Národní bezpečnostní úřad. *Národní bezpečnostní úřad*. [online]. 2016 [cit. 2017-02-10]. Dostupné z WWW: < https://www.nbu.cz/cs/bezpecnostni-zpusobilost/887-obecne-k-bezpecnostni-zpusobilosti/#doklad>.
[27] Národní bezpečnostní úřad. *Národní bezpečnostní úřad*. [online]. 2016 [cit. 2017-02-10]. Dostupné z WWW: < https://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost-oznameni-pro-v-osvedceni-d-t-pt-certifikaty/1045-osvedceni-fyzicke-osoby/>.

nebo osoba podnikatele opomene některou z těchto náležitostí či příloh Úřadu poskytnout, pomůže Úřad této osobě formální nedostatky odstranit. Pokud nelze vady na místě odstranit, Úřad vyzve osobu k nápravě nedostatků žádosti písemně. Lhůta na nápravu je 30 dní ode dne, kdy byla výzva osobě doručena.

Proti rozhodnutí Úřadu vydanému v řízení má účastník řízení právo podat rozklad, pokud se tohoto práva po doručení rozhodnutí písemně nevzdal. O rozkladu rozhoduje ředitel Úřadu na základě návrhu rozkladové komise. Proti rozhodnutí ředitele Úřadu o rozkladu lze podat žalobu podle Soudního řádu správního ve lhůtě 30 dnů ode dne doručení rozhodnutí.[28]

3.1.5 Výkon státní správy

Státní správu v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti vykonává Úřad, který je ústředním správním úřadem. V čele Úřadu je ředitel, kterého jmenuje po projednání ve výboru Poslanecké sněmovny příslušném ve věcech bezpečnosti vláda, která ho též odvolává.[29]

Dále jsou v této části zákona definovány činnosti a oprávnění Úřadu v rámci jeho činnosti, výjimky zpravodajských služeb, Ministerstva vnitra a policie v rámci řízení podle zákona a jejich specifické postavení při provádění úkonů v rámci řízení.

3.1.6 Státní dozor

Tato část zákona obsahuje § 143 a § 144, ve kterých je stanoveno, že státním dozorem v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti je dozor nad tím, jak orgány státu, právnické osoby, podnikající fyzické osoby a fyzické osoby dodržují právní předpisy v této oblasti. Pří výkonu státního dozoru se postupuje dle zákona č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů. Zaměstnanci Úřadu mají povinnost prokázat se platným osvědčením fyzické osoby pro příslušný stupeň utajení, který je odpovídající prováděné kontrole. V případech stanovených zákonem státnímu dozoru nepodléhá činnost zpravodajských služeb a Ministerstva vnitra.

Dále zákon v této části kontrolním pracovníkům Úřadu přiznává oprávnění přijmout neodkladná opatření k zajištění ochrany utajovaných informací. Mezi

[28] ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. Dostupné z WWW: < https://www.zakonyprolidi.cz/cs/2005-412>.
[29] ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-412>.

tato opatření mj. patří i odejmutí utajované informace. Náklady za nutná opatření k zajištění ochrany utajované informace hradí kontrolovaná osoba.[30]

3.1.7 Kontrola činnosti Úřadu

Kontrolu nad činností Úřadu vykonává zvláštní sedmičlenný orgán, který je zřízen Poslaneckou sněmovnou. Členem kontrolního orgánu může být pouze poslanec Poslanecké sněmovny. Zákon stanoví oprávnění a povinnosti zvláštního kontrolního orgánu a dokumenty, které ředitel Úřadu tomuto orgánu předkládá. Výše uvedený orgán kontroluje především, zda Úřad postupuje v souladu s platnými právními předpisy a zda vykovává činnosti pouze ve své stanovené působnosti.

3.1.8 Přestupky a správní delikty

V této části zákon taxativně vymezí činnosti, kterými se osoba dopustí přestupku v oblasti ochrany UI. Tyto činnosti jsou systematicky děleny dle druhu osoby, která se přestupku dopouští. Výše uvedenými osobami jsou:

a) fyzická osoba;
b) fyzická osoba, která má přístup k UI;
c) fyzická osoba, která je držitelem osvědčení fyzické osoby;
d) fyzická osoba, která je držitelem oznámení;
e) fyzická osoba, která je držitelem dokladu;
f) právnická osoba nebo podnikající fyzická osoba, které mají přístup k UI, nebo orgán státu;
g) podnikatel, který má přístup k UI;
h) podnikatel, který je držitelem osvědčení podnikatele;
i) podnikatel.

Zákon stanoví maximální výši pokuty, kterou je možné za přestupek uložit. Pokuty vybírá Úřad a příjem z pokut je příjmem státního rozpočtu.[31]

[30] ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-412>.
[31] ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-412>.

3.1.9 Přechodná a závěrečná ustanovení

Tato část zákona upravuje přechod působnosti předešlých právních předpisů na působnost zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. „Pokud se v dosavadních právních předpisech mluví o utajovaných skutečnostech nebo o státním a služebním tajemství, rozumí se tím utajované informace podle tohoto zákona.“[32] Dále kromě přechodných ustanovení obsahuje ustanovení zmocňovací a zrušovací.

3.2 Seznam utajovaných informací

Nařízení vlády č. 522/2005 Sb. (dále jen Nařízení) stanoví seznamy UI, jenž jsou na základě působností v jednotlivých přílohách rozděleny do níže uvedených oblastí.

V příloze č. 1 Nařízení stanoví obecnou část seznamu utajovaných informací, v příloze č. 2 seznam utajovaných informací v oblasti působnosti Ministerstva dopravy, do kterého patří např. informace o strategických záměrech hospodářského rozvoje dopravy, pokud obsahují údaje, které se týkají obrany a bezpečnosti státu nebo údaje k zajištění speciálních přeprav a interní předpisy s tím související. [33]

V příloze č. 3 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Ministerstva financí, mezi které patří např. činnost celních orgánů při odhalování trestných činů a jejich pachatelů, postupy a výslechy. [34]

V příloze č. 4 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Ministerstva kultury, do kterého mj. patří informace o projektové dokumentaci elektrických zabezpečovacích signalizací, uzavřeného televizního systému, tísňového systému nebo systému pro kontrolu vstupů sloužící ochraně objektů, v nichž jsou uchovávány kulturní statky, proti krádežím, loupežím a poškozování cizí věci.[35]

V příloze č. 5 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Ministerstva obrany, na základě kterého lze za UI považovat např. dokumenty

[32] ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-412>.
[33] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[34] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[35] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.

k zabezpečení bojové a mobilizační pohotovosti, obranných příprav a plán rozvinutí ozbrojených sil České republiky.[36]

V příloze č. 6 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Ministerstva průmyslu a obchodu, mezi které patří např. informace dávající celkový přehled o rozmístění a kapacitách produktovodních tras pro dopravu pohonných hmot a ropy.[37]

V příloze č. 7 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Ministerstva spravedlnosti, do kterého mj. patří informace o totožnosti a podobě utajovaného svědka, způsob zajištění jeho ochrany a informace vztahující se k zajištění zvláštní ochrany a pomoci svědkovi a dalším osobám v souvislosti s trestním řízením nebo informace o přípravě prezidenta republiky o amnestii. [38]

V příloze č. 8 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Ministerstva vnitra, na základě kterého lze za UI považovat např. bezpečnostní opatření směřující k ochraně a bezpečnosti jednotlivce. [39]

V příloze č. 9 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Ministerstva zahraničních věcí, mezi které patří např. informace o obsahu diplomatické a kurýrní zásilky. [40]

V příloze č. 10 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Ministerstva zemědělství, do kterého mj. patří údaje o strategických zásobách zemědělských komodit a potravin. [41]

V příloze č. 11 Nařízení stanoví seznam utajovaných informací v oblasti působnosti České národní banky, do kterého patří také speciální charakteristiky a receptury materiálů používaných při výrobě bankovek. [42]

[36] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[37] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[38] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[39] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[40] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[41] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[42] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.

V příloze č. 12 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Českého telekomunikačního úřadu, ve kterém jsou jako UI uvedeny pouze radiové kmitočty určené pro obranu a bezpečnost státu a jejich seznamy. [43]

V příloze č. 13 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Kanceláře prezidenta republiky, ve kterém je jako UI klasifikován mj. i komplexní systém zabezpečení Českých korunovačních klenotů.[44]

V příloze č. 14 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Národního bezpečnostního úřadu, do kterého patří např. způsob zajištění fyzické bezpečnosti objektů, zabezpečených oblastí a jednacích oblastí, ve kterých jsou ukládány, zpracovávány nebo pravidelně projednávány utajované informace. [45]

V příloze č. 15 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Správy státních hmotných rezerv, na základě kterého se jako UI klasifikují souhrnná skladba položek hmotných rezerv a jejich minimální limity a orientační cílové stavy a dále souhrnné plány nákupu, prodejů a obměn materiálů hmotných rezerv. [46]

V příloze č. 16 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Státního úřadu pro jadernou bezpečnost, do kterého patří např. informace o návrhu způsobu a způsob zajištění fyzické ochrany jaderných materiálů.[47]

V příloze č. 17 Nařízení stanoví seznam utajovaných informací v oblasti působnosti Úřadu vlády České republiky, do kterého mj. patří informace o analýze rizik a hrozeb týkajících se bezpečnosti České republiky. [48]

V příloze č. 18 Nařízení stanoví seznam utajovaných informací v oblasti působnosti zpravodajských služeb České republiky, do kterého patří např. formy, metody, zásady a směrnice pro zpravodajskou činnost.[49]

V každém ze seznamů je vždy uvedeno pořadové číslo, definice informace, která má být utajována a rozmezí stupně jejího utajení. Příklad seznamu viz příloha III. [50]

---

[43] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[44] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[45] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[46] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[47] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[48] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
49 ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
[50] ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.

V §2 Nařízení je uvedeno, že původce klasifikuje UI v takovém rozsahu stupňů utajení, který je vždy uveden u konkrétních informací v jeho jednotlivých přílohách. Jako nejnižší stupeň je zde uváděn stupeň V (vyhrazené). Je však nutné zmínit, že i informace, která je uvedena v některé z příloh Nařízení, nemusí být takového charakteru, aby musela být klasifikována jako utajovaná.

Při posuzování, zda je nutné informaci utajovat, musí původce uvážit, zda by v případě vyzrazení či zneužití této informace mohla vzniknout újma zájmu České republiky nebo by mohlo být pro zájem České republiky nevýhodné. Újma zájmu České republiky a nevýhodnost pro zájmy České republiky jsou specifikovány v § 3 zákona.

3.3 Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků (dále jen vyhláška o fyzické bezpečnosti) stanoví bodové ohodnocení jednotlivých opatření fyzické bezpečnosti a jednacích oblastí, dále uvádí základní metodu hodnocení rizik, definuje další požadavky na opatření, která jsou nezbytná v rámci fyzické bezpečnosti a stanoví náležitosti certifikace technických prostředků.[51]

Vymezení základních pojmů (§ 2)

- **Objekt =** budova nebo jiný ohraničený prostor, ve kterém se zpravidla nacházejí zabezpečené nebo jednací oblasti;
- **Hranice objektu =** plášť budovy, fyzická bariéra (oplocení) nebo jinak viditelně vymezená hranice;
- **Hranice zabezpečené oblasti nebo jednací oblasti** = stavebně nebo jinak viditelně ohraničený prostor;
- **Vstup do objektu, zabezpečené oblasti nebo jednací oblasti** = místo určené pro vstup a výstup osob a místo určené pro vjezd a výjezd dopravních prostředků;
- **Dopravní prostředky** = pozemní, podzemní, vzdušné a vodní prostředky určené k přepravě osob, předmětů a materiálu;
- **Hrozba =** možnost vyzrazení nebo zneužití utajované informace při narušení fyzické bezpečnosti;

[51] ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-528>.

- **Riziko =** pravděpodobnost, že se určitá hrozba uskuteční;
- **Mimořádná situace** = stav, kdy bezprostředně hrozí, že dojde k vyzrazení nebo zneužití utajované informace;
- **Technický prostředek** = bezpečnostní prvek, jehož použitím se zabraňuje, ztěžuje, oznamuje nebo zaznamenává narušení zabezpečení ochrany objektu, zabezpečené oblasti nebo jednací oblasti, a dále ničí utajované informace;
- **Úschovný objekt =** trezor nebo jiná uzamykatelná schránka stanovená v příloze č. 1 vyhlášky o fyzické bezpečnosti;
- **Technické zařízení** = vojenský materiál, zejména elektronická, fototechnická, chemická, fyzikálně-chemická, radiotechnická, optická a mechanická vojenská technika a vojenská výzbroj, který obsahuje utajovanou informaci.

Zabezpečení objektu a zabezpečené oblasti (§ 3)

Vyhláška o fyzické bezpečnosti stanoví, že hranici objektu nebo zabezpečené oblasti, zařazení objektu nebo zabezpečené oblasti do příslušné kategorie a zařazení zabezpečené oblasti do příslušné třídy stanoví odpovědná osoba nebo jí pověřená osoba. Dále vyhláška určí technické prostředky, kterými je třeba objekt zabezpečit v závislosti na příslušné kategorii, hranicích a vyhodnocení rizik. Užití technických prostředků není pro zabezpečení objektu shodné s užitím technických prostředků k zabezpečení zabezpečené oblasti. Zabezpečená oblast je zabezpečována v závislosti na její kategorii, třídě a vyhodnocení rizik. K zabezpečení lze použít certifikované i necertifikované technické prostředky, avšak necertifikované technické prostředky lze použít pouze v případech, které jsou vyjmenovány v příloze č. 1 vyhlášky o fyzické bezpečnosti.[52]

Užití technických prostředků sloužících k zabezpečení objektu

a) pro kategorii Vyhrazené – mechanické zábranné prostředky;
b) pro kategorii Důvěrné a Tajné – mechanické zábranné prostředky a zařízení elektrické zabezpečovací signalizace;

[52] ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-528>.

c) pro kategorii Přísně tajné – mechanické zábranné prostředky, zařízení elektrické zabezpečovací signalizace a speciální televizní systémy. Speciální televizní systémy nesmí narušit ochranu utajovaných informací.

Užití technických prostředků sloužících k zabezpečení zabezpečené oblasti

a) pro kategorii Vyhrazené – mechanické zábranné prostředky;
b) pro kategorii Důvěrné – mechanické zábranné prostředky a zařízení elektrické zabezpečovací signalizace;
c) pro kategorii Tajné a Přísně tajné – mechanické zábranné prostředky, systémy pro kontrolu vstupů, zařízení elektrické zabezpečovací signalizace, speciální televizní systémy, zařízení elektrické požární signalizace. Speciální televizní systémy lze nahradit tísňovými systémy.[53]

V takovém případě, že je hranice objektu shodná s hranicí zabezpečené oblasti, jsou míra a podmínky použití opatření fyzické bezpečnosti určeny požadavky na kategorii dané zabezpečené oblasti.

Zabezpečení jednacích oblastí (§ 4)

Stejně jako v případě zabezpečení objektu nebo zabezpečené oblasti i u jednací oblasti stanoví její hranice osoba pověřená nebo osoba jí pověřená a k zabezpečení lze použít certifikované i necertifikované technické prostředky, avšak necertifikované technické prostředky lze použít pouze v případech, které jsou vyjmenovány v příloze č. 1 vyhlášky o fyzické bezpečnosti.

Zabezpečení technického zařízení (§ 5)

Rozsah použití režimových opatření a technických prostředků k zabezpečení technického zařízení stanoví odpovědná osoba nebo jí pověřená osoba na základě vyhodnocení rizik. Rozsah užití opatření fyzické bezpečnosti k zabezpečení technického zařízení se stanoví v projektu fyzické bezpečnosti. Obsah a forma projektu fyzické bezpečnosti se dle vyhlášky o fyzické bezpečnosti využije **přiměřeně**. Vyhláška

[53] ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-528>.

dále stanoví náležitosti žádosti o certifikaci technického prostředku a dobu platnosti certifikátu.[54]

Režimová opatření (§ 6)

Režimová opatření stanoví, oprávnění osob a dopravních prostředků pro vstup do objektu (§ 7), oprávnění osob pro vstup do zabezpečené oblasti a jednací oblasti a způsob kontroly výše uvedených oprávnění. Za pomoci režimových opatření lze dále regulovat kontrolu osob při vstupu nebo výstupu do / z objektu, zabezpečených oblastí a jednacích oblastí, klíčový režim (§ 8), režim pohybu UI v objektu nebo režim manipulace s technickými prostředky. [55]

Ostraha (§ 9)

Vyhláška o fyzické bezpečnosti ve své příloze č. 1 stanoví bodové hodnoty jednotlivých typů ostrah u objektů.

Ověřování opatření fyzické bezpečnosti a vyhodnocení rizik (§ 10)

Prověřit, zda jednotlivá použitá opatření fyzické bezpečnosti a vyhodnocení rizik odpovídají projektu fyzické bezpečnosti a právním předpisům v oblasti ochrany utajovaných informací, by měla odpovědná osoba nebo jí pověřená osoba průběžně, minimálně však každých 12 měsíců.

Vyhodnocení rizik se provádí

a) identifikací stupňů utajovaných informací a zjištěním množství utajovaných informací, které se v objektu vyskytují nebo budou vyskytovat, zejména z hlediska následku jejich vyzrazení nebo zneužití;
b) popisem a vyhodnocením hrozeb, kterým jsou tyto utajované informace vystaveny;
c) popisem a vyhodnocením zranitelnosti utajovaných informací vůči těmto hrozbám;

[54] ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-528.
[55] ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-528>.

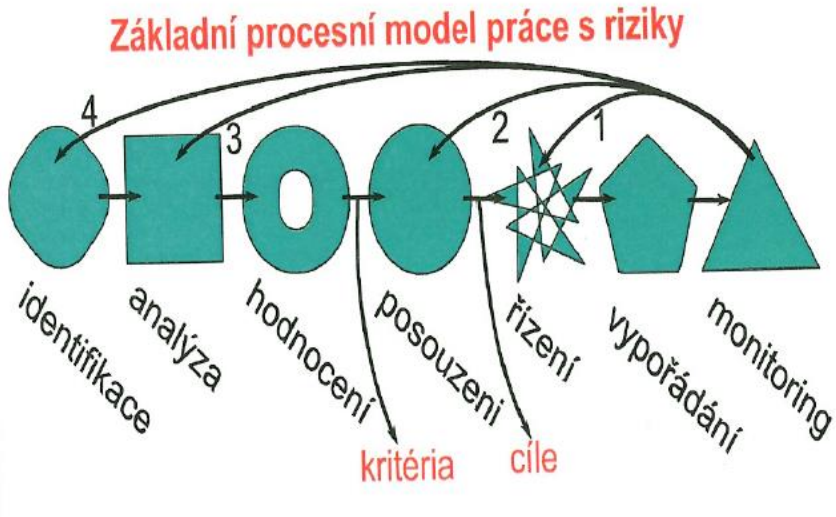
d) stanovením míry rizika, jako "malé", "střední" nebo "velké", na základě vyhodnocení hrozeb a zranitelnosti utajovaných informací.[56]

[56] ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-528>.

4 ANALÝZA RIZIK

Proces řízení rizik probíhá zpravidla ve třech etapách. První etapu nazýváme jako **analýzu rizik**, po které následuje **vyhodnocení rizik** a tato etapa je završena třetí etapou – **zvládáním rizik**.[57]

Obrázek 1: Procesní model práce s riziky dle práce[58]



„Kritéria jsou podmínky, které stanovují, kdy je riziko přijatelné, podmíněně přijatelné či nepřijatelné. Cíle jsou formulace, které vyznačují: mez, na kterou chceme snížit riziko; míru bezpečí systému; či míru bezpečí systému a jeho okolí. Šipky (1, 2, 3 a 4) označují zpětné vazby, které se uplatňují, když riziko je nepřijatelné.“[59]

Obecně lze říci, že zvládání rizik vyžaduje, abychom dokázali brát v úvahu události, které se staly v minulosti, a zároveň jsme očekávali události, které teprve nastanou nebo by za jistých podmínek mohly nastat v budoucnosti.[60]

Analýza rizik by měla probíhat pravidelně nebo při jakékoliv stavební, organizační, či jiné větší změně, která by mohla zapříčinit vznik nových hrozeb. V rámci fyzické a personální bezpečnosti UI lze v této souvislosti hovořit i o takových personálních změnách, které způsobí přístup nových zaměstnanců do oblasti, ve které se nachází UI, neboť i právě tito zaměstnanci mohou být pro UI potenciální hrozbou.

[57] ČERMÁK, M. *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009, s. 17.
[58] PROCHÁZKOVÁ, D. *Krizové řízení pro technické obory*. V Praze: České vysoké učení technické, 2013, s. 37.
[59] PROCHÁZKOVÁ, D. *Krizové řízení pro technické obory*. V Praze: České vysoké učení technické, 2013, s. 37.
[60] PROCHÁZKOVÁ, D. *Rizika spojená s pohromami a inženýrské postupy pro jejich zvládání*. V Praze: České vysoké učení technické, Fakulta dopravní, Ústav bezpečnostních technologií a inženýrství, 2013, s. 208.

4.1 Definice základních pojmů

Základními pojmy v rámci analýzy rizik a fyzické bezpečnosti UI se pro účely práce rozumí:

- **Chráněné zájmy** lidského systému jsou komponenty, vazby a toky v lidském systému, které jsou nutné pro jeho bezpečí a udržitelný rozvoj.[61] Mezi chráněné zájmy lze řadit i UI, neboť by jejich zneužití či vyzrazení mohlo mít přímý účinek nejen na bezpečí, ale také na udržitelný rozvoj lidského systému;
- **Škoda** je újma na životě, zdraví a bezpečí lidí, majetku, veřejném blahu, životním prostředí, infrastruktuře a technologiích, kterou je možné vyjádřit v penězích[62];
- **Zranitelnost** je náchylnost chráněného zájmu ke vzniku škod[63];
- **Dopad** je nepříznivý účinek jevu v daném místě a čase na veškeré chráněné zájmy[64];
- **Pohroma** je jev, který vede nebo za jistých podmínek může vést k nepřijatelnému dopadu na chráněných zájmech[65];
- **Ohrožení** danou pohromou je soubor maximálních dopadů pohromy, kterou lze očekávat v daném čase za specifikovaný časový interval s pravděpodobností, která je rovna stanovené hodnotě[66];
- **Riziko** je míra nepřijatelných dopadů způsobených pohromou o velikosti, jenž je rovna hodnotě ohrožení[67];
- **Bezpečnostní riziko** vyjadřuje výši pravděpodobnosti, že dojde k naplnění konkrétní bezpečnostní hrozby v takovém rozsahu, že požadavky na řešení vzniklé krize přesáhnou možnosti bezpečnostního systému a možné škody s tím spojené budou neakceptované.[68]

[61] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. V Praze: České vysoké učení technické, 2011, s. 96.
[62] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. V Praze: České vysoké učení technické, 2011, s. 97.
[63] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. V Praze: České vysoké učení technické, 2011, s. 97.
[64] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. V Praze: České vysoké učení technické, 2011, s. 97.
[65] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. V Praze: České vysoké učení technické, 2011, s. 97.
[66] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. V Praze: České vysoké učení technické, 2011, s. 98.
[67] PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. V Praze: České vysoké učení technické, 2011, s. 98.
[68] ANTUŠÁK, E. *Krizový management: hrozby – krize – příležitosti*. Praha: Wolters Kluwer Česká republika, 2009, s. 180.

4.2 Popis objektu

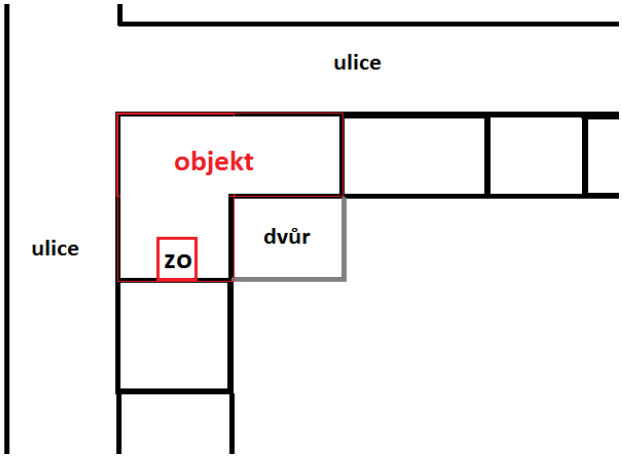
Objektem se rozumí celá budova na adrese XXXX, Praha 10. Hranicí objektu jsou obvodové zdi budovy. K budově přiléhá dvůr, který je oddělen od okolních pozemků fyzickou zděnou bariérou, která je vysoká cca 3 metry. Objekt je typu 2 dle přílohy č. 1 k vyhlášce o fyzické bezpečnosti.[69] Jedná se o rohovou budovu, která se nalézá na rozhraní ulic XX a XX.

Budova má 4 nadzemní a 1 podzemní podlaží, sedlovou střechu a stavebně je provedena jako cihlový masiv tloušťky 60 cm. Stropy a podlahy jsou z masivních dřevěných trámů.

V budově jsou 2 vstupy z ul. XX a 2 vstupy ze dvora. Dvůr je přístupný pouze z budovy. Okna jsou v minimální výšce cca 1 metr nad úrovní chodníku. Všechna okna jsou zajištěna kovovou mříží.

Zabezpečenou oblastí (dále jen ZO), ve smyslu zákona, je prostor objektu v přízemním podlaží. Zabezpečená oblast je kategorie VYHRAZENÉ typu 0. dle vyhlášky o fyzické bezpečnosti. Hranicí ZO jsou zdi oddělující ZO od ostatních prostor objektu. ZO má strop z masivních dřevěných trámů a betonovou podlahu. Zdi jsou z cihel o síle cca 20 cm a představují vnější plášť ZO.

Obrázek 2: Schématické umístění objektu a ZO v prostoru[70]



[69] ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-528>.
[70] Vlastní zdroj

4.3 Volba metody

K tomu, abychom byli schopni rizika kvalifikovaně odhalovat a definovat, je třeba na ně nahlížet v souvislostech v rámci systému, ve kterém rizika hodnotíme. Pro účely práce se tímto systémem rozumí objekt, ve kterém je třeba provést analýzu rizik pro účely následného stanovení a aplikace režimových opatření. Na základě dobré znalosti systému je třeba následně zvolit metodu, která bude aplikována pro analýzu rizik. Některé systémy (budovy) mohou být z hlediska analýzy rizik natolik rozsáhlé a komplikované, že bude třeba využít kombinaci několika z níže uvedených metod.

Základní metody pro stanovení rizik dle práce[71] jsou:

1) **Check List** (kontrolní seznam) je založen na systematické kontrole opatření, která jsou předem stanovena. [72]
2) **Safety Audit** (bezpečnostní kontrola) je taková kontrola, při níž dochází k vyhledávání rizikových situací a na jejich základě se následně navrhují opatření, která povedou ke zvýšení bezpečnosti. Tato metoda je založena na cíleném vyhledávání potenciálních rizikových situací a jejich následném zapracování do bezpečnostní dokumentace. V rámci bezpečnostní kontroly by měly probíhat rozhovory se zaměstnanci zaměřené na odhalení možného rizika spojeného s jejich pracovní činností. Následně by mělo dojít k vyhodnocení všech rozhovorů jako celku a vyvození potřebných závěrů.
3) **What – If Analysis** (analýza toho, co se stane, když) je postupem, který slouží k detekci dopadů konkrétní situace v daném systému. Pro příklad lze zmínit výrobní linku, u které bude třeba zjistit následky výpadku elektrického proudu. Základní otázka bude tedy znít: „Jaké jsou veškeré možné dopady, které bude výpadek proudu ve vztahu k výrobní lince mít?“.
4) **Prelimitary Hazard Analysis** – PHA (předběžná analýza ohrožení nebo úvodní analýza ohrožení) je postup, který slouží k vyhledávání nouzových situací, jejich možných příčin a dopadů a k jejich následnému rozřazení do předem stanovených kategorií. O předběžné analýze ohrožení lze konstatovat, že je složením několika různých technik posuzování.
5) **Process Quantitative Risk Analysis** – QRA (analýza kvantitativních rizik procesu) je uceleným postupem ke kvantifikování možných rizik. Při užití této

[71] PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. V Praze: České vysoké učení technické, 2011, s. 221-222.
[72] Vzhledem k faktu, že tato metoda bude v práci použita, bude podrobněji popsána níže v práci.

metody se postupuje dle procesního modelu práce s riziky, který je uveden na str. 34 této práce. Pro správné provedení metody je zapotřebí propracované databáze a počítačové podpory.

6) **Hazard Operation Process** – HAZOP (analýza ohrožení a provozuschopnosti) využívá pravděpodobnostního ohodnocení ohrožení a z něj plynoucích rizik. Výsledek této metody závisí především na tom, zda uvážíme vnitřní i vnější zdroje rizik, či se omezíme pouze na jedna z nich. Výsledkem analýzy ohrožení a provozuschopnosti by měla být doporučení, která povedou ke zdokonalení procesu.
7) **Event Tree Analysis** – ETA (analýza stromu událostí) je postupem, který sleduje vývoj procesu od jeho samotného počátku na základě dvou možností – příznivé a nepříznivé. Tuto metodu lze považovat za spojení metody statistické a grafické. Podoba systémového stromu má podobu rozvětveného grafu s předem dohodnutou symbolikou.
8) **Failure Mode and Effect Anylysis** – FMEA (analýza poruch a jejich dopadů) je postup, který je založený na analýze způsobu vzniku poruch a jejich možných důsledků. Cílem FMEA je vytvoření doporučení pro zvýšení spolehlivosti systému a s tím spojené zvýšení bezpečnosti.
9) **Fault Tree Analysis** – FTA (analýza stromu poruch) je metoda, která využívá zpětný rozbor událostí za použití řetězce příčin. Na základě získaných faktů se dále odhalují možné řetězce událostí, které vedou ke konkrétní poruše.
10) **Human Reliability Analysis** – HRA (analýza lidské spolehlivosti) je postup, kterým se odhaluje vliv lidského faktoru na vznik pohrom. Metoda analýzy lidské společnosti posuzuje především vliv a míru spolehlivosti a chybovosti lidského faktoru ve sledovaném systému.
11) **Fuzzy Set Method** (metoda fuzzy logiky a verbálních výroků FL-VV) je multikriteriální metodou, která je založena na simulaci procesních modelů.
12) **Relative Ranking** – RR (relativní klasifikace (RR) je strategií, která umožňuje porovnání vlastností několika procesů či činností a následné určení, zda jsou tyto procesy a činnosti nebezpečné do takové míry, že to analytiky opravňuje k dalšímu zkoumání. Z hlediska řízení rizik se jedná o metodu, která porovnává rizika projektů, procesů či zařízení a snaží se zjistit, která kombinace způsobu aplikace těchto projektů, procesů a zařízení je nejvíce bezpečná.
13) **Causes and Consequences Analysis** – CCA (analýza příčin a dopadů) je kombinací metody analýzy stromu poruch a analýzy stromu událostí.

14) **Metoda PSA** (Probabilistic Safety Assessment) stanovuje podíl jednotlivých zranitelných částí systému na jeho celkovou zranitelnost. Tato metoda se používá např. k modelování možných scénářů hypotetických jaderných havárií nebo k modelování chemických havárií. Metoda PSA je specifická tím, že rizika od existujících pohrom řadí dle závažnosti jejich dopadů a tím umožňuje soustředění pozornosti na nejvíce nebezpečné pohromy.

Check List (kontrolní seznam)

Kontrolní seznam je metoda, která je založena na systematické kontrole plnění předem stanovených podmínek. Kontrolní seznam není soubor nahodilých otázek, ale odpovídá procesnímu modelu systému, ve kterém probíhají sledované činnosti. Kontrolní seznamy jsou užitečné pro identifikaci dopadů a zajišťují, že žádné ze stanovených podmínek nejsou přehlédnuty. Výhodou této metody je, že se aplikuje jednoduše a může být použita v jakémkoliv stádiu procesu.[73]

Analýza rizik pomocí kontrolního seznamu se skládá ze dvou základních kroků. Prvním z nich je vytvoření kontrolního seznamu či kontrolních otázek, které jsou v rámci hodnoceného systému relevantní. Druhým krokem je sestavení hodnotového systému, dle kterého se následně budou získané výsledky hodnotit. Volba hodnotového systému se pro různé cíle liší a je třeba brát zde v úvahu stav, jehož chceme za pomoci kontrolního seznamu dosáhnout.

Kontrolní seznamy mají buď formu tabulek, ve kterých v prvním sloupci jsou otázky a v dalších sloupcích jsou následně místa pro odpovědi na otázky nebo mají strukturu po sobě jsoucích otázek. Podstatný je způsob hodnocení, který musí být zvolen adekvátně hodnocenému systému a přizpůsobený dané situaci. S ohledem na cíl hodnocení, není tudíž systém klasifikace odpovědí vždy stejný. Skládá-li se hodnocení bezpečnosti vybraného úseku z několika kontrolních seznamů, mají podle situace všechny buď stejnou váhu, nebo mají váhu rozdílnou. Hodnotové systémy, kdy odpovědi na všechny otázky mají stejnou váhu, jsou těmi nejjednoduššími, ostatní vyžadují vytvoření klasifikačních stupnic speciálními metodami matematické statistiky, teorie mlhavých množin či systémového inženýrství.[74]

[73] PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. V Praze: České vysoké učení technické, 2011, s. 222.
[74] PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. V Praze: České vysoké učení technické, 2011, s. 223.

4.4 Hodnotící stupnice a seznam otázek

4.4.1 Hodnotící stupnice

V odborné literatuře se často používá dále uvedená stupnice hodnocení: [75]

1) 95% odpovědí ANO – Stav hodnoceného systému je podle kontrolního systému vynikající;
2) 70% – 95% odpovědí ANO – Stav hodnoceného systému je podle kontrolního systému uspokojivý;
3) 45% – 70% odpovědí ANO – Stav hodnoceného systému je podle kontrolního systému dobrý;
4) 20% – 45% odpovědí ANO – Stav hodnoceného systému je podle kontrolního systému špatný;
5) 5% – 25% odpovědí ANO – Stav hodnoceného systému je podle kontrolního systému velmi špatný;
6) 0% – 5% odpovědí ANO – Stav hodnoceného systému je podle kontrolního systému katastrofální.

Pro potřeby práce bude využita níže uvedená stupnice.

1) **9x** odpověď ANO – **vynikající** stav hodnoceného systému;
2) **8x** odpověď ANO – **uspokojivý** stav hodnoceného systému;
3) **6x-7x** odpověď ANO – **dobrý** stav hodnoceného systému;
4) **4x-5x** odpověď ANO – **špatný** stav hodnoceného systému;
5) **2x-3x** odpověď ANO – **velmi špatný** stav hodnoceného systému;
6) **0x -1x** odpověď ANO – **katastrofální** stav hodnoceného systému.

4.4.2 Seznam otázek

Pro to, aby byla analýza rizik provedena kvalitně a její výsledky mohly být považovány za relevantní, je důležitá dobrá znalost hodnoceného systému (v tomto případě objektu). Pokud by docházelo k hodnocení objektu bez důkladného prostudování stavební dokumentace, umístění objektu v prostoru, personálních a jiných podmínek, byly by výsledky analýzy zkreslené a následně použitá opatření by neměla žádoucí

[75] PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. V Praze: České vysoké učení technické, 2011, s. 224-225.

účinek. Seznam otázek, který je součástí kontrolního listu, musí obsáhnout veškeré oblasti, které by pro daný objekt mohly za jistých podmínek představovat bezpečnostní riziko. Pro příklad lze zmínit např. nezabezpečení oken mřížemi, nedostatečné nebo nefunkční zabezpečení elektronickým zabezpečovacím systémem, nepřítomnost kamerového systému, nedostatky v klíčovém režimu atd.

Výhodu při tvorbě takového kontrolního listu mají ti bezpečnostní pracovníci, kteří mají možnost v daném objektu pobývat delší časový úsek a mohou tak odhalovat možnost vzniku rizik při různých situacích (výpadek elektrického proudu atp.). Na druhou stranu je třeba, aby ten, kdo analýzu rizik provádí, byl schopen jednat za každé situace profesionálně a neupravoval znění otázek či odpovědí tak, aby nepoškodil např. svého nadřízeného nebo sám sebe. I taková analýza by postrádala veškerý smysl a veškerá opatření, která by na ní byla vystavěna, by byla zcela neúčinná.

Otázky kontrolního listu by měly být formulovány tak, aby nebyly zavádějící a byly srozumitelné i pro člověka, který hodnocený objekt nenavštívil.

Znění otázek kontrolního listu pro účely práce je následující:

1) Je objekt zabezpečen elektronickou zabezpečovací signalizací?
2) Je objekt zajištěn monitorovacím kamerovým systémem?
3) Je prováděna kontrola osob při příchodu do objektu?
4) Je prováděna kontrola osob při východu z objektu?
5) Je prakticky vyloučeno, aby se k utajované informaci v rámci hodnoceného objektu dostala osoba, která není oprávněná se s utajovanou informací seznamovat?
6) Jsou utajované informace vždy řádně uchovávány v úschovném objektu, který je k tomuto určen?
7) Je vstup do zabezpečené oblasti řádně zajištěn?
8) Chybí v zabezpečené oblasti okno, kterým by bylo možné utajovanou informaci nepozorovaně vynést ven z objektu?
9) Je úklid zabezpečené oblasti prováděn pod oprávněným dohledem?
10) Je určen postup, který má být zaměstnanci dodržován při zjištění nepatřičného chování zaměstnance či návštěvy v souvislosti s utajovanými informacemi?

4.5 Zaznamenání výsledků

Tabulka 1: Zaznamenání výsledků kontrolního listu[76]

číslo a znění otázky	ANO	NE
1. Je objekt zabezpečen elektronickou zabezpečovací signalizací?	**X**	
2. Je objekt zajištěn monitorovacím kamerovým systémem?	**X**	
3. Je prováděna důkladná kontrola osob při příchodu do objektu?		**X**
4. Je prováděna důkladná kontrola osob při východu z objektu?		**X**
5. Je prakticky vyloučeno, aby se k utajované informaci v rámci hodnoceného objektu dostala osoba, která není oprávněná se s utajovanou informací seznamovat?	**X**	
6. Jsou utajované informace vždy řádně uchovávány v úschovném objektu, který je k tomuto určen?	**X**	
7. Je vstup do zabezpečené oblasti řádně zajištěn?	**X**	
8. Chybí v zabezpečené oblasti okno, kterým by bylo možné utajovanou informaci nepozorovaně vynést ven z objektu?	**X**	
9. Je úklid zabezpečené oblasti prováděn pod oprávněným dohledem?	**X**	
10. Je určen postup, který má být zaměstnanci dodržován při zjištění nepatřičného chování zaměstnance či návštěvy v souvislosti s utajovanými informacemi?		**X**

4.6 Vyhodnocení výsledků

Na základě získaných výsledků lze stav hodnoceného systému (objektu) považovat za dobrý. Přestože bylo dosaženo horní hranice odpovědí pro tento stav, nelze tuto skutečnost považovat z hlediska ochrany UI za uspokojivou a je tedy třeba promítnout tento fakt do režimových opatření, která do jisté míry mohou tento stav pozitivně ovlivnit.

[76] Vlastní zdroj

5 REŽIMOVÁ OPATŘENÍ

5.1 Obecná definice

„Při ochraně prostor, v nichž se nachází zařízení pro zpracování informací, musí organizace používat bezpečnostní perimetry. Pod pojmem bezpečnostní perimetr se rozumí prostor chráněny řadou fyzických bariér. Např. bránou, zdmi, vstupním turniketem, čipovou kartou, recepcí, bezpečnostní službou.“[77]

Režimová opatření, jak je již výše uvedeno, stanoví oprávnění osob a dopravních prostředků pro vstup do objektu, oprávnění osob pro vstup do zabezpečené oblasti a jednací oblasti a způsob kontroly těchto oprávnění. Dále určí kontrolní opatření při vstupu do objektu, zabezpečených a jednacích oblastí a způsob kontroly těchto opatření. Režimová opatření upraví také klíčový režim, režim manipulace s technickými prostředky a v neposlední řadě režim pohybu utajovaných informací v objektu, zabezpečené oblasti a jednací oblasti.[78]

Vzhledem k charakteru posuzovaného objektu budou jeho název, umístění a jména oddělení, která se v tomto objektu nachází, anonymizovány.

5.2 Návrh režimových opatření

Úvodní ustanovení

Tímto předpisem se stanoví režimová opatření k užívání a ochraně objektu v ul. XX (dále jen „objekt“).

Zaměstnancům a osobám vstupujícím a pohybujícím se v objektu vydáním tohoto předpisu vzniká povinnost dodržovat stanovená režimová opatření.

Vymezení pojmů

Pro účely tohoto předpisu se rozumí

a) zaměstnancem celník nebo občanský zaměstnanec Celní správy České republiky (dále jen „celní správa“);
b) návštěvou osoba, která není zaměstnancem celní správy;

[77] DRASTICH, M. *Systém managementu bezpečnosti informací*. Praha: Grada, 2011, s. 46.
[78] ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-528>.

c) zodpovědnou osobou je vedoucí odd. 000, v jeho nepřítomnosti pověřený pracovník;
d) ostrahou celníci Celního úřadu pro hlavní město Prahu, oddělení Ostrahy objektů, zařazení k výkonu asistenčních činností při ochraně areálu GŘC, vykonávající činnosti ostrahy areálu GŘC;
e) ochranou opatření související se zajištěním bezpečnosti objektu, zejména před vniknutím a pohybem nepovolaných osob, provádění režimových opatření k zabránění vzniku škody na majetku;
f) režimovým opatřením soubor povinností, opatření a činností, mající vztah k užívání a ochraně objektu a týkající se jak zaměstnanců celní správy, tak i návštěv;
g) zabezpečenou oblastí je ohraničený prostor objektu (dále jen „ZO“);
h) provozovatelem IS/V objektu odd. 000;
i) zaměstnancem konajícím nařízenou služební pohotovost určený zaměstnanec zařazený s místem výkonu služby v objektu, který má v pracovních dnech v čase od 15.45 hodin do 7.45 hodin povinnost se v případě poplachu nebo jiné závažné situace z čl. 4 odst. 3 tohoto rozkazu dostavit do objektu a vzniklou situaci příslušně řešit. Ve dnech pracovního volna a pracovního klidu je tato doba stanovena od 00.00 hodin do 24.00 hodin;
j) zabezpečovací technikou technické prostředky a zařízení v systému ochrany objektu, využívané nebo používané ostrahou při výkonu služby, a to zejména

    1) pult centralizované ochrany (dále jen „PCO“);
    2) elektronická zabezpečovací signalizace (dále jen „EZS“);
    3) monitorovací kamerový systém (dále jen „CCTV“);
    4) ruční detektor kovů;
    5) mechanický zábranný prostředek (rolovací mříž, mříže před okny).

Režim pohybu osob a materiálu v objektu

(1) Všichni zaměstnanci provádějící výkon služby v objektu jsou povinni při svém příchodu nebo odchodu zaznamenat svůj příchod nebo odchod do docházkové knihy v listinné podobě. Uvedená povinnost se vztahuje také na zaznamenání odchodů a příchodů v průběhu doby služby (např. přestávka na jídlo, návštěva lékaře, služební cesty atd.).

(2) Ostatní zaměstnanci a návštěvy jsou povinni při příchodu nebo odchodu z objektu budovy provést zápis do přiložené knihy návštěv. Za správnost zápisu odpovídá doprovod, který po celou dobu návštěvy tuto osobu doprovází.

(3) Návštěvy do objektu budou sekretariátem identifikovány přes videovrátník. Návštěvy se po jejich fyzickém vyzvednutí mohou po objektu pohybovat výhradně v doprovodu navštíveného zaměstnance.

(4) Navštívený zaměstnanec zodpovídá za pohyb návštěvy v objektu a je povinen ji po ukončení návštěvy buďto doprovodit zpět k ostraze, či k další navštívené osobě, a to osobně nebo jím pověřeným zaměstnancem.

(5) Do objektu je zakázán vstup s nepovolenými předměty, jakými jsou například střelné zbraně, nože, s výjimkou kapesních nožů s délkou čepele do 10 cm, výbušniny, podezřelé chemikálie, případně i podezřelá elektronická zařízení. Tento zákaz se nevztahuje na zaměstnance celní správy, kteří vykonávají službu s přidělenou služební zbraní. Do objektu je zakázán vstup veškerých zvířat, krom služebních.

(6) Vstupují-li do budovy hromadné návštěvy (např. součinnost bezpečnostních sborů, prezentace celní správy, tiskové konference atp. a jedná-li se o 5 a více osob), je povinností organizátora tuto akci nahlásit vedoucímu odd. 000, případně sekretariátu.

(7) V případě vzniku jakýchkoliv podezřelých okolností, včetně vzniku konfliktních situací, jsou všichni zaměstnanci povinni kontaktovat vedoucího odd. 000, případně jím pověřenou osobu.

(8) Veškerá došlá korespondence určená pro zaměstnance objektu bude zkontrolována za pomoci RTG zařízení.

(9) Přijatá režimová opatření a způsob jejich použití pro ochranu utajovaných informací jsou stanovena a podrobně popsána v Projektu fyzické bezpečnosti objektu.

Provoz objektu

(1) Ostraha objektu je prováděna oddělením Ostrahy objektů CÚ pro hlavní město Praha (dále jen „ostraha“) s místem působiště areálu GŘC.

(2) Zabezpečení objektu je prováděno formou systému EZS, který je napojen na pult centralizované ochrany GŘC v režimu 24/7.

(3) V případě poplachu ostraha vyhodnotí vzniklou situaci a následně vyrozumí příslušníka vykonávajícího nařízenou služební pohotovost mimo pracoviště a v případě nutnosti kontaktuje PČR.

Postup při příchodu na pracoviště

(1) Každý zaměstnanec je povinen při příchodu do objektu prověřit, zda je zapnutý systém EZS. V případě, že systém EZS není zapnutý, vstoupí do objektu a zapíše se do docházkové knihy.
(2) V případě, že systém EZS je zapnutý, postupuje následujícím způsobem:

a) po vstupu do objektu deaktivuje systém EZS;
b) zapíše se do docházkové knihy.

(3) V případě chybné deaktivace systému EZS zaměstnanec neprodleně vyrozumí ostrahu.

Postup při opuštění pracoviště

(1) Každý zaměstnanec je povinen před odchodem ze svého pracoviště prověřit, zda jsou řádně uzavřena všechna okna, vypnuty veškeré elektrické spotřebiče a zařízení, která mimo pracovní dobu nemusí být v provozu a zda je zhasnuto osvětlení. Poté řádně uzavře a uzamkne dveře své kanceláře.
(2) Každý zaměstnanec je povinen po uzamčení svého pracoviště prověřit, zda je v budově poslední.

V případě, že není poslední, postupuje následujícím způsobem:

a) zapíše odchod do docházkové knihy,
b) aktivuje okruh systému EZS pro své pracoviště;
c) opustí objekt.

V případě, že je poslední, postupuje následujícím způsobem:

d) prověří, zda jsou ve společných prostorách řádně uzavřena všechna okna, vypnuty veškeré elektrické spotřebiče a zařízení, která mimo pracovní dobu nemusí být v provozu, a zda je zhasnuto osvětlení;
e) na panelu EZS prověří, zda jsou aktivovány všechny ostatní okruhy EZS;
f) zapíše odchod do docházkové knihy;

g) aktivuje EZS, opustí objekt a uzamkne vchodové dveře;

h) po uzavření automatických vchodových dveří vyčká na úplnou aktivaci EZS, která se projeví blikáním červené diody umístěné vedle kódovacího panelu u vchodových dveří a rolovací mříže.

Závěrečná ustanovení

(1) Zodpovědná osoba zabezpečí uložení generálního klíče, který umožňuje vstup do objektu, do zabezpečené schránky nebo zapečetěné obálky a zapečetí jej tak, aby při jeho použití došlo k nevratnému poškození pečeti. Schránka bude uložena u ostrahy GŘC. Schránkou se rozumí obálka nebo jakýkoliv jiný vhodný obal.

(2) Seznam zaměstnanců konajících nařízenou služební pohotovost v určitém měsíci bude odevzdáván ostraze vedoucím odd. 000 nebo jím pověřeným pracovníkem nejpozději k 25. dni měsíce předešlého.

(3) Úklid objektu bude zabezpečen smluvní externí firmou, která bude předmětné práce vykonávat v pracovních dnech od 7:00 – 9:00 a 14:00 – 16:00 hod., a to vždy v přítomnosti zaměstnance zařazeného s místem výkonu služby v objektu.

Účinnost

Tento předpis nabývá účinnosti dnem 1. června 2017 a pozbývá účinnosti 31. prosince 2019.

Seznam příloh

Příloha č. 1 – Klíčový režim
Příloha č. 2 – Zásahový režim
Příloha č. 3 – Režim pohybu osob a klíčový režim v zabezpečených oblastech

Příloha č. 1 – Klíčový režim

(1) Veškeré klíče od místností objektu musí být opatřeny přesným označením místnosti.

(2) Každý zaměstnanec, zařazený s místem výkonu práce nebo služby v objektu, má přidělen klíč od místnosti, ve které vykonává práci nebo službu, a to v kombinaci s klíčem od vchodových dveří.

(3) Generální klíč je přidělen generálnímu řediteli a bezpečnostnímu správci objektu.

(4) Provozní generální klíč je uložen u zaměstnance sekretariátu.

(5) Výdej a navrácení provozního generálního klíče je zaměstnancem sekretariátu zaznamenán do knihy klíčů.

(6) V případě ztráty, odcizení nebo poškození klíčů musí být o této skutečnosti neprodleně informován vedoucí odd. 000 a bezpečnostní správce objektu. Vedoucí odd. 000 rozhodne, dle povahy případu, o přijetí odpovídajících opatření.

(7) V odůvodněných případech (např. zapomenutí klíče zaměstnancem nebo nepřítomnost zaměstnance) může zaměstnanec sekretariátu na žádost zaměstnance nebo jeho nadřízeného provést otevření místnosti. Za zabezpečení místnosti po jejím otevření zodpovídá zaměstnanec, který si vyžádal její otevření. Po skončení pracovní doby provede příslušný služební funkcionář nebo jím určený zaměstnanec uzamčení místnosti.

(8) Výrobu duplikátů klíčů a výměnu zámků zajišťuje příslušný útvar GŘC pouze na žádost vedoucího odd. 000 nebo jím pověřeného zaměstnance.

(9) Je nepřípustné po dobu nepřítomnosti ponechávat klíče od místností v zámcích z vnější strany. Všechny místnosti v budově musí být po dobu nepřítomnosti příslušného zaměstnance řádně uzamčeny a klíče uschovány.

(10) Každý zaměstnanec je povinen po skončení pracovní doby řádně uložit pracovní dokumenty, tiskopisy a svěřené pracovní pomůcky v místnosti a tuto řádně uzamknout.

(11) Úklid místností zabezpečených oblastí se provádí smluvní externí firmou, která bude předmětné práce vykonávat v pracovních dnech od 7:00 – 9:00 a 14:00 – 16:00 hod., a to vždy v přítomnosti oprávněného zaměstnance zařazeného s místem výkonu služby v objektu.

Příloha č. 2 – Zásahový režim

(1) V případě vzniku mimořádné situace (např. násilné vniknutí, poškození objektu) a dále v případě vyhlášení poplachového signálu prostřednictvím EZS ostraha objektu GŘC neprodleně kontaktuje zaměstnance konajícího nařízenou služební pohotovost na jeho mobilní telefon. Pokud to bude situace vyžadovat, ostraha objektu GŘC kontaktuje i PČR.

(2) Obhlídku prostor provádí zaměstnanec konající nařízenou služební pohotovost, který se v nejkratším možném čase od oznámení mimořádné situace dostaví k objektu. Po příjezdu k objektu zaměstnanec provede obhlídku vnějšího perimetru, aby zjistil, zda došlo k narušení vstupů do objektu. V rámci této činnosti postupuje zaměstnanec v úzké součinnosti s ostrahou objektu GŘC.

(3) Při identifikaci podezření ze spáchání trestného činu ostraha přivolá neodkladně PČR a o situaci neprodleně informuje Operační centrum GŘC, vedoucího odd. 000 a ředitele bezpečnostního odboru.

(4) Při vzniku požáru nebo živelní pohromy nebo kalamitní situace ostraha přivolá neodkladně Hasičský záchranný sbor, a dojde-li ke zranění osob, rovněž zdravotnickou záchrannou službu, případně PČR, a o situaci neprodleně informuje Operační centrum GŘC, vedoucího odd. 000 a ředitele bezpečnostního odboru.

(5) V případě vzniku poruchy a přerušení (výpadku) dodávek na energiích (elektrická energie, plyn), dále v případě poruchy na vodovodním řádu ostraha v pracovní době neprodleně informuje externí servisní firmu, v mimopracovní době pak havarijní dispečink této společnosti.

(6) Vznikne-li porucha na EZS, ostraha neprodleně informuje vedoucího odd. 000. Jedná-li se o poruchu EZS v zabezpečených oblastech, uvědomí ostraha neprodleně o této skutečnosti také ředitele bezpečnostního odboru nebo jím stanoveného zaměstnance.

Příloha č. 3 – Režim pohybu osob a klíčový režim v zabezpečených oblastech

(1) Do zabezpečené oblasti (dále jen „ZO s IS/V“) v objektu mohou vstupovat pouze zaměstnanci, kteří k tomu jsou pověřeni bezpečnostním správcem IS/V.

(2) Za režim pohybu osob v ZO s IS/V odpovídá příslušný bezpečnostní správce IS/V (dále jen „BS“) a jeho zástupce.

(3) Provozovatel IS/V schvaluje pověření/odvolání do/z role BS a uživatelů IS/V na návrh příslušného služebního funkcionáře.

(4) Seznamy uživatelů ZO s IS/V vede příslušný BS.

(5) Klíč od ZO s IS/V má k dispozici příslušný BS a dle potřeby jej vydává oprávněným zaměstnancům, kteří zde vytváří, zpracovávají či ukládají utajované informace. Záložní klíče od ZO s IS/V jsou uloženy v administrativní budově GŘC u ostrahy areálu GŘC v zabezpečené schránce, na které je uveden jmenný seznam zaměstnanců, kteří jsou oprávněni ji vyzvednout.

(6) Přidělené uživatelské klíče od ZO s IS/V jsou v případě ukončení služebního nebo pracovního poměru, při přeložení na jiné pracoviště nebo při změně jejich pracovní nebo služební potřeby vráceny příslušnému BS.

(7) Klíče od úschovného objektu (dále jen „ÚO“) umístěného v ZO s IS/V jsou uloženy v zabezpečené schránce u příslušného BS, který je vydává dle potřeby pověřeným oprávněným zaměstnancům. V době nepřítomnosti BS jsou klíče uloženy a vydávány jeho zástupcem.

(8) Úklid místností ZO se provádí smluvní externí úklidovou firmou, která bude předmětné práce vykonávat v pracovních dnech od 7:00 – 9:00 a 14:00 – 16:00 hod., a to vždy v přítomnosti příslušného oprávněného zaměstnance nebo BS.

(9) O zcizení či poškození výše uváděných klíčů musí být bezodkladně informován příslušný BS a ředitel bezpečnostního odboru.

ZÁVĚR

Význam a hodnota utajovaných informací neustále narůstá v závislosti na současné bezpečností situaci. Proto i nároky na jejich ochranu musí být adekvátně zvyšovány. Tyto nároky se nejčastěji promítají v úpravách legislativy, která ochranu UI upravuje. Nedostatky či nepřesnosti v právní úpravě ochrany UI jsou mnohdy známy, jejich nápravu a tím i riziko s ní však prodlužuje časová náročnost legislativních procesů.

V práci byla zpracována historická chronologie právní úpravy utajovaných informací na území České republiky spolu s analýzou zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Dále obsáhla analýzu působnosti vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. Ve druhé polovině práce byla představena metoda analýzy rizik a základní pojmosloví, které s touto oblastí úzce souvisí.

Na základě studia problematiky fyzické bezpečnosti UI autorka došla k závěru, že vědecký výzkum této oblasti není nutný. Je však žádoucí, aby se státní složky, které s UI pracují, aktivně zajímaly o trendy fyzické bezpečnosti a navzájem si mezi sebou předávaly praxí získané poznatky. Výměnu takovýchto poznatků je třeba provádět i na mezinárodní úrovni např. v rámci bezpečnostních konferencí. Vzhledem k rychlému vývoji technologií je zapotřebí neustálé sledování trhu s prostředky, pomocí kterých je fyzická bezpečnost zajišťována. Pouze tak je možné držet se aktuálních trendů a udržovat bezpečnost objektu na dobré úrovni. Na nutnost vyššího zájmu státních složek o trendy fyzické bezpečnosti poukazuje fakt, že fyzické zabezpečení UI, které se nachází v objektech podnikatelů, je mnohdy na znatelně lepší úrovni, než je možné vidět právě u státních složek.

Na základě získaných poznatků se autorka dále domnívá, že legislativa nedostatečně ošetřuje únik takových informací, které nenáleží do seznamů UI, ale jsou natolik citlivé, že jejich samovolné šíření není pro činnost orgánů veřejné moci výhodné. V úvahu by tedy připadalo řešení v podobě rozšíření seznamů UI o tyto informace, nebo vytvoření a implementace takových opatření, která by znemožňovala zaměstnancům státní správy takové informace dále beztrestně šířit. Jako sekundární prostředek proti úniku informací od zaměstnanců autorka navrhuje cílené zkoušky spolehlivosti, které by byly zaměřeny právě na infomační spolehlivost zaměstnanců. Obsah, struktura, míra provádění atd. jsou dostatečně obsáhlým tématem, kterým by se mohl někdo zabývat ve své bakalářské či diplomové práci.

Dále by autorka chtěla poukázat na zavádějící určení klasifikace utajované informace v nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. Vhodnější rozmezí utajení by dle autorčina názoru bylo např. „**žádné – V (případně D; T; PT)**“, neboť ne všechny informace, které jsou uvedeny v seznamech UI, musí být nutně utajovány.

Práce by mohla sloužit jako metodická opora těm, kteří v rámci výkonu svého zaměstnání vytváří režimová opatření a kteří se sestavováním takových opatření nemají předchozí zkušenosti. Stejný postup, který zvolila autorka k analýze rizik objektu a následné sestavení režimových opatření, může zvolit kdokoliv bez ohledu na to, zda režimová opatření vytváří pro objekt podnikatele, bezpečnostního sboru či jiné státní složky.

SEZNAM POUŽITÝCH ZDROJŮ

Literární zdroje

1. ANTUŠÁK, E. *Krizový management: hrozby – krize – příležitosti*. Praha: Wolters Kluwer Česká republika, 2009. 395 s. ISBN 978-80-7357-488-8.
2. ČERMÁK, M. *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009. 134 s. ISBN 978-80-7399-731-1.
3. DRASTICH, M. *Systém managementu bezpečnosti informací*. Praha: Grada, 2011. ISBN 978-80-247-4251-9.
4. KNÝ, M. a POŽÁR J. *Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti*. Brno: Tribun EU, 2010. 128 s. ISBN 978-80-7399-067-1.
5. POŽÁR, J. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. 309 s. ISBN 80-86898-38-5.
6. PROCHÁZKOVÁ, D. *Analýza a řízení rizik*. V Praze: České vysoké učení technické, 2011. 405 s. ISBN 978-80-01-04841-2.
7. PROCHÁZKOVÁ, D. *Strategické řízení bezpečnosti území a organizace*. V Praze: České vysoké učení technické, 2011. 483 s. ISBN 978-80-01-04844-3.
8. PROCHÁZKOVÁ, D. *Rizika spojená s pohromami a inženýrské postupy pro jejich zvládání*. V Praze: České vysoké učení technické, Fakulta dopravní, Ústav bezpečnostních technologií a inženýrství, c2013. 233 s. ISBN 978-80-01-05479-6.
9. PROCHÁZKOVÁ, D. *Ochrana osob a majetku*. V Praze: České vysoké učení technické, 2011. 301 s. ISBN 978-80-01-04843-6.
10. PROCHÁZKOVÁ, D. *Krizové řízení pro technické obory*. V Praze: České vysoké učení technické, 2013. 303 s. ISBN 978-80-01-05292-1.
11. ŠIMÁK, J., CIRKL B. *Trestní zákon: komentář k zákonu ze dne 12. července 1950, č. 86 Sb*. V Praze: Orbis, 1953. 596 s.

Elektronické zdroje

1. DRAKAS. *DRAKAS* [online]. 2016 [cit. 2017-02-09]. Dostupné z WWW: <http://www.drakas.cz/dotazy.html#utajovana>.
2. Národní bezpečnostní úřad. *Národní bezpečnostní úřad*. [online]. 2016 [cit. 2016-12-27]. Dostupné z WWW: <https://www.nbu.cz/cs/o-nas/o--nas/#otazka12>.

3. Národní bezpečnostní úřad. *Národní bezpečnostní úřad.* [online]. 2016 [cit. 2016-12-29]. Dostupné z WWW: <https://www.nbu.cz/cs/o-nas/o-nas/#otazka01>.
4. Národní bezpečnostní úřad. *Národní bezpečnostní úřad* [online]. 2017 [cit. 2017-02-10]. Dostupné z WWW: <https://www.nbu.cz/cs/bezpecnostni--zpusobilost/887-obecne-k-bezpecnostni-zpusobilosti/#doklad>.
5. Národní bezpečnostní úřad. *Národní bezpečnostní úřad* [online]. 2017 [cit. 2017-02-10]. Dostupné z WWW:<https://www.nbu.cz/cs/informacni-centrum/povinne-zverejnovane-informace/906-vyrocni-zpravy-o-cinnosti-nbu>.
6. Národní bezpečnostní úřad. *Národní bezpečnostní úřad* [online]. 2017 [cit. 2017-02-10]. Dostupné z WWW: <https://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost-oznameni-pro-v-osvedceni-d-t-pt-certifikaty/1045-osvedceni-fyzicke-osoby/>.
7. SVATOŠOVÁ, H. *Utajování versus základní práva a demokratické standardy* včetně *problematiky zbraní* [online]. Iuridicum remedium, 2005 [cit. 2016-12-29]. Dostupné z WWW: <http://www.iure.org/534579>.
8. VONDRUŠKA, P. *Cesta kryptografie do nového tisíciletí: od Kámasutry k osobním zápiskům K. H. Máchy*. [online]. Praha: Crypto-World, 2000 [cit. 2008-04-24]. Dostupné z WWW: <http://www.math.muni.cz/~bulik/vyuka/aplikace/vondruska-cesta.pdf>.

Legislativní dokumenty

1. Česko. Zákon č. 50/1923 Sb., na ochranu republiky. In *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.beck-online.cz/bo/chapterview--document.seam >.
2. Česko. Zákon č. 231/1948 Sb., na ochranu lidově demokratické republiky. In: *Sbírka zákonů České republiky*. Dostupné z WWW:<http://www.zakonyprolidi.cz/cs/1948--231>.
3. ČESKO. Zákon č. 140/1961 Sb., trestní zákon. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/1961-140>.
4. ČESKO. Zákon č. 102/1971 Sb., o ochraně státního tajemství. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/1971-102>.

5. ČESKO. Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/1998-148>.
6. ČESKO. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-412>.
7. ČESKO. Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-522>.
8. ČESKO. Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků. In: *Sbírka zákonů České republiky*. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2005-528>.

Ostatní zdroje

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

- některé z interních dokumentů Celní správy České republiky.

SEZNAM ZKRATEK

CÚ	Celní úřad
GŘC	Generální ředitelství cel
PČR	Policie České republiky
RTG	Rentgen

SEZNAM TABULEK, GRAFŮ A OBRÁZKŮ

Seznam grafů

Seznam obrázků

Seznam tabulek

PŘÍLOHY

Příloha I Vzor dokladu o bezpečnostní způsobilosti

Příloha č. 12 k vyhlášce č. 363/2011 Sb.

Vzor

NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD
Pošt. přihr. 49 150 06
Praha 56

D O K L A D

o bezpečnostní způsobilosti fyzické osoby
ČÍSLO:

Jméno a příjmení:

Rodné příjmení:

Datum narození: **Rodné číslo:**

Místo a stát narození:

Státní občanství:

Datum vydání: **Platnost od:** **Platnost do:**

Podpis oprávněného zástupce Národního bezpečnostního úřadu

Otisk úředního razítka Národního bezpečnostního úřadu

Příloha II Vzor osvědčení fyzické osoby

Příloha č. 7 k vyhlášce č. 363/2011 Sb.

Vzor

Označení subjektu
(uvede se název subjektu, který osvědčení vydal)

O S V Ě D Č E N Í

fyzické osoby

Certificate of Security Clearance/Certificat d´habiliation personnelle

ČÍSLO:

Number/Numéro

Jméno a příjmení
Name and Surname
Nom et prénom

Rodné příjmení
Maiden Name
Nom de naissance

Datum narození
Date of Birth
Date de naissance

Rodné číslo
Personal No.
Numéro d´ identification personnele

Místo narození
Place of Birth
Lieu de naissance

Státní občanství
Nationality
Nationalité

Stupeň utajení
Classification Level
Niveau de classification

Datum vydání
Date of Issue
Date de délivrance

Platnost od
Valid from
Validité á partir de

Platnost do
Date of Expiry
Date d´expiration

Podpis oprávněného zástupce
Signature of the Competent Representative
Signature du représentant autorisé

Otisk úředního razítka
Official Stamp/Cachet offciel

Příloha III Příklad seznamu UI

Příloha č. 2 k nařízení vlády č. 522/2005 Sb.

Seznam utajovaných informací v oblasti působnosti Ministerstva dopravy

Pořadové číslo	**Informace**	**Stupeň utajení**
1.	Strategické záměry hospodářského rozvoje dopravy, pokud obsahují údaje, které se týkají obrany a bezpečnosti státu nebo významných ekonomických zájmů státu	V
2.	Seznamy a související dokumentace dopravních staveb (objektů) důležitých pro obranu a bezpečnost státu	V
3.	Průběh a parametry železniční a silniční sítě důležité pro obranu a bezpečnost státu, včetně plánů jejich technické ochrany a obnovy, a interní předpisy s tím související	V
4.	Údaje k zajištění speciálních přeprav a interní předpisy s tím související	V – D
5.	Dokumentace ke krycím dokladům	V
6.	Způsob zabezpečení řidičských průkazů, osvědčení o registraci vozidla a tabulek s registračními značkami proti padělání a pozměňování	V
Oblast civilního letectví		
7.	Hodnoty nastavení detekčních schopností zařízení na detekci výbušnin, kovových předmětů a radioaktivních látek	V – D
8.	Výsledky akceptačních testů a zkoušek zařízení na detekci výbušnin, kovových předmětů a radioaktivních látek	V – D
9.	Podrobné údaje o výjimkách z technických parametrů a akceptačních testů zařízení podle bodů 7 a 8	V – D